Contents

[Week three assignment of the Ethical hacking course 2](#_Toc217014763)

[1) Website Cloning Lab: 3](#_Toc217014764)

[1) SMB Vulnerability Scanning: 15](#_Toc217014765)

# 

# Week three assignment of the Ethical hacking course

These lab focuses on: Cloning a website for harvesting credential through a social engineering attack and SMB Vulnerability Scanning: Reproduce the Scanning for SMB Vulnerabilities using Enum4Linux.

## Website Cloning Lab:

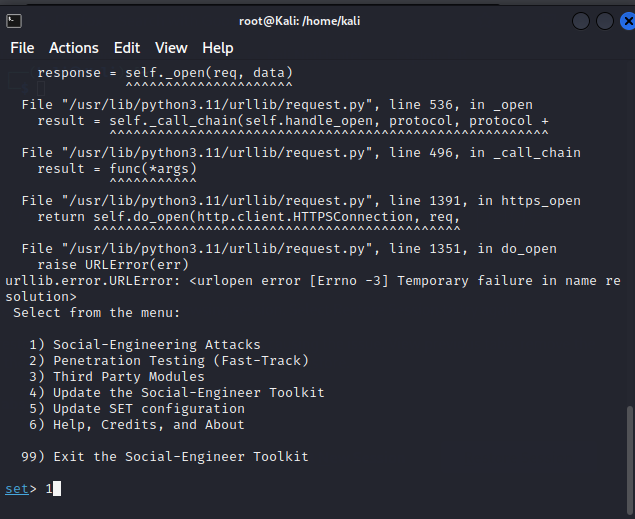
Setoolkit : is a social-engineer toolkit. It is an **open-source penetration testing framework** designed to simulate real-world social engineering attacks. It helps security professionals test an organization's human vulnerabilities (like phishing) in a controlled manner. Its main functions include:

* **Spear-Phishing Attacks**: Crafting and sending targeted emails.
* **Website Attack Vectors: Cloning legitimate sites to capture credentials.**
* **Infectious Media Generator: Creating malicious USB drives or CDs.**
* **QRCode Attacks: Generating malicious QR codes.**
* **SMS Spoofing: Sending deceptive text messages.**

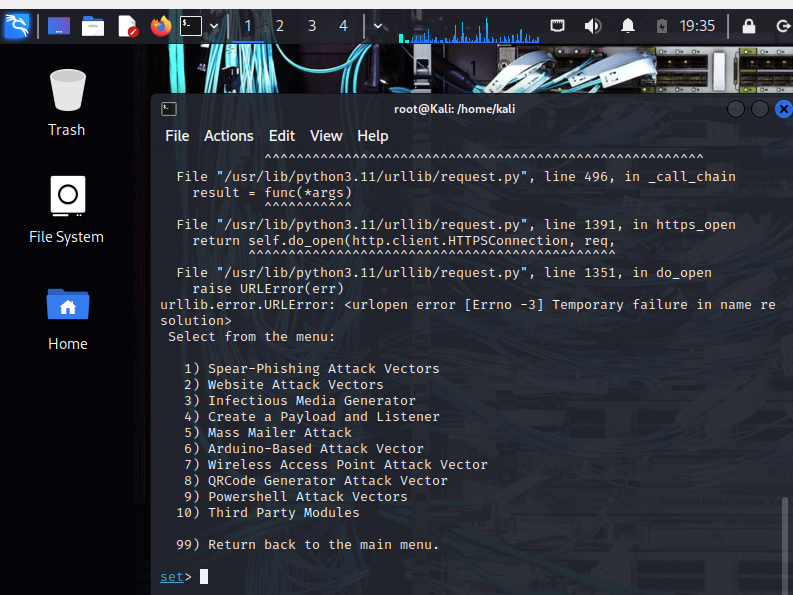
This lab is mainly focused on “**Website Attack Vectors: Cloning legitimate sites to capture credentials.**

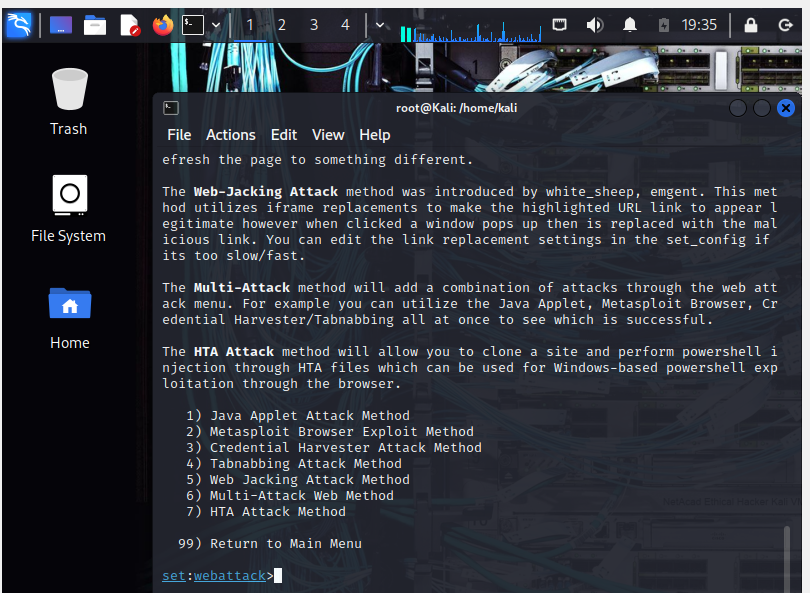
Command : sudo Setoolkit

Select 1 to enter to social engineering attack

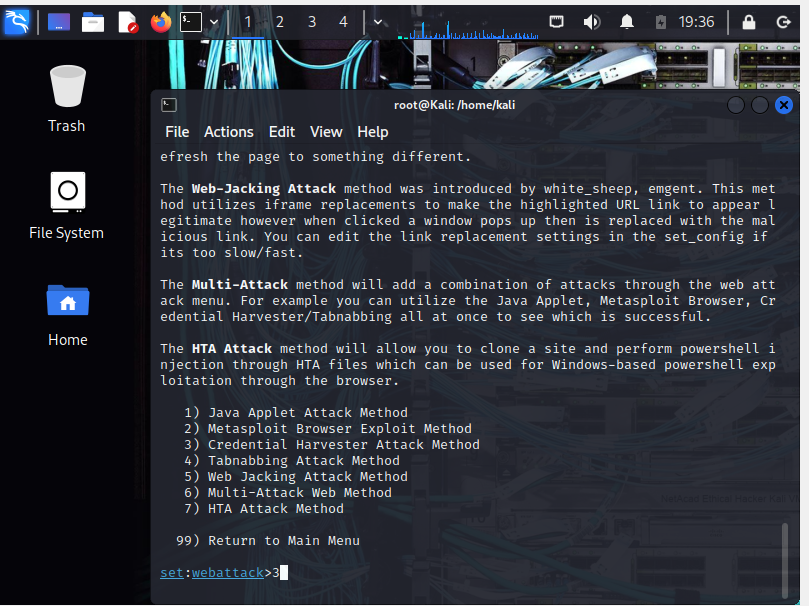


Select 2 – website attack vectors

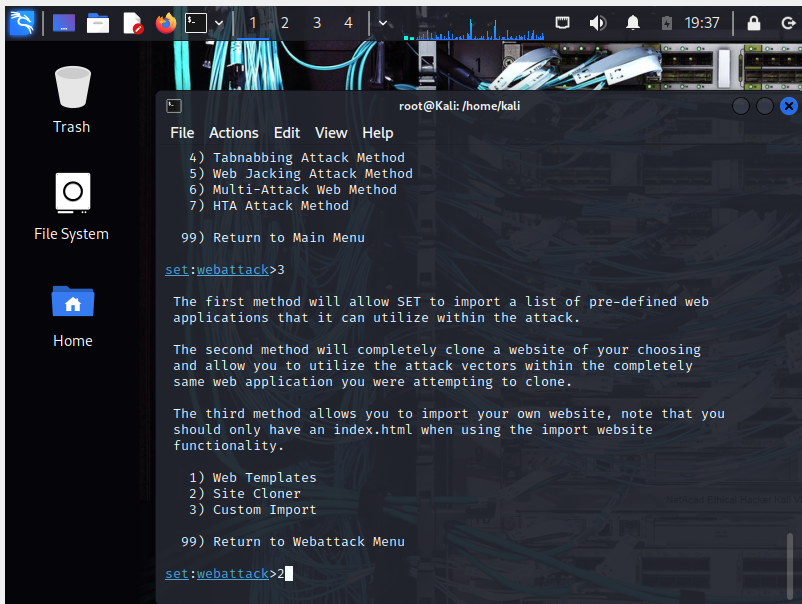




Select 3 Credential harvester attack method

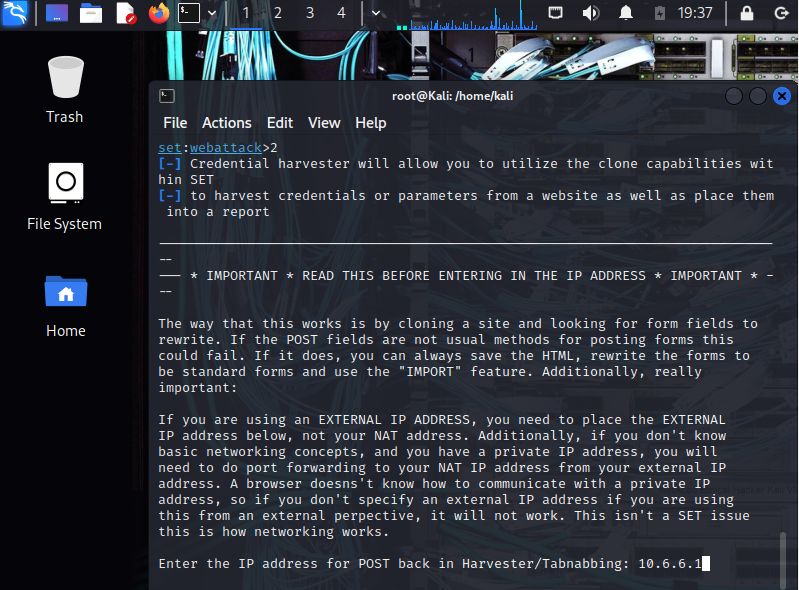


Then select 2 site cloner

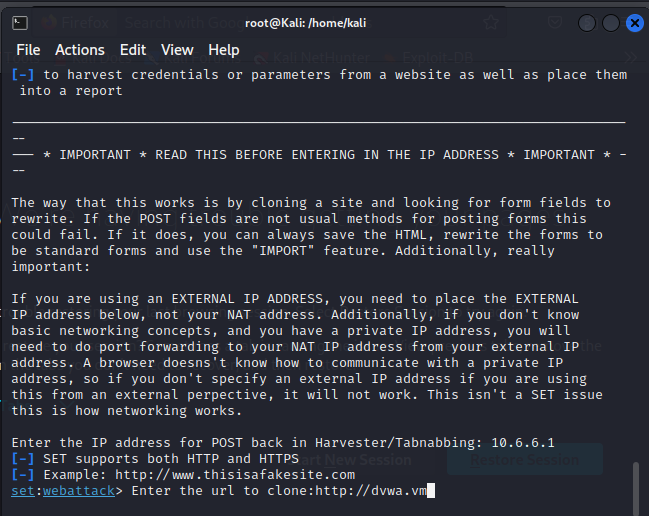


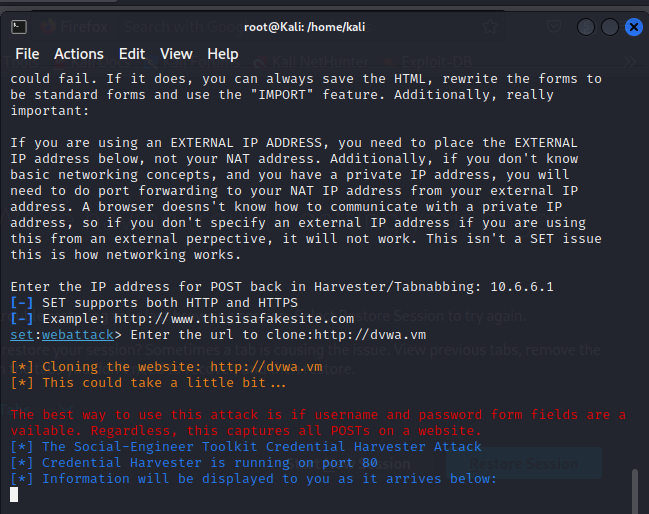
Enter the **IP address of the machine running SEToolkit under** **IP address for post back in harvesting**,

Note:- this is where the cloned malicious website will send any stolen user data (like usernames and passwords) that it harvests from victims.

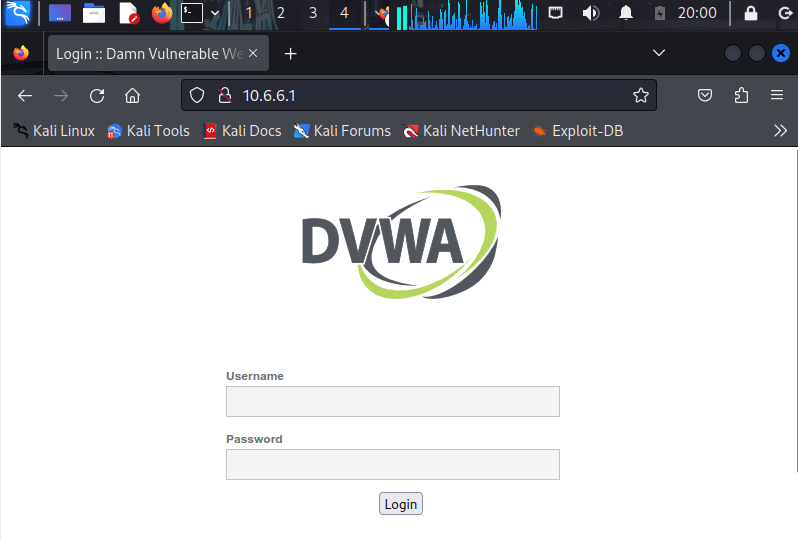


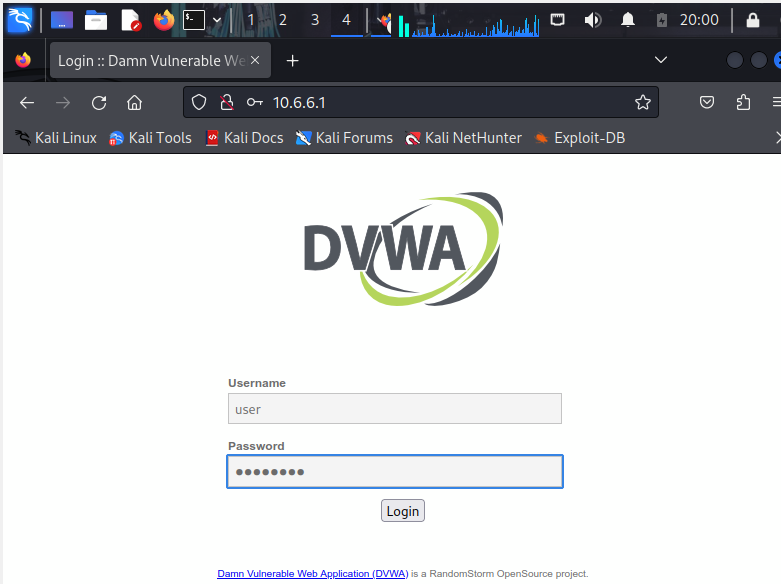
Then enter the URL to clone in this case http://dvwa.vm



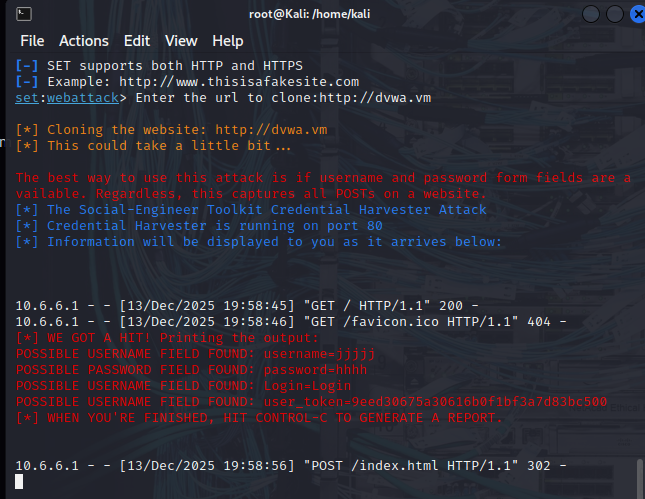


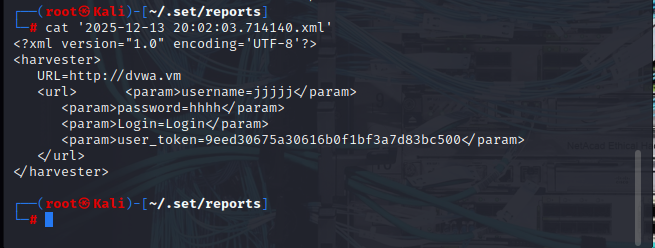
Below is the cloned malicious website that can be used for social engineering attack





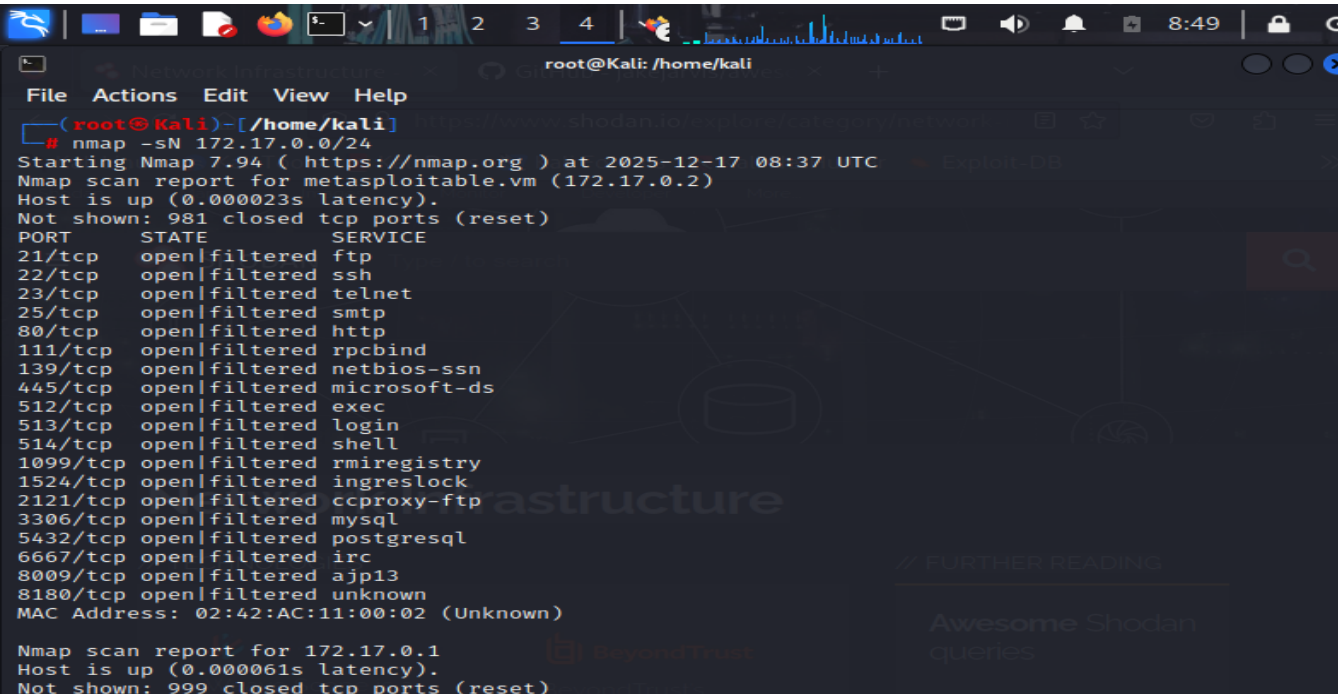
As shown below it will capture all inputs , including user name and password from the user.





## SMB Vulnerability Scanning:

1. **Nmap –sN 172.17.0.0/24:** Performed Nmap scan to check if SMB ports are open on subnet 172.17.0.0/24



Result:

* Two hosts are up , these are 172.17.0.2 and 172.17.0.1
* on 172.17.0.2 port 139 (SMB over netbios) and 445 (SMB over TCP) ports are open

1. **num4linux -U 172.17.0.2 :** Generate list of users that are configured on this specific devices

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 17 09:08:18 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 )=============================

[+] Got domain/workgroup name: WORKGROUP

====================================( Session Check on 172.17.0.2 )====================================

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

=================================( Getting domain SID for 172.17.0.2 )=================================

Domain Name: WORKGROUP

Domain Sid: (NULL SID)

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

========================================( 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,111,, 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)

index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)

index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)

index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)

index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)

index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)

index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)

index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)

index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)

index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)

index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)

index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)

index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)

index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin)Desc: (null)

index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)

index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)

index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)

index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)

index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)

index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)

index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)

index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,,, Desc: (null)

index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)

index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)

index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp Name: (null) Desc: (null)

index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)

index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync Name: sync Desc: (null)

index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)

user:[games] rid:[0x3f2]

user:[nobody] rid:[0x1f5]

user:[bind] rid:[0x4ba]

user:[proxy] rid:[0x402]

user:[syslog] rid:[0x4b4]

user:[user] rid:[0xbba]

user:[www-data] rid:[0x42a]

user:[root] rid:[0x3e8]

user:[news] rid:[0x3fa]

user:[postgres] rid:[0x4c0]

user:[bin] rid:[0x3ec]

user:[mail] rid:[0x3f8]

user:[distccd] rid:[0x4c6]

user:[proftpd] rid:[0x4ca]

user:[dhcp] rid:[0x4b2]

user:[daemon] rid:[0x3ea]

user:[sshd] rid:[0x4b8]

user:[man] rid:[0x3f4]

user:[lp] rid:[0x3f6]

user:[mysql] rid:[0x4c2]

user:[gnats] rid:[0x43a]

user:[libuuid] rid:[0x4b0]

user:[backup] rid:[0x42c]

user:[msfadmin] rid:[0xbb8]

user:[telnetd] rid:[0x4c8]

user:[sys] rid:[0x3ee]

user:[klog] rid:[0x4b6]

user:[postfix] rid:[0x4bc]

user:[service] rid:[0xbbc]

user:[list] rid:[0x434]

user:[irc] rid:[0x436]

user:[ftp] rid:[0x4be]

user:[tomcat55] rid:[0x4c4]

user:[sync] rid:[0x3f0]

user:[uucp] rid:[0x3fc]

enum4linux complete on Wed Dec 17 09:08:21 2025

1. **enum4linux -S 172.17.0.2 : Generated list of shares on the targeted machine**

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 17 09:23:20 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 )=============================

[+] Got domain/workgroup name: WORKGROUP

====================================( Session Check on 172.17.0.2 )====================================

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

=================================( Getting domain SID for 172.17.0.2 )=================================

Domain Name: WORKGROUP

Domain Sid: (NULL SID)

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

==================================( Share Enumeration on 172.17.0.2 )==================================

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.

Server Comment

--------- -------

Workgroup Master

--------- -------

WORKGROUP METASPLOITABLE

[+] Attempting to map shares on 172.17.0.2

//172.17.0.2/print$ Mapping: DENIED Listing: N/A Writing: N/A

//172.17.0.2/tmp Mapping: OK Listing: OK Writing: N/A

//172.17.0.2/opt Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT\_STATUS\_NETWORK\_ACCESS\_DENIED listing \\*

//172.17.0.2/IPC$ Mapping: N/A Listing: N/A Writing: N/A

//172.17.0.2/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A

enum4linux complete on Wed Dec 17 09:23:22 2025

1. **enum4linux -P 172.17.0.2 : generated the configured password policy**

┌──(root㉿Kali)-[/home/kali]

└─#

]

└─# enum4linux -P 172.17.0.2

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 17 09:46:57 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 )=============================

[+] Got domain/workgroup name: WORKGROUP

====================================( Session Check on 172.17.0.2 )====================================

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

=================================( Getting domain SID for 172.17.0.2 )=================================

Domain Name: WORKGROUP

Domain Sid: (NULL SID)

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

=============================( Password Policy Information for 172.17.0.2 )=============================

[+] Attaching to 172.17.0.2 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

[+] METASPLOITABLE

[+] Builtin

[+] Password Info for Domain: METASPLOITABLE

[+] Minimum password length: 5

[+] Password history length: None

[+] Maximum password age: Not Set

[+] Password Complexity Flags: 000000

[+] Domain Refuse Password Change: 0

[+] Domain Password Store Cleartext: 0

[+] Domain Password Lockout Admins: 0

[+] Domain Password No Clear Change: 0

[+] Domain Password No Anon Change: 0

[+] Domain Password Complex: 0

[+] Minimum password age: None

[+] Reset Account Lockout Counter: 30 minutes

[+] Locked Account Duration: 30 minutes

[+] Account Lockout Threshold: None

[+] Forced Log off Time: Not Set

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled

Minimum Password Length: 0

enum4linux complete on Wed Dec 17 09:47:01 2025

**Result : The password policy is very week**

**[+] Minimum password length: 5**

**[+] Password history length: None**

**[+] Maximum password age: Not Set**

**[+] Password Complexity Flags: 000000**

1. **Smbclient –L //172.17.0.2 : list shared resources under 172.17.0.2**

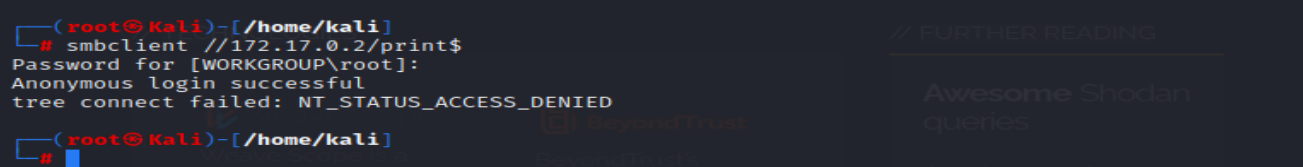
**Note: smbclient is a software component that initiate connection to SMB server to access shared resource. It is used to list and also to connect to a shared resources.**



**Result: Anonymous login was successful and we are able to see list of shared resources**

**With the following command we have tried to connect to the shared resources identified from the previous result**

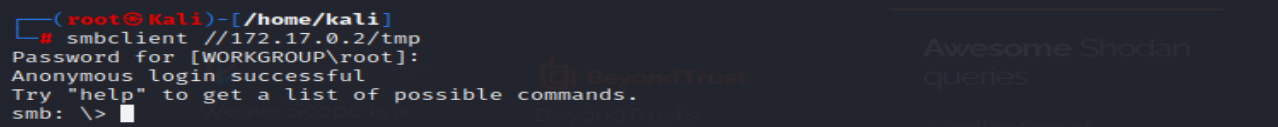
1. **connect to print$**



Result: anonymous login is successful but we are not able to connect to print$ because the resource is not meant to be connected

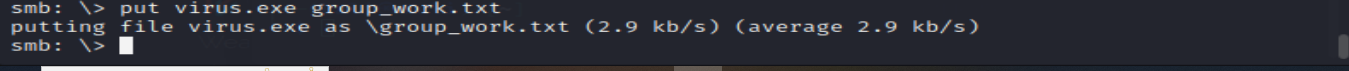
The $ sign in SMB share names has a **special meaning**—it indicates a **hidden administrative share**. We can't connect to shares ending with $ because they're intentionally designed to be **inaccessible via standard network browsing**, but there are specific ways to access them with proper privileges.

1. **Connect to tmp**



Result: anonymous login was successful and we are able to connect to shared file tmp

**3. Implant malicious code in the shared file we have accessed**



Put the file as group\_work.txt to avoid suspicion: put virus.exe group\_work.txt

Result the file is copied as group\_work.txt

