SMB Enumeration Quick Reference

SMB Port Scanning

bash

```
# Basic SMB detection
nmap -p 139,445 target.com

# SMB OS discovery
nmap -p 139,445 --script smb-os-discovery target.com

# SMB share enumeration
nmap -p 445 --script smb-enum-shares target.com

# SMB user enumeration
nmap -p 445 --script smb-enum-users target.com
```

SMB Client Commands

bash

```
# List shares (anonymous)
smbclient -L //target.com -U ""

# Connect to share (anonymous)
smbclient //target.com/share -U ""

# Basic commands inside smbclient
ls              # List files
get filename    # Download file
put filename    # Upload file
cd directory    # Change directory
```

Enum4linux Tool

bash

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

# Just shares and users
enum4linux -S -U target.com

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

RPC Client (Null Sessions)

```bash
# Connect anonymously
rpcclient -U "" target.com

# Inside rpcclient shell:
querydispinfo        # List user accounts
enumdomusers         # Domain users
getdompwinfo         # Password policy
lsaquery             # Security policy info
```

Common SMB Ports

- **Port 139:** NetBIOS Session Service
- **Port 445:** SMB over TCP (modern)

Key Things to Check

- Anonymous/guest access enabled
- Writable shares
- Sensitive files in shares
- Null session authentication
- Weak password policies
- User account enumeration