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

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).

LIKELIHOOD / CONSEQUENCES	INSIGNIFICANT 1	MINOR 2	MODERATE 3	MAJOR 4	CATASTROPHIC 5
ALMOST CERTAIN 5	MEDIUM	HIGH	HIGH	EXTREME	EXTREME
LIKELY 4 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

CONSERVATIVE RISK APPETITE — 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.

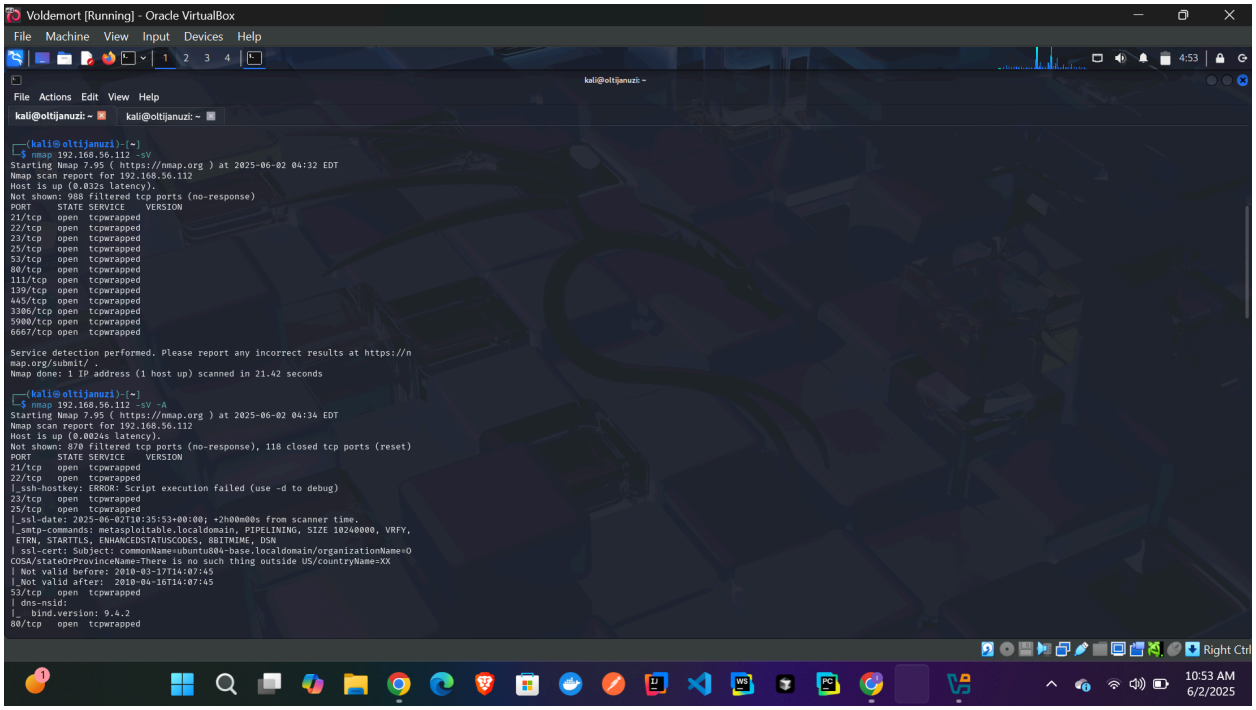
• Network -level, technical penetration testing against internet facing hosts.

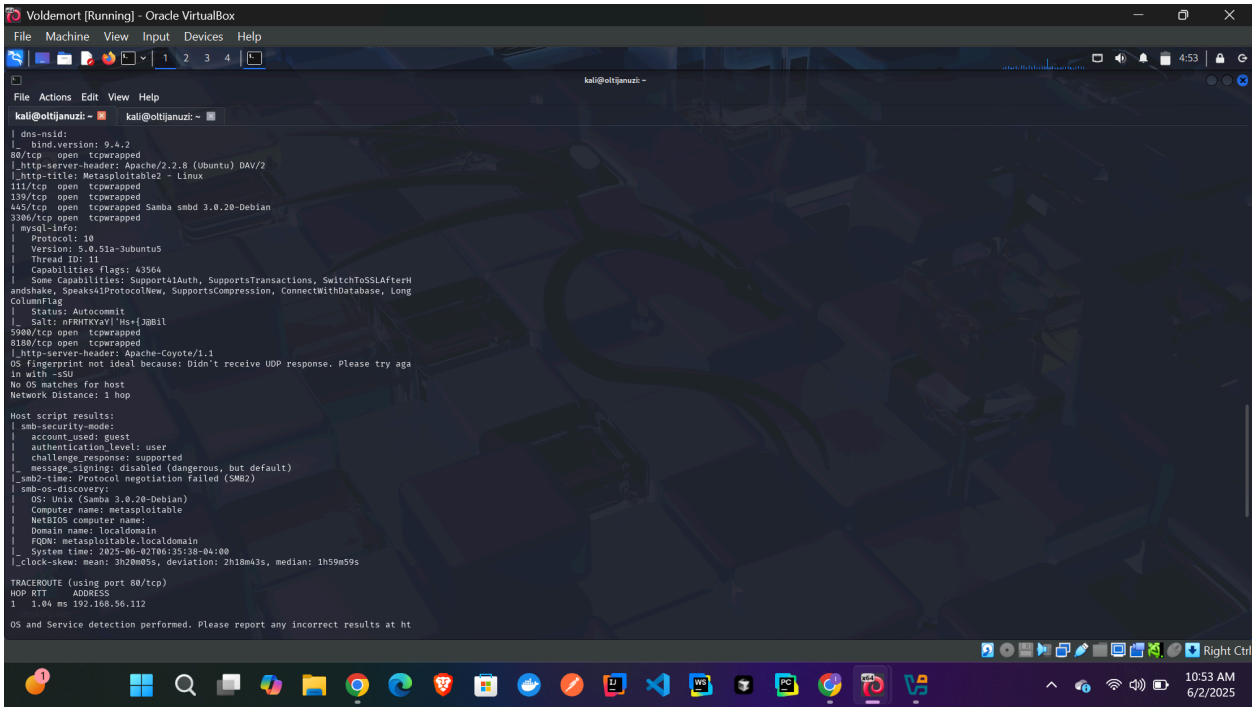
(Remainder of page left intentionally blank)

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@oltijanuzi: ~
┌──(kali㉿oltijanuzi)-[~]
└─$ nmap 192.168.56.112 -sV
Starting Nmap 7.95 (https://nmap.org) at 2025-06-02 04:32 EDT
Nmap scan report for 192.168.56.112
Host is up (0.032s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open tcpwrapped
22/tcp open tcpwrapped
23/tcp open tcpwrapped
25/tcp open tcpwrapped
53/tcp open tcpwrapped
80/tcp open tcpwrapped
111/tcp open tcpwrapped
139/tcp open tcpwrapped
445/tcp open tcpwrapped
3306/tcp open tcpwrapped
5900/tcp open tcpwrapped
6667/tcp open tcpwrapped
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
┌──(kali㉿oltijanuzi)-[~]
└─$ nmap 192.168.56.112 -sV -A
Starting Nmap 7.95 (https://nmap.org) at 2025-06-02 04:34 EDT
Nmap scan report for 192.168.56.112
Host is up (0.002s latency).
Not shown: 870 filtered tcp ports (no-response), 118 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open tcpwrapped
22/tcp open tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
23/tcp open tcpwrapped
25/tcp open tcpwrapped
|_ssl-date: 2025-06-02T10:35:53+00:00; +2h00m00s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
53/tcp open tcpwrapped
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open tcpwrapped
Right Ctrl
10:53 AM
6/2/2025

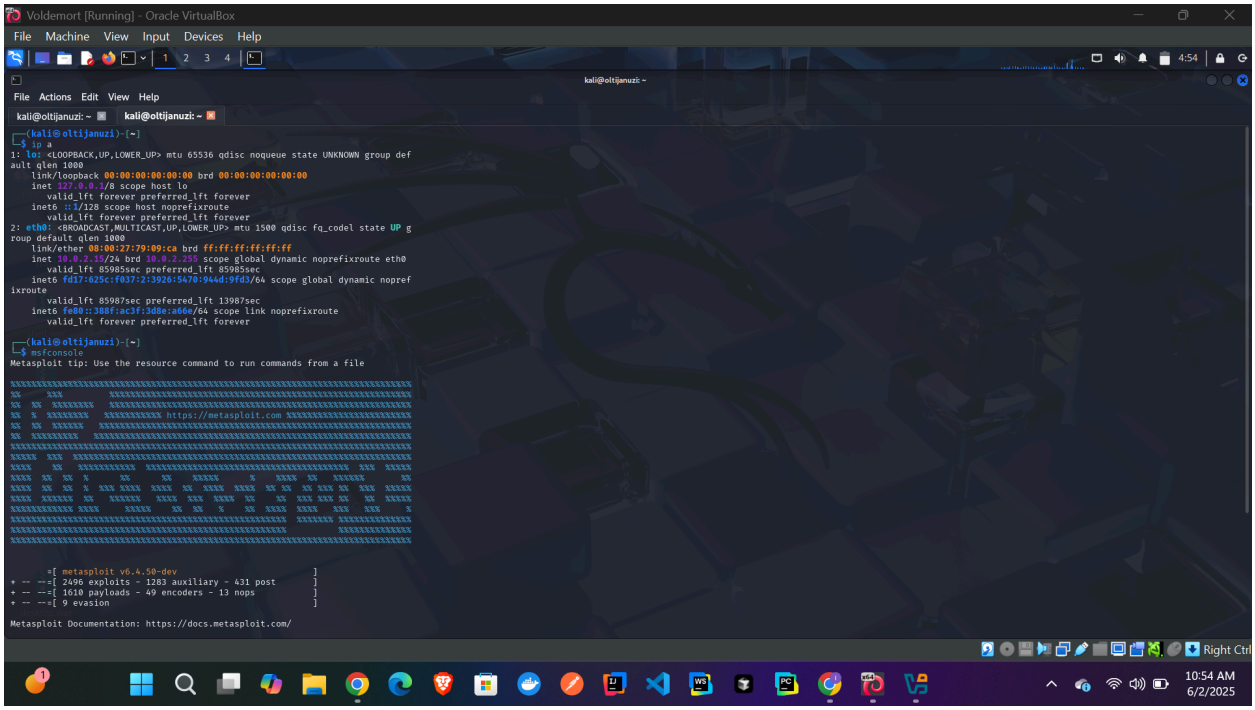

Voldemort [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@oltijanuzi: ~
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open tcpwrapped
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open tcpwrapped
139/tcp open tcpwrapped
445/tcp open tcpwrapped Samba smbd 3.0.20-Debian
3306/tcp open tcpwrapped
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 11
| Capabilities flags: 43564
| Some Capabilities: Support41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, SupportsCompression, ConnectWithDatabase, LongColumnFlag
| Status: Autocommit
|_ Salt: nFRHTKYaY!`Hs+[J@Bil
5900/tcp open tcpwrapped
8180/tcp open tcpwrapped
|_http-server-header: Apache-Coyote/1.1
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-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2025-06-02T06:35:38-04:00
|_clock-skew: mean: 3h20m05s, 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 ht
Right Ctrl
10:53 AM
6/2/2025

Findings

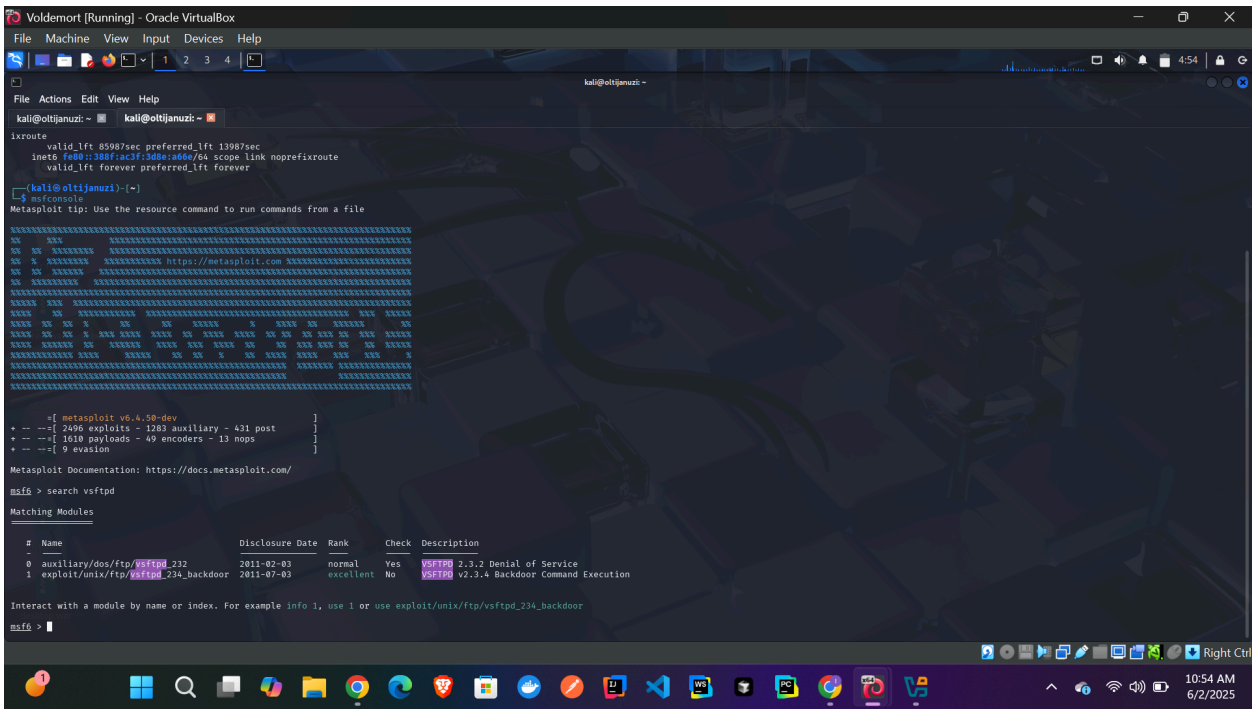
- FTP (21): VSFTPD 2.3.4
- SSH (22)
- HTTP (80): Apache
- Samba (445): smbd 3.x
- MySQL (3306)
- Tomcat (8180)
- More...

Exploiting VSFTPD 2.3.4 Backdoor

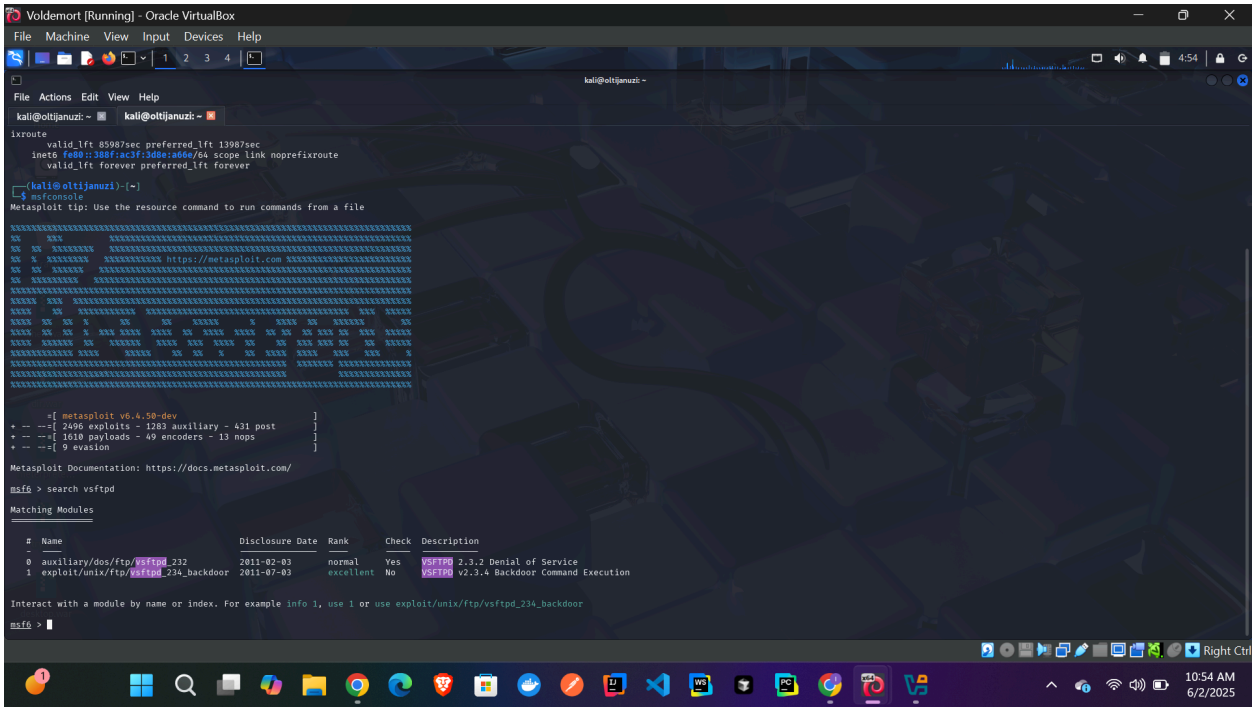
Because of the outdated version I was able to gain control over the system easily, to perform this we open msfconsole first and use exploits to gain access.



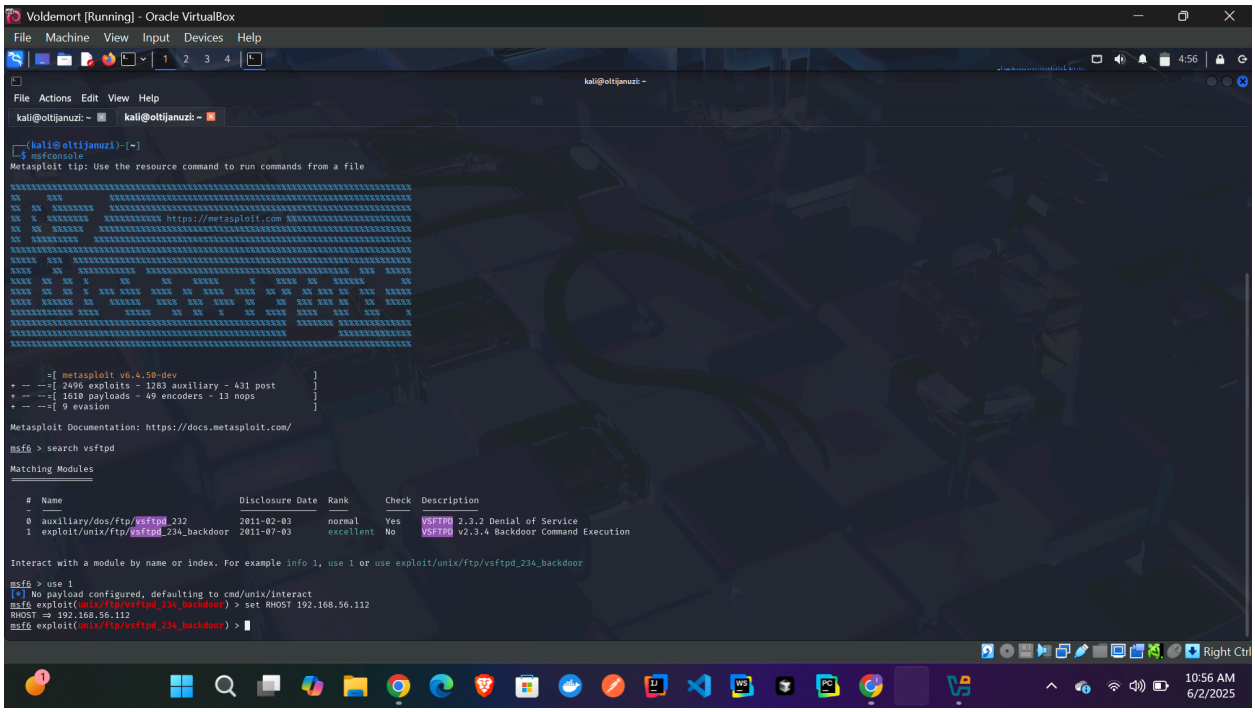
We search for VSFTPD versions



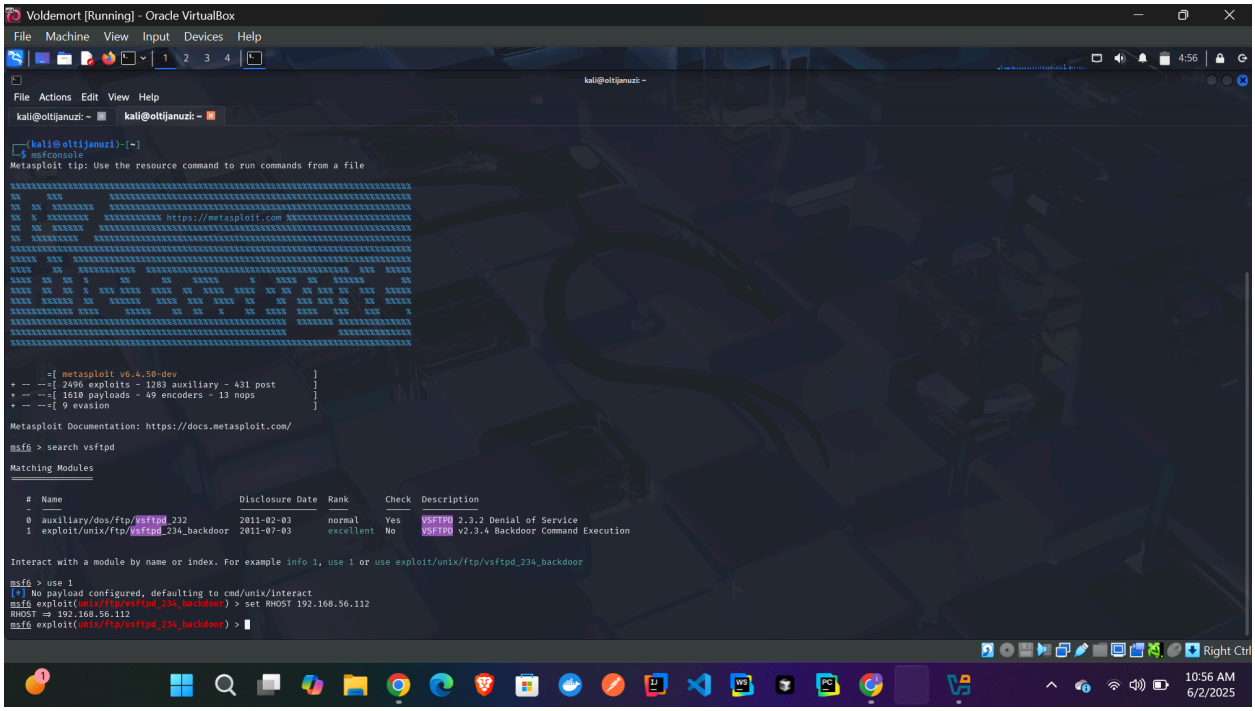
We choose the exploit



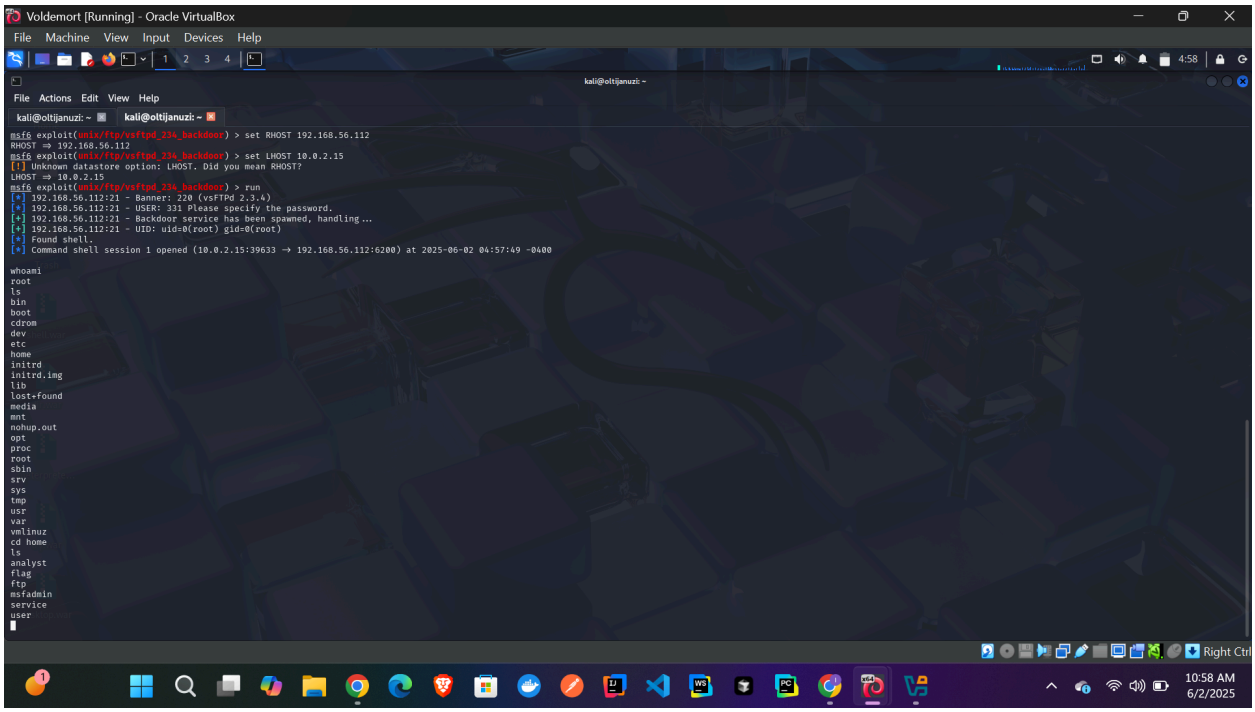
We set the Remote Host ip which is **192.168.56.112**



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

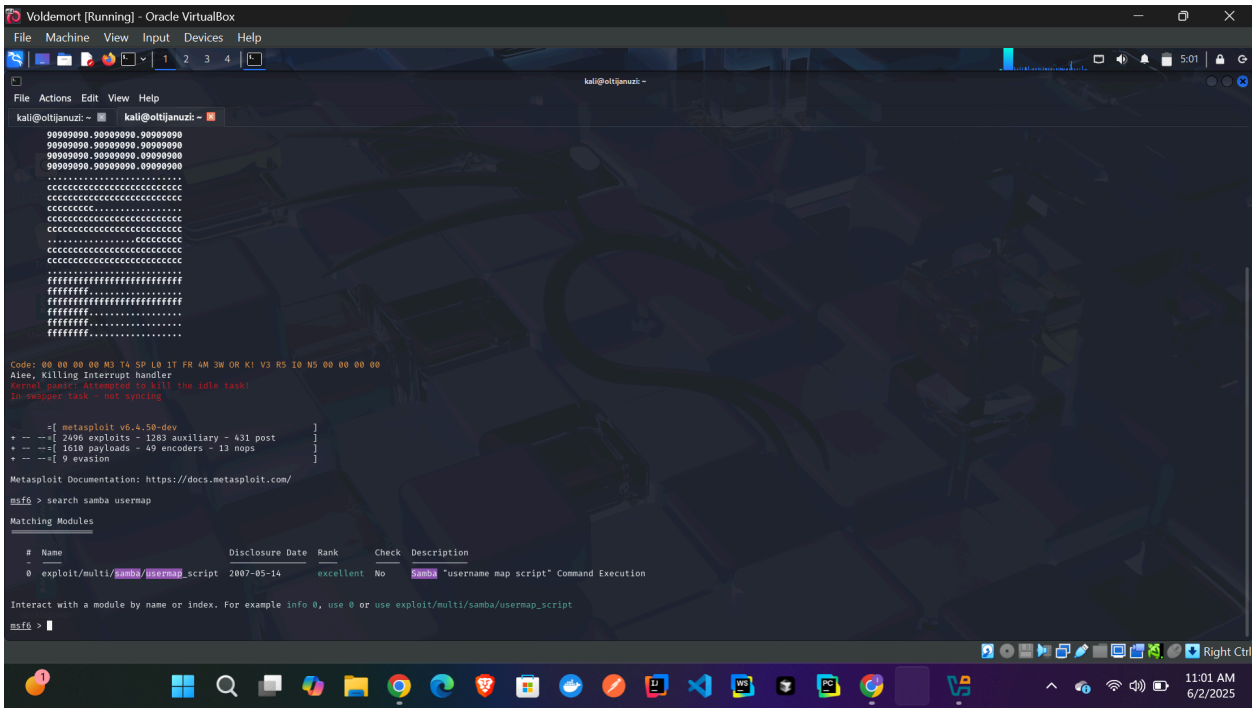


Here we gained access over the system from port 21

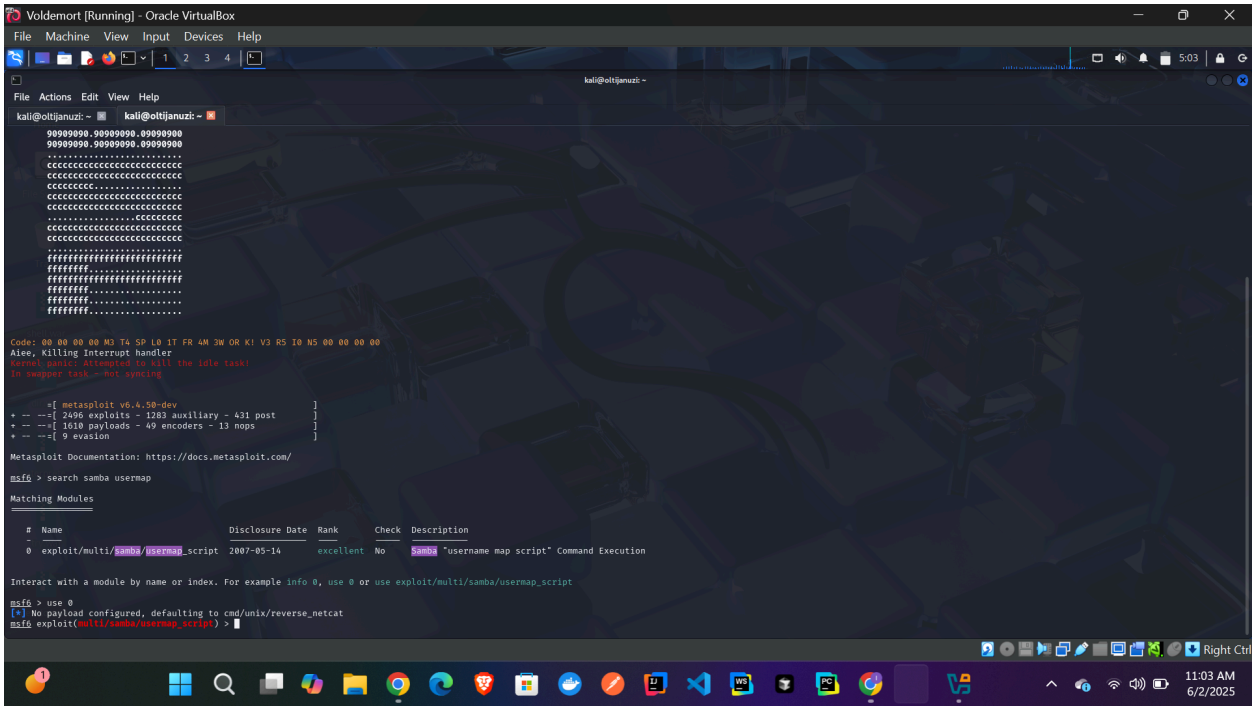


Exploiting Samba Usermap Script

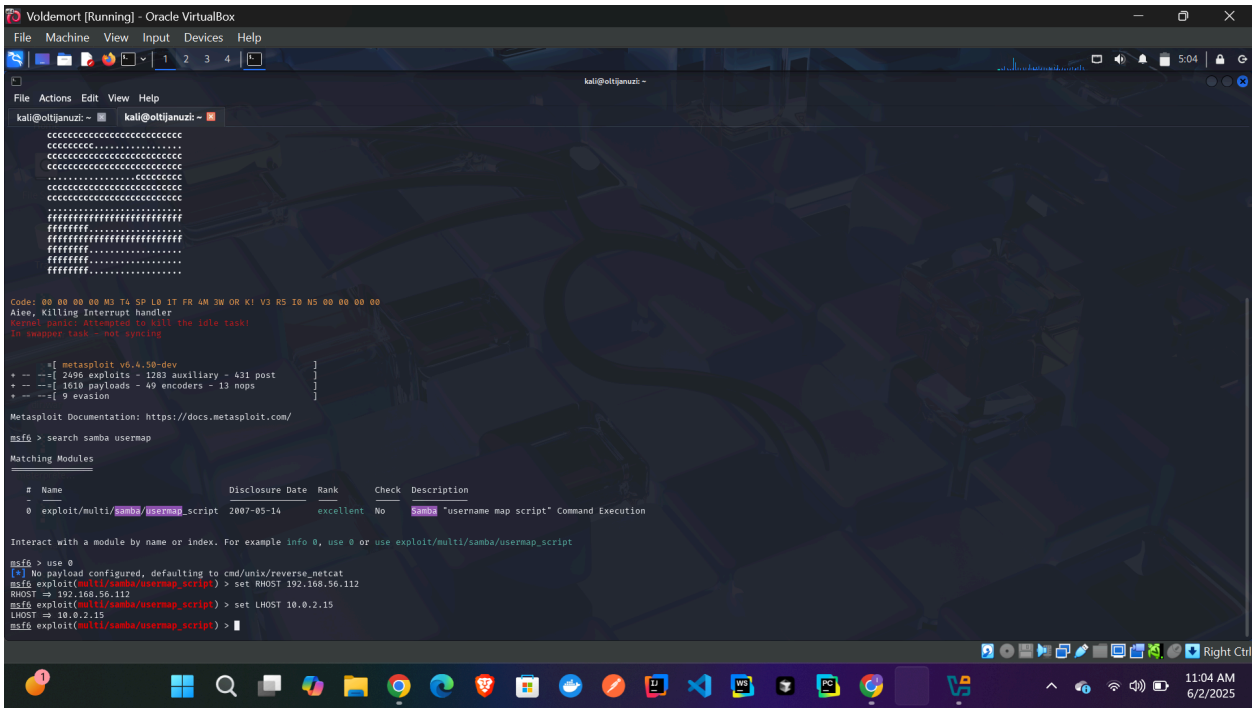
We search for the usermap script exploit



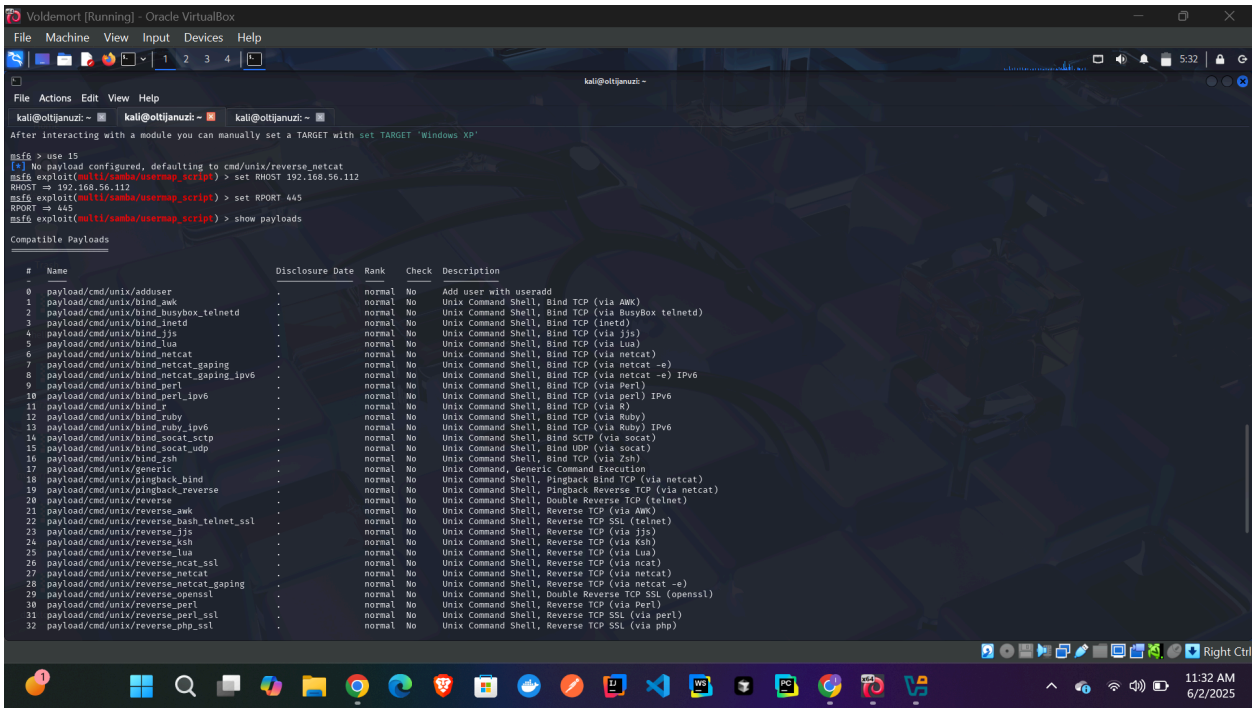
We choose an exploit



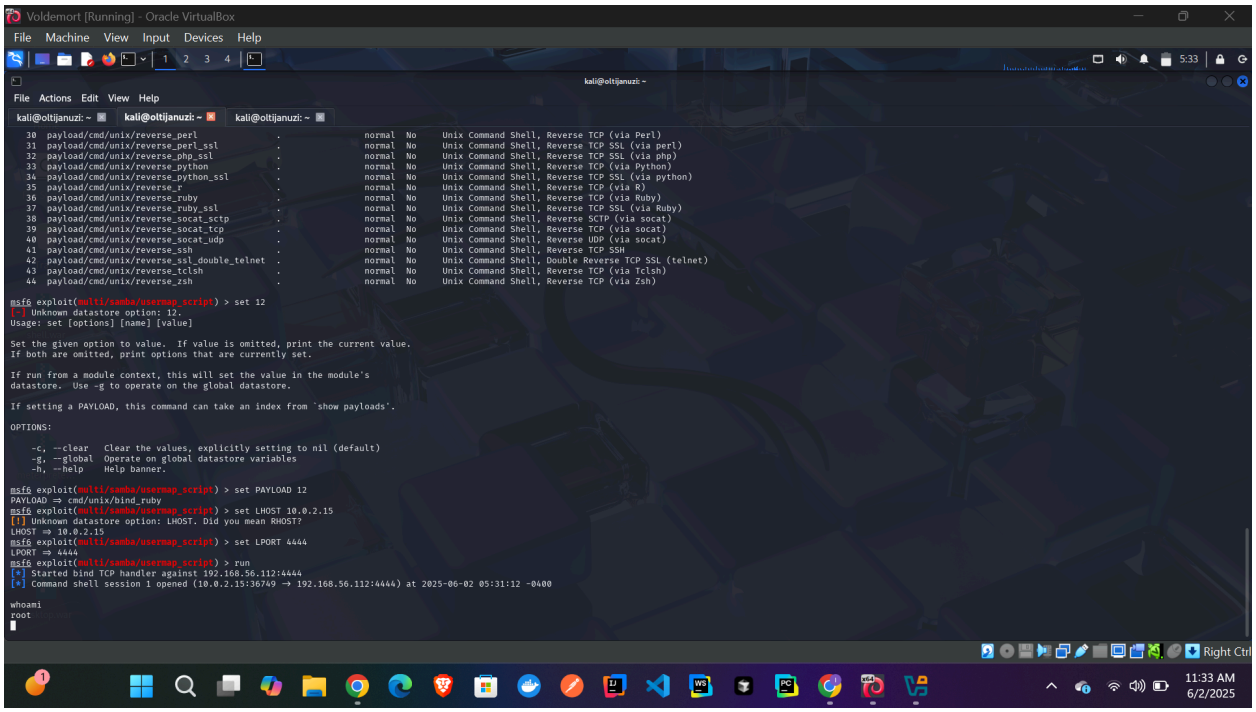
We set the RHOST and LHOST to make the exploit happen



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

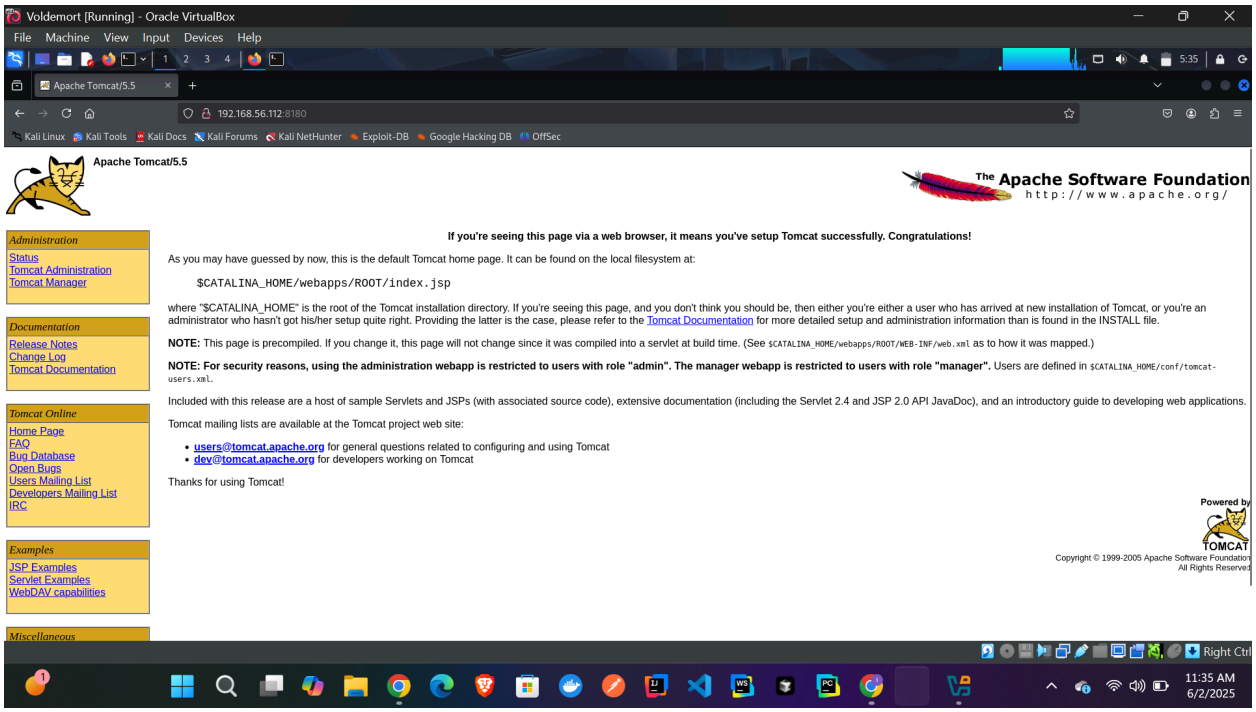


Setting the payload selected and gaining access from the 445 port

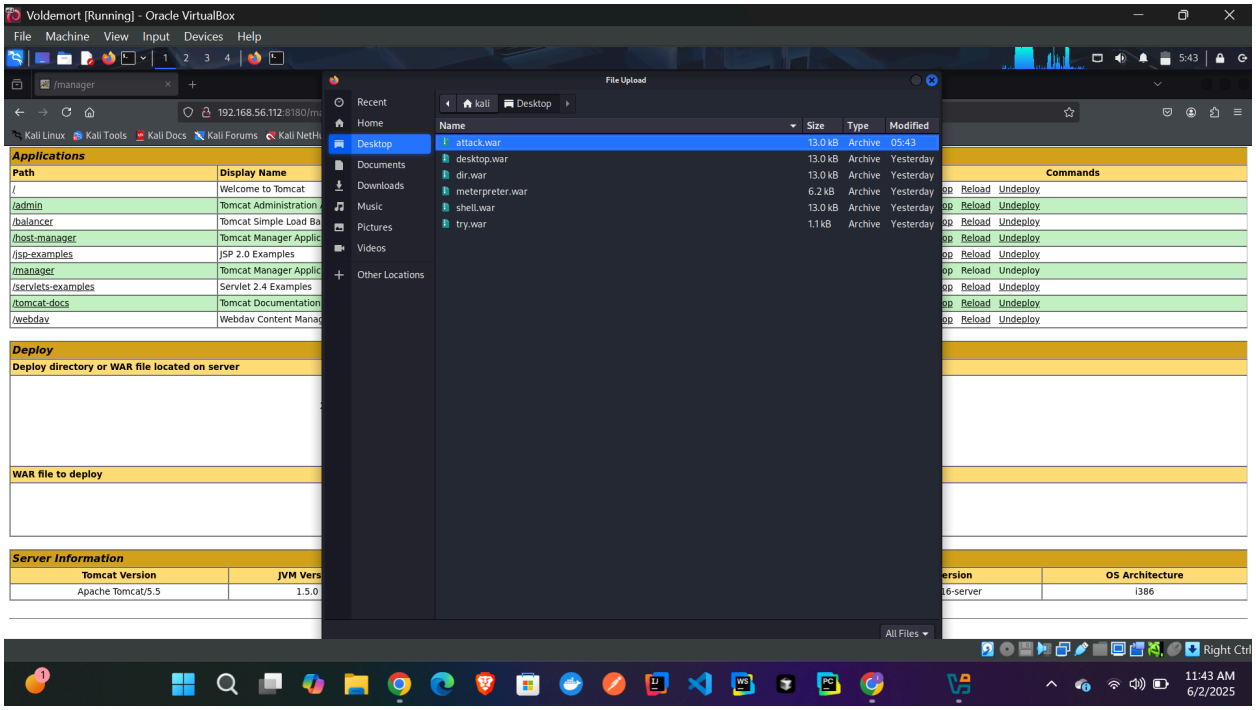


Exploiting Tomcat WAR Upload

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



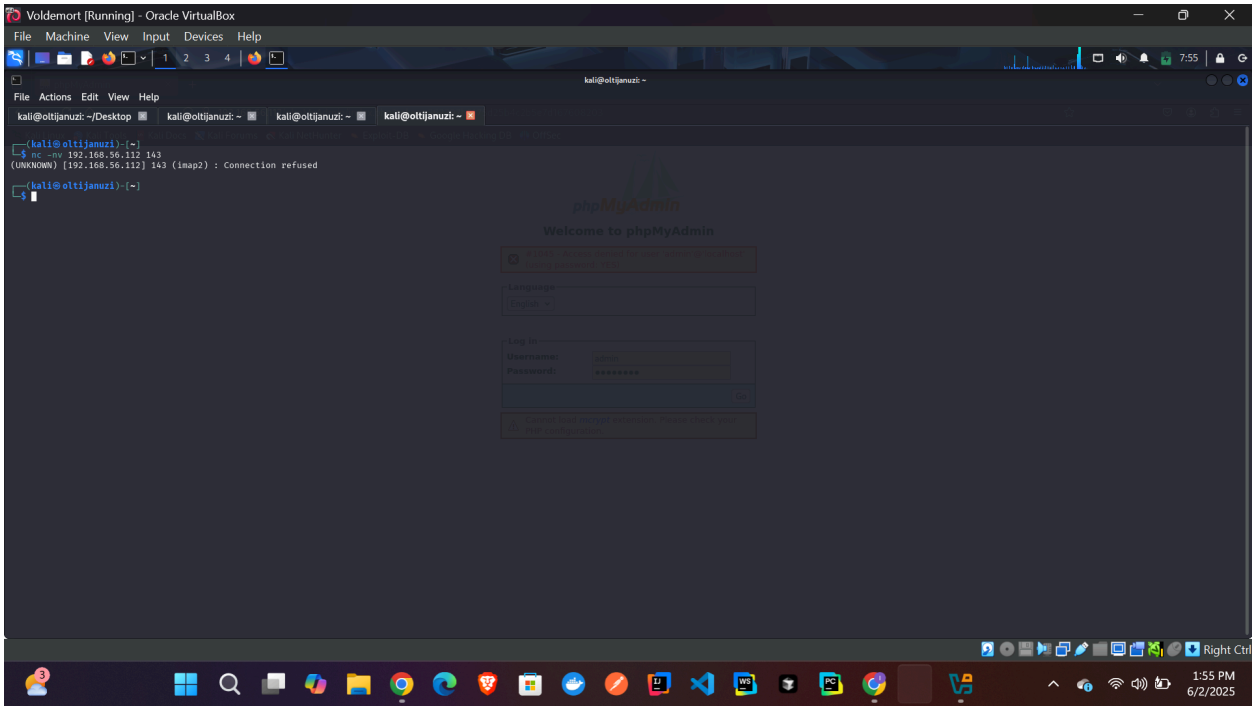
We upload the war which we created using MSFVENOM



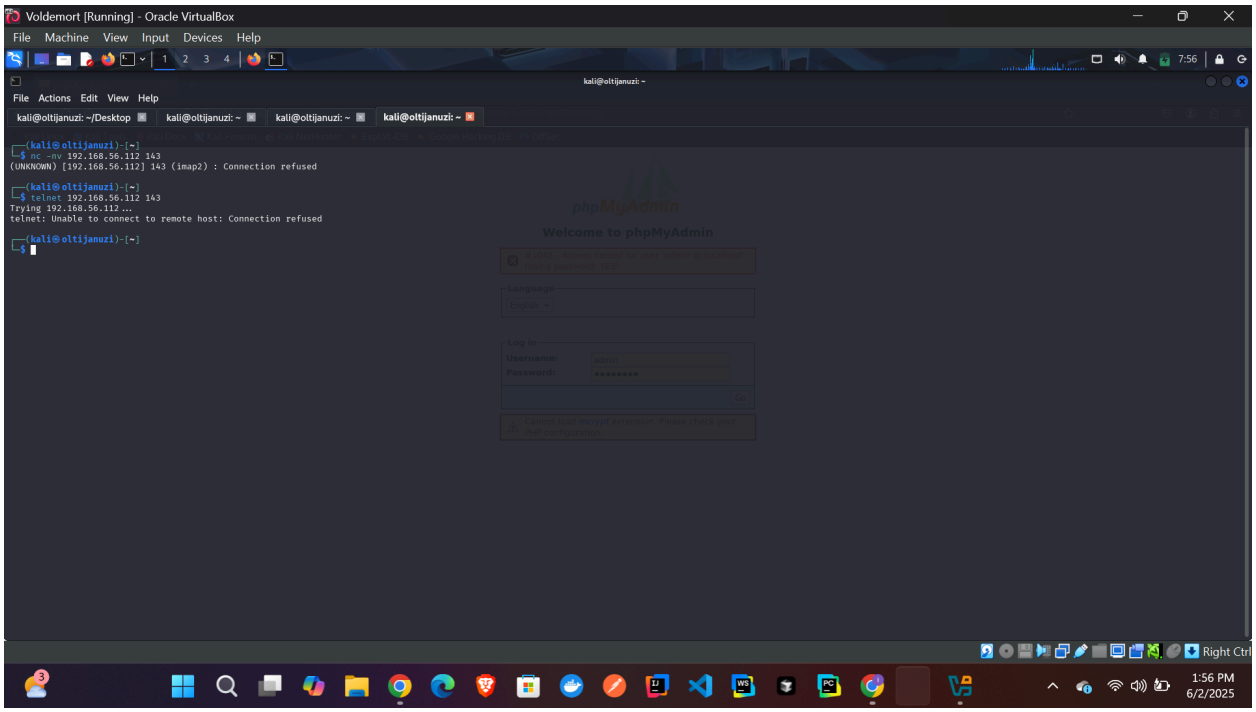
Couldn't trigger the attack.war file which we created with MSFVENOM

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.

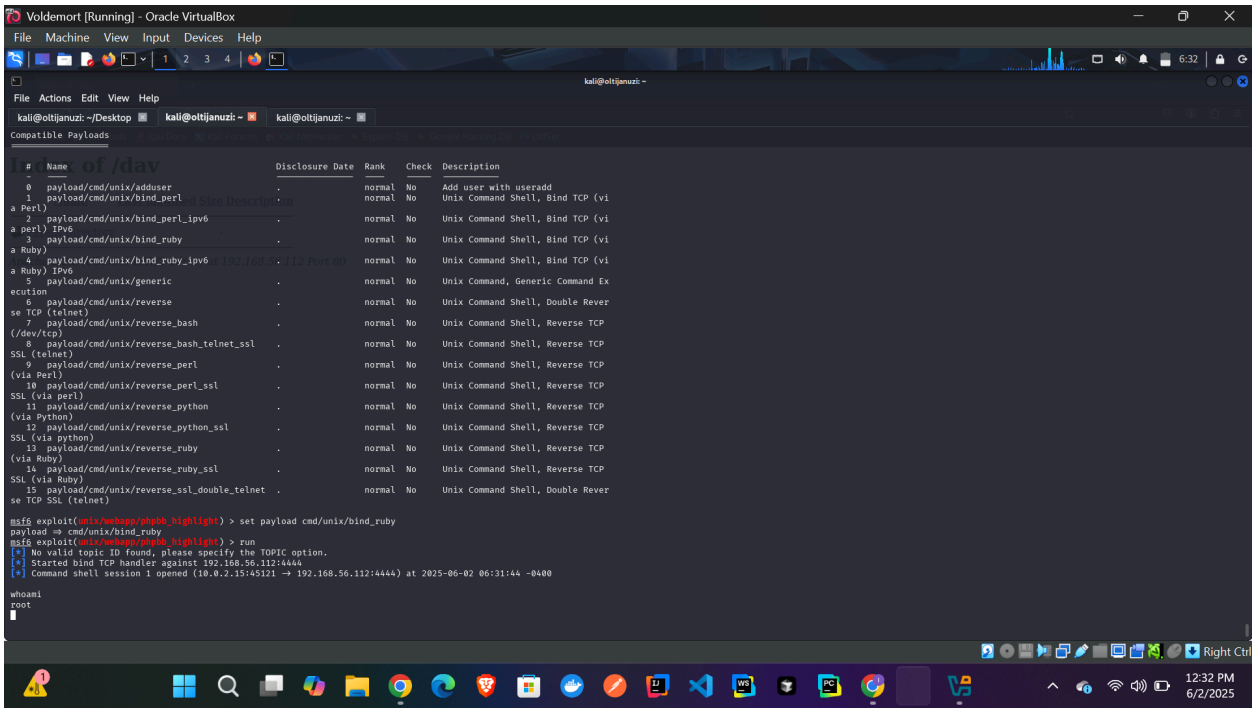


We also tried Telnet-ing into it but it didn't work



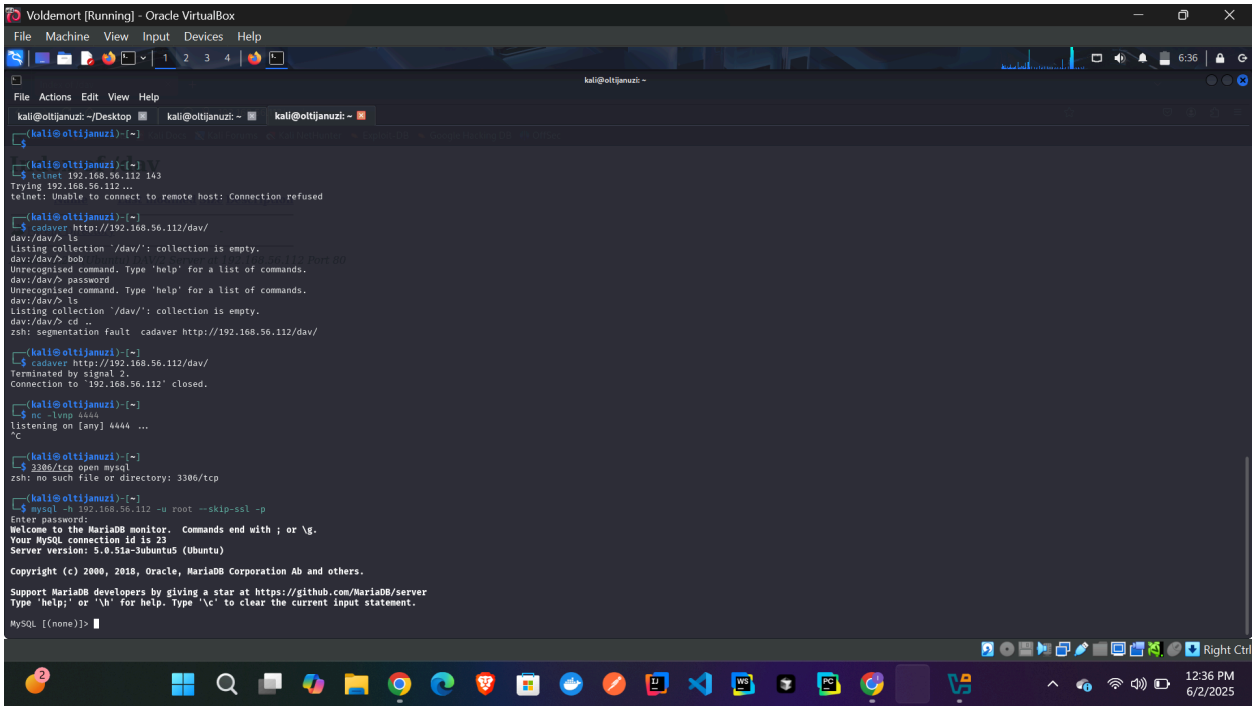
Exploiting WebDAV Upload

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



MySQL Default Credentials

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

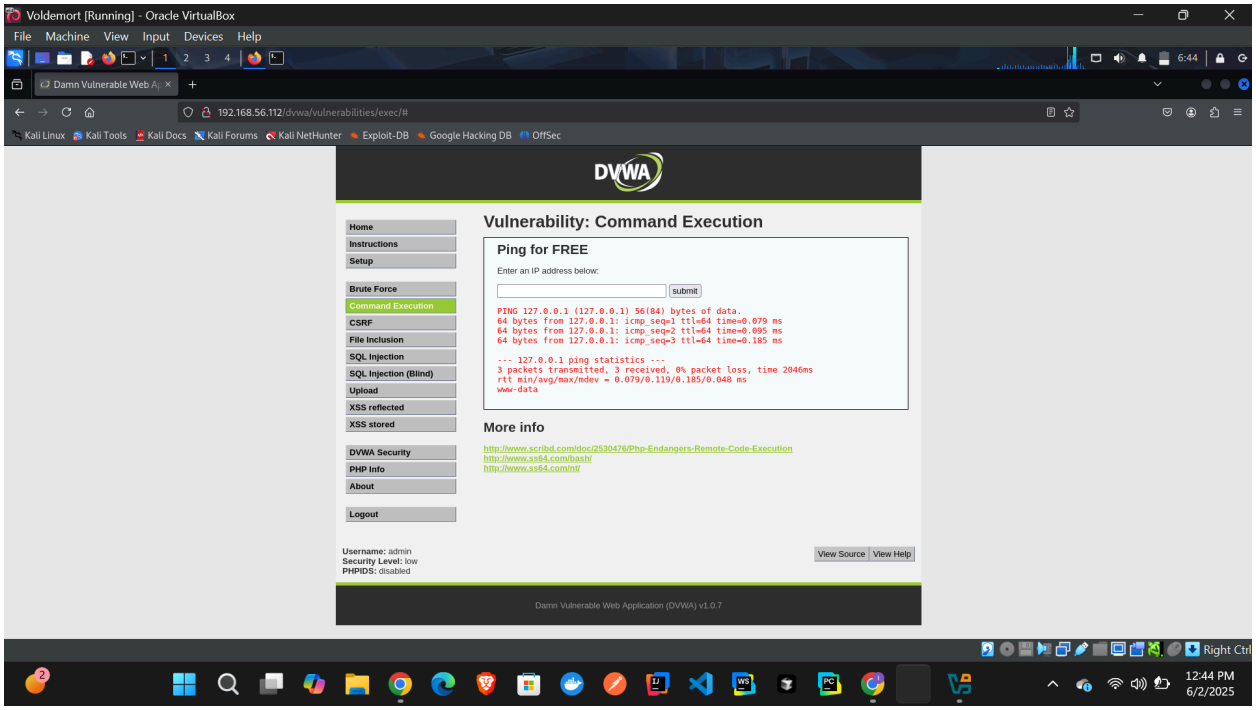


DVWA Command Injection

Here we injected a command inside an input field

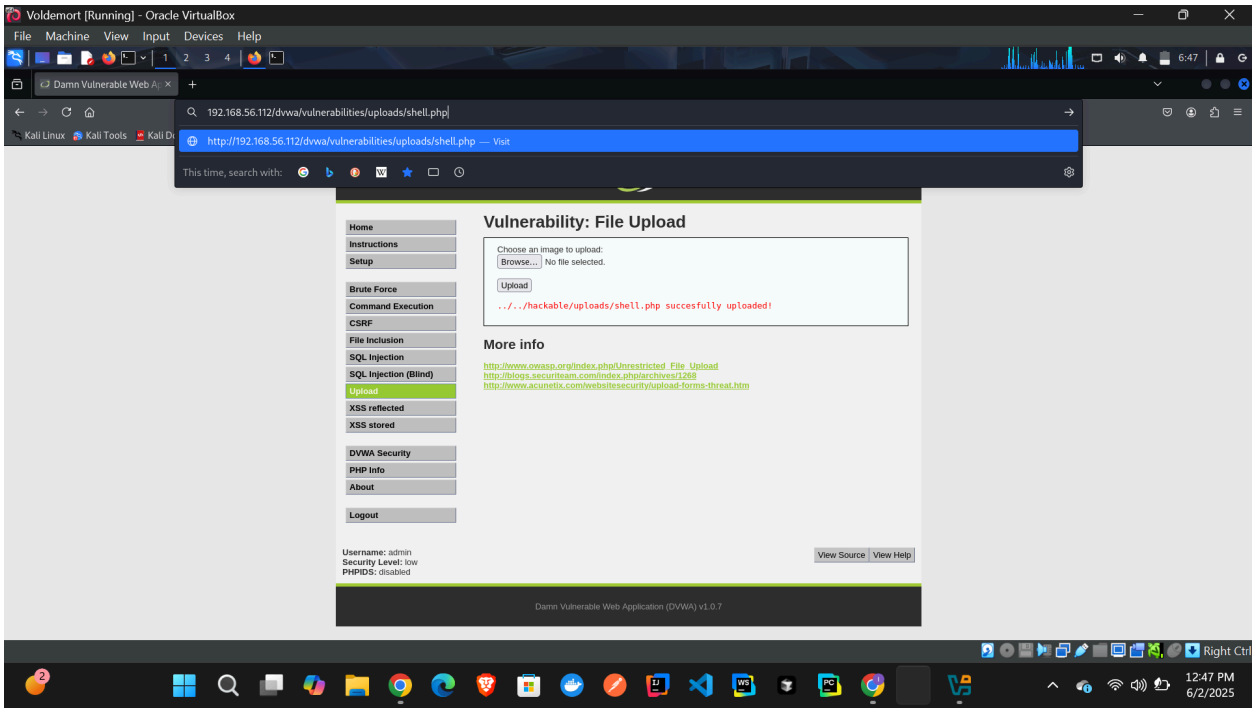
URL: `http://192.168.56.112/dvwa`

Injection: `127.0.0.1; whoami`

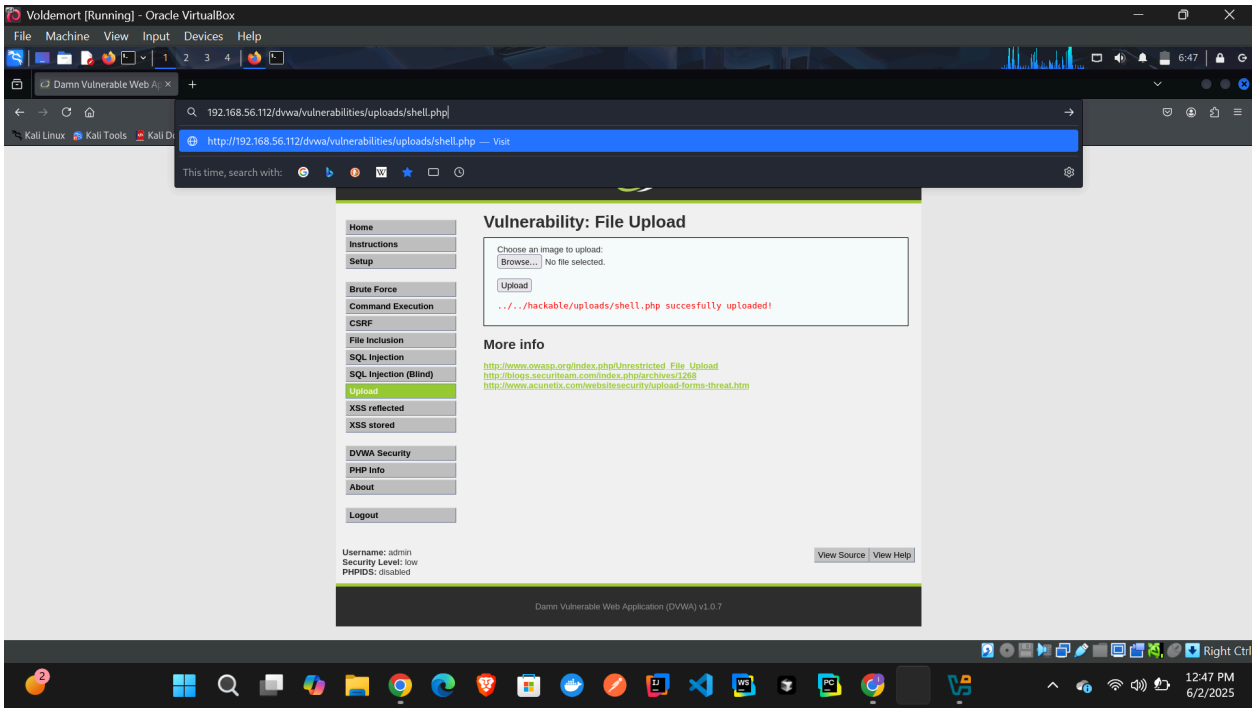


DVWA File Upload

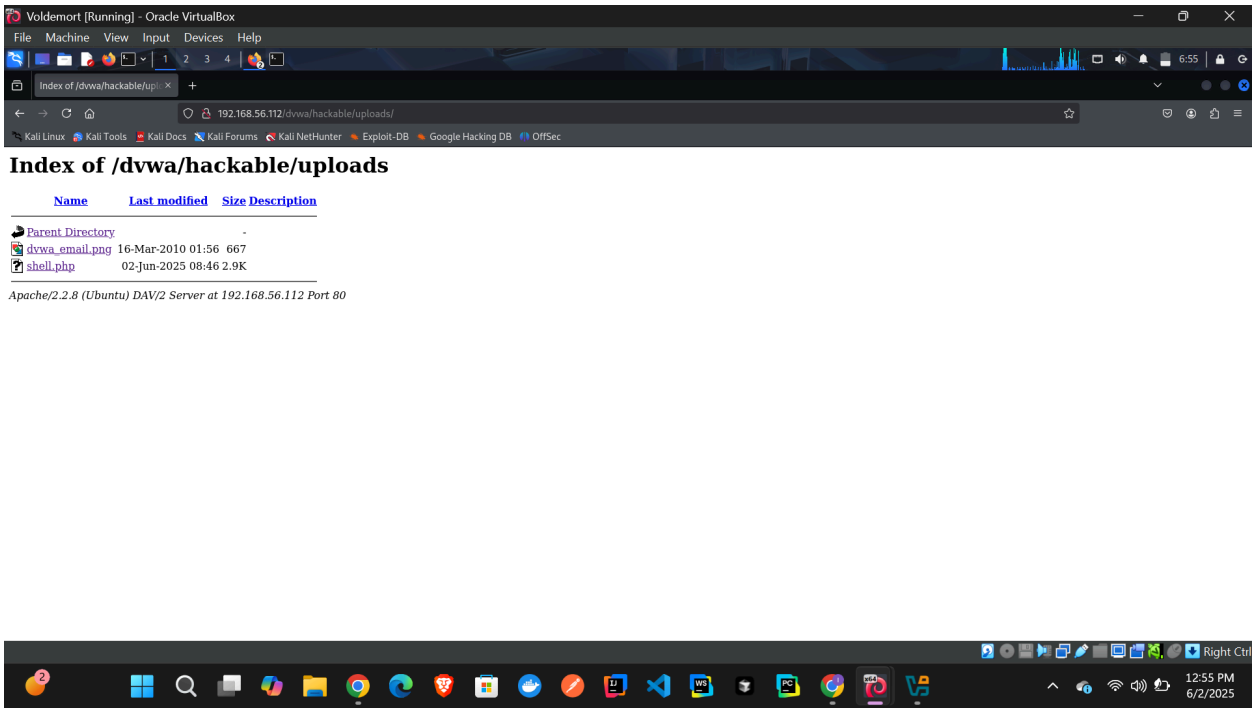
Here we uploaded a shell.php file created and triggered it



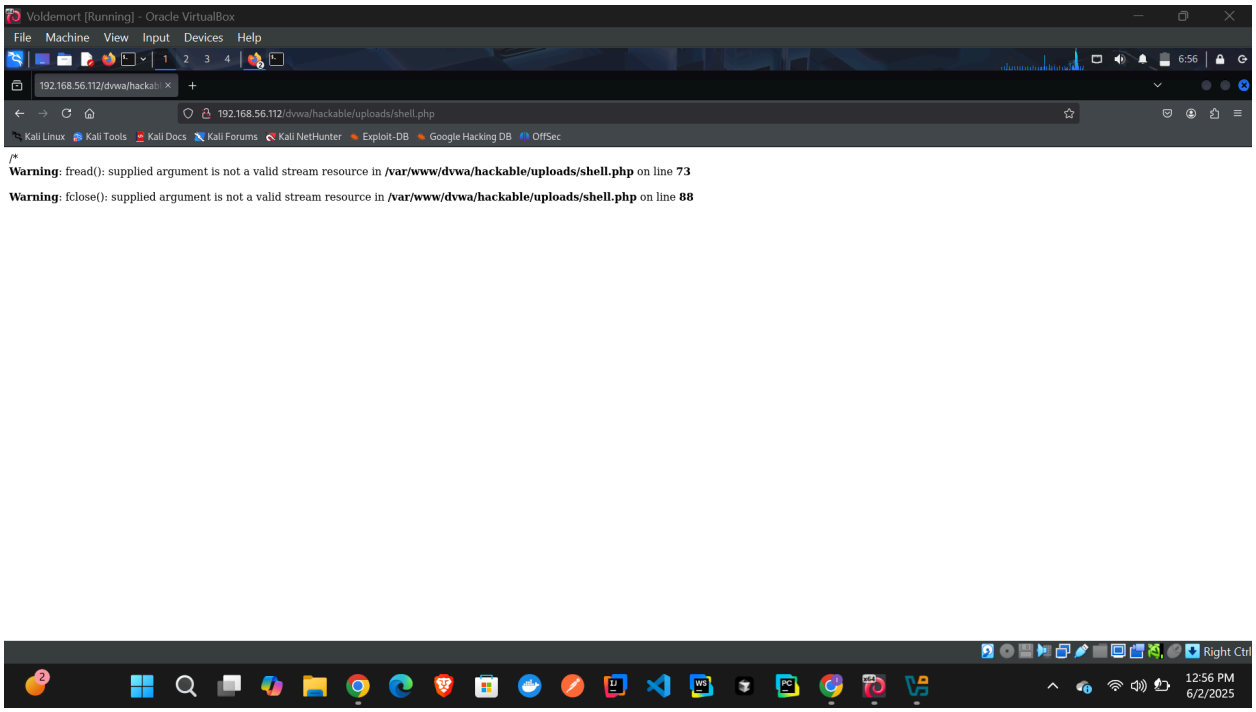
We can see what hides behind the web, close to dir traversal



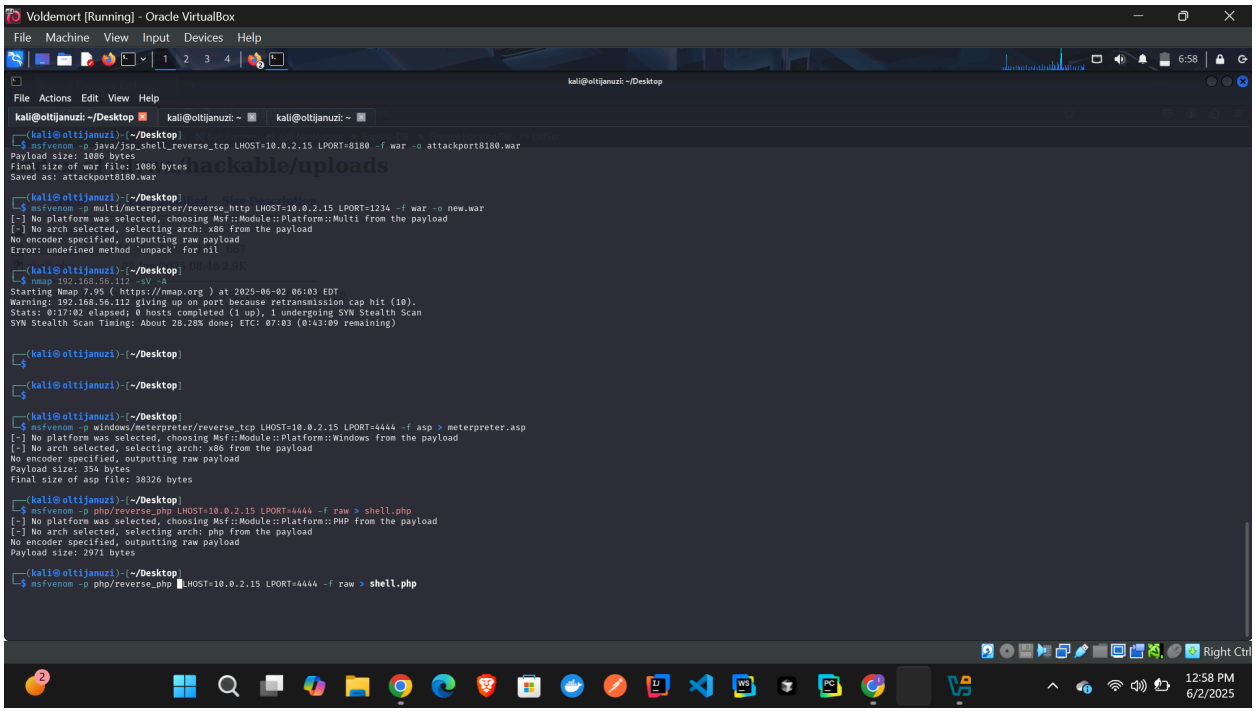
We can see the shell.php that we have uploaded



This is when we triggered it

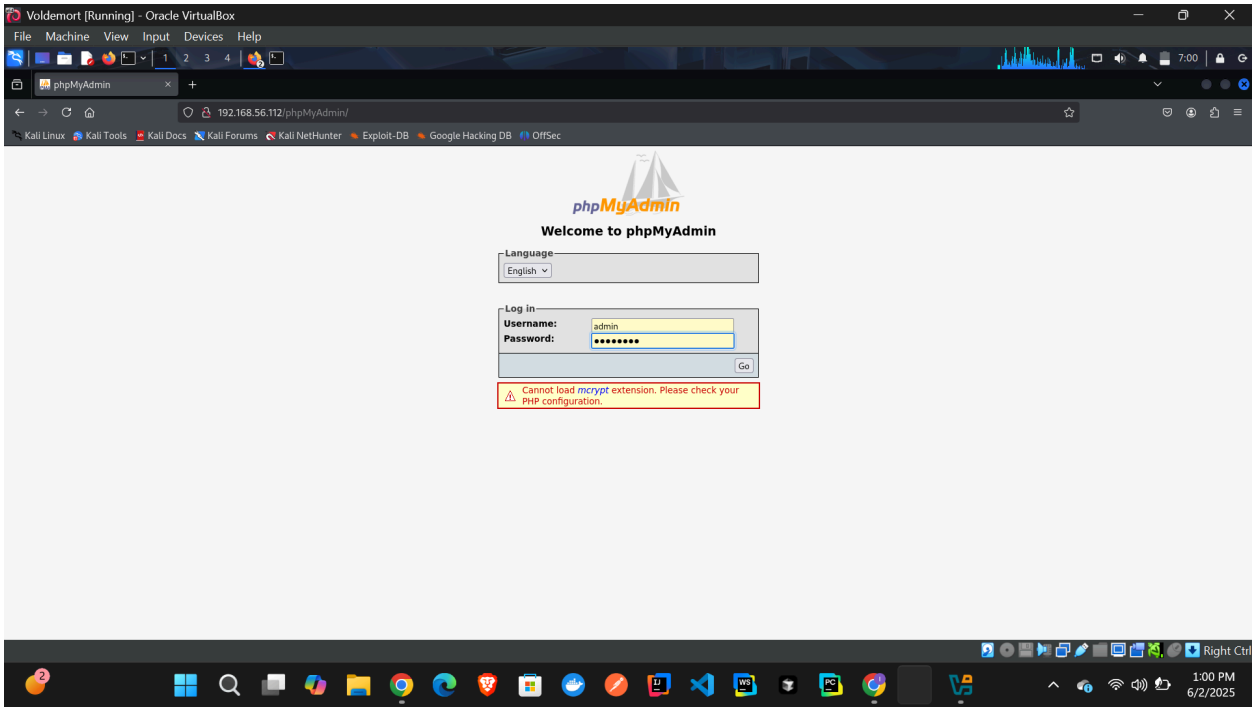


Here is the command used to create the shell.php file that got us access via upload

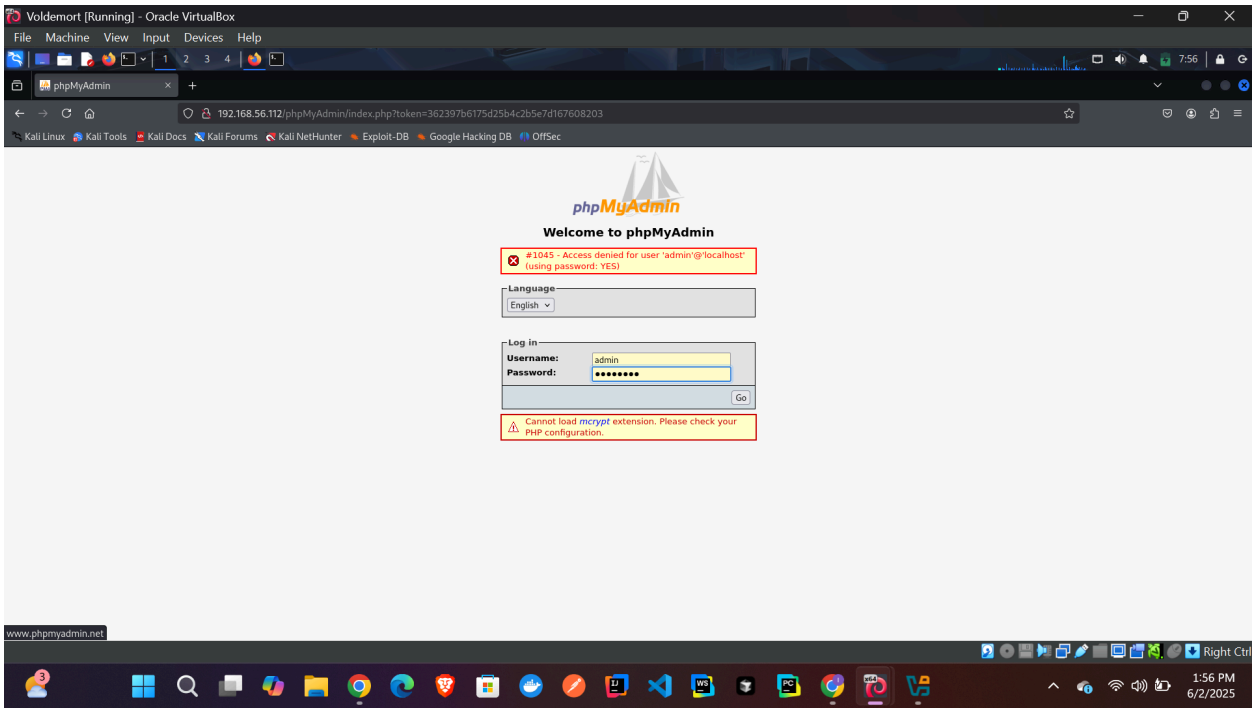


phpMyAdmin Login

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

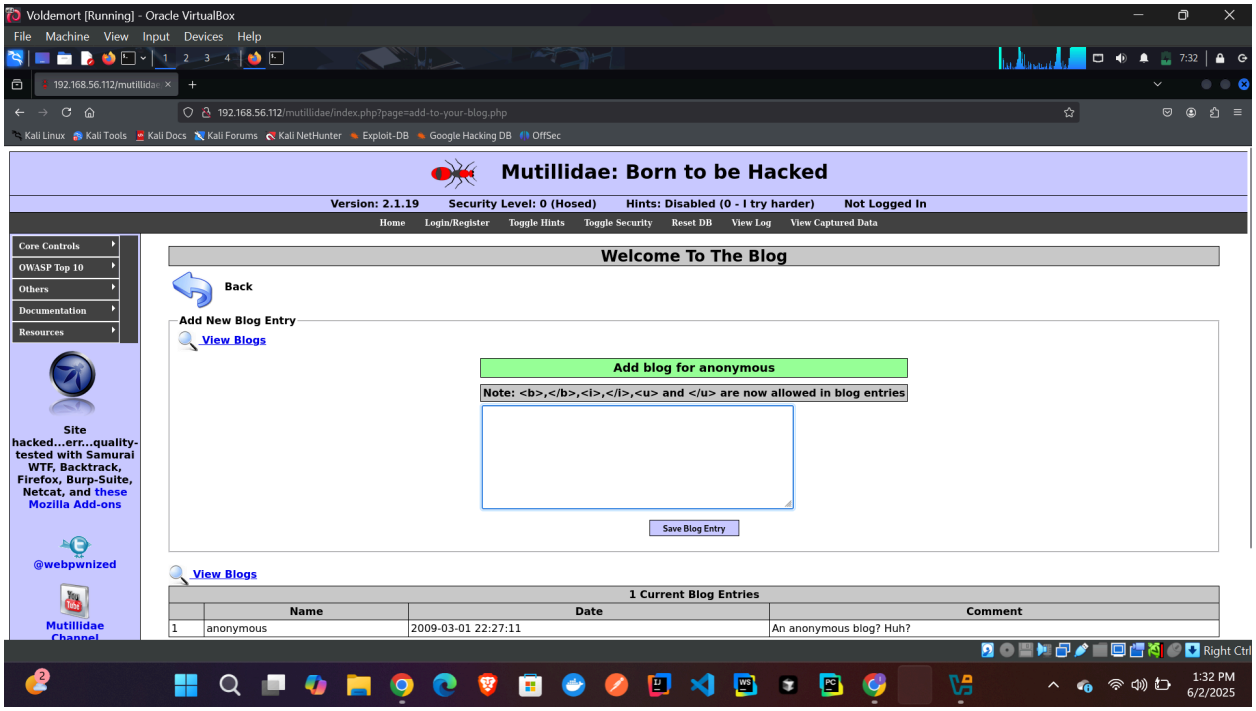


We tried all the default combinations and it didn't work

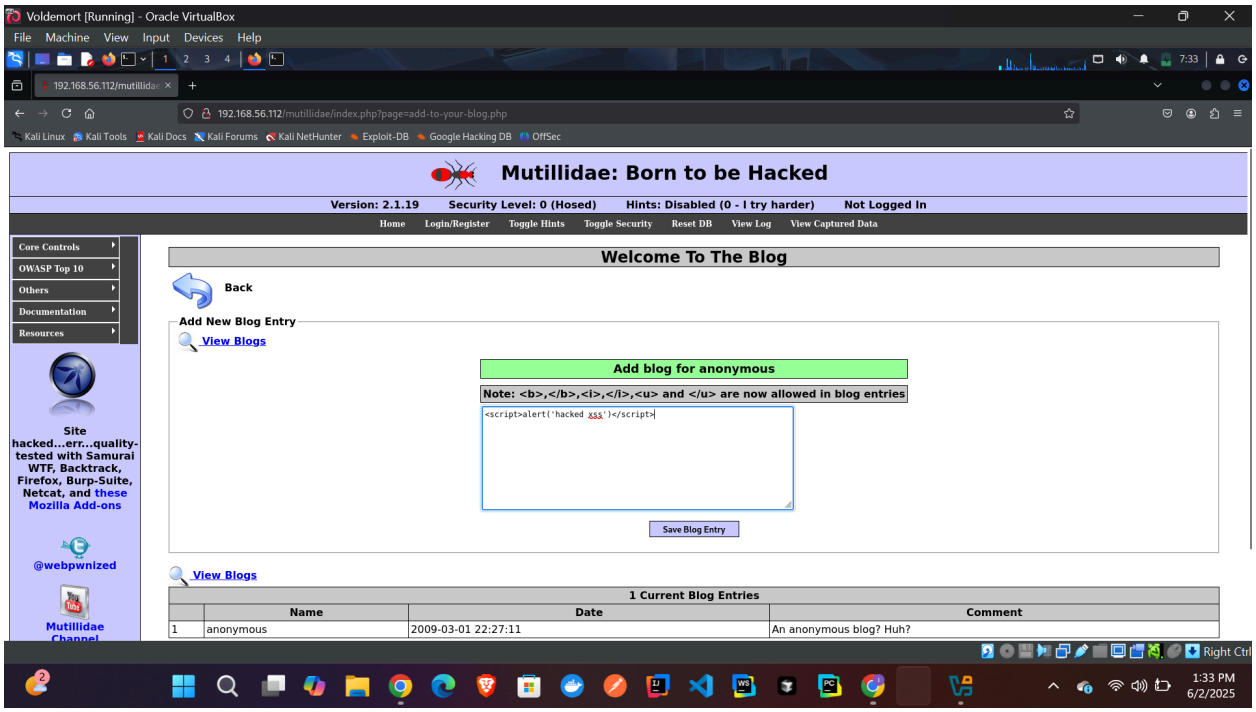


XSS in Mutillidae

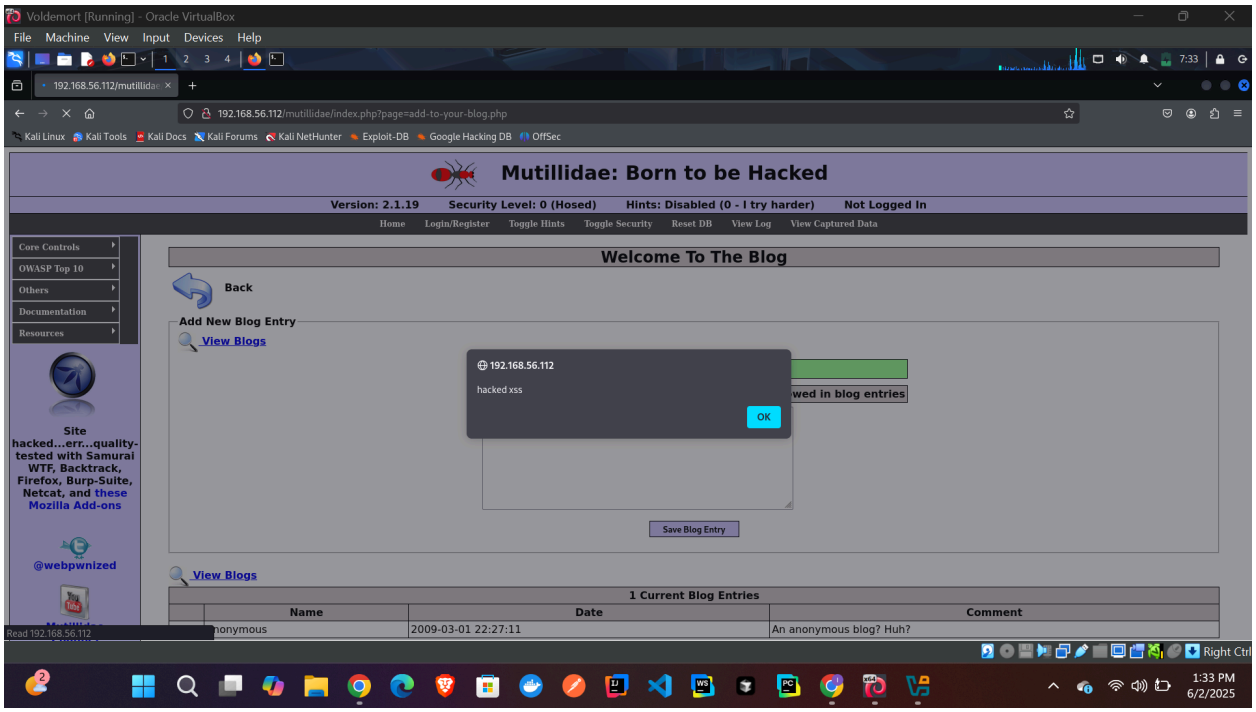
Here we found an unsanitized input field and managed to perform an XSS Injection attack



This is the script used



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