rootsh3ll Labs

NetCat Essentials - File Transfer

Objective

TABLE OF CONTENTS

Skip to Flag 1 - Download and save incoming file to secret.txt >>

NetCat is a flexible tool that allows you to chat with remote computers over a peer to peer connection.
Not limited to chats and shell sharing over TCP/UDP, NetCat can also be used to file-transfers over network. File that is not limited by it's type or size.

As a Penetration Tester, you would often face restricted shells or machines where chances of FTP being enabled are very low.
Luckily enough, sometimes SysAdmins forget to disable utilities like NetCat on the compromised machine which can be exploited by you, as a pen-tester, to download sensitive files from remote server.

Perform file sharing (sending/receiving) using NetCat to complete this lab

1. Download and save incoming file to secret.txt
A server (`10.1.3.31`) is trying to send you a file on port `8000`, connect to it using NetCat and save the response as secret.txt in your current directory.

2. Forward received file to a client trying to download the file from you
A remote machine is trying to download secret.txt from you on port `8080`. Allow the remote user to download secret.txt by listening for connection on port `8080`. Upon successful file transfer you'll get a success.txt file on remote machine's root directory

Flag 1 - Download and save incoming file to secret.txt

Objective: Enter the contents of secret.txt received from `10.1.3.31:8000`

Run `netcat` simply with verbose enabled. To save the incoming file into local storage you can use bash redirector operator ">" to redirect the received data into a file named secret.txt.

```
nc -v  10.1.3.31 8000 > secret.txt
```

When the remote client connects to you, NetCat will show you and open connection response as the following

```
netcat_server.lab_11 [10.1.3.31] 8000 (?) open
```

Flag 2 - Forward received file to a client trying to download the file from you.

Objective: Enter IP address of machine that downloaded success.txt from you via port 8080

Opposite to receiving file, we just change 2 things while sending files with NetCat

1. Remove target IP, add listening options (`-l`)
2. Change the direction of bash redirector

Changing direction of Bash redirector operator allows us to READ the file from local storage and send it as STDIN (Standard Input) to the NetCat listener. While listening to the incoming connections, NetCat will send contents of secret.txt to remote client.

```
nc -lvp 8080 < secret.txt
```

If you entered the command correctly, you'll notice a connection open response in NetCat window.

```
connect to [10.1.3.37] from netcat_client.lab_11 [10.1.3.32] 39460
```

Flag 3 - Verify the transferred file

Objective: Connect back to receiver machine's shell on port `8000` and enter the content of success.txt recovered from it's root directory

If the secret.txt is successfully transferred to the remote client, a file named success.txt will be compiled in response to correct data transferred in secret.txt. Connect to the remote server that downloaded secret.txt from you in previous step and locate success.txt

```
nc -v 10.1.3.32 8000
```

After successful connection, run a simple linux command '`ls`' to list the directory content and look for `success.txt`

```
ls
bin
boot
config
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
success.txt
sys
tmp
usr
var
```

If success.txt exists, print the file's content to grab the final flag.

```
cat success.txt
```