Nmap tehtävä

Tavoite: Tutustua Nmap-ohjelman perusteisiin, ominaisuuksiin ja peruskäyttöön

OSA 1

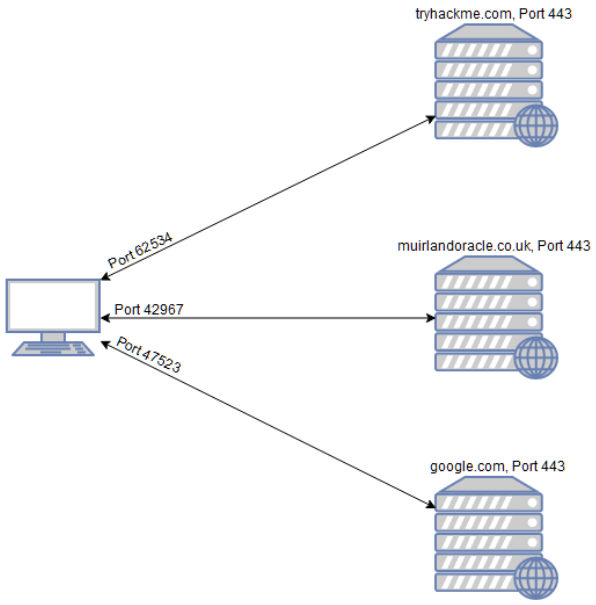
Lue aluksi oheiset TryHackMe.com Nmap-harjoitusmateriaaleista peräisin olevat tekstit.

Vastaa tämän jälkeen kysymyksiin, jotka liittyvät kyseisiin teksteihin tai tekstissä on ohjeet kysymyksiin vastaamiseksi.

Introduction

When it comes to hacking, knowledge is power. The more knowledge you have about a target system or network, the more options you have available. This makes it imperative that proper enumeration is carried out before any exploitation attempts are made.

Say we have been given an IP (or multiple IP addresses) to perform a security audit on. Before we do anything else, we need to get an idea of the "landscape" we are attacking. What this means is that we need to establish which services are running on the targets. For example, perhaps one of them is running a webserver, and another is acting as a Windows Active Directory Domain Controller. The first stage in establishing this "map" of the landscape is something called port scanning. When a computer runs a network service, it opens a networking construct called a "port" to receive the connection. Ports are necessary for making multiple network requests or having multiple services available. For example, when you load several webpages at once in a web browser, the program must have some way of determining which tab is loading which web page. This is done by establishing connections to the remote webservers using different ports on your local machine. Equally, if you want a server to be able to run more than one service (for example, perhaps you want your webserver to run both HTTP and HTTPS versions of the site), then you need some way to direct the traffic to the appropriate service. Once again, ports are the solution to this. Network connections are made between two ports – an open port listening on the server and a randomly selected port on your own computer. For example, when you connect to a web page, your computer may open port 49534 to connect to the server's port 443.



As in the previous example, the diagram shows what happens when you connect to numerous websites at the same time. Your computer opens up a different, high-numbered port (at random), which it uses for all its communications with the remote server.

Every computer has a total of 65535 available ports; however, many of these are registered as standard ports. For example, a HTTP Webservice can nearly always be found on port 80 of the server. A HTTPS Webservice can be found on port 443. Windows NETBIOS can be found on port 139 and SMB can be found on port 445. It is important to note; however, that especially in a CTF setting, it is not unheard of for even these standard ports to be altered, making it even more imperative that we perform appropriate enumeration on the target.

If we do not know which of these ports a server has open, then we do not have a hope of successfully attacking the target; thus, it is crucial that we begin any attack with a port scan. This can be accomplished in a variety of ways – usually using a tool called nmap, which is the focus of this room. Nmap can be used to perform many different kinds of port scan – the most common of these will be introduced in upcoming tasks; however, the basic theory is this: nmap will connect to each port of the target in turn. Depending on how the port responds, it can be determined as being open, closed, or filtered (usually by a firewall). Once we know which ports are open, we can then look at enumerating which services are running on each port – either manually, or more commonly using nmap.

So, why nmap? The short answer is that it's currently the industry standard for a reason: no other port scanning tool comes close to matching its functionality (although some newcomers are now matching it for speed). It is an extremely powerful tool – made even more powerful by its scripting engine which can be used to scan for vulnerabilities, and in some cases even perform the exploit directly! Once again, this will be covered more in upcoming tasks.

For now, it is important that you understand: what port scanning is; why it is necessary; and that nmap is the tool of choice for any kind of initial enumeration.

Questions:

1. What networking constructs are used to direct traffic to the right application on a server?

   ports

2. How many of these are available on any network-enabled computer?

   65535

3. **[Research]** How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)
   Hint: Search in Google "How many well-known ____ are there", substituting in your answer to Question 1.

   1023

Nmap Switches

Like most pentesting tools, nmap is run from the terminal. There are versions available for both Windows and Linux. For this room we will assume that you are using Linux; however, the switches should be identical. Nmap is installed by default in Kali Linux

Nmap can be accessed by typing nmap into the terminal command line, followed by some of the "switches" (command arguments which tell a program to do different things) we will be covering below.

All you will need for this is the help menu for nmap (accessed with nmap -h) and/or the nmap man page (access with man nmap). For each answer, include all parts of the switch unless otherwise specified. This includes the hyphen at the start (-).

Questions:

4. What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

-sS

5. Which switch would you use for a "UDP scan"?

-sU

6. If you wanted to detect which operating system the target is running on, which switch would you use?

-O

7. Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV

8. The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

-v

9. Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two? (Note: it's highly advisable to always use at least this option)

-vv

We should always save the output of our scans -- this means that we only need to run the scan once (reducing network traffic and thus chance of detection), and gives us a reference to use when writing reports for clients.

10. What switch would you use to save the nmap results in three major formats?

-oA

11. A very useful output format: how would you save results in a "grepable" format?

-oG

Sometimes the results we are getting just aren't enough. If we do not care about how loud we are, we can enable "aggressive" mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning.

12. How would you activate this setting?

-A

Nmap offers five levels of "timing" template. These are essentially used to increase the speed your scan runs at. Be careful though: higher speeds are noisier, and can incur errors!

13. How would you set the timing template to level 5?

-T5

We can also choose which port(s) to scan.

14. How would you tell nmap to only scan port 80?

-p80;

15. How would you tell nmap to scan ports 1000-1500?

-p1000-1500;

A very useful option that should not be ignored:

16. How would you tell nmap to scan all ports?

-p-

17. How would you activate a script from the nmap scripting library (lots more on this later!)?

--script

18. How would you activate all of the scripts in the "vuln" category?

Hint: There are two variants of this switch. One with a space, one with the equals sign.
The answer is 13 characters long

--script=vuln

OSA 2

Nmapin käyttöä käytännössä

Käynnistä kaikki labrasi koneet Win7, Win10 ja Kali Linux.
Varmista, että Win7 ja W10 koneilla on Xampissa ja siinä käynnissä ainakin Apache ja MySQL.
Kirjoita vastaukseesi mitä olet tekemässä, ota kuvaruudunkaappaus tai –kaappauksia tuloksista sekä lopuksi analysoi, mitä voit tuloksista päätellä. esim.
Win 7:lla
portti 80 = http-portti, mitä käyttää Apache. Täytyy olla avoinna, että www-palvelu voi toimia.

Voit vastata joko seuraavien kysymysten jälkeen tai tuottaa erillisen dokumentin ja palauttaa sen

19. Skannaa Nmapilla labraverkkoasi siten, että tuloksissa näkyy avoimet portit verkossa olevista laitteista.

Ideana saada avoimet portit labraverkossani olevista laitteista. Oikea komento on ” sudo nmap 10.117.48.0/24”.

```
┌──(noa㉿noa)-[~]
└─$ sudo nmap 10.117.48.0/24                                    1 ⚙
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-29 13:39 EET
Nmap scan report for 10.117.48.22
Host is up (0.00050s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 08:00:27:6E:FE:38 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.117.48.23
Host is up (0.00069s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 08:00:27:48:2F:11 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.117.48.30
Host is up (0.0000070s latency).
All 1000 scanned ports on 10.117.48.30 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 34.94 seconds

┌──(noa㉿noa)-[~]
└─$                                                             1 ⚙
```

Löydettiin molemmat windows koneet (.22 ja .23), ja niiltä portit 80 http yhteyttä varten, 443 https yhteyttä varten. Portti 3306 on MySql varten.

20. Skannaa Nmapilla labraverkkoasi siten, että tuloksissa näkyy myös käyttöjärjestelmä sekä ohjelmien nimi ja versio.

Ideana saada käyttöjärjestelmät, ohjelmien nimet ja versiot labraverkon koneista. Oikea komento on ”sudo nmap –O –sV 10.117.48.0/24”.

```
Nmap scan report for 10.117.48.22
Host is up (0.00057s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
443/tcp  open  ssl/http Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
3306/tcp open  mysql    MariaDB (unauthorized)
MAC Address: 08:00:27:6E:FE:38 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clo
sed port
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsof
t:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Micros
oft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
```

Windows-7 tietokoneen tulos.

```
Nmap scan report for 10.117.48.23
Host is up (0.00062s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
443/tcp  open  ssl/http Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
3306/tcp open  mysql    MariaDB (unauthorized)
MAC Address: 08:00:27:48:2F:11 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clo
sed port
Aggressive OS guesses: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Window
s 7 (93%), Microsoft Windows 10 1511 - 1607 (93%), Microsoft Windows Phone 7.5 or 8.0 (92%),
Microsoft Windows 10 1607 (92%), Microsoft Windows 10 1511 (92%), Microsoft Windows Server 20
08 R2 or Windows 8.1 (92%), Microsoft Windows Embedded Standard 7 (91%), Microsoft Windows Vi
sta SP2, Windows 7 SP1, or Windows Server 2008 (91%), Microsoft Windows Server 2016 (90%), Mi
crosoft Windows 7 Professional or Windows 8 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Windows-10 tietokoneen tulos.

Nmap tunnisti tietokoneiden käyttöjärjestelmät oikein versioiden kanssa.

21. Skannaa Nmapilla labraverkkostasi vain laitteiden http- ja https-portit

Ideana saada tietoon labraverkon http ja https portit. Oikea komento on ”sudo nmap –p http,https 10.117.48.0/24”

```
┌──(noa㉿noa)-[~]
└─$ sudo nmap -p http,https 10.117.48.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-29 13:58 EET
Nmap scan report for 10.117.48.22
Host is up (0.00038s latency).

PORT     STATE    SERVICE
80/tcp   open     http
443/tcp  open     https
8008/tcp filtered http
MAC Address: 08:00:27:6E:FE:38 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.117.48.23
Host is up (0.00064s latency).

PORT     STATE    SERVICE
80/tcp   open     http
443/tcp  open     https
8008/tcp filtered http
MAC Address: 08:00:27:48:2F:11 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.117.48.30
Host is up (0.000044s latency).

PORT     STATE  SERVICE
80/tcp   closed http
443/tcp  closed https
8008/tcp closed http

Nmap done: 256 IP addresses (3 hosts up) scanned in 30.38 seconds
```

Nähdään, että käytössä on vain muutama portti, jotka on varattu http tai https-yhteydelle.

22. Skannaa Nmapilla labraverkkosi laitteista vain yleiset UDP-portit

Ideana saada labraverkon laitteiden yleiset UDP portit tietoon. Oikea komento on ”sudo nmap –sU –p U:53 10.117.48.0/24

```
┌──(noa㉿noa)-[~]
└─$ sudo nmap -sU -p U:53 10.117.48.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-29 14:04 EET
Nmap scan report for 10.117.48.22
Host is up (0.00029s latency).

PORT   STATE         SERVICE
53/udp open|filtered domain
MAC Address: 08:00:27:6E:FE:38 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.117.48.23
Host is up (0.00049s latency).

PORT   STATE         SERVICE
53/udp open|filtered domain
MAC Address: 08:00:27:48:2F:11 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.117.48.30
Host is up (0.000075s latency).

PORT   STATE  SERVICE
53/udp closed domain

Nmap done: 256 IP addresses (3 hosts up) scanned in 28.27 seconds
```

23. Skannaa Nmapilla labraverkkoasi siten, että tuloksissa näkyy myös käyttöjärjestelmä, ohjelmien nimi ja versio sekä tallenna haun tulokset tekstitiedostoon

Ideana tallentaa labraverkon laitteista tieto niiden käyttöjärjestelmästä, ohjelmien nimistä ja versioista tekstitiedostoon. Oikea komento on ”sudo nmap –O –sV –oN /home/noa/hauntulos.txt 10.117.48.0/24”.

```
# Nmap 7.91 scan initiated Fri Jan 29 14:12:31 2021 as: nmap -O -sV -oN /home/noa/Työpöytä/hauntulos.txt 10.117.48.0/24
Nmap scan report for 10.117.48.22
Host is up (0.00062s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
443/tcp  open  ssl/http Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
3306/tcp open  mysql    MariaDB (unauthorized)
MAC Address: 08:00:27:6E:FE:38 (Oracle VirtualBox virtual NIC)
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 7|8|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_se
rver_2008::sp1
OS details: Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP
1, or Windows Server 2008
Network Distance: 1 hop

Nmap scan report for 10.117.48.23
Host is up (0.00059s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
443/tcp  open  ssl/http Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
3306/tcp open  mysql    MariaDB (unauthorized)
MAC Address: 08:00:27:48:2F:11 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1511 - 1607 (95%), Microsoft Windows Phone 7.5 or 8.0 (94%), Microsoft Windows 10 1607 (93%), Microsoft Windows 10 1511 (93%), Micr
osoft Windows Server 2008 R2 or Windows 8.1 (93%), Microsoft Windows Server 2016 (93%), Microsoft Windows 7 Professional or Windows 8 (93%), Microsoft Windows Vista SP0 or SP1
, Windows Server 2008 SP1, or Windows 7 (93%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (93%), Microsoft Windows Embedded Standard 7 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 10.117.48.30
Host is up (0.000055s latency).
All 1000 scanned ports on 10.117.48.30 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jan 29 14:13:24 2021 -- 256 IP addresses (3 hosts up) scanned in 54.09 seconds
```

Kuvankaappaus hauntulos.txt tiedostosta. Nähdään, että haun tulos on sama kuin aiemmin kuin aiemmin tehdyn haun tulos, nyt vain tallennettu tekstitiedostoon terminal-ikkunan lisäksi.