

## INDICE

|   |    |
|---|----|
| INTRODUCCIÓN.....   | 2  |
| ¿Que es legion?.....  | 2  |
| Características.....  | 2  |
| PRIMEROS PASOS.....   | 2  |
| Instalación.....  | 2  |
| Ejecución.....  | 3  |
| Aregar Objetivos.....   | 3  |
| ESCANEO DE OBJETIVOS.....   | 4  |
| Selección de opciones (Banderas nmap).....                                | 4  |
| 1. Selección de objetivos.....  | 5  |
| 2. Selección de modo.....   | 5  |
| 3. Opciones modo facil.....   | 5  |
| 4. Opciones de tiempo y rendimiento ( -T ).....                           | 7  |
| 5. Opciones de escaneo de puertos ( -sT -sS -sF -sN -sX -sP -sU -f )..... | 8  |
| 6. Opciones de detección de host (-Pn -PB -PE -PT -PS -PP -PM ).....      | 9  |
| 7. Opciones personalizadas.....   | 10 |
| COMPRENSIÓN DE LA INTERFAZ Y RESULTADOS.....                              | 10 |
| Pestañas.....   | 11 |
| Services:.....  | 11 |
| Scrips:.....  | 12 |
| Information:.....   | 13 |
| CVE'S:.....   | 14 |
| Notas:.....   | 15 |
| Otras Pestañas:.....  | 15 |
| Mas opciones de escaneo.....  | 16 |
| Ataques a contraseñas.....  | 18 |
| Fuerza Bruta.....   | 18 |
| Diccionario.....  | 19 |
| FIX LEGION.....   | 20 |
| Bibliográfica y Vínculos de interes.....                                  | 20 |

## INTRODUCCIÓN

### **¿Que es legion?**

**Legion** es una bifurcación de Sparta de SECFORCE, es un network penetration testing framework (marco de pruebas de penetración de red) de código abierto, fácil de usar, súper extensible y semiautomático que ayuda en el descubrimiento, reconocimiento y explotación de sistemas de información.

### Características

- Reconocimiento y escaneo automático con NMAP, whataweb, nikto, Vulners, Hydra, SMBenum, dirbuster, sslyzer, webslayer y más (con casi 100 scripts programados automáticamente).
- Interfaz gráfica fácil de usar con ricos menús contextuales y paneles que permiten a los pentesters encontrar y explotar rápidamente vectores de ataque en hosts.
- La funcionalidad modular permite a los usuarios personalizar Legion fácilmente y llamar automáticamente a sus propios scripts/herramientas.
- Múltiples configuraciones de escaneo personalizadas ideales para probar diferentes entornos de diversos tamaños y complejidades.
- Escaneo de escenario altamente personalizable para evasión IPS tipo ninja.
- Detección automática de CPE's (Common Platform Enumeration) y CVE's (Common Vulnerabilities and Exposures).
- Vincula CVE a Exploits como se detalla en Exploit-Database.
- Guardado automático en tiempo real de los resultados y tareas del proyecto.

## PRIMEROS PASOS

### Instalación

Normalmente viene instalada con el sistema Kali-Linux, pero de ser necesaria su instalación podemos hacerlo de varias maneras.

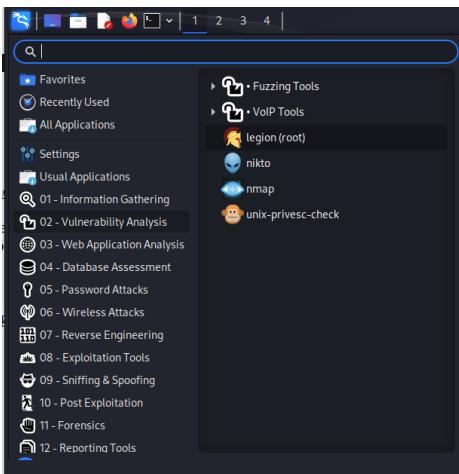
Después de actualizar la base de datos, podemos instalar Legion usando apt-get ejecutando el siguiente comando:

```
sudo apt-get -y install legion
```

Clonando un repositorio Git. Se da por echo que se tiene instalado Python 3.6. En la terminal:

```
git clone https://github.com/GoVanguard/legion.git  
cd legion  
sudo chmod +x startLegion.sh  
sudo ./startLegion.sh
```

## Ejecución



Luego de la instalación, para ejecutar la interfaz grafica, debemos simplemente tipiar en la consola con permisos de súper usuario:

```
# sudo legion
```

O simplemente desde el menú de aplicaciones:

Menú > Análisis de vulnerabilidades > legion

## Agregar Objetivos

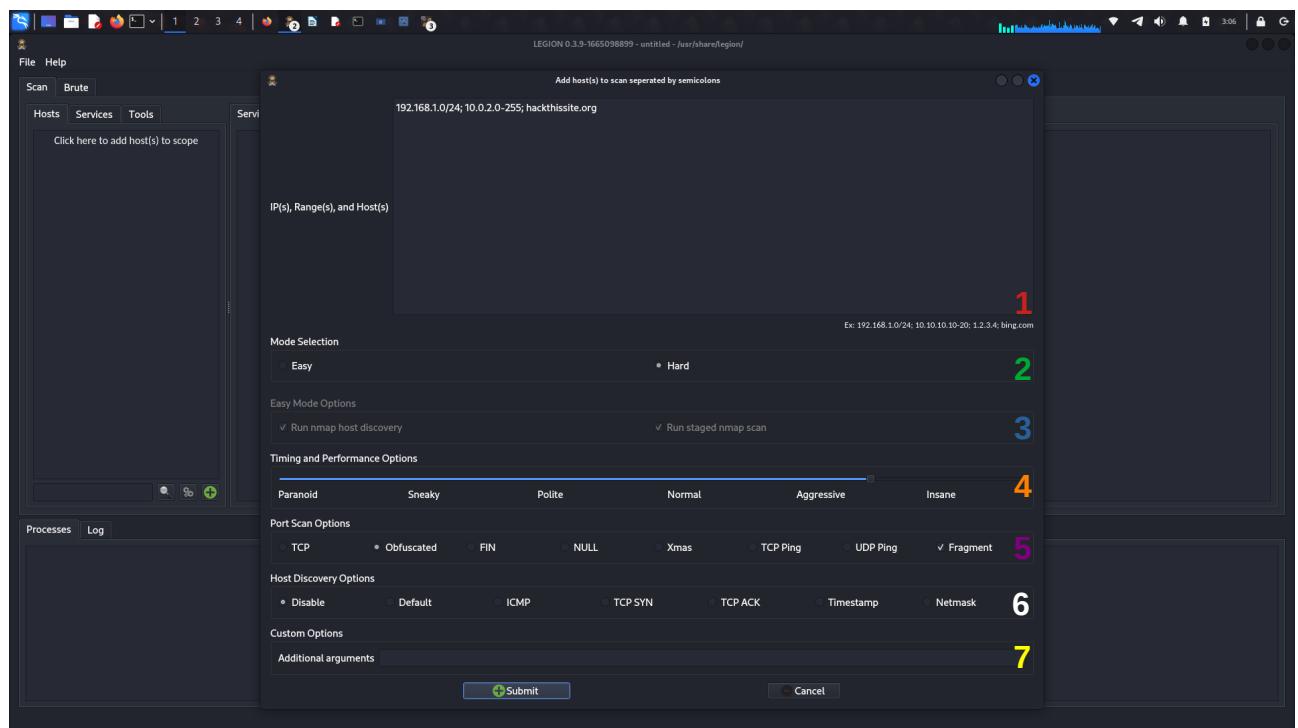
Para agregar uno o mas objetivos hacemos click dentro del rectángulo como se indica en inglés “click here to add host(s) to scope” (Haga clic aquí para agregar host(s) al alcance). Si no desde el símbolo de “+” verde ubicado abajo a la derecha dentro de la pestaña host.

Menú de selección de objetivos

Filtros de visualización, desde aquí podemos seleccionar que deseamos ver de los host escaneados, los vivos, muertos, con puertos abiertos, filtrados, cerrados, etc. También podemos ingresar filtros manualmente.

## ESCANEO DE OBJETIVOS

### Selección de opciones (Banderas nmap)



Al efectuar click en “agregar host”, se nos abre otra ventana con diferentes opciones, las cuales están divididas en 7 secciones.

**1 » Selección de ip's, dominio's.**

**2 » Selección de modo**

**3 » Opciones modo fácil**

**4 » Opciones de tiempo y rendimiento**

**5 » Opciones de escaneo de puertos**

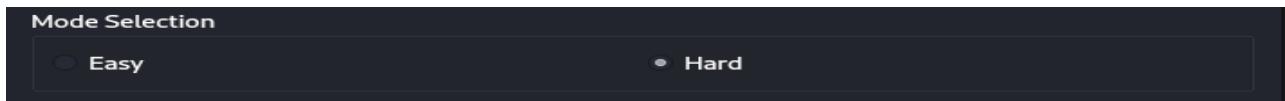
**6 » Opciones de detección de host**

**7 » Opciones personalizadas**

## 1. Selección de objetivos

Aquí podemos agregar uno o varios hosts para escanear. Podemos agregar una única IP (192.168.1.1) o un rango de IP's (192.168.1.1-255) una subred entera usando la notación CIDR (Classless Inter-Domain Routin 192.168.1.0/24) o nombres de dominio(por ejemplo: hackthissite.com) Para agregar varios objetivos, debemos separarlos con punto y coma.

## 2. Selección de modo

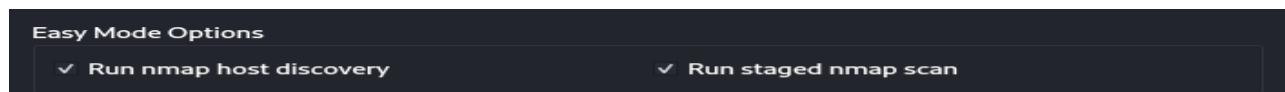


Aquí tenemos dos opciones de selección Modo FÁCIL o DIFÍCIL

Si elegimos la opción FÁCIL se habilitaran los espacios de configuración 3 y 4 (easy mode y timing and performance)

Si elegimos DIFÍCIL lo haran los espacion 4, 5 y 6. (timing and performance, port scan y Host discovery) pero no el 3 (easy mode)

## 3. Opciones modo facil



**Run nmap Host Discovery ---->** Si dejamos activa esta casilla enviaremos una bandera “-O” al comando que se ejecutara de nmap, con esta opcion el comando es:

```
nmap -n -sV -O --version-light -T4 [IP]
```

-n/-R: No hacer resolución DNS / Siempre resolver por omisión: a veces

-sV: Verificar la versión de los puertos escaneados.

-O: Intenta detectar el sistema operativo

--version-light: Limitar a los escaneos más probables (intensidad 2)

-T4: valor por defecto, tiempo y rendimiento del escaneo.

**Run Staged Nmap Scan** ----> Activada por defecto en un escaneo en modo fácil, produce una serie de escaneos de diferentes etapas, de la 1 a la 6.

**Comandos Utilizados en las diferentes etapas :**

Etapa 1 Ping (herramienta hping3): **hping3 -V -C 13 -c 1 [IP]**

Etapa 2 (fast TCP): **nmap -Pn -sV -sC -F -T4 -vvvv [IP]**

Etapa 3 (fast UDP): **nmap -n -Pn -sU -F --min-rate=1000 -vvvv [IP]**

Etapa 4 (vulner): **nmap -sV --script=./scripts/nmap/vulners.nse -vvvv [IP]**

Etapa 5 (full TCP): **nmap -Pn -sV -sC -O -p- -T4 -vvvv [IP]**

Etapa 6 (full UDP): **nmap -n -Pn -sU -p- -T4 -vvvv [IP]**

**Puertos utilizados en las diferentes etapas:**

**Etapa » Puertos:**

**E1»** T:80,81,443,4443,8080,8081,8082

**E2»** T:25,135,137,139,445,1433,3306,5432, U:137,161,162,1434

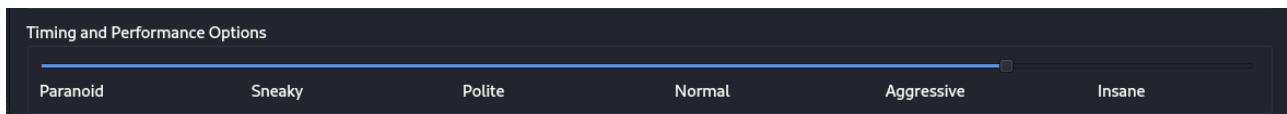
**E3»** NSE|vulners

**E4»** T:23,21,22,110,111,2049,3389,8080,U:500,5060

**E5»** T:0-20,24,26-79,81-109,112-134,136,138,140-442,444,446-1432,1434-2048,2050-3305,3307-3388,3390-5431,5433-8079,8081-29999

**E6»** T:30000-65535

#### 4. Opciones de tiempo y rendimiento ( -T )

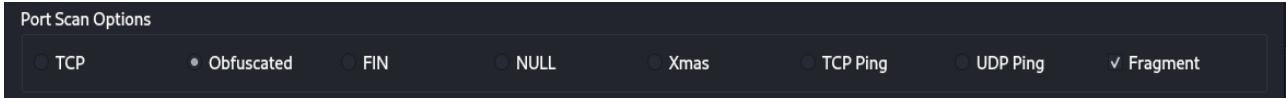


Simplemente deslizando la barra elegiremos entre los diferentes modos de ataque, de las plantillas de temporizado de nmap (las banderas -T0 / -T5) hacia la derecha escaneos mas rápidos, pero mas ruidosos y agresivos, hacia la izquierda lo contrario, menos ruido, menos agresividad, mas “sigilo” pero mucho mas lentos.

**-T4 es el utilizado por defecto.**

|  | T0  | T1         | T2         | T3         | T4         | T5         |
|--|---|------------|------------|------------|------------|------------|
| Name   | Paranoid                                  | Sneaky     | Polite     | Normal     | Aggressive | Insane     |
| min-rtt-timeout                                  | 100 ms                                    | 100 ms     | 100 ms     | 100 ms     | 100 ms     | 50 ms      |
| max-rtt-timeout                                  | 5 minutes                                 | 15 seconds | 10 seconds | 10 seconds | 1250 ms    | 300 ms     |
| initial-rtt-timeout                              | 5 minutes                                 | 15 seconds | 1 second   | 1 second   | 500 ms     | 250 ms     |
| max-retries                                      | 10  | 10         | 10         | 10         | 6          | 2          |
| Initial (and minimum) scan delay (---scan-delay) | 5 minutes                                 | 15 seconds | 400 ms     | 0          | 0          | 0          |
| Maximum TCP scan delay                           | 5 minutes                                 | 15,000     | 1 second   | 1 second   | 10 ms      | 5 ms       |
| Maximum UDP scan delay                           | 5 minutes                                 | 15 seconds | 1 second   | 1 second   | 1 second   | 1 second   |
| host-timeout                                     | 0   | 0          | 0          | 0          | 0          | 15 minutes |
| script-timeout                                   | 0   | 0          | 0          | 0          | 0          | 10 minutes |
| min-parallelism                                  | Dynamic, not affected by timing templates |            |            |            |            |            |
| max-parallelism                                  | 1   | 1          | 1          | Dynamic    | Dynamic    | Dynamic    |
| min-hostgroup                                    | Dynamic, not affected by timing templates |            |            |            |            |            |
| max-hostgroup                                    | Dynamic, not affected by timing templates |            |            |            |            |            |
| min-rate   | No minimum rate limit                     |            |            |            |            |            |
| max-rate   | No maximum rate limit                     |            |            |            |            |            |
| defeat-rst-ratelimit                             | Not enabled by default                    |            |            |            |            |            |

## 5. Opciones de escaneo de puertos (-sT -sS -sF -sN -sX -sP -sU -f )



Las diferentes opciones para el escaneo de puertos son:

| Opciones | TCP        | Ofuscado     | FYN        | NULL       | Xmas       | TCP Ping   | UPD Ping   | Fragmentar |
|----------|------------|--------------|------------|------------|------------|------------|------------|------------|
| Bandera  | <b>-sT</b> | <b>(-sS)</b> | <b>-sF</b> | <b>-sN</b> | <b>-sX</b> | <b>-sP</b> | <b>-sU</b> | <b>-f</b>  |

**-sT:** realiza un escaneo de conexión TCP. Es el análisis predeterminado para los usuarios sin privilegios. El TCP Connect Scan intenta conectarse directamente al objetivo sin utilizar ningún sigilo. Establece una conexión directa y completa.

**Ofuscado (-sS):** El escaneo TCP SYN es la opción por defecto para usuarios root. Intenta identificar los 1000 puertos TCP más utilizados. Conocido como “half open” (medio abierto), no establece una conexión por completo. Se lo considera sigiloso y es uno de los escaneos mas comunes y rapidos

**-sF:** Escaneo TCP FIN, marca el bit TCP FIN activo, envía un paquete TCP con la bandera FIN establecida para determinar si un puerto está abierto o cerrado.

**-sN:** Escaneo TCP NULL, hace que Nmap envíe paquetes sin indicadores TCP habilitados. Esto es posible estableciendo el encabezado del paquete en 0. El NULL, desactiva todas las banderas (en esta técnica podíamos ver que si tenemos puertos cerrados es un LINUX y puertos abiertos es un WINDOWS).

**-sX:** Escaneo Xmas (navidad), Nmap envía paquetes con URG, FIN y PSH. Se le llama Xmas por que se activan los flags FIN, PSH y URG, que vistos desde Wireshark parecen un árbol de navidad.

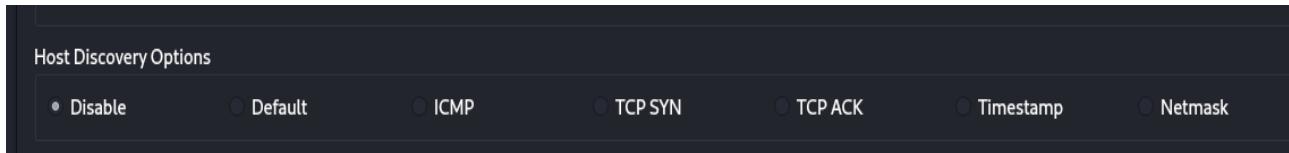
**-sF -sN -sX:** son técnicas de escaneo para poder evitar los filtros de paquetes (ya que muchos analizan los SYN), entonces lo que envían son paquetes determinados (por ejemplo un RST) hacia puertos cerrados, y a los puertos cerrados cuya respuesta las ignoraran (por deducción sabremos si se encuentran activos)

**-sP:** Llamado Escaneo Ping o Ping Sweep, para poder realizar un relevamiento de dispositivos activos. Lo que realiza es mandar un ACK al puerto 80 (por default), si obtiene un RST, la máquina esta activa, es más fiable que hacer ping a la dirección de broadcast, ya que algunos equipos no responden a ese tipo de consultas.

**-sU:** Se utiliza para escanear a través de puertos UDP. Mientras que TCP es el más protocolo de uso común, muchos servicios de red (como DNS, DHCP y SNMP) todavía utilizan UDP.

**-f:** Simplemente divide el escaneo en paquetes de 8 bytes, existen otras banderas para fragmentar, como --mtu 16 o –mtu 32 Algunos S.O pueden necesitar –send-eth combinando con -f o -mtu para realizarlo correctamente.

## **6. Opciones de detección de host (-Pn -PB -PE -PT -PS -PP -PM )**



Las diferentes opciones de escaneo son:

| Opciones       | Disable    | Default    | ICMP       | TCP SYN        | TCP ACK    | Timestamp  | Netmask    |
|----------------|------------|------------|------------|----------------|------------|------------|------------|
| <b>Bandera</b> | <b>-Pn</b> | <b>-PB</b> | <b>-PE</b> | <b>-PT -PS</b> | <b>-PT</b> | <b>-PP</b> | <b>-PM</b> |

**-Pn:** (No Ping) Simplemente no hace ping hacia el host/s, omite la comprobación de detección y realiza el escaneo, si un firewall bloquea las peticiones ICMP, esta bandera nos sera útil.

**-PB:** Opción por default, realiza un ping ICMP y un ping TCP con paquetes ACK.

**-PE:** Esta bandera envía un ping ICMP estándar al destino. Este tipo de descubrimiento funciona mejor en redes locales donde se pueden transmitir paquetes ICMP con pocas restricciones. Sin embargo, muchos hosts de Internet no responden a Paquetes ICMP por razones de seguridad.

**-PT -PS:** Esta opción utiliza dos banderas diferentes, -PT y -PS

**-PT:** Esta a bandera se utiliza para escanear puertos TCP utilizando técnicas de escaneo sin conexión, lo que permite un escaneo más rápido y menos intrusivo.

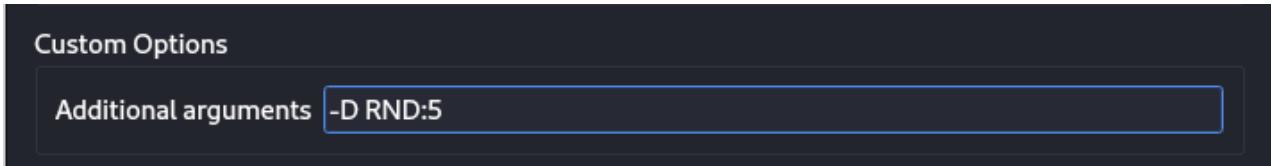
**-PS:** Envía un paquete SYN al sistema de destino y escucha una respuesta. Este método de detección alternativo es útil para sistemas configurados para bloquear pings ICMP. Nota El puerto predeterminado para -PS es 80.

**-PP:** Realiza un ping con una marca de tiempo ICMP. Si bien la mayoría de los sistemas con firewall están configurados para bloquear las solicitudes de eco ICMP, algunos sistemas están configurados incorrectamente y aún pueden responder a las solicitudes con marca de tiempo ICMP. (Estas solicitudes se utilizan para determinar la latencia de una conexión.)

**-PM:** Es una consulta ICMP no convencional (similar a la opción -PP) intenta hacer ping al host especificado utilizando registros ICMP alternativos. Este tipo de ping puede que ocasionalmente pase a través de un firewall que está configurado para bloquear solicitudes estándar.

## 7. Opciones personalizadas

Podemos agregar banderas que no se encuentren dentro de las opciones de la ventana



-D RND:5 = selecciona 5 IPs al azar. (Ejemplo)

Después de seleccionar las opciones deseadas simplemente clickear en Submit para comenzar el escaneo. Dependiendo de la cantidad de host's y opciones elegidas tardara mas o menos tiempo en completarse el escaneo.

Si queremos saber mas sobre las posibles banderas y funcionamiento de nmap:

<https://nmap.org/book/toc.html>

## COMPRENSIÓN DE LA INTERFAZ Y RESULTADOS.

Una vez finalizado el escaneo, veremos un resultado como este (en este caso se uso metasploitable 3 y ubuntuserver para el ejemplo)

A la derecha dentro de la pestaña Scan, 3 pestañas mas, Host (nos muestra los host dependiendo de los filtros elegidos), Services (filtra por servicios y no por host) y tool (filtra por herramientas utilizadas)

A screenshot of the Nmap interface showing the results of a scan. The interface has a dark theme with light-colored text. At the top, it says 'LEGION 0.3.9-1665098899 - untitled - /usr/share/legion/'. On the left, there are tabs for 'File', 'Help', 'Scan', and 'Brute'. Under 'Scan', there are tabs for 'Hosts', 'Services', 'Tools', and 'Log'. The 'Services' tab is currently selected. It shows a table of open ports for two hosts: 192.168.1.25 (metasploitable3-ub...) and 192.168.1.11 (unknown). The table includes columns for Port, Protocol, State, and Name. For host 192.168.1.25, ports 21, 22, 80, 445, 631, 3306, 3500, 6697, and 8080 are open, with services like ftp, ssh, http, microsoft-ds, ipp, mysql, httpd, irc, and http-proxy respectively. For host 192.168.1.11, ports 21, 80, and 445 are open, with services like ftp-default, httpd, and smbnenum. Below the table, there are sections for 'Processes' and 'Log', which show the status of various tools used during the scan, such as mysql-default, screenshot, and smbclient.

## Pestañas

En el panel de la derecha podemos observar 4 pestañas principales (**Services, Scripts, Information, CVEs**). Seguido **Notes** y las siguientes dependiendo del caso Capturas de pantalla y los Log's de salida de los scripts ejecutados

### Services:

Nos muestra una tabla con el **puerto** escaneado, el **protocolo** utilizado tcp/udp, el **estado** del puerto (abierto, cerrado, filtrado), el **nombre** del puerto y después la **versión**.  
(La información se puede organizar haciendo click en la parte superior de cada columna)

En el caso del primer puerto:

Puerto: 21 | Protocolo: tcp | Estado: abierto | Nombre: ftp | Versión: ProFTPD 1.3.5

| Port | Protocol | State | Name        | Version   |
|------|----------|-------|-------------|---|
| 21   | tcp      | open  | ftp         | ProFTPD 1.3.5   |
| 22   | tcp      | open  | ssh         | OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0) |
| 80   | tcp      | open  | http        | Apache httpd 2.4.7  |
| 445  | tcp      | open  | netbios-ssn | Samba smbd 3.X - 4.X (workgroup: WORKGROUP)                     |
| 631  | tcp      | open  | ipp         | CUPS 1.7  |
| 3306 | tcp      | open  | mysql       | MySQL (unauthorized)  |
| 8080 | tcp      | open  | http        | Jetty 8.1.7.v20120910   |

En el caso del puerto 445 nos indica la versión aproximada de Samba, entre 3.X y 4.X y tambien que hay un grupo de trabajo que se llama WORKGROUP

En el caso del puerto 3306 que el acceso no es autorizado, ya que no encontró las credenciales de acceso dentro de los parámetros establecidos.

## Scrips:

Los scripts de Nmap (NSE Nmap Scripting Engine) son pequeños programas o instrucciones que se utilizan junto con la herramienta de escaneo para realizar tareas específicas, como detección de servicios, detección de vulnerabilidades o recopilación de información sobre hosts en una red.

.En este caso observamos que se utilizaron 2 script's **vulners** y **http-server-header**.

### El script Vulners:

```
nmap -sV --script vulners [--script-args mincvss=<arg_val>] <target>
```

Para cada CPE (Common Platform Enumeration) disponible, el script muestra las vulnerabilidades conocidas y tambien el puntajes CVSS (Common Vulnerability Scoring System) correspondientes.

Funciona sólo cuando se identifica alguna versión de software para un puerto abierto  
Busca todos los CPE conocidos para el servicio (de la salida nmap -sV estándar)  
realiza una consulta a un servidor remoto (API de vulners.com) para saber si existen vulnerabilidades conocidas para ese CPE.

Si no encuentra informacion probara solo con el nombre del servicio

**Utilizando este script se hacen solicitudes a un servicio remoto. Aún así, todas las solicitudes contienen solo dos campos: el nombre del software y su versión (o CPE), de esta manera se preserva la identidad de los usuarios**

### El script http-server-header:

El script "http-server-header" puede ser inviable hoy en día debido a cambios en los estándares de seguridad y privacidad en la web.

| Services         | Scripts  | Information | CVEs   | Notes     | screenshot (80/tcp)     | screenshot (8080/tcp)                              | mysql-default (3306/tcp) |
|------------------|----------|-------------|--|-----------|-------------------------|--|--------------------------|
| Script           | Port     |             |  |           |                         |  |                          |
| vulners          | 21/tcp   | 10.0        | https://vulners.com/saint/SAINT:1B08F4664C428B180EBC9617B41D9A2C | *EXPLOIT* | PROFTPD_MOD_COPY 10.0   | https://vulners.com/canvas/PROFTPD_MOD_COPY        | *EXPLOIT*                |
| vulners          | 22/tcp   |             |  |           | PACKETSTORM:162777 10.0 | https://vulners.com/packetstorm/PACKETSTORM:162777 |                          |
| http-server-h... | 80/tcp   |             |  |           | *EXPLOIT*               |  |                          |
| vulners          | 80/tcp   |             |  |           | PACKETSTORM:132218 10.0 | https://vulners.com/packetstorm/PACKETSTORM:132218 |                          |
| http-server-h... | 631/tcp  |             |  |           | *EXPLOIT*               |  |                          |
| vulners          | 631/tcp  |             |  |           | PACKETSTORM:131567 10.0 | https://vulners.com/packetstorm/PACKETSTORM:131567 |                          |
| http-server-h... | 8080/tcp |             |  |           | *EXPLOIT*               |  |                          |
|                  |          |             |  |           | PACKETSTORM:131555 10.0 | https://vulners.com/packetstorm/PACKETSTORM:131555 |                          |
|                  |          |             |  |           | *EXPLOIT*               |  |                          |
|                  |          |             |  |           | PACKETSTORM:131505 10.0 | https://vulners.com/packetstorm/PACKETSTORM:131505 |                          |
|                  |          |             |  |           | *EXPLOIT*               |  |                          |
|                  |          |             |  |           | EDB-ID:49908 10.0       | https://vulners.com/exploitdb/EDB-ID:49908         | *EXPLOIT*                |
|                  |          |             |  |           | CVE-2015-3306 10.0      | https://vulners.com/cve/CVE-2015-3306              |                          |
|                  |          |             |  |           | 1337DAY-ID-36298 10.0   | https://vulners.com/zdt/1337DAY-ID-36298           | *EXPLOIT*                |
|                  |          |             |  |           | 1337DAY-ID-23720 10.0   | https://vulners.com/zdt/1337DAY-ID-23720           |                          |

## Information:

En esta pestaña encontramos el estado del host:

State: up (Activo, down si fuera inactivo)

Puertos abiertos: 9 | Puertos cerrados: 2 | Puertos filtrados: 65524

Tipo de Sistema Operativo y el porcentaje de precisión del resultado obtenido: en este caso no obtuvo resultados

Direcciones: IPV4 – IPV6 – MAC-vendedor - ASN(Autonomous System Number) - ISP

Localización: No obtubo resultados pero encontraríamos información sobre el país, ciudad y posición geográfica

| Services              | Scripts                               | Information | CVEs                  | Notes | screenshot (80/tcp) | screenshot (8080/tcp) | mysql-default (3306/tcp) |
|-----------------------|---------------------------------------|-------------|-----------------------|-------|---------------------|-----------------------|--------------------------|
| Host Status           | Addresses                             |             | Location              |       |                     |                       |                          |
|                       | IPv4: 192.168.1.25                    |             |                       |       |                     |                       |                          |
| State: up             | IPv6: unknown                         |             | Country Code: unknown |       |                     |                       |                          |
| Open Ports: 9         | MAC: 08:00:27:21:04:60                |             | City: unknown         |       |                     |                       |                          |
|                       | Vendor: Oracle VirtualBox virtual NIC |             |                       |       |                     |                       |                          |
| Closed Ports: 2       | ASN: unknown                          |             | Latitude: unknown     |       |                     |                       |                          |
|                       | ISP: unknown                          |             | Longitude: unknown    |       |                     |                       |                          |
| Filtered Ports: 65524 |                                       |             |                       |       |                     |                       |                          |
| Operating System      |                                       |             |                       |       |                     |                       |                          |
| Name: unknown         |                                       |             |                       |       |                     |                       |                          |
| Accuracy: NaN         |                                       |             |                       |       |                     |                       |                          |

## CVE'S:

En esta pestaña se imprimen los resultados de las vulnerabilidades encontradas con su respectivo puntaje, como se detalla en la pestaña de SCRIPT'S (pag.12), pero organizada de una mejor manera y con mas información:

Las columnas mas iportantes a tener en cuenta:

CVE id: Identificador CVE (Common Vulnerabilities Exposures) Ejemplo: CVE-2015-3306

CVVS Score: Puntaje CVVS Ejemplo 10.0

Version: 1.35

CVE URL: En este caso no esta el link hacia la pagina.(cve.org)

Source: Fuente donde proviene el CVE, en este caso Proftpd

Producto: Tambien es Proftpd

ExploitDb ID: Identifiador de exploit database

ExlploitDb URL: Hipervinculo a dicho exploit.

En la imagen de abajo la informacion no concuerda con las columnas (=debido a una mala configuración en este caso en particular:)

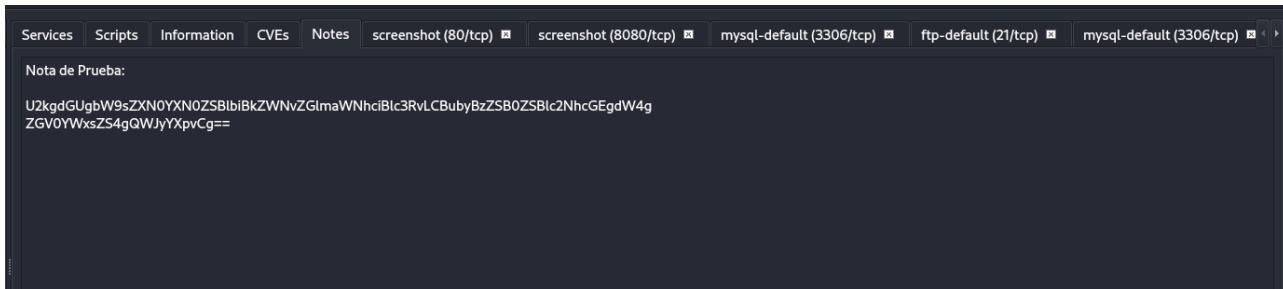
| LEGION 0.3.9-1665098899 - untitled - /usr/share/legion/ |            |         |         |         |         |              |           |               |  |  |
|---|------------|---------|---------|---------|---------|--------------|-----------|---------------|--|--|
| Scan  |            | Brute   |         |         |         |              |           |               |  |  |
| CVE Id  | CVSS Score | Product | Version | CVE URL | Source  | ExploitDb ID | ExploitDb | ExploitDb URL |  |  |
| SAINT:FD1752E124A72FD3A26EEB9B315E8382                  | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| SAINT:950EB68D408A40399926A4CCAD3CC62E                  | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| SAINT:63FB77B9136D48259E4F004CDA35E957                  | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| SAINT:1B08F4664C4288180EEC9617B41D9A2C                  | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| PROFTPD_MOD_COPY  | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| PACKETSTORM:162777                                      | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| PACKETSTORM:132218                                      | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| PACKETSTORM:131567                                      | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| PACKETSTORM:131555                                      | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| PACKETSTORM:131505                                      | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| EDB-ID:49908  | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| CVE-2015-3306   | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| 1337DAY-ID-36298  | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| 1337DAY-ID-23720  | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |
| 1337DAY-ID-23544  | proftpd    | 1.3.5   | 10.0    | proftpd | unknown | unknown      | unknown   | unknown       |  |  |

| Processes  |         | Log            |       |                         |              |          |  |
|------------|---------|----------------|-------|-------------------------|--------------|----------|--|
| Progress   | Elapsed | Est. Remaining | Pid   | Tool                    | Host         | Status   |  |
| ██████████ | 8.34s   | 0.00s          | 69369 | nmap (stage 1)          | 192.168.1.25 | Finished |  |
| ██████████ | 5.03s   | 0.00s          | 69378 | nmap (stage 1)          | 192.168.1.11 | Finished |  |
| ██████████ | 0.00s   | 0.00s          | 69446 | nmap (stage 2)          | 192.168.1.11 | Finished |  |
| ██████████ | 4.20s   | 0.00s          | 69517 | nmap (stage 3)          | 192.168.1.11 | Finished |  |
| ██████████ | 0.00s   | 0.00s          | 69528 | mysql-default (3306/... | 192.168.1.11 | Finished |  |
| ██████████ | 0.00s   | 0.00s          | 0     | screenshot (80/tcp)     | 192.168.1.11 | Finished |  |

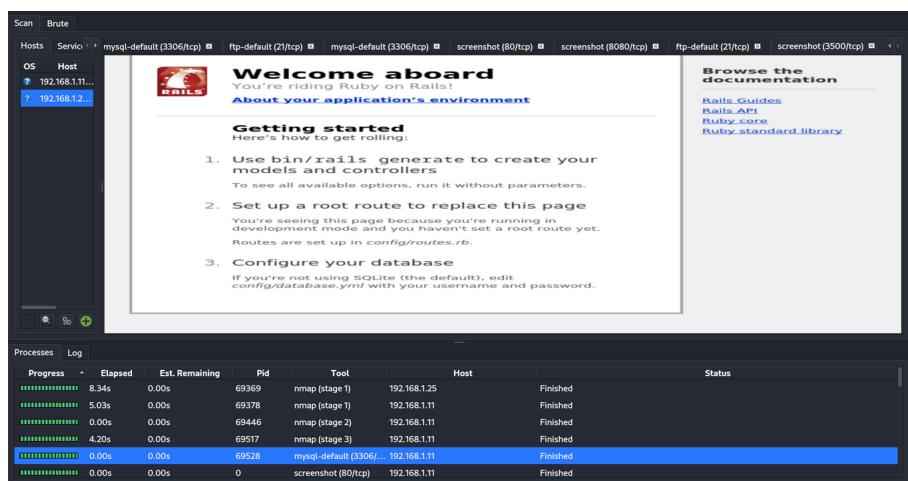
## Notas:

En el caso de guardar los resultados de un ataque, se podrán dejar apuntes directamente dentro de la interfaz.



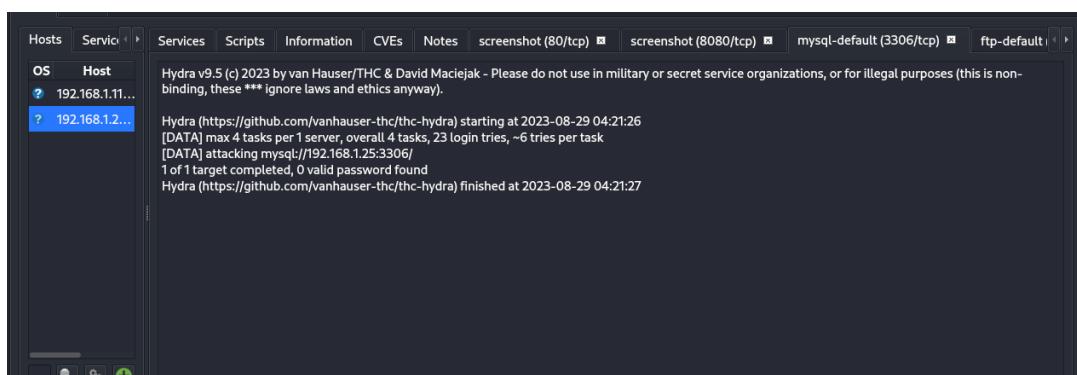
## Otras Pestañas:

Dependiendo del tipo y resultado del escaneo, podemos observar otro tipo de pestañas que varían entre capturas de pantalla (screenshot) y las salidas de los distintos log's de las herramientas utilizadas:



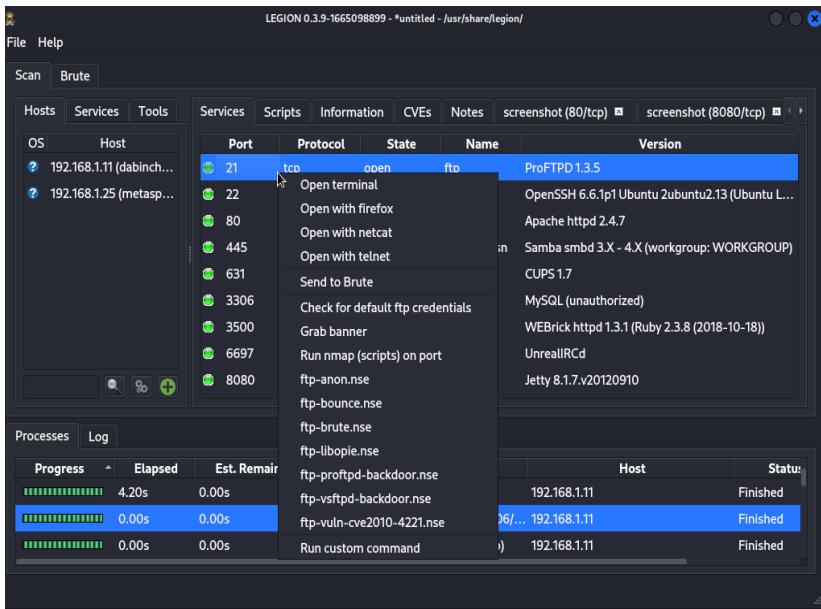
## Pestaña screenshot:

**Pestaña de log** de un script de hydra, se realizó sin resultados positivos, un ataque de diccionario (mas adelante veremos algunos ejemplos con hydra):



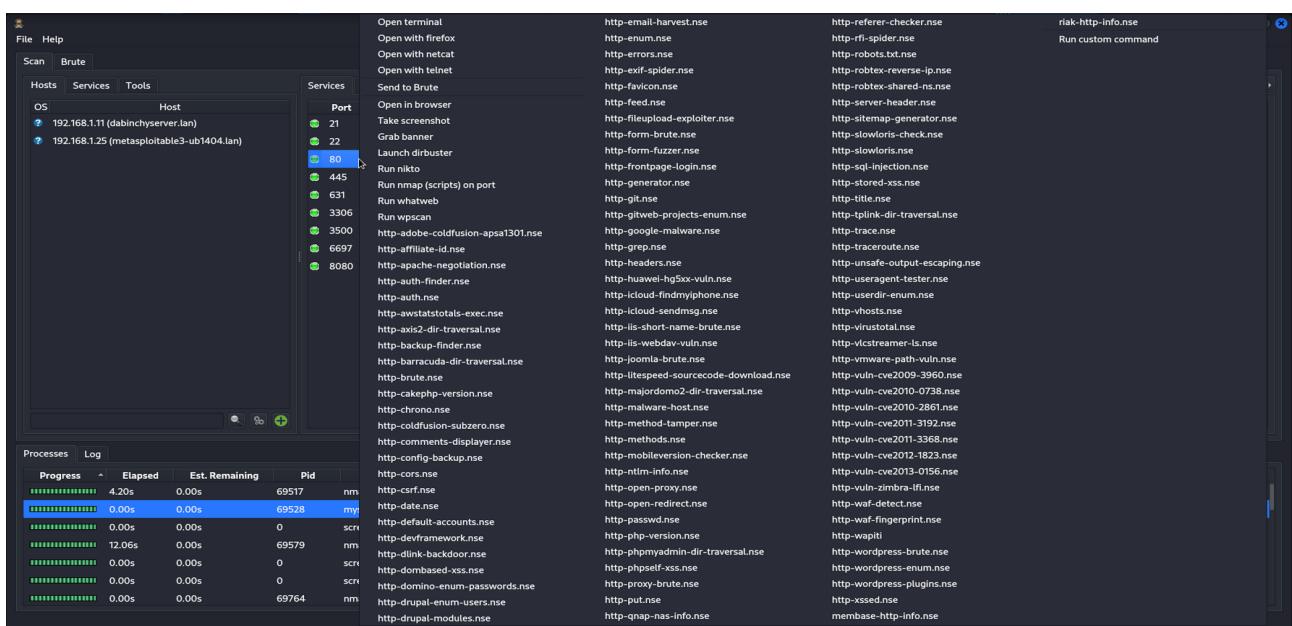
## Mas opciones de escaneo

Si todavía no estamos conformes o se nos olvido tal vez algún parámetro a la hora de iniciar nuestro escaneo, simplemente haciendo click derecho en el puerto se desplegará un menú con diferentes opciones.

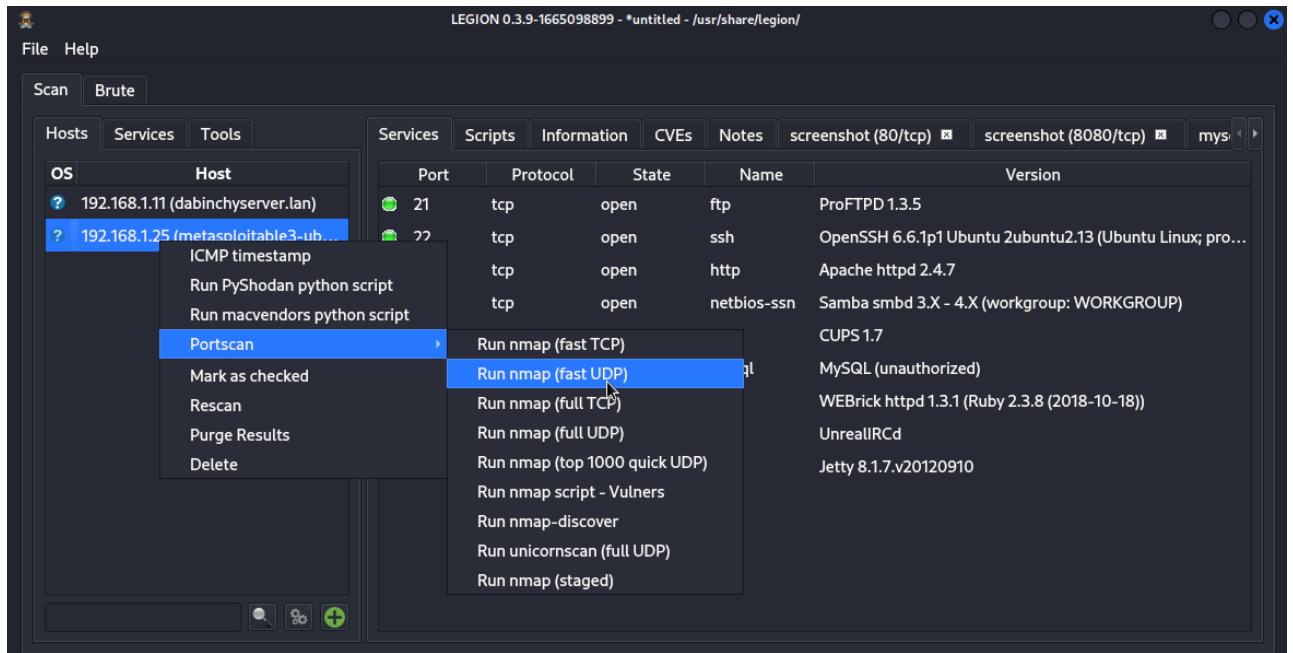


Cada puerto o servicio tiene diferentes opciones uno de los otros en este caso Puerto 21 Servicio ftp, las opciones varias de simplemente abrir un servicio de ftp al puerto 21 en la terminal, enviar para fuerza bruta, Grab banner, escaner scrip's de nmap en el puerto, etc

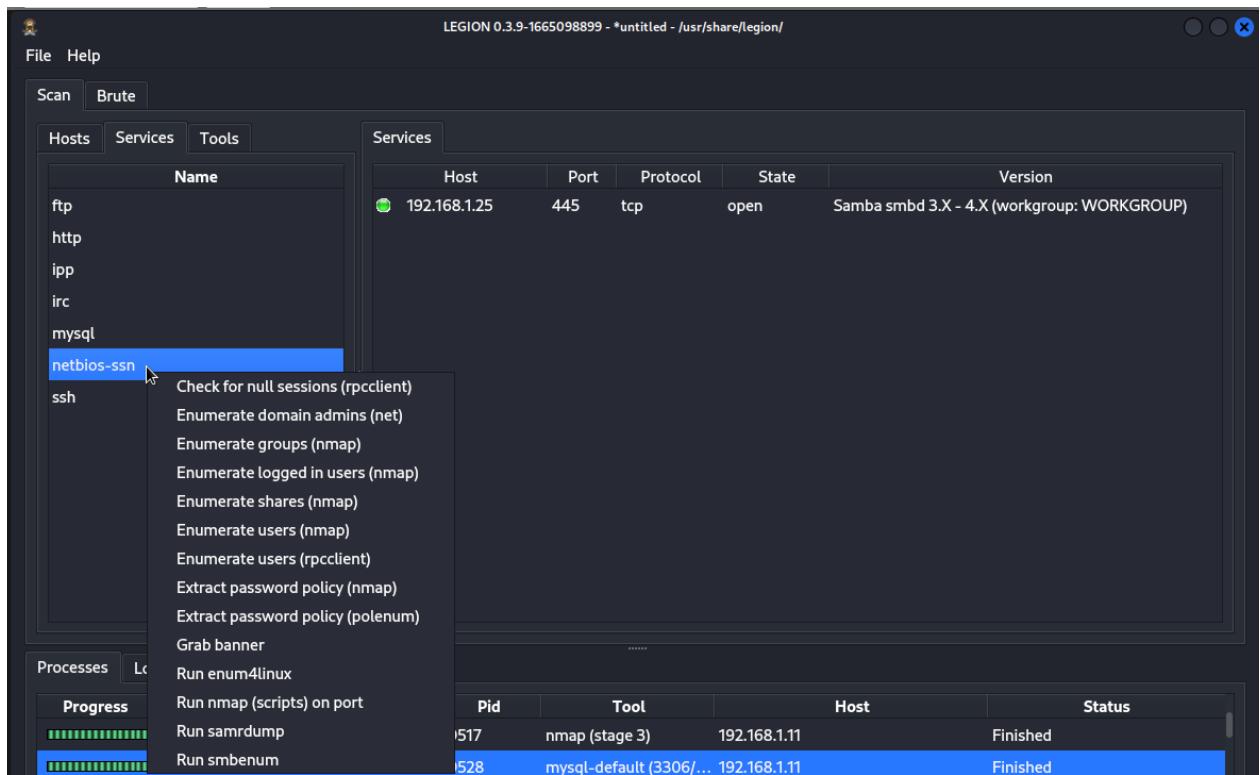
Puerto 80 servicio http: observemos la cantidad de opciones, desde un simple screenshot, pasando por todos los NSE de nmap, escanear con nikto, wafatweb, entre otras. Cada vez que hagamos click en un opción de este menu, se abrirá una pestaña con la información obtenida.(como en el ejemplo de la pagina anterior pestaña de log)



Lo mismo podemos realizar con el menú de la derecha en Host o en Services, si hacemos click derecho en el IP o nombre de host, podremos re-escanear el objetivo, eliminarlo, hacer un ICMP timestamp, entre otras opciones.



Ejemplo desde la Pestaña servicio, sus opciones y la manera de imprimir en la pantalla los resultados organizando por servicio.



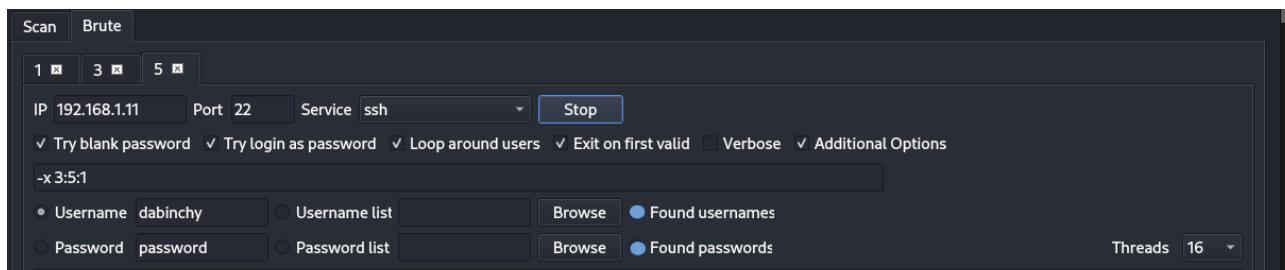
## Ataques a contraseñas

Desde la pestaña **Scan » Services**, haciendo click derecho sobre cualquier fila de un puerto/servicio y después seleccionar “**Send to Brute**”, podemos enviar de una manera muy sencilla el puerto y servicio elegidos para ser atacado. Por cualquiera de las formas que explicaremos. Si no también podemos ingresar los datos manualmente.

Estos ataques se realizaran utilizando la herramienta hydra ( instalada por defecto en Kali Linux )

## Fuerza Bruta

Para realizar un ataque de fuerza bruta solo se necesita accionar las casillas “**Found Usernames**”, “**Found Passwords**”, dependiendo siempre de la necesidad del usuario y tabien del conocimiento del objetivo



## Selección manual de credenciales

A la izquierda se encuentran las casillas de Username y Password, podemos seleccionar las credenciales que conozcamos manualmente.

Por defecto Username: root y Password: Password.

Hay otras casillas como Try blank password (Probar password en blanco), Try login as password (Probar login como password), Loop around users ( Girar alrededor de los usuarios), Exit on first valid (salir al descubrir la primera acreditación valida), Vervose y Additional Options (Opciones adicionales) aquí agregaremos parametros de hydra.

## Diccionario

Para realizar este tipo de ataque una vez cargado los datos del host objetivo, debemos elegir las casillas Username list (listas de usuarios) y Password list (listas de passwords). Despues desde el boton de Browse (buscar) y elegir la ubicación donde se encuentra el archivo de texto que contiene la lista de usuarios, passwords, pueden ser el mismo o diferentes archivos.

En la imagen se observa que despues de 264 intentos, de un tota de 57377624 posibilidades, resolvio que las credenciales de acceso son login o nombre de usuario: “dabinchy” y el password: “1234”.

The screenshot shows the LEGION 0.3.9 interface. In the top navigation bar, there are links for File, Help, Scan, and Brute. The Brute tab is selected. Below the tabs, there are two tabs labeled 1 and 2. The IP address is set to 192.168.1.11, Port to 22, and Service to ssh. The Stop button is visible. Under the configuration section, there are checkboxes for Try blank password, Try login as password, Loop around users, Exit on first valid, Verbose, and Additional Options. There are also fields for Username (root) and Password (password), both with browse buttons. A Threads dropdown is set to 16. The main window displays the log output of the attack:

```
[RE-ATTEMPT] target 192.168.1.11 - login "admin" - pass "cookie" - 260 of 57377624 [child 2] (0/4)
[ATTEMPT] target 192.168.1.11 - login "dabinchy" - pass "cookie" - 261 of 57377624 [child 0] (0/4)
[ATTEMPT] target 192.168.1.11 - login "" - pass "cookie" - 262 of 57377624 [child 14] (0/4)
[RE-ATTEMPT] target 192.168.1.11 - login "root" - pass "1234" - 262 of 57377624 [child 0] (0/4)
[ATTEMPT] target 192.168.1.11 - login "admin" - pass "1234" - 263 of 57377624 [child 8] (0/4)
[ATTEMPT] target 192.168.1.11 - login "dabinchy" - pass "1234" - 264 of 57377624 [child 6] (0/4)
[ATTEMPT] target 192.168.1.11 - login "" - pass "1234" - 265 of 57377624 [child 5] (0/4)
[22][ssh] host: 192.168.1.11 login: dabinchy password: 1234
[STATUS] attack finished for 192.168.1.11 (valid pair found)
```

Below the log, there is a Processes tab and a Log tab. The Processes tab shows a table with columns: Progress, Elapsed, Est. Remaining, Pid, Tool, Host, and Status. All entries are finished:

| Progress   | Elapsed | Est. Remaining | Pid  | Tool                     | Host         | Status   |
|------------|---------|----------------|------|--------------------------|--------------|----------|
| ██████████ | 5.52s   | 0.00s          | 4146 | nmap (stage 1)           | 192.168.1.11 | Finished |
| ██████████ | 0.00s   | 0.00s          | 4214 | nmap (stage 2)           | 192.168.1.11 | Finished |
| ██████████ | 7.03s   | 0.00s          | 4282 | nmap (stage 3)           | 192.168.1.11 | Finished |
| ██████████ | 15.54s  | 0.00s          | 4291 | mysql-default (3306/...) | 192.168.1.11 | Finished |
| ██████████ | 0.00s   | 0.00s          | 0    | screenshot (80/tcp)      | 192.168.1.11 | Finished |
| ██████████ | 0.00s   | 0.00s          | 4380 | nmap (stage 4)           | 192.168.1.11 | Finished |

Desde la izquierda podemos seleccionar las casillas Username y/o Password para establecer las credenciales en caso de conocer ambas o una de ellas.

## FIX LEGION

En caso de que legion presente problemas a la hora de su ejecución, se recomienda una instalación limpia de Nmap.

Ejecutar legion, seguido ir a Help » Config

Y reemplazar la sección de configuración de niveles nmap con los siguientes parámetros:

[StagedNmapSettings]

stage1-ports="PORTS|T:80,81,443,4443,8080,8081,8082"

stage2-ports="PORTS|T:25,135,137,139,445,1433,3306,5432,U:137,161,162,1434"

stage3-ports="NSE|vulners"

stage4-ports="PORTS|T:23,21,22,110,111,2049,3389,8080,U:500,5060"

stage5-ports="PORTS|T:0-20,24,26-79,81-109,112-134,136,138,140-442,444,446-1432,1434-2048,2050-3305,3307-3388,3390-5431,5433-8079,8081-29999"

stage6-ports="PORTS|T:30000-65535"

## Bibliográfica y Vínculos de interés

<https://nmap.org/book/toc.html>

(The Official Nmap Project Guide to Network Discovery and Security Scanning)

<https://github.com/GoVanguard/legion>

Nmap Cookbook The Fat free Guide to Network Scanning by Nicholas.pdf (si es requerido se pude brindar una copia del .pdf)

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

<https://www.exploit-db.com/>

<https://cve.mitre.org/>