HACKTHEBOX

Informe Técnico

Máquina Preignition

Dirección IP: 10.129.69.80
Dificultad: Very easy
Creador: Nombre

30 de mayo del 2022

Índice

1. Antecedentes

El presente documento está escrito a modo de guía o referencia para todas aquellas personas que quieran hacer la máquina **Preignition** de la plataforma **Hack The Box**. Cabe aclarar que la manera en la que yo resolví la máquina no es la definitiva, esto es sólo una referencia que les puede ser de ayuda en caso de que la necesiten.

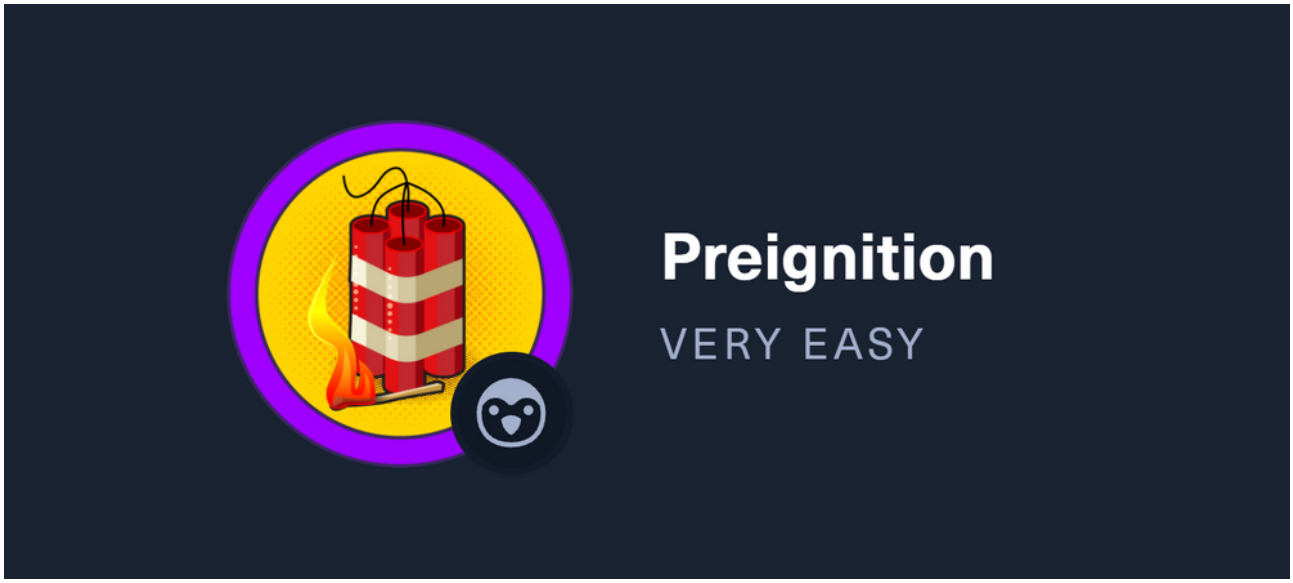

Figura 1: Máquina Preignition

Dirección URL

https://app.hackthebox.com/starting-point

2. Objetivos

Comprometer la máquina **Preignition** con el fin de llegar a ser el usuario con máximos privilegios utilizando técnicas de reconocimiento, escaneo, enumeración, análisis de vulnerabilidades, explotación y post-explotación.

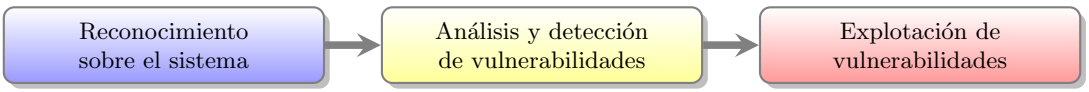

Figura 2: Flujo de trabajo

3. Análisis de Vulnerabilidades

3.1. Reconocimiento Inicial

Se comenzó realizando una análisis inicial sobre el sistema, verificando que el sistema objetivo se encontrara accesible desde el segmento de red en el que se opera a través del comando *ping*:

```
user@bash:~$ ping -c 1 10.129.69.80
PING 10.129.69.80 (10.129.69.80) 56(84) bytes of data.
64 bytes from 10.129.69.80: icmp_seq=1 ttl=63 time=58.5ms

--- 10.129.69.80 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 58.472/58.472/58.472/0.000 ms

```

Código 1: Reconocimiento inicial sobre la máquina víctima

3.2. Fase de escaneos

Una vez verificada la conectividad con la máquina víctima, se realizó un escaneo haciendo uso de la herramienta **nmap** para la detección de puertos abiertos, obteniendo los siguientes resultados:

```
user@bash:~$ nmap -p- -sS --min-rate 5000 --open -n -vvv -Pn 10.129.69.80 -oG allPorts

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Nmap scan report for 10.129.69.80
Host is up, received user-set (0.16s latency).
Scanned at 2021-12-13 16:01:07 CST for 129s
Not shown: 52946 filtered tcp ports (no-response), 12588 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 129.00 seconds
           Raw packets sent: 124779 (5.490MB) | Rcvd: 12591 (503.652KB)

```

Código 2: Escaneo de puertos a la máquina víctima

Con este escaneo lo que estamos efectuando es un escaneo de tipo TCP SYN Port a todo el rango de puertos (1-65535) en la máquina víctima (10.129.69.80)

- **-p-:** Rango de puertos 1-65535
- **-sS:** TCP SYN Scan
- **–min-rate <# de paquetes por segundo>:** Le indicamos el número mínimo de paquetes que queremos enviar por segundo.
- **–open:** Filtramos por puertos abiertos
- **-n:** Para que no aplique resolución DNS
- **-vvv:** Para que nos muestre por consola los puertos abiertos a medida que los va encontrando
- **-Pn:** Para que no haga descubrimiento de hosts a través del protocolo ARP (resolución de direcciones)

En esta ocasión, el único puerto abierto que fue descubierto fue el puerto 80. Como bien sabemos el servicio que corre en este puerto es el HTTP. Para saber el nombre y la versión de dicho servicio, ejecutaremos el siguiente escaneo:

```
user@bash:~$ nmap -sC -sV -p80 10.129.69.80

Nmap scan report for 10.129.69.80
Host is up (0.060s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Welcome to nginx!

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.15 seconds

```

Código 3: Escaneo para detectar versión y servicio de los puertos abiertos

Con este escaneo lo que realizamos es lanzar una serie de scripts básicos de reconocimiento a la vez de scripts para la detección del nombre y versión del servicio que está corriendo sobre el puerto que le especificamos, en este caso, el puerto 80.

- **-sC:** Serie de scripts básicos de reconocimiento
- **-sV:** Scripts para detectar la versión y el servicio que corre para los puertos especificados
- **-p:** Especificamos el/los puerto/s que queremos escanear

3.3. Enumeración

El servicio como ya habíamos dicho antes es el HTTP y, como podemos ver, la versión es **nginx 1.14.2**

Una vez que tenemos esto y sabemos que está corriendo un servidor web, lo primero que podemos hacer es visitar el sitio web a través de nuestro navegador. Para esto en el apartado de la URL pondremos la dirección ip de la máquina seguido de *":"* y el puerto 80. Tal como se muestra en la siguiente imagen:

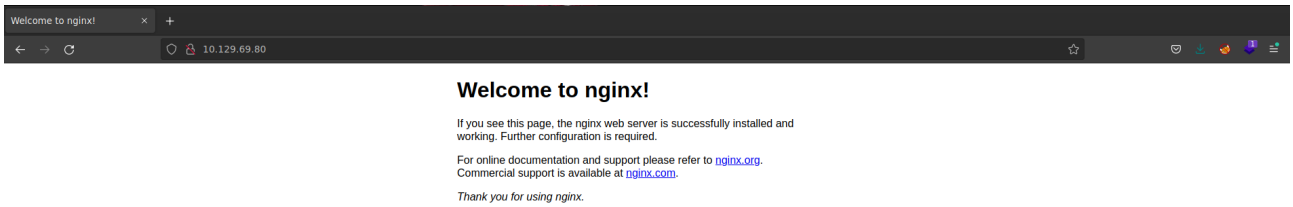

Figura 3: Servidor web visto desde el navegador

De esta manera podemos ver ante lo que estamos y cómo es que se nos muestra

Lo que haremos a continuación se conoce como *fuzzing*, consiste en buscar a través de un ataque de diccionario recursos existentes en el servidor, ya sean directorios o archivos.

Para esto, en esta ocasión utilizaremos la herramienta *GoBuster*, herramienta programada en Go hecha para realizar este tipo de tareas. El comando a ejecutar será el siguiente:

```
user@bash:~$ gobuster dir -u http://10.129.69.80 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.162.94/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/12/13 17:15:19 Starting gobuster in directory enumeration mode
===============================================================
/admin.php            (Status: 200) [Size: 999]

===============================================================
2021/12/13 17:15:48 Finished
===============================================================

```

Código 4: Uso básico de GoBuster

- **dir:** Se pone en modo de enumeración de directorio/archivos
- **-u:** Especificamos URL
  - *http://10.129.69.80*
- **-w:** Proporcionamos diccionario a usar
  - */usr/share/wordlists/dirb/common.txt*

Como podemos darnos cuenta, la herramienta es muy visual y podemos identificar rápidamente los directorios y archivos encontrados. En este caso podemos ver como la herramienta encontró el archivo ***/admin.php***.

Al probarlo en nuestro navegador se nos muestra lo siguiente:

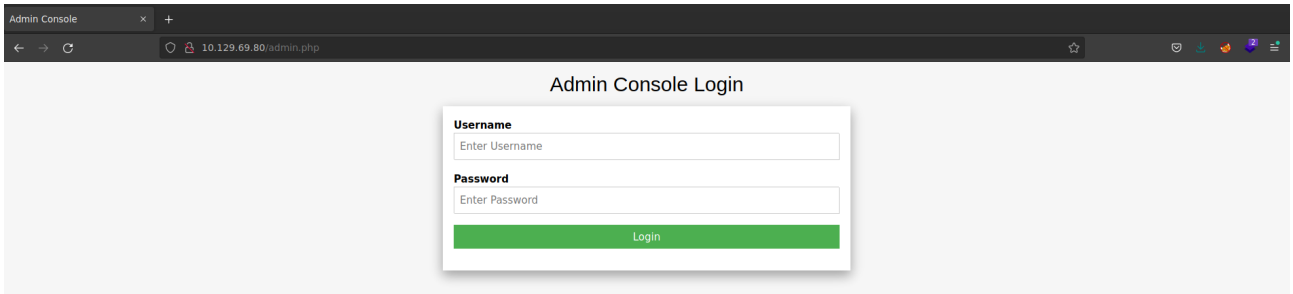

Figura 4: Panel de admin en /admin.php

Procedemos a probar credenciales comúnes o genéricas, por ejemplo:

- admin:admin
- root:root
- guest:guest
- root:password
- admin:password

Probando, nos damos cuenta que el usuario: *admin* y la contraseña: *admin* son válidas. Una vez logramos acceder, nos muestra automáticamente la flag necesaria para indicarle a HTB que hemos terminado:

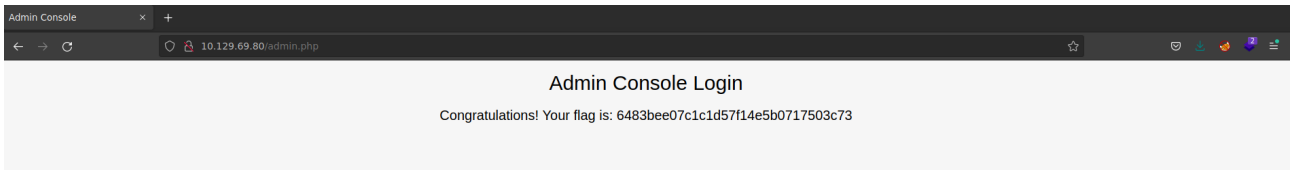

Figura 5: Flag de HTB

La verdad es una máquina muy sencilla, no hace falta quebrarnos la cabeza.

A continuación les dejaré el link del video de mi canal de YouTube en el que resuelvo la máquina:

Walkthrough: Hack The Box - Starting Point - Máquina Preignition (very easy)

4. Créditos

Autor: Arturo Cantú (aka 4rtii)

Inspirado en: Marcelo Vázquez (aka s4vitar): Cómo crear un reporte profesional en LaTeX

Sitio Web: 4rtii.github.io

YouTube: 4rtii

Twitch: 4rtii

GitHub: 4rtii

Hack The Box: 4rtii