**Informe Profesional de la Máquina CTF**

**"Hacker de Recompensas"**

**Introducción:**

El presente informe detalla los pasos y hallazgos clave durante la exploración y resolución del desafío de la máquina CTF denominada "Hacker de Recompensas". A continuación, se presenta un resumen de los seis puntos principales que condujeron a la finalización exitosa del CTF.

1. **Escaneo de Nmap:**

Se llevó a cabo un escaneo de Nmap en la dirección IP objetivo, 10.10.132.192, revelando los siguientes puertos abiertos:

* Puerto 21/tcp: Servicio FTP.
* Puerto 22/tcp: Servicio SSH.
* Puerto 80/tcp: Servicio HTTP.

***Comandos:***

* ***nmap -A <ip>***
* ***nmap -sS -sV <ip>***

1. **Investigación del servicio FTP:**

Accediendo al servicio FTP con el usuario "anonymous", se descubrieron dos archivos: "locks.txt" y "task.txt". Estos archivos proporcionaron información valiosa para avanzar en el desafío.

***Comandos:***

* ***ftp <ip>***

**Contenido del archivo "locks.txt":**

El archivo "locks.txt" contenía una lista de posibles contraseñas, las cuales podrían ser empleadas en diferentes contextos dentro del CTF. Estas contraseñas se consideraron relevantes para progresar en el desafío.

**Contenido del archivo "task.txt":**

El archivo "task.txt" reveló dos tareas a cumplir: proteger a Vicious y planificar una recogida en la luna relacionada con Red Eye. Estas tareas ofrecieron pistas sobre el objetivo del desafío y la dirección a seguir.

1. **Descubrimiento de usuarios en el servicio HTTP:**

A través de la exploración del servicio HTTP en la dirección "http://10.10.132.192", se encontró varios mensajes con los nombres de los usuarios. Esta información resultó relevante para la siguiente etapa del CTF.

1. **Fuerza bruta en el servicio SSH y Acceso con SSH:**

Utilizando los nombres de usuario encontrados y el archivo "locks.txt", se realizó un ataque de fuerza bruta mediante Hydra al servicio SSH. Se logró acceder exitosamente a la cuenta de usuario "lin" utilizando la contraseña "RedDr4gonSynd1cat3".

***Comandos:***

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

1. **Escalada de privilegios:**

Se identificó que el usuario "lin" tenía permisos de ejecución para el comando "/bin/tar" como root. Aprovechando esta configuración, se ejecutó el comando "sudo tar" para obtener una shell como root y así escalar privilegios.

***Comandos:***

***sudo -l***

***sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh***

**Conclusiones:**

Mediante la realización de los pasos mencionados anteriormente, se logró completar exitosamente el desafío "Hacker de Recompensas" en la máquina CTF. El acceso a la máquina se obtuvo mediante el descubrimiento de usuarios en el servicio HTTP, seguido de una fuerza bruta exitosa en el servicio SSH. A través de estos logros, se adquirió control y acceso a la máquina objetivo.

Cabe destacar que todas las acciones realizadas se llevaron a cabo dentro de un entorno de CTF legítimo, con el consentimiento correspondiente y siguiendo las prácticas de seguridad y ética adecuadas.

**Recomendaciones:**

* Continuar mejorando las habilidades de enumeración y escaneo de puertos.
* Implementar contraseñas más sólidas y seguras para los servicios.
* Mantenerse actualizado sobre las técnicas de escalada de privilegios y la protección de sistemas.