OFFENSIVE SECURITY

Penetration Test Report for 10.0.0.197

Table of Contents

1.0 Comprehensive Network Discovery and Vulnerability Assessment Report for IP Address 10.0.0.197

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 10.0.0.197. 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 10.0.0.197, 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 10.0.0.197 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

10.0.0.197. 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 10.0.0.197, 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 10.0.0.197, 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
10.0.0.197	135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open 3389/tcp open ms-wbt-server 8089/tcp open ssl/http

3.0 Penetration

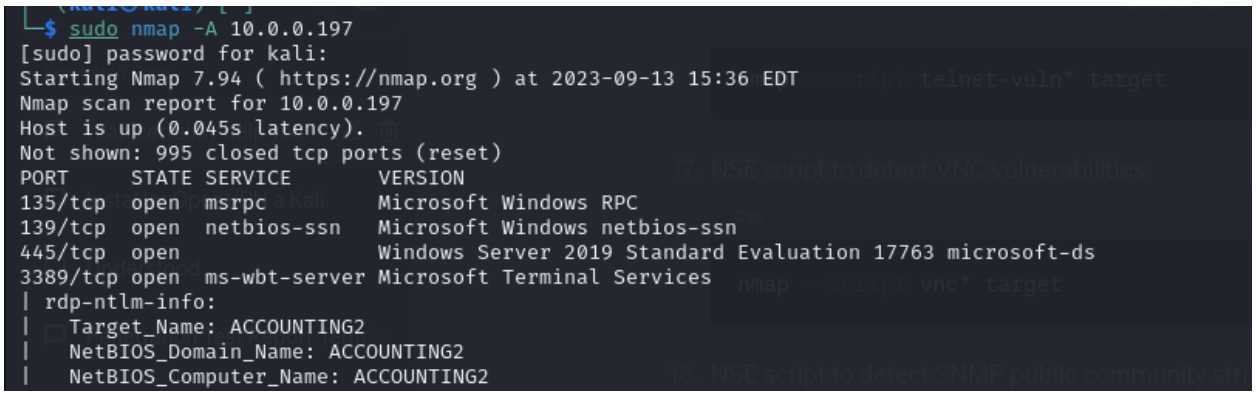
The penetration testing phase of our assessment is centered on gaining unauthorized access to the system at IP address 10.0.0.197. Throughout this penetration test, we successfully obtained access to this specific system within the IP range 10.0.0.0/24.

3.1 Service Enumeration

As part of our comprehensive penetration testing, we conducted service enumeration on the specified IP address 10.0.0.197. 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 Penetration Testing Discoveries of 10.0.0.197

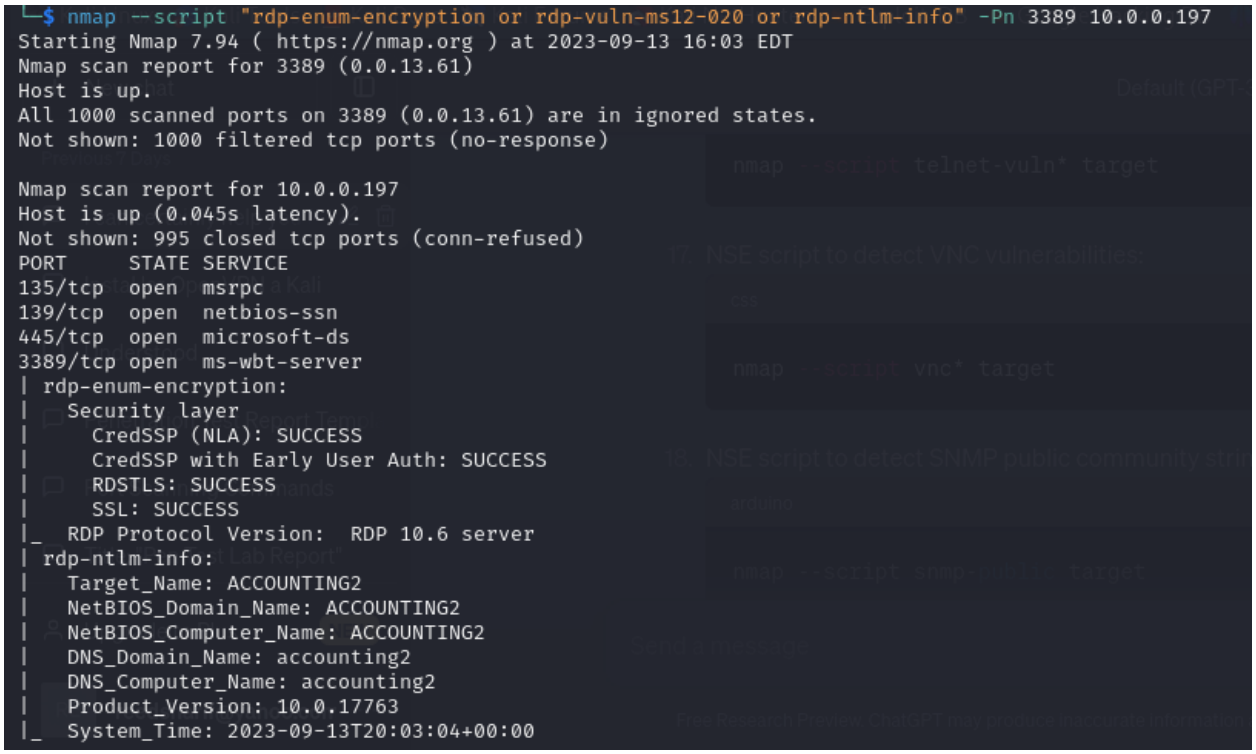
Vulnerability Scan



```
|   DNS_Domain_Name: accounting2
|   DNS_Computer_Name: accounting2
|   Product_Version: 10.0.17763
|_  System_Time: 2023-09-13T19:37:08+00:00
|_ssl-date: 2023-09-13T19:37:16+00:00; -8s from scanner time.
| ssl-cert: Subject: commonName=accounting2
| Not valid before: 2023-09-06T20:13:20
|_Not valid after:  2024-03-07T20:13:20
8089/tcp open  ssl/http      Splunkd httpd
|_http-title: splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2021-06-07T19:35:56
|_Not valid after:  2024-06-06T19:35:56
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: 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=7.94%E=4%D=9/13%OT=135%CT=1%CU=40221%PV=Y%DS=2%DC=T%G=Y%TM=65020F
OS:74%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10E%TS=U)SEQ(SP=101%GCD=1%
OS:ISR=10E%TI=I%TS=U)SEQ(SP=FD%GCD=1%ISR=110%TI=RD%TS=U)OPS(O1=M4ECNW0NNS%O
OS:2=M4ECNW8NNS%O3=M4ECNW8%O4=M4ECNW8NNS%O5=M4ECNW0NNS%O6=M4ECNNS)OPS(O1=M4
OS:ECNW8NNS%O2=M4ECNW8NNS%O3=M4ECNW8%O4=M4ECNW8NNS%O5=M4ECNW8NNS%O6=M4ECNNS
OS:)WIN(W1=FA00%W2=FFFF%W3=FFFF%W4=FFFF%W5=FA00%W6=FF70)WIN(W1=FFFF%W2=FFFF
OS:%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M4ECNW8NNS%C
OS:C=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=O%F=AS%RD=0%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F
OS:=AS%RD=0%Q=)T2(R=N)T2(R=Y%DF=Y%T=80%W=FA00%S=O%A=O%F=AS%O=M4ECNW0NNS%RD=
OS:0%Q=)T3(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)
OS:T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)I
OS:E(R=N)

Network Distance: 2 hops
```

```
Host script results:
|_clock-skew: mean: 1h23m52s, deviation: 3h07m50s, median: -8s
| smb2-time:
|   date: 2023-09-13T19:37:08
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: ACCOUNTING2, NetBIOS user: <unknown>, NetBIOS MAC: 06:be:eb:02:f1:45 (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows Server 2019 Standard Evaluation 17763 (Windows Server 2019 Standard Evaluation 6.3)
|   Computer name: accounting2
|   NetBIOS computer name: ACCOUNTING2\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-09-13T12:37:08-07:00

TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1   44.15 ms 172.27.232.1
2   44.22 ms 10.0.0.197

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.25 seconds
```

Enumeration Scan:
nmap --script "rdp-enum-encryption or rdp-vuln-ms12-020 or rdp-ntlm-info" -Pn 3389 10.0.0.197



4.0 Maintaining Access

As Binary Bandits 01, preserving access to the compromised system at IP address 10.0.0.197 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 10.0.0.197. 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 10.0.0.197. 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 10.0.0.197. 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 10.0.0.197, 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 10.0.0.197.

6.0 Conclusion

Binary Bandits 01, on behalf of Simcorp, executed a comprehensive internal penetration test focusing on IP address 10.0.0.197. 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 10.0.0.197.
- Strongly recommend addressing these promptly for improved security.

Assessment Highlights:

- In-depth examination of open ports, services, and potential vulnerabilities on IP address 10.0.0.197.
- Meticulous approach to uncover system details on IP address 10.0.0.197.

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 10.0.0.197.