UFRN

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE INSTITUTO METRÓPOLE DIGITAL

IMD0718 - Forense Computacional

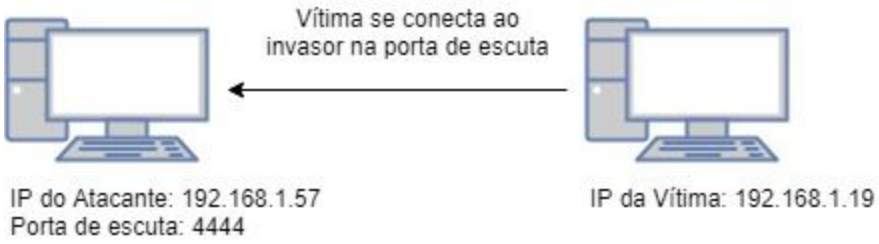
Prof. Ramon dos Reis Fontes

Jadson Lucas Gomes Souza

Simulação de Backdoor

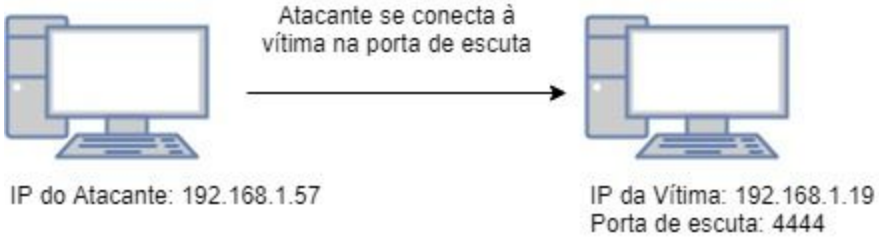
Reverse Shell

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.

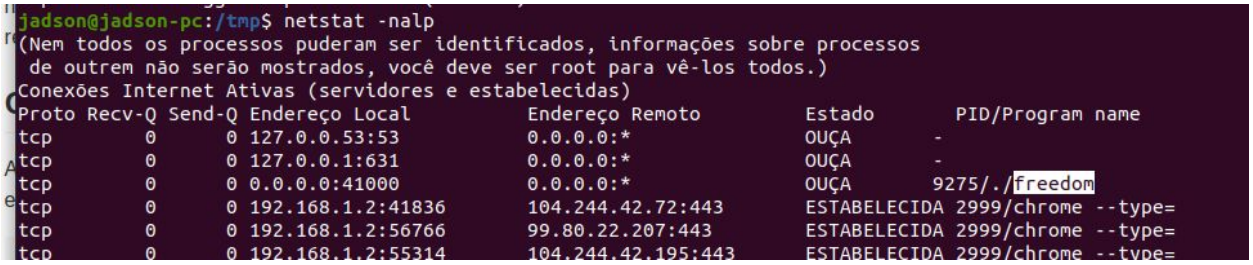


Na prática sugerida o nosso computador atua como o cliente sendo assim estamos falando de um Bind Shell.

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”:

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



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
-r--------   1 jadson jadson 0 out 20 18:49 auxv
-r--r--r--   1 jadson jadson 0 out 20 18:49 cgroup
--w-------   1 jadson jadson 0 out 20 18:49 clear_refs
-r--r--r--   1 jadson jadson 0 out 20 18:44 cmdline
-rw-r--r--   1 jadson jadson 0 out 20 18:49 comm
-rw-r--r--   1 jadson jadson 0 out 20 18:49 coredump_filter
-r--r--r--   1 jadson jadson 0 out 20 18:49 cpuset
lrwxrwxrwx   1 jadson jadson 0 out 20 18:46 cwd -> /tmp
-r--------   1 jadson jadson 0 out 20 18:49 environ
lrwxrwxrwx   1 jadson jadson 0 out 20 18:46 exe -> '/tmp/freedom (deleted)'
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 3 -> 'socket:[77202]'
```

```
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
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=1274
GTK_MODULES=gail:atk-bridge
PWD=/tmp
LOGNAME=jadson
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
WINDOWPATH=2
HOME=/home/jadson
USERNAME=jadson
```

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