



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Networks and Cybersecurity Essentials (ACCA4024)

Lab 7: Tools to check on Threats and Vulnerabilities

Cisco | **Networking Academy**[®]
| **Mind Wide Open**[™]

Objectives

Using Packet Capturing tools and network monitoring tools.

Tasks

1. Use Nmap to scan
- 2.

Required Resources

- PC with Ubuntu 16.0.4 LTS installed in a VirtualBox or VMware virtual machine. (*Alternatively, Any Linux Platform*)
- Internet Connection to refer the outcomes
- References: <https://nmap.org/>

Task 1

- ➔ Login as User Cisco.
- ➔ Go to Terminal and Type the following commands and examine
 - To do that we are using Nmap.
 - Network Mapper, or Nmap, is an open source utility used for network discovery and security auditing. Administrators also use Nmap for monitoring hosts or managing service upgrade schedules.
 - Nmap determines
 - what hosts are available on a network,
 - what services are running,
 - what operating systems are running,
 - What packet filters or firewalls are running?
 - So, basically if you could get all the above details using Nmap, you could get few information which could be used later in performing attacks or mitigating attacks.

➔ Commands to execute

○ Step 1:

▪ **nmap localhost**

(This is a scan performed to get information about the services that are bound to the localhost)

```
1 IP address.
127.0.0.1
map scan report for localhost (127.0.0.1)
Host is up ( 0.000099s latency)
Not shown: 997 closed ports
Port State Service
22/tcp open ssh
23/tcp open telnet
```

○ Step 2:

▪ **Replace the above command with your IP Address and other hosts (if connected/ else ignore) in your network to check the outcomes.**

Type the command you used to find out your host IP Address
ip addr show

Type the command you used to scan after finding your host IP Address
nmap 127.0.0.1

Record the outcomes of the above command here

```
nmap scan report for localhost (127.0.0.1)
Host is up ( 0.000099s latency)
Not shown: 997 closed ports
Port State Service
22/tcp open ssh
23/tcp open telnet
631/tcp open ipp
```

○ Step 3: Analyse the outputs/outcomes from Step 1 and 2 and record your reflections. (Hint: Analyse what is the difference between local host and ip address of the host, If ports displayed are different, Why is it different? etc (not limited to the hints))

On the nmap local host, 631/tcp is not displayed whereas on nmap 127.0.0.1 it is.

- Step 4: Why is the nmap scan only scans the first 1000 ports? What will be the command to scan all the ports?

nmap only scans the first 1000 ports as they are the most common and this makes it quicker. To scan all ports you could use `nmap -p-` followed by the IP address.

- Step 5: Scan the UDP Ports
 - **`nmap -sU localhost`**

(This is a scan performed to get information about the UDP ports and to execute this command you need root privileges. So, try)

- **`sudo nmap -sU localhost`**

Record the outcomes of the above command here (Hint: what UDP ports could you find open through your scan)

68, 631 & 5353

- Step 6: From the above outcomes select any ports which is open
 - **`sudo nmap -p137 localhost`**

(Change the port number 137 to any port which you found as open in the previous step (5).)

Record the outcomes of the above command here (Hint: Is the port open or closed? Why? Also, record the use of `-p` command)

```
sudo nmap -p68 localhost
```

State is closed.

- Step 7: Try other port related commands and record its purpose.
 - **`sudo nmap -pportnumber host_ip`**
 - **`sudo nmap -pportnumber_startrange-portnumber_endrange host_ip`**
 - **`sudo nmap -pportnumber,portnumber host_ip`**

- not limited to the above (*Do a google search, refine your search and find out other port related commands, Hint:nmap.org*)

Record the outcomes of the above commands here

```
sudo nmap -p63 127.0.0.1 - check status of port 63
sudo nmap -p63-100 127.0.0.1 - check ports 63 through 100
sudo nmap -p63,65,89 localhost - check ports 63, 65 & 89
```

- Step 8: Detecting the version is a very important part of information gathering. Try to find out the version.
 - **nmap -sV localhost**

Record the outcomes of the above commands here

```
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu1
23/tcp open telnet Linux telnetd
```

- Step 9: Try other commands to detect other versions and record its purpose.
 - Command to identify the Operating System version

Record the outcomes of the above commands here

```
hostnamectl
Ubuntu 16.04 LTS
```

- Command to identify the Service Version

Record the outcomes of the above commands here

```
nmap -sV 127.0.0.1
```

Learnings from tutorials so far:

Part 1 (Packet Tracer, Host Machines)

- ✓ *Build a home Network*
- ✓ *Understand and configure IP Address*
- ✓ *Use Ping/ Trace route Utility to check the connection status*
- ✓ *Use ipconfig /all command to determine the MAC address of a Windows computer on an Ethernet network.*
- ✓ *Analyze a MAC address to determine the manufacturer.*
- ✓ *Analyze the Wired and Wireless Network connection.*
- ✓ *Analyze Address Resolution Protocol (ARP).*
- ✓ *Connect to a Wireless Router and configure the basic settings in a wireless router and add security features.*
- ✓ *Use nslookup command to understand the url to ip conversion.*
- ✓ *Configure basic connectivity settings in Intermediate devices (Switch/ Router).*
- ✓ *Work with SBA Packet Tracer Files/ environment*
- ✓ *Configure ftp, web, email, dns, ntp and aaa Servers*

Part 2

- ✓ *Set up a virtual lab environment*
- ✓ *Troubleshooting the virtual lab environment*
- ✓ *Working with virtual machines*
- ✓ *Authentication, Authorization and Accounting*
- ✓ *Threats and Vulnerabilities – Using NMAP*



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Networks and Cybersecurity Essentials (ACCA4024)

Lab 8: Let's play Hide and Seek
(Steganography)

Cisco | **Networking Academy**[®]
| **Mind Wide Open**[™]

Objectives

Using open source steganography program to hide a document within an image file.

Tasks

1. Use Steghide to hide a data file within an image file

Required Resources

- PC with Ubuntu 16.0.4 LTS installed in a VirtualBox or VMware virtual machine. (*Alternatively, Any Linux Platform*)
- Internet Connection to refer the outcomes
- References: <http://steghide.sourceforge.net/>

Task 1

- ➔ Login as User Cisco.
- ➔ Go to Terminal and Type the following commands and examine
- ➔ Run Steghide program
 - `cisco@ubuntu:~$ cd Downloads/`
 - Enter libreoffice secret.odt & at the prompt to view the document.
 - `cisco@ubuntu:~/Downloads$ libreoffice secret.odt &`

Here, & is used to append the operation to run in background

What is the message in the secret.odt?

The secret document

- Enter gimp keyboard.jpg & at the prompt to view the image.
 - `cisco@ubuntu:~/Downloads$ gimp keyboard.jpg &`
- Enter the command to embed using steghide. The jpg file keyboard.jpg is used to embed the document secret.odt.
 - `cisco@ubuntu:~/Downloads$ steghide embed -cf keyboard.jpg -ef secret.odt`
 - It will ask for a passphrase, use Cisco.
 - Re-enter the passphrase when prompted.

You have embedded the document, secret.odt, into the image file, keyboard.jpg.

- Open the files, secret.odt and keyboard.jpg. Did these files change?

No visible change in libre or in GIMP.

➔ Extract the hidden file.

- To verify the hidden file.

- `cisco@ubuntu:~/Downloads$ steghide info keyboard.jpg`
- Type y at the prompt. (Do not press Enter).
- Enter the passphrase Cisco and press Enter.
- The results below shows that the file, secret.odt, is encrypted and compressed.

```
Enter passphrase:
embedded file "secret.odt":
size: 8.1 KB
encrypted: rijndael-128, cbc
compressed: yes
cisco@ubuntu:~/Downloads$
```

➔ Extract the hidden file.

- To extract the hidden file.

- `cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg`
- Enter the passphrase, Cisco, and press Enter.
- Enter y when prompted to overwrite the existing secret.odt file with the new extracted secret.odt file.

```
cisco@ubuntu:~/Downloads$ steghide extract -sf keyboard.jpg
Enter passphrase:
the file "secret.odt" does already exist. overwrite ? (y/n) y
wrote extracted data to "secret.odt".
```

You have extracted the file. Open the extracted secret.odt file with LibreOffice.

Could you open the file? Is the secret message the same as before?

Yes

➔ **Task 1 to complete.** I have shared an image file class1.jpg with you in Teams Channel. That file has a hidden message. What is that?

➔ You need a passphrase to extract the information. Find out the passphrase.

Hint: (6,6) (2,3) (5,4) (3,5) (10,3) (9,5) (8,2) (5,4)

1	2	3	4	5	6	7	8	9	10
2	a	e	e	r	;	j	o	h	j
3	p	a	r	r	r	t	r	t	d
4	c	r	a	s	l	a	r	m	g
5	v	a	d	k	k	e	r	r	f
6	h	u	g	a	w	a	m	n	d
7	k	l	a	h	q	q	w	a	s

Enter the text in the document here.....

one

- ➔ **Task 2 to complete.** Create your own file, hide it in an image and challenge your friends to find out the hidden text. Challenge at least one of your classmate via team's channel (one notebook platform) and accept one challenge.

Learnings from tutorials so far:

Part 1 (Packet Tracer, Host Machines)

- ✓ *Build a home Network*
- ✓ *Understand and configure IP Address*
- ✓ *Use Ping/ Trace route Utility to check the connection status*
- ✓ *Use ipconfig /all command to determine the MAC address of a Windows computer on an Ethernet network.*
- ✓ *Analyze a MAC address to determine the manufacturer.*
- ✓ *Analyze the Wired and Wireless Network connection.*
- ✓ *Analyze Address Resolution Protocol (ARP).*
- ✓ *Connect to a Wireless Router and configure the basic settings in a wireless router and add security features.*
- ✓ *Use nslookup command to understand the url to ip conversion.*
- ✓ *Configure basic connectivity settings in Intermediate devices (Switch/ Router).*
- ✓ *Work with SBA Packet Tracer Files/ environment*
- ✓ *Configure ftp, web, email, dns, ntp and aaa Servers*

Part 2

- ✓ *Set up a virtual lab environment*
- ✓ *Troubleshooting the virtual lab environment*
- ✓ *Working with virtual machines*
- ✓ *Authentication, Authorization and Accounting*
- ✓ *Threats and Vulnerabilities – Using NMAP*
- ✓ *Hide and Seek – Use Steghide to hide a data file within an image file*