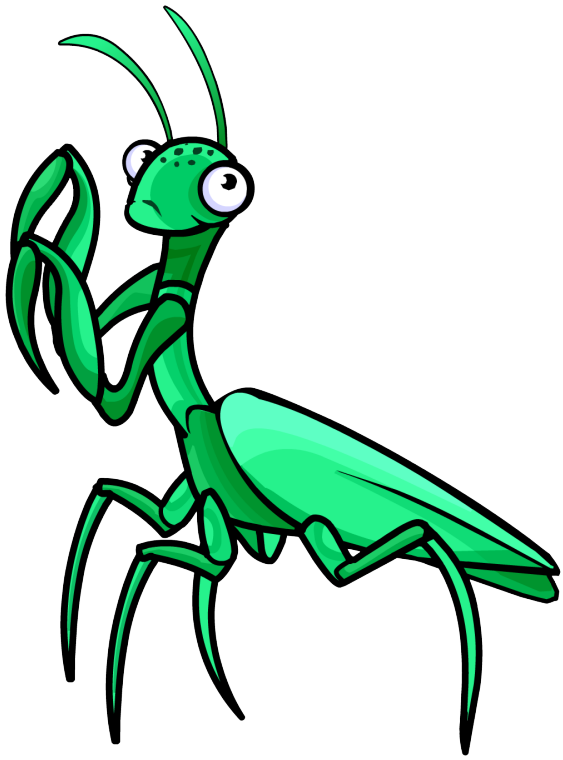
Hack The Box
PEN-TESTING LABS

Informe Técnico

Máquina Mantis



18 de Juunio de 2022

Indice

1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase de auditoría de la maquina **Mantis** de la plataforma **HackTheBox**.

Imagen 1: Detalles de la maquina

Dirección URL

https://hackthebox.es/home/machines/profile/98

2. Objetivos

Conocer el estado de seguridad del servidor **Mantis**, enumerando posibles vectores de explotyación y determinando el alcance e impacto que un atacante podría ocasionar sobre el sistema en producción.

2.1. Consideraciones

Una vez finalizadas las jornadas de auditoría, se llevará a cabo una fase de saneamientos y buenas practicas con el objetivo de securizar el servidor y evitar ser víctimas de un futuro ataque en base a los vectores explotados.

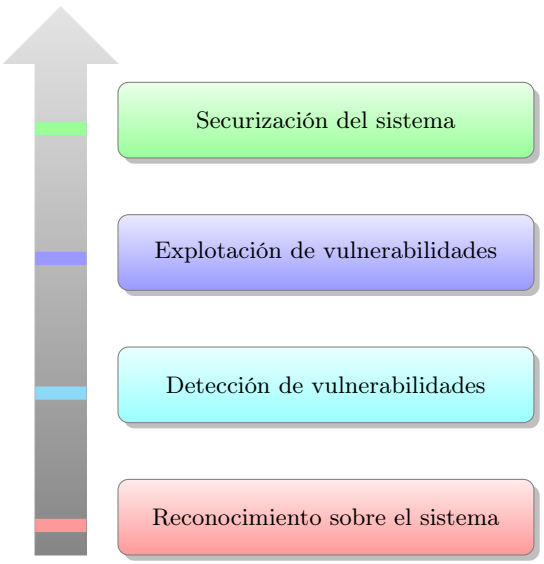


Imagen 2: Flujo de trabajo

3. Análisi de vulnerabilidades

3.1. Reconocimiento inicial

Se comenzó realizando un analisis inicial sobre el sistema, verificando que el sistema objetivo se encontrara accesible desde el segmento de red en el que se opera.

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 300

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.1.1     52:54:00:12:35:00      1      60  Unknown vendor
192.168.1.2     52:54:00:12:35:00      1      60  Unknown vendor
192.168.1.3     08:00:27:86:2f:1e      2     120  PCS Systemtechnik GmbH
192.168.1.104   08:00:27:28:8f:62      1      60  PCS Systemtechnik GmbH

root@kali:~# netdiscover -r 192.168.1.0/24
```

Imagen 3: Reconocimiento inicial sobre el sistema objetivo

Una vez localizado se realizó un escaneo nmap a traves de la herramienta **nmap** para la detección de puertos abiertos, obteniendo los siguientes resultados:

```
~/Documents/HTB/Starting-Point/Vaccine
❯ cat nmap.out
# Nmap 7.91 scan initiated Fri Jan 22 10:47:23 2021 as: nmap -sC -sC --top-ports 1000 -o nmap.out 10.10.10.46
Nmap scan report for 10.10.10.46
Host is up (0.026s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
| ssh-hostkey:
|   3072 c0:ee:58:07:75:34:b0:0b:91:65:b2:59:56:95:27:a4 (RSA)
|   256 ac:6e:81:18:89:22:d7:a7:41:7d:81:4f:1b:b8:b2:51 (ECDSA)
|_  256 42:5b:c3:21:df:ef:a2:0b:c9:5e:03:42:1d:69:d0:28 (ED25519)
80/tcp open  http
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: MegaCorp Login

# Nmap done at Fri Jan 22 10:47:25 2021 -- 1 IP address (1 host up) scanned in 2.83 seconds
```

Imagen 4: Reconocimiento inicial sobre el sistema objetivo

Asimismo, con el objetivo de evitar falsos positivos, se diseñó un script en **Bash** para enumerar posibles puertos adiccionales que la herramienta nmap no llegara a detectar:

```
#!/bin/Bash

for port in $(seq 1 65535); do
    timeout 1 bash -c "echo > /dev/tcp/10.10.10.52/$port" > /dev/null && echo "$port/tcp"
&
done; wait


```

Código 1: Script personalizado para la enumeración de puertos

A través de este script, fue posible detectar puertos addiconalmente abiertos:

TCP

Puertos
593, 1337

Una vez finalizada la fase de enumertación de puertos, se detectaron los servicios y versiones que corrian bajo estos, representando a continuación los mas significativos bajo los cuales fue posiblñe explotar el sistema:

```
~/Documents/HTB/Starting-Point/Vaccine
❯ cat nmap.out
# Nmap 7.91 scan initiated Fri Jan 22 10:47:23 2021 as: nmap -sC -sC --top-ports 1000 -o nmap.out 10.10.10.46
Nmap scan report for 10.10.10.46
Host is up (0.026s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
| ssh-hostkey:
|   3072 c0:ee:58:07:75:34:b0:0b:91:65:b2:59:56:95:27:a4 (RSA)
|   256 ac:6e:81:18:89:22:d7:a7:41:7d:81:4f:1b:b8:b2:51 (ECDSA)
|_  256 42:5b:c3:21:df:ef:a2:0b:c9:5e:03:42:1d:69:d0:28 (ED25519)
80/tcp open  http
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: MegaCorp Login

# Nmap done at Fri Jan 22 10:47:25 2021 -- 1 IP address (1 host up) scanned in 2.83 seconds
```

Imagen 5: Enumeración de servicios y versiones

Tal y como se aprecia en la figura 5 de la página 5 es posible identificar que se trata de una máquina con **Directorio Activo** configurado.