# Ashutosh Yadav
# **CISC**
# **Netcat** – Swiss Army Knife Tool



https://github.com/offensivekernel

# Table of Content

- What is Netcat
- Uses of Netcat
- Features of Netcat
- Alternative of Netcat
- Why it's the favorite tool of Hacker
- Demo

# What is Netcat?

- Computer Network Utiltiy
- Network connections using TCP or UDP
- Dependable back-end
- Feature-rich network debugging and investigation tool

# Uses of Netcat

- Netcat can operate in 2 modes:
- **Client Mode**: The client always initiates the connection with the listener. All the errors in client mode are put into the standard error. In client mode, it requires the IP address and port of the listener.
- **Listener Mode**: In this mode, the listener always listens for the connection on a specific port. Its output can be a standard output, file etc. It asks for just listening port.

# Continue....

- Data Transfer
- Create a Backdoor
- Reverse Shell
- Port Scanning
- Port Forwarding
- Network chat
- Banner Grabbing
- secure tunnel

# Is it only for Hackers?

- This utility can used for except Hacking in :-
- Network Analytic
- Debugging
- Investigation

# Features of Netcat

- Outbound or inbound connections, TCP or UDP, to or from any **ports**
- Ability to use any local source port
- **Built**-in port-scanning capabilities
- Optional telnet-options responder
- Tunnel mode
- etc

# Alternative of Netcat

- Some of popular tools and utility are:-
- ncat
- Socat

# Why it's the favorite tool of Hacker

- **All in One**
- Banner grabbing
- Network chatting in Private Network
- Making your own tunnel
- First Priority is continentality of Data under a secure tunnel

# Let's Try some Demo

- Port Scanning
- How to connect to a port
- Network Chat
- File Transfer - file | cmd.exe | terminal
- Secure Shell chat
- Banner Grabbing

# Port Scanning

- **Nc –nvz** (**IP Address**) (**Port Number/Port Range**)
- Nc – Netcat
- **-n** – Unknown host resolve
- **-v** – Verbose Mode
- **-z** – For scan

# How to connect to a port

- After find a open port type this
- **Nc –nv (IP Address) (port number)**
- **-n** for unhost resolve
- **-v f**or verbose mode

# Network Chatting

- Example **Person1(P1)** to chat with **Person2(P2)** Anonymously in his private network
- **P1's (PC)** : **nc –nvlp (Port Number)**
- **Rescan check [nc –nvz (IP) (Port range)]**
- **P2's (PC)** : **nc –nv (P1's IP) (Port number)**
- **Now check it!**

# File Transfer

- What if I saw you not only chat but share your attachment, now look carefully the command
- Make a file in first machine "example1.txt" and in second machine "example2.txt" respectively
- First PC: **nc -nv 192.168.0.147 4000 < example1.txt**
- second PC: **nc -nvlp 4000 > d:\example2.txt**
- **Now look the receiver content and verify it as same as sender**

# File Transfer – command prompt

- **Nc –nvlp 4000** –e(**execution**) cmd.exe - Windows Machine
- **Nc –nv 192.168.0.147 4000 - KaLi Linux** OR **OS**

# File Transfer - Terminal

- First PC: **nc -nvlp 4000** -e **/bin/bash**
- Second PC: **nc -nv 192.168.0.147 4000**

# Secure Shell chat

- First PC: **nc -nvlp 4000 –ssl**
- Filtering the connection to allowed once
- nc -**nvlp 4000** --allow **192.168.0.147**

# Thank you

https://github.com/offensivekernel