SMB Enumeration

Server Message Block (SMB) is a network protocol used for sharing files, printers, and other resources between computers on a local network. While SMB provides convenient file sharing capabilities, improper configuration or the use of older, insecure versions can leave systems vulnerable to enumeration and exploitation.

SMB Enumeration with nmap

To perform SMB Enumeration, we can take help of our good old friend nmap. We will specify the -sV flag and -sC for the default scripts to divulge as much information as we can.

```
sudo nmap -p 445 -sV -sC 192.168.29.141
```

We can also use nmap scripts to enumerated SMB shares, usernames and protocol version using specified scripts. Lets see each one of them.

```
sudo nmap -p 445 --script smb-enum-shares 192.168.29.141

sudo nmap -p 445 --script smb-enum-users 192.168.29.141

sudo nmap -p 445 --script smb-protocols 192.168.29.141
```

Version Detection and Enumerating shares with Metasploit

We can also use metasploit smb_version auxilariy module to enumerate version of the SMB server running. This can later help us to find potential vulnerabilities related to it.

```
use auxiliary/scanner/smb/smb_version
set RHOSTS <TARGET>
run
```

We can also enumerate available SMB share with it. For that, we have to use smb_enumshare auxiliary module.

```
use auxiliary/scanner/smb/smb_enumshares
set RHOSTS <Target>
set ShowFiles true
run
```

Enumeration with smbclient

Now we will see how we can enumerate SMB using smbclient, this is hands down my favourite and go to tool to perform SMB enumeration.

First to list SMB shares, we just have to provide the target IP with -L flag.

```
smbclient -L IP
```

Now that we have the shares listed. Lets access them. For that, we will do

```
smbclient //IP/TargetShare
```

If we have credentials of a valid user we can also pass it to smbclient.

```
smbclient //IP/TargetShare -U user --password=password
```

Enumerating with Smbmap

Another tool, alternative to smbclient is SMBmap. It also takes IP address as input with -H flag.

```
smbmap -H IP
```

One cool thing about this tool is that it also list out the permissions we have on particular shares.

We can also check the subfolders inside our target share recursively using smbmap.

```
smbmap -R C$ -H <IP>
```

Next, we have user and password of a user, we can also pass it to the smbmap.

```
smbmap -H <target IP> -u username -p password
```

We can also download a file on our system using the download option in smbmap.

```
smbmap -R tmp -H 10.10.10.3 --download 'tmp\vgauthsvclog.txt.0'
```

Identifying OS with crackmapexec

We can use SMB to find out the exact model and version of the Target OS. For that, we will use crackmapexec. Crackmapexec is a great tool which is primarily focused on Windows Active Directory post exploitation, this is also one of the few tools that i love the most.

So, we will use crackmapexec on the target to find out its underlying OS version. This will help us to tailor specific attack vector for the target later.

```
crackampexec smb IP --shares
```

Using Enum4linux for SMB enumeration

At last, we have another tool for performing SMB and Samba enumeration and that is enum4linux.

```
python3 enum4linux-ng.py -A IP
```

So, whatever we have done till now manually. Enum4linux just automates the whole process making it easier and faster for us to enumerate.

Apart from that, there is a possibility of bruteforce attacks using hydra and metasploit to get the password of an SMB user. But we keep bruteforce as the last resort, even in exploitation also as it creates a lot of noise and successful results are not guaranteed every time.
