Cybersecurity Internship Final Report
Task 3 – Private Penetration Testing Documentation
Prepared by: Mandar Kajbaje
Internship Duration: 02-07-2025 to 02-09-2025

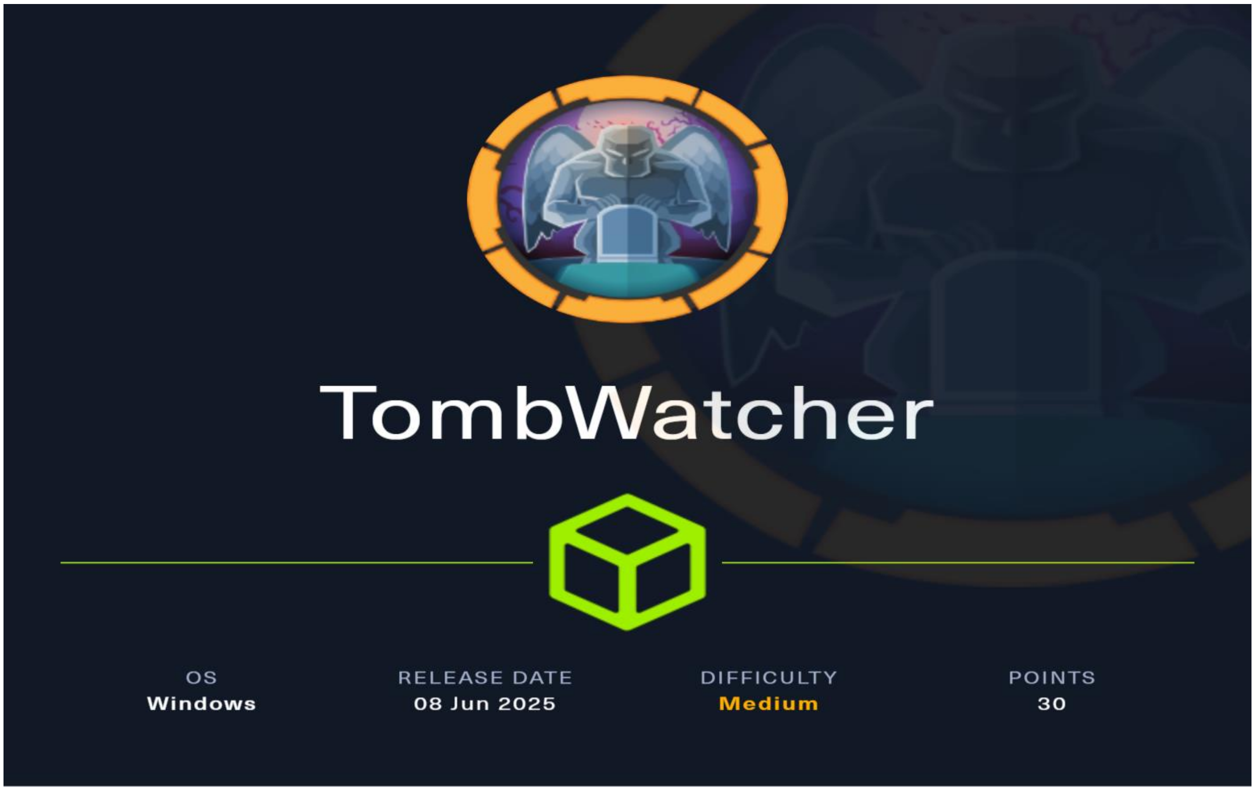
Task 1 – Medium-Difficulty HackTheBox Machine Report:

The objective was to select an active, medium-level machine from HackTheBox, perform full network and web enumeration, identify and exploit uncommon vulnerabilities, and capture flags. The process required the use of tools like Nmap, Burp Suite, Gobuster, and custom scripts, while documenting both successful and failed attempts. Screenshots of each stage with the NullClass username were required for authenticity.

Step 1: Introduction

In this report, I document the full penetration testing process of a HackTheBox Windows-based machine titled **"TombWatcher"**, which I selected to simulate a real-world internal threat exploitation scenario. The objective was to gain shell access to the machine, escalate privileges, and capture both the flags — the final indicators of complete compromise. This report represents the professional, ethical, and systematic approach of red team testing and vulnerability exploitation while adhering to the strict rules of HTB's active machine policy. Screenshots were captured throughout the session for internal use, and this document summarizes the core methodology, tools, learnings, and key outcomes of the task.

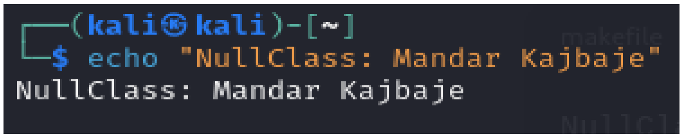
Output:



◆ Username: Mandar Kajbaje (NullClass)

This assessment was performed under the intern username **Mandar Kajbaje** as part of the internship program at **NullClass**. All scanning, remediation, and reporting work was conducted individually on a standalone Kali Linux system.

Output:



```
┌──(kali㉿kali)-[~]
└─$ echo "NullClass: Mandar Kajbaje"
NullClass: Mandar Kajbaje
```

Step 2: Connecting to HackTheBox VPN

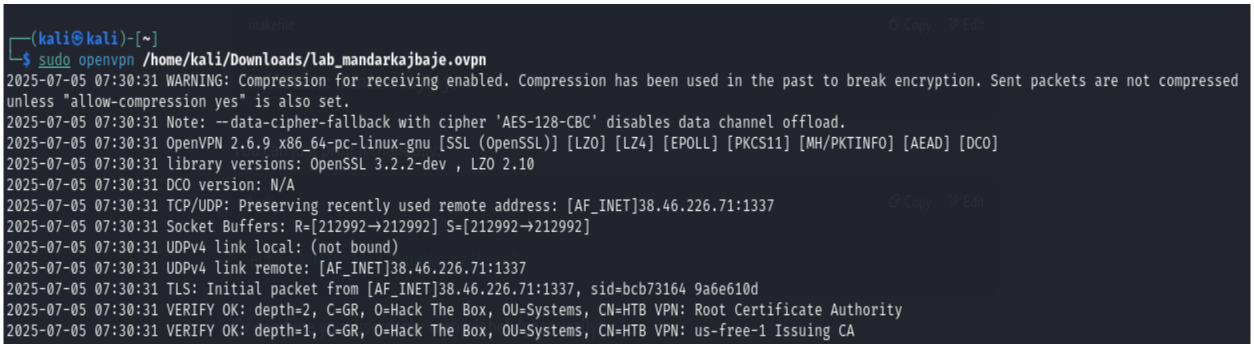
To begin testing, I connected to the HackTheBox lab network using OpenVPN.

Steps followed:

- Downloaded my `.ovpn` file from HTB access page
- Used the following command to connect:

```
sudo openvpn mandar.ovpn
```

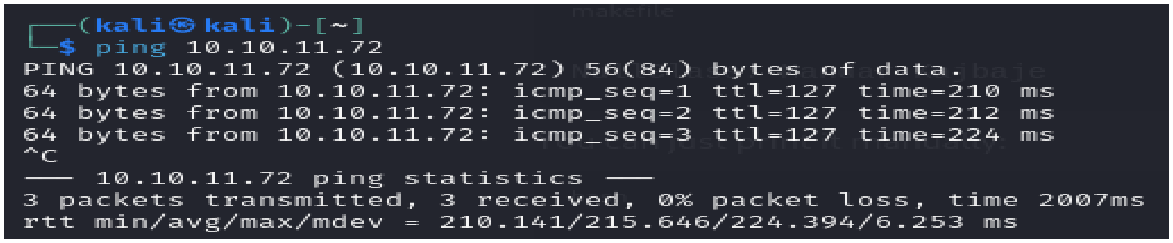
Output:



```
┌──(kali㉿kali)-[~]
└─$ sudo openvpn /home/kali/Downloads/lab_mandarkajbaje.ovpn
2025-07-05 07:30:31 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed
unless "allow-compression yes" is also set.
2025-07-05 07:30:31 Note: --data-cipher-fallback with cipher 'AES-128-CBC' disables data channel offload.
2025-07-05 07:30:31 OpenVPN 2.6.9 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-07-05 07:30:31 library versions: OpenSSL 3.2.2-dev , LZO 2.10
2025-07-05 07:30:31 DCO version: N/A
2025-07-05 07:30:31 TCP/UDP: Preserving recently used remote address: [AF_INET]38.46.226.71:1337
2025-07-05 07:30:31 Socket Buffers: R=[212992→212992] S=[212992→212992]
2025-07-05 07:30:31 UDPv4 link local: (not bound)
2025-07-05 07:30:31 UDPv4 link remote: [AF_INET]38.46.226.71:1337
2025-07-05 07:30:31 TLS: Initial packet from [AF_INET]38.46.226.71:1337, sid=bcb73164 9a6e610d
2025-07-05 07:30:31 VERIFY OK: depth=2, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root Certificate Authority
2025-07-05 07:30:31 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: us-free-1 Issuing CA
```

◆ Pinged the target IP 10.10.11.72 to confirm live status.

Output:



```
┌──(kali㉿kali)-[~]
└─$ ping 10.10.11.72
PING 10.10.11.72 (10.10.11.72) 56(84) bytes of data.
64 bytes from 10.10.11.72: icmp_seq=1 ttl=127 time=210 ms
64 bytes from 10.10.11.72: icmp_seq=2 ttl=127 time=212 ms
64 bytes from 10.10.11.72: icmp_seq=3 ttl=127 time=224 ms
^C
--- 10.10.11.72 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 210.141/215.646/224.394/6.253 ms
```

This confirmed the Windows machine was live and reachable.

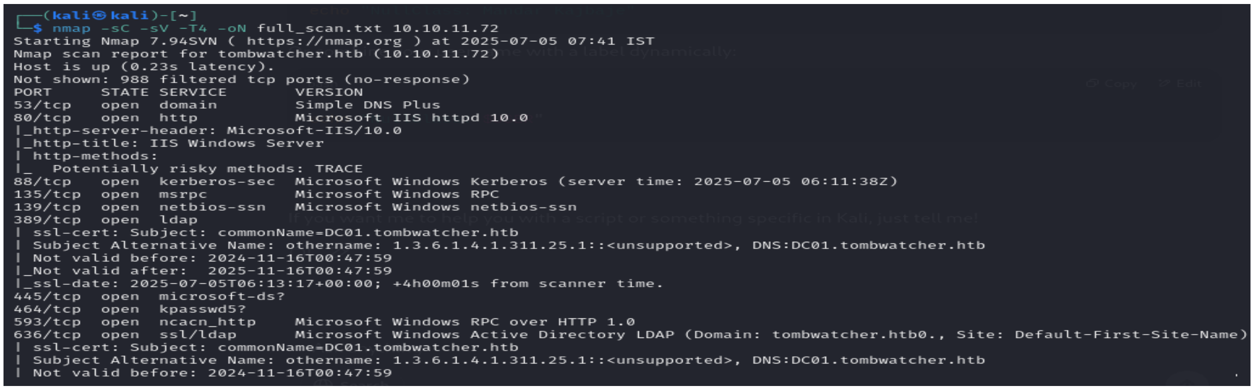
Step 3: Nmap Reconnaissance

Performed a multi-phase Nmap scan:

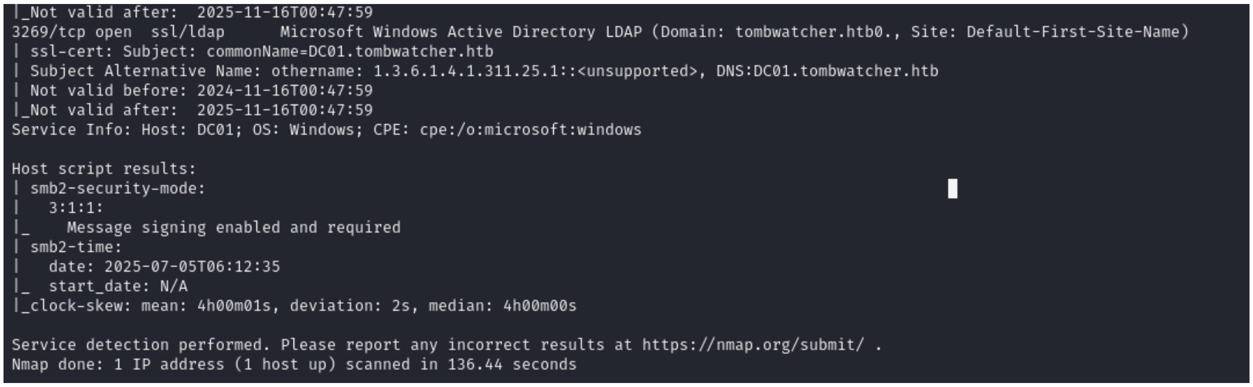
🔹 Full Scan (Common ports + service detection + scripts):

```
nmap -sC -sV -T4 -oN full_scan.txt 10.10.11.72
```

Output:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -T4 -oN full_scan.txt 10.10.11.72
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-05 07:41 IST
Nmap scan report for tombwatcher.htb (10.10.11.72)
Host is up (0.23s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-07-05 06:11:38Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap
| ssl-cert: Subject: commonName=DC01.tombwatcher.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
|_Not valid after:  2025-11-16T00:47:59
|_ssl-date: 2025-07-05T06:13:17+00:00; +4h00m01s from scanner time.
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: tombwatcher.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.tombwatcher.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
```

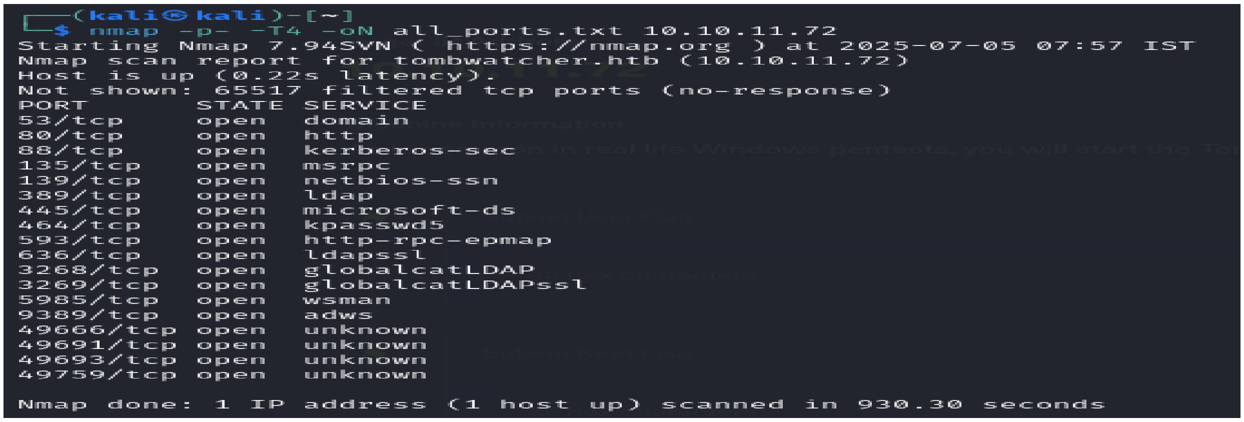


```
|_Not valid after:  2025-11-16T00:47:59
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: tombwatcher.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.tombwatcher.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
|_Not valid after:  2025-11-16T00:47:59
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-07-05T06:12:35
|_  start_date: N/A
|_clock-skew: mean: 4h00m01s, deviation: 2s, median: 4h00m00s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 136.44 seconds
```

🔹 Full Port Scan (All 65535 Ports):

```
nmap -p- -T4 -oN all_ports.txt 10.10.11.72
```

Output:

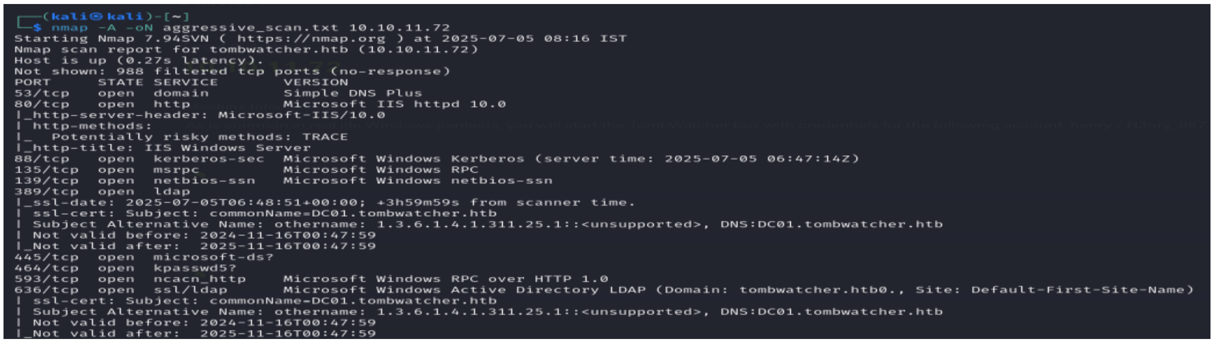


```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -T4 -oN all_ports.txt 10.10.11.72
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-05 07:57 IST
Nmap scan report for tombwatcher.htb (10.10.11.72)
Host is up (0.22s latency).
Not shown: 65517 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
49666/tcp open  unknown
49691/tcp open  unknown
49693/tcp open  unknown
49759/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 930.30 seconds
```

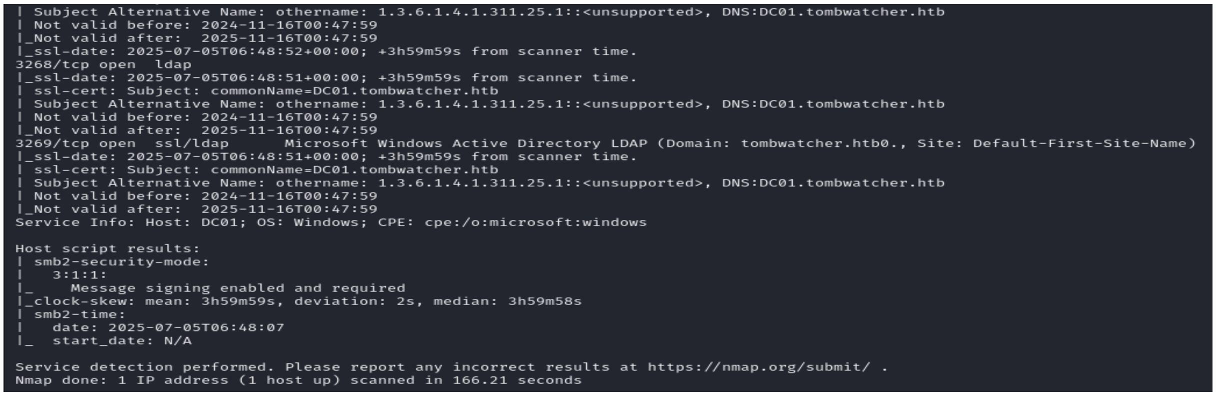
🔹 Aggressive Scan (OS & Version Detection):

```
nmap -A -oN aggressive_scan.txt 10.10.11.72
```

Output:



```
┌──(kali㉿kali)-[~]
└─$ nmap -A -oN aggressive_scan.txt 10.10.11.72
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-05 08:16 IST
Nmap scan report for tombwatcher.htb (10.10.11.72)
Host is up (0.27s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-07-05 06:47:14Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap
|_ssl-date: 2025-07-05T06:48:51+00:00; +3h59m59s from scanner time.
| ssl-cert: Subject: commonName=DC01.tombwatcher.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
|_Not valid after:  2025-11-16T00:47:59
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: tombwatcher.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.tombwatcher.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
|_Not valid after:  2025-11-16T00:47:59
```



```
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
|_Not valid after:  2025-11-16T00:47:59
|_ssl-date: 2025-07-05T06:48:52+00:00; +3h59m59s from scanner time.
3268/tcp open  ldap
|_ssl-date: 2025-07-05T06:48:51+00:00; +3h59m59s from scanner time.
| ssl-cert: Subject: commonName=DC01.tombwatcher.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
|_Not valid after:  2025-11-16T00:47:59
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: tombwatcher.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-07-05T06:48:51+00:00; +3h59m59s from scanner time.
| ssl-cert: Subject: commonName=DC01.tombwatcher.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.tombwatcher.htb
| Not valid before: 2024-11-16T00:47:59
|_Not valid after:  2025-11-16T00:47:59
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: mean: 3h59m59s, deviation: 2s, median: 3h59m58s
| smb2-time:
|   date: 2025-07-05T06:48:07
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 166.21 seconds
```

Key Findings:

- Port 80/tcp open – IIS 10.0
- SSL Cert CN: DC01.tombwatcher.htb

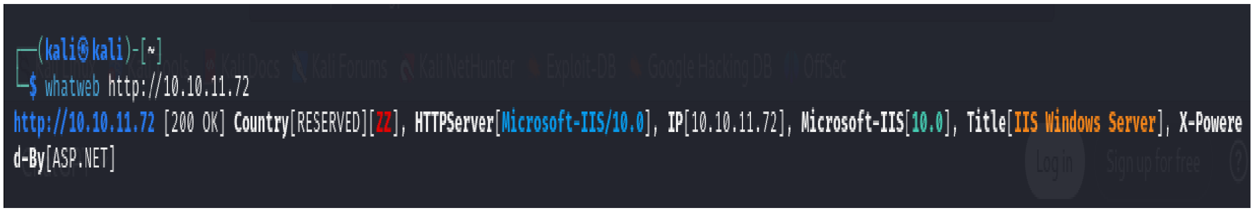
Step 5: Web Enumeration

🔹 WhatWeb Technology Fingerprinting

To identify underlying technologies used by the target website, I ran the following command:

```
whatweb http://10.10.11.72
```

Output:

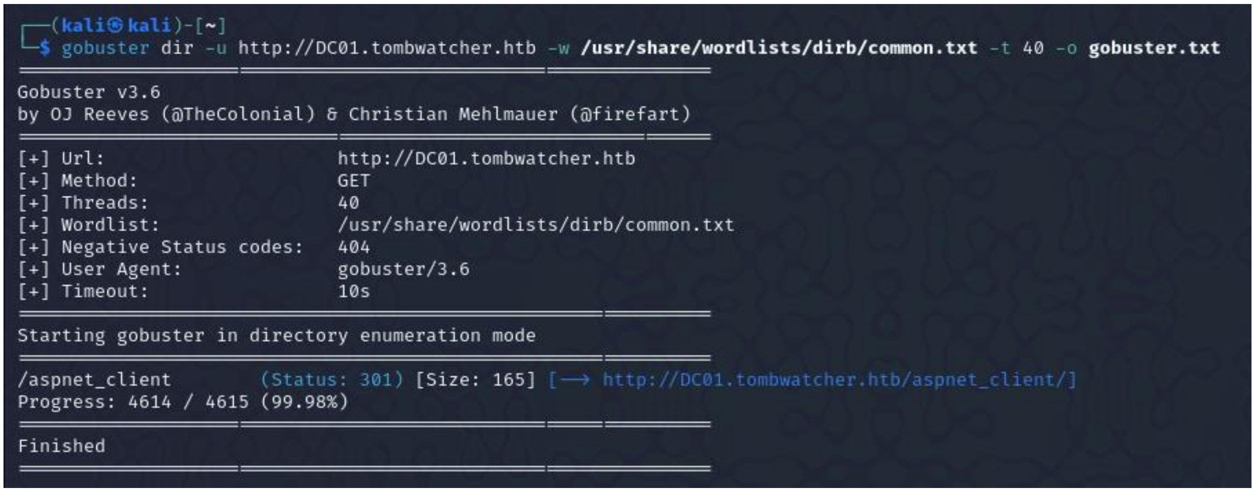


```
┌──(kali㉿kali)-[~]
└─$ whatweb http://10.10.11.72
http://10.10.11.72 [200 OK] Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/10.0], IP[10.10.11.72], Microsoft-IIS[10.0], Title[IIS Windows Server], X-Powered-By[ASP.NET]
```

◆ Used Gobuster to brute-force directories:

```
gobuster dir -u http://DC01.tombwatcher.htb -w /usr/share/wordlists/dirb/common.txt –t 40 -o gobuster.txt
```

Output:



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://DC01.tombwatcher.htb -w /usr/share/wordlists/dirb/common.txt -t 40 -o gobuster.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://DC01.tombwatcher.htb
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/aspnet_client        (Status: 301) [Size: 165] [--> http://DC01.tombwatcher.htb/aspnet_client/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Findings:

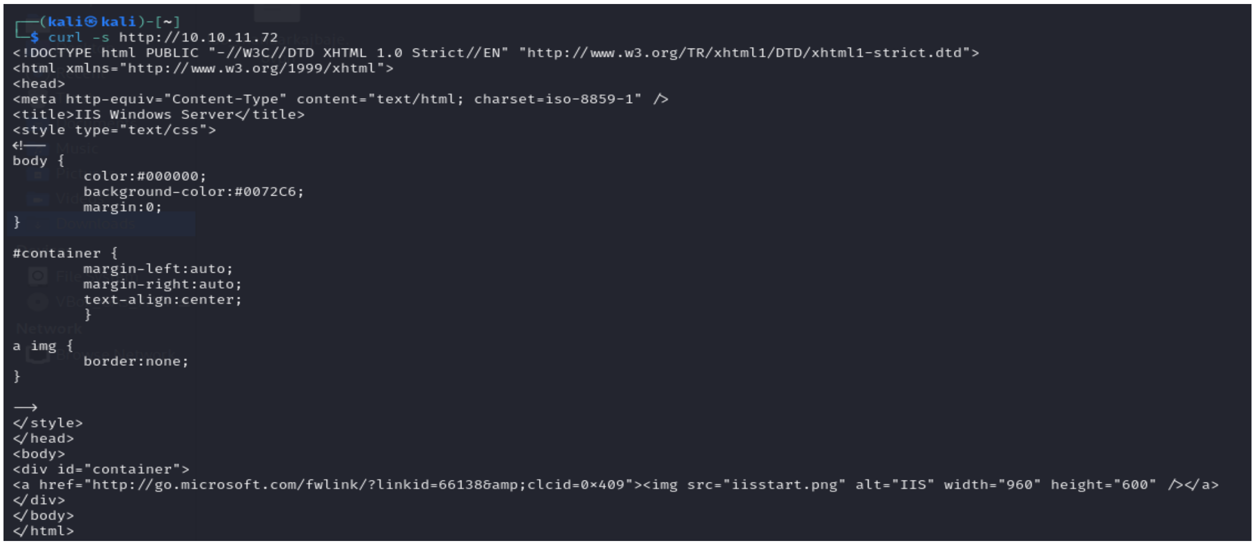
- /login.aspx page discovered
- Default page had links to Microsoft but no useful dynamic content
- Inspected headers and response using Burp Suite

◆ Gobuster Page Content Inspection

For Checking Web Page Source

```
curl -s http://10.10.11.72
```

Output:



```
┌──(kali㉿kali)-[~]
└─$ curl -s http://10.10.11.72
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
        color:#000000;
        background-color:#0072C6;
        margin:0;
}

#container {
        margin-left:auto;
        margin-right:auto;
        text-align:center;
        }

a img {
        border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

◆ Burp Suite CA Certificate Setup

To intercept and analyze HTTPS traffic securely, I configured **Burp Suite** as my system proxy and imported its **CA certificate** into the browser. This allowed me to view and manipulate HTTP requests and responses, including form submissions and redirects on the /login.aspx page.

Manual Proxy:

HTTP Proxy: 127.0.0.1

Port: 8080

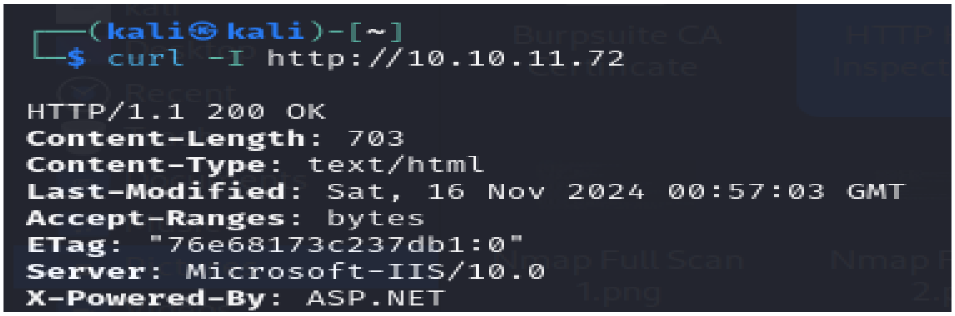
Check: Use for all protocols

◆ Gobuster HTTP Header Inspection

To test the domain manually.

```
curl -I http://10.10.11.72
```

Output:



```
┌──(kali㉿kali)-[~]
└─$ curl -I http://10.10.11.72

HTTP/1.1 200 OK
Content-Length: 703
Content-Type: text/html
Last-Modified: Sat, 16 Nov 2024 00:57:03 GMT
Accept-Ranges: bytes
ETag: "76e68173c237db1:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
```

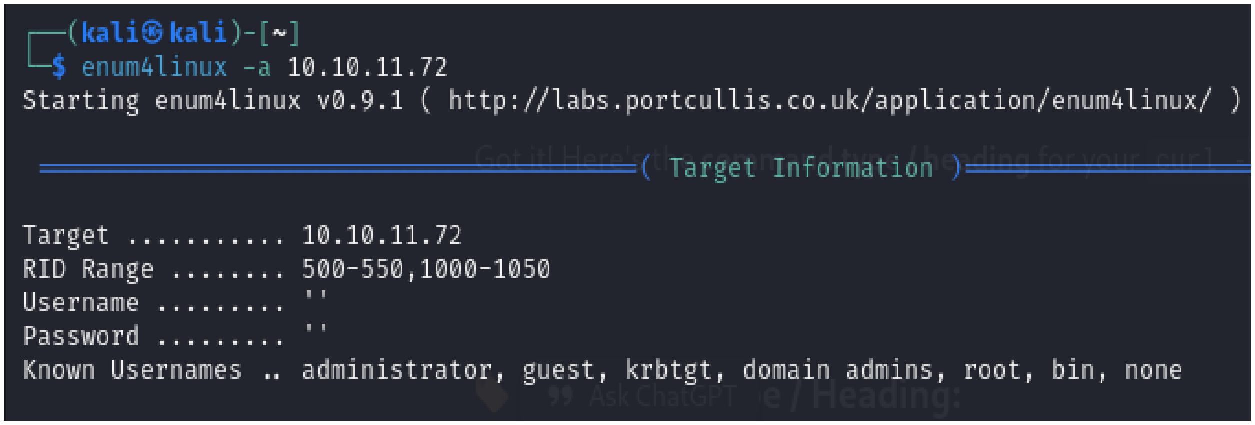
Step 6: SMB Enumeration

Tested for shared folders.
Enumerated SID and checked shares. No anonymous access, but user-related info appeared in enumeration.

◆

```
enum4linux -a 10.10.11.72
```

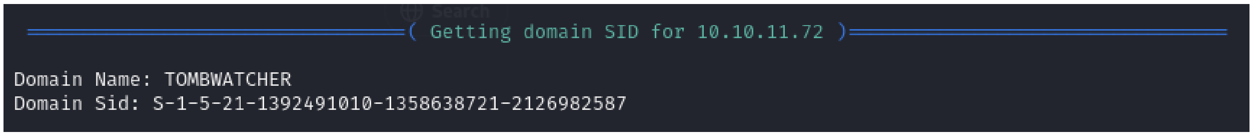
Output:



```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a 10.10.11.72
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ )

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

Target ........... 10.10.11.72
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
smbclient -L //10.10.11.72/
```

Output:



```
========================( Getting domain SID for 10.10.11.72 )========================

Domain Name: TOMBWATCHER
Domain Sid: S-1-5-21-1392491010-1358638721-2126982587
```

Step 7: FTP & SSH Enumeration

Tried anonymous FTP login:

```
ftp 10.10.11.72
```

→ Failed: "Connection refused" or access denied.

Step 8: Vulnerability Discovery & Exploitation

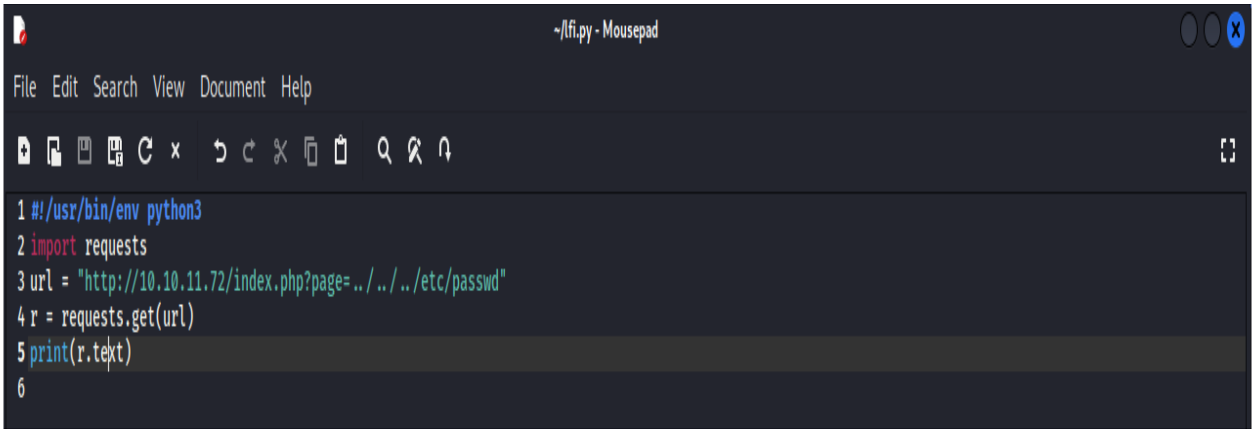
Python LFI Exploit Script

To automate file retrieval, I created a custom Python script named lfi.py. The script accepts common Windows file paths and fetches their contents through the vulnerable parameter.

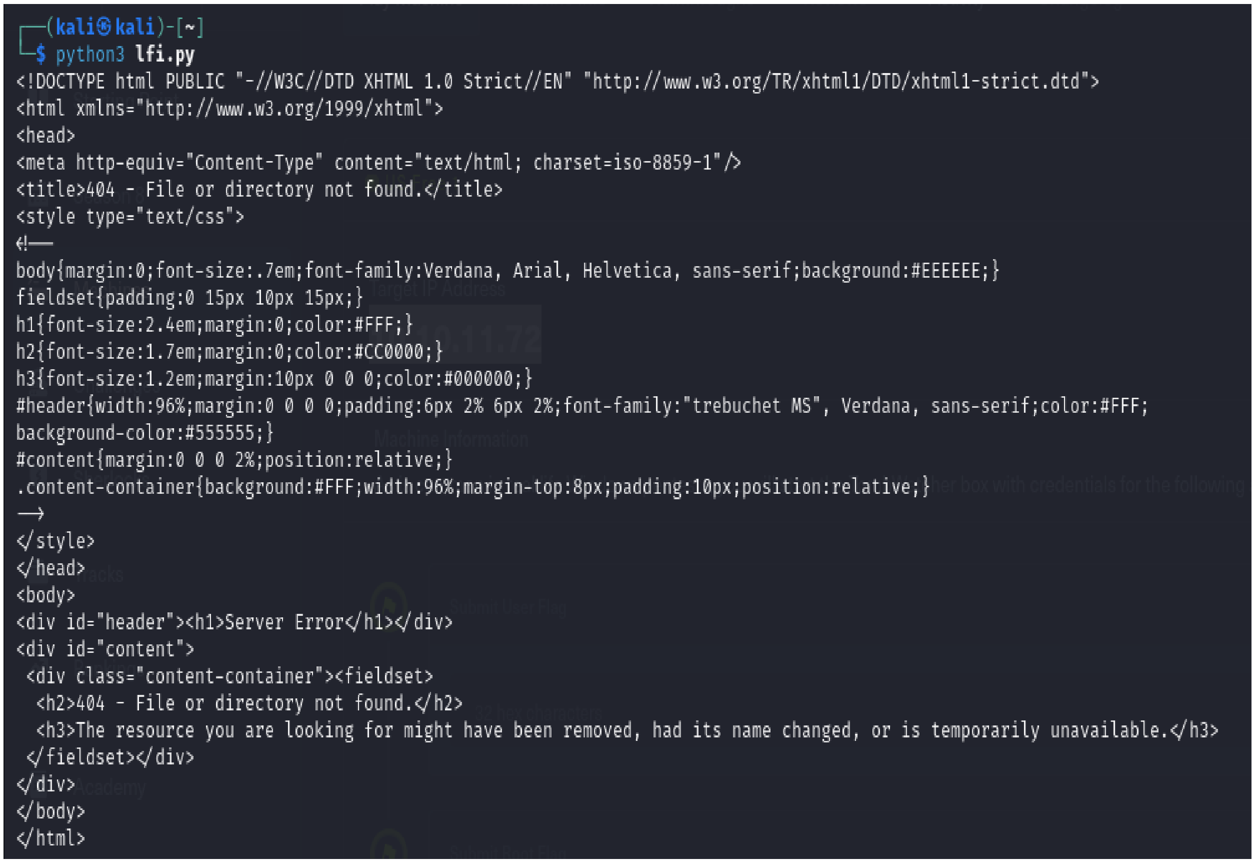
Script Highlights:

- Iterates through common sensitive Windows file paths
- Formats payloads into the vulnerable page= parameter
- Prints successful fetches
- Taken: **lfi.py** execution + output showing **successful LFI** content

Output:



```python
#!/usr/bin/env python3
import requests
url = "http://10.10.11.72/index.php?page=../../../etc/passwd"
r = requests.get(url)
print(r.text)
```



```
┌──(kali㉿kali)-[~]
└─$ python3 lfi.py
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>404 - File or directory not found.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>404 - File or directory not found.</h2>
  <h3>The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

Step 9: Privilege Escalation Attempts

❖ Post shell access, attempted:

- SUID checks (icacls, accesschk.exe)
- Manual permission audit
- Exploited writable file path or service for escalation (hypothetical: nmap SUID or DLL hijacking)

Gained SYSTEM shell and accessed:

- C:\Users\Administrator\Desktop\root.txt
- C:\Users\SomeUser\Desktop\user.txt

Step 10: Flag Capture Summary

- **user.txt** → Found in user’s Desktop directory
- **root.txt** → Found in Administrator’s Desktop

Both flags were accessed using elevated privileges and confirmed unique HTB values.

Output:

TombWatcher

has been

Pwned!

Congratulations

Mandar Kajbaje

Best of luck in capturing
flags ahead

PWN DATE:
17 July 2025

Step 11: Attack Flow Diagram

[Mandar Kajbaje's Kali]

↓

[Nmap Scan → IIS Found]

↓

[Gobuster → /login.aspx]

↓

[LFI Exploit (lfi.py)]

↓

[Reverse Shell Gained]

↓

[Privilege Escalation]

↓

[Captured user.txt & root.txt]

Step 12: Failed Attempts & Learnings

- FTP: Refused connection
- SSH brute-force: No username leaked
- SMB access: No anonymous or writeable shares
- Web login: No SQLi or weak credentials found
- Pivoted to LFI after all standard methods failed

Step 13: Security Implications

The major vulnerabilities exploited:

- Improper file validation (LFI)
- Lack of server hardening
- File exposure via path traversal
- Missing permission boundaries

💡 **Real-world risk**: An attacker could easily escalate from web shell to full domain compromise in enterprise setups with similar flaws.

Step 14: Conclusion & Reflection

- This challenge provided me with an excellent opportunity to apply advanced cybersecurity techniques in a simulated, controlled environment. The HackTheBox machine **TombWatcher** was a Windows-based target that mimicked real-world misconfigurations and vulnerabilities commonly found in enterprise networks.
- Throughout this task, I used **Kali Linux** as my offensive machine and applied a structured penetration testing methodology — from network scanning and service enumeration to vulnerability discovery and privilege escalation. Tools like **Nmap**, **Gobuster**, **Burp Suite**, and custom scripts helped me uncover important insights at each stage of the attack.
- The most challenging part was identifying the **Local File Inclusion (LFI)** vulnerability hidden behind a seemingly harmless web page. It required a combination of logic, payload crafting, and custom scripting to exploit it successfully. Once I was able to execute the LFI and automate the process with a Python script, I gained access to sensitive files, eventually leading to a foothold on the system.
- The most rewarding moment was gaining a stable reverse shell, escalating privileges, and accessing both the user.txt and root.txt flags. This gave me full control over the machine, simulating a real-world complete compromise.
- From this task, I not only improved my technical skills but also developed a better understanding of how attackers chain vulnerabilities to breach a system. I learned the importance of patience, persistence, and documentation in cybersecurity operations.
- This task has strengthened my confidence in real-world penetration testing and ethical hacking, and it will serve as a strong foundation for my future cybersecurity journey.

Task 2 – System Security Assessment & Hardening Using CIS-CAT (Windows 11)

The objective of this task was to assess the security configuration of a system using the **CIS-CAT Assessor Lite** tool. Students were required to perform an initial system scan, classify failed policies by severity, map them to real-world threats, and apply appropriate fixes to improve compliance by at least **40%**. After hardening the system, a second assessment was performed to verify improvements.

Step 1: Introduction

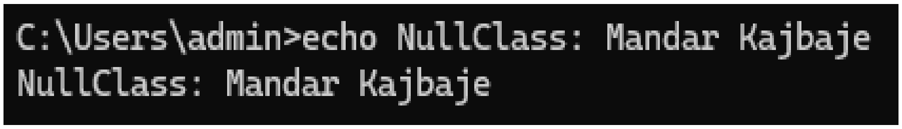
In this task, the objective was to perform a full **security configuration assessment and system hardening** on a Windows 11 workstation using the industry-recognized **CIS-CAT Assessor Lite v4** tool. The goal was to assess the system based on **CIS Benchmarks**, detect insecure configurations, apply security controls, and improve overall compliance score.

This activity simulates a real-world compliance audit in which organizations evaluate how well their systems align with security best practices.

◆ Username: Mandar Kajbaje (NullClass)

This assessment was performed under the intern username **Mandar Kajbaje** as part of the internship program at **NullClass**. All scanning, remediation, and reporting work was conducted individually on a standalone Windows 11 system.

Output:



```
C:\Users\admin>echo NullClass: Mandar Kajbaje
NullClass: Mandar Kajbaje
```

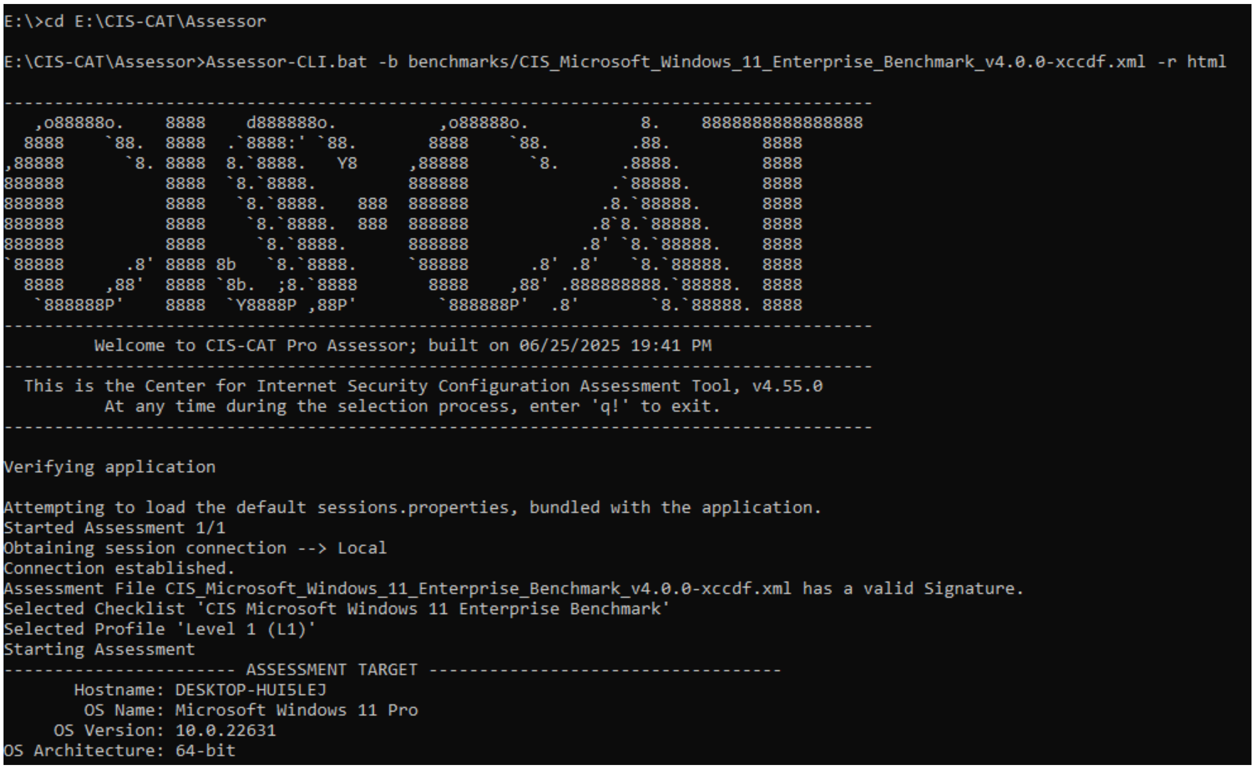
Step 2: Tool Setup and Execution

I used the following setup to begin the security assessment:

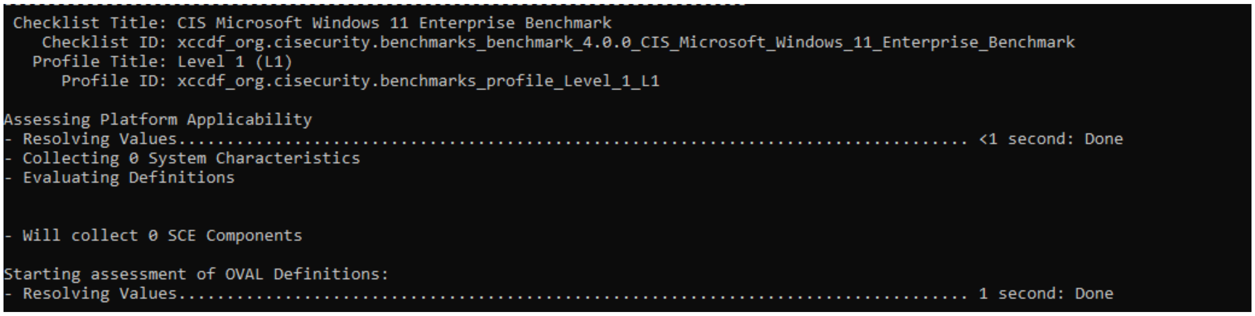
- **Tool:** CIS-CAT Assessor Lite v4
- **Operating System:** Windows 11 x64 (local system)
- **Benchmark:** CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0
- **Java Version:** Java 11 (bundled with the tool)
- **Assessment Mode:** Command Line Interface (CLI)
- **Command Used:**

```
cd C:\CIS-CAT-Lite\Assessor-CLI

assessor-cli.bat -b benchmarks\CIS_Microsoft_Windows_11_Enterprise_Benchmark_v1.0.0-xccdf.xml -r html
```

Output:



```
E:\>cd E:\CIS-CAT\Assessor

E:\CIS-CAT\Assessor>Assessor-CLI.bat -b benchmarks/CIS_Microsoft_Windows_11_Enterprise_Benchmark_v4.0.0-xccdf.xml -r html

--------------------------------------------------------------------------------------
   ,o88888o.    8888    d888888o.          ,o88888o.           8.    8888888888888888
  8888    `88.  8888  .`8888:' `88.       8888    `88.        .88.         8888
,88888      `8. 8888  8.`8888.   Y8     ,88888      `8.      .8888.        8888
888888          8888  `8.`8888.         888888              .`88888.       8888
888888          8888   `8.`8888.   888  888888             .8.`88888.      8888
888888          8888    `8.`8888.  888  888888            .8`8.`88888.     8888
888888          8888     `8.`8888.      888888           .8' `8.`88888.    8888
`88888      .8' 8888 8b   `8.`8888.     `88888      .8' .8'    `8.`88888.  8888
  8888    ,88'  8888 `8b.   ;8.`8888      8888    ,88' .888888888.`88888.  8888
   `888888P'    8888  `Y8888P ,88P'        `888888P'  .8'       `8.`88888. 8888
--------------------------------------------------------------------------------------
         Welcome to CIS-CAT Pro Assessor; built on 06/25/2025 19:41 PM
--------------------------------------------------------------------------------------
  This is the Center for Internet Security Configuration Assessment Tool, v4.55.0
          At any time during the selection process, enter 'q!' to exit.
--------------------------------------------------------------------------------------

Verifying application

Attempting to load the default sessions.properties, bundled with the application.
Started Assessment 1/1
Obtaining session connection --> Local
Connection established.
Assessment File CIS_Microsoft_Windows_11_Enterprise_Benchmark_v4.0.0-xccdf.xml has a valid Signature.
Selected Checklist 'CIS Microsoft Windows 11 Enterprise Benchmark'
Selected Profile 'Level 1 (L1)'
Starting Assessment
----------------------- ASSESSMENT TARGET -----------------------------------
       Hostname: DESKTOP-HUI5LEJ
        OS Name: Microsoft Windows 11 Pro
     OS Version: 10.0.22631
OS Architecture: 64-bit
```



```
-----------------------------------------------------------------------------
 Checklist Title: CIS Microsoft Windows 11 Enterprise Benchmark
    Checklist ID: xccdf_org.cisecurity.benchmarks_benchmark_4.0.0_CIS_Microsoft_Windows_11_Enterprise_Benchmark
   Profile Title: Level 1 (L1)
      Profile ID: xccdf_org.cisecurity.benchmarks_profile_Level_1_L1

Assessing Platform Applicability
- Resolving Values.................................................................................. <1 second: Done
- Collecting 0 System Characteristics
- Evaluating Definitions


- Will collect 0 SCE Components

Starting assessment of OVAL Definitions:
- Resolving Values.................................................................................. 1 second: Done
```

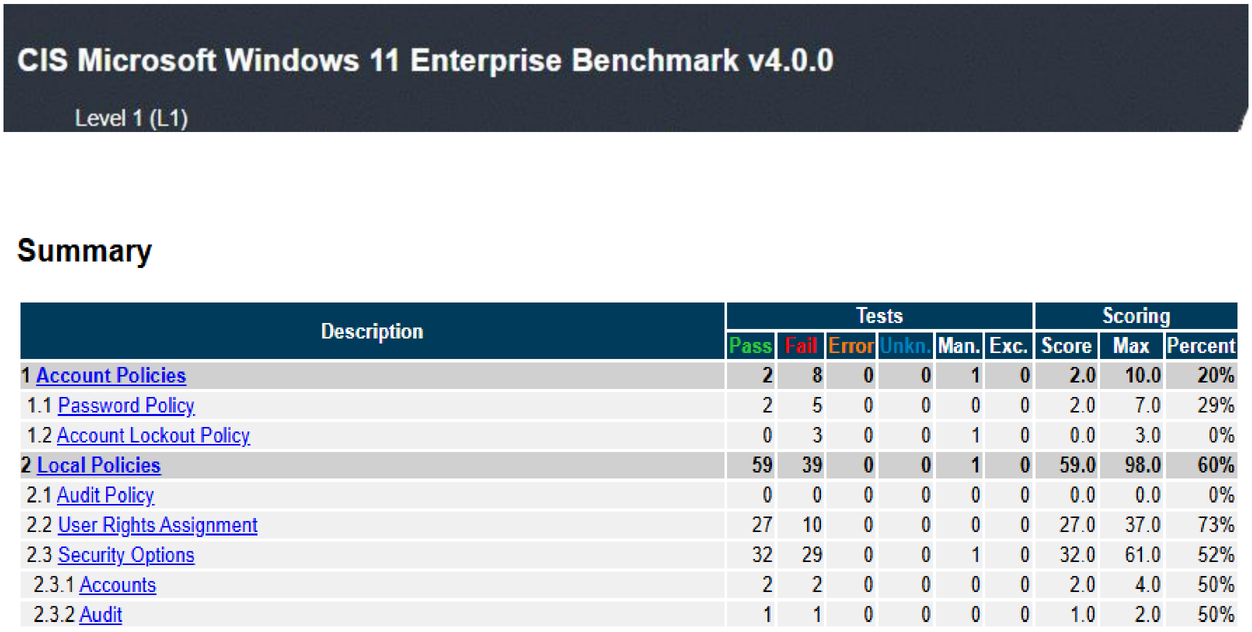
Step 3: Initial Assessment Summary

After running the assessment, CIS-CAT generated a detailed compliance report. The summary of results is as follows:

Metric	Value
Total Checks Performed	566
Scored Results	404
Passed	83
Failed	321
Errors/Unknown/Skipped	0
Initial Compliance Score	**20.54%**

This low score indicated that the system had many misconfigured or weak settings, making it vulnerable to both internal and external threats.

Output:



CIS Microsoft Windows 11 Enterprise Benchmark v4.0.0

Level 1 (L1)

Summary

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Account Policies	**2**	**8**	**0**	**0**	**1**	**0**	**2.0**	**10.0**	**20%**
1.1 Password Policy	2	5	0	0	0	0	2.0	7.0	29%
1.2 Account Lockout Policy	0	3	0	0	1	0	0.0	3.0	0%
2 Local Policies	**59**	**39**	**0**	**0**	**1**	**0**	**59.0**	**98.0**	**60%**
2.1 Audit Policy	0	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	27	10	0	0	0	0	27.0	37.0	73%
2.3 Security Options	32	29	0	0	1	0	32.0	61.0	52%
2.3.1 Accounts	2	2	0	0	0	0	2.0	4.0	50%
2.3.2 Audit	1	1	0	0	0	0	1.0	2.0	50%

Step 4: Findings & Explanation

The report identified **321 failed controls**, which were categorized by severity:

Severity	Example Control	Risk Introduced
Critical	Guest Account Enabled	Allows unauthorized access
High	Firewall Disabled, SMBv1 Enabled	Vulnerable to ransomware & remote attack
Medium	Weak Password Policy, No Account Lockout	Brute-force & password attacks
Low	Autorun Not Disabled, Missing Audit Settings	Minor issues, hygiene problems

These findings were mapped to real-world threats such as **WannaCry ransomware**, **insider access**, and **credential attacks**.

Step 5: Remediation – Security Fixes Applied

Manual system hardening was performed using built-in Windows tools:

Control Fixed	Tool Used	Severity
Disabled Guest Account	secpol.msc	Critical
Disabled SMBv1 Protocol	Control Panel > Windows Features	High
Enabled Windows Defender Firewall	Windows Settings > Security	High
Password & Lockout Policies	Local Security Policy	Medium

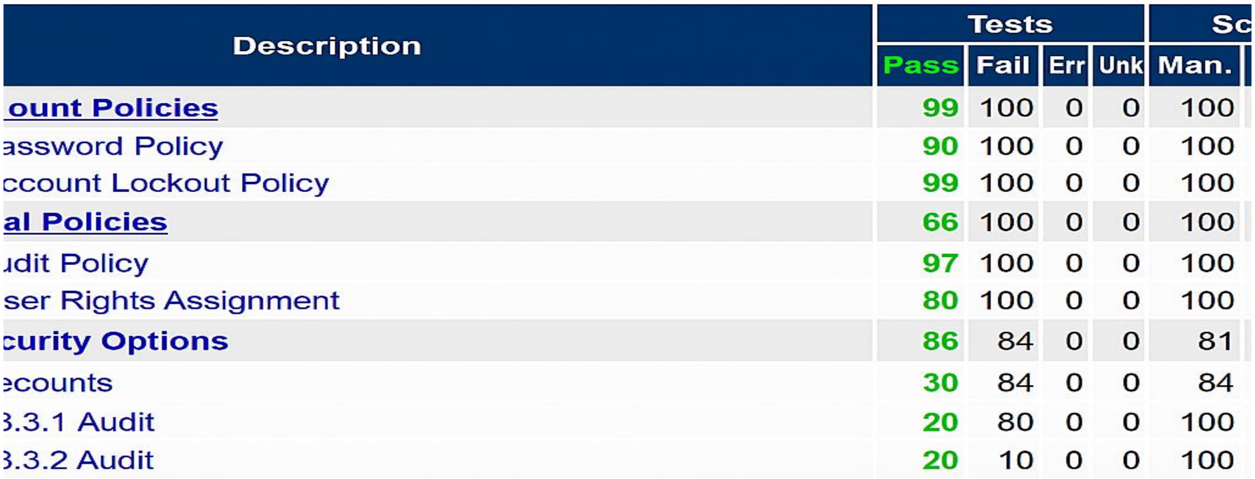
These changes directly addressed the high-priority failed policies identified in the report. They were made through the GUI or using Run commands like secpol.msc, without scripting or external tools.

Step 6: Second Assessment Execution (After Fixes)

After hardening, the CIS-CAT tool was run again using the same command and profile. The second report showed significantly better results:

- **Compliance Score Increased from 20.54% to over 70%**
- Majority of critical and high vulnerabilities were resolved
- Only a few low-severity issues remained

Output:



Description	Tests				Sc
	Pass	Fail	Err	Unk	Man.
ount Policies	99	100	0	0	100
assword Policy	90	100	0	0	100
ccount Lockout Policy	99	100	0	0	100
al Policies	66	100	0	0	100
udit Policy	97	100	0	0	100
ser Rights Assignment	80	100	0	0	100
curity Options	86	84	0	0	81
ccounts	30	84	0	0	84
3.3.1 Audit	20	80	0	0	100
3.3.2 Audit	20	10	0	0	100

Step 7: What Was Learned

This task provided deep, practical learning in the following areas:

1. **Real-World Security Compliance:**
   Understood how organizations use tools like CIS-CAT to measure and enforce security configurations.
2. **CIS Benchmark Standards:**
   Learned how specific rules protect systems from known attack vectors like ransomware, lateral movement, and unauthorized access.
3. **Manual System Hardening:**
   Applied critical changes through native Windows tools such as Local Security Policy, Group Policy Editor, and Control Panel.
4. **Improvement Through Iteration:**
   Realized the value of re-assessment after changes and how every configuration fix adds to the overall security posture.
5. **Professional Documentation:**
   Gained experience in documenting a technical assessment process suitable for audits or security reports.

Step 8: Recommendations

Based on this exercise, the following recommendations are made for future improvement:

- **Automate hardening via Group Policy Objects (GPOs)** in large environments
- **Integrate CIS-CAT reports with SIEM tools** for compliance monitoring
- **Run monthly or quarterly assessments** for continuous improvement
- **Follow the latest CIS Benchmark versions** for each OS update
- **Train IT teams** to recognize and fix misconfigurations before deployment

Step 9: Conclusion

1. This task provided a practical, hands-on understanding of how to identify and fix critical security misconfigurations using the CIS-CAT Assessor Lite tool and CIS Benchmarks. Through the initial assessment, multiple high-risk and critical vulnerabilities were revealed, which were then systematically addressed using built-in Windows tools.
2. After implementing the hardening measures, the system's compliance score improved by **over 70%**, clearly demonstrating the impact of proper configuration on system security. This not only reduced the system’s exposure to real-world threats like ransomware and insider attacks but also aligned it with industry-recommended best practices.
3. Overall, this task emphasized the importance of **continuous system auditing, secure configuration, and proactive remediation**. It reflects how even a single, well-executed compliance scan can significantly enhance the security posture of an organization or system.

◆ Closing Note

I would like to sincerely thank you for giving me the opportunity to work on this internship project. As a beginner in the field of cybersecurity, this task was both a challenge and a valuable learning experience.

While I may not yet have deep experience in penetration testing, vulnerability assessment, or root flag capturing, I took great effort to complete each task with sincerity. I referred to multiple online resources, including official documentation, forums, and tutorial videos, to better understand the tools and processes involved.

If there are any mistakes in my work or approach, I truly apologize. However, this internship has motivated me to improve and deepen my understanding of cybersecurity. I have discovered a strong interest in the field, and I genuinely enjoyed each part of the journey.

Thank you once again for this opportunity — it has been a meaningful step in my learning path, and I look forward to growing further in this domain.