SMB Enumeration: enum4linux & crackmapexec

Using enum4linux

enum4linux is a tool used for enumerating information from Windows machines via SMB (Server Message Block). It's particularly useful in penetration testing to gather details like users, groups, shares, OS info, and more.

Basic Syntax:
  enum4linux [options] <IP address>
Example:
  enum4linux 192.168.1.100

Commonly Used Options:
- -a: Run all enumeration options (recommended for initial scans).
- -U: Get list of users.
- -S: Get list of shares.
- -G: Get list of groups.
- -P: Enumerate passwords policy.
- -o: OS information.
- -d: Get domain SID.
- -i: Get printer info.

Run Full Enumeration:
  enum4linux -a 192.168.1.100

User and Share Enumeration Only:
  enum4linux -U -S 192.168.1.100

With Credentials (if needed):
  enum4linux -u <username> -p <password> 192.168.1.100

Save Output to a File:
  enum4linux -a 192.168.1.100 > enum_results.txt

Install enum4linux:
  git clone https://github.com/CiscoCXSecurity/enum4linux.git
  cd enum4linux
  chmod +x enum4linux.pl
  ./enum4linux.pl -a <IP>

Pro Tip:
- Combine with smbclient or smbmap for further interaction.
- Try smbclient -L //<IP> -N to list shares anonymously.

Does it only work on Windows machines?

Short Answer: enum4linux is designed specifically for enumerating SMB services — so while it's mainly used against Windows machines, it can also work on Linux/Unix systems that run Samba, which is the Linux implementation of SMB.

It works on:
- Windows machines (XP, 7, 10, 11, Server versions)
- Linux/Unix machines running Samba

What Can Be Enumerated on Samba?
- Usernames
- Shared folders
- Password policies
- OS and domain info
- Group memberships (if configured)

Using crackmapexec

crackmapexec (CME) is like the Swiss army knife for SMB/Active Directory enumeration and exploitation. It's more advanced and flexible than enum4linux, and supports multiple protocols (SMB, WinRM, RDP, etc.).

Basic Syntax:
```
crackmapexec smb <target_ip_or_range> [options]
```

Examples:
1. Check SMB Info:
```
crackmapexec smb 192.168.1.100
```
2. Test Credentials:
```
crackmapexec smb 192.168.1.100 -u admin -p password123
```
3. Enumerate Shares:
```
crackmapexec smb 192.168.1.100 -u guest -p '' --shares
```
4. Enumerate Users:
```
crackmapexec smb 192.168.1.100 -u admin -p password123 --users
```
5. Password Policy:
```
crackmapexec smb 192.168.1.100 -u admin -p password123 --pass-pol
```
6. Remote Command Execution:
```
crackmapexec smb 192.168.1.100 -u admin -p password123 -x "ipconfig /all"
```
7. Password Spray:
```
crackmapexec smb 192.168.1.100 -u users.txt -p "Summer2020"
```

Install via pipx (Recommended):

```
sudo apt update && sudo apt install pipx -y
pipx ensurepath
pipx install crackmapexec
```

Install From Source:

```
sudo apt install git python3-pip python3-venv build-essential libssl-dev libffi-dev python3-dev -y
git clone https://github.com/Porchetta-Industries/CrackMapExec
cd CrackMapExec
python3 -m venv cme-venv
source cme-venv/bin/activate
pip install --upgrade pip
pip install -r requirements.txt
python setup.py install
```

TryHackMe Rooms for Practice

Beginner-Friendly:

1. Blue – EternalBlue + SMB enumeration
2. Ignite – SMB and file upload vulnerability

Intermediate:

3. Network Services – SMB + FTP + other services
4. Attacktive Directory – Active Directory enumeration
5. Overpass 2 - Hacked – Advanced enumeration + persistence

Advanced / Red Team:

6. Wreath – Red team post-exploitation path
7. SUDOv3 – Privilege escalation, enumeration

Bonus Practice Labs:

8. Simple CTF – Linux SMB enumeration
9. Relevant – SMBv1, EternalBlue, and reverse shells