

Informe Tecnico.

Maquina Cheese



Este documento es confidencial y contiene informacion sensible.
Esta informacion no deberia compartirse con terceros.



Índice

1. Antecedentes	2
2. Objetivos	2
2.1. Consideraciones	2
3. Reconocimiento del sistema.	3
3.1. Reconocimiento Inicial.	3
4. Explotacion de vulnerabilidades.	4
4.1.Codigo de panel vulnerable a ataque de Inyeccion SQL	4



1. Antecedentes

El presente documentos recoge los resultados de la auditoria realizad a la maquina **Cheese** de la plataforma [TryHackme](#).



c3lis 1: Detalles de la maquina.

Url

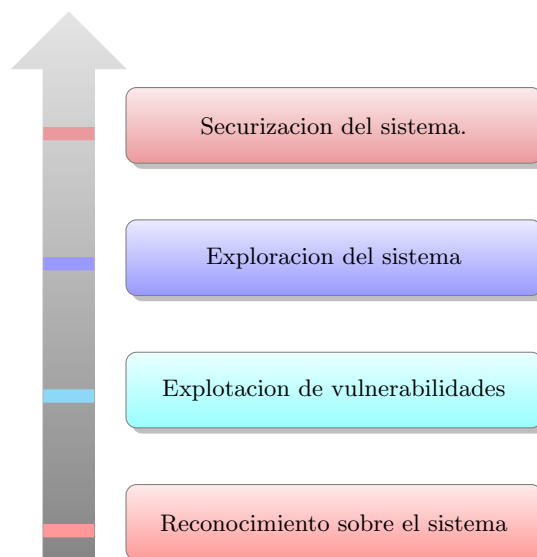
<https://tryhackme.com/r/room/cheesectfv10>

2. Objetivos

Conocer el estado de actual de el servidor de **Cheese**, enumerando posibles vectores de explotacion y determinando el alcance de impacto, que un atacante podria ocasionar en un sistema en produccion.

2.1. Consideraciones

Una vez finalizada las jornadas de auditoria se llevara a cabo un serie de saneamientos y buenas practicas con el objetivo de securizar el servidor he evitar ser victima de un futuro ataque.





3. Reconocimiento del sistema.

3.1. Reconocimiento Inicial.

Se comenzo realizando un analisis inicial sobre el sistema verificando que el sistema oobjetivo que puertos tiene abiertos.

```
Nmap scan report for 10.10.118.129
Host is up (0.35s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
4444/tcp  open|filtered krb524

# Nmap done at Sat Oct  5 21:56:57 2024 -- 1 IP address (1 host up)
```

c3lis 2: Reconocimiento de puertos abiertos por el servidor.

Asi mismo para evitar ciertos falsos positivos se construyo en bash un script en bash para verificar con exactitud la cantidad de puertos abiertos en el servidor.

codigo 1: Script

```
#!/bin/bash

for por in $(seq 1 6555);do
    time out 1 bash -c "echo _>_/_/dev/tcp/10.10.118.129/$port" >/dev/null && echo $?
done; wait
```

A travez del anterior script es posible detectar los siguientes puertos.

TCP
Puertos
22, 80, 4444

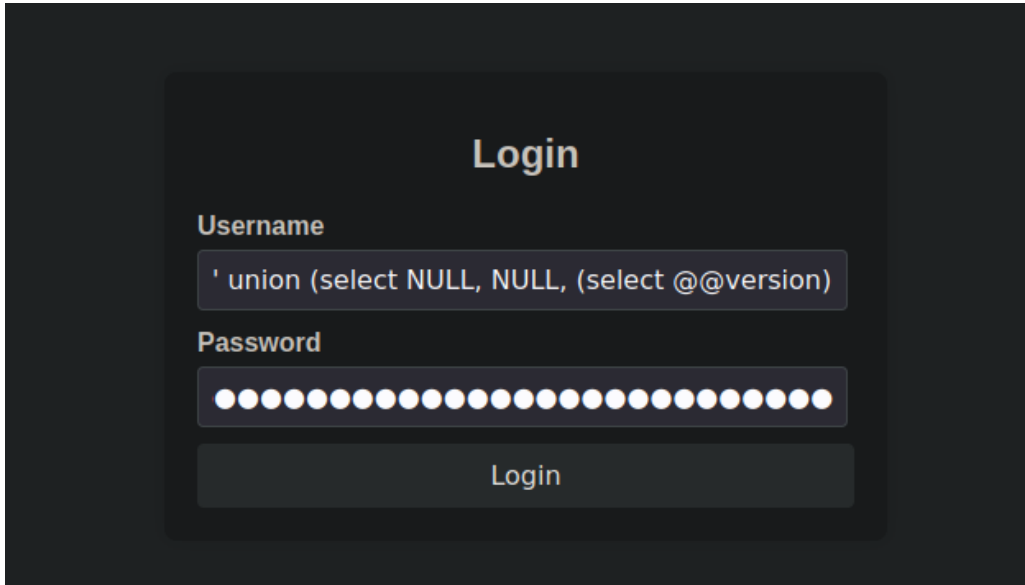
Una vez finalizado el escaneo se detectaron la version y servicio que corrian bajo estos, representando a continuacion los puertos criticos los cuales fueron la continuidad a la explotacion del sistema.



4. Explotacion de vulnerabilidades.

4.1. Codigo de panel vulnerable a ataque de Inyeccion SQL

Posteriormente se empezo con el analisis de rutas existente por parte del puerto **80=HTTP** descubriendo que era susceptible a una ataque de inyeccion **SQL**.



The image shows a dark-themed web application interface with a 'Login' form. The form has two input fields: 'Username' and 'Password'. The 'Username' field contains the SQL injection payload: `' union (select NULL, NULL, (select @@version))`. The 'Password' field is filled with 20 white dots. Below the fields is a 'Login' button.