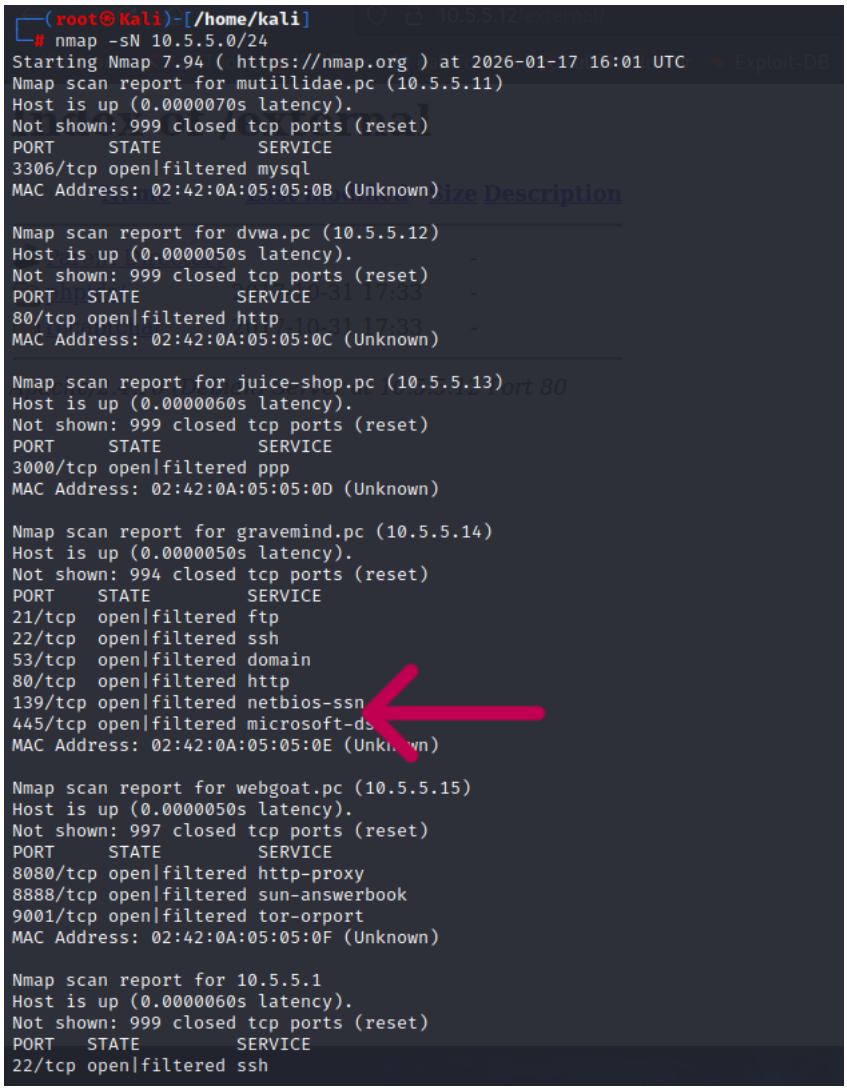
Challenge 3: Exploit open SMB Server Shares

In this part, I wanted to discover if there are any unsecured shared directories located on an SMB server in the 10.5.5.0/24 network. I can use any of the tools you learned in earlier labs to find the drive shares available on the servers.

Step 1: Scan for potential targets running SMB.

Used scanning tools to scan the 10.5.5.0/24 LAN for potential targets for SMB enumeration.
Command: nmap -p139,445 10.5.5.0/24



Which host on the 10.5.5.0/24 network has open ports indicating it is likely running SMB services?

Gravemind.pc (10.5.5.0/24)

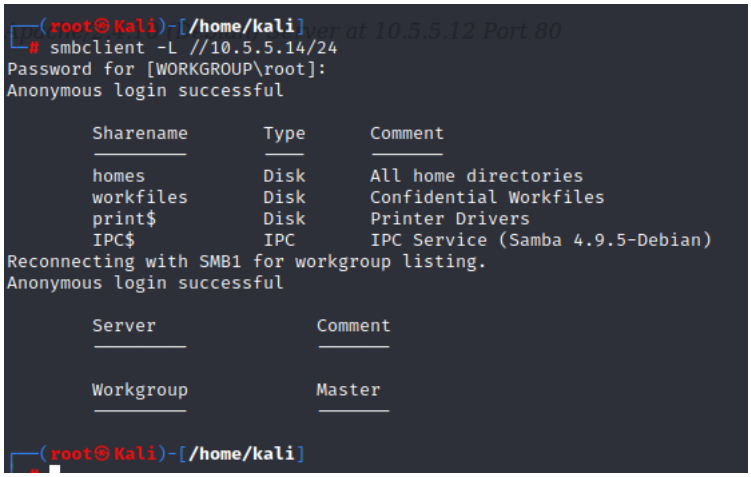
Ports opened 139 and 445

Services opened: netbios-ssn and microsoft-ds

Step 2: Determine which SMB directories are shared and can be accessed by anonymous users

Command: enum4linux -S 10.5.5.14

-S: This option get share list



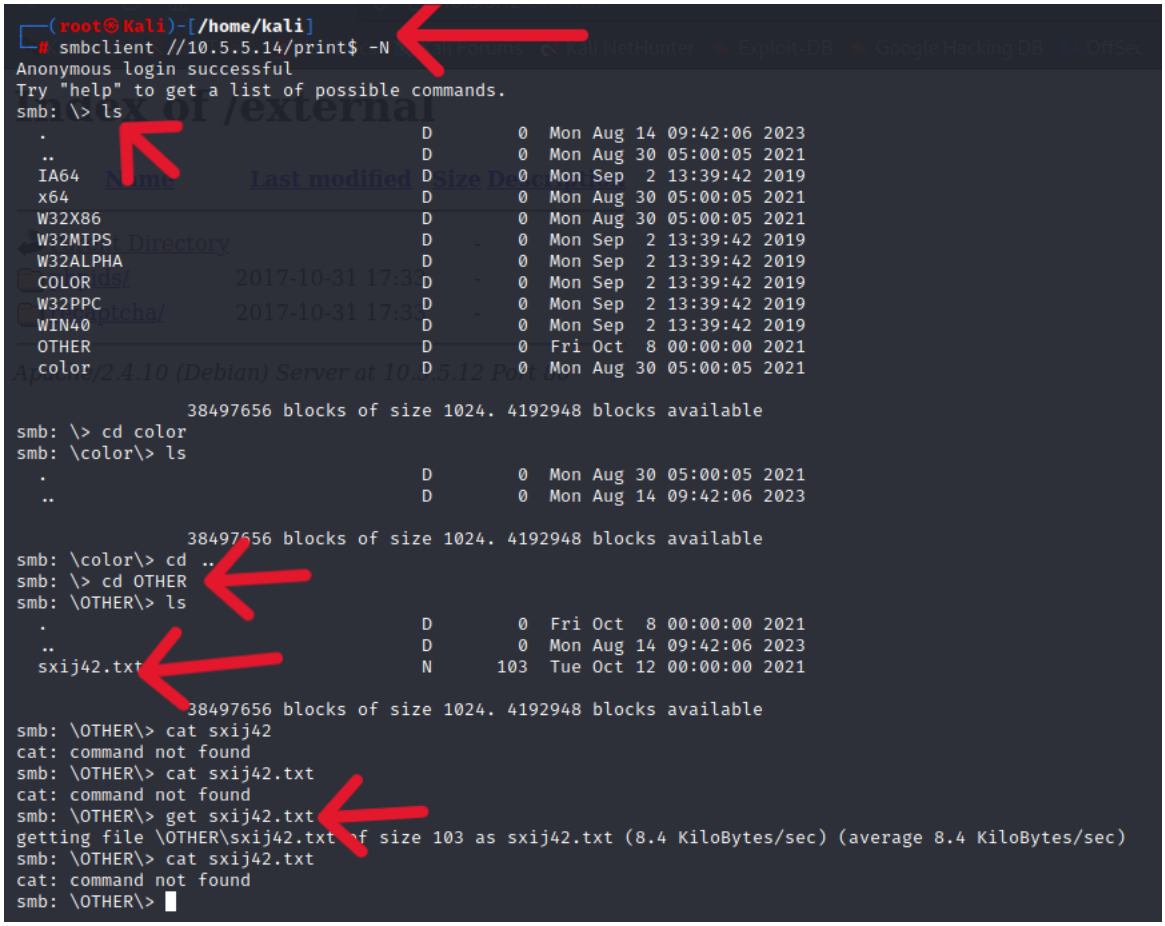
Step 3: Investigate each shared directory to find the file

Use the SMB-native client to access the drive shares on the SMB server. Use the dir, ls, cd, and other commands to find subdirectories and files.

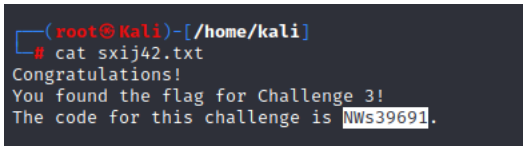
Command: smbclient -L //10.5.5.14 -N

-L: Get a list of shares available on a host

-N: Don't ask for a password



Locate the file with the Challenge 3 code. Download the file and open it locally.



Step 4: Research and propose SMB attack remediation.

What are two remediation methods for preventing SMB servers from being accessed?

Two key remediation methods for preventing unauthorized SMB server access are:

- Network segmentation and firewall rules to restrict access to trusted IPs/VLANs
- Disabling legacy SMB versions (SMBv1) and enforcing strong authentication (like Kerberos/NTLMv2 with MFA) to prevent exploits and interception.