Executive Post Graduate Certification in Cyber Security and Ethical Hacking Project

Bhargav Rohit. D

23/01/25

Problem Statement: As a cybersecurity analyst entrusted with evaluating the security landscape of a client's network. Initial investigations reveal potential vulnerabilities in the network's file-sharing service. Your mission is to conduct a comprehensive network reconnaissance, identifying open communication channels and services in operation. Subsequently, delve into the exploration of the file-sharing infrastructure to extract crucial insights about the target environment.

Task to be Completed:

● Perform an exhaustive network reconnaissance leveraging Nmap to conduct an initial scan, thereby identifying open ports and active services within the target network/system. Subsequently, document the findings of the Nmap scan and discern potential targets for further enumeration. Additionally, based on the results obtained from Nmap, concentrate on scrutinizing the SMB service. Employ smbclient to establish connections with SMB shares and utilize enum4linux to collect pertinent information about the target's Windows environment

Scope: - The scope of this investigation is scanning network searching for service and port scanning using Nmap. I will focus on finding open or filtered ports, running service, OS. I will be then trying to access the sharable Folder (FTP) using smbclient to anonymously access files. Followed by enum4linux to collect pertinent information about the target's Windows environment

Limitation: - The whole testing will only be done on a controlled personal lab environment. The lab is specially configured to simulate the project to achieve the objective.

Target System/Network: Personal laboratory environment, fully authorized for testing. (WIN Server 2022).

Tools Used:

- Nmap
- smbclient
- enum4linux

Findings: -

Nmap: - Open-source tool used for network discovery and security auditing. It can scan large networks or single hosts and provide detailed information about the devices and services running on them. In simple words, it can scan those IP which are connected to internet.

In Nmap there are multiple options, we would use -A which would aggressively scan and present all the important details we need including OS, file permission of (FTP).

Here are the valid screen shots of my findings. We will be mainly focus on port relating to ftp (21) and smb (445) as it is the scope of this testing.

```
└─$ nmap -A 10.10.1.22 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-24 00:04 EST
Nmap scan report for 10.10.1.22
Host is up (0.00062s latency).
Not shown: 975 closed tcp ports (reset)
PORT     STATE SERVICE         VERSION
53/tcp   open  domain          Simple DNS Plus
80/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
88/tcp   open  kerberos-sec    Microsoft Windows Kerberos (server time: 2025-01-24 05:04:19Z)
111/tcp  open  rpcbind         2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|   100024  1           2049/udp6  status
```

Below is the FTP, with this we can understand ftp is open, so file transfer is taken place between the users.

```
2968/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-rw-   1 ftp      ftp          243 Oct 23  2023 .htaccess [NSE: writeable]
| -rwxrwxrwx   1 ftp      ftp          161 Oct 30  2023 bssfvr.bat [NSE: writeable]
| drw-rw-rw-   1 ftp      ftp            0 Oct 29  2023 HoneyBOT [NSE: writeable]
| drw-rw-rw-   1 ftp      ftp            0 Oct 22  2023 inetpub [NSE: writeable]
| drw-rw-rw-   1 ftp      ftp            0 May 08  2021 PerfLogs [NSE: writeable]
| dr--r--r--   1 ftp      ftp            0 Oct 22  2023 Program Files
| drw-rw-rw-   1 ftp      ftp            0 Jul 19  2024 Program Files (x86) [NSE: writeable]
| drw-rw-rw-   1 ftp      ftp            0 Oct 22  2023 SQLServer2017Media [NSE: writeable]
| dr--r--r--   1 ftp      ftp            0 Oct 22  2023 Users
| drw-rw-rw-   1 ftp      ftp            0 Oct 23  2023 wamp64 [NSE: writeable]
|_drw-rw-rw-   1 ftp      ftp            0 Oct 30  2023 Windows [NSE: writeable]
|_ftp-bounce: bounce working!
| ftp-syst:
```

```
└─$ nmap -A 10.10.1.22 -p 21 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-24 00:22 EST
Nmap scan report for 10.10.1.22
Host is up (0.00055s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
MAC Address: 00:0C:29:B3:3C:84 (VMware)
Warning: OSScan results may be unreliable because we could not find at
Device type: general purpose
Running: Microsoft Windows 2022
OS CPE: cpe:/o:microsoft:windows_server_2022
OS details: Microsoft Windows Server 2022
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.55 ms 10.10.1.22
```

Below are the target details such as Target name, domain names, OS which is Windows Server 2022, MAC address.

```
3389/tcp open  ms-wbt-server   Microsoft Terminal Services
|_ssl-date: 2025-01-24T05:07:20+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=SERVER2022.CEH.com
| Not valid before: 2024-12-25T13:45:08
|_Not valid after:  2025-06-26T13:45:08
| rdp-ntlm-info:
|   Target_Name: CEH
|   NetBIOS_Domain_Name: CEH
|   NetBIOS_Computer_Name: SERVER2022
|   DNS_Domain_Name: CEH.com
|   DNS_Computer_Name: SERVER2022.CEH.com
|   DNS_Tree_Name: CEH.com
|   Product_Version: 10.0.20348
|_  System_Time: 2025-01-24T05:06:52+00:00
```

```
MAC Address: 00:0C:29:B3:3C:84 (VMware)
Device type: general purpose
Running: Microsoft Windows 2022
OS CPE: cpe:/o:microsoft:windows_server_2022
OS details: Microsoft Windows Server 2022
Network Distance: 1 hop
Service Info: Host: SERVER2022; OS: Windows; CPE: cpe:/o:microsoft:windows
```

SMB port is open, now we can easily try to connect anonymously using smbclient to access the files or data.

```
445/tcp  open  microsoft-ds    Windows Server 2022 Standard Evaluation 20348 microsoft-ds (workgroup: CEH)
```

```
Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-time:
|   date: 2025-01-24T05:06:52
|_  start_date: N/A
|_nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:b3:3c:84 (VMware)
|_clock-skew: mean: 1h35m59s, deviation: 3h34m39s, median: 0s
| smb-os-discovery:
|   OS: Windows Server 2022 Standard Evaluation 20348 (Windows Server 2022 Standard Evaluation 6.3)
|   Computer name: SERVER2022
|   NetBIOS computer name: SERVER2022\x00
|   Domain name: CEH.com
|   Forest name: CEH.com
|   FQDN: SERVER2022.CEH.com
|_  System time: 2025-01-23T21:06:51-08:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.62 ms 10.10.1.22
```

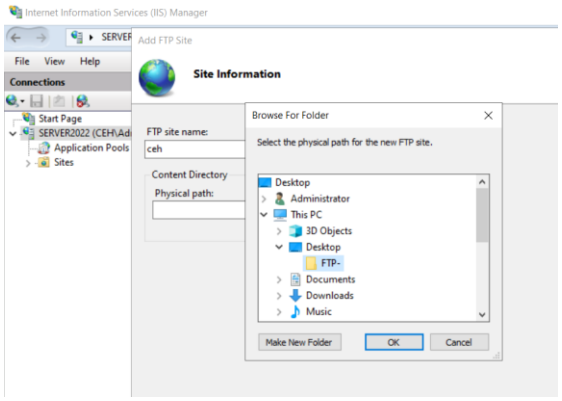
Configuring Windows environment: -

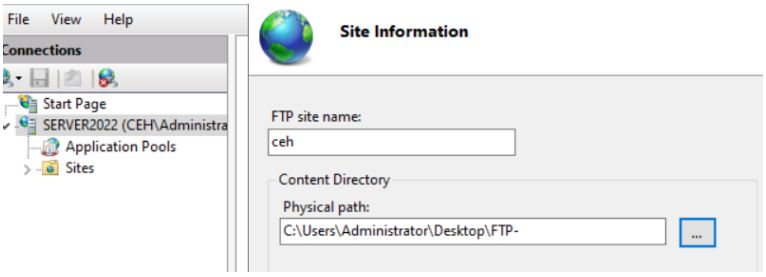
IIS Manager can also be used to enable file sharing and accessibility within connected computers through its FTP (File Transfer Protocol).

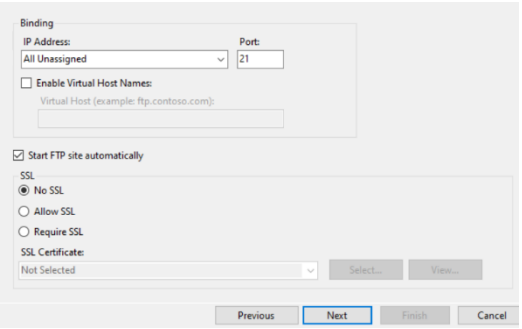
FTP allows you to set up an environment where files can be uploaded and downloaded securely. With IIS Manager, you can create and manage FTP sites to facilitate file exchanges within your network.

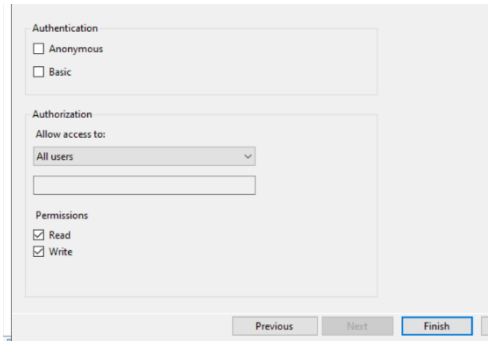
Open IIS and create a new FTP site, by double clicking over Sites and click on **Add FTP**

write a **name** as **CEH** and enter the **path** to **FTP-** folder. Follow the rest steps a in ss below.



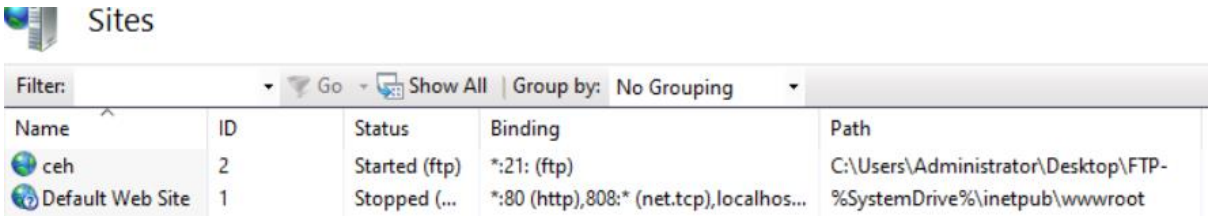






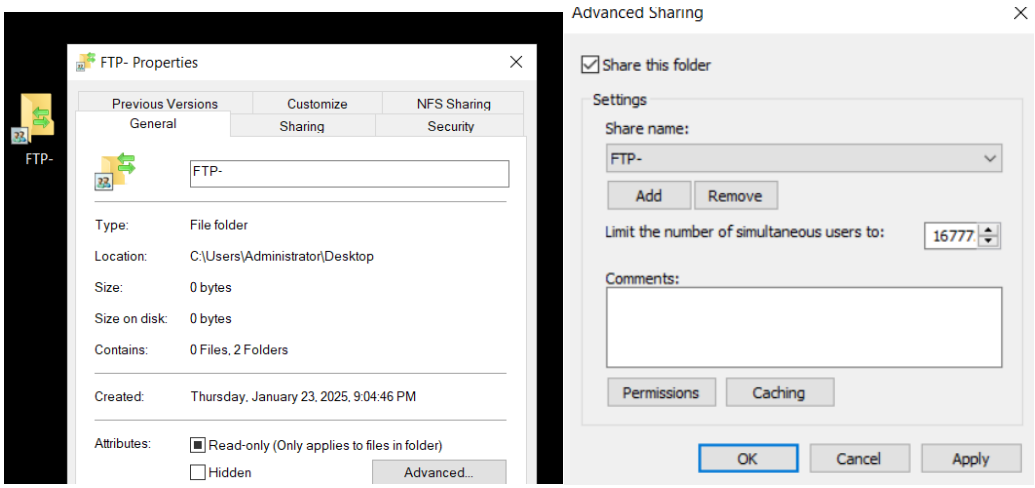
Press Finish.

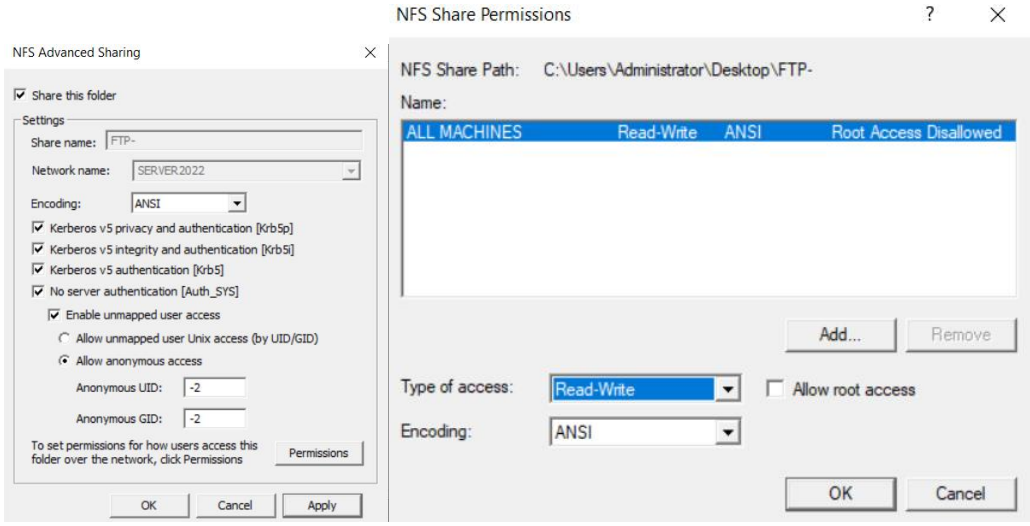
Click on Sites, to verify the status , weather the ftp is started or not, which in our case is started.



Previosly We added a path of FTP- above, which is a folder accessible to the users in a server.

Now, we will change the properties of this file to allow anonymous access, Read-write access to all users. This way, I can access FTP- file while enumerating SMB port using smbclient.





Smbclient : - **smbclient** is a command-line tool that provides an interface to communicate with SMB/CIFS servers. It's a part of the Samba suite and is used for various purposes related to file sharing and network resource management. I would use smbclient to access the file remotely. Enter the below command using smbclient.

```
└─$ smbclient //10.10.1.22/IPC$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
mkfifo         more           mput           newer          notify
open           posix          posix_encrypt  posix_open     posix_mkdir
posix_rmdir    posix_unlink   posix_whoami   print          prompt
put            pwd            q              queue          quit
readlink       rd             recurse        reget          rename
reput          rm             rmdir          showacls       setea
setmode        scopy          stat           symlink        tar
tarmode        timeout        translate      unlock         volume
vuid           wdel           logon          listconnect    showconnect
tcon           tdis           tid            utimes         logoff
..             !
```

quit by ctrl + c.

Reminder:- We previosly allowed anonymous access for the file above.

I will enter the -U option to provide username as CEH/Administrator. As soon as we enter the password, we get access to the target. By using ls we can list the data or files which is present. We suucessfly accessed the folder , as it has read-write option, I can modify according to the ease.

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.1.22/FTP- -U CEH/Administrator
Password for [CEH\Administrator]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Jan 24 00:04:46 2025
  ..                                 DR        0  Fri Jan 24 00:04:52 2025

                15568127 blocks of size 4096. 10552137 blocks available
smb: \> ls
  .                                   D        0  Fri Jan 24 03:41:59 2025
  ..                                 DR        0  Fri Jan 24 00:04:52 2025
  Managers' leaked mms                D        0  Fri Jan 24 03:41:45 2025
  snsitive data                       D        0  Fri Jan 24 03:41:30 2025

                15568127 blocks of size 4096. 10552133 blocks available
smb: \> SMBecho failed (NT_STATUS_CONNECTION_RESET). The connection is disconnected now
```

enum4linux: - To collect pertinent information of Windows server such as users, services, shares, domain names, Netstat, Password Policy, etc.

Enter the below command, -a for complete testing from user lists to password policy. Instead of entering options individually, we use -a instead.

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a 10.10.1.22
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jan 24 01:14:44 2025

 ========================================( Target Information )========================================

Target ........... 10.10.1.22
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.10.1.22 )============================


[+] Got domain/workgroup name: CEH


 ==============================( Nbtstat Information for 10.10.1.22 )==============================

Looking up status of 10.10.1.22
        SERVER2022      <00> -         B <ACTIVE>  Workstation Service
        CEH             <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        CEH             <1c> - <GROUP> B <ACTIVE>  Domain Controllers
        SERVER2022      <20> -         B <ACTIVE>  File Server Service
        CEH             <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
        CEH             <1b> -         B <ACTIVE>  Domain Master Browser
        CEH             <1d> -         B <ACTIVE>  Master Browser
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

        MAC Address = 00-0C-29-B3-3C-84
```

List of important services used for sharing files within users in network.

```
 ========================================( Getting domain SID for 10.10.1.22 )========================

Domain Name: CEH
Domain Sid: S-1-5-21-3011248926-652701544-240057437
```

```
 ==============================( Users on 10.10.1.22 )==============================

index: 0×edb RID: 0×1f5 acb: 0×00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest acce
in

user:[Guest] rid:[0×1f5]

 ==============================( Share Enumeration on 10.10.1.22 )==============================

do_connect: Connection to 10.10.1.22 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------

Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.1.22
```

No password policy is been set to this account, which means cracking passwords are easy as this is less secure server.

```
 ==========================( Password Policy Information for 10.10.1.22 )=====


[+] Attaching to 10.10.1.22 using a NULL share

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:10.10.1.22)

[+] Trying protocol 445/SMB ...

[+] Found domain(s):

        [+] CEH
        [+] Builtin

[+] Password Info for Domain: CEH

        [+] Minimum password length: None
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
```

List of all the Builtin groups: -

```
[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 0


 ========================================( Groups on 10.


[+] Getting builtin groups:

group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]
```

Below is the interesting findings which is users list. All the user name in this server are listed below. Using the user list, I can try to crack the passwords for the individuall account as there is no password policy used and high chances of using easy passwrods.

```
Group: Denied RODC Password Replication Group' (RID: 572) has member: Couldn't lookup SIDs

[+]  Getting domain groups:

group:[Enterprise Read-only Domain Controllers] rid:[0×1f2]
group:[Domain Users] rid:[0×201]
group:[Domain Guests] rid:[0×202]
group:[Domain Computers] rid:[0×203]
group:[Group Policy Creator Owners] rid:[0×208]
group:[Cloneable Domain Controllers] rid:[0×20a]
group:[Protected Users] rid:[0×20d]
group:[DnsUpdateProxy] rid:[0×44e]

[+]  Getting domain group memberships:

Group: 'Domain Users' (RID: 513) has member: CEH\Administrator
Group: 'Domain Users' (RID: 513) has member: CEH\krbtgt
Group: 'Domain Users' (RID: 513) has member: CEH\jason
Group: 'Domain Users' (RID: 513) has member: CEH\martin
Group: 'Domain Users' (RID: 513) has member: CEH\shiela
Group: 'Group Policy Creator Owners' (RID: 520) has member: CEH\Administrator
```

Conclusion: I will be concluding my findings by listing some security recommendation to strengthen security protocols. Overall, the test has a positive result, as I could achieve the objective that is scanning networks using Nmap for finding important clues, using it as a leverage for enumerate using **smbclient** and **enum4linux**.

Recommendation: -

- Close all the unwanted ports.
- Shutdown the service when not in use to avoid any breach or eaves dropping.
- Use of solutions offer RBAC.
- Inculcate MFA.
- Use good password policy.
- Restrict the read, write for the users according to role and not accessible to others.
- Restrict the file access to No to anonymous users rather than allowing all users.
- Use of good firewall, blocking the eaves drop for port scanning using Nmap.
- Use of solution which offer IDS and IPS with respect to a good configured firewall.
- Regular security patches.
- Restrict to sites which are safe and used as resource for the company.
- Blocking unwanted and phishing sites by implicating proxy.
- Educating employees the ill effects of security breach and how their action might affect the environment.

----------END----------