NetCat Tool Documentation

This documentation provides instructions on how to use the various capabilities of the NetCat tool. This tool supports sending OS fingerprints, port scanning, executing commands, and setting up command shells.

Basic Usage

To run the NetCat tool, use the following command:

$ python netcat.py [OPTIONS]

Options

- **-c, --command**: Initialize a command shell.
- **-e, --execute**: Execute a specified command.
- **-l, --listen**: Listen on a specified IP and port.
- **-p, --port**: Specify a port (default is 5555).
- **-t, --target**: Specify a target IP (default is 10.0.2.15).
- **-f, --fingerprint**: Send the OS fingerprint to the target and exit.
- **-s, --scan**: Scan specified ports or ranges (comma-separated).

Examples:

The following examples uses 192.168.5.128 as the Target machine, and 192.168.5.129 as the malicious User IP address.

1. Send OS Fingerprint to Target

Description: Send the OS fingerprint from the current machine to a specified target machine.

Steps:

- **Start the listener on the target machine (User Machine):**

$ python netcat.py -t 192.168.5.128 -p 6000 -l

- **Send the fingerprint from the source machine (VM2) to the target machine (VM1):**

$ python netcat.py -t 192.168.5.128 -p 6000 -f

Output on User Machine:

```
Listening...
Received fingerprint:
system: Linux node: vm2
 release: 5.4.0-74-generic version: #83-Ubuntu SMP Wed Jun 2 23:21:25 UTC 2021
 machine: x86_64 processor: x86_64
```

2. Scan Specific Ports

Description: Scan specified ports or ranges on a target machine.

Steps:

- **Scan a list of specific ports:**

$ python netcat.py -t 192.168.5.128 -s 22,80,443

- **Scan a range of ports:**

$ python netcat.py -t 192.168.5.128 -s 20-25,80

Output:

Scanning ports [22, 80, 443] on 192.168.5.128
Port 22: Open
Port 80: Open
Port 443: Open
Time taken: X.XXXX seconds

3. Execute Command on Target

Description: Execute a specified command on a target machine.

Steps:

- **Start the listener on the target machine (User Machine):**

$ python netcat.py -t 192.168.5.128 -p 6000 -l -e "ls"

- **Send a request from VM2 to execute the command:**

$ echo 'Execute command' | python netcat.py -t 192.168.5.128 -p 6000

Output on User Machine:

Listening... bin boot dev etc home ...

4. Command Shell

Description: Initialize a command shell on the target machine.

Steps:

- **Start the listener on the target machine (User Machine):**

  python netcat.py -t 192.168.5.128 -p 6000 -l -c

- **Connect to the command shell from VM2:**

  $ python netcat.py -t 192.168.5.128 -p 6000

Interactive Shell on VM2:

$ type command to execute.

Notes

- Ensure the port number used in the commands is open and not blocked by any firewall or security group.
- The listener must be running before the sender attempts to connect.
- Command shells can be dangerous; use with caution and in secure environments only.
- Always test in a controlled environment to understand the tool's behavior.

This documentation should cover the basic usage and examples of how to use the NetCat tool for various purposes.