**Phase 5**

**The Capstone Project**

**Executive Summary**

The goal of this Penetration exercise is to find out the security of the Kioptrix level 1 server by finding the vulnerabilities, misconfigurations and analysing their impacts on the server in case of real-world attack. This exercise Revealed certain number of high-risk vulnerabilities including outdated services, misconfigured network components. These issues allowed attacker to exploit the server and attain highest level of privileges possible on the server. Immediate remediation is recommended.

**Tools & Environment**

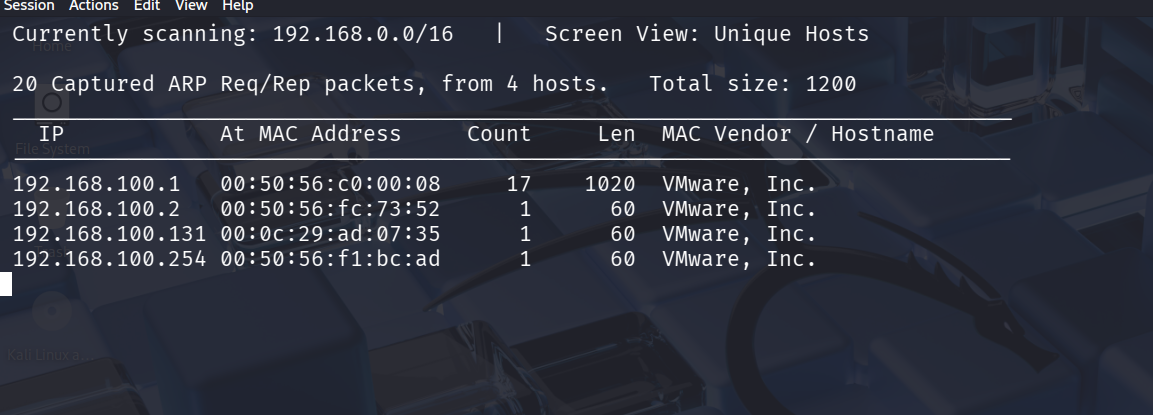
1. Kali Linux Environment
2. Kioptrix VM
3. Metasploit
4. OpenVAS
5. Netdiscover
6. Nmap

**Methodology**

1. **Reconnaissance**

First step is to discover the Kioptrix Level 1 On the Network. We can do this by switch to sudo user and using netdiscover command.

****

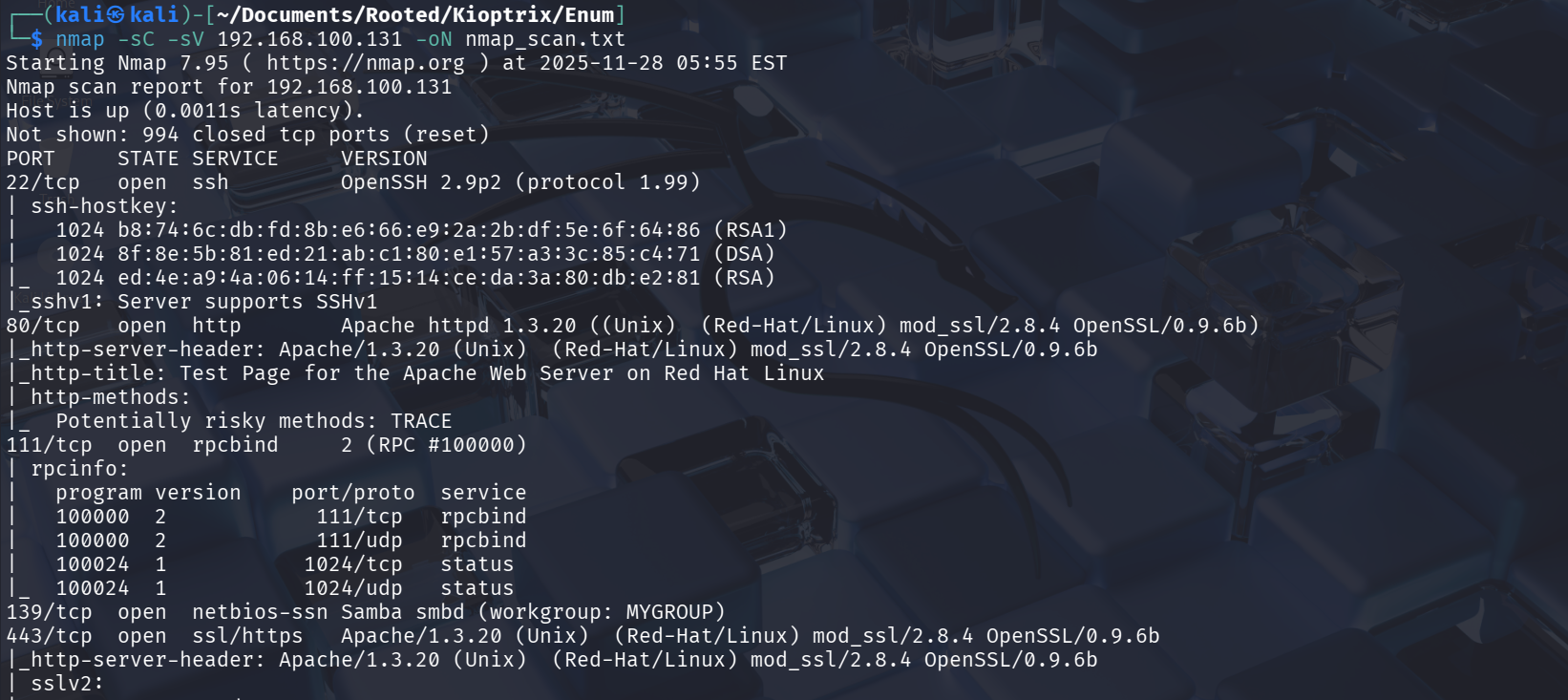
****

By the Above snapshot/output we can determine the IP address of the **Kioptrix Level 1 = 192.168.100.131**

1. **Nmap Scanning of the Kioptrix**

Now we perform Nmap Enumeration/Scan on the Kioptrix machine.

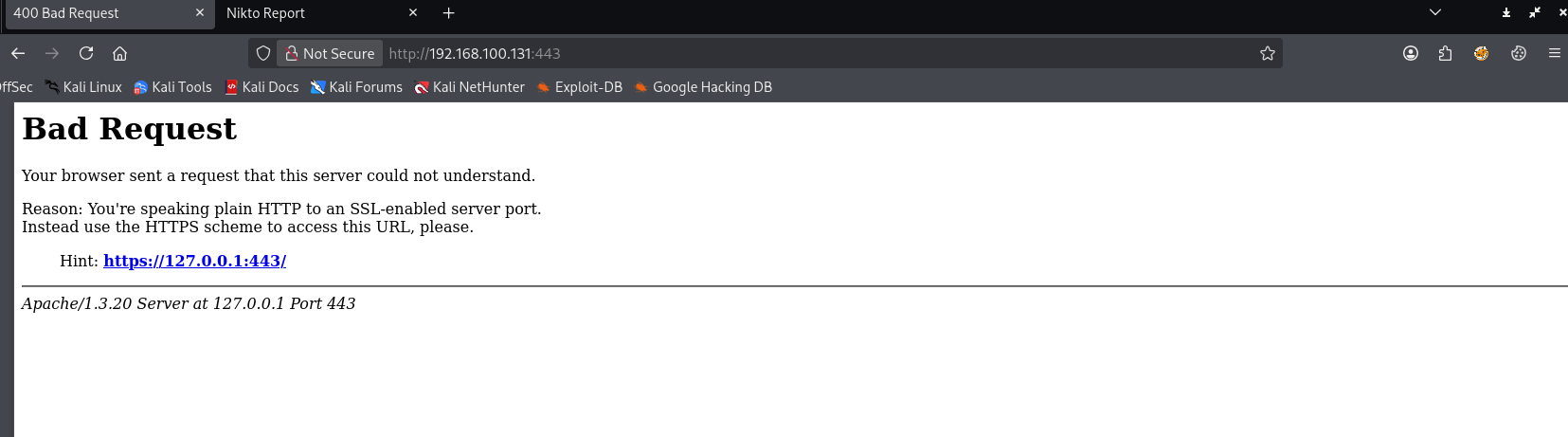




The Scan Resulted in several Open services and the scan output was saved for further processing.



Port 80 HTTP Page from the Kioptrix

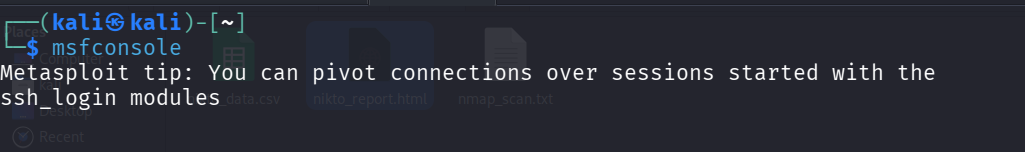


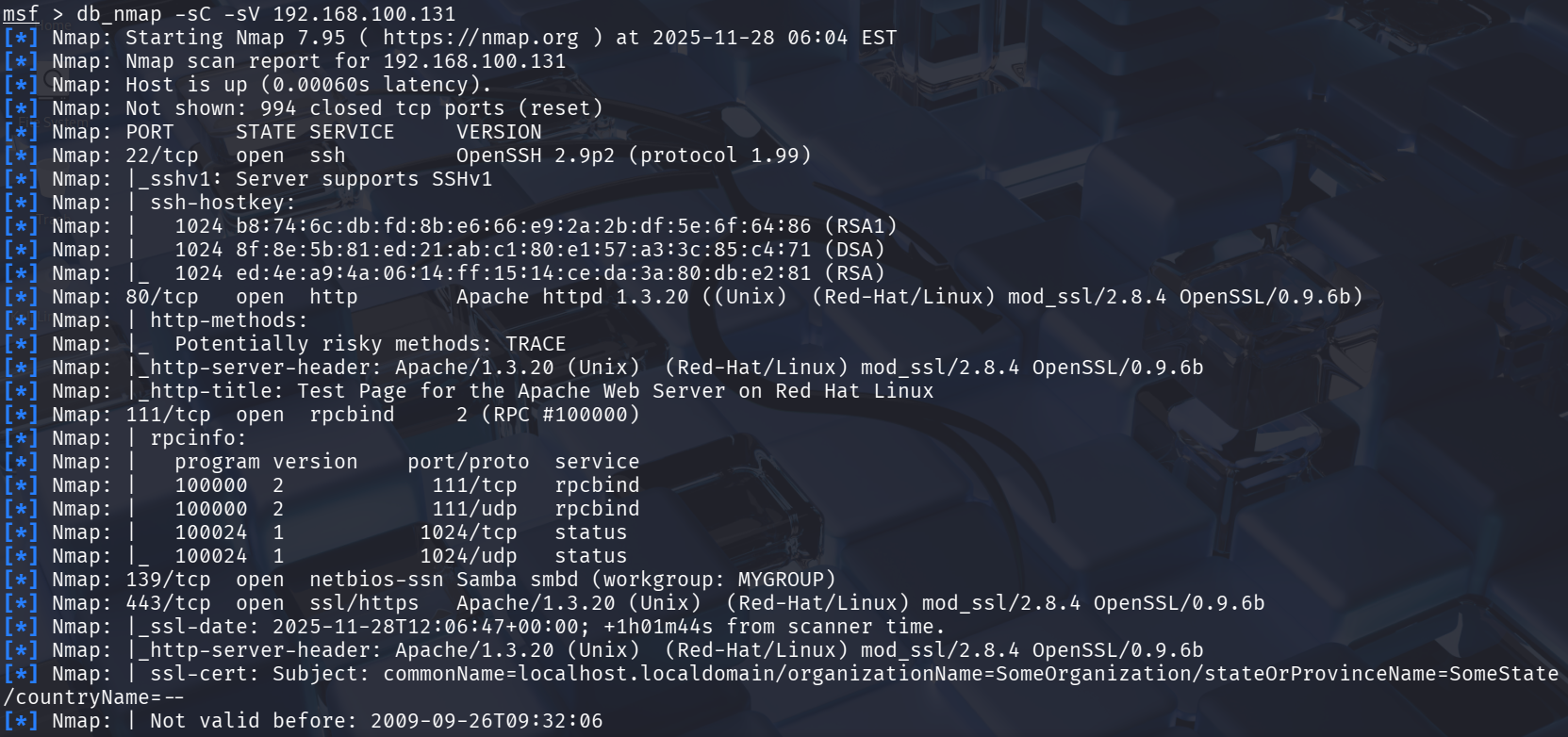
Port 443 HTTPs Page from the Kioptrix

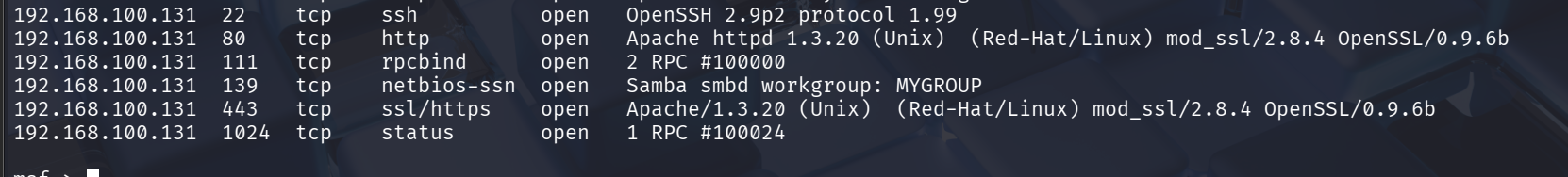
We will continue our Penetration testing by enumerating other services using Metasploit further on.

1. **Using Metasploit for further Penetration testing**

Opening Metasploit using the command **msfconsole**. And rerunning the nmap scan again with the command **db\_nmap -sC -sV 192.168.100.131**.

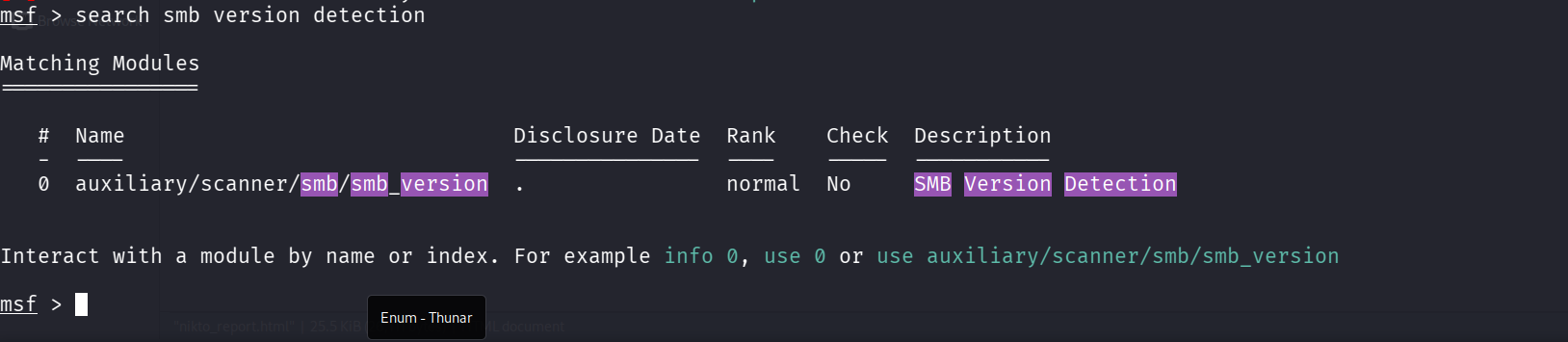


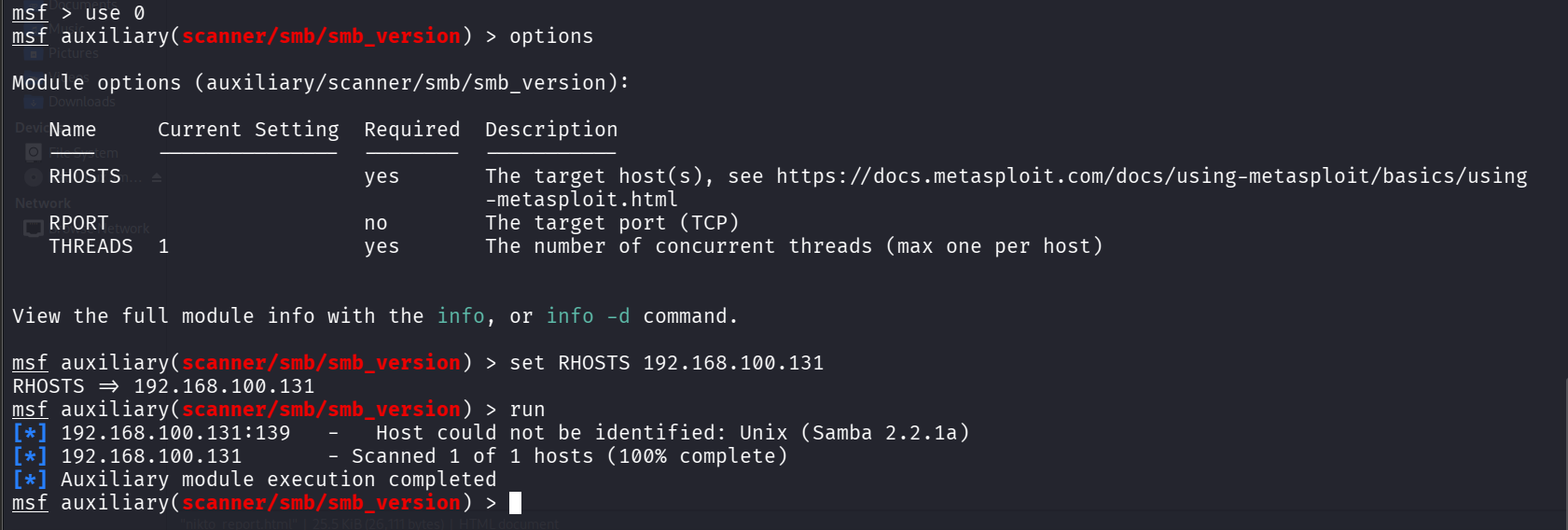




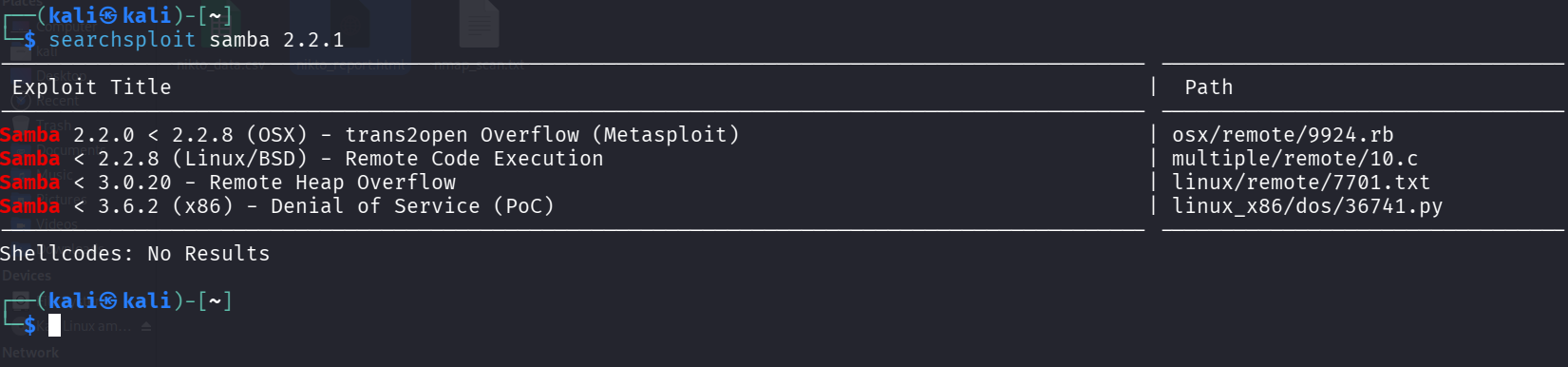
The Full Nmap scan was performed to identify open services. The target had Apache on port 80, SSH on port 22 and Samba on Port 139 and 445.

We will further search for the version of the Samba that is running on this machine.

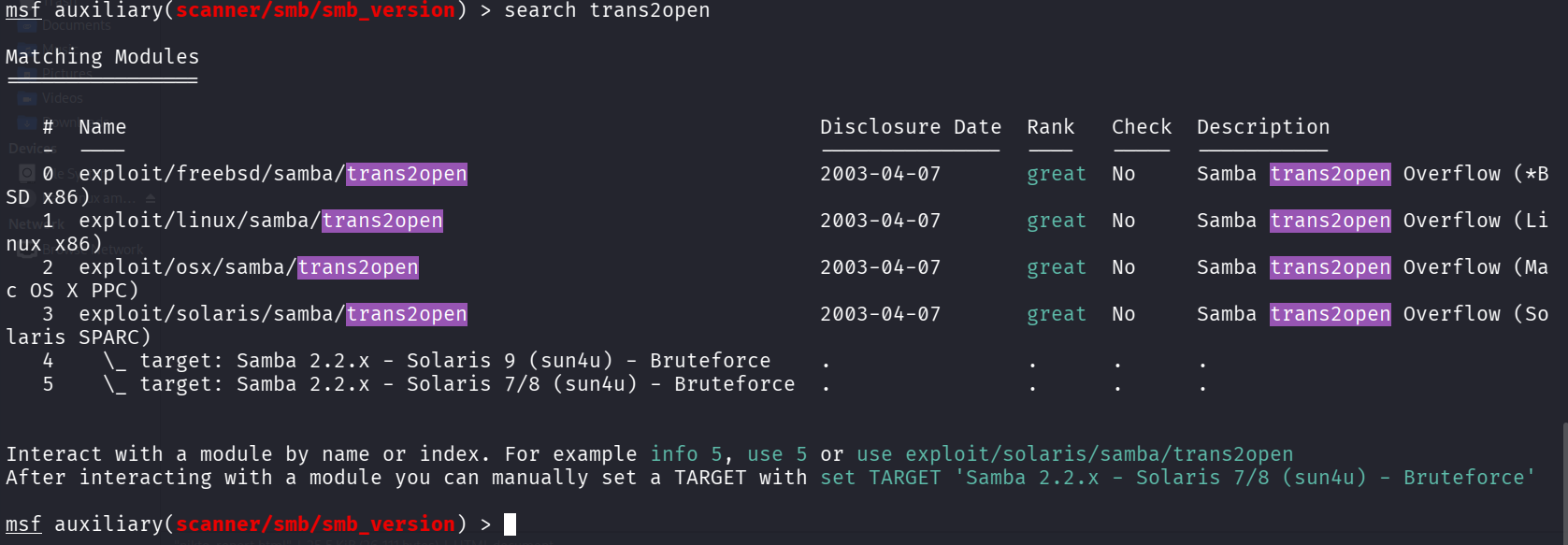




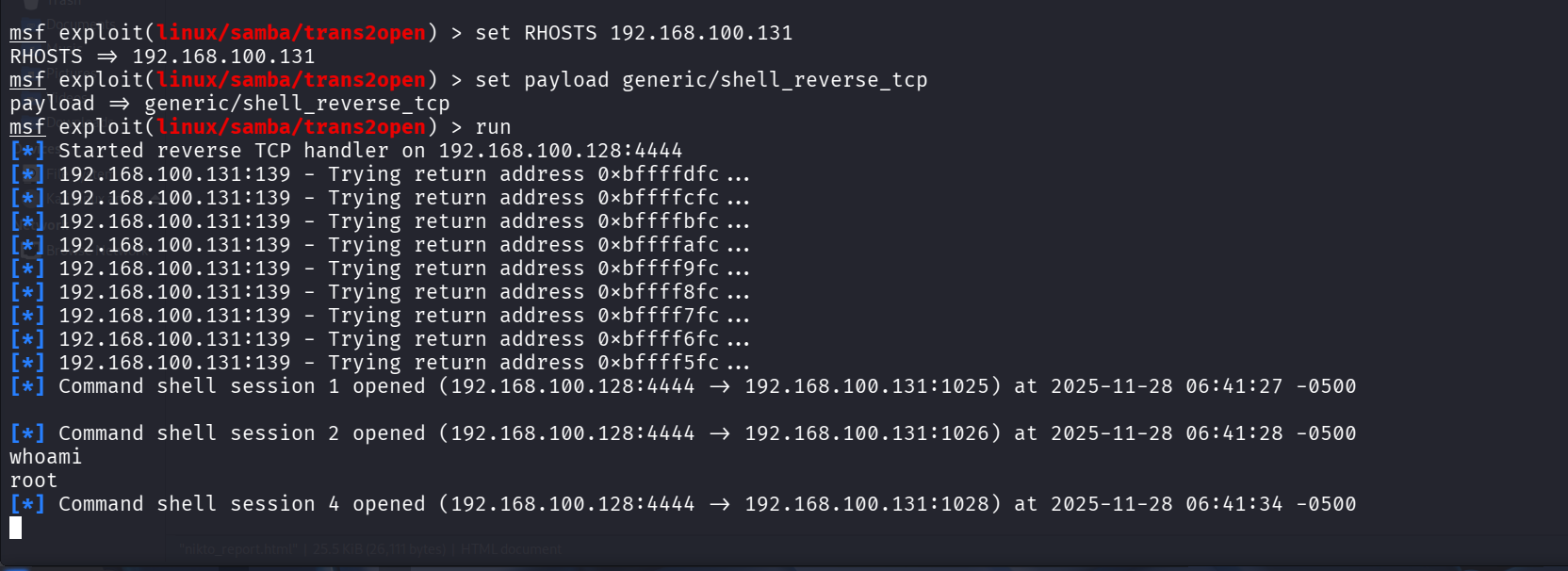
We came to know the version of samba i.e. is 2.2.1a. Let’s see if there is any exploit available for this in searchsploit.



We are able to see one exploit that is available in the Metasploit trans2open overflow let’s check it out.



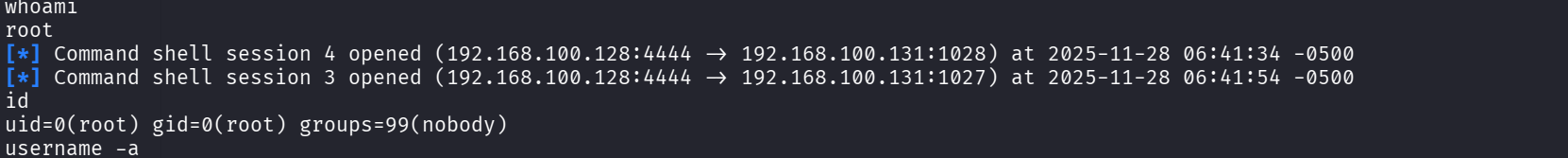
From our Previous Enumeration Phase we know that the Operating system we are dealing with is Linux so we will select Option 2.



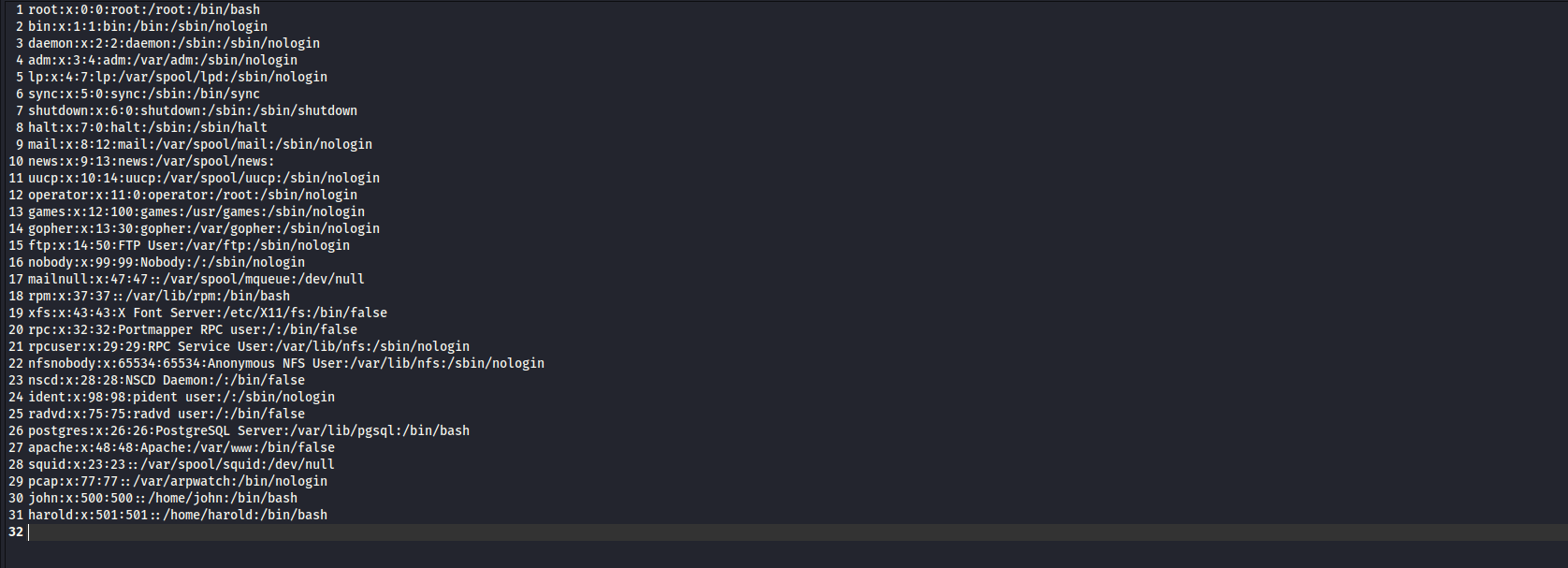
We were able to get Remote code execution and Root access.

1. **Post Exploitation**

We will gather information about system.

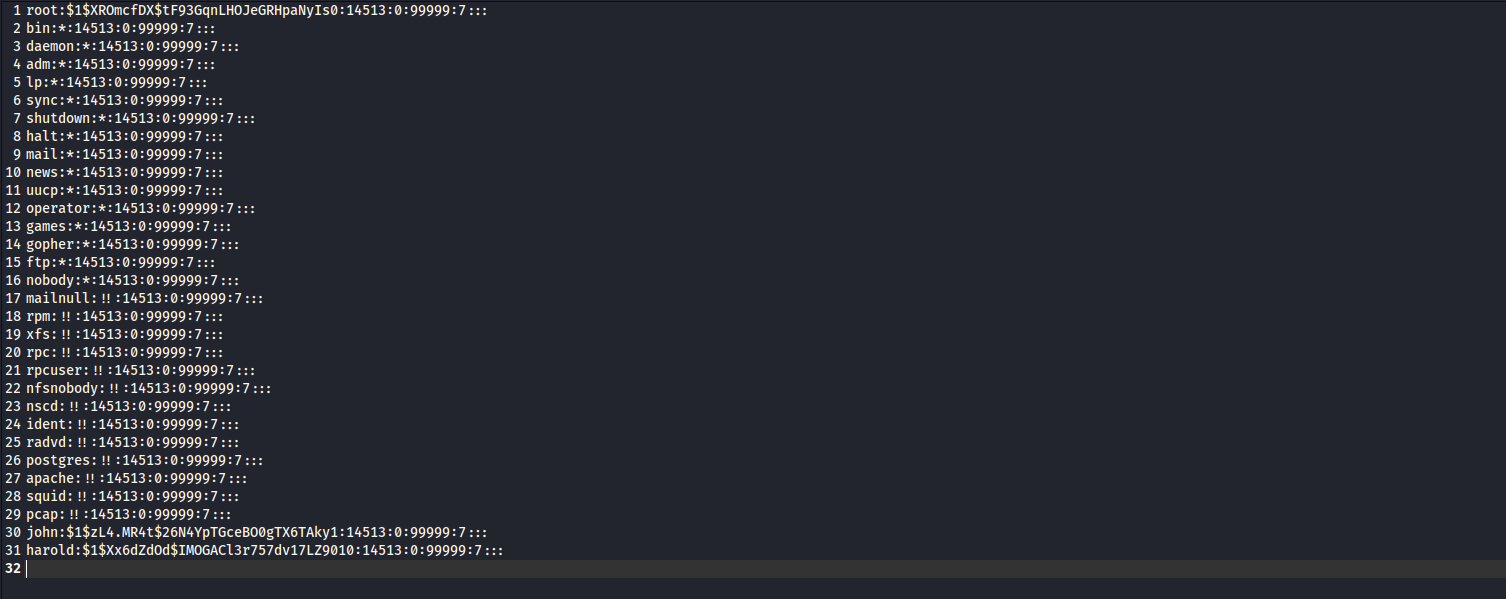


We will also get the passwd file



Hash **“bcb3cd6223a859e97e75e436923730408c09335dc08c6a02f439c25c0ef10fd4”**

Then we will get Shadow file

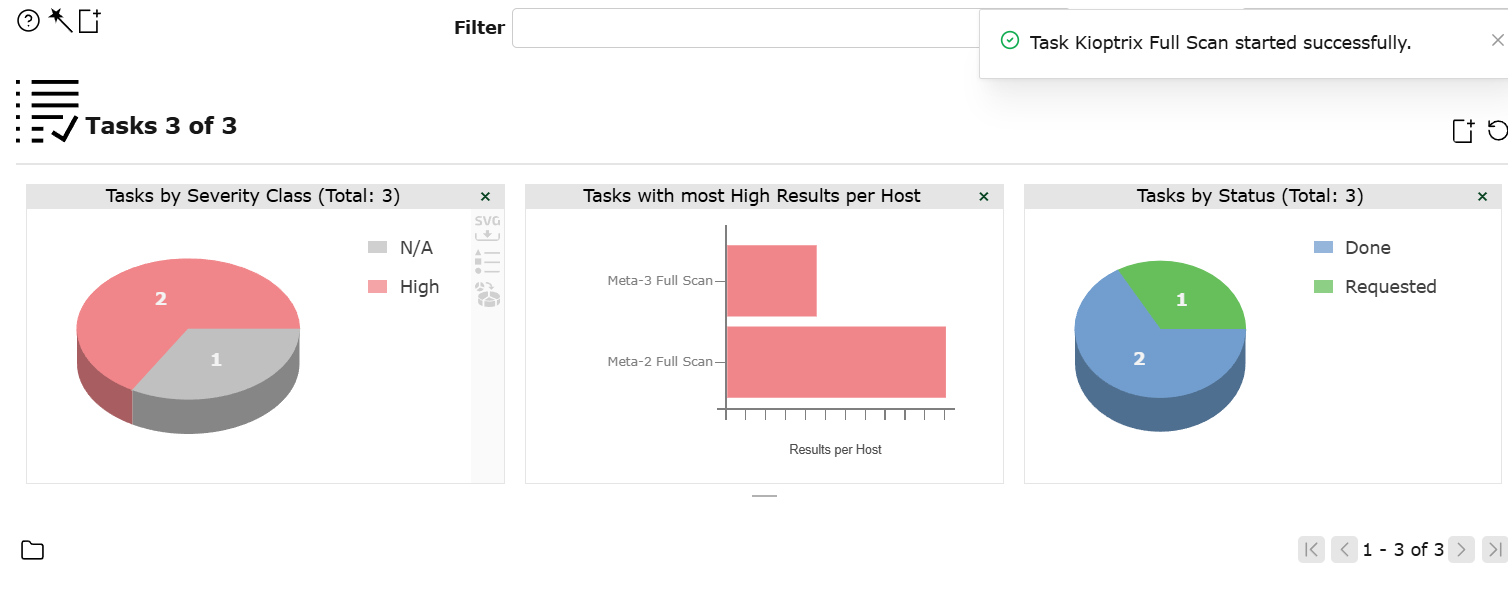


Hash **“6578a00432b987151d02431ae8c96943674d415bd963048ebca1abee21e5cd31”**

We collect 5these files for forensic / integrity purposes which serve as the proof for the compromise of this machine

1. **OpenVAS findings**

The scan was performed on the OpenVAS Vulnerability scanner and the output was saved. Findings table has been extracted form the report.





**Remediation**

1. Update Samba to a supported version (2.2.1a is end-of-life).
2. Disable anonymous SMB access.
3. Apply firewall rules to restrict SMB to trusted IPs.
4. Upgrade Apache to latest branch.
5. Disable directory negotiation or restrict extensions.

**Rescan:**

Re-run Nmap/OpenVAS after applying patches.

**Non-Technical Summary**

The Penetration test on Kioptrix level 1 system resulted in several serious weakness. This puts the system in the region of highly comprisable target. Outdated services, outdated encryption technologies and misconfigured configurations allowed attacker to gain complete root access of the Kioptrix system. The Most critical issue was Samba. It is a service that is used to perform printing tasks which was out dated and vulnerable. Immediate corrective actions suggested are to update the software and improving misconfigured services.