Assignment 2: System Compromise

Business Confidential

Date: 10 February 2026

Project: PS-A2

Version 1.0

Table of Contents

1. Confidentiality Statement

This document is the exclusive property of Rapid2 On Metasploitable-2 and PENTESTER SIDDIQ. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Rapid2 and PENTESTER SIDDIQ. Rapid2 may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

2. Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period. Time-limited engagements do not allow for a full evaluation of all security controls. PENTESTER SIDDIQ prioritized the assessment to identify the weakest security controls an attacker would exploit. PENTESTER SIDDIQ recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

3. Contact Information

Name	Title	Contact Information
Rapid2		
Mr.Xyz	Global Information Security Manager	Email: xyz@Rapid2.com
Pentester Siddiq		
Mr.Siddiq Baig	Lead Penetration Tester	Email: contact@pentestersiddiq.com

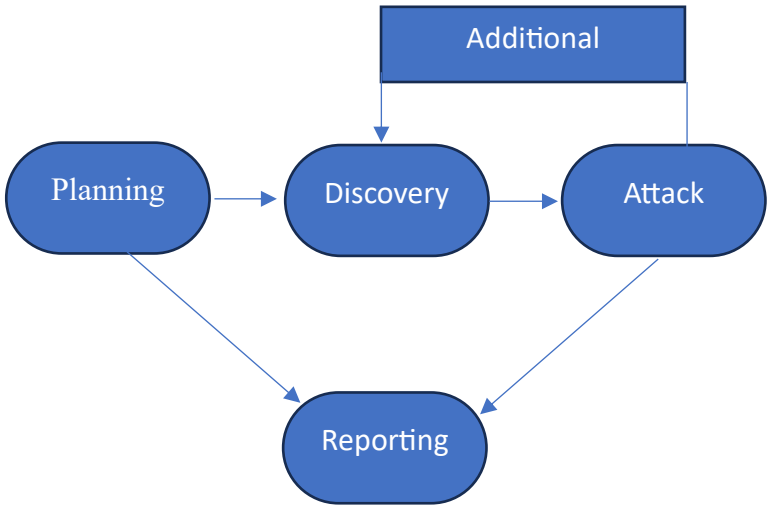
4. Assessment Overview

From February 8th, 2026 to February 10th, 2026, Rapid2 engaged Pentester Siddiq to perform a simulated security assessment against a scoped internal lab environment. The objective of this engagement was to evaluate the security posture of a Linux-based system within Rapid2's internal network and identify security weaknesses when compared to commonly accepted security best practices.

The assessment included a simulated internal penetration test conducted in a controlled lab environment. Testing activities were guided by generally accepted penetration testing methodologies, including concepts outlined in the NIST SP 800-115 Technical Guide to Information Security Testing and the OWASP Testing Guide (v4).

The penetration testing activities were conducted across the following phases:

- Planning – Engagement objectives, scope, and rules of engagement were defined prior to testing.
- Discovery – Scanning and enumeration were performed to identify exposed services, potential vulnerabilities, and misconfigurations.
- Attack – Identified vulnerabilities were validated through exploitation to assess real-world impact and potential risk.
- Reporting – All confirmed vulnerabilities, exploitation results, and remediation recommendations were documented.



5. Assessment Components

Internal Penetration

The internal penetration test simulated an attacker operating from within Rapid2's internal network against a scoped Linux-based system. The objective of this assessment was to identify exposed services, security misconfigurations, and known vulnerabilities that could be exploited by an internal threat actor.

Testing activities included network scanning, service enumeration, vulnerability identification, and controlled exploitation of discovered weaknesses. The assessment focused on validating the real-world impact of insecure services, weak authentication mechanisms, and outdated software versions that could result in unauthorized system access.

Where exploitation was successful, post-exploitation activities were performed to confirm the level of access obtained and assess the potential impact to the target system. No lateral movement, domain-based attacks, or data exfiltration activities were conducted as part of this engagement.

6. Scope & Limitations

Scope

The scope of this engagement was limited to a single Linux-based system within Rapid2's simulated internal lab environment. The objective was to identify and exploit security weaknesses that could be leveraged by an internal attacker with network access.

The following system was included in scope:

- Target System: Metasploitable2
- Operating System: Linux
- IP Address: 10.0.2.3
- Assessment Type: Simulated Internal Penetration Test

Testing activities focused on identifying exposed services, vulnerable software versions, weak authentication mechanisms, and insecure configurations that could lead to unauthorized system access.

Limitations

This assessment was conducted in a controlled academic lab environment and was intentionally limited in scope. The following activities were out of scope for this engagement:

- Testing of multiple hosts or network segments
- Active Directory or domain-based attacks
- Lateral movement between systems
- Denial-of-Service (DoS) attacks
- Data exfiltration or persistence mechanisms

All findings documented in this report reflect the system state at the time of testing and are based solely on the scoped target.

7. Methodology

The penetration testing activities were conducted using a structured methodology that mirrors real-world internal penetration testing engagements. The goal of this approach was to systematically identify, validate, and document security weaknesses within the scoped target system.

The following phases were performed during the assessment:

Reconnaissance and Enumeration

Initial reconnaissance was conducted to identify active services and exposed network ports on the target system. Service enumeration and version detection were performed to discover potentially vulnerable software and misconfigurations.

Vulnerability Identification

Identified services were analyzed for known vulnerabilities, insecure configurations, and weak authentication mechanisms that could be exploited by an internal attacker.

Exploitation

Confirmed vulnerabilities were exploited in a controlled manner to validate their impact and determine the level of access that could be obtained. Exploitation focused on achieving unauthorized system access while minimizing disruption to the target system.

Post-Exploitation

Where access was successfully obtained, post-exploitation activities were conducted to verify user privileges and assess the severity of compromise. No persistence or data exfiltration activities were performed.

Reporting

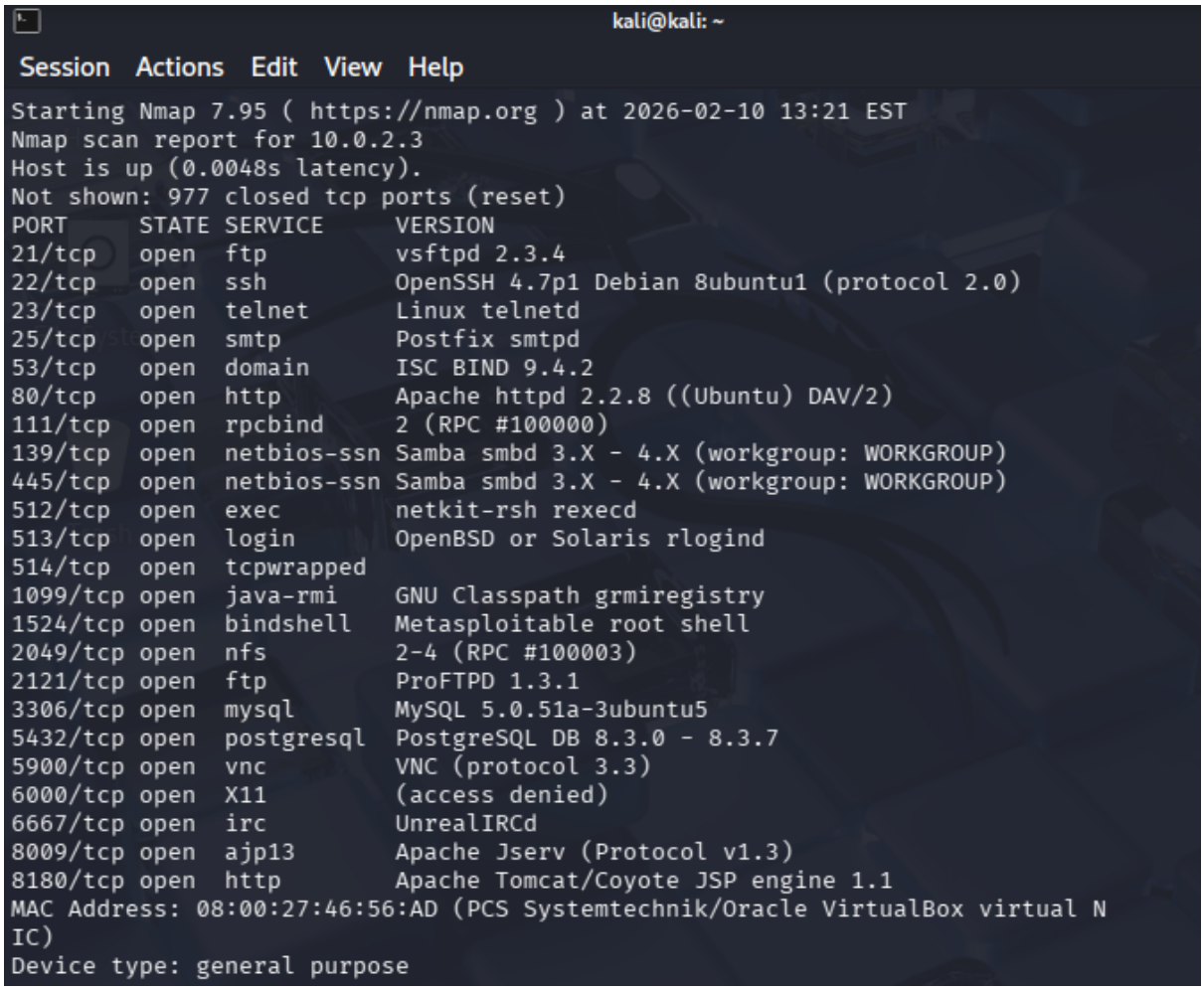
All confirmed vulnerabilities, exploitation results, and remediation recommendations were documented to provide a clear understanding of risk and impact.

8. Findings Summary

The following security findings were identified during the internal penetration test conducted against Rapid2's simulated lab environment. Each finding was evaluated based on the likelihood of exploitation and the potential impact to the target system if successfully exploited.

ID	Vulnerability	Affected Service	Port(s)	Risk Level	Likelihood	Impact
F-01	FTP Backdoor Vulnerability (vsftpd 2.3.4)	FTP	21	**Critical**	High	Full system compromise with root-level access
F-02	Samba Command Injection Vulnerability (user_map_script)	SMB	139, 445	**Critical**	High	Remote command execution resulting in root access
F-03	Weak Authentication on Telnet Service	Telnet	23	**High**	High	Unauthorized system access and privilege escalation
F-04	Insecure Remote Shell Services Enabled	rexecd, rlogind	512, 513	**High**	Medium	Unauthorized remote command execution
F-05	Unauthenticated Remote Desktop Access	VNC	5900	**High**	Medium	Full remote desktop access to the system
F-06	Exposed Development and Management Services	Java RMI, Bind Shell	1099, 1524	**High**	Medium	Arbitrary code execution and backdoor access
F-07	Outdated and Unsecured Database Services	MySQL, PostgreSQL	3306, 5432	**Medium**	Medium	Exposure or manipulation of sensitive data
F-08	Outdated Web and Application Services	Apache HTTPD, Tomcat	80, 8180	**Medium**	Medium	Web-based exploitation and information disclosure

Evidence:



9. Detailed Findings and Exploitation

9.1 F-01 – FTP Backdoor Vulnerability (vsftpd 2.3.4)

Description

During the enumeration phase, the FTP service running on port 21 was identified as vsftpd version 2.3.4. This version is known to contain a backdoor vulnerability that allows attackers to gain unauthorized remote access to the system.

The vulnerable service was exposed on the internal network and did not require authentication to exploit, making it a critical security weakness.

Vulnerability Classification

- CVE: CVE-2011-2523

- CWE: CWE-306 – Missing Authentication for Critical Function
- CVSS v3.1 Base Score: 10.0 (Critical)
- CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

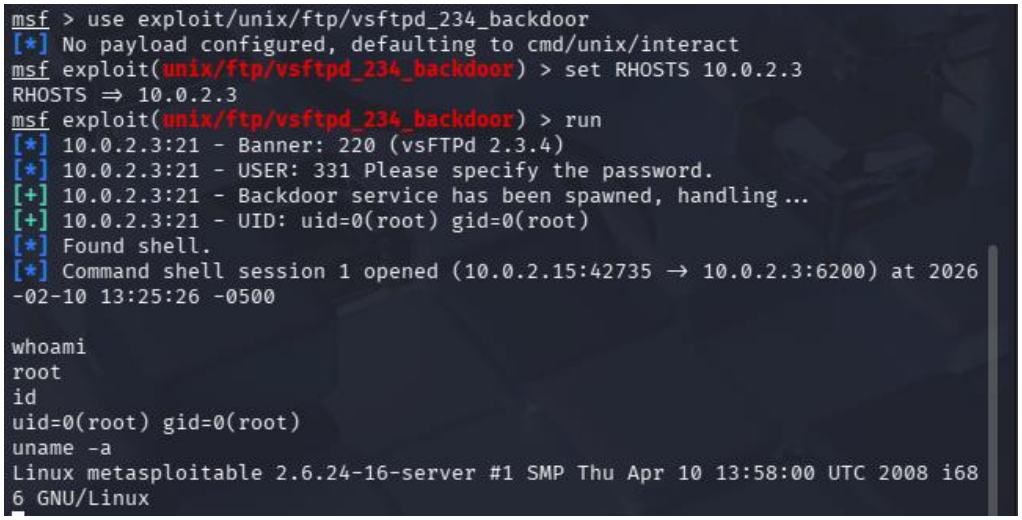
Exploitation Details

The vulnerability was exploited using the Metasploit Framework. The exploit successfully triggered the backdoor functionality and established a command shell on the target system

Validation of Access

After exploitation, standard system commands were executed to validate the level of access obtained. The results confirmed that the attacker gained root-level privileges on the target system.

Evidence:



Security Impact

The successful exploitation of this vulnerability allows an attacker to gain full control of the system. With root-level access, an attacker could modify system files, install persistent backdoors, disrupt services, or leverage the compromised host to attack other internal systems.

Remediation Recommendations

- Remove or upgrade the vulnerable vsftpd service
- Disable FTP if not required for business operations
- Restrict access to legacy services using firewall controls
- Implement regular patch management processes

9.2 F-02 – Samba Command Injection Vulnerability (user_map_script)

Description

During the enumeration phase, the Samba service running on ports 139 and 445 was identified as an outdated and vulnerable version of Samba smbd 3.x–4.x. This version is susceptible to the user_map_script command injection vulnerability, which allows remote attackers to execute arbitrary system commands without authentication.

The Samba service was exposed within the internal network and did not require valid credentials for exploitation, significantly increasing the risk of compromise.

Vulnerability Classification

- CVE: CVE-2007-2447
- CWE: CWE-77 – Command Injection
- CVSS: 10.0 (Critical)

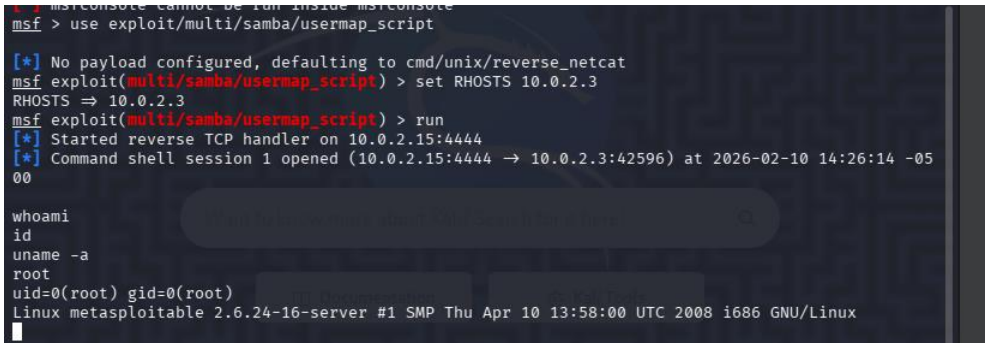
Exploitation Details

The vulnerability was exploited using the Metasploit Framework module:

exploit/multi/samba/usermap_script

After configuring the target host and executing the module, a reverse shell session was successfully established on the target system.

Evidence:



Validation of Access

Following successful exploitation, system-level commands were executed to verify the privilege level of the session. The output confirmed that the session was running with root-level privileges, indicating complete compromise of the system.

Example validation commands:

```
whoami
id
uname -a
```

The results confirmed **uid=0 (root)** access on the target host.

Security Impact

This vulnerability allows unauthenticated remote command execution with root privileges. An attacker exploiting this flaw could:

- Gain full administrative control of the system
- Modify or delete system files
- Install persistent backdoors
- Use the compromised host to pivot within the internal network

Because exploitation does not require valid credentials, this vulnerability represents a severe security risk.

Remediation Recommendations

- Upgrade Samba to a patched and supported version
- Disable unnecessary SMB services if not required
- Restrict access to SMB ports (139/445) using firewall controls
- Conduct regular patch management and vulnerability scanning

9.3 F-03 – Weak Authentication on Telnet Service

Description

During service enumeration, the Telnet service was identified as running on port 23. Telnet is an insecure remote access protocol that transmits credentials in plaintext and does not provide encryption.
Further testing revealed that the service allowed authentication using weak default credentials (msfadmin:msfadmin). The use of weak or default credentials significantly increases the likelihood of unauthorized access by internal or external attackers.

Vulnerability Classification:

- CWE: CWE-798 – Use of Hard-coded Credentials
- CWE-319 – Cleartext Transmission of Sensitive Information
- Type: Misconfiguration / Weak Authentication

Exploitation Details

A connection to the Telnet service was established from the attacker machine using the following command:

telnet 10.0.2.3

The login prompt accepted the default credentials:

Username: msfadmin
Password: msfadmin

Authentication was successful, and access to the system shell was granted without requiring advanced exploitation techniques.

Evidence:

Validation of Access

After logging in, system commands were executed to confirm access to the target system.

Example validation commands:

whoami
id

The output confirmed authenticated access to the system under the msfadmin user account. From this position, privilege escalation could potentially be attempted, depending on system configuration.

Security Impact

The presence of Telnet combined with weak credentials exposes the system to unauthorized access. Since Telnet transmits credentials in plaintext, attackers could also intercept login information through network sniffing attacks.

If exploited in a real environment, this weakness could allow attackers to:

- Gain unauthorized internal access
- Escalate privileges
- Move laterally within the network
- Access sensitive data

Remediation Recommendations

- Disable the Telnet service and replace it with SSH
- Enforce strong password policies
- Remove default or weak credentials
- Implement account lockout policies and monitoring

10. Overall Risk Analysis

The internal penetration test conducted against Rapid2's simulated lab environment identified multiple critical security weaknesses that allow unauthorized access and full system compromise.

The most severe findings involved vulnerabilities that enabled unauthenticated remote code execution with root-level privileges, specifically:

- FTP Backdoor Vulnerability (vsftpd 2.3.4)
- Samba Command Injection Vulnerability (user_map_script)

Both vulnerabilities allowed direct system compromise without requiring valid credentials. Successful exploitation resulted in complete administrative control of the target host.

Additionally, the presence of insecure services such as Telnet with weak authentication mechanisms significantly increases the likelihood of unauthorized access within the internal environment.

Risk Themes Identified

The assessment revealed several recurring security issues:

- Use of outdated and vulnerable software versions
- Insecure legacy services enabled by default
- Weak or default authentication credentials
- Lack of service hardening and network restrictions

If deployed in a real production environment, these weaknesses could allow an attacker to:

- Gain full control of internal systems
- Modify or delete critical system files

- Establish persistence mechanisms
- Use compromised hosts to pivot deeper into the network

Overall, the security posture of the assessed system is considered high risk due to the presence of multiple critical vulnerabilities that can be exploited with minimal effort.

11. Remediation Summary

The vulnerabilities identified during this assessment stem primarily from outdated software versions, insecure legacy services, and weak authentication mechanisms. Addressing these issues will significantly reduce the attack surface and improve the overall security posture of the environment.
The following remediation actions are recommended:

1. Patch Management and Software Updates

All outdated services, including FTP (vsftpd), Samba, and web application components, should be upgraded to supported and secure versions. A structured patch management process should be implemented to ensure regular updates and vulnerability remediation.

2. Disable Unnecessary Services

Legacy and insecure services such as Telnet, rexecd, rlogin, and unused bind shells should be disabled if not required for operational purposes. Reducing exposed services minimizes potential attack vectors.

3. Replace Insecure Protocols

Telnet should be replaced with SSH to ensure encrypted remote access. Plaintext authentication protocols should not be permitted in production environments.

4. Strengthen Authentication Controls

- Remove default credentials
- Enforce strong password policies
- Implement account lockout mechanisms
- Apply the principle of least privilege

5. Network Segmentation and Access Control

Restrict access to critical services such as SMB, database servers, and management interfaces through firewall rules and internal network segmentation.

6. Continuous Monitoring and Vulnerability Scanning

Regular vulnerability assessments and internal security testing should be conducted to proactively identify and remediate emerging threats.
By implementing these remediation measures, Rapid2 can significantly reduce the likelihood of system compromise and improve overall internal security resilience.

12.Conclusion

This simulated internal penetration test conducted against Rapid2's lab environment demonstrated that the target system contains multiple critical security weaknesses that can be exploited to achieve full system compromise.

Through structured enumeration and controlled exploitation, it was confirmed that outdated services, insecure configurations, and weak authentication mechanisms expose the system to unauthorized access. Notably, exploitation of the FTP backdoor vulnerability and the Samba command injection flaw resulted in root-level access, highlighting the severity of unpatched and misconfigured services.

The presence of insecure legacy protocols such as Telnet further increases the risk of compromise, particularly within internal environments where trust assumptions may reduce defensive controls.

Overall, the assessment indicates that the system, in its current state, presents a high security risk. Immediate remediation of critical vulnerabilities, removal of insecure services, and implementation of structured patch management and access control practices are strongly recommended.

This engagement demonstrates the importance of proactive vulnerability management and regular security assessments to identify and remediate weaknesses before they can be exploited by malicious actors.

Last Page