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

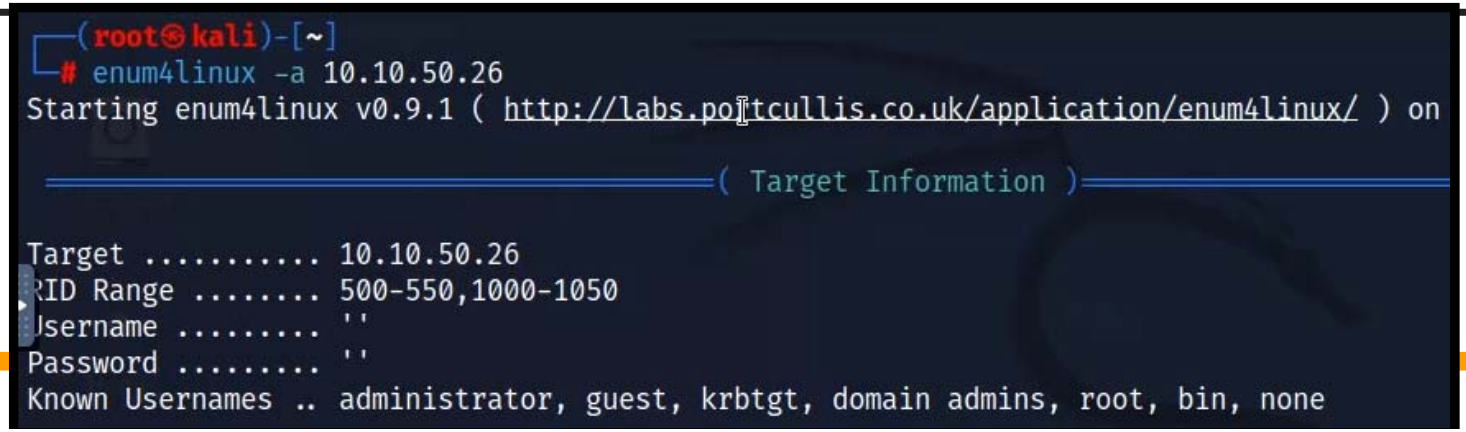
Nmap -sS -T4 10.10.50.26

```
┌──(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
```



Enumeration

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

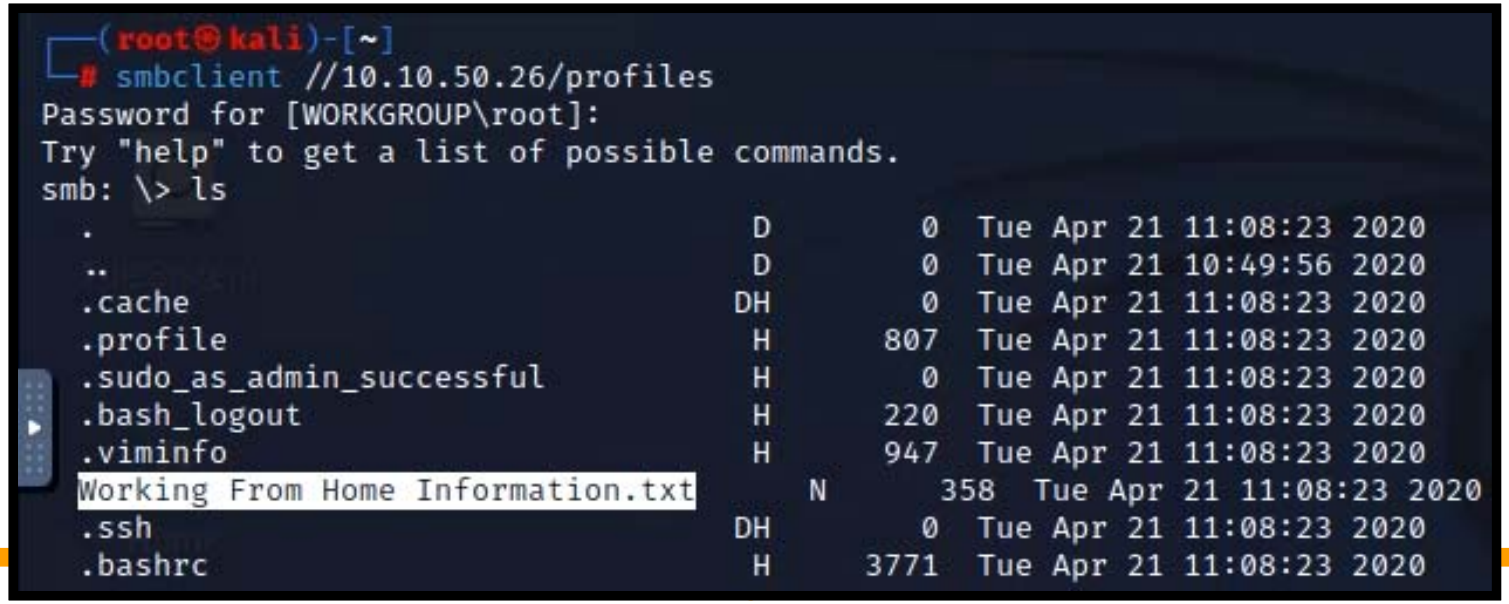
```
sudo nmap --script smb-os-discovery.nse 10.10.50.26
```

Exploitation

- Smbclient can be used to access shares

Smbclient -L (to list all shares)

Smbclient //10.10.50.26/share (access it)



DEMO

THANKS