**Lab #6 - Penetration Testing with Nmap**

1. **Lab Objectives**

At the end of this lab exercise, you will be able to:

* Get familiar with Nmap
* Understand and explain what Nmap is used for
* Perform basic penetration testing using Nmap
* Find vulnerabilities using Nmap

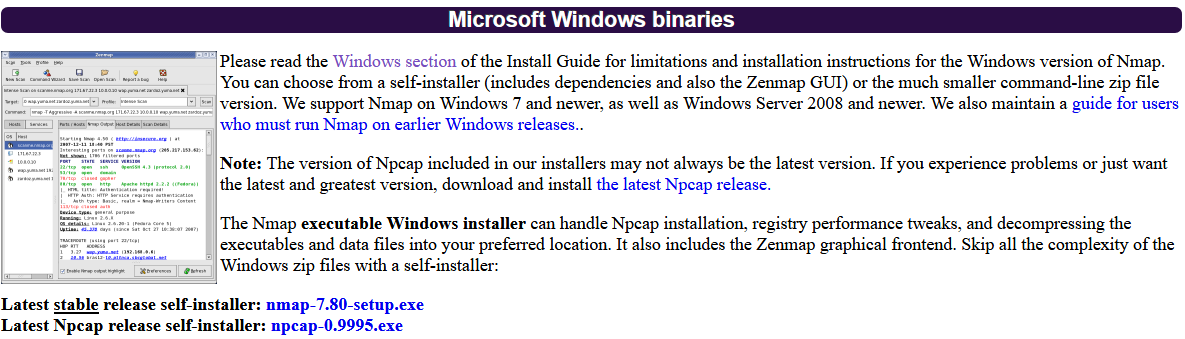
1. **Introduction**

Nmap or Network Mapper is an open source tool used for many purposes such as network discovery, device discovery and security auditing. In a nutshell, Nmap can be used to answer the following questions:

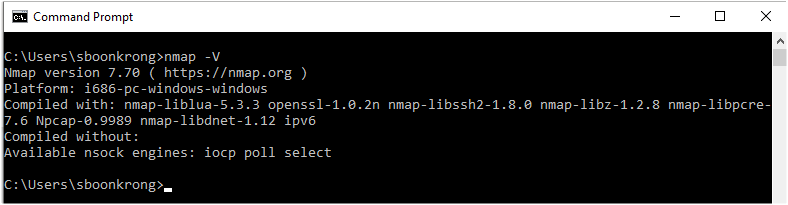
* What hosts are available on my network?
* What services is each host offering?
* What operating system is each host running?
* What are the vulnerabilities of each host (if any)?

1. **Nmap Installation**

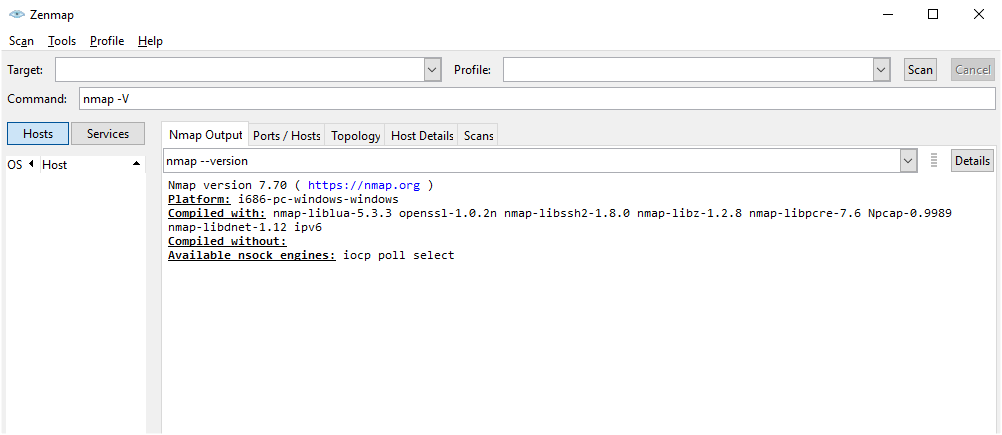
The first step is for you to acquire Nmap and install it on your system. If you use Windows, Nmap can be downloaded from https://nmap.org/download.html. However, if you run Kali Linux, Nmap should already be available for you.



Note that Nmap comes in two varieties. The first is the command line version.



The second comes with graphical interface and is known as Zenmap.



It does not matter which one you use, the commands are exactly the same. However, according to geek-university, Zenmap has the following advantages.

* Comparison – you can use Zenmap to graphically show the differences between two scans. This can help you to track new hosts or services appearing on their networks, or existing ones going down.
* Repeatability – you can use Zenmap’s command profiles to run the same scan more than once.
* Ease of use – Zenmap is easy to use and is especially useful for people without much experience in Linux shell.

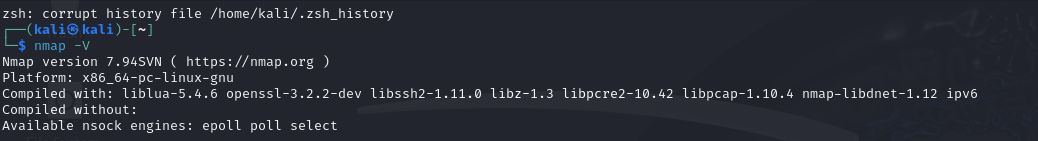
1. **Run Nmap**

Once you have installed Nmap, you need to test whether or not it can run properly on your system. For this lab, we will focus on the command-line version of Nmap. However, if you want to use Zenmap, you can, too.

You can check whether you freshly installed Nmap works by opening your Windows terminal and typing in the command: nmap -V, which will return the version of your Nmap.

**Task 1** – Issue the command nmap -V in the terminal. What do you see? (Capture your screen and paste it in the space provided.)

Insert your screen capture here: (1 Mark)



1. **Discover your IP address**

As you already know, there are two types of IP addresses. The first is the private addresses, which are used on a local network such as our home network and our organisation’s network. The second is the public addresses which are used in communications with the outside world or with other devices on the Internet.

**Task 2** – You are required to state what your machine’s IP address is.

The method I used to discover my private IP address was: (1 Mark)

ifconfig

My Private IP address is: (1 Mark)

10.0.2.15

The method I used to discover my public IP address was: (1 Mark)

curl ifconfig.me or

https://www.whatismyipaddress.com

My Public IP address is: (1 Mark)

IPv4: 203.158.1.35

IPv6: 2001:fb1:14c:7e4:3d6f:a4dc:ed3e:c8f4

1. **Nmap Basics**

Nmap can be used to scan a single host with an objective of finding out which ports are closed and which are open on that particular host. The command to be issued can simply be: nmap host.com

where *host.com* is the name of the host you want to scan, such as google.com. You can also use the IP address of the host in place of the name as

nmap abc.def.ghi.jkl

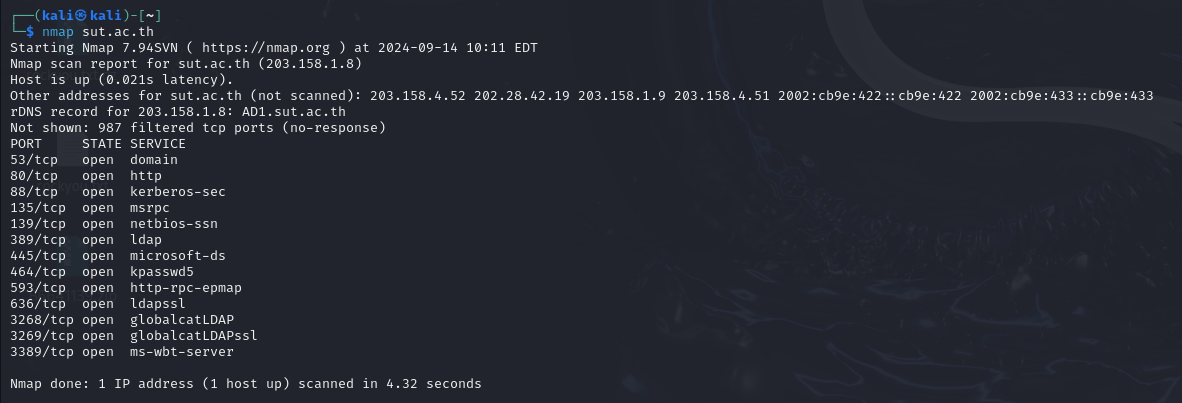
where abc.def.ghi.jkl is the IP address of the host, such as 192.168.1.1.

**Task 3** – Pick a host or IP address of your choice. It could be your own Web site or such host as *example.com* or *target.com*. Issue the command similar to the above. What do you see? (Capture or copy your screen and paste it in the space provided.)

The command I issued was: (1 Mark)

nmap sut.ac.th

The obtained result is: (1 Mark)



You can also add the -v option to the command. For example:

nmap -v host.com

**Task 4** – Use the same host as before. This time issue the command with the -v option. Answer the following question.

What do you think the -v option is used for? (1 Mark)

บอกรายละเอียดระดับข้อมูลเพิ่มเติม จากปกติที่เปิดแค่การเปิด-ปิดของ port

By issuing the above command, you should see the status of the scanned host. Nmap provides the information of which ports are open (and which are closed). Remember that the port numbers are used to identity the services that can be run on that particular host.

**Task 5** – Look at the result you obtained from scanning the host. Answer the following question.

How many ports are open on the host you scanned? (2 Marks)

13 port ที่เปิดอยู่มี 53/tcp , 80/tcp , 88/tcp , 135/tcp , 139/tcp , 389/tcp , 445/tcp, 464/tcp , 593/tcp , 636/tcp , 3268/tcp , 3269/tcp, 3389/tcp

What services are available on the host you scanned? (2 Marks)

Domain , http , kerberos-sec , msrpc , netbios-ssn , ldap , microsoft-ds , open kpasswd5 , http-rpc-epmap , ldapssl , globalcatLDAP , globalcatLDAPssl , ms-wbt-server

1. **Host Discovery**

In the previous section, you learned how to scan a host to see the status of its ports. This is also known as *port scanning*. However, there will be times when you only want to find out which hosts are up or alive on a particular network without wanting to know the status of the ports. Nmap allows you to do such thing by simple issuing the command:

nmap -sn host.com/24

where *host.com* is the name of the host (it could also be an IP address) and /24 is the subnet mask (it could be other numbers such as 28 depending on the class of the IP address). What this command does is that it will attempt to list the hosts that respond to the scan. This is sometimes known as the *ping scan*.

**Task 6** – Issue the command to discover live hosts on a network.

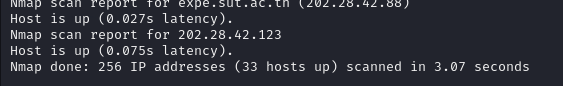
What command did you issue to carry out the ping scan? (1 Mark)

nmap -sn sut.ac.th/24

How many hosts are up or alive? (1 Mark)

256 IP addresses (33 hosts up)

Capture the screen to show the number of live hosts and paste it here. (1 Mark)



1. **Scanning a Specified Port**

It is possible for you to scan any particular port on any host in order to see whether or not that port is closed or open. For example, you may own several servers and you want to check the status of a port such as port 80 on each server. You can issue the command:

nmap -p 80 host.com

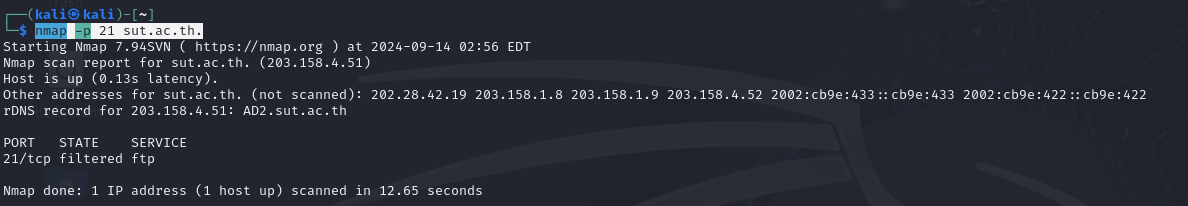
where *host.com* is the name of the host you want to scan. The -p option followed by a *number* tells Nmap to only scan for that particular port number.

**Task 7** – Use the same host as in previous exercises. Issue a command to check whether or not the following services are running: FTP, SSH, Telnet, HTTP and HTTPS.

The command I issued to check the FTP port was: (1 Mark)

nmap -p 21 sut.ac.th.

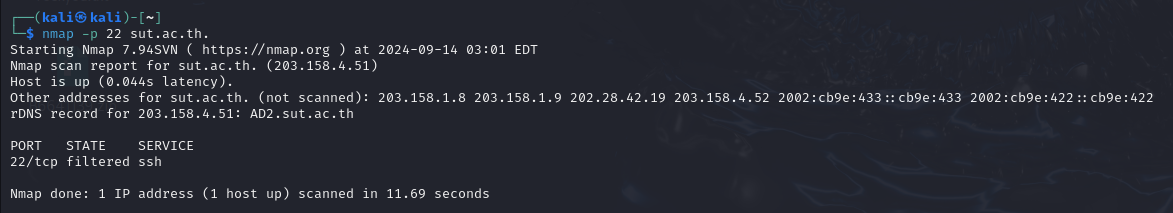
Is FTP port open or closed? (Paste your screen capture here) (1 Mark)



The command I issued to check the SSH port was: (1 Mark)

nmap -p 22 sut.ac.th.

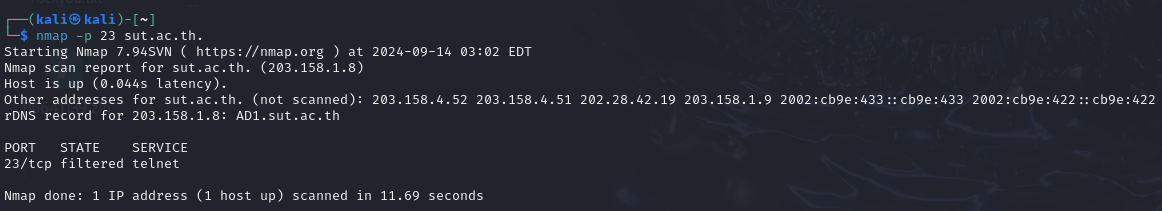
Is SSH port open or closed? (Paste your screen capture here) (1 Mark)



The command I issued to check the Telnet port was: (1 Mark)

nmap -p 23 sut.ac.th.

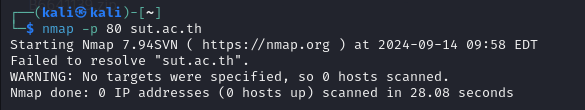
Is Telnet port open or closed? (Paste your screen capture here) (1 Mark)



The command I issued to check the HTTP port was: (1 Mark)

nmap -p 80 sut.ac.th

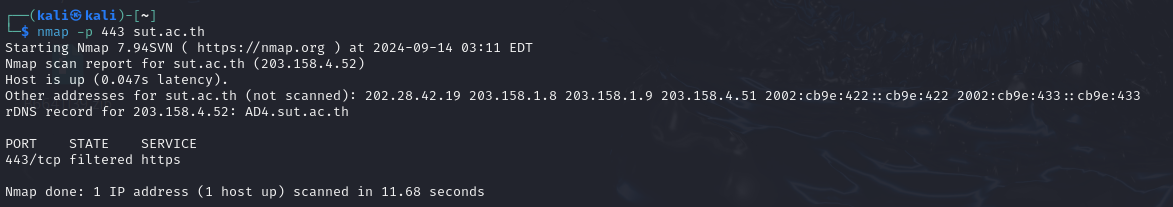
Is HTTP port open or closed? (Paste your screen capture here) (1 Mark)



The command I issued to check the HTTPS port was: (1 Mark)

nmap -p 443 sut.ac.th

Is HTTPS port open or closed? (Paste your screen capture here) (1 Mark)



1. **Operating System and Versions of the Running Services**

Nmap is a tool that not only tells you the status of the ports of a host. It also has the ability to inform you about the operating system running on that particular host and the version of each of the running services.

The reason you want to know about the operating system and service versions is because you can then use the obtained information to find out whether or not any of the installed software or operating system has a weakness and needs attention. The command you can use for finding the mentioned information is:

nmap -O -sV host.com

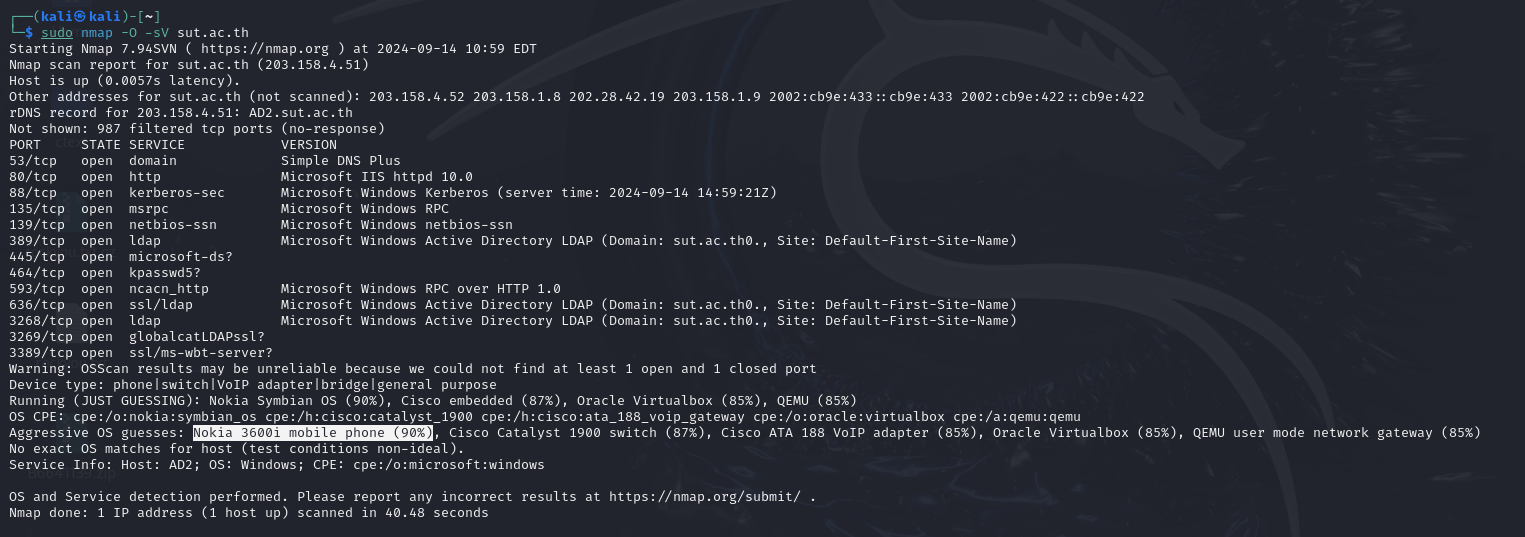
where *host.com* is the name of the host you are scanning. The -O option is the one that will inform you about the operating system installed on the host. The -sV will give you the detail of each running service on the host.

**Task 8** – Issue the above command to scan your selected host.

What command did you issue? (1 Mark)

sudo nmap -O -sV sut.ac.th

What did you see when you issued the command? (Place your screen capture here) (1 Mark)



What is the operating system installed on the scanned host? (1 Mark)

Nokia 3600i mobile phone

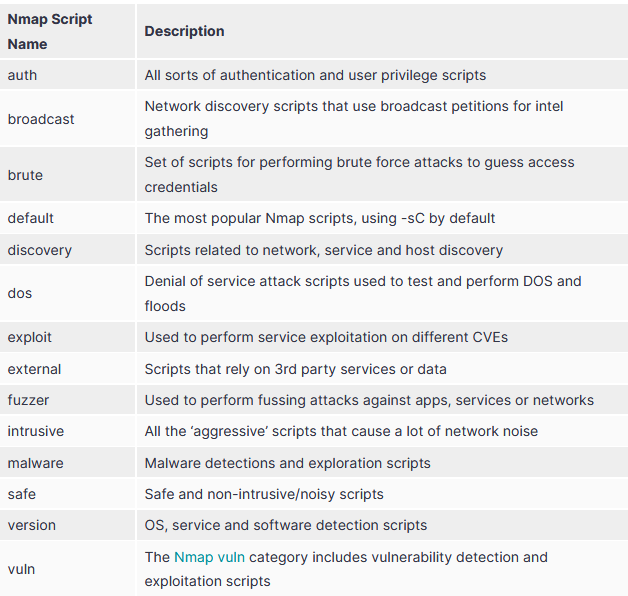
1. **Nmap Scripting Engine (NSE)**

You should have now grasped some basic Nmap commands and be ready for the next step of Nmap. This tool is very powerful especially when the scripting engine known as NSE is available. Nmap has already provided many ready-to-use options such as the ones you have used so far in this lab assignment. However, Nmap also allows you to create your own scripts to automate variety of tasks. One of those is, of course, vulnerability scanning.

Before you get into how you can run basic Nmap scripts, you should feel lucky that there are already many scripts (or NSE files) available for you to use. You can see what is available by going to the directory in which Nmap is installed and then opening the scripts folder.

NSE is grouped under many categories, which are:

(The NSE group table is taken from: https://securitytrails.com/blog/nmap-scripts-nse.)



NSE is activated with the -sC option. Many people, however, have opted to use the --script instead. That means if the command nmap -sC host.com is issued, the default scripts will be run. Similarly, the command nmap --script default host.com provides the same result.

Why don’t you try using the above command on your selected host and see what happens?

Since you know that there are many NSE groups, you can incorporate the group name into the script command, too. For example, if you want to carry out service discovery on a host, you can simply use the command:

nmap --script discovery host.com

Using the same command syntax, you can replace the discovery category with any NSE group you want.

If you want to be more specific, you can issue the command with any one script that you want to run. The names of the scripts can be found in the scripts directory. For example, if you want to run a brute force script to perform basic password auditing, the following command is to be issued:

nmap --script “http-brute” host.com

The phrase in the quote is the actual name of the nse file and can be replaced with any script name that you require. (Note that the above command is just an example and only works of the host requires authentication.)

Nmap allows you to run scripts using wildcards (\*), which means that you can run multiple scripts that contain any pattern in the names. For example, if you want to run any scripts beginning with the word http, you can use the command:

nmap --script “http-\*” host.com

Similarly, if you want to run the scripts that contain the word malware in the middle of the names, you can issue the command:

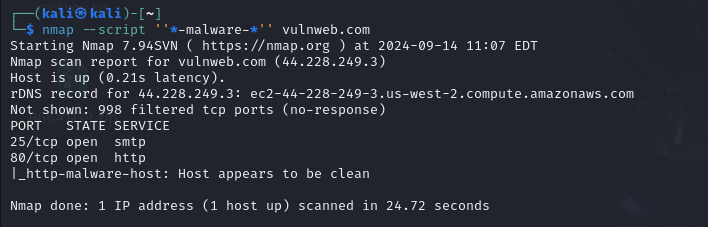
nmap --script “\*-malware-\*” host.com

**Task 9** - You are assigned to check whether or not vulnweb.com is infected with malware.

What command did you issue? (1 Mark)

nmap --script ''\*-malware-\*'' vulnweb.com

What did you see when you issued the command? (Place your screen capture here) (1 Mark)



Is the scanned host infected with any malware? (2 Marks)

ไม่ติด malware

1. **CVE Detection**

CVE stands for common vulnerabilities and exposures. CVE is usually associated with a number which provides a reference for known security vulnerability. For example, CVE-2014-0160 is a vulnerability called “Heartbleed” which is a weakness in older versions of OpenSSL. CVE-2018-8174 is a remote code execution flaw found in Internet Explorer. CVE or common vulnerabilities can be searched for at https://cve.mitre.org/cve/search\_cve\_list.html.

Why do you need to know that CVE is? The reason is that Nmap has the ability to scan for vulnerabilities on a specified host. Of course, the way to do it is the use NSE or Nmap scripting engine. This is known as vulnerability detection and can easily be done with the command:

nmap -v --script vuln host.com

Note that vuln is short for vulnerability and is one of the NSE groups.

**Task 10** - You are assigned to check whether there are any vulnerabilities on testphp.vulnweb.com Your job is to find out whether this site has any vulnerabilities.

What command did you issue? (1 Mark)

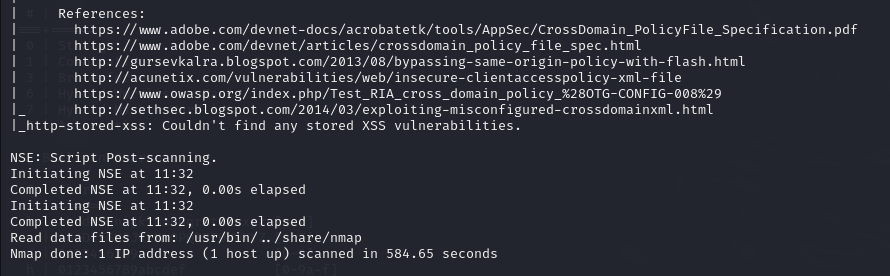
nmap -v --script vuln testphp.vulnweb.com

Does the scanned host contain any vulnerabilities? (Yes/No) (1 Mark)

No

If the site has vulnerabilities, capture your screen (the vulnerable parts) and put them here.

(1 Mark)



What are the vulnerabilities (if any)? Explain. (2 Marks)

ไม่พบช่องโหว่

**Task 11** - You are assigned to check whether there are any *SSL* vulnerabilities on manager.co.th Find out!

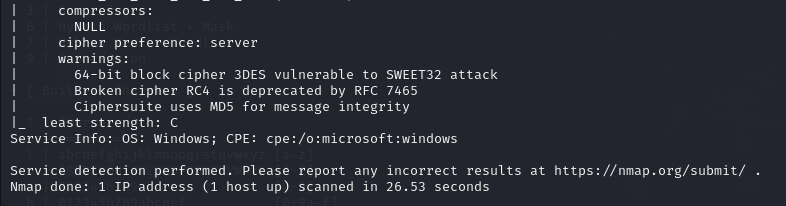
What command did you issue? (1 Mark)

nmap -sV -script ssl-enum-ciphers manager.co.th

Does the scanned host contain any SSL vulnerabilities? (Yes/No) (1 Mark)

Yes

Show the screen capture of the output. (1 Mark)



What does the output mean? Explain it to P’TA. (2 Marks)

มีการเข้ารหัสที่ไม่ปลอดภัย เช่น 3DES , RC4 , MD5 ดับความปลอดภัย "C" เป็นสัญญาณเตือนว่า ระบบการเข้ารหัสของserver มีความเสี่ยงสูงในการที่จถูกโจมตีจากผู้ไม่หวังดี

64-bit block cipher 3DES vulnerable to SWEET32 attack

Broken cipher RC4 is deprecated by RFC 7465

Ciphersuite uses MD5 for message integrity

**Task 12** – Another popular nmap vulnerability scanner script is known as *vulscan*. But the script is not included in the nse directory. Your task is to install the vulscan nse script. After you have installed it, use the vulscan script to scan [vulnweb.com](http://www.example.com)

|  |
| --- |
| Which command(s) did you use to install the vulscan nse script?  git clone https://github.com/scipag/vulscan.git  Which command did you use to scan [vulnweb.com](http://www.example.com) with vulscan script?  nmap -p 80,443,8080 -sV --script=vulscan/vulscan.nse vulnweb.com  Did you find any vulnerabilties? (You can show your findings by using the screen capture.) |

**Task 13** - You are asked to pick a host or a domain. You will then run nmap in order to find as much information about the selected host as possible. Your task is to write a report explaining what you do and what you find. (You can also capture your screen and put it as a part of your findings.)

|  |
| --- |
| 13.1 Which host did you choose to scan?  https://elearning2.sut.ac.th/  13.2 Why did you choose that host?    เพราะว่าเป็นเว็บไซต์ที่เข้าใช้งานทุกวัน และต้องใช้รหัสผ่านเข้าทุกครั้งที่ใช้  13.3 Which commands did you issue to scan the host?  nmap -v -script vuln -d elearning2.sut.ac.th  13.4 What did you find? Explain your findings to P’TA in details.    ไม่พบช่องโหว่ |

Congratulations. You have reached the end of this basic Nmap lab. You should be able to carry out simple scans using basic Nmap commands. There are many resources where you can learn more about Nmap. The one I recommend is <https://nmap.org/book/man.html>