

SMB Exploitation

@mmar



SMB - Server Message Block Protocol - is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network

Scanning

- ❖ Nmap can be used for scanning the SMB port

```
Nmap -sS -T4 10.10.50.26
```

```
(root@kali)-[~]
└─# sudo nmap -sS -T4 --script vuln 10.10.50.26
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-09 14:23 UTC
Nmap scan report for ip-10-10-50-26.eu-west-1.compute.internal (10.10.50.26)
Host is up (0.0053s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 02:52:2A:2A:61:4F (Unknown)
```

Enumeration

- ❖ Enum4linux is a tool used to enumerate SMB shares on both Windows and Linux systems. It is basically a wrapper around the tools in the Samba package and makes it easy to quickly extract information from the target pertaining to SMB. It's installed by default on Parrot and Kali

```
enum4linux -a 10.10.50.26
```

```
(root@kali)-[~]
└─# enum4linux -a 10.10.50.26
Starting enum4linux v0.9.1 ( http://labs.p0tcullis.co.uk/application/enum4linux/ ) on

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

Target ..... 10.10.50.26
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

Enumeration

- ❖ Nmap also has a script that can be used to enumerate SMB

```
sudo nmap --script smb-os-discovery.nse 10.10.50.26
```

```
(root@kali)-[~]
└─# sudo nmap --script smb-os-discovery.nse 10.10.150.159
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-09 14:46 UTC
Nmap scan report for ip-10-10-150-159.eu-west-1.compute.internal (10.10.150.159)
Host is up (0.011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 02:BA:93:4A:82:25 (Unknown)

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: polosmb
|   NetBIOS computer name: POLOSMB\x00
```

Exploitation

- ❖ Smbclient can be used to access shares

Smbclient -L (to list all shares)

Smbclient //10.10.50.26/share (access it)

```
(root@kali)-[~]
└─# smbclient //10.10.50.26/profiles
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Tue Apr 21 11:08:23 2020
..               D           0   Tue Apr 21 10:49:56 2020
.cache           DH          0   Tue Apr 21 11:08:23 2020
.profile         H           807 Tue Apr 21 11:08:23 2020
.sudo_as_admin_successful H          0   Tue Apr 21 11:08:23 2020
.bash_logout    H           220 Tue Apr 21 11:08:23 2020
.viminfo        H           947 Tue Apr 21 11:08:23 2020
Working From Home Information.txt N          358 Tue Apr 21 11:08:23 2020
.ssh             DH          0   Tue Apr 21 11:08:23 2020
.bashrc         H          3771 Tue Apr 21 11:08:23 2020
```

DEMO



THANKS