Challenge 3

Target: 10.5.5.14 (SMB Server)

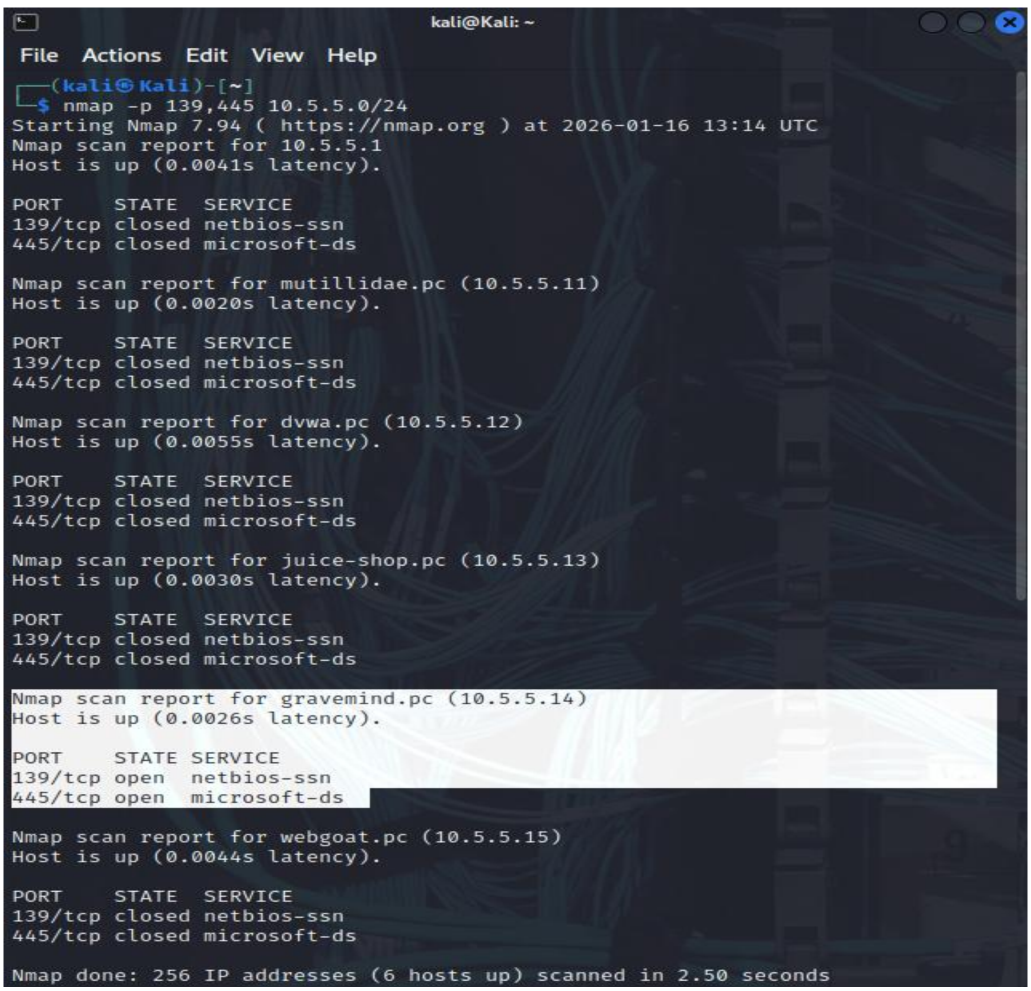
Vulnerability: Unsecured SMB Share (Anonymous Access)

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.

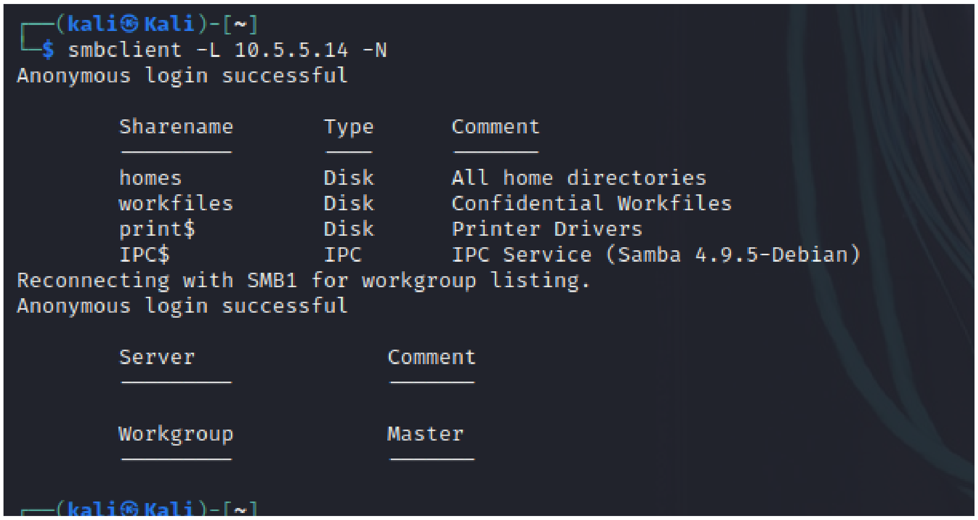
2. Reconnaissance & Target Identification

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.



Tools Used:

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



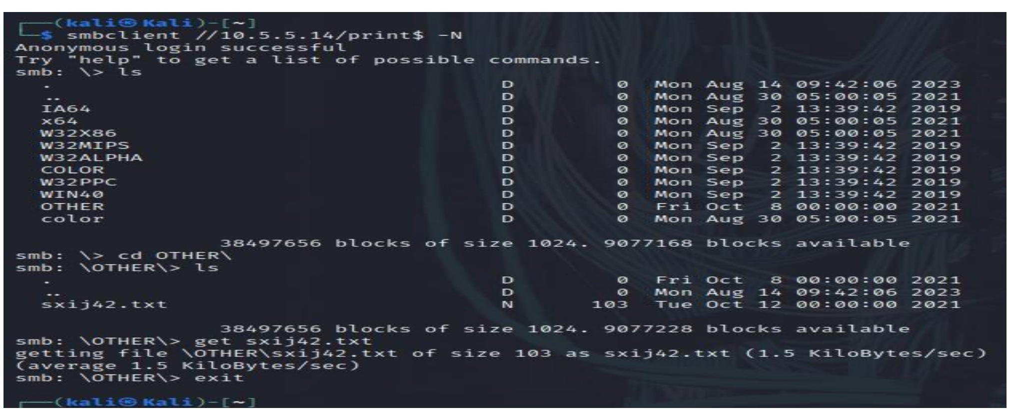
3. Exploitation (Share Enumeration)

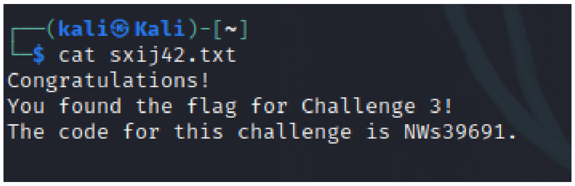
The server was found to allow "Null Sessions" (anonymous logins without a password). While several shares were listed, the **print$** share was found to contain sensitive files.

- **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.





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.