OFFENSIVE SECURITY

Penetration Test Report for 10.0.0.74

Table of Contents

1.0 Comprehensive Network Discovery and Vulnerability Assessment Report for IP Address 10.0.0.74

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 on the specific IP address 10.0.0.74. 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 the specified target, IP address 10.0.0.74, as directed by our Red Team, Binary Bandits 01. Our team is responsible for adhering to a systematic methodology to gain access to this specific target, mirroring the processes involved in a real-world penetration test. This simulation aims to replicate the complexities of an actual penetration test on the target IP address, 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 on IP address 10.0.0.74 highlights the critical importance of promptly addressing the identified vulnerabilities specific to this target. We strongly advise Simcorp to initiate a comprehensive patching process for this IP address to mitigate these vulnerabilities effectively. It is essential to recognize that this system necessitates regular and consistent patching. Ensuring that it remains on a recurring patch schedule is vital to safeguard against potential future vulnerabilities that may arise on IP address

10.0.0.74. By adhering to a proactive patch management approach for this specific target, 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 to assess the specific target, IP address 10.0.0.74, outlining the steps taken to identify and exploit various systems and documenting the specific vulnerabilities discovered during our assessment of this target.

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. While our primary focus is on IP address 10.0.0.74, we have also included an overview of key findings and vulnerabilities within this broader network for context. The following table presents the results of our scan, highlighting notable findings and vulnerabilities across the network.

2.1 Scanned IP Address

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

3.0 Penetration

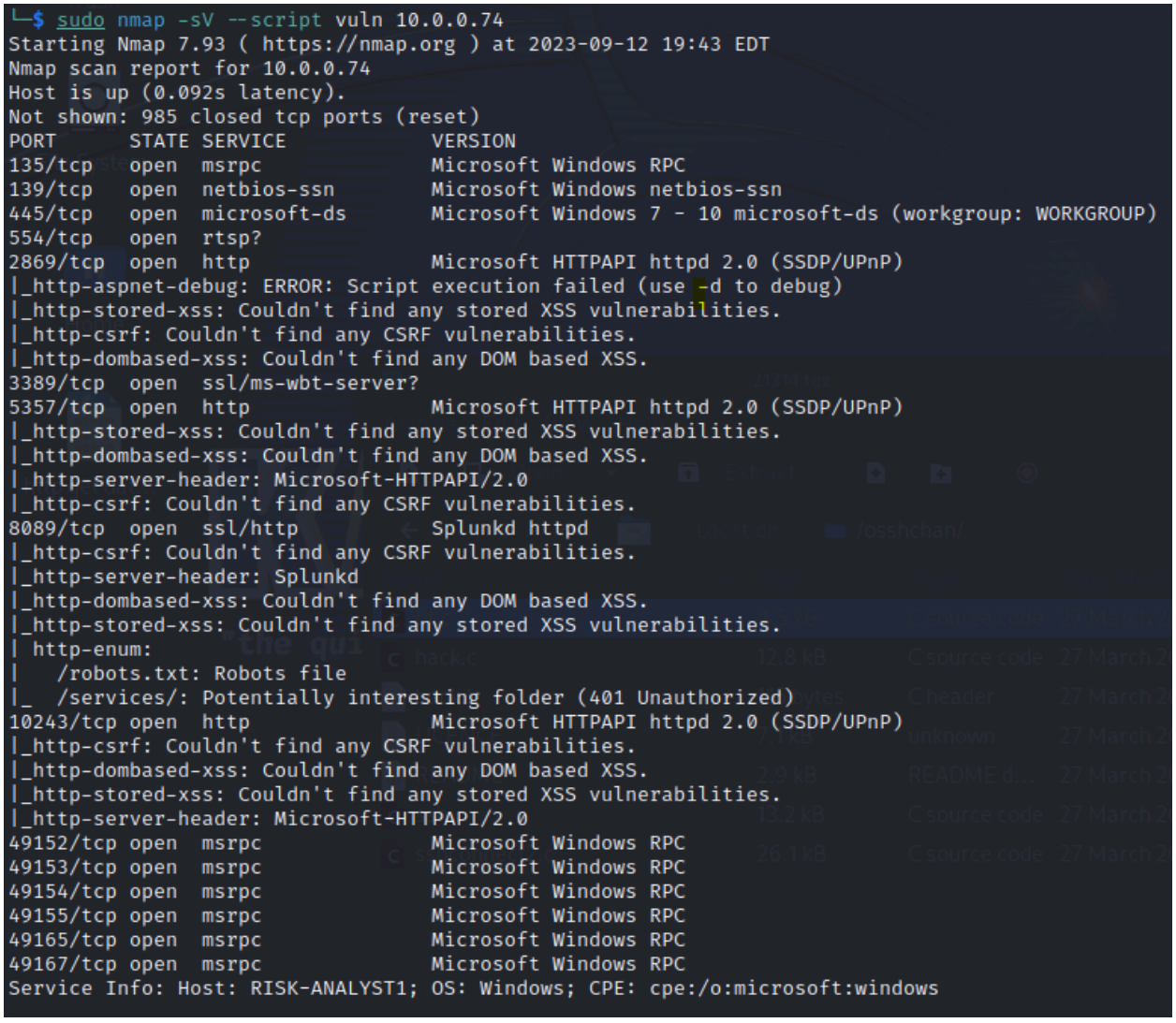
The penetration testing phase of our assessment is centered on gaining unauthorized access to the system at IP address 10.0.0.74. Throughout this penetration test, we successfully obtained access to this specific system within the IP range 10.0.0.0/24.

3.1 Service Enumeration

As part of our comprehensive penetration testing, we conducted service enumeration on the specified IP address 10.0.0.74. This critical phase involves collecting crucial information regarding the active services running on the target system. Such insights are invaluable to potential attackers, offering detailed knowledge about possible avenues for exploiting the 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 cases, certain ports may not be listed as part of this enumeration process.

3.1 Vulnerability Assessment Report for IP Address 10.0.0.74

Vulnerability scan



```
└─$ sudo nmap -sV --script vuln 10.0.0.74
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 19:43 EDT
Nmap scan report for 10.0.0.74
Host is up (0.092s 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)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
3389/tcp  open  ssl/ms-wbt-server?
5357/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
8089/tcp  open  ssl/http           Splunkd httpd
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: Splunkd
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /robots.txt: Robots file
|_  /services/: Potentially interesting folder (401 Unauthorized)
10243/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
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
Service Info: Host: RISK-ANALYST1; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
┌──(kali㉿kali)-[~]
└─$ rdesktop 10.0.0.74
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses and invalid security certificate which can not be trusted for
the following identified reasons(s);

 1. Certificate issuer is not trusted by this system.

     Issuer: CN=RISK-ANALYST1


Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection atempt will be aborted:

    Subject: CN=RISK-ANALYST1
     Issuer: CN=RISK-ANALYST1
 Valid From: Wed Sep  6 16:14:03 2023
         To: Thu Mar  7 15:14:03 2024

  Certificate fingerprints:

       [redacted]

Do you trust this certificate (yes/no)? yes
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific cer
Connection established using SSL.
disconnect: Logout initiated by user.
```

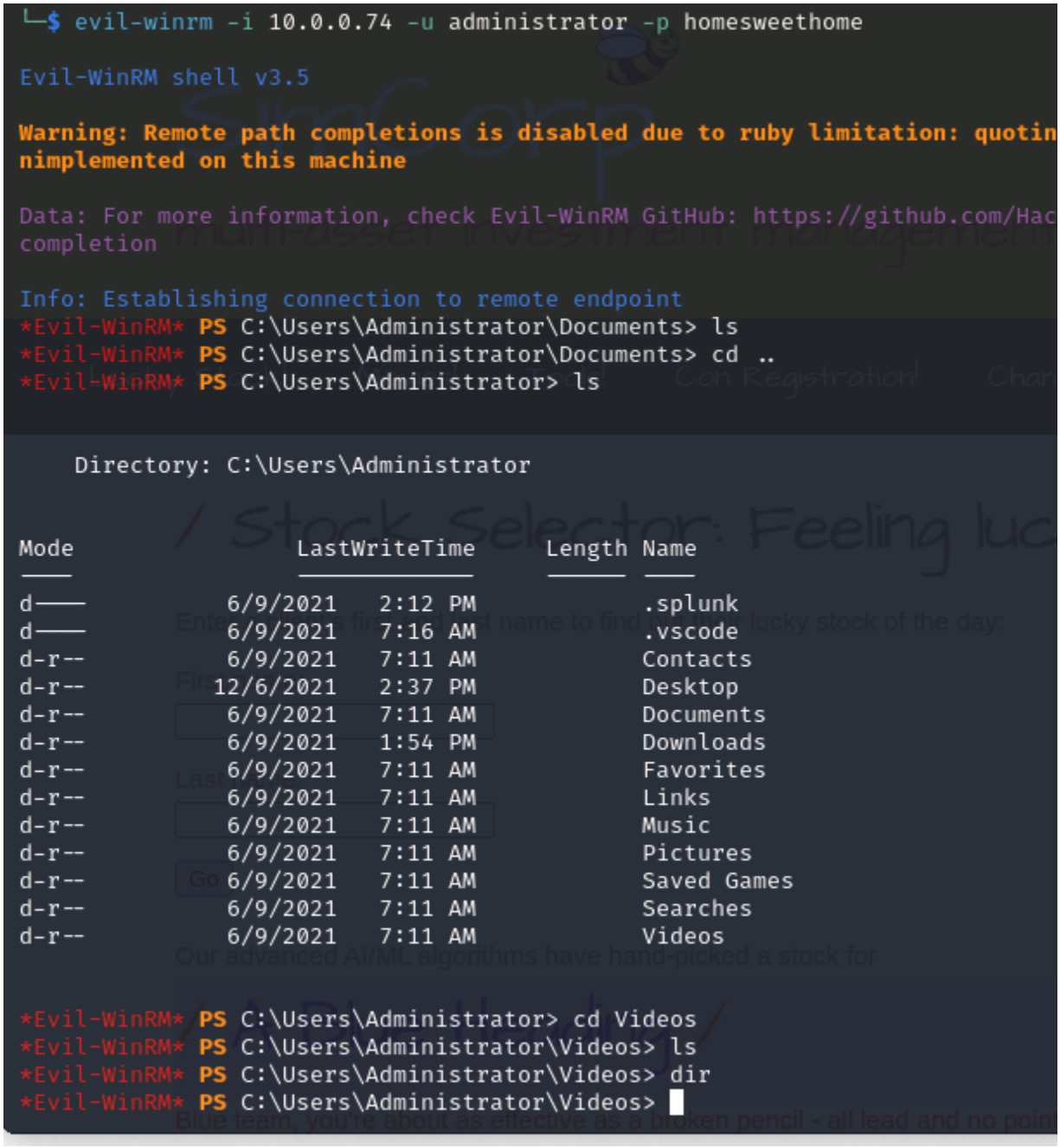
Enumeration command:

- nmap --script "rdp-enum-encryption or rdp-vuln-ms12-020 or rdp-ntlm-info" -p 3389 10.0.0.74

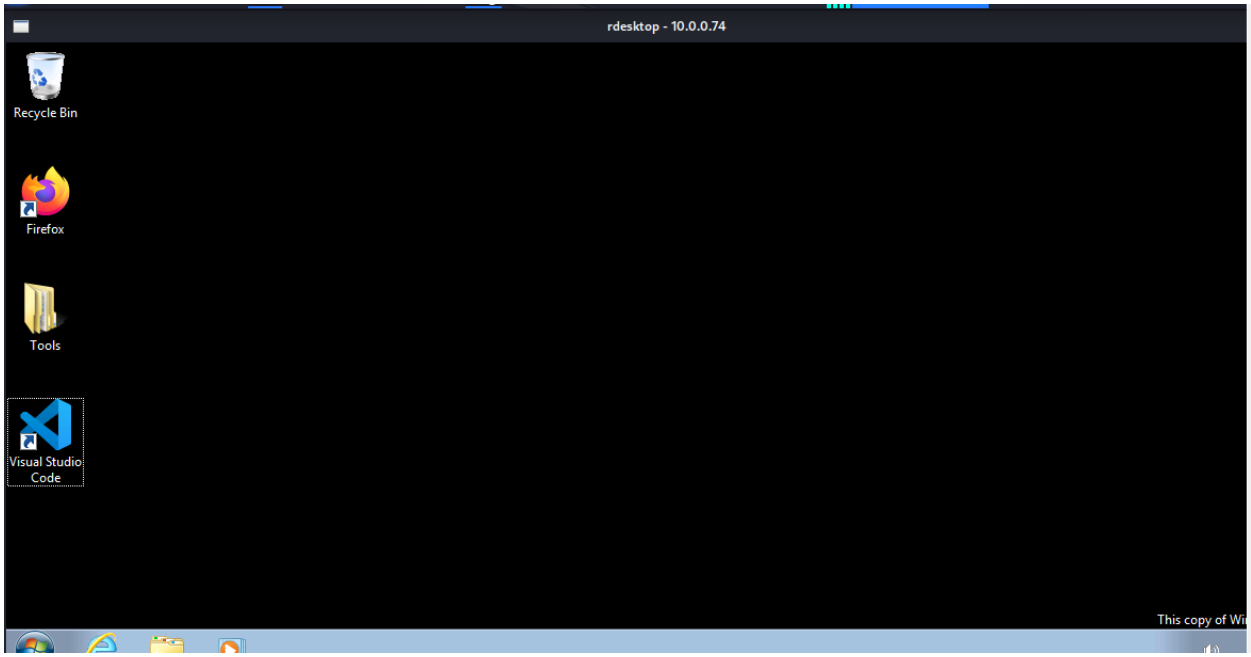
```
┌──(kali㉿kali)-[~]
└─$ nmap --script "rdp-enum-encryption or rdp-vuln-ms12-020 or rdp-ntlm-info" -p 3389 10.0.0.74
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-12 13:42 EDT
Nmap scan report for 10.0.0.74
Host is up (0.042s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-ntlm-info:
|   Target_Name: RISK-ANALYST1
|   NetBIOS_Domain_Name: RISK-ANALYST1
|   NetBIOS_Computer_Name: RISK-ANALYST1
|   DNS_Domain_Name: RISK-ANALYST1
|   DNS_Computer_Name: RISK-ANALYST1
|   Product_Version: 6.1.7601
|_  System_Time: 2023-09-12T17:42:28+00:00
| rdp-enum-encryption:
|   Security layer
|     CredSSP (NLA): SUCCESS
|     CredSSP with Early User Auth: SUCCESS
|     Native RDP: SUCCESS
|     RDSTLS: SUCCESS
|     SSL: SUCCESS
|   RDP Encryption level: Client Compatible
|     40-bit RC4: SUCCESS
|     56-bit RC4: SUCCESS
|     128-bit RC4: SUCCESS
|     FIPS 140-1: SUCCESS
|_  RDP Protocol Version:  RDP 5.x, 6.x, 7.x, or 8.x server

Nmap done: 1 IP address (1 host up) scanned in 60.59 seconds
```

  - Username: Has Been Identified
  - Password: Has Been Identified

evil-winrm:


└─$ evil-winrm -i 10.0.0.74 -u administrator -p homesweethome
Evil-WinRM shell v3.5
Warning: Remote path completions is disabled due to ruby limitation: quotin
nimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hac
completion
Info: Establishing connection to remote endpoint
Evil-WinRM PS C:\Users\Administrator\Documents> ls
Evil-WinRM PS C:\Users\Administrator\Documents> cd ..
Evil-WinRM PS C:\Users\Administrator> ls
Directory: C:\Users\Administrator
Mode LastWriteTime Length Name
d----- 6/9/2021 2:12 PM .splunk
d----- 6/9/2021 7:16 AM .vscode
d-r-- 6/9/2021 7:11 AM Contacts
d-r-- 12/6/2021 2:37 PM Desktop
d-r-- 6/9/2021 7:11 AM Documents
d-r-- 6/9/2021 1:54 PM Downloads
d-r-- 6/9/2021 7:11 AM Favorites
d-r-- 6/9/2021 7:11 AM Links
d-r-- 6/9/2021 7:11 AM Music
d-r-- 6/9/2021 7:11 AM Pictures
d-r-- 6/9/2021 7:11 AM Saved Games
d-r-- 6/9/2021 7:11 AM Searches
d-r-- 6/9/2021 7:11 AM Videos
Evil-WinRM PS C:\Users\Administrator> cd Videos
Evil-WinRM PS C:\Users\Administrator\Videos> ls
Evil-WinRM PS C:\Users\Administrator\Videos> dir
Evil-WinRM PS C:\Users\Administrator\Videos>

Remote Desktop Connection



4.0 Maintaining Access

As Binary Bandits 01, preserving access to the compromised system at IP address 10.0.0.74 is a crucial aspect of our penetration test. It is imperative that we maintain the ability to re-enter this specific 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 at IP address 10.0.0.74. 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 Binary Bandits 01, our commitment to professionalism extends to the cleanup phase of our assessment, particularly on IP address 10.0.0.74. It is imperative that we leave no trace of our penetration test behind on this specific system, ensuring the utmost discretion and security for our clients.

During this phase, our primary goal is to meticulously remove any remnants of our presence from IP address 10.0.0.74. 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 on IP address 10.0.0.74, our team diligently removes all traces of our presence. It is our commitment that Offensive Security, our client, should not need to undertake any additional cleanup efforts as a result of our engagement on this specific system.

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, including IP address 10.0.0.74.

6.0 Conclusion

Binary Bandits 01, on behalf of Simcorp, executed a comprehensive internal penetration test focusing on IP address 10.0.0.74. The team consisted of Natasha Siramarco, David Prutch, Raheem Reed, and Dustin Haggett. Our objective was to assess security and provide insights specific to this system.

Key Findings:

- Identified vulnerabilities on IP address 10.0.0.74.
- Strongly recommend addressing these promptly for improved security.

Assessment Highlights:

- In-depth examination of open ports, services, and potential vulnerabilities on IP address 10.0.0.74.
- Meticulous approach to uncover system details on IP address 10.0.0.74.

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, with specific attention to IP address 10.0.0.74.