TCS332, Fundamental of Information Security and Blockchain

B. Tech CSE III Semester

Instructor:

Dr Mohammad Wazid

Professor, Department of CSE

Graphic Era (Deemed to be University), Dehradun, India

Email: wazidkec2005@gmail.com

Homepage: https://sites.google.com/site/mwazidiiith/home

netcat - The Swiss Army Knife

Overview

- Netcat (also known as ‘nc’ or ‘Swiss Army knife’) is a networking utility (tool) used for reading or writing from TCP and UDP sockets using an easy interface.
- Netcat is a utility that reads and writes data across network connections, using the TCP or UDP protocol.

Overview

- Netcat is designed as a Dependable ‘back-end’ device that can be used directly or easily driven by other programs and scripts.
- Netcat is a treat to **network administrators**, **programmers**, and **pen-testers** as it’s a feature rich **network debugging** and **investigation tool**.

Overview

- It can create almost any kind of connection you would need and has several interesting built-in capabilities.
- In 2000, Netcat was voted the second most functional network security tool.

Overview

- It is capable of numerous additional tasks like chatting, file transfer, port scanning, opening remote shells to even setting up a honey pot.
- An important feature of Netcat is that it can serve both as a client and a server (more detail later). It is available for both Linux and Windows.

Overview

- PortScanning is the act of systematically scanning a computer's ports.
- Use netcat as a Port Scanner Tool
- Open a new terminal and run the following command to perform a TCP port scan.

nc -v -z 127.0.0.1 25

- The -v option is used to run netcat in verbose mode so the user can see what is happening and -z option tells netcat to not make a full connection since we are only interested to know the state of the port.
- nc -v -z host port-range. Exemple **nc -v -z 127.0.0.1 1300-13000**

Chat application using netcat

- We use facebook , email and other social networks to communicate with each other.
- How do you chat with your friend in the college's lab without internet connection ? Netcat does the magic for you.
- Since Netcat creates almost any kind of connection and is designed to read and write data across both TCP and UDP why not try to set up a simple chat ?
- Open in one terminal and type

nc -l -p 12345

- Open the other terminal and type

nc localhost 12345

Chat application using netcat

- We need a server and client to connect to our server.
- One of you guys should be the server and he should learn about the -l option which put netcat in server mode. Example **nc -l -p 12345.**
- This will set up the server using netcat in listening mode.
- We will use port 12345 and will specify the port number with -p option.
- The client needs the server IP to connect to it.
- My server and my client are on the same machine so I use **localhost** for the hostname. The command ‘nc hostname port’ puts netcat in client mode and connects to the specified hostname on the specified port. Example **nc localhost 12345**

Web server using nc

- The netcat tool nc can operate as a TCP client.
- Because HTTP works over TCP, nc can be used as an HTTP server!
- Because nc is a UNIX tool, we can use it to make custom web servers: servers which return any HTTP headers you want, servers which return the response.
- You can also use nc as a quick-and-dirty static file server.
- Here’s an example. Run your web server by telling nc to listen for new connections on port 11000.

web server using nc

- **create a html file as follows:**

```
<html>
<head>                <title>Test Page</title>
</head>
<body>
<h1>Hello</h1>
<h2>Welcome to GEU</h2>
<p>How are you?</p>
 </body>
</html>
```

Save the file as “home.html"

web server using nc

- Step1 (Type in one terminal)

mwazid@mwazid:~$ nc -l -p 11000

This will act like the web server

- Step2 (Type in the other terminal)

curl localhost:11000/home.html

Step3 (We get following output at server side)

GET /home.html HTTP/1.1User-Agent:

curl/7.35.0Host:

localhost:11000Accept: */*

Step4

Now type at server side:

HTTP/1.1 200 Everything Is Just Fine

Server: netcat!

Content-Type:text/html;

charset=UTF-8

<!doctype html>

<html>

<body>

<h1>Welcome to GEU</h1>

</body>

</html>

Step5

You will be able to see following response in your terminal at the client side:

HTTP/1.1 200 Everything Is Just Fine

Server: netcat!

Content-Type: text/html; charset=UTF-8

<!doctype html>

<html>

<body>

<h1>Welcome to GEU

</h1>

</body>

</html>

- That's means we got the response and connection was established successfully.
- The curl command transfers data to or from a network server, using one of the supported protocols (HTTP, HTTPS, FTP, FTPS, SCP, SFTP, TFTP, DICT, TELNET, LDAP or FILE).

End of lecture