rootsh3ll Labs

NetCat Essentials 101

Objective

NetCat is a networking tool mainly used to read and write through network connections using TCP and UDP. Famous for being the Swiss army knife for hackers, NetCat helps a hacker to access system's terminal shell remotely.

Your challenge is to perform basic operations using NetCat to complete this lab.

Operations like

1. Connect to a remote server
A server (10.1.3.31) is running a shell prompt on port 8080, connect to it using NetCat and get the secret flag stored in root directory.

2. Start a listener
A client is probing for your device on port 8000. Share your terminal via NetCat and retrieve the flag posted on the shell prompt after successful connection.

3. TCP Banner Grab
The server that connected to you is running a web server on port 8090. Connect to it with NetCat and grab the flag from /flag directory using HTTP/1.0 protocol.

TABLE OF CONTENTS

Skip to Flag 1 - Connecting to Remote Server >>

Flag 1 - Connecting to remote server

Objective: Connect to server 10.1.3.31's remote shell on port 8080, retrieve secret.txt in the root directory and enter the flag.

Connecting to a remote server using NetCat is simple.

`nc [Target IP] [Target Port]`

```
nc 10.1.3.31 8080
```

Upon successful connection, you won't see a notification in the Terminal window. To see the connection state you need to enable verbose output for NetCat. Just add -v to the command above.

```
nc -v 10.1.3.31 8080
```

When the output says connection [OPEN]. You shall check if you have entered the shell. Run a simple 'ls' command to ensure you can have basic shell access.

In the output, you'd see a file named secret.txt
Read the contents of the file and enter the flag.

```
cat secret.txt
```

Flag 2 - Listen to incoming connections

Objective: Start a NetCat listener on port 8000 and enter the flag received on STDIN

As it goes with connection, listening to remote incoming connections is equally straight-forward with NetCat.

Tell NetCat that you want to "listen" (`-l`), in verbose mode (`-v`) on port number `8000`. That's it. NetCat will start listening to all the network traffic from all interface on port 8000.
And shows you output in verbose mode.

```
nc -lvp 8000
```

Flag 3 - Identify incoming request server's IP address

Objective: What IP address connected to your NetCat listener on port *8000*

Enabling the verbose mode in the previous command gives us the information on the remote incoming connection. Information like:

1. Remote client's IP address
2. Hostname of remote client
3. State of connection (Open/Close/Error)

Simply note the IP address from previous command's output.

Flag 4 - Connect to remote web server and fetch web response

Objective: Enter the flag received from the web-server's **`/flag`** running on port `8090`

Connecting to a web server with NetCat is same as connecting to a remote NetCat instance. The difference is that you have to pass the HTTP VERB (Method), web server path and Protocol request type for web server to understand what kind of response is being requested by the client.

Run the simple **nc [IP] [PORT]** to connect to the remote web-server.

```
nc 10.1.3.32 8090
```

Then, to fetch the flag, tell remote web-server to GET the flag on **`/flag`** directory using HTTP version 1.0 protocol. Not 1.1.

```
GET /flag HTTP/1.0
```

Then hit [**ENTER**], twice.

This will show you the output of the web server's response which shall contain the flag in response upon successful command execution.

Note that, the web server only supports HTTP version 1.0, if you try using http/1.1 the server will throw a 400 error response.

Submit the Flags

Go to **Verify Flags** section on the lab details page, enter the recovered flags in appropriate areas.