

# UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE INSTITUTO METRÓPOLE DIGITAL

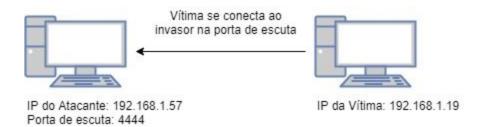
IMD0718 - Forense Computacional Prof. Ramon dos Reis Fontes

Jadson Lucas Gomes Souza

## Simulação de Backdoor

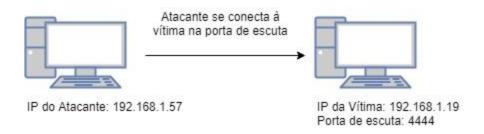
#### Reverse Shell

No lugar de se ligar a uma porta, um reverse shelll se conecta a computador remoto enviando seu shell para um usuário específico. A máquina da vítima atua como um cliente e inicia uma conexão com o servidor de escuta do invasor.



#### **Bind Shell**

O alvo vira o servidor e cria um handler em uma determinada porta aguardando a conexão do explorador. A máquina do atacante atua como um cliente e a máquina da vítima atua como um servidor abrindo uma porta de comunicação na vítima e aguardando o cliente se conectar a ele.



Na prática sugerida o nosso computador atua como o cliente sendo assim estamos falando de um Bind Shell.

### PASSOS DA ATIVIDADE PRÁTICA

No primeiro momento executamos alguns comandos para que os nossos fossem excluídos e tentássemos uma recuperação, como também criamos uma porta suspeita denominada "freedom", "41000":

```
jadson@jadson-pc:/tmp

jadson@jadson-pc:/tmp$ cp /bin/nc/tmp/freedom
cp: falta o operando arquivo de destino após '/bin/nc/tmp/freedom'
Tente "cp --help" para mais informações.
jadson@jadson-pc:/tmp$ cp /bin/nc /tmp/freedom
jadson@jadson-pc:/tmp$ ./freedom -k -w 1 -l 41000 > /dev/null &

[1] 9275
jadson@jadson-pc:/tmp$ rm freedom
jadson@jadson-pc:/tmp$ rm freedom
jadson@jadson-pc:/tmp$
```

Após termos feito isto usamos o comando netstat -nalp para verificarmos as portas suspeitas, uma porta de escuta que não reconhecemos:

```
adson@jadson-pc:/tmp$ netstat -nalp
(Nem todos os processos puderam ser identificados, informações sobre processos
de outrem não serão mostrados, você deve ser root para vê-los todos.)
Conexões Internet Ativas (servidores e estabelecidas)
Proto Recv-Q Send-Q Endereço Local
                                                   Endereço Remoto
                                                                                 Estado
                                                                                                PID/Program name
                    0 127.0.0.53:53
0 127.0.0.1:631
tcp
                                                    0.0.0.0:*
             0
                                                                                 OUÇA
tcp
                                                    0.0.0.0:*
                                                                                 OUCA
             0
                     0 0.0.0.0:41000
                                                    0.0.0.0:*
                                                                                              9275/./freedom
tcp
                                                                                 OUÇA
                                                                                 ESTABELECIDA 2999/chrome --type=
ESTABELECIDA 2999/chrome --type=
             0
                     0 192.168.1.2:41836
                                                    104.244.42.72:443
tcp
                                                    99.80.22.207:443
                     0 192.168.1.2:56766
                     0 192.168.1.2:55314
                                                    104.244.42.195:443
                                                                                 ESTABELECIDA 2999/chrome
```

Verificamos que o seu PID e: 9275

```
jadson@jadson-pc:/tmp$ ls -al /proc/9275
total 0
dr-xr-xr-x 9 jadson jadson 0 out 20 18:44
dr-xr-xr-x 268 root root 0 out 20 15:13 ...
-r--r--r-- 1 jadson jadson 0 out 20 18:49 arch_status
dr-xr-xr-x 2 jadson jadson 0 out 20 18:44 attr
rw-r--r-- 1 jadson jadson 0 out 20 18:49 autogroup
   ----- 1 jadson jadson 0 out 20 18:49 auxv
            1 jadson jadson 0 out 20 18:49 cgroup
            1 jadson jadson 0 out 20 18:49 clear_refs
r--r--r--
            1 jadson jadson 0 out 20 18:44 cmdline
            1 jadson jadson 0 out 20 18:49 comm
- FW- F-- F--
            1 jadson jadson 0 out 20 18:49 coredump filter
            1 jadson jadson 0 out 20 18:49 cpuset
r--r--r--
lrwxrwxrwx 1 jadson jadson 0 out 20 18:46 cwd -> /tmp
            1 jadson jadson 0 out 20 18:49 environ
                                              -> 1/tmp/freedom (deteted)
lrwxrwxrwx
            1 jadson jadson 0 out 20 18:46
dr-x----- 2 jadson jadson 0 out 20 18:44 fd
```

Vimos também que o arquivo /tmp/freedom foi deletado. Agora recuperamos o binário com o comando cp /proc/9275/exe /tmp/recovered bin

Executamos um hash para ver o que corresponde aos binários.

```
jadson@jadson-pc:/tmp$ cp /proc/9275/exe /tmp/recovered_bin
jadson@jadson-pc:/tmp$ sha1sum /bin/nc
142391ab131af2520a0e4a1622643dbfd3057d52 /bin/nc
jadson@jadson-pc:/tmp$ <hash here>
bash: erro de sintaxe próximo ao token inesperado `newline'
jadson@jadson-pc:/tmp$ sha1sum /tmp/recovered_bin
142391ab131af2520a0e4a1622643dbfd3057d52 /tmp/recovered_bin
jadson@jadson-pc:/tmp$ cat /proc/9275/comm
freedom
jadson@jadson-pc:/tmp$ cat /proc/9275/cmdline
./freedom-k-w1-l41000jadson@jadson-pc:/tmp$ strings /proc/9275/environ
SHELL=/bin/bash
SESSION_MANAGER=local/jadson-pc:@/tmp/.ICE-unix/1335,unix/jadson-pc:/tmp/.ICE-unix/1335
QT ACCESSIBILITY=1
COLORTERM=truecolor
XDG CONFIG DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
LANGUAGE=pt_BR:pt:en
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
```

Foi usado tambem o comando ls -al /proc/9275/fd para verificar os malwares

```
jadson@jadson-pc:/tmp$ ls -al /proc/9275/fd
total 0
dr-x----- 2 jadson jadson 0 out 20 18:44 .
dr-xr-xr-x 9 jadson jadson 0 out 20 18:44 ..
lrwx----- 1 jadson jadson 64 out 20 18:44 0 -> /dev/pts/1
l-wx----- 1 jadson jadson 64 out 20 18:44 1 -> /dev/null
lrwx----- 1 jadson jadson 64 out 20 18:44 2 -> /dev/pts/1
lrwx----- 1 jadson jadson 64 out 20 18:44 2 -> /dev/pts/1
```

```
jadson@jadson-pc:/tmp$ cp /proc/9275/exe /tmp/recovered_bin
adson@jadson-pc:/tmp$ sha1sum /bin/nc
L42391ab131af2520a0e4a1622643dbfd3057d52 /bin/nc
adson@jadson-pc:/tmp$ <hash here>
pash: erro de sintaxe próximo ao token inesperado `newline'
adson@jadson-pc:/tmp$ sha1sum /tmp/recovered_bin
L42391ab131af2520a0e4a1622643dbfd3057d52 /tmp/recovered_bin
jadson@jadson-pc:/tmp$ cat /proc/9275/comm
freedom
jadson@jadson-pc:/tmp$ cat /proc/9275/cmdline
./freedom-k-w1-l41000jadson@jadson-pc:/tmp$ strings /proc/9275/environ
SHELL=/bin/bash
SESSION_MANAGER=local/jadson-pc:@/tmp/.ICE-unix/1335,unix/jadson-pc:/tmp/.ICE-unix/1335
T_ACCESSIBILITY=1
OLORTERM=truecolor
KDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
KDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
_ANGUAGE=pt_BR:pt:en
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
(MODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=1274
GTK_MODULES=gail:atk-bridge
PWD=/tmp
_OGNAME=jadson
(DG_SESSION_DESKTOP=ubuntu
KDG SESSION TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
KAUTHORITY=/run/user/1000/gdm/Xauthority
VINDOWPATH=2
HOME=/home/jadson
JSERNAME=jadson
```

```
jadson@jadson-pc:/tmp$ cat /proc/9275/stack
cat: /proc/9275/stack: Permissão negada
jadson@jadson-pc:/tmp$
```