ATTACK DEFENSE

by PentesterAcademy

Name	Tools : Netcat
URL	https://attackdefense.com/challengedetails?cid=1813
Type	Beginner Skills : Linux For Pentesters

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Learn netcat tool by doing the following activities.

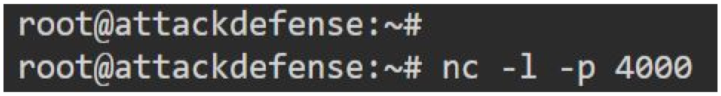
1. Use netcat to listen on TCP port 4000 of the localhost. Open a new tab and use netcat to connect to the listening instance.
2. Use netcat to listen on UDP port 4000 of the localhost. Open a new tab and use netcat to connect to the listening instance.
3. Use netcat to listen on port 4000 of the localhost and provide bash access to any session connecting to it. Open a new tab and use netcat to connect to the listening instance.
4. Use netcat to listen on port 4000 of the localhost and log the communication exchange into a file. Open a new tab and use netcat to connect to the listening instance.
5. Use netcat to listen on port 4000 of the localhost. Open a new tab and use netcat to connect to the listening instance. Transfer a dummy file from connecting instance t listening instance.
6. Use netcat as a port scanner to scan the first 1000 ports of the other two machines present on the network and discover their open ports.
7. Connect to telnet service running on a remote machine with netcat using the following credentials.
   - Username: administrator
   - Password: 1q2w3e4r
8. Connect to a web server using netcat and fetch the index page.
9. Create a dummy web server using netcat. Use curl command to interact with this dummy web server.

Solution:

Task 1: Use netcat to listen on TCP port 4000 of the localhost. Open a new tab and use netcat to connect to the listening instance.

In first terminal, use netcat to listen on TCP port 4000

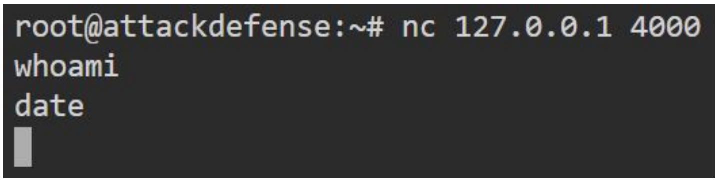
Command: nc -l -p 4000



```
root@attackdefense:~#
root@attackdefense:~# nc -l -p 4000
```

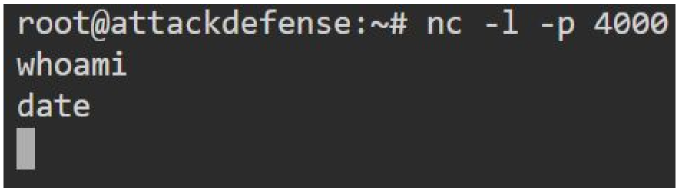
Open another terminal and use netcat to connect to this

Command: nc 127.0.0.1 4000



```
root@attackdefense:~# nc 127.0.0.1 4000
whoami
date
```

Whatever the user types on this side, will be replayed to the other side.



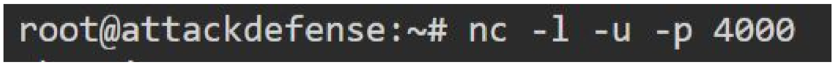
```
root@attackdefense:~# nc -l -p 4000
whoami
date
```

In this manner, netcat can be used to create a listener and connector.

Task 2: Use netcat to listen on UDP port 4000 of the localhost. Open a new tab and use netcat to connect to the listening instance.

In first terminal, use netcat to listen on UDP port 4000

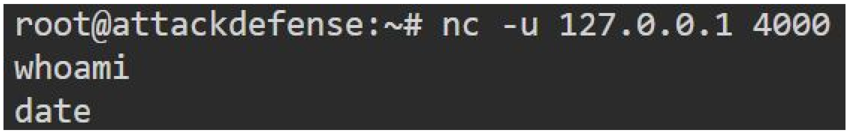
Command: nc -l -u -p 4000



```
root@attackdefense:~# nc -l -u -p 4000
```

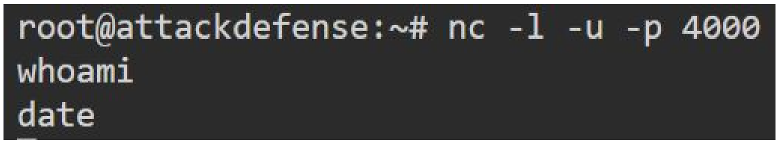
Open another terminal and use netcat to connect to this

Command: nc -u 127.0.0.1 4000



```
root@attackdefense:~# nc -u 127.0.0.1 4000
whoami
date
```

Whatever the user types on this side, will be replayed to the other side.

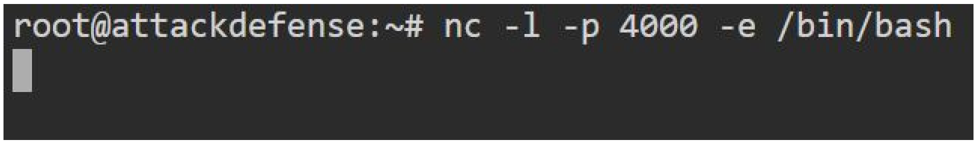


```
root@attackdefense:~# nc -l -u -p 4000
whoami
date
```

Task 3: Use netcat to listen on port 4000 of the localhost and provide bash access to any session connecting to it. Open a new tab and use netcat to connect to the listening instance.

In first terminal, use netcat to listen on UDP port 4000

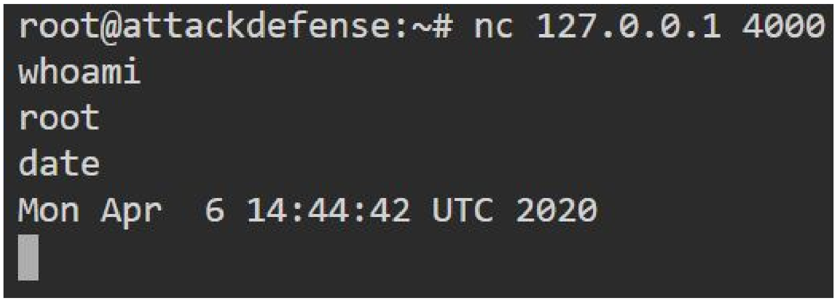
Command: nc -l -p 4000 -e /bin/bash



```
root@attackdefense:~# nc -l -p 4000 -e /bin/bash
```

Open another terminal and use netcat to connect to this

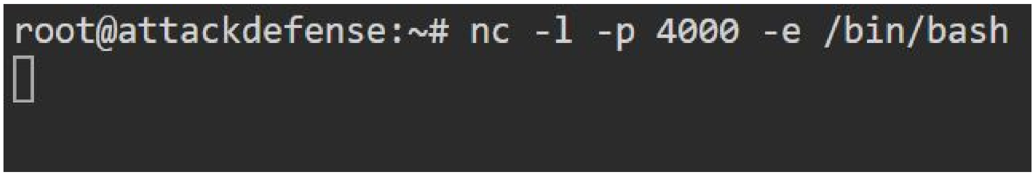
Command: nc 127.0.0.1 4000



```
root@attackdefense:~# nc 127.0.0.1 4000
whoami
root
date
Mon Apr  6 14:44:42 UTC 2020
```

The setup is just like before, however this time, the output of the commands will appear on the connector side.

But no commands will appear on the listener side.

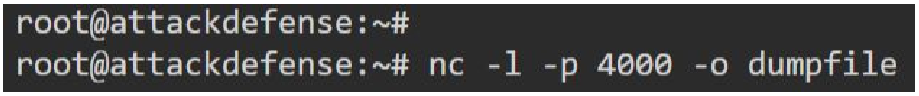


```
root@attackdefense:~# nc -l -p 4000 -e /bin/bash
```

Task 4: Use netcat to listen on port 4000 of the localhost and log the communication exchange into a file. Open a new tab and use netcat to connect to the listening instance.

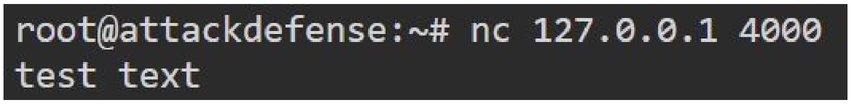
Start nc in listen mode on port 4000 and define file for content logging

Command: nc -l -p 4000 -o dumpfile



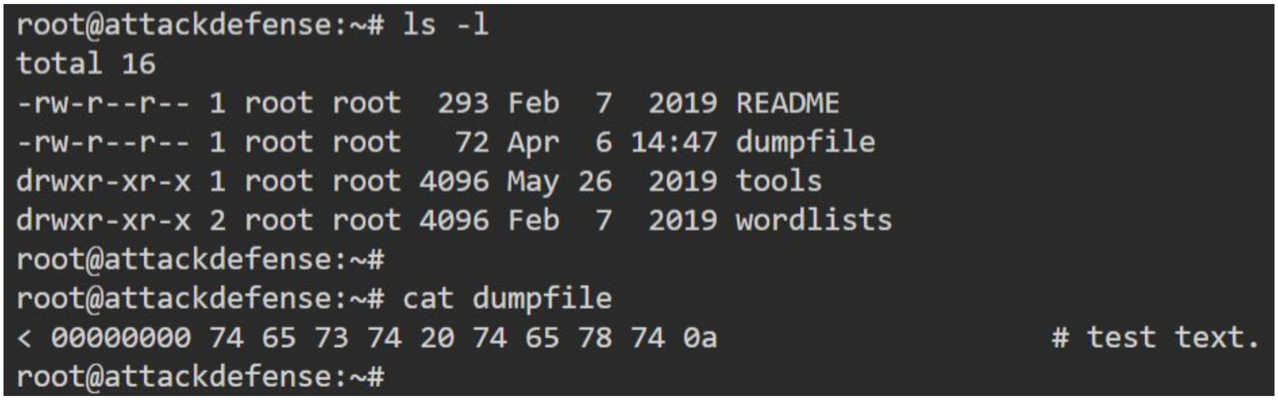
```
root@attackdefense:~#
root@attackdefense:~# nc -l -p 4000 -o dumpfile
```

From the second terminal, connect to the listen socket and send some data



```
root@attackdefense:~# nc 127.0.0.1 4000
test text
```

Close the listening nc and check the contents of the log file.



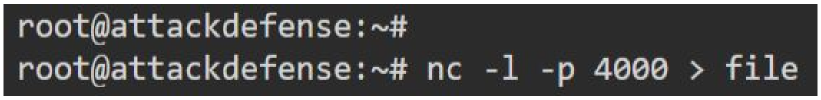
```
root@attackdefense:~# ls -l
total 16
-rw-r--r-- 1 root root  293 Feb  7  2019 README
-rw-r--r-- 1 root root   72 Apr  6 14:47 dumpfile
drwxr-xr-x 1 root root 4096 May 26  2019 tools
drwxr-xr-x 2 root root 4096 Feb  7  2019 wordlists
root@attackdefense:~#
root@attackdefense:~# cat dumpfile
< 00000000 74 65 73 74 20 74 65 78 74 0a                   # test text.
root@attackdefense:~#
```

One can observe that the data posted from the connector side is saved in this file.

Task 5: Use netcat to listen on port 4000 of the localhost. Open a new tab and use netcat to connect to the listening instance. Transfer a dummy file from connecting instance t listening instance.

Redirect the output of netcat listener to a file

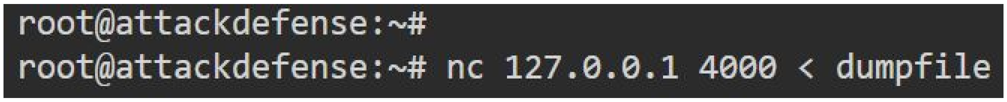
Command:



```
root@attackdefense:~#
root@attackdefense:~# nc -l -p 4000 > file
```

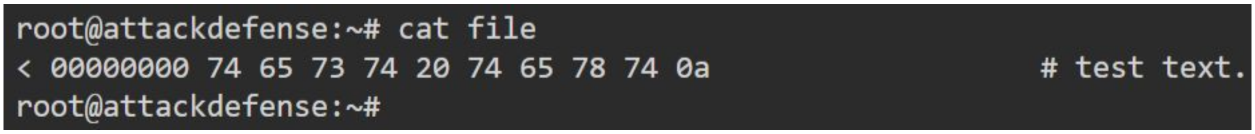
Connect to listen socket and pass the dumpfile through it.

Command:



```
root@attackdefense:~#
root@attackdefense:~# nc 127.0.0.1 4000 < dumpfile
```

Stop the netcat listener. Check the contents of transferred file

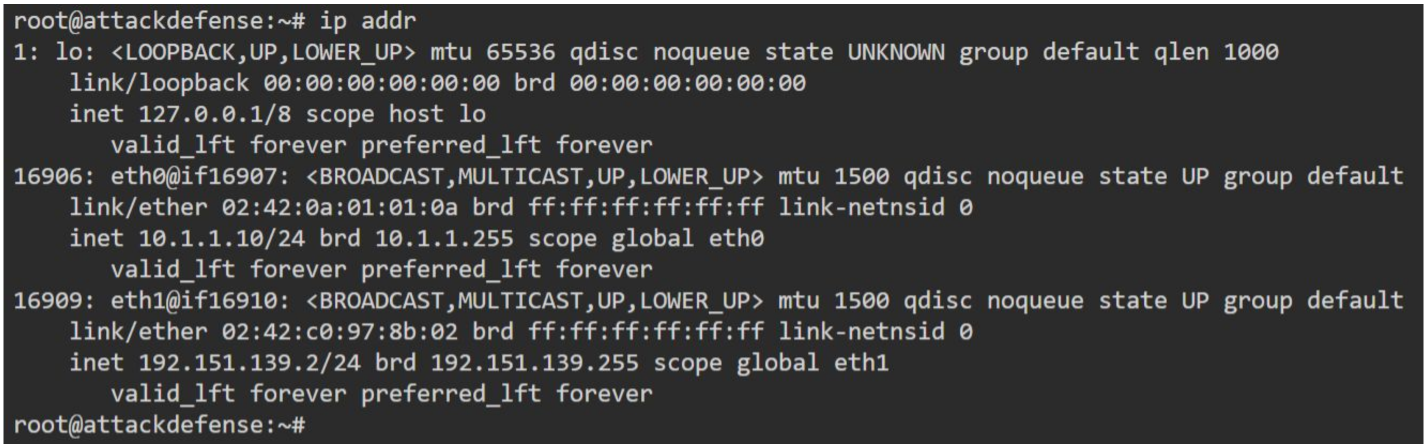


```
root@attackdefense:~# cat file
< 00000000 74 65 73 74 20 74 65 78 74 0a                  # test text.
root@attackdefense:~#
```

Task 6: Use netcat as a port scanner to scan the first 1000 ports of the other two machines present on the network and discover their open ports.

Check the IP address of attacker Kali machine

Command: ip addr

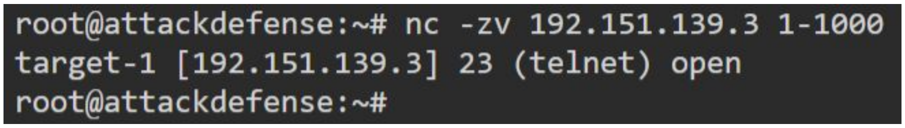


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
16906: eth0@if16907: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:0a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.10/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
16909: eth1@if16910: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:97:8b:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.151.139.2/24 brd 192.151.139.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP of user’s machine is 192.151.139.2, so as per the guidelines the IP of remote Linux machines should be 192.151.139.3 onwards.

Scan first 1000 ports of target machine 192.151.139.3

Command: nc -zv 192.151.139.3 1-1000

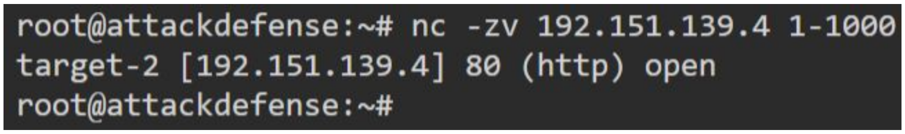


```
root@attackdefense:~# nc -zv 192.151.139.3 1-1000
target-1 [192.151.139.3] 23 (telnet) open
root@attackdefense:~#
```

Telnet service is running on the remote mahine.

Scan first 1000 ports of target machine 192.151.139.4

Command: nc -zv 192.151.139.4 1-1000



```
root@attackdefense:~# nc -zv 192.151.139.4 1-1000
target-2 [192.151.139.4] 80 (http) open
root@attackdefense:~#
```

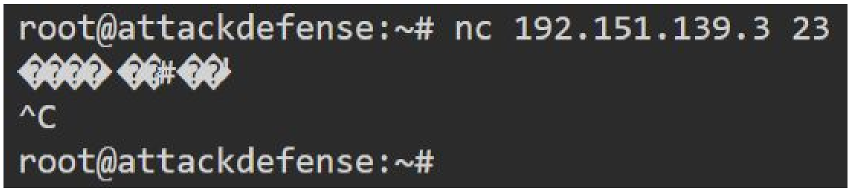
HTTP service is running on the remote mahine.

Task 7: Connect to telnet service running on a remote machine with netcat using the following credentials.

- **Username: administrator**
- **Password: 1q2w3e4r**

Try to connect to port 23 of the remote server.

Command: nc 192.151.139.3 23

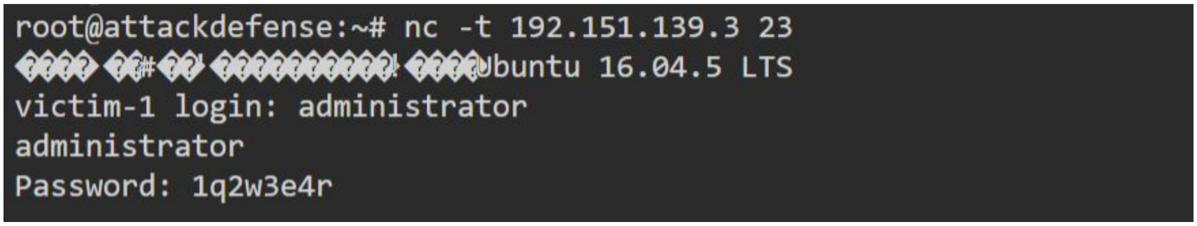


```
root@attackdefense:~# nc 192.151.139.3 23
���� ��#��'
^C
root@attackdefense:~#
```

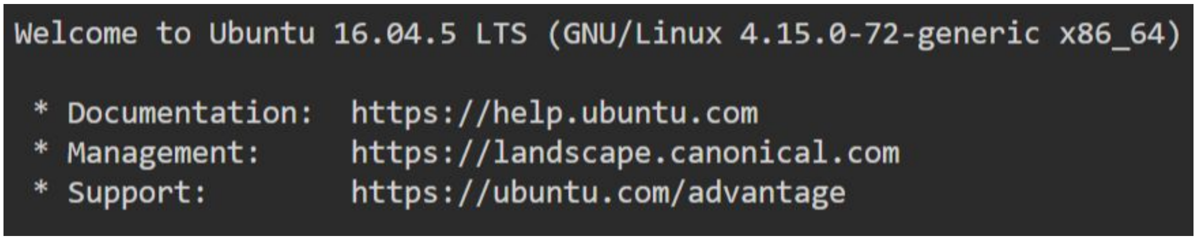
It will not work because netcat is not able to comprehend telnet.

Try again to connect to port 23 of the remote port but use -t option this time.

Command: nc -t 192.151.139.3 23



```
root@attackdefense:~# nc -t 192.151.139.3 23
���� ��#�� ����������!����Ubuntu 16.04.5 LTS
victim-1 login: administrator
administrator
Password: 1q2w3e4r
```



```
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.15.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

Provide credentials when prompted.

Task 8: Connect to a web server using netcat and fetch the index page.

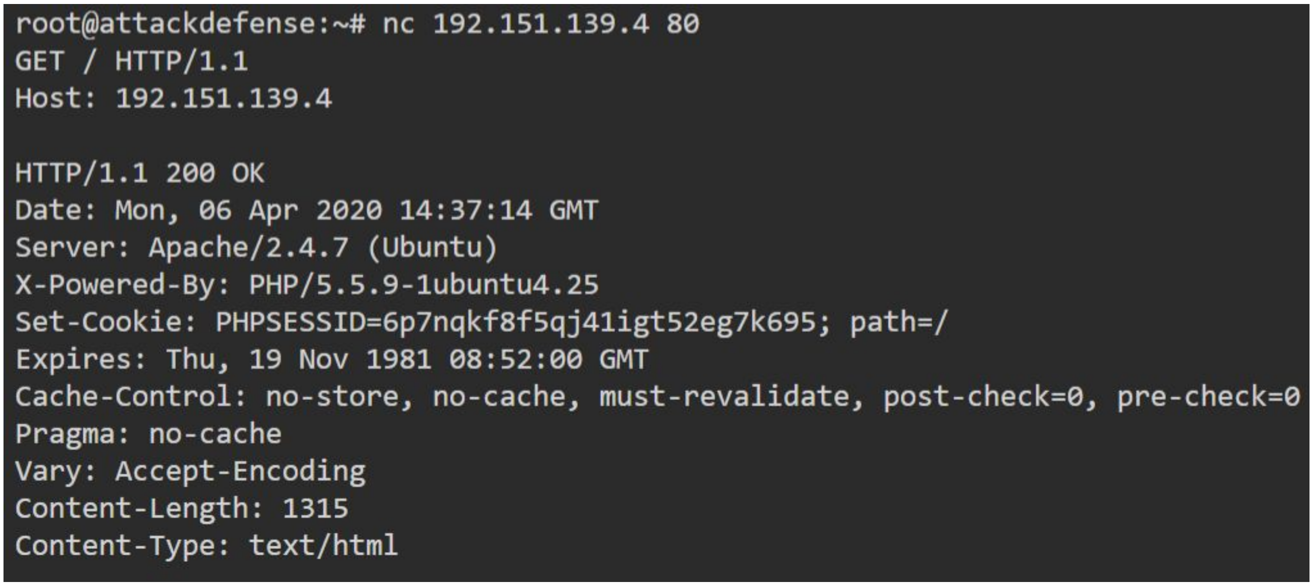
Connect to port 80 of the remote server.

Command: nc 192.151.139.4 80

Once the netcat connects, write the following

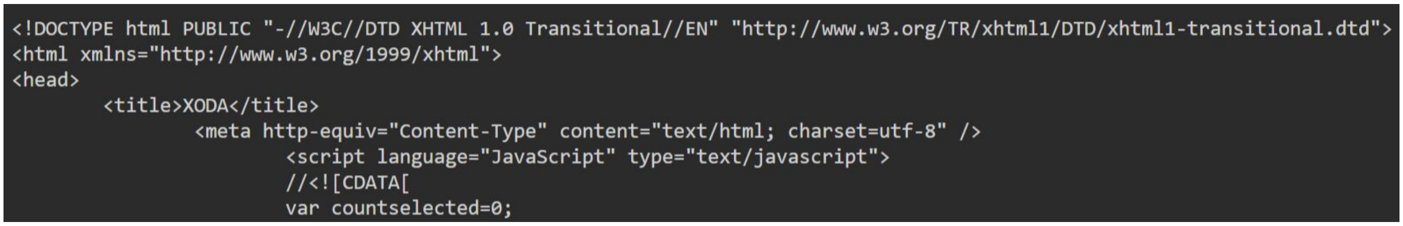
GET / HTTP/1.1
Host: 192.151.139.4

Press the enter button twice.



```
root@attackdefense:~# nc 192.151.139.4 80
GET / HTTP/1.1
Host: 192.151.139.4

HTTP/1.1 200 OK
Date: Mon, 06 Apr 2020 14:37:14 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.25
Set-Cookie: PHPSESSID=6p7nqkf8f5qj41igt52eg7k695; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1315
Content-Type: text/html
```

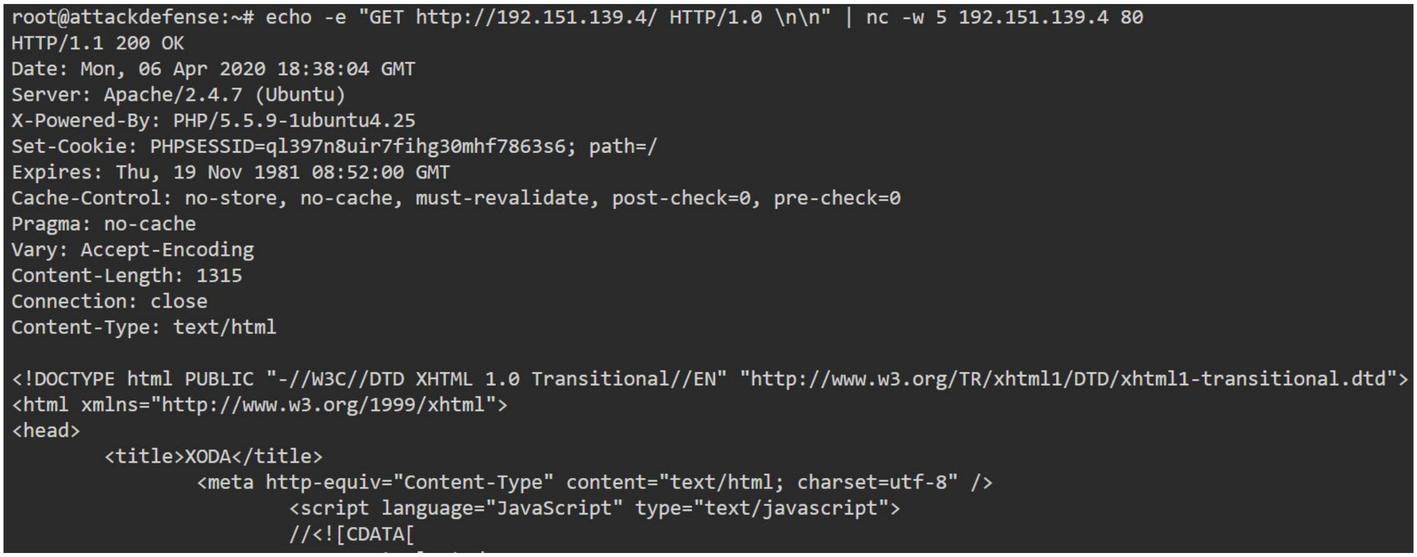


```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
        <title>XODA</title>
                <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
                        <script language="JavaScript" type="text/javascript">
                        //<![CDATA[
                        var countselected=0;
```

The web page can be accessed in this manner.

Alternatively,

Command: echo -e "GET http://192.151.139.4/ HTTP/1.0 \n\n" | nc -w 5 192.151.139.4 80



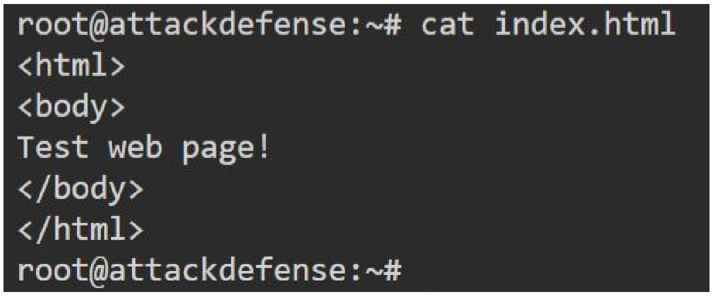
```
root@attackdefense:~# echo -e "GET http://192.151.139.4/ HTTP/1.0 \n\n" | nc -w 5 192.151.139.4 80
HTTP/1.1 200 OK
Date: Mon, 06 Apr 2020 18:38:04 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.25
Set-Cookie: PHPSESSID=ql397n8uir7fihg30mhf7863s6; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1315
Connection: close
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
        <title>XODA</title>
                <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
                        <script language="JavaScript" type="text/javascript">
                        //<![CDATA[
```

Task 9: Create a dummy web server using netcat. Use curl command to interact with this dummy web server.

Create a sample index.html file

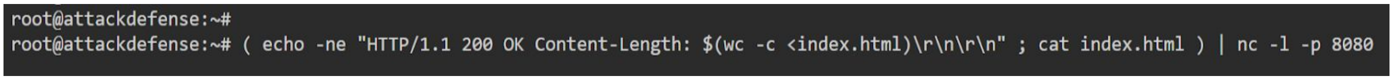
Command: vim index.html



```
root@attackdefense:~# cat index.html
<html>
<body>
Test web page!
</body>
</html>
root@attackdefense:~#
```

Serve it using netcat listener, listening at port 8080

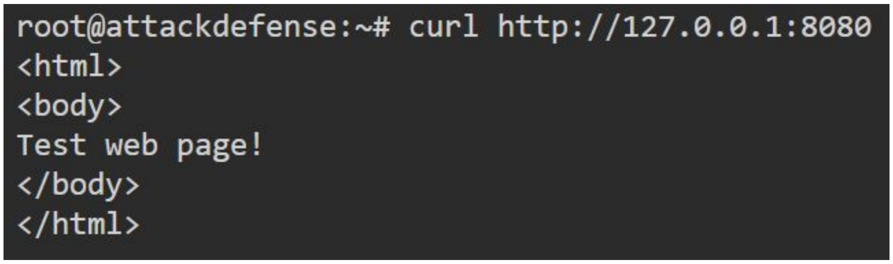
Command: (echo -ne "HTTP/1.1 200 OK Content-Length: $(wc -c <index.html)\r\n\r\n" ; cat index.html) | nc -l -p 8080



```
root@attackdefense:~#
root@attackdefense:~# ( echo -ne "HTTP/1.1 200 OK Content-Length: $(wc -c <index.html)\r\n\r\n" ; cat index.html ) | nc -l -p 8080
```

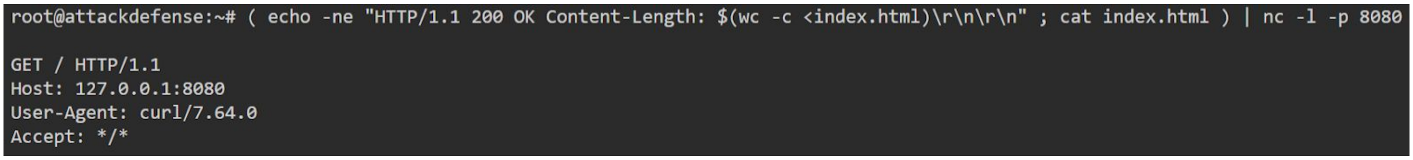
Use curl to access the webpage served by netcat

Command: curl http://127.0.0.1:8080



```
root@attackdefense:~# curl http://127.0.0.1:8080
<html>
<body>
Test web page!
</body>
</html>
```

The HTTP request made by the curl will be logged by the listener.



```
root@attackdefense:~# ( echo -ne "HTTP/1.1 200 OK Content-Length: $(wc -c <index.html)\r\n\r\n" ; cat index.html ) | nc -l -p 8080

GET / HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: curl/7.64.0
Accept: */*
```