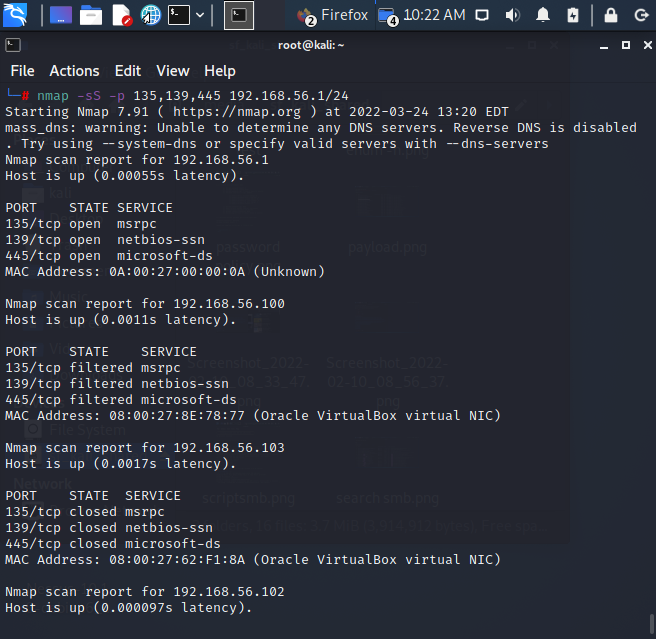
**Task 1:**

**Overview**

1. Let’s start by launching a Syn scan on our potential victims:

Nmap- sS –p 135, 139, 445 {target-range}



2. Write down the IPs of the potential targets

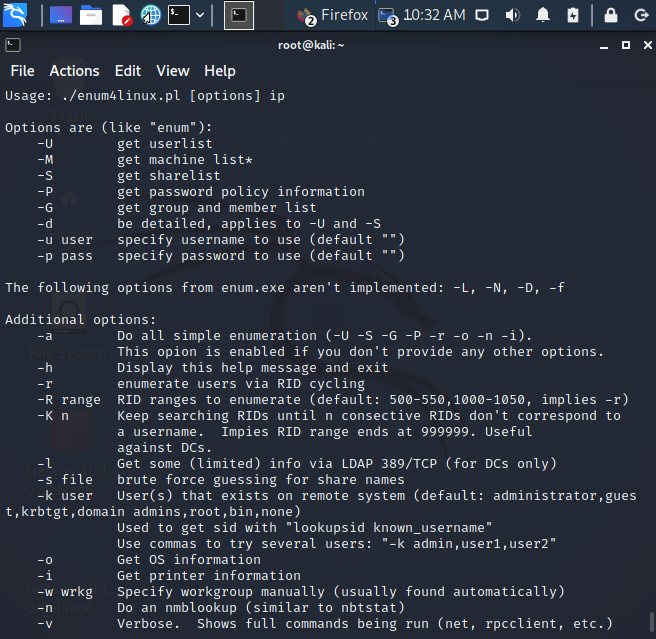
192.168.56.1

192.168.56.100

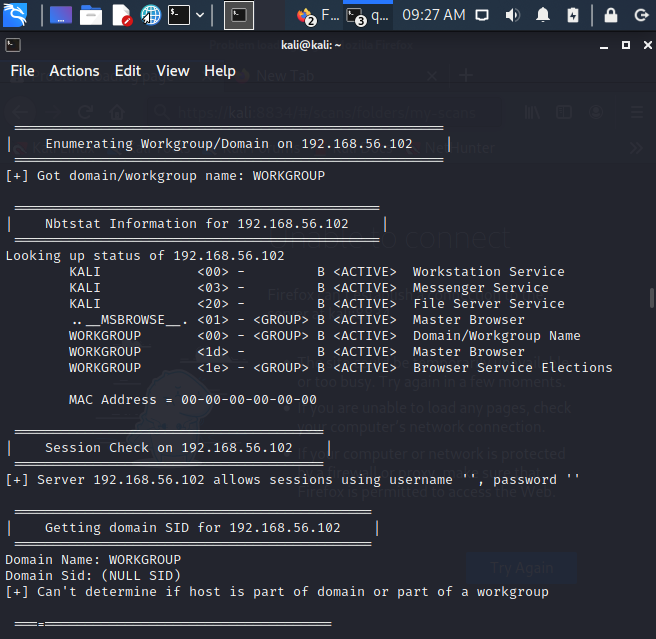
192.168.56.102

192.168.56.103

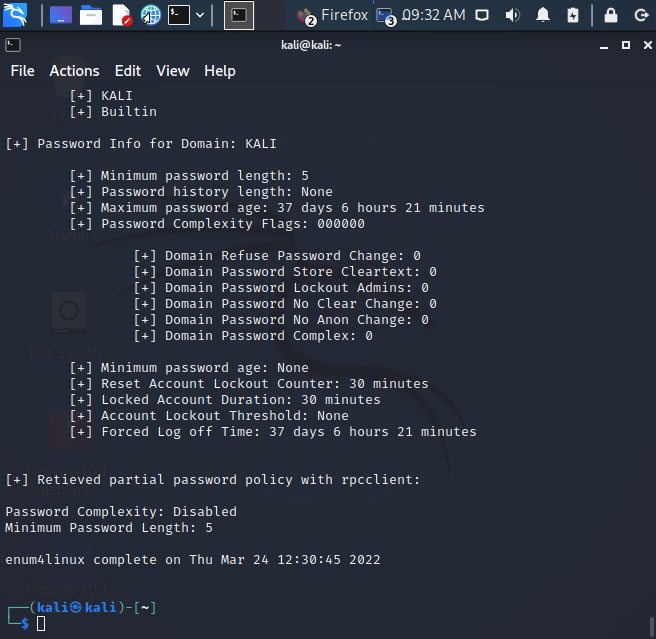
3. Use the enum4linux tool to identify hosts with null-sessions. Type the command {Enum4linux } without any options, write down the possible options that could help to get information about the target system.



4. Type the command with the (-n) option. In the output, refer to the Nbtstat information section, and identify the entry with value <20>. What does it mean?

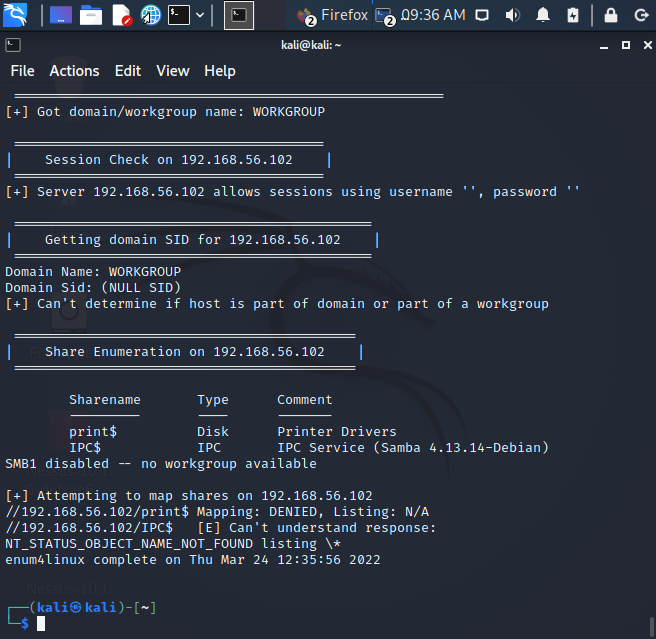


5. Run the command again with the (-P) option, note down the password policy on the target system. How could this information help attackers?

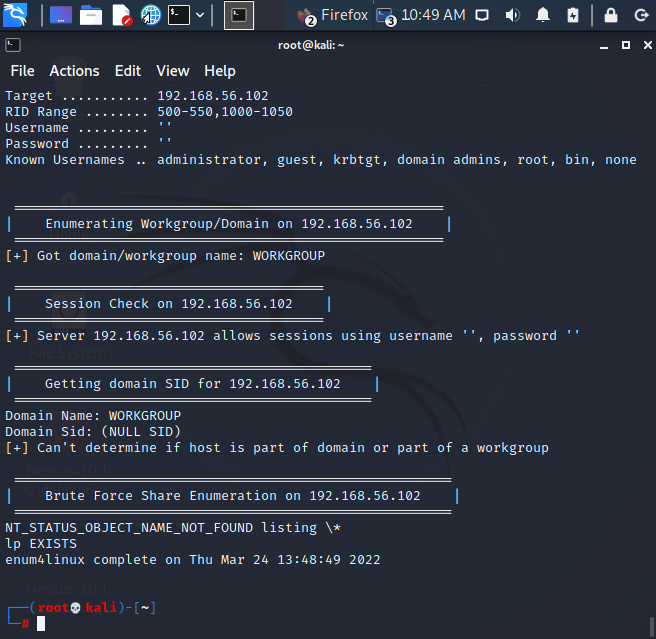


This provides useful information about the password policies present on the machine. Here we can see information like the minimum password length, password age, and complexity requirements. This can be extremely useful to an attacker in the information-gathering phase of an attack, as it can help narrow down password brute-force attempts.

6. Run the command with the (-S) option. Note down the names of the shared resources.



7. Now let’s try to enumerate all shared drivers on the target machine: Enum4linux –s {path to the brute force list} {Target IP}. Run the previous command and write down the outcome? Compare this outcome with the one on step 6.



8. Run the tool with (-a) option. Observe the output of the command and note down some interesting findings.

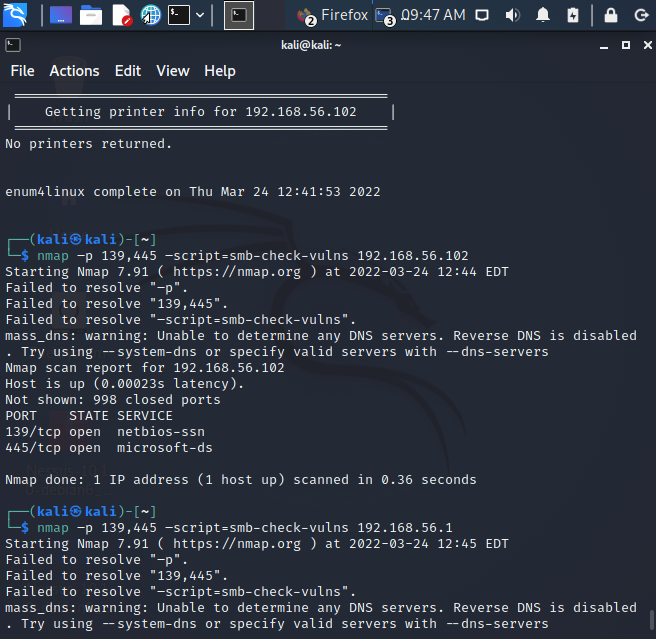
**Task 2:**

In this task, we will check if the target is vulnerable to any known SMB vulnerabilities, and then will collect information on this vulnerability.

1. One way to check for SMB vulnerabilities is using the nmap tool.

Type the following: Nmap –p 139,445 –script=smb-check-vulns {target IP address}

Make a note of the checked vulnerabilities:



2. Which of the checked vulnerabilities was your system vulnerable to? Search the web to get more information about this vulnerability