# SMB Enumeration

**@mmar**

# What is SMB

**SMB (Server Message Block)** is a network protocol used for file sharing, printer sharing, and other communication between computers in a network. It is commonly associated with Microsoft Windows environments. SMB operates over TCP/IP and uses a range of ports for different purposes

# SMB Ports

✓ **TCP port 445:** This is the primary port used by SMB for file sharing and communication. It handles the majority of SMB traffic, including file access, printer sharing, and remote administration

✓ **UDP ports 137 and 138:** These ports are used by SMB for NetBIOS name resolution and datagram services, similar to NetBIOS

✓ **TCP port 139:** This port is used by older versions of SMB for session establishment and file sharing. It is commonly used in conjunction with NetBIOS over TCP/IP (NBT)

# Nmap

**The Swiss Army Knife**

# Nmap

❖ Nmap can be used to scan and enumerate the smb service and then we can use various tools to enumerate smb

>sudo nmap -A –p 445 192.168.18.110

>sudo nmap --script smb-os-discovery.nse 192.168.18.110

>nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 192.168.18.110

```
Host script results:
| smb-os-discovery:
|    OS: Unix (Samba 3.0.20-Debian)
|    Computer name: metasploitable
|    NetBIOS computer name:
|    Domain name: localdomain
```

# Nmap

❖ There are a number of scripts to enumerate smb. You can check more scripts by the following command

cd /usr/share/nmap/scripts; ls |  grep smb

# Enum4linux

## Most important Enumeration Tool

# Enum4linux

❖ Enum4linux is a tool used for network enumeration and information gathering. Enum4linux leverages various SMB and NetBIOS enumeration techniques to gather information about a target system

> >enum4linux -a 192.168.18.110

```
kali@kali: ~ ×    kali@kali: ~ ×
┌──(kali㉿kali)-[~]
└─$ enum4linux -a 192.168.18.110
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Jun 10 08:42:55 202
3

========================( Target Information )========================

Target .......... 192.168.18.110
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames ... administrator, guest, krbtgt, domain admins, root, bin, none
```

# Demo

# THANKS