Explore the Social Engineer Toolkit (SET)

Objectives

Many exploits begin with a social engineering attack that is designed to obtain credentials or plant malware to create entry points into the target network. One of the tools used to perform these social engineering attacks is the Social Engineer Toolkit (SET), developed by David Kennedy.

- Launching SET and exploring the toolkit
- Cloning a website to obtain user credentials
- Capturing and viewing user credentials

Cloning a website and obtaining user credentials.

This activity is performed under carefully controlled conditions within a virtual environment. SET tools should only be used for penetration testing in situations where you have written permission to perform social engineering exploits.

In an actual penetration test, this procedure could be used to reveal problems with user security training and the need take measures to educate users about various types of phishing attacks.

Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

Instructions

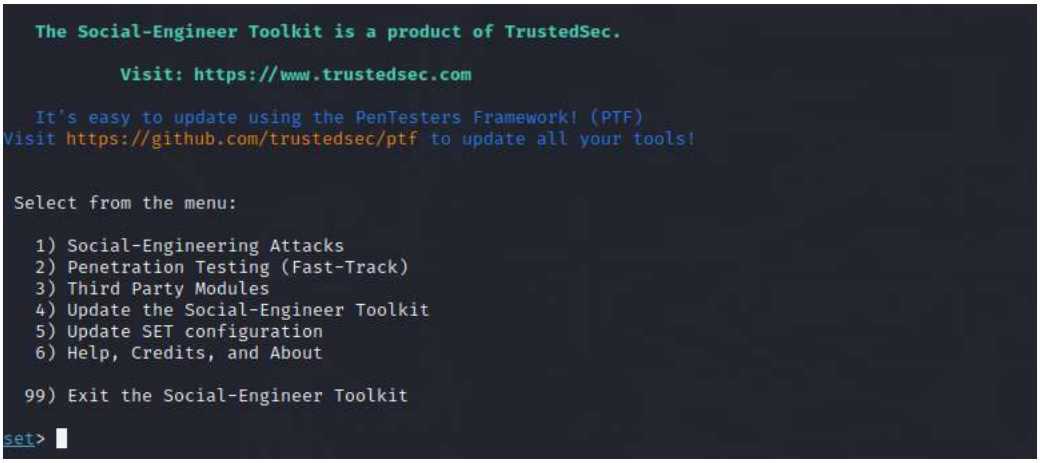
Part 1: Launching SET and Exploring the Toolkit

Step 1: Load the SET application.

a. Start 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. SET must be run as root. Use the **sudo -i** command to obtain persistent root access. At the prompt, enter the command **setoolkit** to load the SET menu system. The Social Engineering Toolkit can also be run from the **Applications >Social Engineering Tools >social engineering toolkit (root)** choice on the Kali menu.

```
sudo -i
[sudo] password for kali:
```

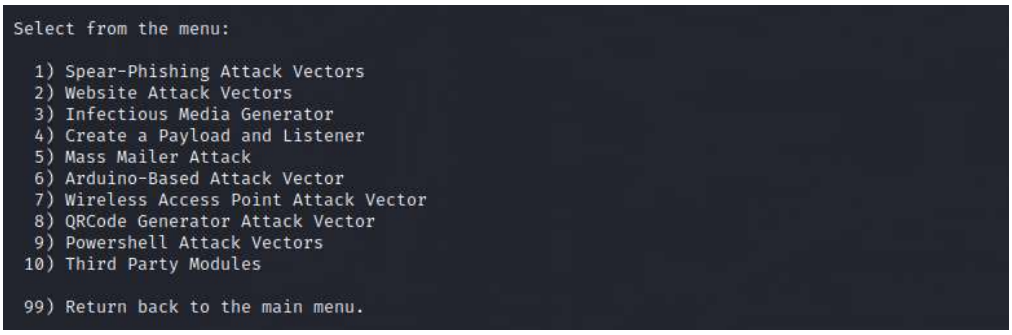
The initial SET menu is displayed, as shown:



Step 2: Examine the Available Social-Engineering Attacks.

a. At the SET prompt, enter **1** and press **Enter** to access the Social-Engineering Attacks submenu.

set> **1**
Select from the menu:



b. Select each option to see a brief description of each exploit and what the tool does for each.

Note: Some options may not have a choice. In that case, use **CTRL-C** or enter **99** to return to the main menu.

Part 2: Cloning a website to Obtain User Credentials

In this part of the lab, you will create a perfect copy of the login page for a website. The fake login page will gather all credentials submitted to it and then redirect the user to the real website.

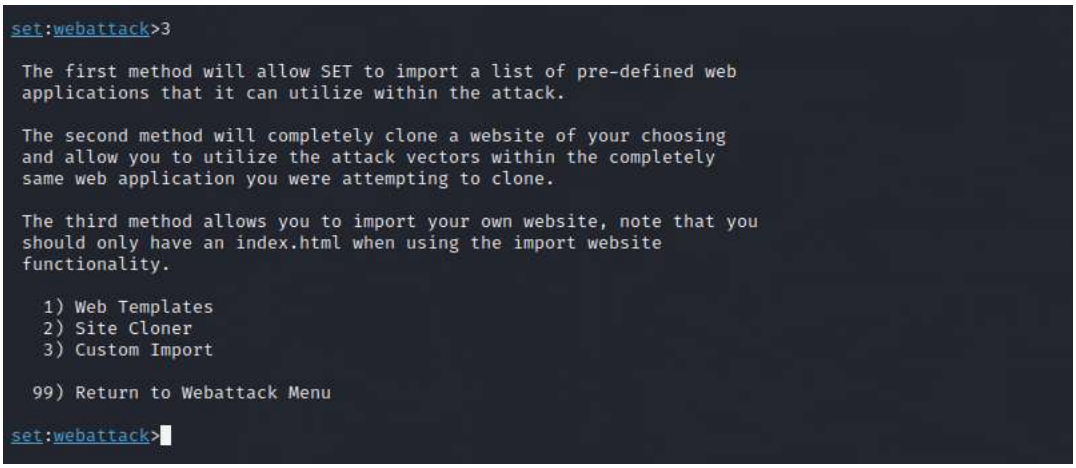
Step 1: Investigate Web Attack Vectors in SET.

a. From the Social-Engineering Attacks submenu, choose **2) Website Attack Vectors** to begin the website cloning exploit.

set> **2**

b. Review the brief attack description of each type of attack.

c. Select **3) Credential Harvester Attack Method** from the menu. A description of the ways to configure this exploit is displayed.



Step 2: Clone the DVWA.vm Login Screen.

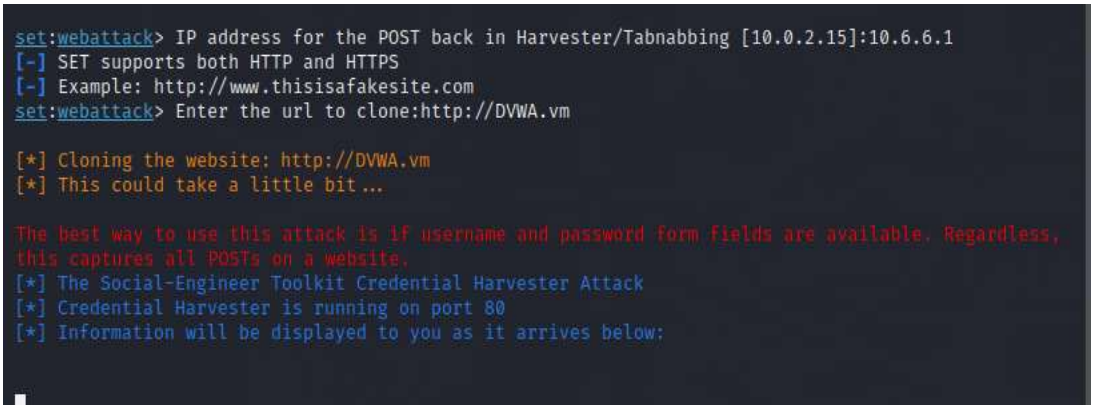
In this step, you will create a cloned website that duplicates the DVWA.vm login website. The SET application creates a website hosted on your Kali Linux computer. When the target users

enter their credentials in the cloned website, the credentials and the users will be redirected to the real website without being aware of the exploit. This is similar to an on-path attack.

a. In this lab, we are using the internal website hosted on the DVWA.vm virtual machine. To see what the website looks like, open the Kali Firefox browser, and enter the URL **http://DVWA.vm/**. The login screen will appear. If the URL is not found, enter http://10.6.6.13/ to access the web server using its IP address.
b. Return to the terminal session. Select **2) Site Cloner** from the **Credential Harvester Attack Method** menu. Information describing which IP address is needed to host the fake website and to receive the POST data is displayed. Enter the web attacker IP address at the prompt. This is the IP address of the virtual Kali internal interface on the 10.6.6.0/24 network. In an actual exploit, this would be the external (internet facing) address of the attack computer.

b. At the prompt, enter the IP address **10.6.6.1**.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:**10.6.6.1**



e. When the website is cloned, the following message appears on the terminal.

Note: No prompt will be returned to you. This is because a listener is now active on port 80 on the Kali computer and all port 80 traffic will be redirected to this screen. Do not close the terminal window. Continue to Part 3.

Part 3: Capturing and Viewing User Credentials

Step 1: Create the Social Engineering Exploit.

In a "real-life" exploit, at this point, a phishing exploit containing a link or QR code that sends the user to the fake website is created and sent. In this lab, an html document is created to direct the user to the fake webpage. This document simulates a distributed phishing URL. It could be distributed as a file attachment in phishing emails.

a. Open the Kali Linux Mousepad text editor using the **Applications > Favorites > Text Editor** choice from the menu. Enter the HTML code shown into the Mousepad document.

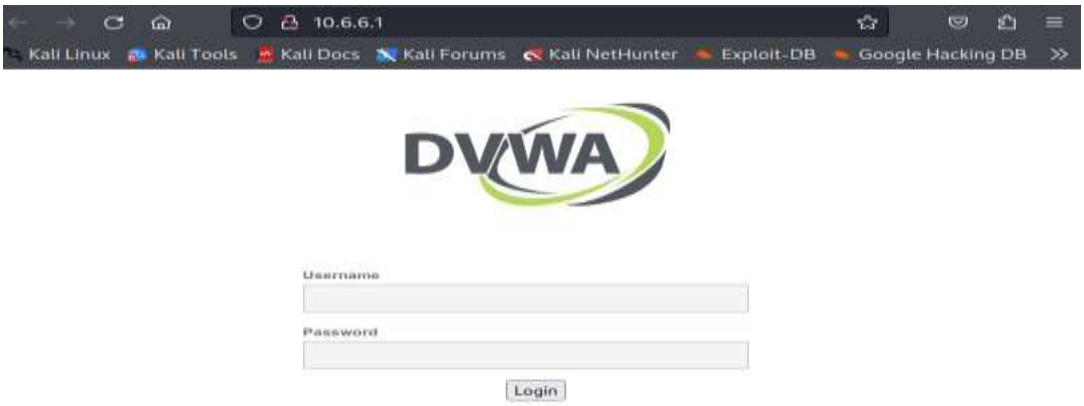
```
<html>
<head>
<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
</head>
</html>
```

b. Select **File > Save** from the Mousepad menu. Name the document **Great_link.html** and save it in the **/home/kali/Desktop** Folder. The icon appears on the Kali desktop.
c. Close the Mousepad application.

Step 2: Capture User Credentials.

The purpose of the cloned website is to present a web page that looks identical to the one that the user is expecting. A good hacker would create a fake URL that would be very similar to the actual URL, so that unless the user inspects the URL very closely, it would go unnoticed.

a. Double-click the desktop icon for the **Great_link.html** page. The DVWA login page that you viewed in **Part 2, Step 2a** should appear in a browser window.



b. Enter some information in the Username and Password fields and click **Login** to send the form.

Username: **some.user@gmail.com**
Password: **Pa55w0rdd!**

Step 3: View the Captured Information.

a. Return to the terminal session that is running the SET application. Output from the login attempt should appear as shown below:

Scanning for SMB Vulnerabilities with enum4linux

In the world of ethical hacking and penetration testing, understanding the vulnerabilities of SMB (Server Message Block) services is crucial. SMB is a protocol that enables file and print sharing between systems, primarily on Windows networks. In this lab, we will use the enum4linux tool, a powerful SMB enumeration tool, to discover information about SMB services on target systems. This information can be vital for identifying potential vulnerabilities and strengthening network security. Let's walk through the objectives step by step.

Part 1: Launch enum4linux and Explore Its Capabilities

Step 1: Verify enum4linux Installation and View the Help File

1. **Access Kali Linux**: First, log in to your Kali Linux virtual machine using the username **kali** and the password **kali**. Open a terminal session.

2. **Gain Root Access**: Most enum4linux commands require root privileges. To obtain persistent root access, use the **sudo su** command.

```
┌──(kali㉿Kali)-[~]
└─$sudo su
```

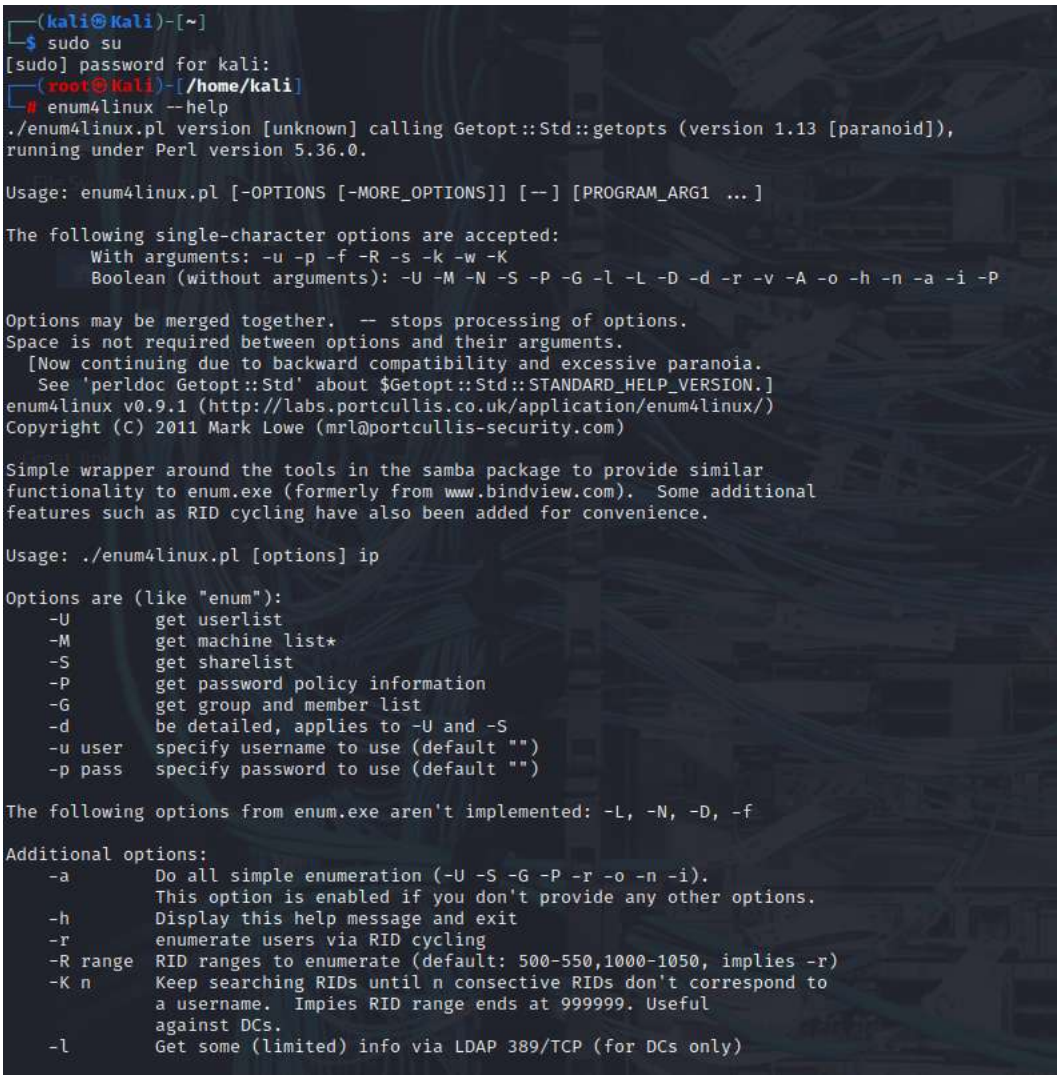
3. View Help File: To understand enum4linux's capabilities and syntax, access the help file using the **enum4linux --help** command.

```
┌──(root㉿Kali)-[~]
└─# enum4linux --help
```

The help file contains valuable information about the available options and the dependencies on Samba utilities.

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

The Samba utilities used by enum4linux are rpcclient, net, nmblookup, and smbclient.



Step 2: Research Terms Associated with SMB Functions

Understanding SMB-related terms is essential for interpreting enum4linux output effectively. Here are some terms and their definitions:

- **Relative Identifier (RID)**: Uniquely identifies a user, group, system, or domain.
- **Security Identifier (SID)**: Uniquely identifies users and groups within the local domain and can work globally between domains.
- **Domain Controller (DC)**: Manages network and identity security requests, authenticates users, and controls access to IT resources.
- **Lightweight Directory Access Protocol (LDAP)**: A directory access protocol enabling communication for services and clients using LDAP naming services.
- **Workgroup**: A group of standalone computers administered independently.

Part 2: Use Nmap to Find SMB Servers

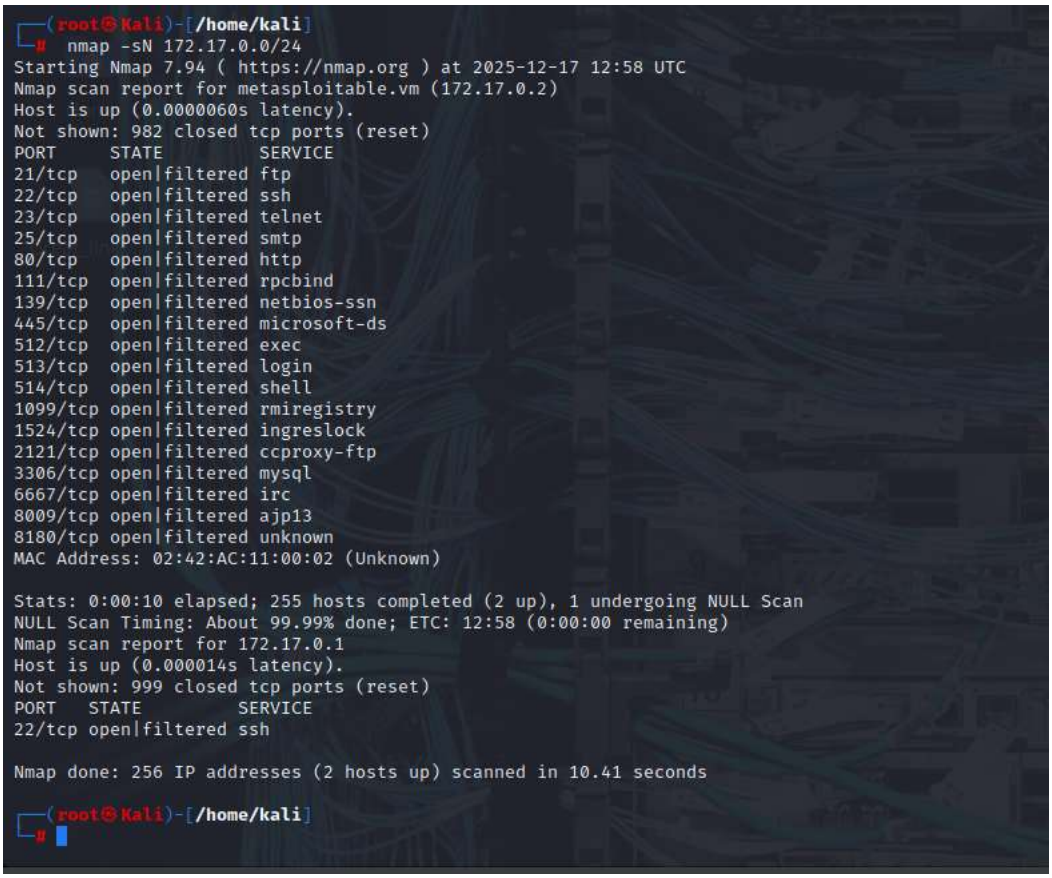
Step 1: Scan Virtual Networks to Find Potential Targets

Identifying potential SMB targets involves scanning open ports. Common ports associated with SMB services include:

- 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

1. **Scan 172.17.0.0 Virtual Network**: Use the `nmap -sN` command to find services on hosts in the 172.17.0.0 virtual network.



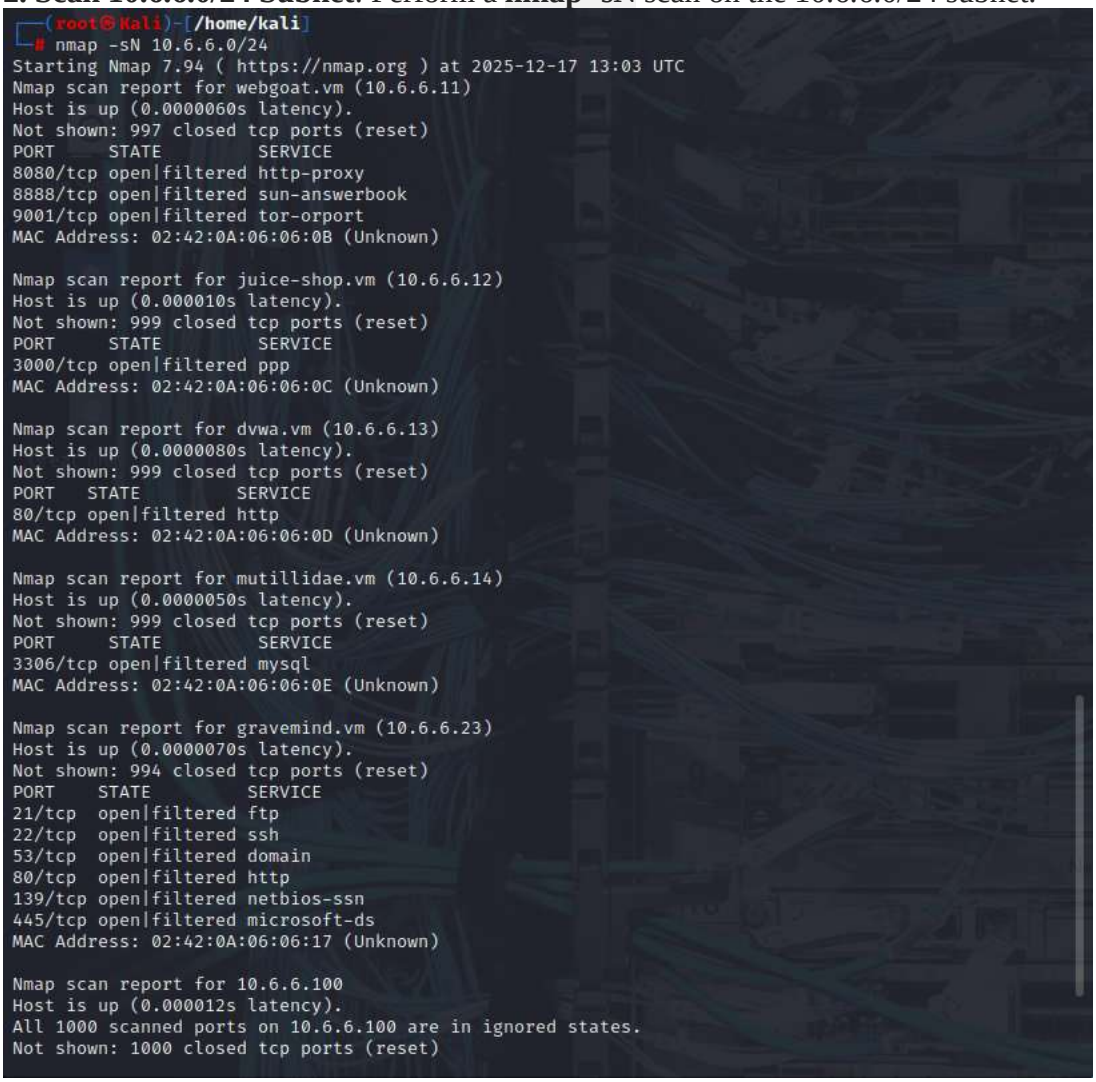
What does Nmap reveal about hosts on the 172.17.0.0/24 network?

Only one host is present, identified as 172.17.0.2.

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

The open ports on the host 172.17.0.2 are TCP 139 (netbios-ssn) and TCP 445 (microsoft-ds).

2. Scan 10.6.6.0/24 Subnet: Perform a **nmap -sN** scan on the 10.6.6.0/24 subnet.



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

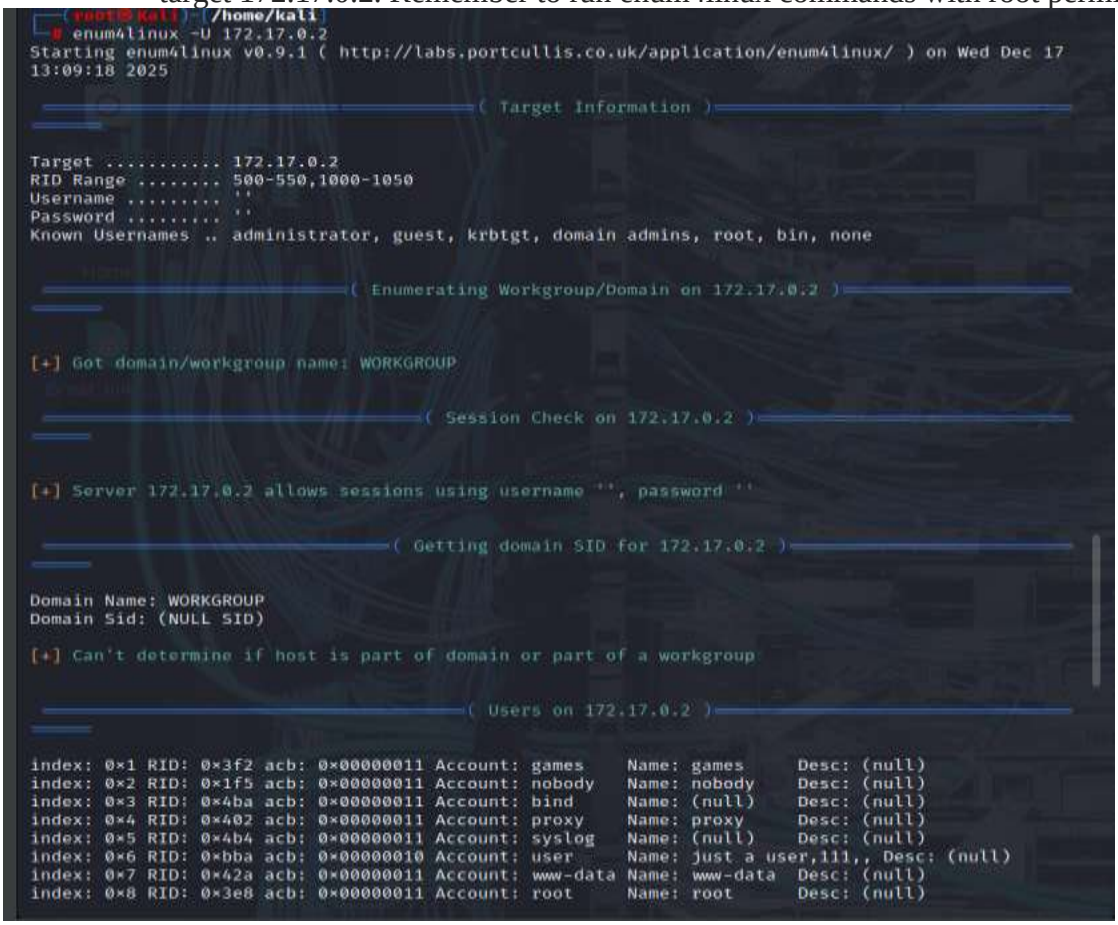
Yes, the computer at 10.6.6.23 is a potential target. It has ports 139 and 445 open, indicating SMB services.

Part 3: Use enum4linux to Enumerate Users and Network File Shares

In this section, we will use enum4linux to gather more information about potential targets.

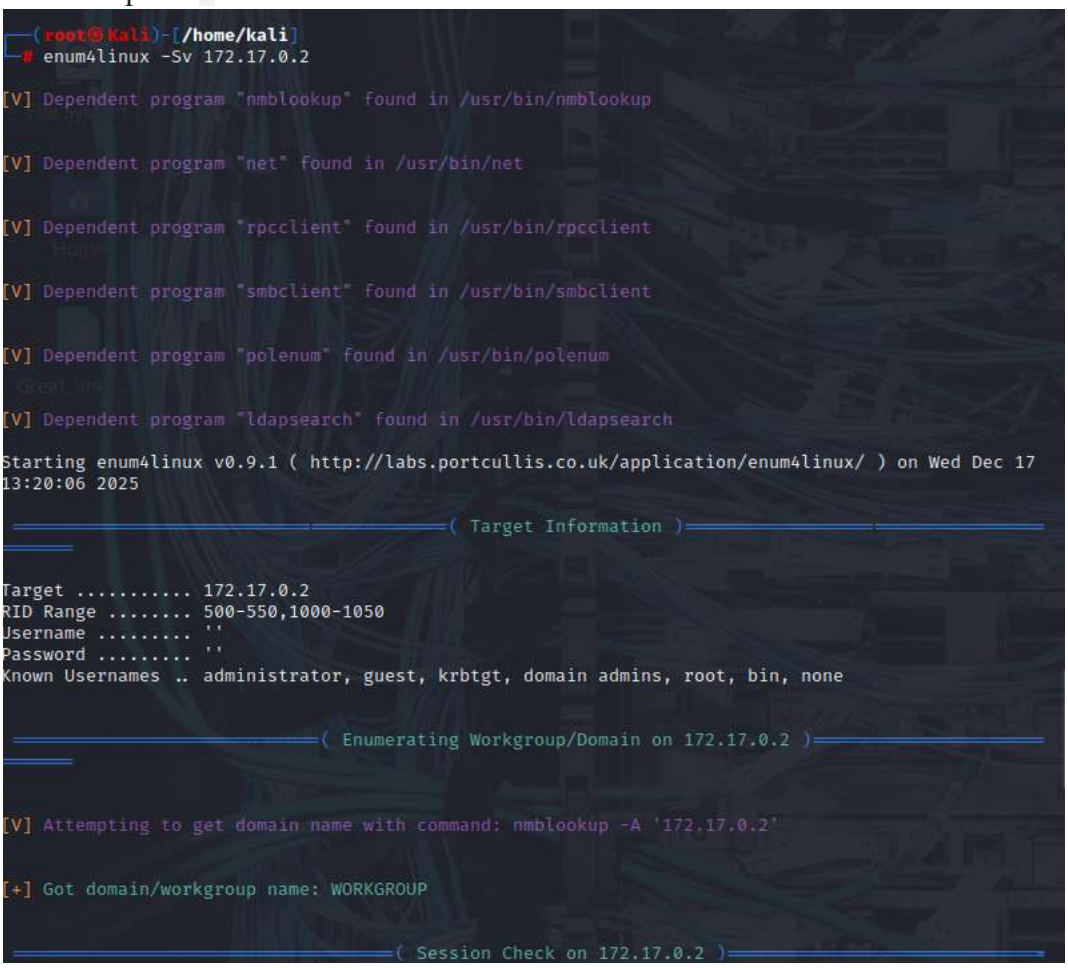
Step 1: Perform enum4linux Scan on Target 172.17.0.2

1. **Enumerate Users**: Use the **enum4linux -U** option to list the users configured on the target 172.17.0.2. Remember to run enum4linux commands with root permissions.



Enum4linux aggregates output from multiple Samba tools to provide concise results. If needed, you can use the verbose option **-v** to see how each feature is used.

2. **List File Shares**: Enumerate file shares on 172.17.0.2 using **enum4linux -S**. Use the verbose option **v** to understand which Samba tools are used.



Which Samba tool was used to map the file shares?

The Samba tool used to map file shares is smbclient.

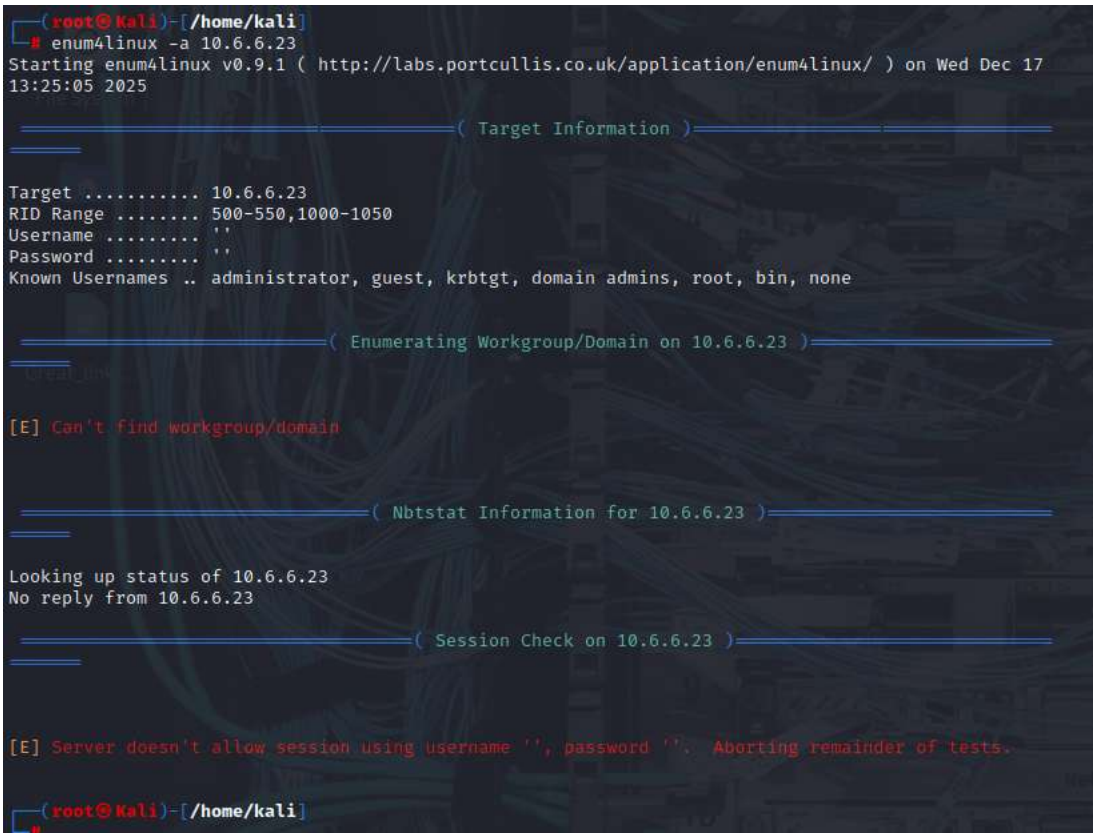
How many file shares are listed for target 172.17.0.2? What does the $ indicate at the end of the share name?

***There are five file shares listed for 172.17.0.2. The $ at the end of the share name indicates hidden shares*.**

3. **List Password Policies**: To understand the password policies on the target system, use the **enum4linux -P** command.

Step 2: Perform Simple Enumeration Scan on Target 10.6.6.23

1. **Combine Enumeration Options**: Enum4linux has an option to combine multiple enumeration operations into one command using the **a** argument. This allows quick enumeration of SMB information.



Part 4: Use smbclient to Transfer Files Between Systems

Smbclient is a valuable tool for transferring files between systems, similar to an FTP client. We will use smbclient to transfer a file to the target system at 172.17.0.2 as a simulated malware exploit.

1. **Create a Text File**: Use the **cat** command to create a text file named **badfile.txt** with desired content. For example:

```
cat >> badfile.txt
This is a bad file.
Press CTRL-C to write the file.
```

Press **CTRL-C** when done.

2. Explore smbclient Options: Check smbclient options using the **smbclient --help** command.

2. **List Shares on Target**: List shares on the target host (172.17.0.2) using the **smbclient -L** command.

3. **Connect to a Share**: Connect to the **tmp** share on the target using **smbclient**.

5. Explore smbclient Commands: Once connected, you can explore available commands by typing **help**.

6. Upload a File: Upload the **badfile.txt** to the target server using the **put** command.

```
put badfile.txt badfile.txt
```

This transfers the file to the target server.

7. Verify Upload: Use the **dir** command to verify that the file was successfully uploaded.

```
dir
```

8. Exit smbclient: Type **quit** to exit **smbclient** and return to the command prompt.