LAB 13 – Penetration Testing and Ethical Hacking

By :- Faraz Ahmed

Table of Contents

I. Report Outline

1. Executive Summary

We are penetration testing on a website and checking if we can gain root access to that website and to the same IP address. So, first we search the whole network linked to the device IP address using Nmap. Then we get external IP of 10.43.32.99 which is not our and has running http port 80 which we can export. So, using that information we enter the IP address and the port as URL of that website as “http://10.43.32.99:80”. After getting access to the website, we need admin access in order to upload malicious file (in this case php-reverse-shell file) in the website. So, we used SQL Injection script in order to gain admin access. We used “ ‘ OR ‘1 “ script to gain admin control and after getting that we uploaded the malicious file into the website for it to store there. After all of this finally we will run “Girbuster” on terminal and make a full scan of that website to find that reverse shell file. Once Girbuster gain access to that file, we can use “nc nvlp 80” to listen to all port of 80 to confirm our connection with the port 80 and to that website. Once there we will run the search directory inside it using “find / -perm -o=r -type f2” which will load a lot of files and we will find coolbash in these files. A "coolbash" file is essentially a Bash script file that contains a collection of particularly useful or "cool" shell commands designed to perform some advanced things which we can’t perform normally. After that we will enter “whoami” to check if we gained root access. So as a pen-testing our final aim was to gain root access so that we can do a lot of things with that high privilege.

2. Scope

So, the penetration test took place on 4th December 2024 at 3:30 pm on Virtual Machine named "Kali" in vSphere. The IP address of Kali device is "192.168.13.165" and when we will use Nmap in the servernet, we will find an external IP which is not ours which is "10.43.32.99". That's the IP address on which we will execute or try our penetration testing. When we run Nmap using "sudo nmap -p- 10.43.32.99" where -p- to run nmap to all host under that ip address. We can observe "http with port number 80" (as shown in Figure 7) open and running so we know by this that we can attack the website using ip address as URL of the website for penetration testing.

3. Methodology

So for detection any external devices connection to the device's ip address,we will run Nmap in the servernet. There we can see an external IP address which is not ours is the one which is "10.43.32.99" so we know we will perform penetration testing on that. Them we will excute command nmap using "sudo nmap -p- 10.43.32.99" where -p- to run nmap to all host under that ip address to find out what services is up and running under that external IP address. As we can observe from the figure that "http is open with port 80" so we can attack that http website with URL "10.43.32.99:80" and try penetration testing on that.

3.1 Tools Used

All of the tools used for this penetration testing are :-

- Nmap
- Dirbuster
- SQL injections

4. Findings

4.1 SQL injection on the website (Likelihood: high, Impact: High)

- So, SQL Injection is basically inserting the malicious script into the database of that website because of which an attack can access any random sensitive data stored in that database. So we used a random SQL script which is " ' OR '1 " in username and we can type anything in password as shown in figure 1.

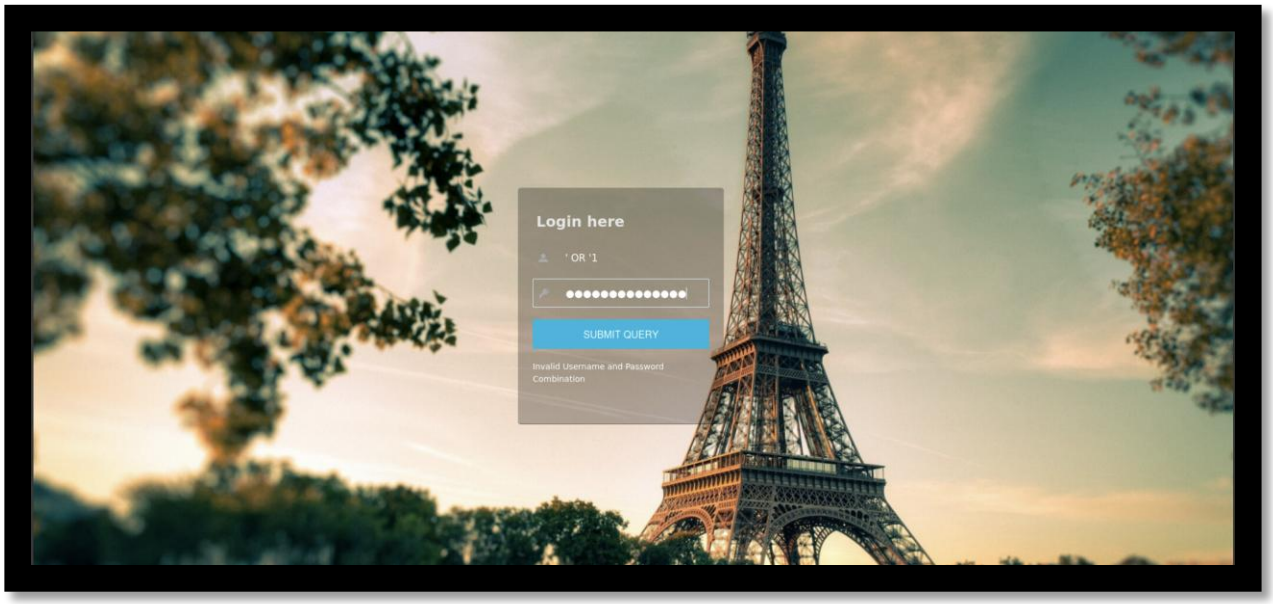

Figure 1: Screenshot of SQL Injection in Website.

- Then due to SQL Injection, we can get admin access so because of that we can upload any malicious file into the websites as shown in figure 2.

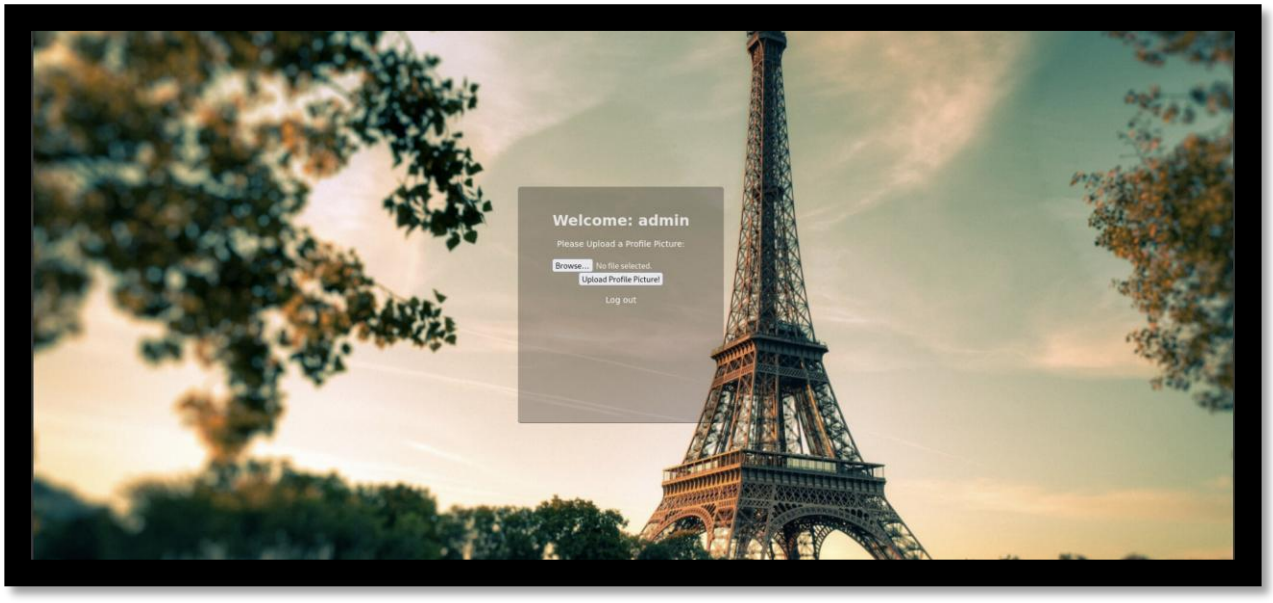

Figure 2: Screenshot of Upload file of "php-reverse-shell" on the website.

4.2 Uploading Reverse Shell PHP file on the website (Likelihood: Low, Impact: Low)

- Then we can upload malicious file like “php-reverse-shell.php” which we did as shown in figure 3.

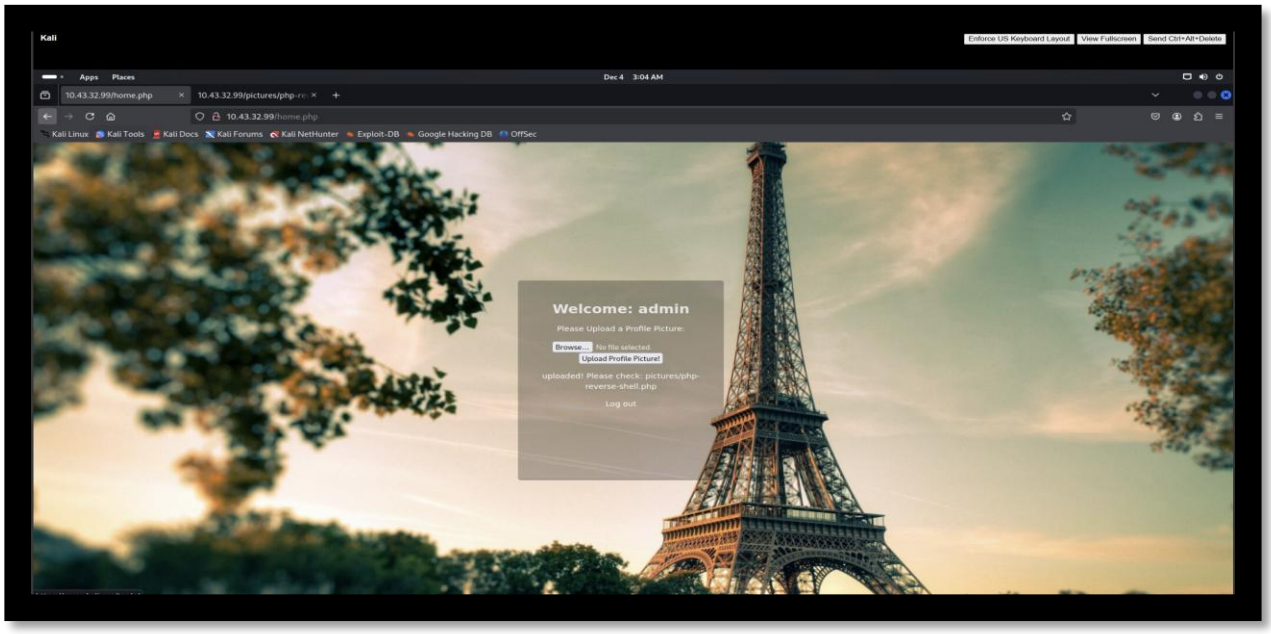

Figure 3: Screenshot of Upload malicious File on the website.

4.3 Running Dirbuster (Likelihood: Low, Impact: High)

- Then we will open terminal and enter “dirbuster” which will open OWASP Dirbuster window (as shown in figure 4) and then wait for the scan to complete.

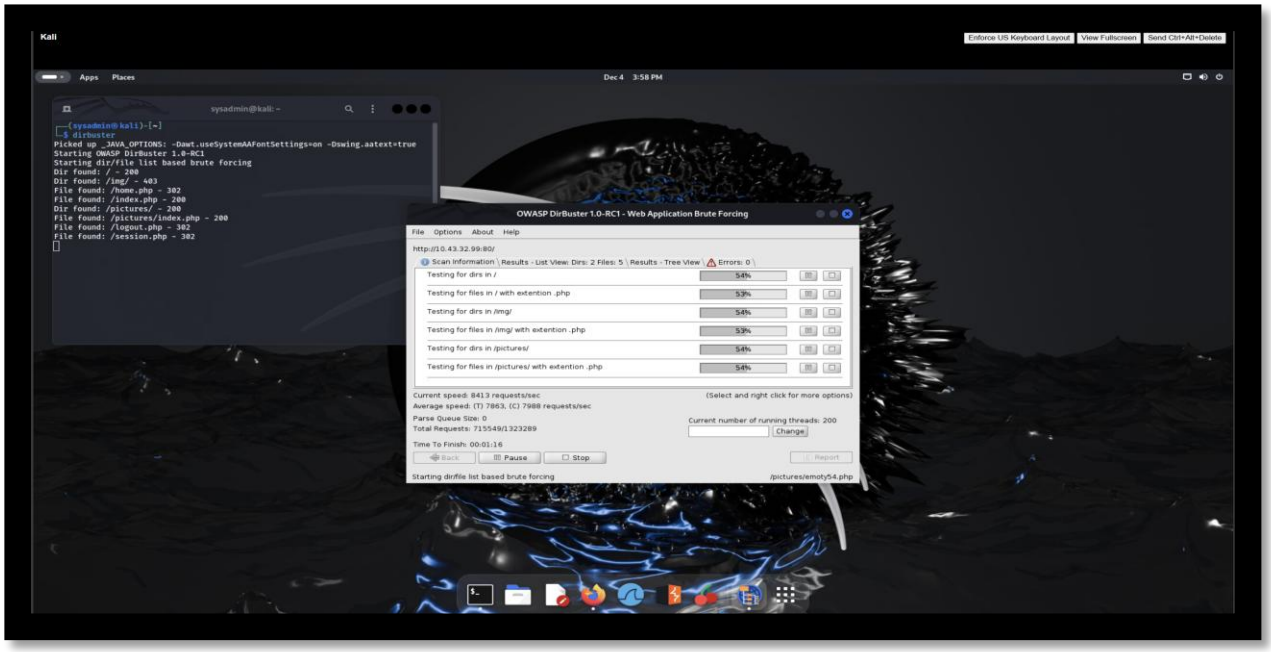

Figure 4: Screenshot of Running of Girbuster.

4.4 Linux- SUID Binaries (Likelihood: Low, Impact: High)

- Then enter “nc nlvp 80” which is let it listen all of the 80 ports available and then after we can confirm that we are connected to the website as root.

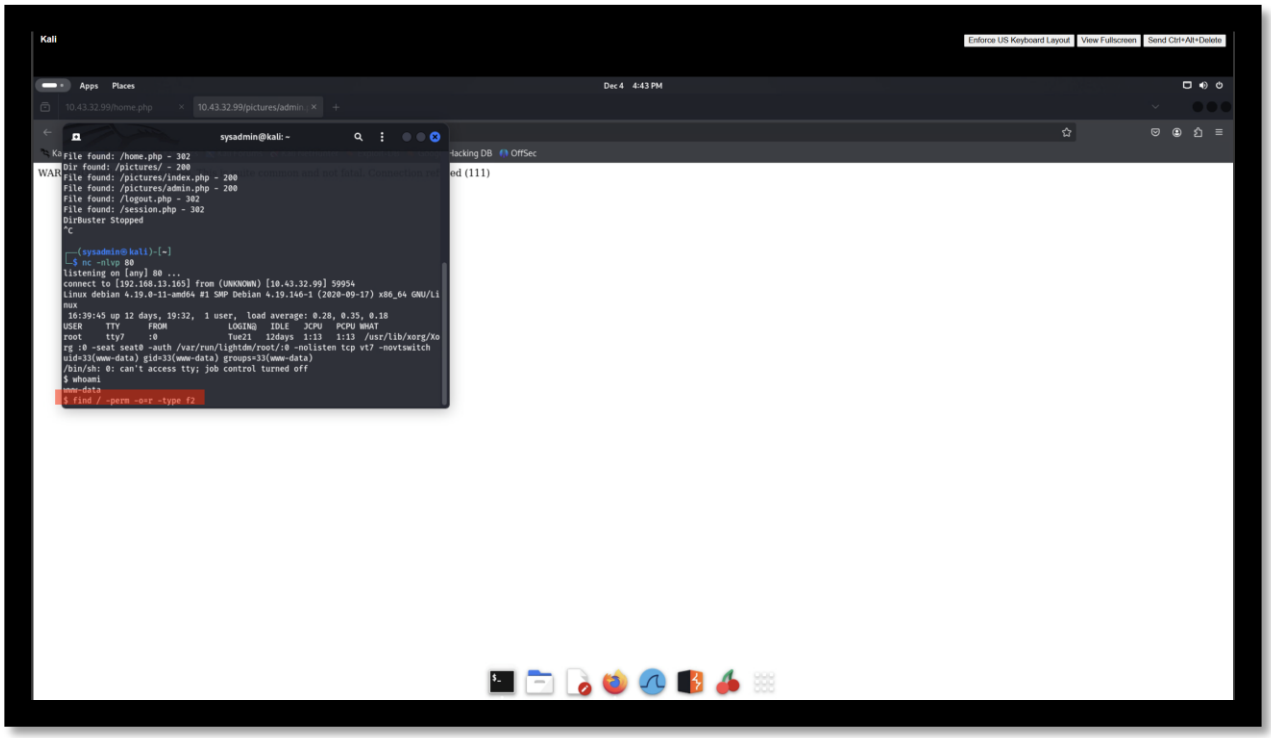

Figure 5: Screenshot of “nc -nlvp 80” to listen to port 80.

- Then we will run the directory search by using “find / -perm -o=r -type f2” as highlighted in figure 5 to find coolbash file location. After finding it, we will type its location (coolbash) then enter whoami to see if we got root access or not.

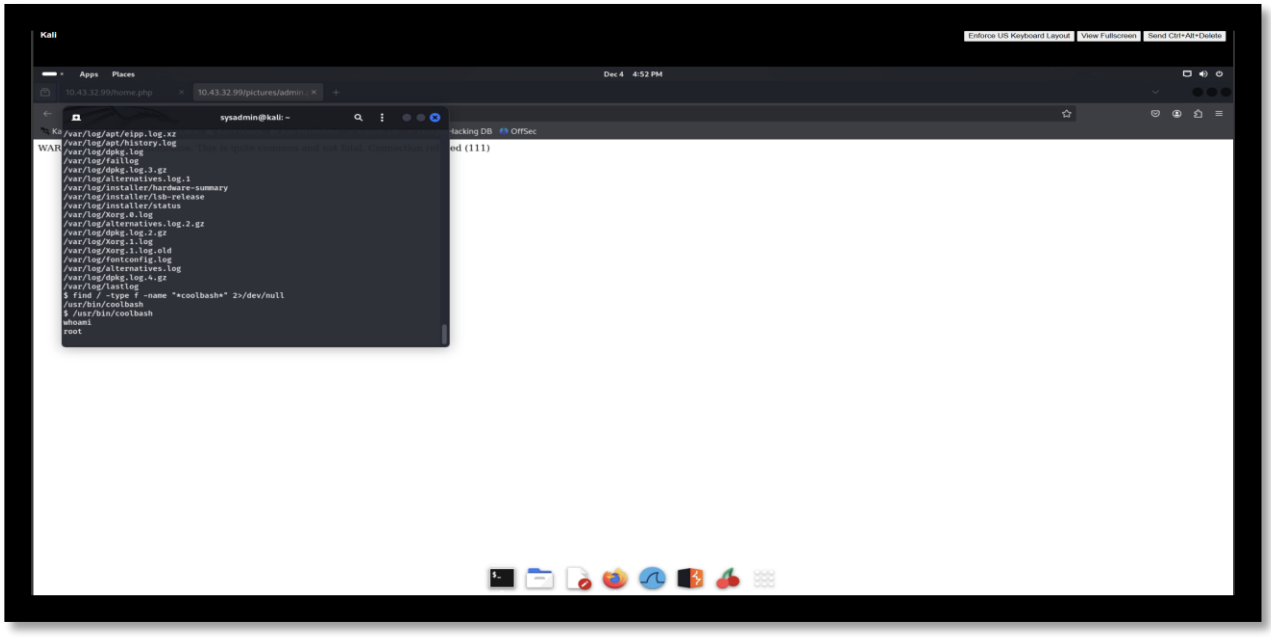

Figure 6: Screenshot of location of “coolbash” and gain of root access.

5. Works Cited

1. 50 cool Bash scripts! and what they do … | by William Maina | **AI monks.io** | Medium
2. Checklist - Linux Privilege Escalation | HackTricks

6. Appendix A

Figure 7: Screenshot of scan of all Ip address in that range using "sudo nmap -p- 10.43.32.99".