

**INSTITUTE OF EMERGING CAREERS**

### COHORT – 6

**Course: Cyber Security**

**Week: 14**

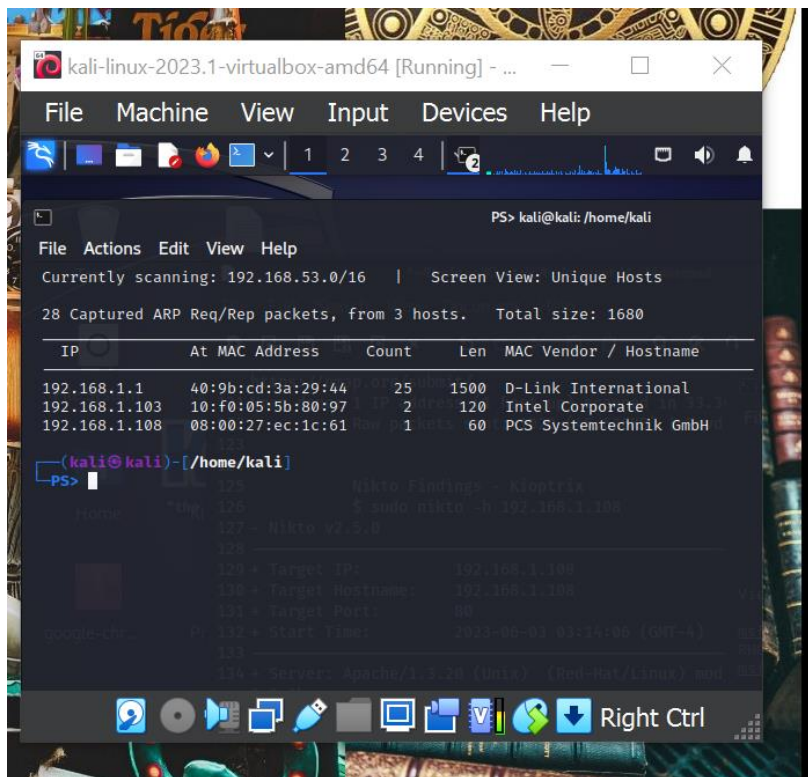
## Assignment 14: Find vulnerabilities and attack the machine

**Name of the Student: Muhammad Umer Taj**

**Topic:** Kioptrix

## Challenge: Solve the CTF machine

## Identifying the IP of the target Machine



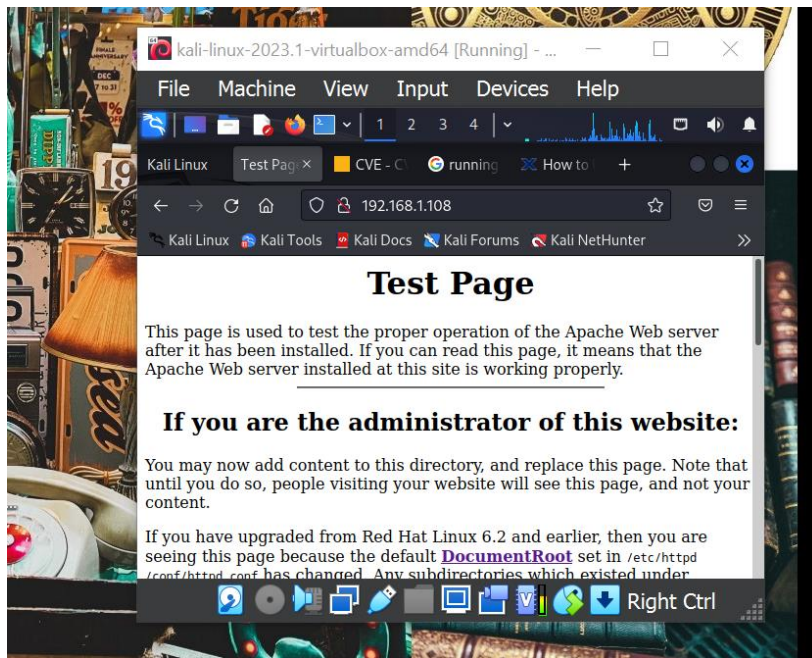
## Running NMAP on 192.168.1.108

```
1 Kiotrnx Nmapot Scan
2 $ sudo nmap -v -sV -A 192.168.1.108
3 Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-03 03:06 EDT
4 NSE: Loaded 155 scripts for scanning.
5 NSE: Script Pre-scanning.
6 Initiating NSE at 03:06
7 Completed NSE at 03:06, 0.00s elapsed
8 Initiating NSE at 03:06
9 Completed NSE at 03:06, 0.00s elapsed
10 Initiating NSE at 03:06
11 Completed NSE at 03:06, 0.00s elapsed
12 Initiating ARP Ping Scan at 03:06
13 Scanning 192.168.1.108 [1 port]
14 Completed ARP Ping Scan at 03:06, 0.06s elapsed (1 total hosts)
15 Initiating Parallel DNS resolution of 1 host. at 03:06
16 Completed Parallel DNS resolution of 1 host. at 03:06, 13.04s elapsed
17 Initiating SYN Stealth Scan at 03:06
18 Scanning 192.168.1.108 [1000 ports]
19 Discovered open port 139/tcp on 192.168.1.108
```

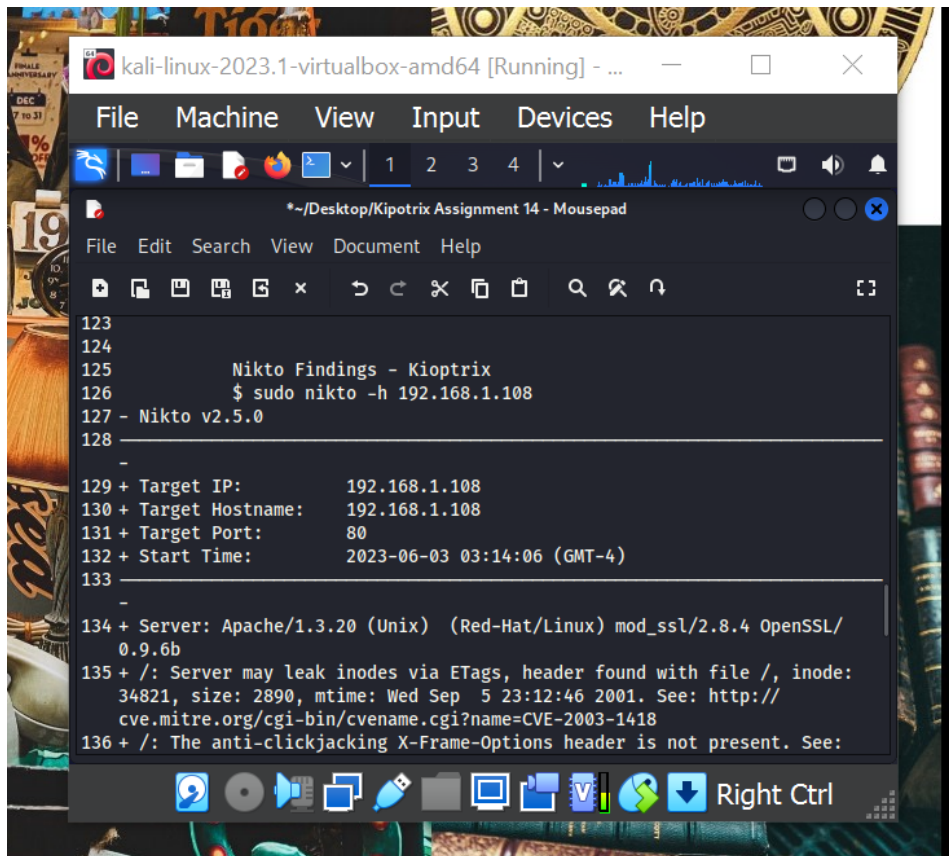
Found a few open ports including port 80, 443 and 139

```
9 Completed NSE at 03:06, 0.00s elapsed
10 Initiating NSE at 03:06
11 Completed NSE at 03:06, 0.00s elapsed
12 Initiating ARP Ping Scan at 03:06
13 Scanning 192.168.1.108 [1 port]
14 Completed ARP Ping Scan at 03:06, 0.06s elapsed (1 total hosts)
15 Initiating Parallel DNS resolution of 1 host. at 03:06
16 Completed Parallel DNS resolution of 1 host. at 03:06, 13.04s elapsed
17 Initiating SYN Stealth Scan at 03:06
18 Scanning 192.168.1.108 [1000 ports]
19 Discovered open port 139/tcp on 192.168.1.108
20 Discovered open port 443/tcp on 192.168.1.108
21 Discovered open port 80/tcp on 192.168.1.108
22 Discovered open port 111/tcp on 192.168.1.108
23 Discovered open port 22/tcp on 192.168.1.108
24 Discovered open port 32768/tcp on 192.168.1.108
25 Completed SYN Stealth Scan at 03:06, 0.07s elapsed (1000 total ports)
26 Initiating Service scan at 03:06
27 Scanning 6 services on 192.168.1.108
```

Information on Port 80

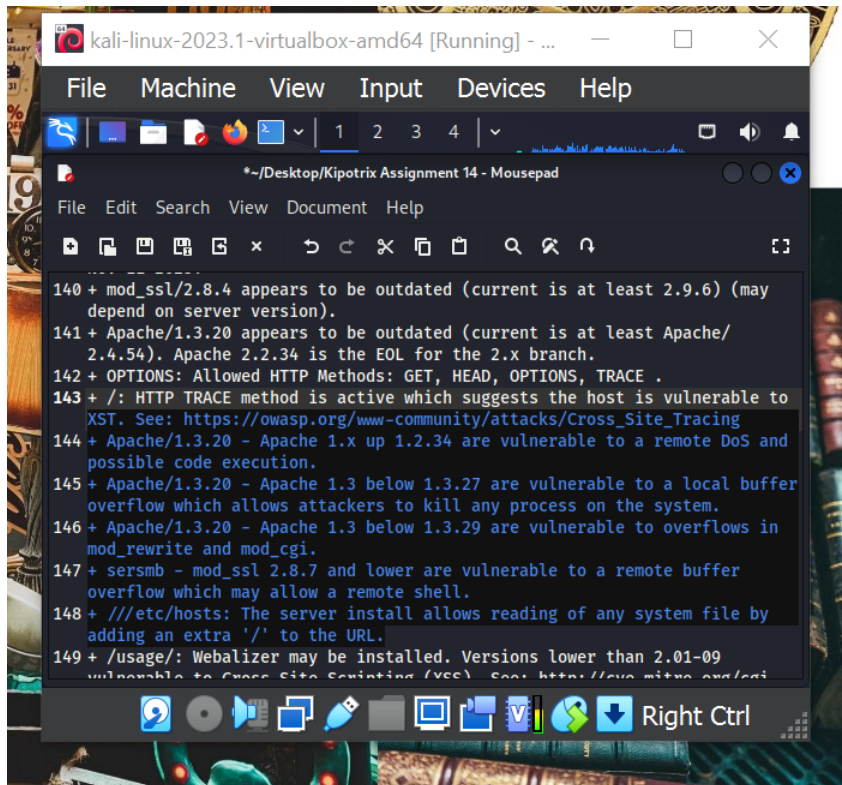


Running Nikto on the target machine and identifying vulnerabilities

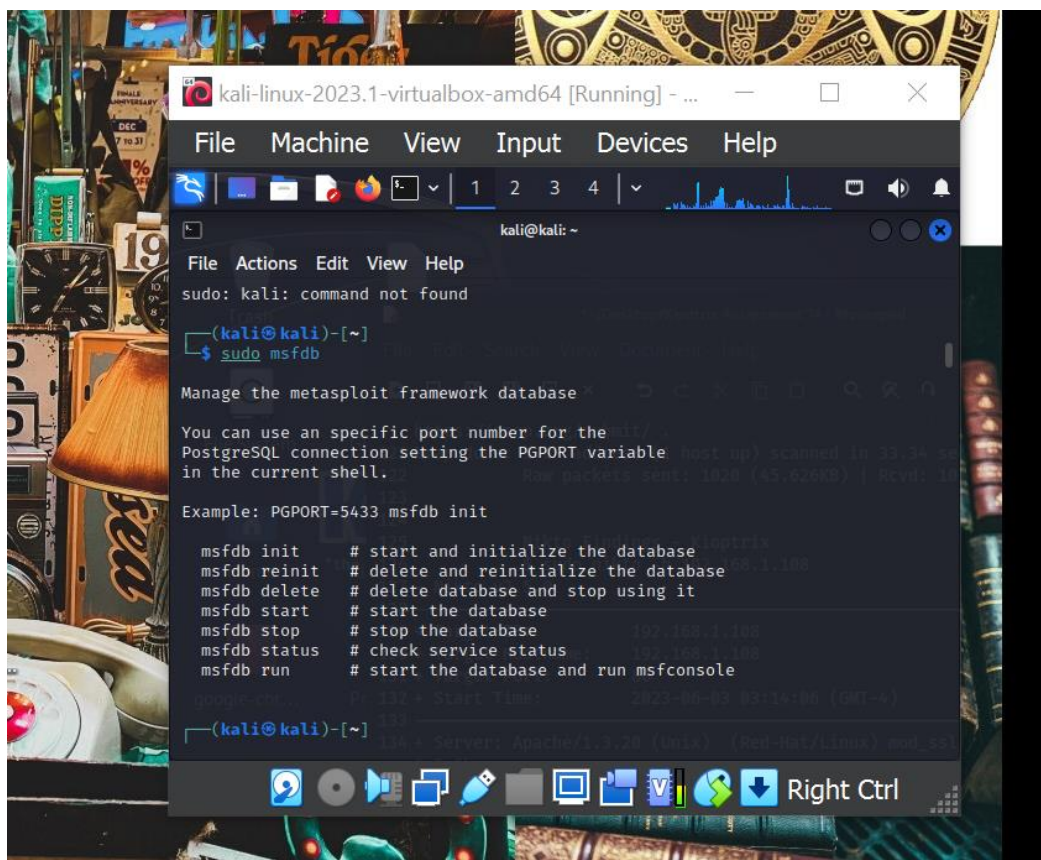




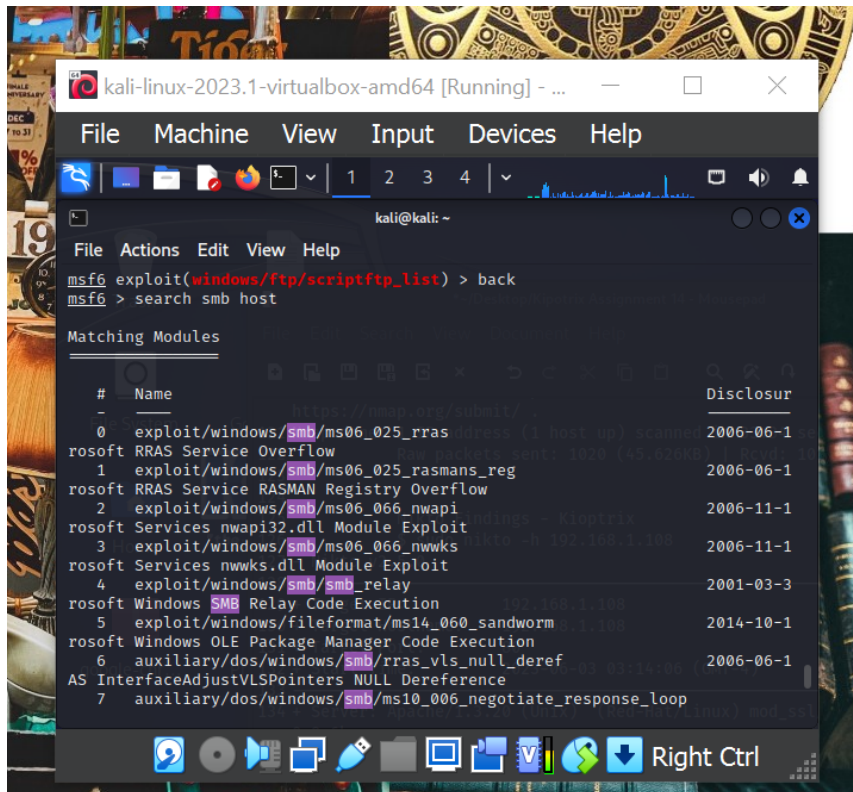
## Identifying vulnerabilities to be exploited



Metasploit framework initialized:

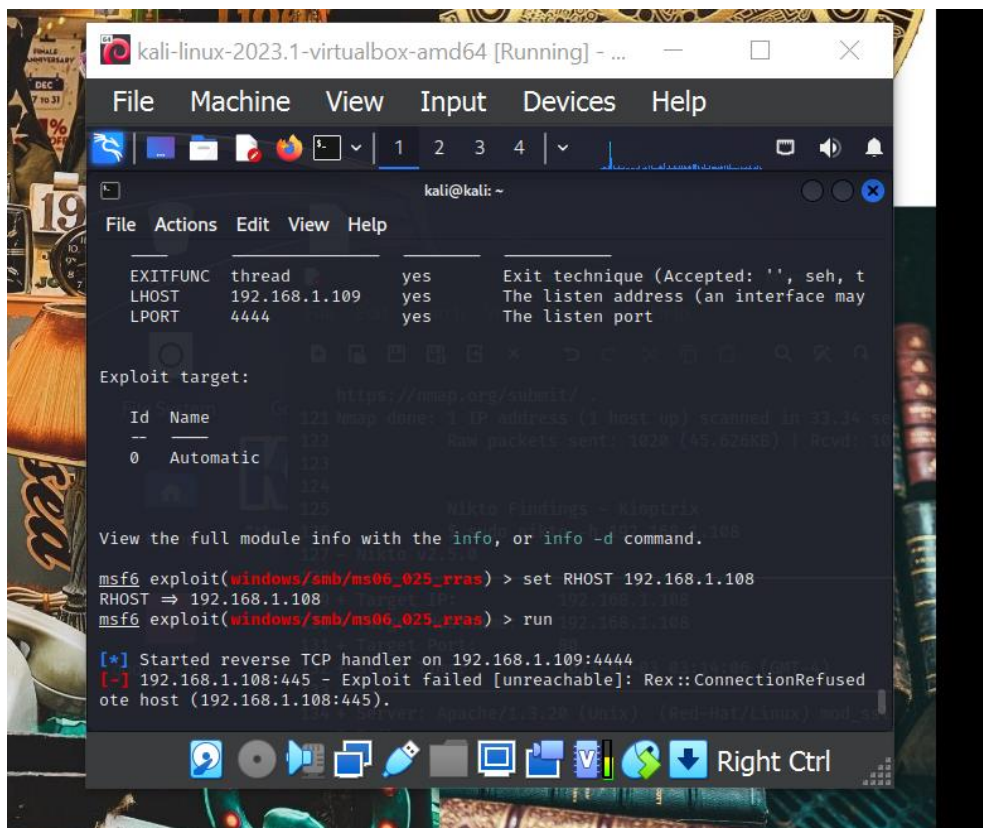


## Ran a search for the vulnerabilities found

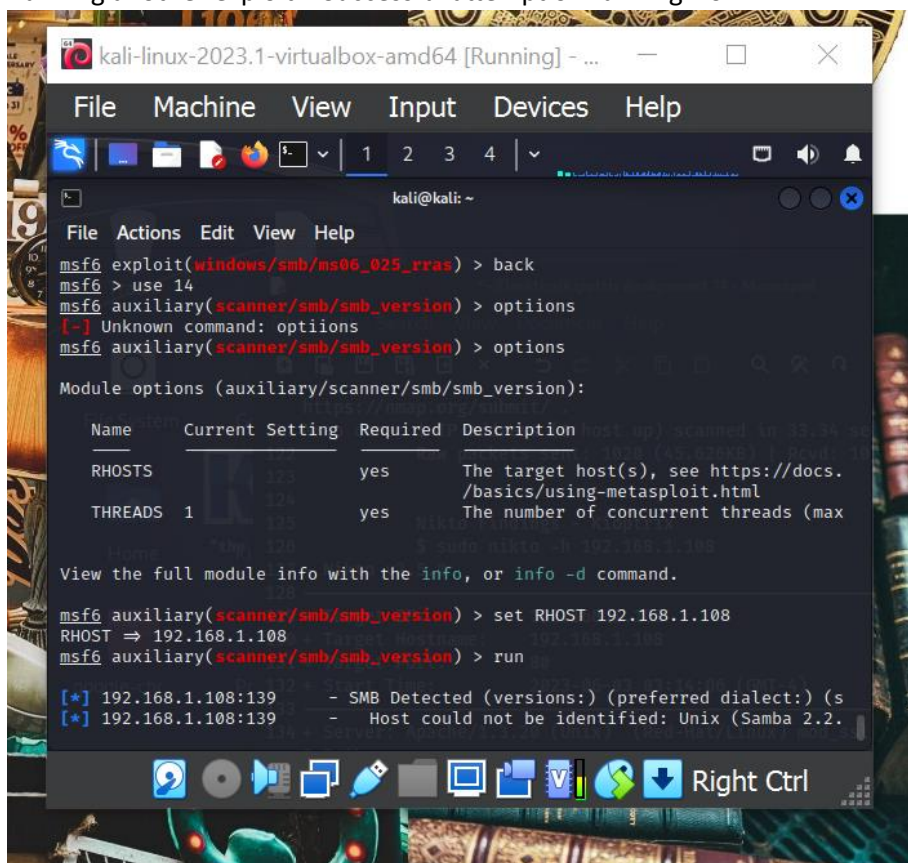


Found exploit capable of running remote shell that the machine was found vulnerable to through Nikto scanner.

### Running the exploit – Unsuccessful attempt

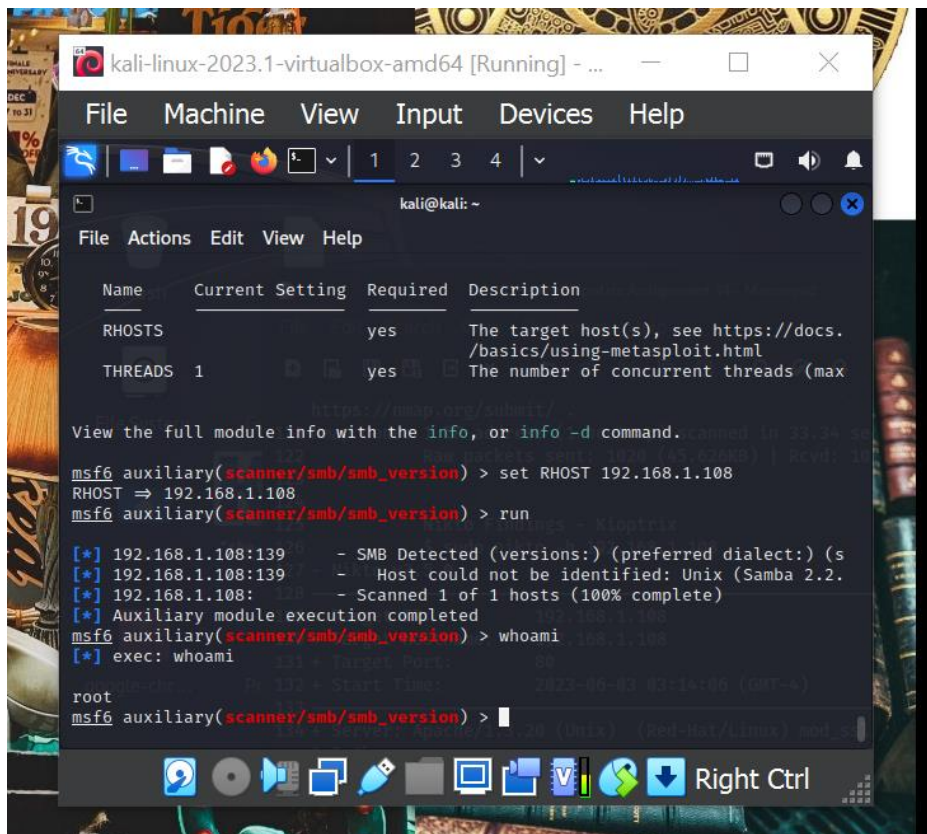


Running another exploit – Successful attempt on running No. 14





## Root privileges acquired



The screenshot shows a Kali Linux terminal window titled "kali-linux-2023.1-virtualbox-amd64 [Running] - ...". The terminal displays the Metasploit Meterpreter (msf6) interface. The user has set the RHOST to 192.168.1.108 and executed the 'auxiliary/scanner/smb/smb\_version' module. The output shows SMB detected on 192.168.1.108:139, identifying the host as Unix (Samba 2.2.0). Subsequently, the user executed 'whoami', which returned 'root', indicating that root privileges were successfully acquired.

```
kali@kali: ~  
File Actions Edit View Help  
Name      Current Setting  Required  Description  
-----  
RHOSTS    192.168.1.108    yes       The target host(s), see https://docs.  
/basics/using-metasploit.html  
THREADS   1                yes       The number of concurrent threads (max  
https://www.exploit-db.com/submit/  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.1.108  
RHOST => 192.168.1.108  
msf6 auxiliary(scanner/smb/smb_version) > run  
[*] 192.168.1.108:139 - SMB Detected (versions:) (preferred dialect:) (s  
[*] 192.168.1.108:139 - Host could not be identified: Unix (Samba 2.2.  
[*] 192.168.1.108:139 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/smb/smb_version) > whoami  
[*] exec: whoami  
root  
msf6 auxiliary(scanner/smb/smb_version) >
```