**Service Enumeration**

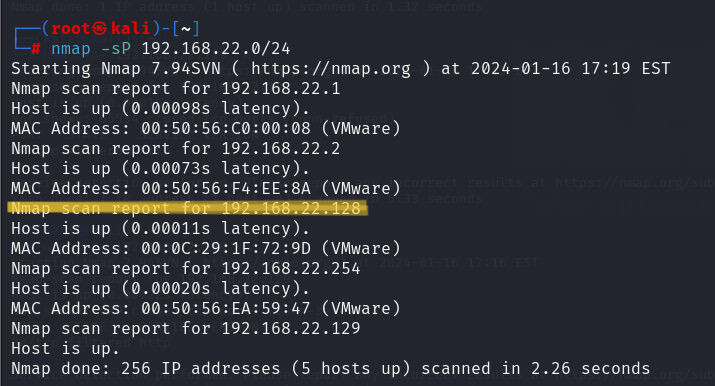
The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168.22.128 | **TCP:** 22, 80, 111, 139, 443,1024 |

**Initial Shell Vulnerability Exploited:   
*Additional info about where the initial shell was acquired from:***

**Nmap Scan Results:**

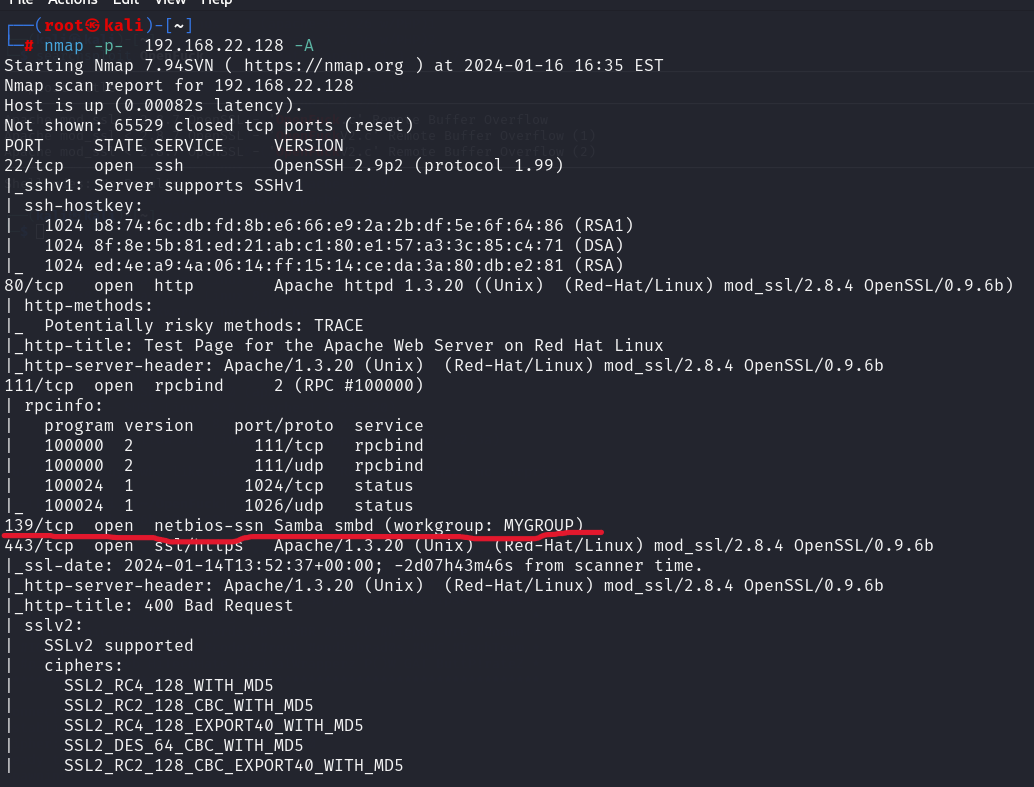
At first I found the correct IP address for the machine.

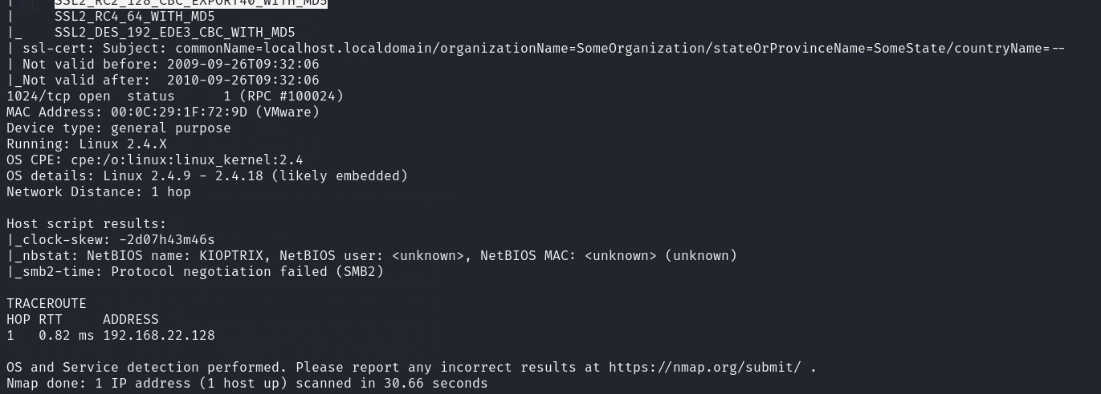


I found that the target runs two open services that I also listed in the table above based on Nmap results.

* 1. Port 22 OpenSSH 2.9p2
  2. Port 80 Apache httpd 1.3.20
  3. Port 111 2 (RPC #100000)
  4. Port 139 Samba smbd
  5. Port 443 Apache 1.3.20
  6. Port 1024 1 (RPC #100024)

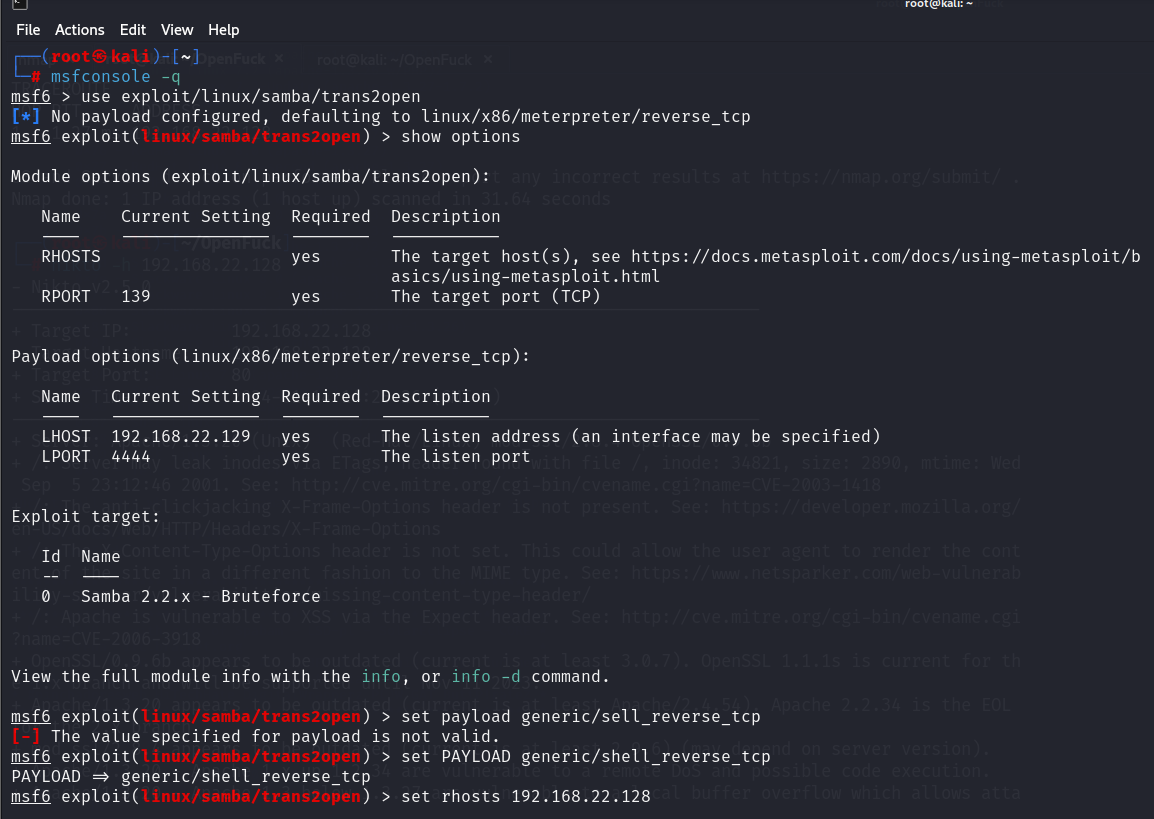
I performed an nmap check on the required IP address, and found that port 139 is open.

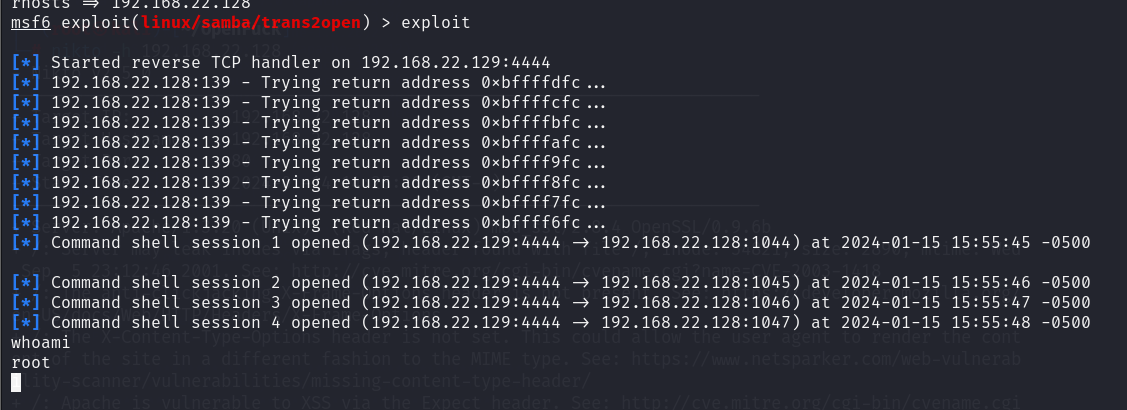




Then after we found the existing ports on the machine, in order to get to the shell I entered Metasploit to use the appropriate exploit (exploit/linux/samba/trans2open).

After I entered the appropriate values ​​for the exploit, I activated it and managed to take over the machine with root privileges.



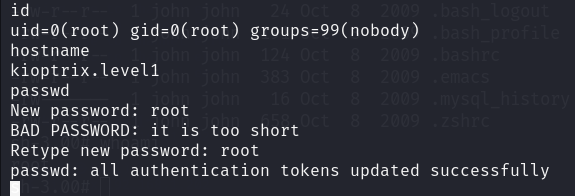


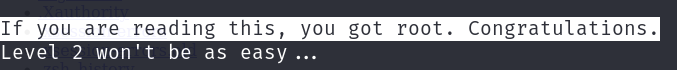
**Vulnerability Explanation:**

Vulnerabilities using port 139:  
The vulnerability in this case is related to a weakness in the Linux Samba service.  
The version of port 139 is Samba smb, so to get to the shell we use Metasploit in order to target the attack on the machine, and thus we can gain access to the system.

**Vulnerability Fix:** To solve the problem of the hacks and the weakness, you need to update the version of smb in order to prevent it.  
Update version in Linux

**Initial Shell Screenshot:**





**Privilege Escalation:  
*Additional Priv Esc info:***

Due to the fact that we received root permission in the initial shell, there is no need to explain about Privilege Escalation, because we have already reached the highest privileges