enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/irked/nmap.txt 10.10.10.117
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-23 09:33 EDT
Nmap scan report for 10.10.10.117
Host is up (0.21s 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          44981/udp6  status
|   100024  1          52331/tcp   status
|   100024  1          60122/udp   status
|_  100024  1          60408/tcp6  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 32.55 seconds
```

full nmap scan

```
nmap -sC -sV -p- -oN /home/kali/machines/retired/irked/nmap_complete.txt 10.10.10.117
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-23 09:41 EDT
Nmap scan report for 10.10.10.117
Host is up (0.19s latency).
```

```
Not shown: 65528 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          44981/udp6  status
|   100024  1          52331/tcp   status
|   100024  1          60122/udp   status
|_  100024  1          60408/tcp6  status
6697/tcp  open  irc     UnrealIRCd
8067/tcp  open  irc     UnrealIRCd
52331/tcp open  status  1 (RPC #100024)
65534/tcp open  irc     UnrealIRCd
Service Info: Host: irked.htb; 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 1567.09 seconds
```

running nmap script scan

```
nmap --script vuln
10.10.10.117
130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-23 09:40
EDT
Nmap scan report for
10.10.10.117
```

```
Host is up (0.31s
latency).
Not shown: 997 closed
ports
PORT    STATE
SERVICE
22/tcp  open
ssh
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /manual/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 43.88 seconds
```

```
nmap --script dns-service-discovery -p 111
10.10.10.117
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-23 09:44 EDT
Nmap scan report for 10.10.10.117
Host is up (0.23s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 1.22 seconds
```

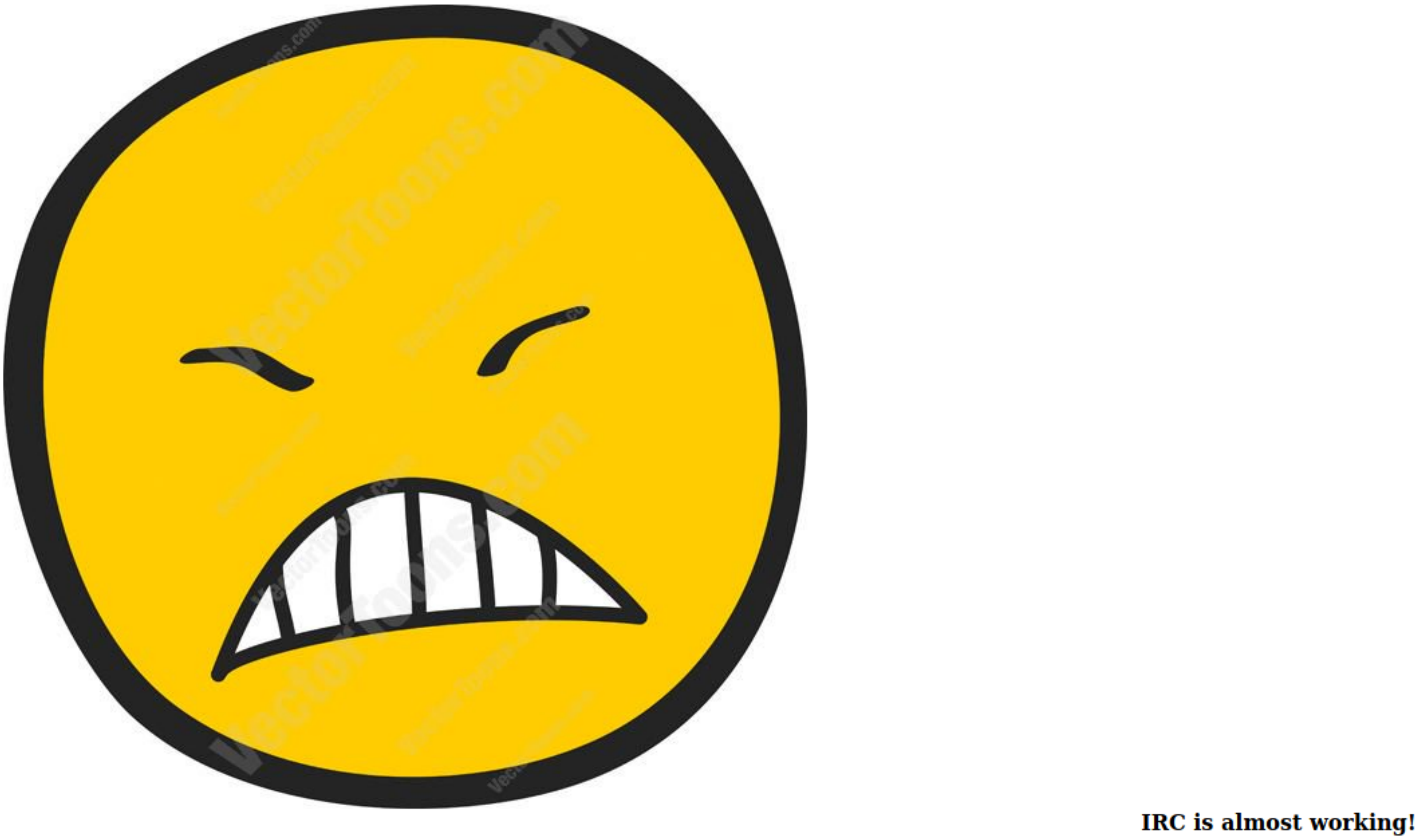
scripts reviled no results

lets wait for full port scan

```
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)

80/tcp  open  http    Apache httpd 2.4.10 ((Debian))

111/tcp open  rpcbind 2-4 (RPC #100000)

6697/tcp  open  irc     UnrealIRCd
8067/tcp  open  irc     UnrealIRCd
52331/tcp open  status  1 (RPC #100024)
65534/tcp open  irc     UnrealIRCd
```

and in full scan we also saw this open ports

we see port 80 lets see whats in there

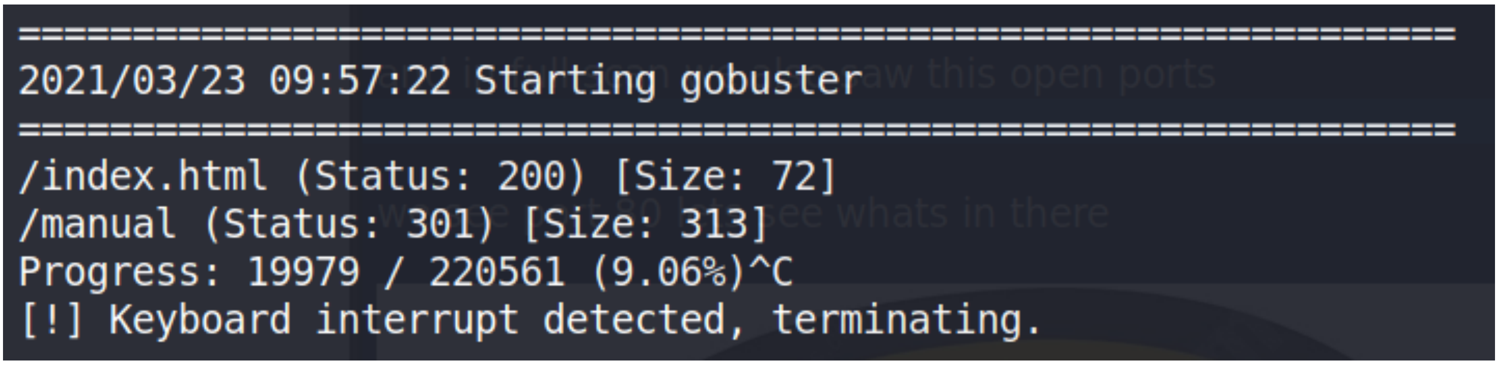


IRC is almost working!

this on page 80

lets run gobuster and see if any directories

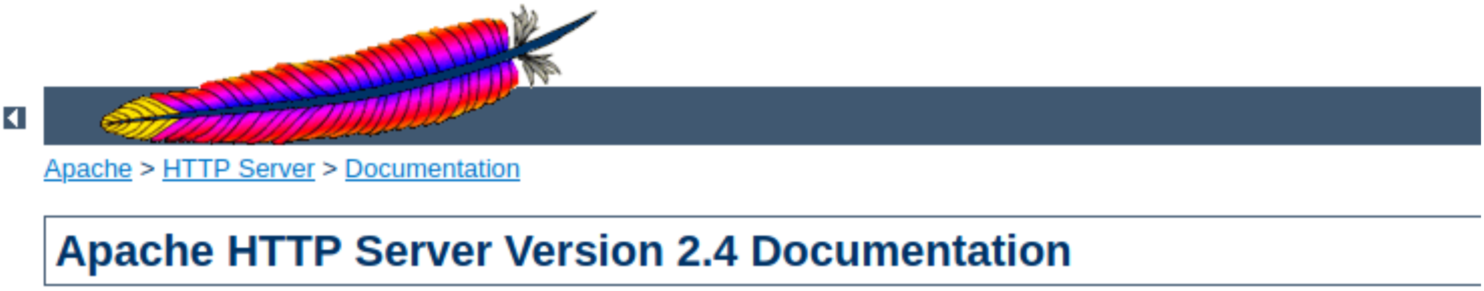
this is result of gobuster



```
===============================================================
2021/03/23 09:57:22 Starting gobuster
===============================================================
/index.html (Status: 200) [Size: 72]
/manual (Status: 301) [Size: 313]
Progress: 19979 / 220561 (9.06%)^C
[!] Keyboard interrupt detected, terminating.
```

we have a directory /manual lets see whats in this

going to manual we are taken to this page

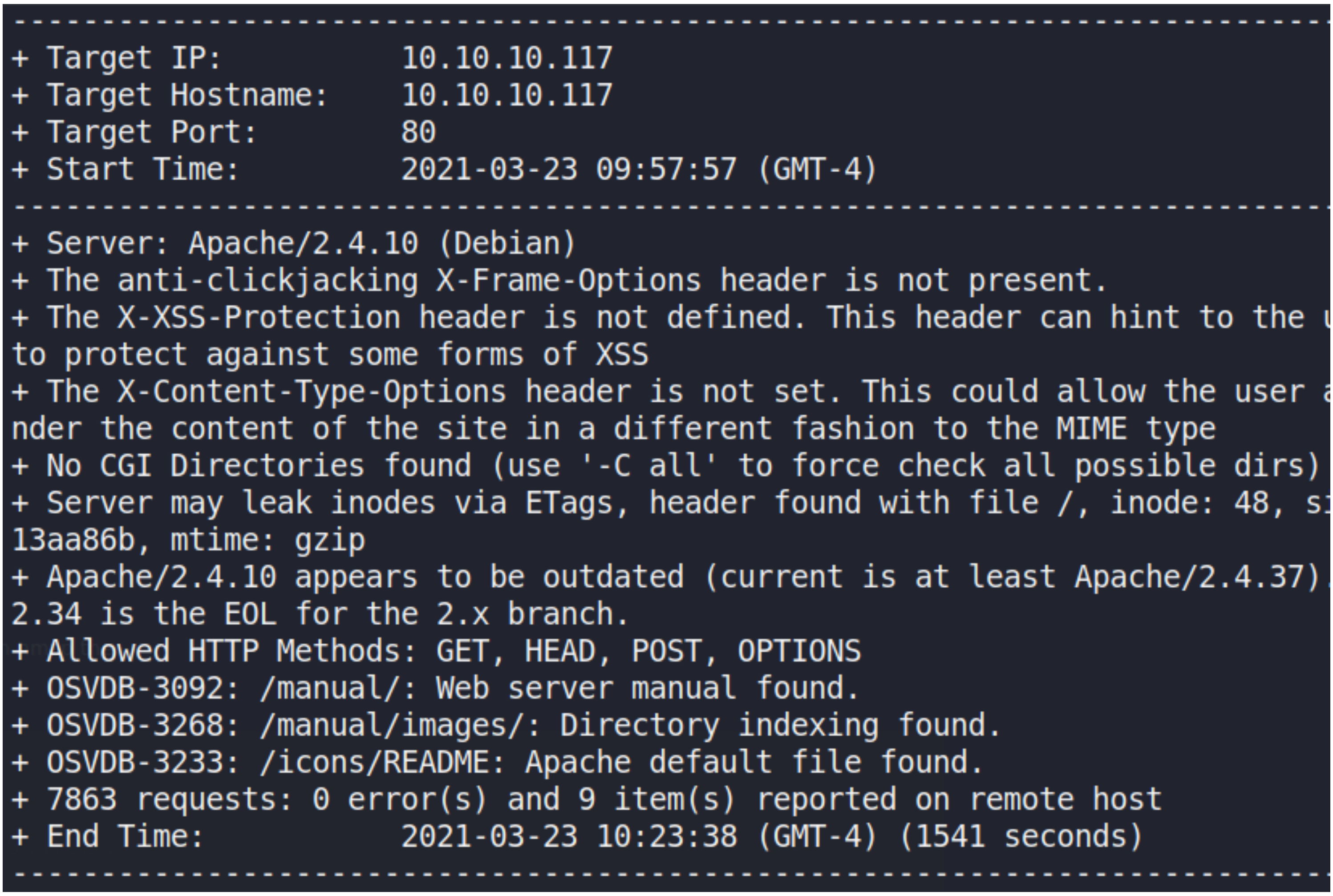


Apache > HTTP Server > Documentation

Apache HTTP Server Version 2.4 Documentation

we have to find other way as iscbind is installed their is a dns server we have to do the zone transfer to get the classified domain names

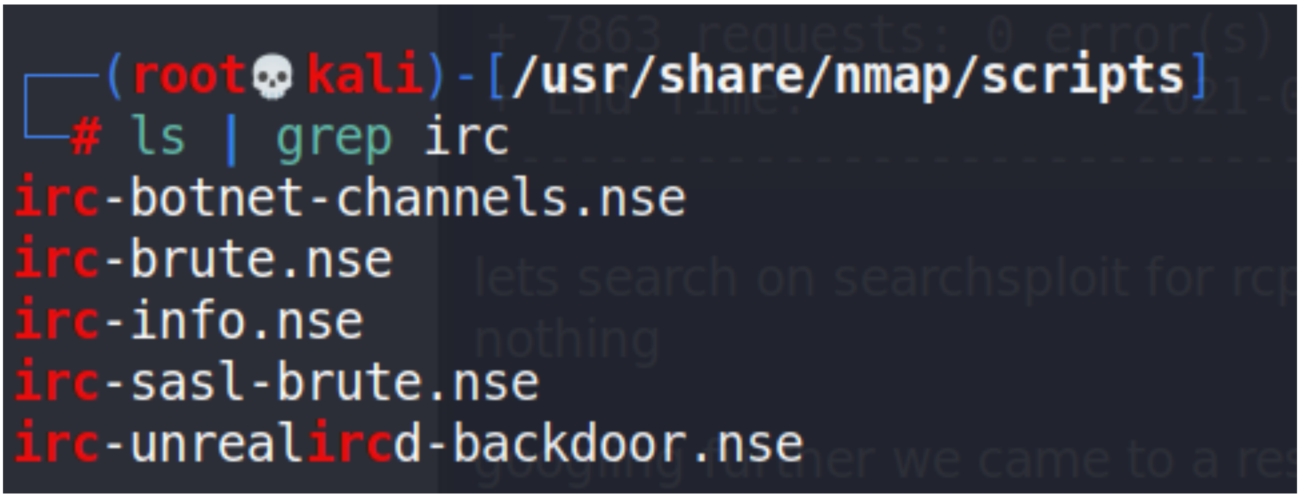
result of nikto



```
---------------------------------------------------------------------------
+ Target IP:          10.10.10.117
+ Target Hostname:    10.10.10.117
+ Target Port:        80
+ Start Time:         2021-03-23 09:57:57 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the u
to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user a
nder the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 48, si
13aa86b, mtime: gzip
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37).
2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7863 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2021-03-23 10:23:38 (GMT-4) (1541 seconds)
---------------------------------------------------------------------------
```

lets search on searchsploit for rcpbind
nothing

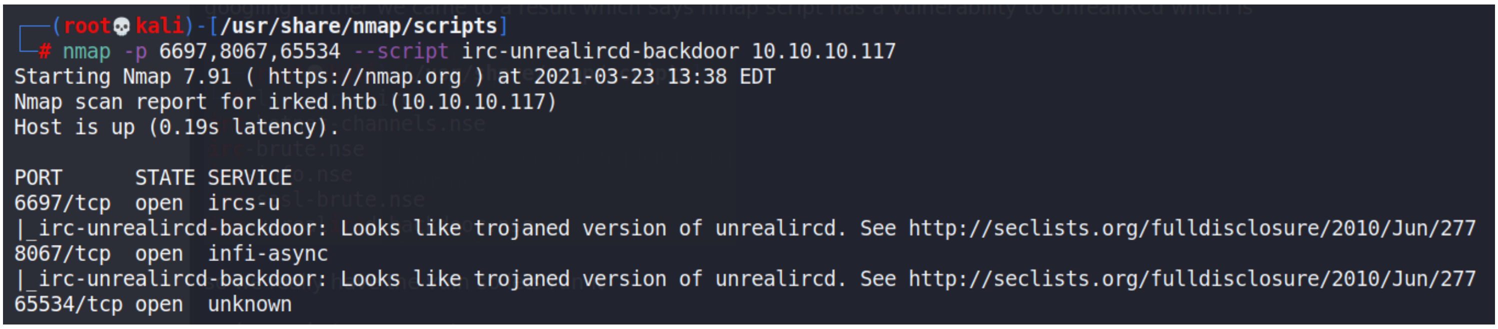
googling further we came to a result which says nmap script has a vulnerability to UnrealIRCd which is



```
┌──(root💀kali)-[/usr/share/nmap/scripts]
└─# ls | grep irc
irc-botnet-channels.nse
irc-brute.nse
irc-info.nse
irc-sasl-brute.nse
irc-unrealircd-backdoor.nse
```

so we really have the vuln so lets run it

and see what we can get



```
┌──(root💀kali)-[/usr/share/nmap/scripts]
└─# nmap -p 6697,8067,65534 --script irc-unrealircd-backdoor 10.10.10.117
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-23 13:38 EDT
Nmap scan report for irked.htb (10.10.10.117)
Host is up (0.19s latency).

PORT      STATE SERVICE
6697/tcp  open  ircs-u
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277
8067/tcp  open  infi-async
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277
65534/tcp open  unknown
```

we see port 8067 and 6697 are both have a backdoor capabilty and script says it will give a netcat session

so lets see how we can get a netcat from this script