**Phase 6**

**The Capstone Project**

**Executive Summary**

The Objective of this phase is to conduct full scale penetration testing on the HTB machine LAME to evaluate systems security posture and identify vulnerabilities. We followed Penetration Testing execution standard (PTES). We covered reconnaissance, enumeration, exploitation, post exploitation.

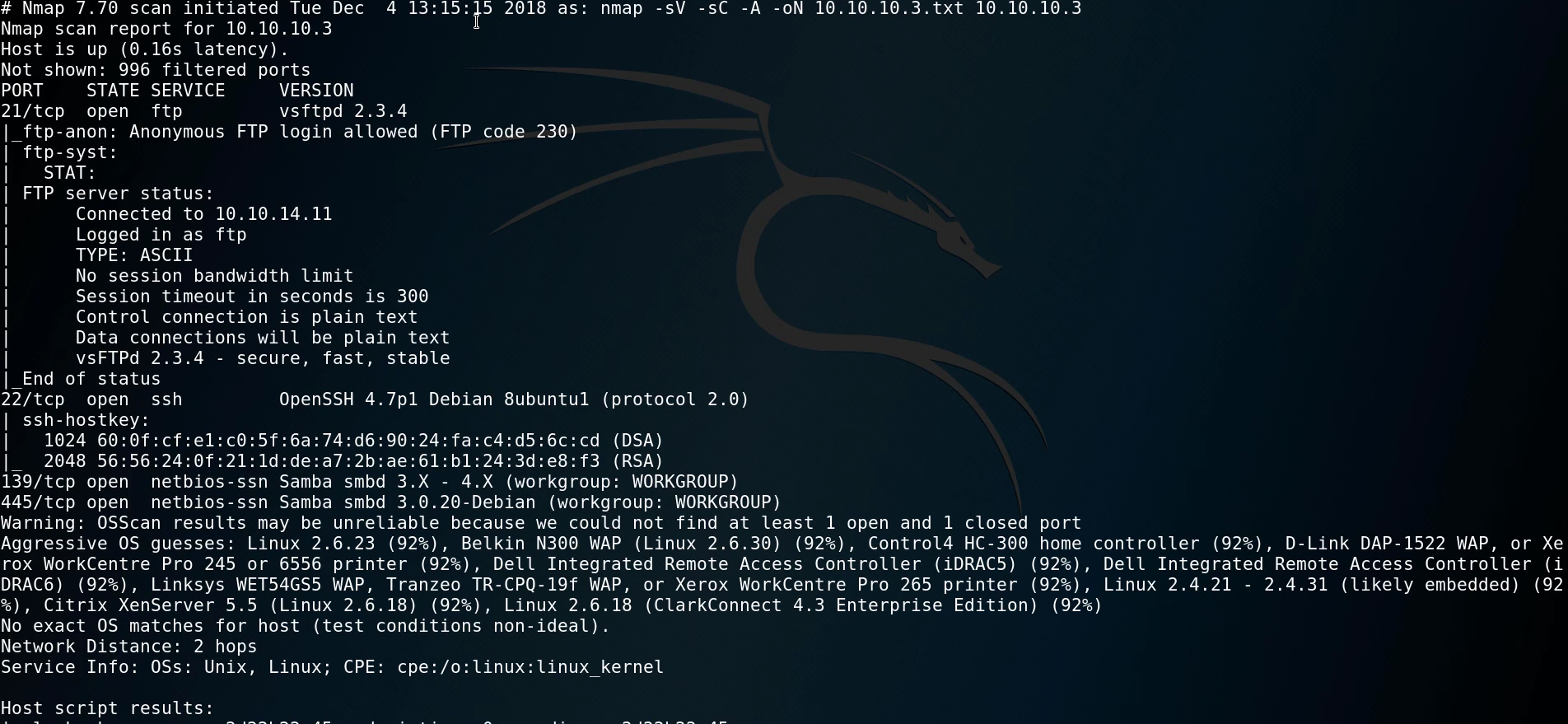
**Tools & Environment**

1. Kali Linux Environment
2. HTB Lame machine
3. Metasploit
4. Nmap
5. Searchsploit

**Methodology**

1. **Nmap Scanning of the Lame Machine**

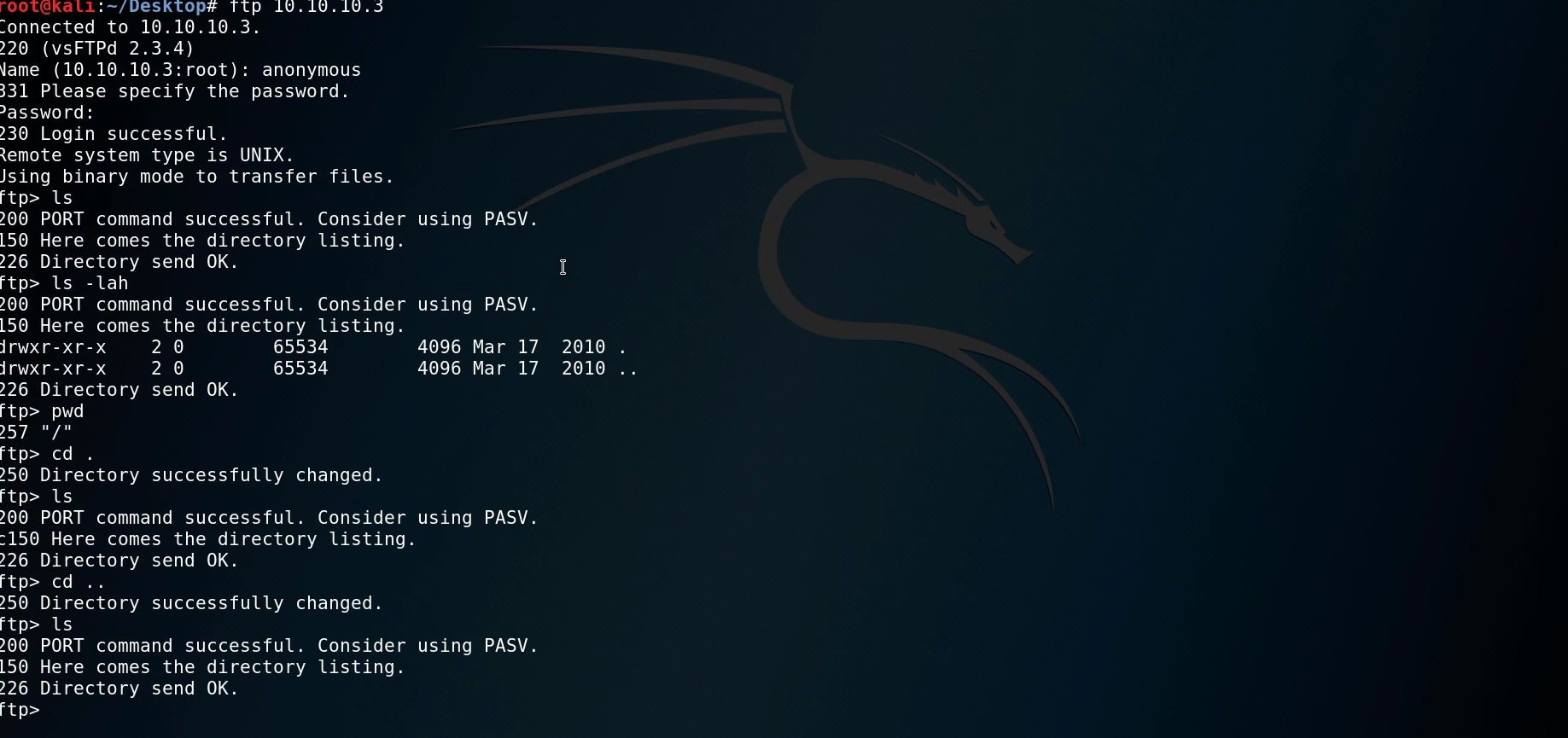
Now we perform Nmap Enumeration/Scan on the Lame VM machine.



* The Scan Identified 4 ports open ftp 21, ssh 22, NetBIOS 139, 445 SMB. Nmap OS detection indicated Linux kernel in 2.6.x family.
* The Anonymous FTP login is allowed. Samba service running on port 445 seems to be vulnerable.

1. **Trying to log into FTP as anonymous.**

We can login to FTP as anonymous if the machine is configured for it. In this machine its enable so we check it out.



We don’t find much useful in FTP service.

1. **Searching for vulnerable service of FTP**

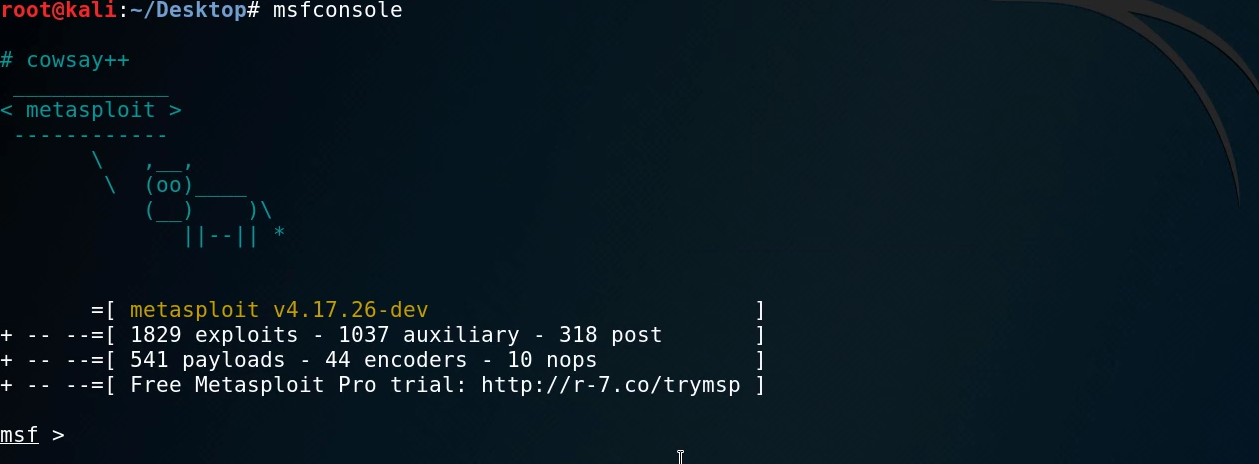
We use searchsploit to findout if the FTP service 2.3.4 is vulnerable and if there is any RCE exploit available.



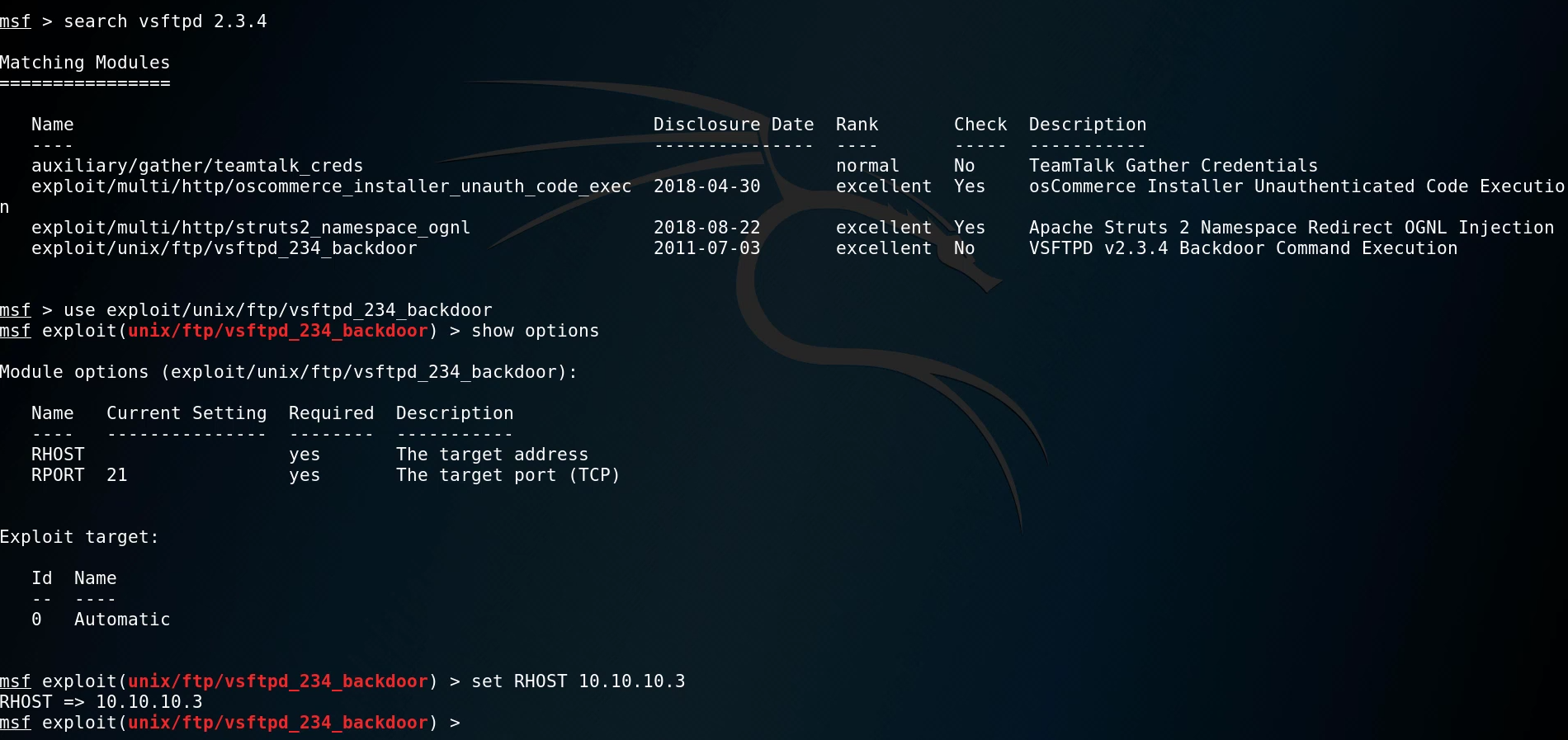
We found out one exploit is available. Lets try to use it in Metasploit.

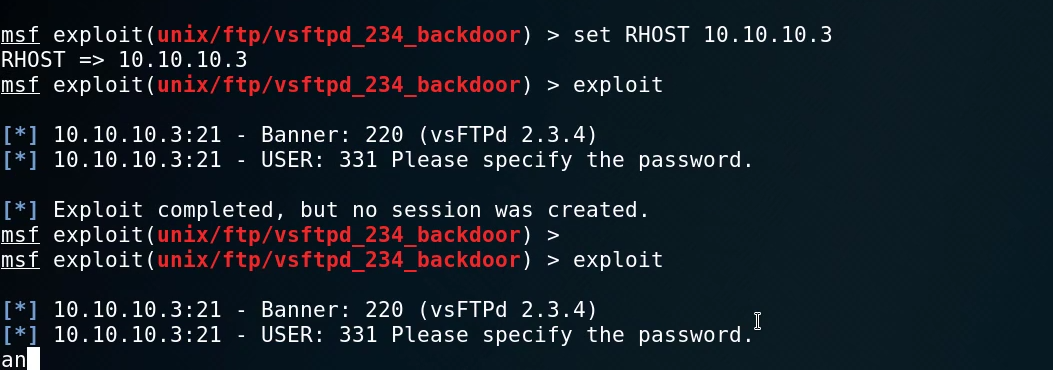
1. **Using Metasploit to perform Exploitation**

Starting Metasploit with the command msfconsole



Configuring the Exploit as per needed by our requirement.

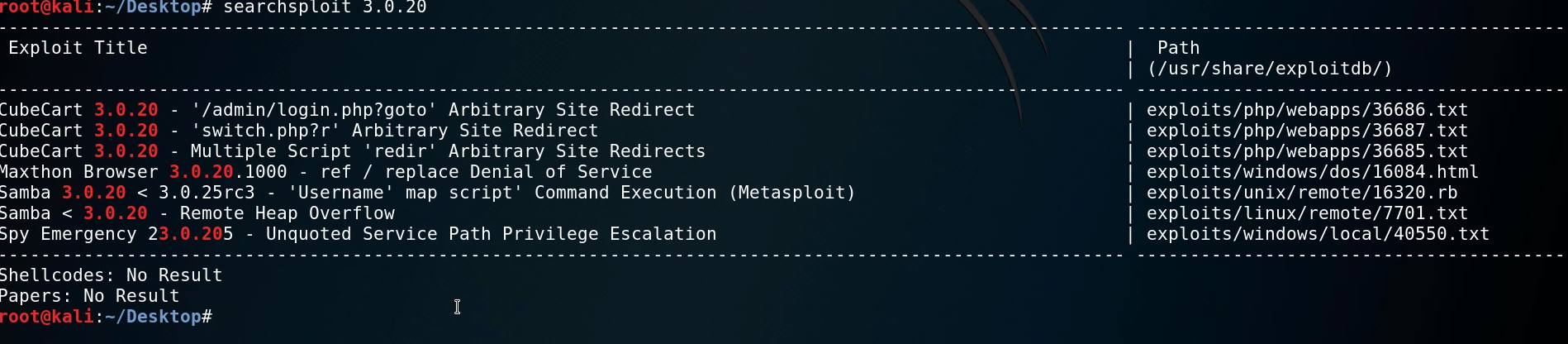




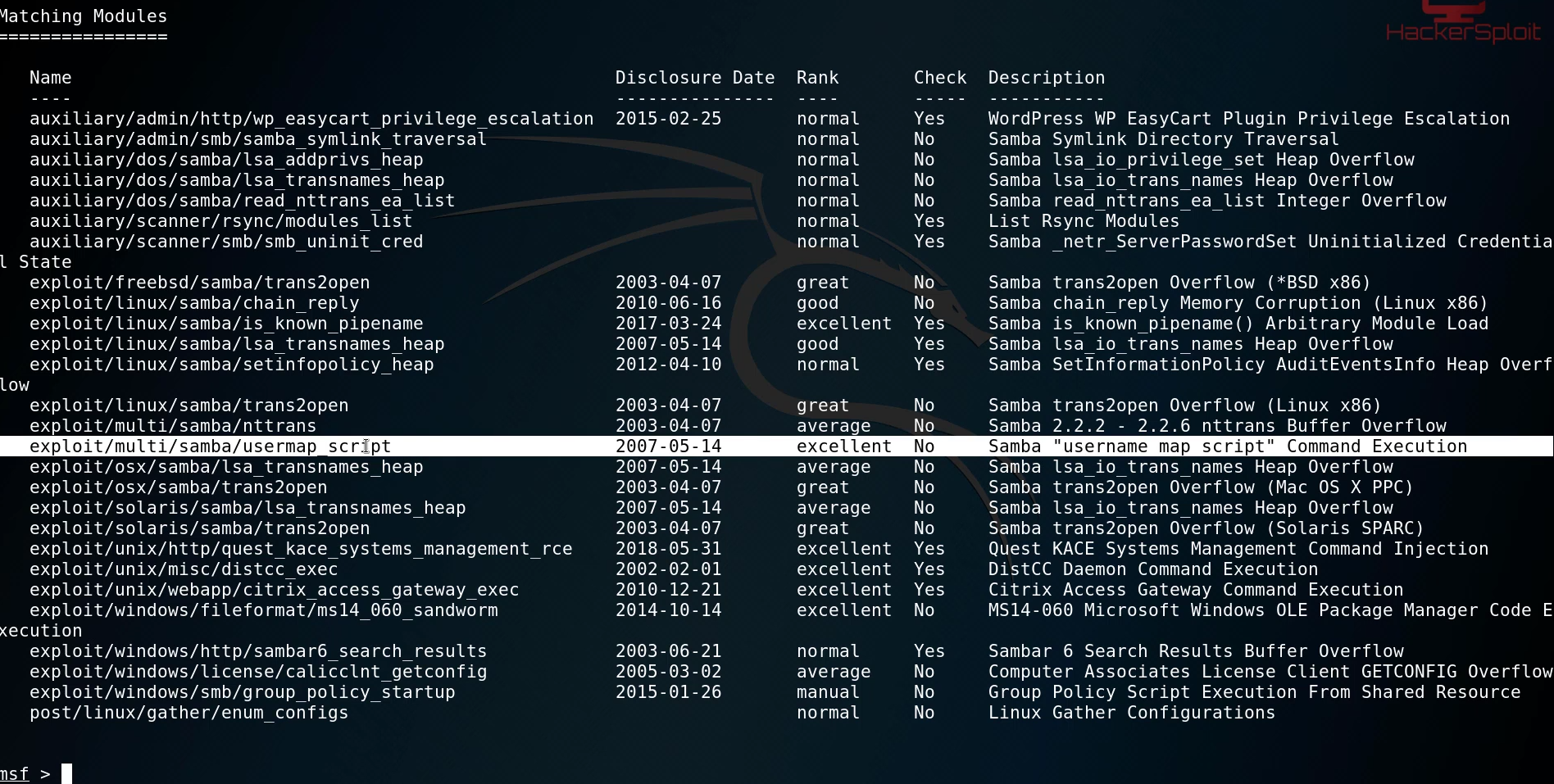
We are unable to find any RCE as the Exploit is not working .

1. **Exploiting Samba 3.0.20**

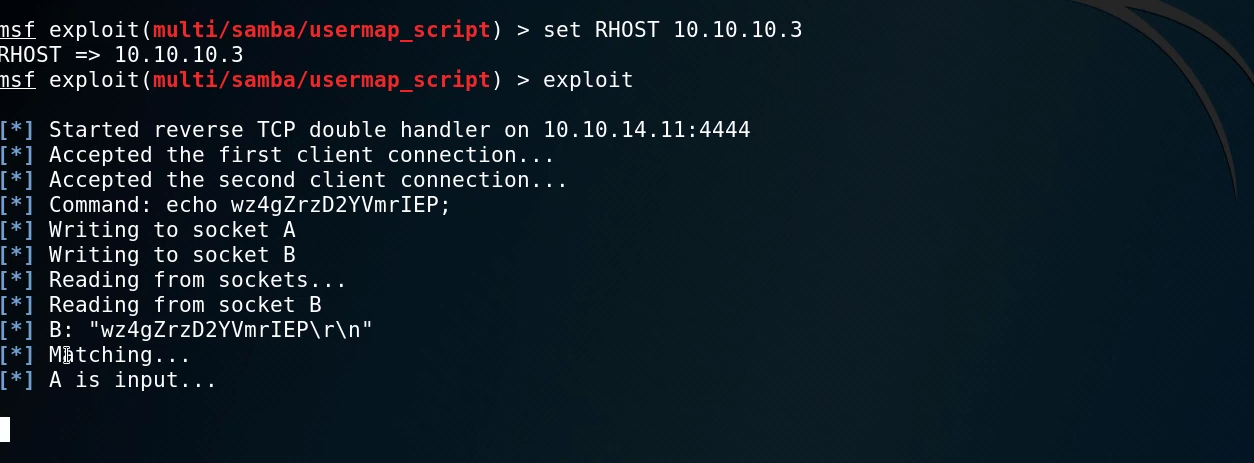
We were unable to exploit vsftpd service. We will try to exploit Samba 3.0.20 service as its also vulnerable.



By searching in searchsploit we are able to find another exploit that is available in Metasploit. Let’s exploit that.



We found the exploit we will configure it and try to exploit it.



We were successfully able to get Remote code execution.

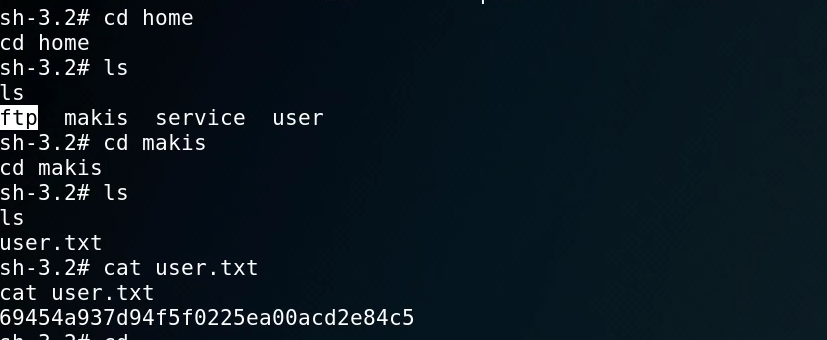
1. **Post Exploitation**

First, we will check our privileges as we got our shell.

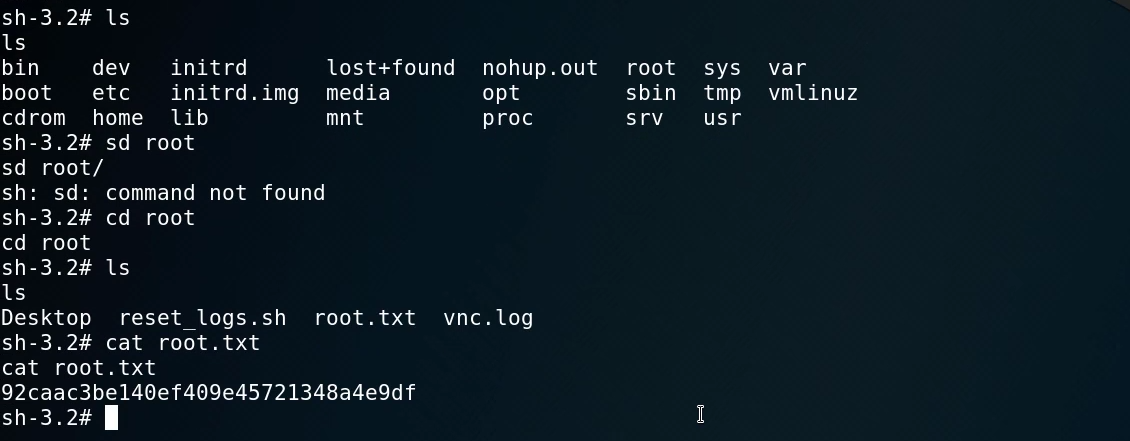


From the above snapshot we can determine that we were able to get root privileges.

Let’s try to get user flag now.

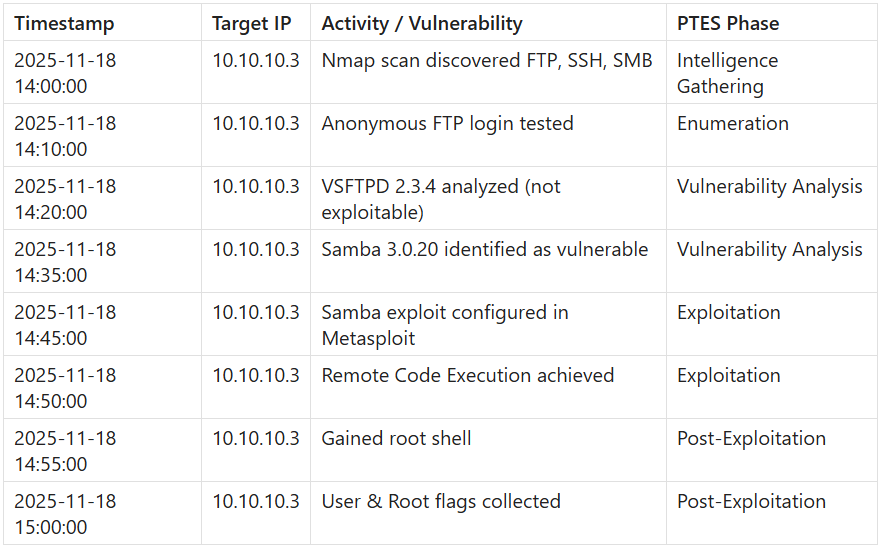


We got the User flag. Now Let’s try to get the Root Flag which is usually in the Root Directory.



We got the root flag as well.

**Attack Timeline**

****

**Remediation Recommendations**

By the result of our full-scale penetration test we are able to determine the VM Lame by HTB have high severity RCE vulnerabilities. Here are some of the recommendations to improve security posture of the machine.

* Update vsftpd 2.3.4 as it is widely known vulnerable service
* Patch samba services as we were able to get RCE
* Disable anonymous ftp misconfiguration
* Regularly update Operating system and services
* Implement Access control lists and firewall
* Enable Logging and monitoring for better traceability.

**Non-Technical Summary**

A full-scale Penetration test was launched against the HTB VM Lame. The results determined that it had several high impact vulnerabilities. These vulnerabilities were found in the outdated services FTP and Samba. This weakness allowed us to gain complete control of the system without authorized credentials. Once inside we were able to access system files and we could retrieve sensitive private system files. It could do further damage and disrupt operations.

This assessment was conducted in controlled environment and no real-world target was harmed in any way. The purpose of this assessment was to find out the security posture and highlight the importance of the software updates which include updates of the services. To reduce the risk of real attack we recommend to update the software regularly and patch misconfigurations, and disabling un-needed services which will greatly improve security posture and decrease attacks surface significantly.