Incomplete Lab - Scanning for SMB Vulnerabilities with enum4linux

Objectives

Enum4linux is a tool for enumerating information from Windows and Samba. Samba is an application that enables Linux and Apple clients to participate in Windows networks. It enables non-Windows clients to utilize the Server Message Block (SMB) protocol to access file and print services. Samba servers can participate in a Windows domain, both as a client and a server.

In this lab, you will complete the following objectives:

- Launch enum4linux and explore its capabilities.
- Identify computers with SMB services running.
- Use enum4linux to enumerate users and network file shares.
- Use smbclient to transfer files between systems.

Background / Scenario

Poorly secured and managed Windows server networks are a huge security risk. Penetration testers must uncover any vulnerabilities in file and print sharing functions that can leave an organization vulnerable to attack. In this activity, you will explore the capabilities of the enum4linux tool to enumerate user and file sharing information from Samba servers. Finally, you will use the smbclient utility to transfer files between systems.

Required Resources

- Kali VM customized for the Ethical Hacker course

Instructions

Part 1: Launch enum4linux and explore its capabilities.

Step 1: Verify that enum4linux is installed and view the help file.

a. Load Kali Linux using the username **kali** and the password **kali**. Open a terminal session from the menu bar at the top of the screen.
b. Most enum4linux commands must be run as root, so use the **sudo su** command to obtain persistent root access.

   At the prompt, enter the command to view the enum4linux help file.

```
┌──(kali㉿kali)-[~]

└─$ sudo su

[sudo] password for kali:
```

```
┌──(root㉿kali)-[/home/kali]
└─# enum4linux -help
```

The help file contains the syntax and options available to enumerate host and server information on networks that use SMB. Enum4linux requires that Samba be installed on the host system, in this case the Kali Linux computer, because it is dependent on the built-in Samba utilities.

Which Samba utilities does the help file indicate are used by the enum4linux tool?

Answer Area

<!----><!---->

Step 2: Research terms associated with SMB functions.

Many terms used in Windows and SMB functions may not be familiar to you, so the output of the enum4linux commands may be difficult to interpret at first. Use an internet search engine to find the definition of the terms listed.

Relative Identifier (RID)

Answer Area

<!----><!---->

Security Identifier (SID)

Answer Area

<!----><!---->

Domain Controller (DC)

Answer Area

<!----><!---->

Lightweight Directory Access Protocol (LDAP)

Answer Area

<!----><!---->

Workgroup

Answer Area

<!----><!---->

Part 2: Use Nmap to Find SMB Servers.

Step 1: Scan the virtual networks to find potential targets.

One way to identify potential targets for SMB enumeration is to examine the open ports. In an earlier lab, you used Nmap to find and enumerate open ports on target systems. Common open ports on SMB servers are:

TCP 135	RPC
TCP 139	NetBIOS Session
TCP 389	LDAP Server
TCP 445	SMB File Service
TCP 9389	Active Directory Web Services
TCP/UDP 137	NetBIOS Name Service
UDP 138	NetBIOS Datagram

a. Two virtual networks are included in the Kali VM with Docker containers. Use the **nmap -sN** command to find the services available on hosts in the 172.17.0.0 virtual network.

Note: **sudo** is not required if you executed the **sudo su** command above.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sN 172.17.0.0/24
```

What does Nmap reveal about hosts on the 172.17.0.0/24 network?

Answer Area

<!----><!---->

What ports are open on the host that identify running SMB services? What does Nmap call these services?

Answer Area

<!----><!---->

b. Conduct a **nmap -sN** scan on the **10.6.6.0/24** subnet.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sN 10.6.6.0/24
```

Are there any potential target computers on this subnet running SMB services? Which computer or computers? How do you know?

Answer Area

```
<!----><!---->
```

Part 3: Use enum4linux to enumerate users and network file shares.

In this part, you will use enum4linux to discover more information about the two potential targets.

Step 1: Perform an enum4linux scan on target 172.17.0.2.

In Part 1, Step 1c, you used the enum4linux help page to learn about the options available to enumerate potential targets. The most common options are:

-U find configured users

-S get a list of file shares

-G get a list of the groups and their members

-P list the password policies

-i get a list of printers

a. Use the **enum4linux -U** option to list the users configured on the target 172.17.0.2. Remember that enum4linux commands require root permissions to execute.

```
┌──(root㉿kali)-[/home/kali]

└─# enum4linux -U 172.17.0.2
```

The output of this command can generate multiple screens of information if many users are discovered. Enum4linux aggregates output from multiple Samba tools to produce a concise result. If you want to see how each feature is used, use the verbose option (**-v**) with the command.

b. List the file shares available on 172.17.0.2 using the **enum4linux -S** command. Use the verbose option to see the Samba tools that are used to obtain the information.

```
┌──(root㉿kali)-[/home/kali]

└─# enum4linux -Sv 172.17.0.2
```

Note the **[V]** at the beginning of some of the lines of output. The verbose mode provides a narrative of how the results were obtained. For example, in the **Enumerating Workgroup/Domain** section of the output, enum4linux attempted to get the domain name using the command: **nmblookup -A ‘172.17.0.2’**.

Which Samba tool was used to map the file shares?

Answer Area

```
<!----><!---->
```

How many file shares are listed for target 172.17.0.2? What does the $ indicate at the end of the share name? (You may need to research this answer.)

Answer Area

```
<!----><!---->
```

c. Penetration testers may not have uncovered a known username/password combination to further their exploit. In this case, they need to do a brute-force password attack to obtain the necessary credentials. It is a benefit to know the password policies in place on the target system to structure the brute-force effort. Use the **enum4linux -P** command to list the password policies.

```
┌──(root㉿kali)-[/home/kali]
└─# enum4linux -P 172.17.0.2
```

What is the minimum password length set for accounts on this server? What is the account lockout threshold setting?

Answer Area

```
<!----><!---->
```

How would rate the security of the password policy set for this domain? Low, medium, or high? Explain.

Answer Area

```
<!----><!---->
```

Step 2: Perform a simple enumeration scan on target 10.6.6.23.

Enum4linux has an option that combines the -U, -S, -G, -P, -r, -o, -n, -i options into one command. This requires using the **-a** argument. This option quickly performs multiple SMB enumeration operations in one scan.

Use the **enum4linux -a** command to perform a scan on the potential Samba server target that you identified in Part 2.

```
┌──(root㉿kali)-[/home/kali]
└─# enum4linux -a 10.6.6.23
```

This command can produce multiple screens of output.

How many local users and groups are there on target 10.6.6.23?

Answer Area

```
<!----><!---->
```

What are the shares that are located on this target?

Answer Area

```
<!----><!---->
```

Part 4: Use smbclient to transfer files between systems.

Smbclient is a component of Samba that can store and retrieve files, similar to an FTP client. You will use smbclient to transfer a file to the target system at 172.17.0.2. This simulates exploiting a network host with malware through an SMB vulnerability.

a. Create a text file using the **cat** command. Name the file **badfile.txt**. Enter the desired text. In this example, **This is a bad file.** was used. Be sure that you know the path to the file. Press **CTRL-C** to when finished.

```
┌──(root㉿kali)-[/home/kali]

└─# cat >> badfile.txt

This is a bad file.

Press CRTL-C to write the file.
```

b. Take a look at the options available with smbclient using the command **smbclient –help** command.

```
┌──(root㉿kali)-[/home/kali]

└─# smbclient --help
```

c. Use the **smbclient -L** command to list the shares on the target host. This command produces a similar output to what the enum4linx command did in Part 3. When asked for a password, press enter. The double / character before the IP address and the / following it are necessary if the target is a Windows computer.

```
┌──(root㉿kali)-[/home/kali]

└─# smbclient -L //172.17.0.2/

Password for [WORKGROUPkali]: <Press enter>
```

d. Connect to the **tmp** share using the **smbclient** command by specifying the share name and IP address.

```
┌──(root㉿kali)-[/home/kali]

└─# smbclient //172.17.0.2/tmp

Password for [WORKGROUPkali]: <Press enter>

smb: >
```

Note that the prompt changed to the **smb:>** prompt. Type **help** to see what commands are available.

e. Enter **dir** to view the contents of the share.

f. Upload the **badfile**.**txt** to the target server using the **put** command. The syntax for the command is:

```
 put local-file-name remote-file-name
```

```
smb: > put badfile.txt badfile.txt

Putting file badfile.txt as badfile.txt (19.5 kb/s) (average 19.5 kb/s)
```

g. Verify that the file successfully uploaded using the **dir** command.

```
smb: > dir
```

h. Type **quit** to exit the **smbclient** and return to the CLI prompt.

Reflection

You are conducting a penetration test of a client network. You have gained access to an internal network by social engineering the username and password of an ad hoc webserver that is not behind the firewall. You can remotely access the network from a Kali VM configured with the enum4linux tool.

What steps would you follow to send a dummy malware file to hosts on the network as part of the penetration test?

Answer Area

```
<!----><!---->
```