IT 250 Fundamentals of Information Assurance and Security

Assignment 6 – Host Hardening and Firewalls

Objective: To improve security of Windows host through various hardening steps.

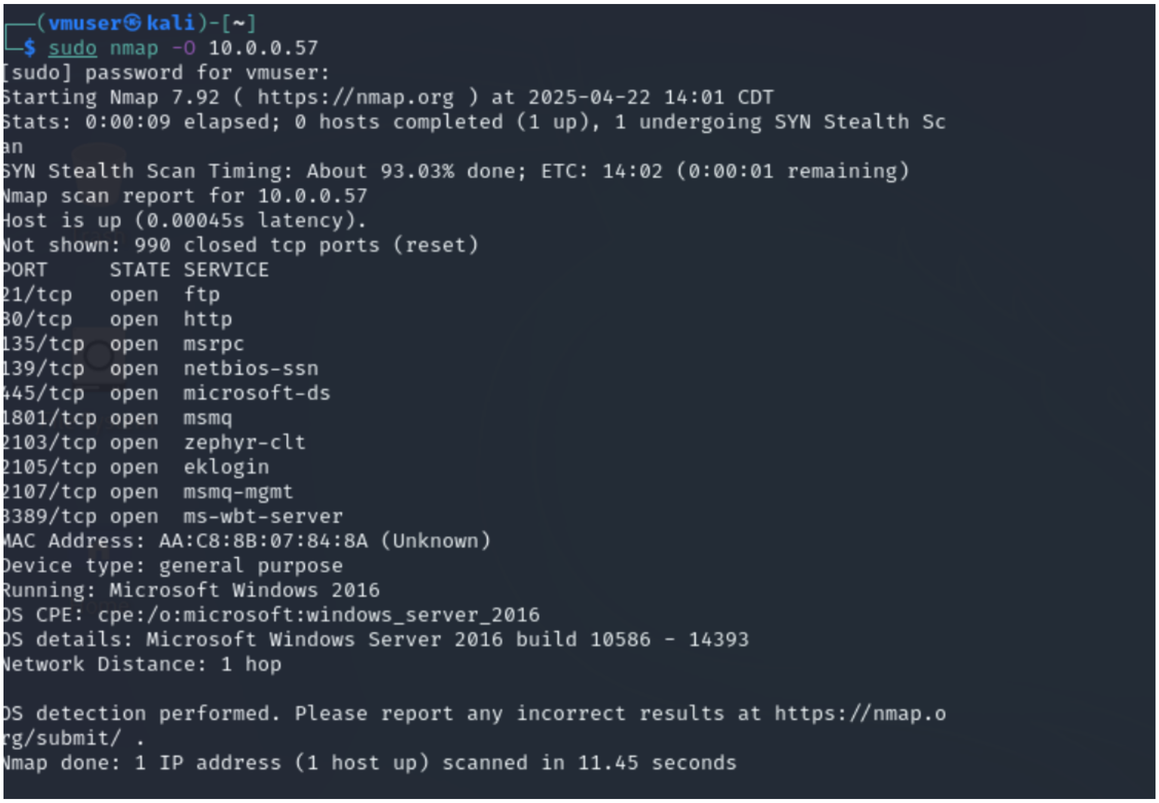
Part 1: Use Nmap tool to scan a host for its operating system, open ports and services running on these ports.

Nmap® is a well-known port scanner that has been around for many years and is available on a variety of operating systems. It has a GUI interface that makes it user-friendly. Nmap can tell you which operating system a machine is running, which services are available, and can give you a graphical representation of a network. Nmap has long been an industry staple for IT security professionals.

Warning: Remember to scan ONLY your own computers or machines designated by your instructor. Many organizations (corporations, governments, universities, etc.) have intrusion detection systems that will notice these scans.

We will use Nmap install on Kali Linux VM. Login to Kali Linux VM and open a terminal. Use this reference for Nmap commands https://linux.die.net/man/1/nmap.

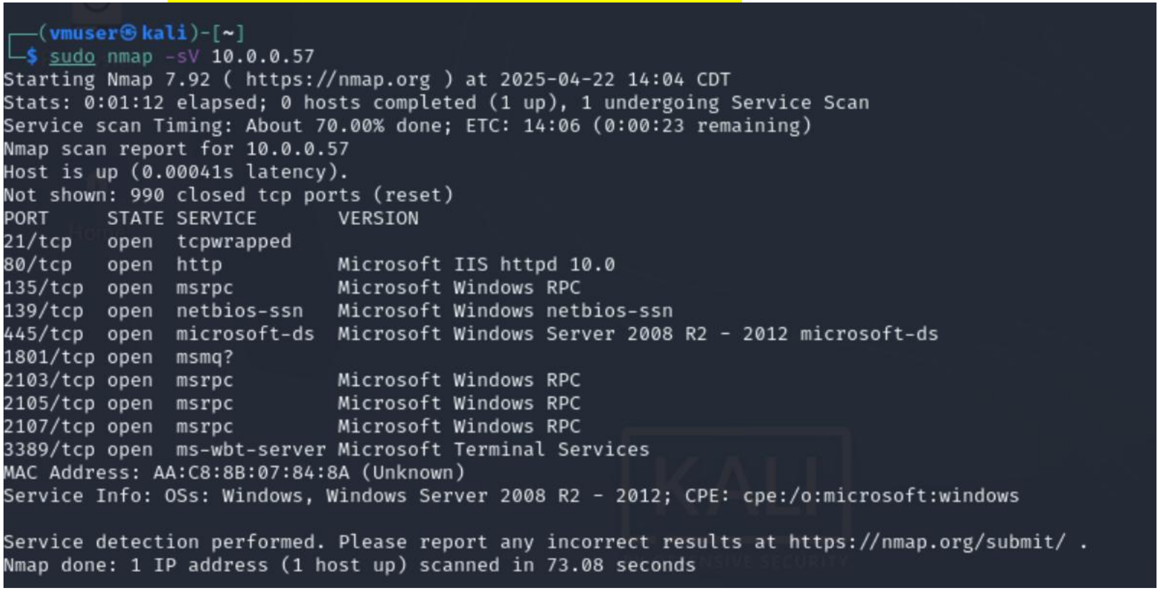
1. Type the command “sudo nmap -O *your Windows Server 2016 VM IP*” directly into the command box. Replace the IP address in the command. The -O switch will try to guess the Operating System and version of the OS of the target. Keeping the same value for the target, click the “Scan” button to start the scan. Insert a screen shot of the scan results here. (3 pts)



```
┌──(vmuser㉿kali)-[~]
└─$ sudo nmap -O 10.0.0.57
[sudo] password for vmuser:
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-22 14:01 CDT
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 93.03% done; ETC: 14:02 (0:00:01 remaining)
Nmap scan report for 10.0.0.57
Host is up (0.00045s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
MAC Address: AA:C8:8B:07:84:8A (Unknown)
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.45 seconds
```

2. Type the command "sudo nmap -sV *your Windows Server 2016 VM IP*" directly into the command box. This will try to guess the open ports and services running on those ports. Insert a screen shot of the scan results here. (3 pts)



```
┌──(vmuser㉿kali)-[~]
└─$ sudo nmap -sV 10.0.0.57
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-22 14:04 CDT
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 70.00% done; ETC: 14:06 (0:00:23 remaining)
Nmap scan report for 10.0.0.57
Host is up (0.00041s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  tcpwrapped
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: AA:C8:8B:07:84:8A (Unknown)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; 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 73.08 seconds
```

Question 1: What open application ports did you discover in the scan? What services do these ports correspond to? (3 pts)

The ports discovered in the scan are: 135/tcp, 139/tcp, 445/tcp, 593/tcp, 2103/tcp, 2107/tcp, 2108/tcp, 3389/tcp, 49664/tcp, 49665/tcp, 49666/tcp, 49667/tcp, 49668/tcp, 49669/tcp, 49670/tcp, and 49671/tcp. The services associated with these ports are msrpc, netbios-ssn, microsoft-ds, http-rpc-epmap, msrpc,msrpc, msrpc, msrpc, and then a series of dynamically assigned RPC ports.

Question 2: How might an attacker use the version information to attack a system? Briefly explain. (3 pts)
Attackers can use specific software version information to find and exploit known security weaknesses that are unique to that version.

Part 2: Perform vulnerability research on the host and patch the vulnerability.

1. Select a service and its corresponding version from the Nmap results in previous part. Navigate to the Common Vulnerabilities and Exposures Official Site at https://cve.mitre.org/ and select "Search CVE List".

2. Enter the name of the version of your selected service is running, for example, "OpenSSH 4.3". If multiple CVEs are found, choose one. The CVE provides information and resources about the vulnerability.

3. Click "Learn more at National Vulnerability Database" for more information and the CVSS score. Conduct research on your vulnerability by googling your CVE-ID. Some additional websites to check out as you research:
   a. https://www.rapid7.com/db/vulnerabilities/
   b. https://nvd.nist.gov/vuln/search
   c. https://www.cvedetails.com

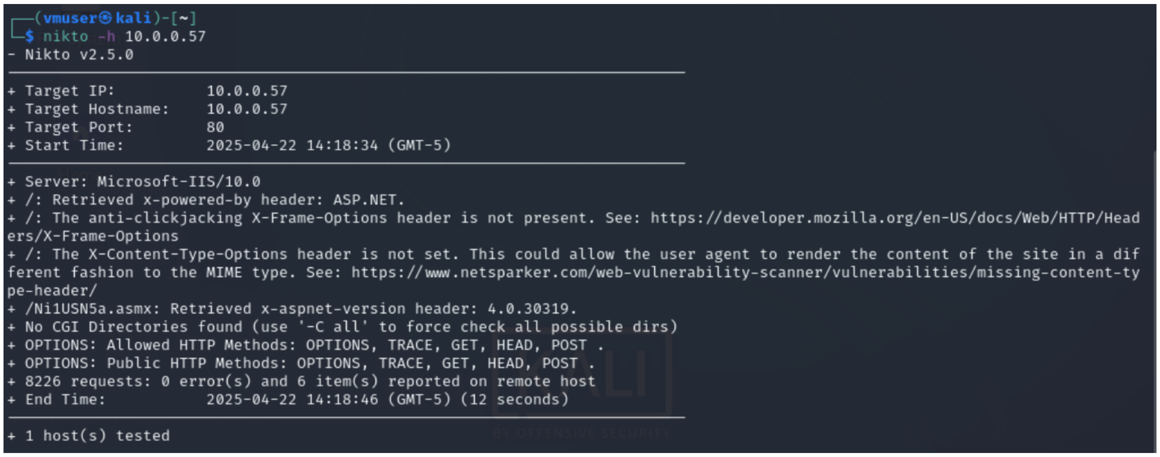
Question 3: Provide the CVE-ID that you chose and the vulnerability's CVSS Score. Explain the vulnerability briefly and how an attacker might use it to exploit a system. Is there a patch for your vulnerability? List the URL where you found the patch. (3 pts)
CVE-ID Chosen: CVE-2021-41773 7.5 score. This vulnerability in Apache HTTP Server 2.4.49 allows path traversal and remote code execution if CGI is enabled. an attacker can exploit it to access sensitive files or run commands on the server. patched in version 2.4.51. https://httpd.apache.org/security/vulnerabilities_24.html

4. Use an automated vulnerability scanning tool such as Nikto available in Kali Linux to find vulnerabilities in a host. Nikto scans web-based applications and web servers for known bad files that could potentially be dangerous. Other things that it can detect include outdated configs, port scanning, username enumeration and more. Use the

following command from the terminal to scan vulnerabilities in the Window server 2016 webserver

nikto -h *your Windows Server 2016 VM IP*

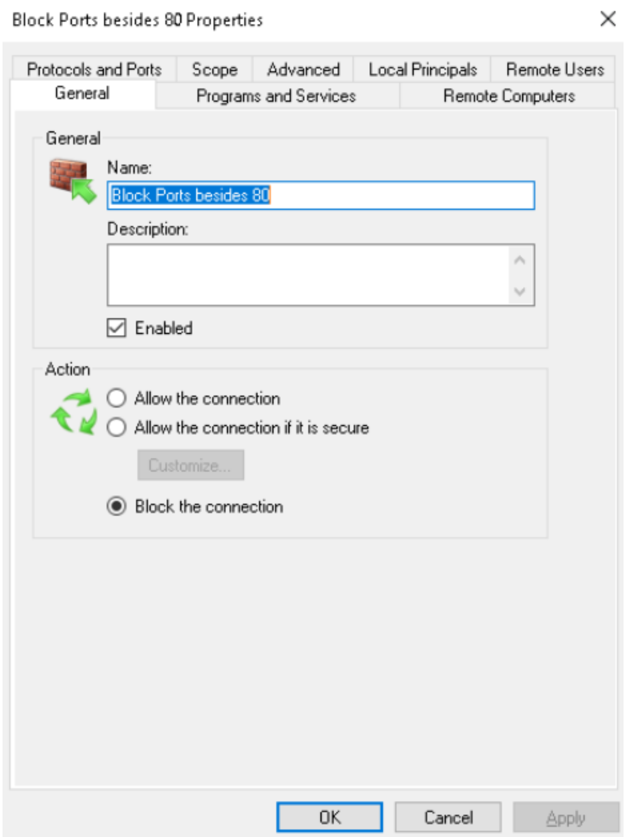
Insert a screenshot here of the results from this tool. What vulnerabilities did you discover? (3 pts)



```
┌──(vmuser㉿kali)-[~]
└─$ nikto -h 10.0.0.57
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.0.57
+ Target Hostname:    10.0.0.57
+ Target Port:        80
+ Start Time:         2025-04-22 14:18:34 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ /: Retrieved x-powered-by header: ASP.NET.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Head
ers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a dif
ferent fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-ty
pe-header/
+ /Ni1USN5a.asmx: Retrieved x-aspnet-version header: 4.0.30319.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ 8226 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-04-22 14:18:46 (GMT-5) (12 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Part 3: Minimize the number of services.

1. Close one of the network ports other than 80 from the Nmap results of Part 1. To do this you will have to either stop the relevant service or add a firewall rule. Add screen shot to show evidence. (3 pts).

2. 

General

Name: Block Ports besides 80

Description:

☑ Enabled

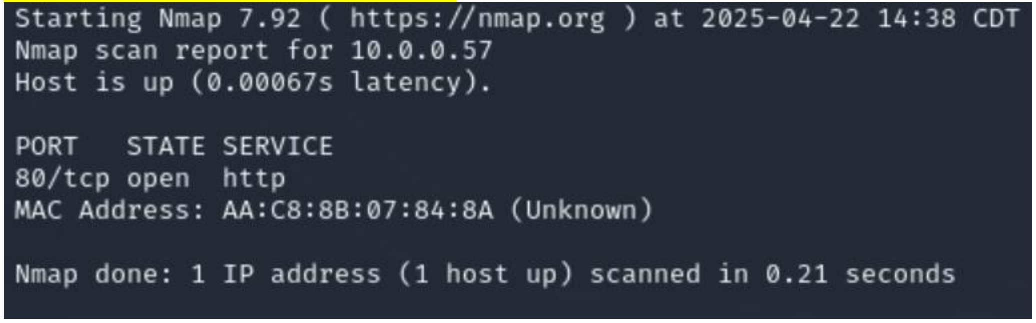
Action

○ Allow the connection

○ Allow the connection if it is secure

● Block the connection

3. Run Nmap from Kali Linux again (using Part 1) to show that the port it is closed. Add screen shot to show evidence. (3 pts).

4. 

```
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-22 14:38 CDT
Nmap scan report for 10.0.0.57
Host is up (0.00067s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: AA:C8:8B:07:84:8A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Part 4: In this part, you will practice port forwarding, which is an application of NAT that is used in a router/firewall to forward traffic from the Internet to internal hosts (with private IP), based on the destination port. E.g., to make a webserver on an internal host accessible from outside the LAN.
Open a web browser inside the Kali Linux VM and type the following in the URL address bar to ensure that you are able to access the movie scope website inside the LAN.
Windows Server 2016 VM IP/moviescope

Start your pfsense VM. Login to pfSense VM using user:admin and password:pfsense. Once logged in, from the menu then choose 3 to reset the web configurator password, and finally choose 11 to restart the web configurator

Now you will set up port forwarding on the pfSense router to access this website from outside the private LAN. You will use the web configurator tool for pfSense from inside Kali Linux VM to do this

Open browser inside Kali Linux VM and type the LAN IP address of the pfSense router in the URL address bar and open the web configuration page for pfSense. Login using username: admin and password: pfsense.

From the menu, go to Firewall -> NAT and under port forward add a new rule.

In Destination, choose WAN address.

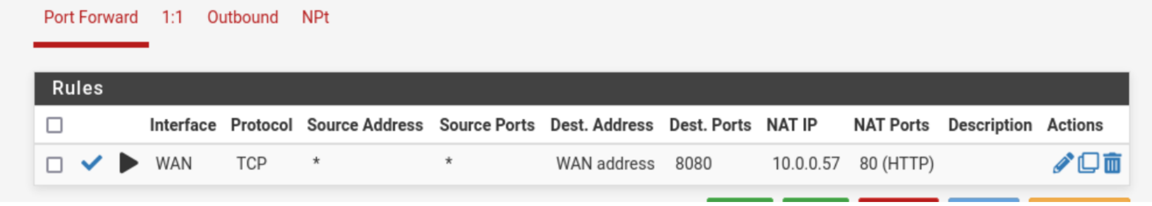
In Destination port range, select other and type 8080 in the custom textbox.

In redirect target IP, type *Windows Server 2016 VM IP*.

In redirect target port, choose HTTP.

In the filter rule association, select pass.

Click save and apply the rule. Take a screen shot showing that the rule was added, and insert it here: (3 pts)



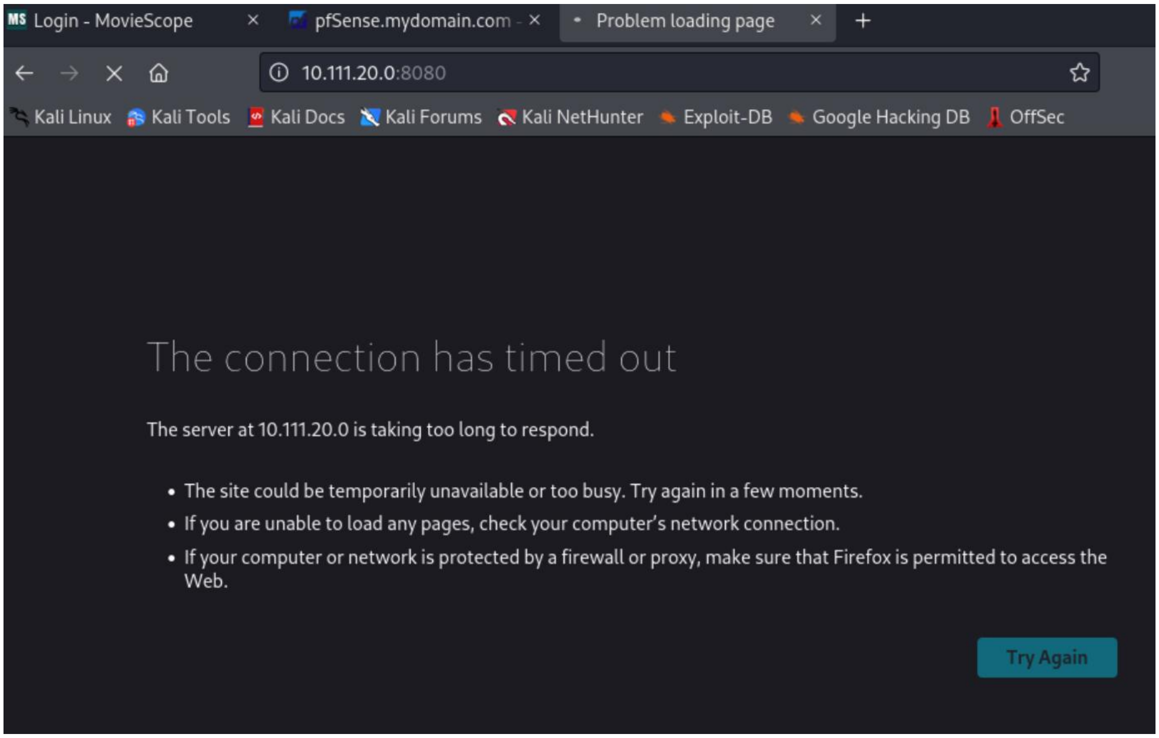
Rules

□		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓ ▶	WAN	TCP	*	*	WAN address	8080	10.0.0.57	80 (HTTP)		

To check that the rule works, try accessing the website from the Windows 10 VM outside the LAN. Login to the VM and open a browser and type the following in the URL address bar:

WAN IP address:8080

You can find the WAN IP address (Public IP) from the pfsense VM. Provide a screen shot showing the website is accessible: (3 pts)



The connection has timed out

The server at 10.111.20.0 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.