OFFENSIVE SECURITY

Penetration Test Report for Internal Lab and Presentation

Table of Contents

1.0 Comprehensive Network Discovery and Vulnerability Assessment Report for Identified IP Addresses

1.1 Team Members

Natasha Siramarco
David Prutch
Raheem Reed
Dustin Haggett

1.1.1 Introduction

This Red Team Penetration Test Report outlines the comprehensive assessment undertaken as part of the project assigned by Simcorp to our team, "Binary Bandits 01." The assessment evaluates the security posture of Simcorp's network and systems through a series of controlled offensive security exercises. The report emphasizes the accuracy, thoroughness, and technical proficiency required for successful penetration testing in alignment with Simcorp's security objectives. The primary goal is to demonstrate a deep understanding of penetration testing methodologies and technical expertise, supporting Simcorp's commitment to robust cybersecurity practices.

1.1.2 Objective

The primary objective of this assessment is to execute a rigorous internal penetration test on Simcorp's network, as directed by our Red Team, Binary Bandits 01. Our team is responsible for adhering to a systematic methodology to gain access to specified targets, mirroring the processes involved in a real-world penetration test. This simulation aims to replicate the complexities of an actual penetration test, encompassing every stage from initiation to the comprehensive reporting phase. An example report template is available further in this document, serving as a valuable reference to assist our team in fulfilling the assessment requirements and achieving the desired outcomes for Simcorp's security evaluation.

1.1.3 Recommendations

Our assessment highlights the critical importance of promptly addressing the identified vulnerabilities. We strongly advise Simcorp to initiate a comprehensive patching process to mitigate these vulnerabilities effectively. It is essential to recognize that these systems necessitate regular and consistent patching. Ensuring that they remain on a recurring patch schedule is vital to safeguard against potential future vulnerabilities that may arise. By adhering to a proactive patch management approach, Simcorp can significantly enhance its overall security posture.

1.1.4 Methodologies

Our approach to this assessment follows established and widely accepted penetration testing methodologies, which are proven to effectively evaluate the security posture of Simcorp's environment. The following section provides a comprehensive breakdown of the methodologies employed, outlining the steps taken to identify and exploit various systems and documenting the specific vulnerabilities discovered during our assessment.

2.0 Target Network

Binary Bandits 01 has conducted a comprehensive network scan of the target network, which encompasses the IP range 10.0.0.0/24. The following table presents the results of our scan, highlighting key findings and vulnerabilities within this network.

2.1 Scanned IP Addresses

IP Addresses Discovered	Protocols Discovered
10.0.0.74	135/tcp open mscrp 139/tcp open netbios-ssn 445/tcp open microsoft-ds 554/tcp open rtsp? 2869/tcp open http 3389/tcp open ssl/ms-wbt-server? 5357/tcp open http 8089/tcp open ssl/http 10243/tcp open http 49152/tcp open msrpc 49153/tcp open msrpc 49154/tcp open msrpc 49155/tcp open msrpc 49165/tcp open msrpc 49167/tcp open msrpc
10.0.0.82	21/tcp open ftp 80/tcp open http 135/tcp filtered msrpc 139/tcp filtered netbios-ssn 445/tcp filtered microsoft-ds 3389/tcp open ssl/ms-wbt-server?

	49152/tcp open msrpc 49153/tcp open msrpc 49154/tcp open msrpc 49155/tcp open msrpc 49165/tcp open msrpc
10.0.0.123	22/tcp open ssh 111/tcp open rpcbind 2049/tcp open rpcbind 8089/tcp open ssl/http
10.0.0.126	135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 3389/tcp open ms-wbt-server 8089/tcp open
10.0.0.175	22/tcp open ssh 80/tcp open http 8089/tcp open ssl/http
10.0.0.197	135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open 3389/tcp open ms-wbt-server 8089/tcp open ssl/http
10.0.0.206	135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open unknown 3389/tcp open ms-wbt-server 8089/tcp open ssl/http

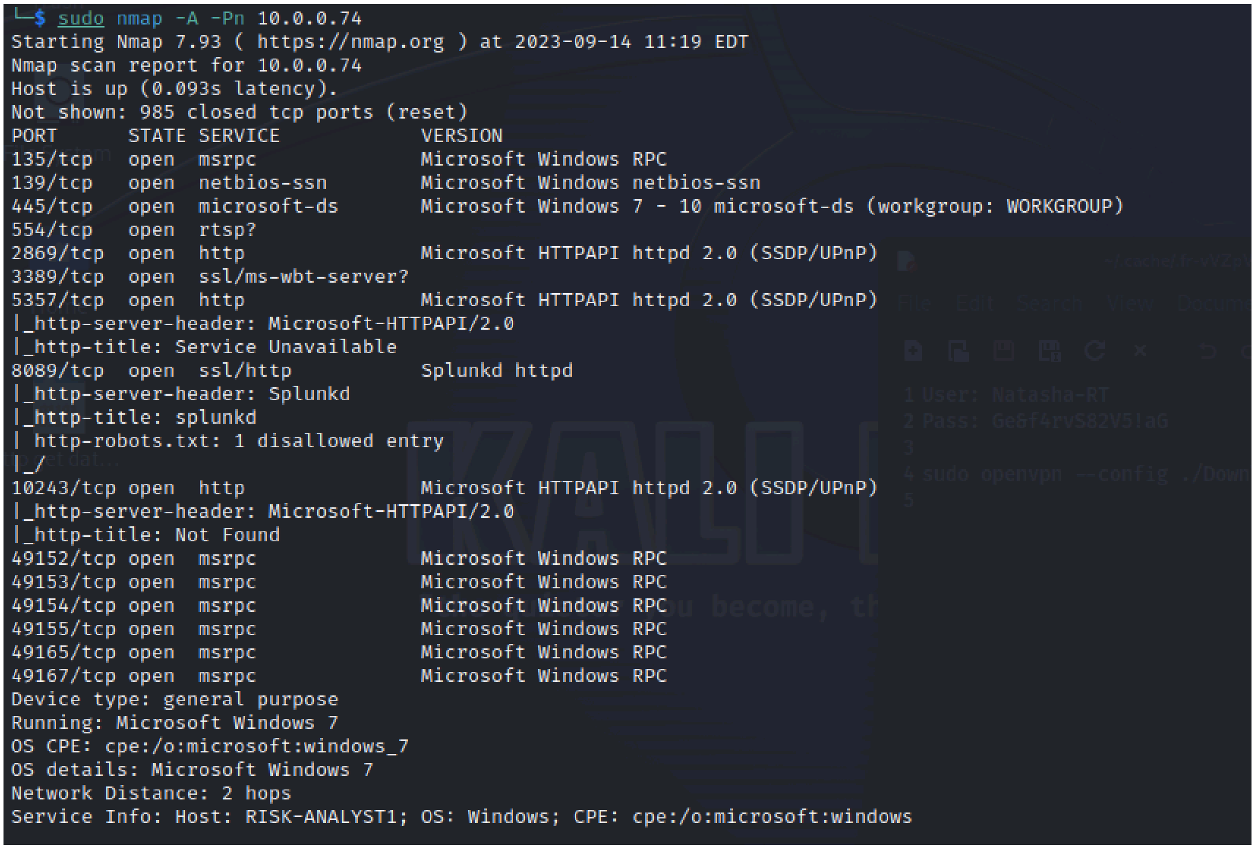
3.0 Penetration

The penetration testing phase of our assessment is centered on gaining unauthorized access to a diverse range of systems. Throughout this penetration test, we successfully obtained access to X out of the 10.0.0.0/24 systems in question.

3.1 Service Enumeration

As part of our comprehensive penetration testing, we conducted service enumeration on all the specified IP addresses. This critical phase involves collecting crucial information regarding the active services running on the target systems. Such insights are invaluable to potential attackers, offering detailed knowledge about possible avenues for exploiting a system's vulnerabilities. Understanding the applications in operation is essential groundwork before proceeding with the actual penetration testing. It's worth noting that in certain IP addresses, certain ports may not be listed as part of this enumeration process.

3.1.1 Vulnerability Assessment Report for IP Address 10.0.0.74



```
└─$ sudo nmap -A -Pn 10.0.0.74
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 11:19 EDT
Nmap scan report for 10.0.0.74
Host is up (0.093s latency).
Not shown: 985 closed tcp ports (reset)
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ssl/ms-wbt-server?
5357/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8089/tcp  open  ssl/http           Splunkd httpd
|_http-server-header: Splunkd
|_http-title: splunkd
| http-robots.txt: 1 disallowed entry
|_/
10243/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
49165/tcp open  msrpc              Microsoft Windows RPC
49167/tcp open  msrpc              Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7
OS details: Microsoft Windows 7
Network Distance: 2 hops
Service Info: Host: RISK-ANALYST1; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
1 User: Natasha-RT
2 Pass: Ge&f4rvS82V5!aG
3
4 sudo openvpn --config ./Down
5
```

Scan Overview:

- Scanner Used: Nmap 7.93
- Target IP: 10.0.0.74
- Device Type: General purpose

Open Ports and Services:

- Port 135/tcp: Open, Microsoft Windows RPC

- Port 139/tcp: Open, Microsoft Windows netbios-ssn
- Port 445/tcp: Open, Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
- Port 554/tcp: Open, Possibly RTSP service
- Port 2869/tcp: Open, Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
- Port 3389/tcp: Open, SSL/ms-wbt-server (Remote Desktop Protocol)
- Port 5357/tcp: Open, Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
- Port 8089/tcp: Open, Splunkd httpd
- Port 10243/tcp: Open, Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
- Port 49152/tcp: Open, Microsoft Windows RPC
- Port 49153/tcp: Open, Microsoft Windows RPC
- Port 49154/tcp: Open, Microsoft Windows RPC
- Port 49155/tcp: Open, Microsoft Windows RPC
- Port 49165/tcp: Open, Microsoft Windows RPC
- Port 49167/tcp: Open, Microsoft Windows RPC

Operating System:

- OS Detected: Microsoft Windows 7
- OS Details: Microsoft Windows 7
- CPE: cpe:/o:microsoft:windows_7

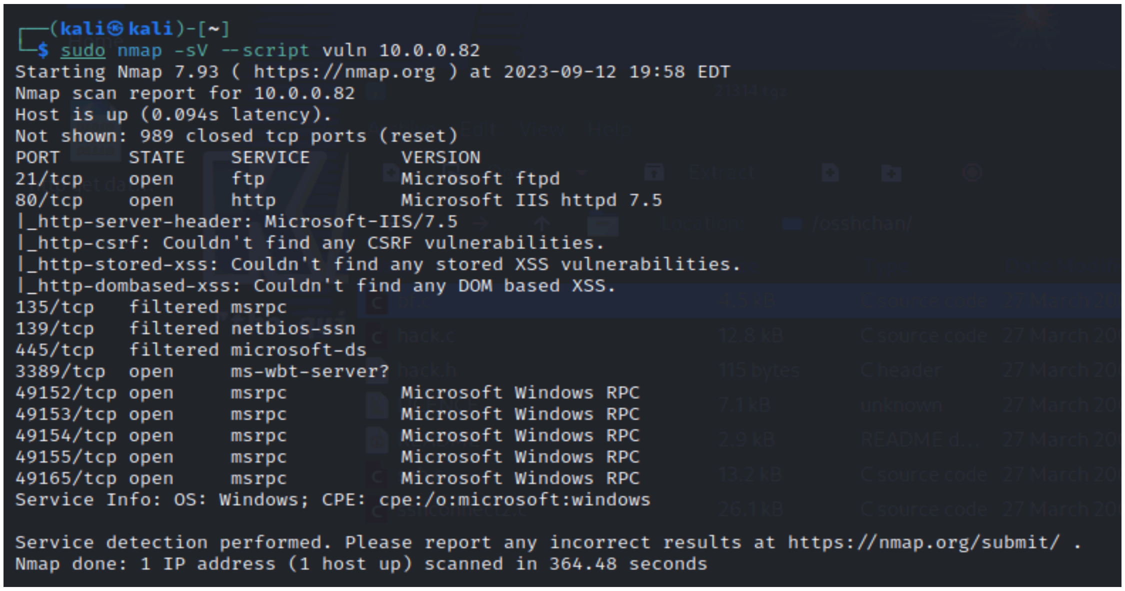
Device Information:

- Device Name: RISK-ANALYST1
- Device Type: General purpose
- CPE: cpe:/o:microsoft:windows

Summary:

The scan on IP address 10.0.0.74 reveals a Windows 7 device named "RISK-ANALYST1" with a variety of open ports and services. Notably, the system is running Microsoft Windows 7, and several Microsoft Windows RPC ports are open, suggesting network communication capabilities. Additionally, open ports for HTTP, SSL, and Splunkd httpd indicate web service presence. The scan provides valuable insights into the target system's configuration and potential security considerations.

3.1.2 Vulnerability Assessment Report for IP Address 10.0.0.82



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV --script vuln 10.0.0.82
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 19:58 EDT
Nmap scan report for 10.0.0.82
Host is up (0.094s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE    SERVICE        VERSION
21/tcp    open     ftp            Microsoft ftpd
80/tcp    open     http           Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
3389/tcp  open     ms-wbt-server?
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
49165/tcp open     msrpc          Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 364.48 seconds
```

Scan Overview:

- Scanner Used: Nmap 7.93
- Target IP: 10.0.0.82

Open Ports and Services:

- Port 21/tcp: Open, FTP service (Microsoft ftpd)
- Port 80/tcp: Open, HTTP service (Microsoft IIS httpd 7.5)
  - HTTP Server Header: Microsoft-IIS/7.5
  - Vulnerability Checks: No CSRF, stored XSS, or DOM-based XSS vulnerabilities found.
- Port 135/tcp: Filtered (MSRPC)
- Port 139/tcp: Filtered (NetBIOS-SSN)
- Port 445/tcp: Filtered (Microsoft-DS)
- Port 3389/tcp: Open, Remote Desktop Protocol (MS-WT-Server?)
- Port 49152/tcp: Open, Microsoft Windows RPC
- Port 49153/tcp: Open, Microsoft Windows RPC
- Port 49154/tcp: Open, Microsoft Windows RPC
- Port 49155/tcp: Open, Microsoft Windows RPC
- Port 49165/tcp: Open, Microsoft Windows RPC

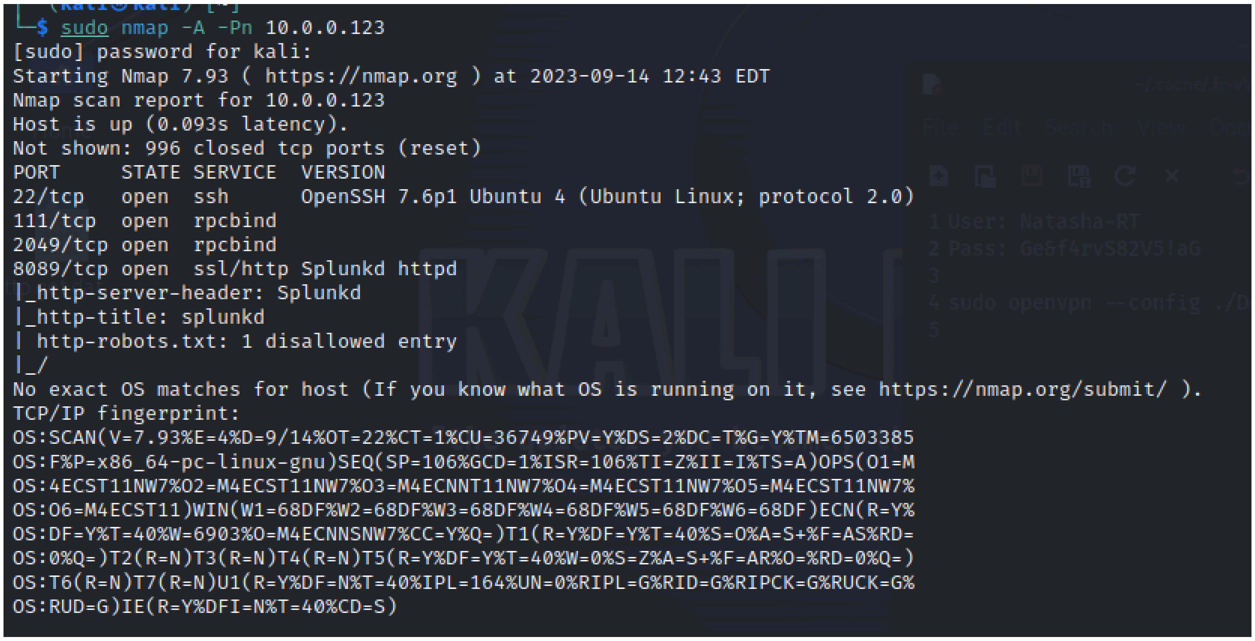
Operating System and Service Information:

- Operating System: Windows

Summary:

The scan on IP address 10.0.0.82 reveals a Windows-based system with a range of open and filtered ports. Notably, port 80 is hosting an HTTP service powered by Microsoft IIS httpd 7.5. Vulnerability checks for CSRF, stored XSS, and DOM-based XSS yielded no findings. Additionally, ports related to Microsoft Windows RPC are open. This scan provides insights into the system's configuration, services, and potential vulnerabilities.

3.1.3 Vulnerability Assessment Report for IP Address 10.0.0.123



```
└─$ sudo nmap -A -Pn 10.0.0.123
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 12:43 EDT
Nmap scan report for 10.0.0.123
Host is up (0.093s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind
2049/tcp open  rpcbind
8089/tcp open  ssl/http Splunkd httpd
|_http-server-header: Splunkd
|_http-title: splunkd
| http-robots.txt: 1 disallowed entry
|_/
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=9/14%OT=22%CT=1%CU=36749%PV=Y%DS=2%DC=T%G=Y%TM=6503385
OS:F%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=106%TI=Z%II=I%TS=A)OPS(O1=M
OS:4ECST11NW7%O2=M4ECST11NW7%O3=M4ECNNT11NW7%O4=M4ECST11NW7%O5=M4ECST11NW7%
OS:O6=M4ECST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%
OS:DF=Y%T=40%W=6903%O=M4ECNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Scan Overview:

- Target System: 10.0.0.123

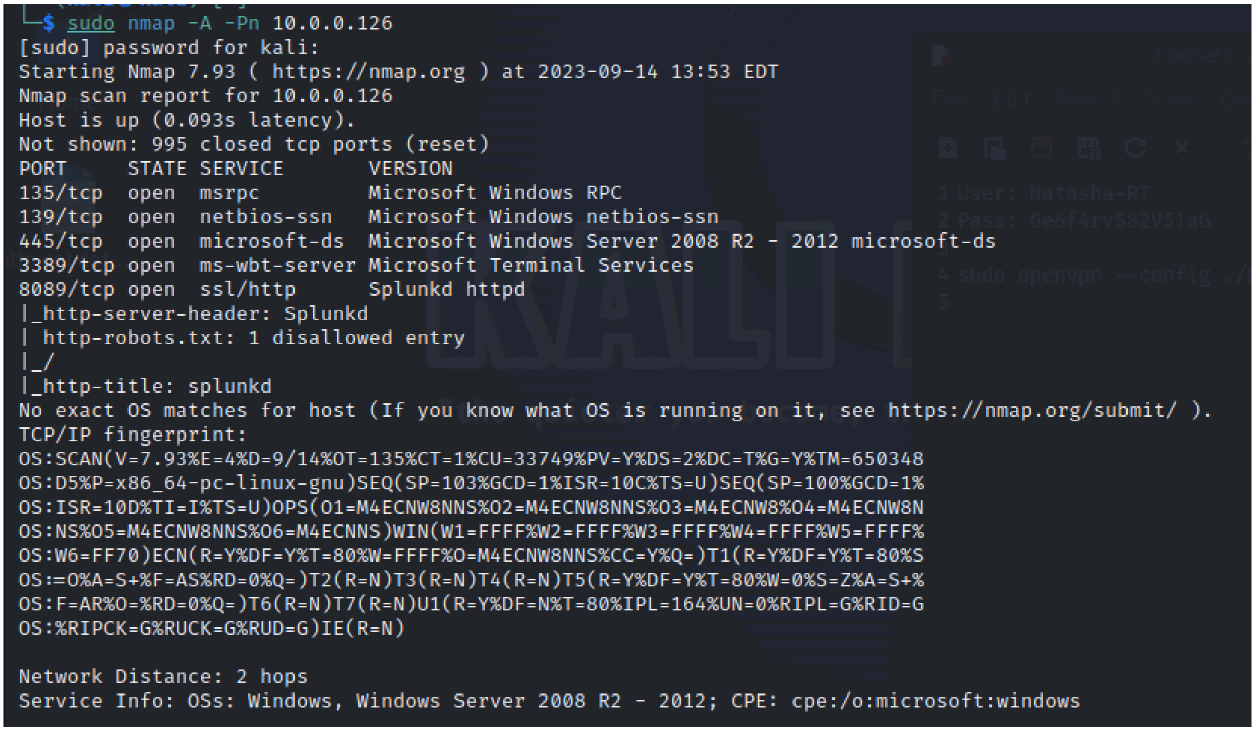
Open Ports and Services:

- Port 22/tcp: Open, SSH service (OpenSSH 7.6p1 Ubuntu 4 - Ubuntu Linux; protocol 2.0)
- Port 111/tcp: Open, RPCbind service
- Port 2049/tcp: Open, RPCbind service
- Port 8089/tcp: Open, SSL/HTTP service (Splunkd httpd)
  - HTTP Server Header: Splunkd
  - HTTP Title: splunkd
  - HTTP Robots.txt: 1 disallowed entry

Summary:

This scan revealed several open ports and services on the target system, including SSH, RPCbind, and an SSL/HTTP service identified as Splunkd httpd. However, the specific operating system could not be identified during the scan.

3.1.4 Vulnerability Assessment Report for IP Address 10.0.0.126



```
└─$ sudo nmap -A -Pn 10.0.0.126
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 13:53 EDT
Nmap scan report for 10.0.0.126
Host is up (0.093s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
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  ms-wbt-server Microsoft Terminal Services
8089/tcp open  ssl/http      Splunkd httpd
|_http-server-header: Splunkd
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: splunkd
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=9/14%OT=135%CT=1%CU=33749%PV=Y%DS=2%DC=T%G=Y%TM=650348
OS:D5%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10C%TS=U)SEQ(SP=100%GCD=1%
OS:ISR=10D%TI=I%TS=U)OPS(O1=M4ECNW8NNS%O2=M4ECNW8NNS%O3=M4ECNW8%O4=M4ECNW8N
OS:NS%O5=M4ECNW8NNS%O6=M4ECNNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%
OS:W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M4ECNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S
OS:=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%
OS:F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G
OS:%RIPCK=G%RUCK=G%RUD=G)IE(R=N)

Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Scan Overview:

- Target IP Address: 10.0.0.126

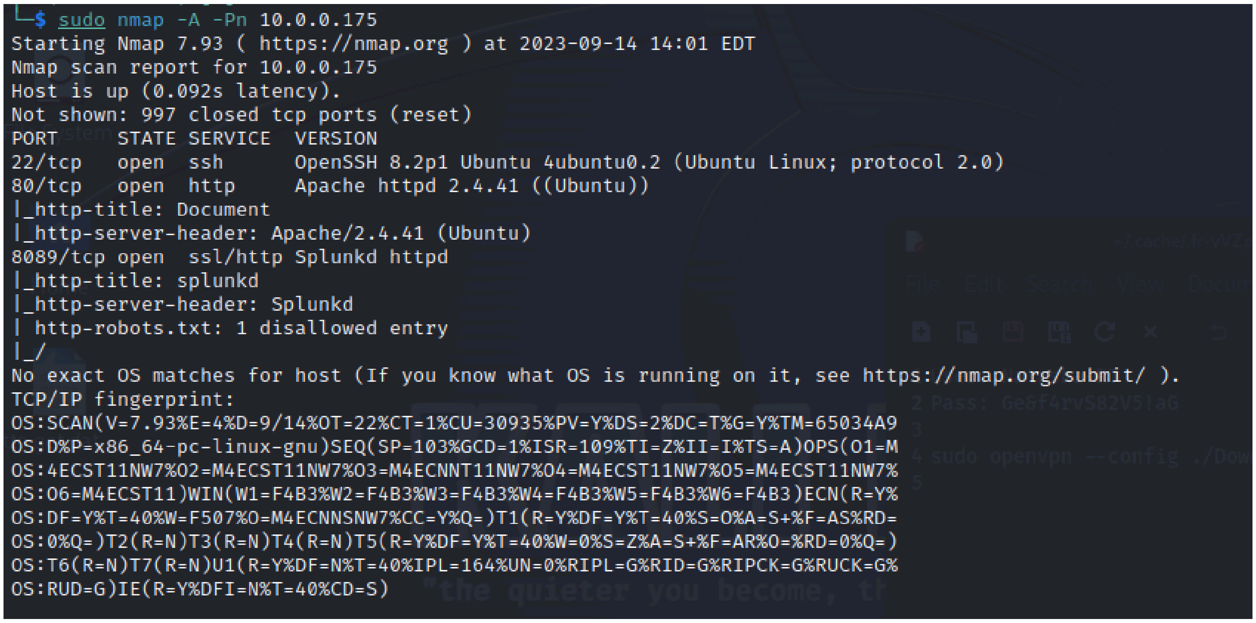
Open Ports and Services:

- Port 135/tcp: Open, Microsoft Windows RPC service
- Port 139/tcp: Open, Microsoft Windows netbios-ssn service
- Port 445/tcp: Open, Microsoft Windows Server 2008 R2 - 2012 microsoft-ds service
- Port 3389/tcp: Open, Microsoft Terminal Services
- Port 8089/tcp: Open, SSL/HTTP service (Splunkd httpd)
    - HTTP Server Header: Splunkd
    - HTTP Robots.txt: 1 disallowed entry
    - HTTP Title: splunkd

Summary:

The scan of IP address 10.0.0.126 revealed several open ports and services running on the target system. Notable services include Microsoft Windows RPC, Microsoft Windows netbios-ssn, Microsoft Windows Server 2008 R2 - 2012 microsoft-ds, Microsoft Terminal Services, and an SSL/HTTP service identified as Splunkd httpd. The host's exact operating system could not be determined during this scan.

3.1.5 Vulnerability Assessment Report for IP Address 10.0.0.175



```
└─$ sudo nmap -A -Pn 10.0.0.175
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 14:01 EDT
Nmap scan report for 10.0.0.175
Host is up (0.092s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Document
|_http-server-header: Apache/2.4.41 (Ubuntu)
8089/tcp open  ssl/http Splunkd httpd
|_http-title: splunkd
|_http-server-header: Splunkd
| http-robots.txt: 1 disallowed entry
|_/
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=9/14%OT=22%CT=1%CU=30935%PV=Y%DS=2%DC=T%G=Y%TM=65034A9
OS:D%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=109%TI=Z%II=I%TS=A)OPS(O1=M
OS:4ECST11NW7%O2=M4ECST11NW7%O3=M4ECNNT11NW7%O4=M4ECST11NW7%O5=M4ECST11NW7%
OS:O6=M4ECST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%
OS:DF=Y%T=40%W=F507%O=M4ECNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Scan Overview:

- Target IP Address: 10.0.0.175

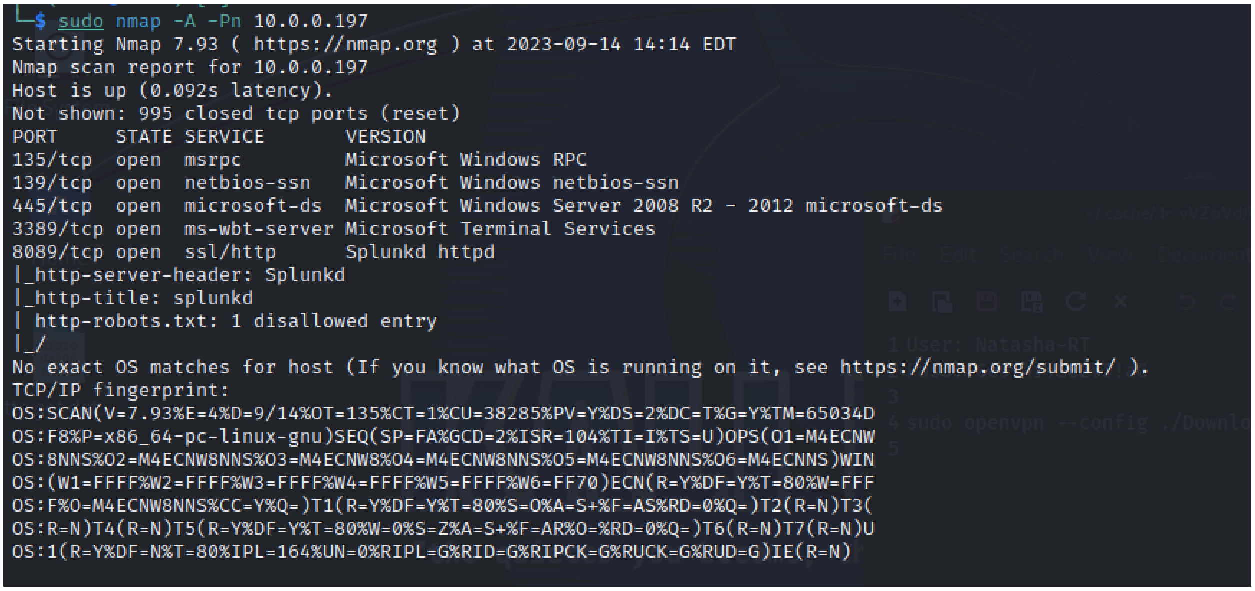
Open Ports and Services:

- Port 22/tcp: Open, SSH service (OpenSSH 8.2p1 Ubuntu 4ubuntu0.2)
- Port 80/tcp: Open, HTTP service (Apache httpd 2.4.41 on Ubuntu)
  - HTTP Server Header: Apache/2.4.41 (Ubuntu)
  - HTTP Title: Document
- Port 8089/tcp: Open, SSL/HTTP service (Splunkd httpd)
  - HTTP Server Header: Splunkd
  - HTTP Robots.txt: 1 disallowed entry
  - HTTP Title: splunkd

Summary:

The scan of IP address 10.0.0.175 revealed several open ports and services running on the target system. Notable services include SSH (OpenSSH 8.2p1 on Ubuntu), HTTP (Apache httpd 2.4.41 on Ubuntu), and an SSL/HTTP service identified as Splunkd httpd. The host's exact operating system could not be determined during this scan.

3.1.6 Vulnerability Assessment Report for IP Address 10.0.0.197



```
└─$ sudo nmap -A -Pn 10.0.0.197
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 14:14 EDT
Nmap scan report for 10.0.0.197
Host is up (0.092s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
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  ms-wbt-server Microsoft Terminal Services
8089/tcp open  ssl/http      Splunkd httpd
|_http-server-header: Splunkd
|_http-title: splunkd
| http-robots.txt: 1 disallowed entry
|_/
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=9/14%OT=135%CT=1%CU=38285%PV=Y%DS=2%DC=T%G=Y%TM=65034D
OS:F8%P=x86_64-pc-linux-gnu)SEQ(SP=FA%GCD=2%ISR=104%TI=I%TS=U)OPS(O1=M4ECNW
OS:8NNS%O2=M4ECNW8NNS%O3=M4ECNW8%O4=M4ECNW8NNS%O5=M4ECNW8NNS%O6=M4ECNNS)WIN
OS:(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFF
OS:F%O=M4ECNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(
OS:R=N)T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U
OS:1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=N)
```

Scan Overview:

- Target IP Address: 10.0.0.197

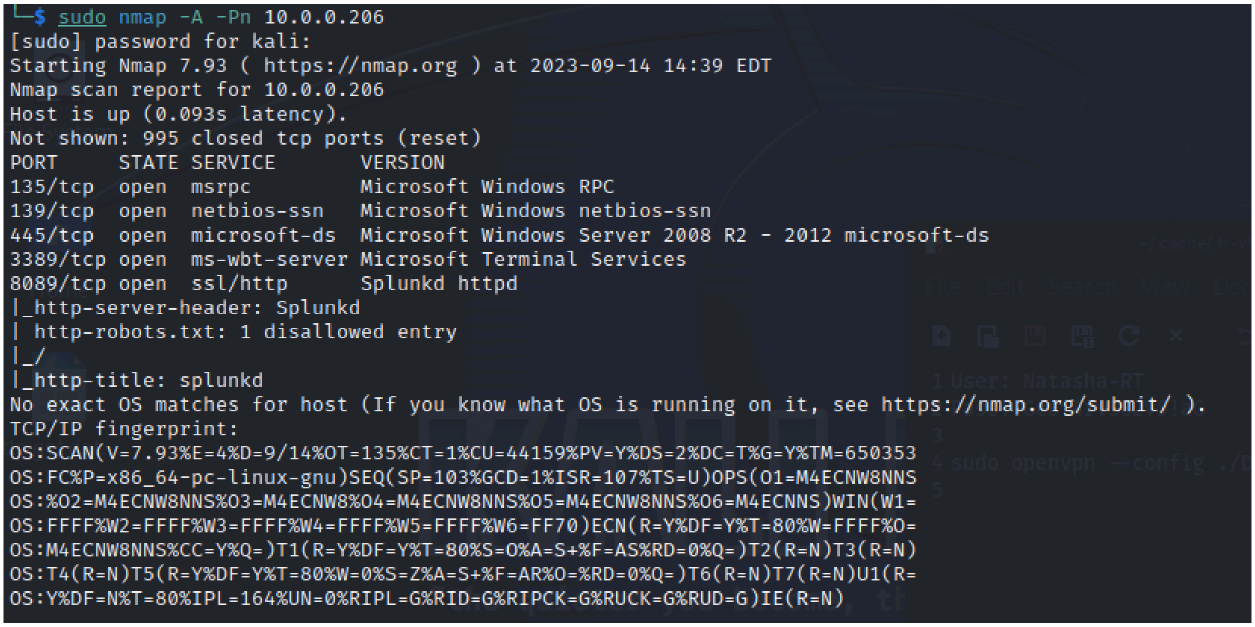
Open Ports and Services:

- Port 135/tcp: Open, Microsoft Windows RPC service
- Port 139/tcp: Open, Microsoft Windows netbios-ssn service
- Port 445/tcp: Open, Microsoft Windows Server 2008 R2 - 2012 microsoft-ds service
- Port 3389/tcp: Open, Microsoft Terminal Services (ms-wbt-server)
- Port 8089/tcp: Open, SSL/HTTP service (Splunkd httpd)
  - HTTP Server Header: Splunkd
  - HTTP Robots.txt: 1 disallowed entry
  - HTTP Title: splunkd

Summary:

The scan of IP address 10.0.0.197 identified several open ports and services running on the target system. Notable services include Microsoft Windows RPC (port 135), Microsoft Windows netbios-ssn (port 139), Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (port 445), Microsoft Terminal Services (port 3389), and an SSL/HTTP service identified as Splunkd httpd (port 8089).

3.1.7 Vulnerability Assessment Report for IP Address 10.0.0.206



```
└─$ sudo nmap -A -Pn 10.0.0.206
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 14:39 EDT
Nmap scan report for 10.0.0.206
Host is up (0.093s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
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  ms-wbt-server Microsoft Terminal Services
8089/tcp open  ssl/http      Splunkd httpd
|_http-server-header: Splunkd
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: splunkd
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=9/14%OT=135%CT=1%CU=44159%PV=Y%DS=2%DC=T%G=Y%TM=650353
OS:FC%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=107%TS=U)OPS(O1=M4ECNW8NNS
OS:%O2=M4ECNW8NNS%O3=M4ECNW8%O4=M4ECNW8NNS%O5=M4ECNW8NNS%O6=M4ECNNS)WIN(W1=
OS:FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=
OS:M4ECNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)
OS:T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=
OS:Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=N)
```

Scan Overview:

- Target IP Address: 10.0.0.206

Open Ports and Services:

- Port 135/tcp: Open, Microsoft Windows RPC service
- Port 139/tcp: Open, Microsoft Windows netbios-ssn service
- Port 445/tcp: Open, Microsoft Windows Server 2008 R2 - 2012 microsoft-ds service
- Port 3389/tcp: Open, Microsoft Terminal Services (ms-wbt-server)
- Port 8089/tcp: Open, SSL/HTTP service (Splunkd httpd)
  - HTTP Server Header: Splunkd
  - HTTP Robots.txt: 1 disallowed entry
  - HTTP Title: splunkd

Summary:

The scan of IP address 10.0.0.206 identified several open ports and services running on the target system. Notable services include Microsoft Windows RPC (port 135), Microsoft Windows netbios-ssn (port 139), Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (port 445), Microsoft Terminal Services (port 3389), and an SSL/HTTP service identified as Splunkd httpd (port 8089).

4.0 Maintaining Access

As the Binary Bandits 01, preserving access to a compromised system is a crucial aspect of our penetration test. It is imperative that we maintain the ability to re-enter a system even after it has been successfully exploited. This phase of the penetration test revolves around guaranteeing our continuous administrative control over the compromised system. We understand that certain exploits may only be applicable once, and once executed, we may lose the opportunity to regain access to the system. Therefore, our goal is to establish persistent access methods that ensure our control remains intact, enabling us to conduct further assessments, gather valuable intelligence, and simulate real-world threat scenarios effectively.

5.0 House Cleaning

As the Binary Bandits 01, our commitment to professionalism extends to the cleanup phase of our assessment. It is imperative that we leave no trace of our penetration test behind, ensuring the utmost discretion and security for our clients. The house cleaning segment of the assessment is dedicated to this critical task.

During this phase, our primary goal is to meticulously remove any remnants of our presence from the target systems. This includes eliminating any artifacts, tools, or user accounts that were created or manipulated during the penetration test. We understand that leaving behind fragments of our activities on an organization's computer can potentially lead to security issues in the future.

Upon successfully collecting trophies and achieving our assessment objectives within the Lab network, our team diligently removes all traces of our presence. This encompasses the removal of user accounts, passwords, and any Meterpreter services that may have been installed during the assessment. It is our commitment that Offensive Security, our client, should not need to undertake any additional cleanup efforts as a result of our engagement.

By conducting thorough house cleaning, we demonstrate our professionalism, respect for client environments, and commitment to ensuring that our penetration test activities have no adverse impact on the security and integrity of the systems we assess.

6.0 Conclusion

Binary Bandits 01, on behalf of Simcorp, executed a comprehensive internal penetration test. The team consisted of Natasha Siramarco, David Prutch, Raheem Reed, and Dustin Haggett. Our objective was to assess security and provide insights.

- Key Findings:
  - Identified vulnerabilities in the 10.0.0.0/24 network.
    Strongly recommend addressing these promptly for improved security.
- Assessment Highlights:
  - In-depth examination of open ports, services, and potential vulnerabilities.
  - Meticulous approach to uncover system details.

In summary, Binary Bandits 01 is dedicated to delivering professional penetration tests. We prioritize security and provide actionable insights. We stand ready to assist Simcorp in enhancing its cybersecurity posture.