**Informe de Actividades - Máquina CTF "Death Note"**

**Resumen:**

En este informe, se detallan las actividades realizadas durante el proceso de ataque a la máquina CTF "Death Note" con el objetivo de obtener privilegios root. A continuación, se presenta un resumen de las acciones llevadas a cabo:

1. **Escaneo de Puertos:**

Se realizó un escaneo Nmap para identificar los puertos abiertos en la máquina. Se encontraron los siguientes resultados:

* Puerto 22/tcp: Abierto, servicio SSH (OpenSSH 7.9p1 Debian 10+deb10u2).
* Puerto 80/tcp: Abierto, servicio HTTP (Apache httpd 2.4.38).

***Comandos:***

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

1. **Enumeración de Directorios con Gobuster:**

**Escaneo 1 - http://192.168.20.27/:**

* /index.html: Estado 200 (OK), Tamaño: 197 bytes.
* /.html: Estado 403 (Prohibido), Tamaño: 278 bytes.
* /wordpress: Estado 301 (Movido permanentemente), Redirección a http://192.168.20.27/wordpress/.
* /manual: Estado 301 (Movido permanentemente), Redirección a http://192.168.20.27/manual/.
* /robots.txt: Estado 200 (OK), Tamaño: 68 bytes.
* /.php: Estado 403 (Prohibido), Tamaño: 278 bytes.
* /server-status: Estado 403 (Prohibido), Tamaño: 278 bytes.

***Comandos:***

* ***gobuster dir -u http://<IP>/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt***

**Escaneo 2 - http://deathnote.vuln/wordpress/:**

* /.html: Estado 403 (Prohibido), Tamaño: 279 bytes.
* /.php: Estado 403 (Prohibido), Tamaño: 279 bytes.
* /wp-content: Estado 301 (Movido permanentemente), Redirección a http://deathnote.vuln/wordpress/wp-content/.
* /index.php: Estado 301 (Movido permanentemente), Redirección a http://deathnote.vuln/wordpress/.
* /license.txt: Estado 200 (OK), Tamaño: 19,915 bytes.
* /wp-includes: Estado 301 (Movido permanentemente), Redirección a http://deathnote.vuln/wordpress/wp-includes/.
* /wp-login.php: Estado 200 (OK), Tamaño: 6,799 bytes.
* /readme.html: Estado 200 (OK), Tamaño: 7,346 bytes.
* /wp-trackback.php: Estado 200 (OK), Tamaño: 135 bytes.
* /wp-admin: Estado 301 (Movido permanentemente), Redirección a http://deathnote.vuln/wordpress/wp-admin/.
* /xmlrpc.php: Estado 405 (Método no permitido), Tamaño: 42 bytes.
* /.php: Estado 403 (Prohibido), Tamaño: 279 bytes.
* /.html: Estado 403 (Prohibido), Tamaño: 279 bytes.
* /wp-signup.php: Estado 302 (Encontrado), Redirección a http://deathnote.vuln/wordpress/wp-login.php?action=register.

***Comandos:***

* ***gobuster dir -u http://deathnote.vuln/wordpress/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt***

1. **Configuración del dominio "deathnote.vuln":**

Se agregó la entrada "192.168.20.27 deathnote.vuln" en el archivo /etc/hosts para asociar el dominio con la dirección IP de la máquina.

***Comandos:***

* ***nano /etc/host***

1. **Análisis del archivo robots.txt:**

El archivo robots.txt reveló información adicional:

Contenido: "fuck it my dad\nadded hint on /important.jpg\nryuk please delete it".

Descargamos el archivo /important.jpg

***Comandos:***

* ***Wget http://<IP>/important.jpg***

1. **Análisis del archivo important.jpg:**

Al leer el archivo important.jpg, se descubrió que era un archivo de texto en formato ASCII.

Contenido:

"i am Soichiro Yagami, light's father\ni have a doubt if L is true about the assumption that light is kira\ni can only help you by giving something important\nlogin username : user.txt\ni don't know the password. find it by yourself\nbut i think it is in the hint section of the site".

El contenido revela que la persona que escribe el mensaje es Soichiro Yagami, el padre de Light. Además, expresa dudas sobre la veracidad de la suposición de L de que Light es Kira. Sin embargo, lo más importante es la información relacionada con un inicio de sesión.

Se menciona que hay un archivo llamado user.txt, que probablemente contenga el nombre de usuario necesario para iniciar sesión, pero no se conoce la contraseña. Se sugiere buscarla en la sección de pistas del sitio.

***Comandos:***

* ***file important.jpg***
* ***cat important.jpg***

1. **Acceso al directorio /wordpress:**

En la pestaña /HINT. Encontramos información interesante. Aquí está el contenido relevante:

"Encuentra un archivo notes.txt en el servidor" - Esta pista indica que hay un archivo llamado notes.txt en el servidor que puede contener información relevante para avanzar en el desafío.

"SEE the L comment" - Esta pista sugiere que debes prestar atención al comentario relacionado con L. Es posible que contenga información valiosa.

"mi línea favorita es iamjustic3" - Esta frase indica que la línea favorita es "iamjustic3". Puede ser útil recordar esta información para su uso posterior.

"L on i will eliminate you L!" - Esta línea menciona a L y sugiere que él eliminará a alguien. Podría tener alguna relación con el desafío.

1. **Análisis de la página /wordpress/wp-login.php y el panel de administración de WordPress**

**Usuario "Kira" en el panel de inicio de sesión de WordPress:** Has descubierto que hay un usuario con el nombre "Kira" en el panel de inicio de sesión de WordPress.

**Inicio de sesión exitoso:** Pudiste iniciar sesión con el usuario "Kira" y la contraseña "iamjustic3".

**Análisis del panel de administración de WordPress:** Al intentar colocar una reverseshell en los templates de PHP, encontraste errores. Luego, exploraste la biblioteca y encontraste un archivo llamado notes.txt. Intentaste descargar este archivo utilizando el comando wget y la URL proporcionada en la página.

**Archivo notes.txt:** El contenido del archivo notes.txt parece ser una lista de contraseñas.

**Creamos archivo users.txt:** Considerando los usuarios que has encontrado en la página, como "l", "kira", "user.txt", "Soichiro", "Yagami", puedes utilizar el archivo de contraseñas para intentar encontrar coincidencias y así acceder a otros usuarios o recursos dentro del sistema.

***Comandos:***

* ***wget http://<IP>/notes.txt***

1. **Fuerza Bruta con Hydra**

**Resultados**

Host: 192.168.20.27

Usuario: l

Contraseña: death4me

***Comandos:***

* ***hydra -L users.txt -P notes.txt ssh://<IP> -I***

1. **Acceso a la Maquina Death Note**

Logramos entrar con ssh con las credenciales que obtuvimos en el paso anterior

***Comandos:***

* ***ssh l@<IP>***

1. **Escalación de Privilegios de Usuario**

Estuvimos enumerando con sudo -l buscando archivos con privilegios root, y hasta con linpeas para escalar privilegios pero no logramos encontrar nada, entonces realizamos búsquedas de archivos con el comando find y encontramos lo siguiente:

**Directorio /opt/L/kira-case:** Encontramos un directorio llamado "kira-case" dentro de "/opt/L". En este directorio, hay un archivo llamado "case-file.txt" con el siguiente contenido:

the FBI agent died on December 27, 2006

1 week after the investigation of the task-force member/head.

aka.....

Soichiro Yagami's family .

hmmmmmmmmm......

and according to watari ,

he died as other died after Kira targeted them .

and we also found something in

fake-notebook-rule folder .

Este archivo proporciona información sobre la muerte de un agente del FBI y la relación con Soichiro Yagami y las personas que Kira ha atacado, además nos menciona sobre un folder fake-notebook-rule.

**Directorio relacionado con "fake-notebook-rule":** Luego de buscar en ese directorio, encontraste dos archivos: case.wav y hint

**case.wav:** Has leído el contenido de este archivo utilizando el comando "cat". Parece ser una secuencia de caracteres hexadecimales: "63 47 46 7a 63 33 64 6b 49 44 6f 67 61 32 6c 79 59 57 6c 7a 5a 58 5a 70 62 43 41 3d".

**hint:** También has leído el contenido de este archivo utilizando el comando "cat". El contenido es la palabra "cyberchef".

Luego, has utilizado la herramienta "CyberChef" y la función "From Hex" para decodificar la secuencia hexadecimal en el archivo case.wav. El resultado fue "cGFzc3dkIDoga2lyYWlzZXZpbCA=". Utilizando el comando "echo "cGFzc3dkIDoga2lyYWlzZXZpbCA=" | base64 -d", has obtenido la contraseña "kiraisevil".

Finalmente, has utilizado las credenciales "kira" y "kiraisevil" para conectarte a la máquina CTF "Death Note" como el usuario "kira".

***Comandos:***

* ***find / -name kira 2>/dell/null***
* ***cat case.wav***
* ***cat hint***
* ***echo "cGFzc3dkIDoga2lyYWlzZXZpbCA=" | base64 -d***

1. **Escalacion Privilegios ROOT**

Con sudo -l vemos que el usuario tiene todos los privilegios

**(ALL : ALL) ALL**

Y por ello solo basta en colocar sudo su para obtener los privilegios de root

***Comandos:***

* ***su root***

**Conclusiones:**

En este informe, se detallaron las actividades llevadas a cabo para obtener privilegios root en la máquina CTF "Death Note". A través del escaneo de puertos, la enumeración de directorios, la búsqueda de pistas y archivos, el análisis de credenciales y la escalación de privilegios, se logró obtener el acceso como root.

**Se destacan los siguientes hallazgos significativos:**

* Descubrimiento de pistas y directorios relacionados con "kira" y "fake-notebook-rule".
* Obtención de credenciales para el usuario "kira" y escalación de privilegios a root.

**Recomendaciones:**

* Documentar y registrar todas las actividades realizadas, incluyendo comandos utilizados, resultados obtenidos y cualquier información relevante.
* Seguir las mejores prácticas de seguridad y ética durante el proceso de ataque y explotación.
* Mantener la integridad y confidencialidad de la máquina CTF "Death Note" y sus datos.