



Universidad Latino

Tecnología de la Seguridad en Redes y Comunicaciones

Segundo Parcial

Integrantes: Jesus Enrique Jimenez

24/03/2025

## Configuración de usuario y correo electrónico en git bash

```
MINGW64/c/Users/franc x + v
franc@FrancoPC MINGW64 ~
$ git --version
git version 2.49.0.windows.1

franc@FrancoPC MINGW64 ~
$ git config --global user.name "YSQ-Franco"

franc@FrancoPC MINGW64 ~
$ git config --global user.email "franco.motta@alumno.universidadlatino.edu.mx"

franc@FrancoPC MINGW64 ~
$ |
```

## Creación del Repositorio Local

```
franc@FrancoPC MINGW64 ~
$ mkdir Parcial2

franc@FrancoPC MINGW64 ~
$ cd Parcial2

franc@FrancoPC MINGW64 ~/Parcial2
$ mkdir PortafolioPentesting

franc@FrancoPC MINGW64 ~/Parcial2
$ cd PortafolioPentesting

franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting
$
```

## Creación de herramientas para cada herramienta

```
franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting
$ mkdir NMAP Masscan GoogleDorks Shodan SQLMAP Wireshark InyeccionSQL_DVWA

franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting
$ touch NMAP/detalles.txt Masscan/detalles.txt GoogleDorks/detalles.txt Shodan/detalles.txt SQLMAP/detalles.txt Wireshark/detalles.txt InyeccionSQL_DVWA/detalles.txt

franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting
$ ls -l
GoogleDorks/
InyeccionSQL_DVWA/
Masscan/
NMAP/
Shodan/
SQLMAP/
Wireshark/

franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting
$
```

## Inicializar el repositorio git

```
franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting
$ git init
Initialized empty Git repository in C:/Users/franc/Parcial2/PortafolioPentesting/.git/

franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting (master)
$ |
```

## Primer commit después de agregar los archivos al git

```
new file:   NMAP/Resultados Nmap.txt
new file:   NMAP/detalles.txt
new file:   README.md
new file:   SQLNAP/detalles.txt
new file:   Shodan/Resultados Shodan.png
new file:   Shodan/detalles.txt
new file:   Wireshark/Resultados WireShark.png
new file:   Wireshark/detalles.txt

franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting (main)
$ git commit -m "Iniciación del repositorio y estructura básica"
[main (root-commit) cfa94a5] Inicialización del repositorio y estructura básica
20 files changed, 159 insertions(+)
create mode 100644 Evidencias.pdf
create mode 100644 GoogleDorks/Comandos de Busqueda GoogleDorks.txt
create mode 100644 GoogleDorks/Resultados GoogleDorks.png
create mode 100644 GoogleDorks/detalles.txt
create mode 100644 InyeccionSQL_DVWA/Procedimiento InyeccionSQL DVWA.txt
create mode 100644 InyeccionSQL_DVWA/Resultados InyeccionSQL DVWA.png
create mode 100644 InyeccionSQL_DVWA/detalles.txt
create mode 100644 Masscan/Resultados Masscan.png
create mode 100644 Masscan/Resultados NMAP.png
create mode 100644 Masscan/detalles.txt
create mode 100644 NMAP/Resultados NMAP imagen 1.png
create mode 100644 NMAP/Resultados NMAP imagen 2.png
create mode 100644 NMAP/Resultados Nmap.txt
create mode 100644 NMAP/detalles.txt
create mode 100644 README.md
create mode 100644 SQLNAP/detalles.txt
create mode 100644 Shodan/Resultados Shodan.png
create mode 100644 Shodan/detalles.txt
create mode 100644 Wireshark/Resultados WireShark.png
create mode 100644 Wireshark/detalles.txt
```

## Generar y configurar una Clave SSH para Github

```
franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting (main)
$ ssh-keygen -t ed25519 -C "franco.motta@alumno.universidadlatino.edu.mx"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/c/Users/franc/.ssh/id_ed25519):
Created directory '/c/Users/franc/.ssh'.
Enter passphrase for "/c/Users/franc/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /c/Users/franc/.ssh/id_ed25519
Your public key has been saved in /c/Users/franc/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:Wj20xmSE8ZYq81ELTFBTAJNixgh8+6+P6i4K06wzAU franco.motta@alumno.universidadlatino.edu.mx
The key's randomart image is:
+--[ED25519 256]--+
  o o+o+=00+
  +. oo+++
  . . =
  . o B o
  E . S B
  .. o + .
  . .... o
  *o... .
  |O*..oo..
+-----[SHA256]-----+
```

## Copiamos la clave publica

```
franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting (main)
$ cat ~/.ssh/id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJFKou+dgj4TrioYp8bH2pw5HIM2I/VgeNDWmk5Xz175 franco.motta@alumno.universidadlatino.edu.mx

franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting (main)
$
```

## Conectamos ambos repositorios de forma remota

```

franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting (main)
$ git remote add origin git@github.com:YSQ-Franco/PortafolioPentesting_FrancoMotta.git

franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting (main)
$ git push -u origin main
The authenticity of host 'github.com (140.82.114.3)' can't be established.
ED25519 key fingerprint is SHA256:+DiY3mVV6TuJJhbpZisF/zLDA0zPMSvHdkr4UvCoQU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'github.com' (ED25519) to the list of known hosts.
Enter passphrase for key '/c/Users/franc/.ssh/id_ed25519':
Enumerating objects: 23, done.
Counting objects: 100% (23/23), done.
Delta compression using up to 8 threads
Compressing objects: 100% (21/21), done.
Writing objects: 100% (23/23), 983.23 KiB | 4.29 MiB/s, done.
Total 23 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
To github.com:YSQ-Franco/PortafolioPentesting_FrancoMotta.git
 * [new branch]      main -> main
branch 'main' set up to track 'origin/main'.

franc@FrancoPC MINGW64 ~/Parcial2/PortafolioPentesting (main)
$

```

## Evidencias de Herramientas

### Zenmap

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-24 12:27 Hora
estándar central (México)
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Initiating ARP Ping Scan at 12:27
Scanning 192.168.0.101 [1 port]
Completed ARP Ping Scan at 12:27, 0.60s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:27
Completed Parallel DNS resolution of 1 host. at 12:27, 0.01s elapsed
Initiating SYN Stealth Scan at 12:27
Scanning realme-GT3-240W (192.168.0.101) [1000 ports]
Completed SYN Stealth Scan at 12:27, 2.16s elapsed (1000 total ports)
Initiating Service scan at 12:27
Initiating OS detection (try #1) against realme-GT3-240W
(192.168.0.101)
Retrying OS detection (try #2) against realme-GT3-240W
(192.168.0.101)
NSE: Script scanning 192.168.0.101.
Initiating NSE at 12:27
Completed NSE at 12:27, 5.11s elapsed
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Nmap scan report for realme-GT3-240W (192.168.0.101)
Host is up (0.0069s latency).

```

```

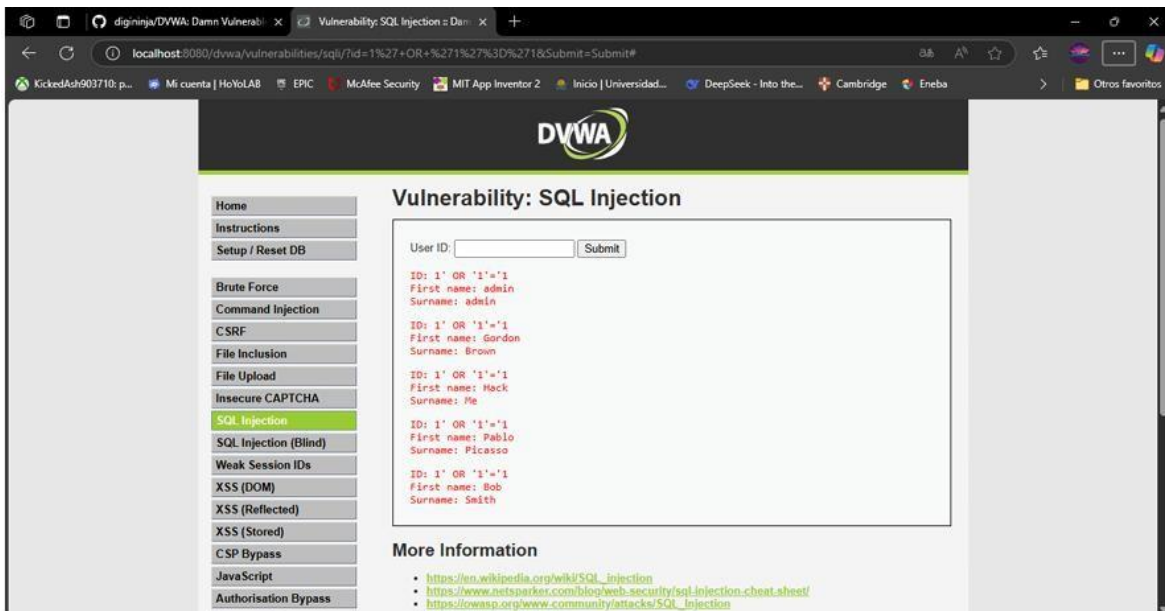
All 1000 scanned ports on realme-GT3-240W (192.168.0.101) are in
ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 92:77:44:9D:2A:BA (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    6.90 ms  realme-GT3-240W (192.168.0.101)

NSE: Script Post-scanning.
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Initiating NSE at 12:27
Completed NSE at 12:27, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.34 seconds
Raw packets sent: 1013 (45.696KB) | Rcvd: 1014 (41.780KB)

```

## Inyección SQL



The screenshot shows the DVWA web application interface. The browser address bar indicates the URL is `localhost:8080/dvwa/vulnerabilities/sql/?id=1%27+OR+%271%27%3D%271&Submit=Submit#`. The page title is "Vulnerability: SQL Injection".

**Navigation Sidebar:**

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection**
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- Authorisation Bypass

**Main Content Area:**

**Vulnerability: SQL Injection**

User ID:

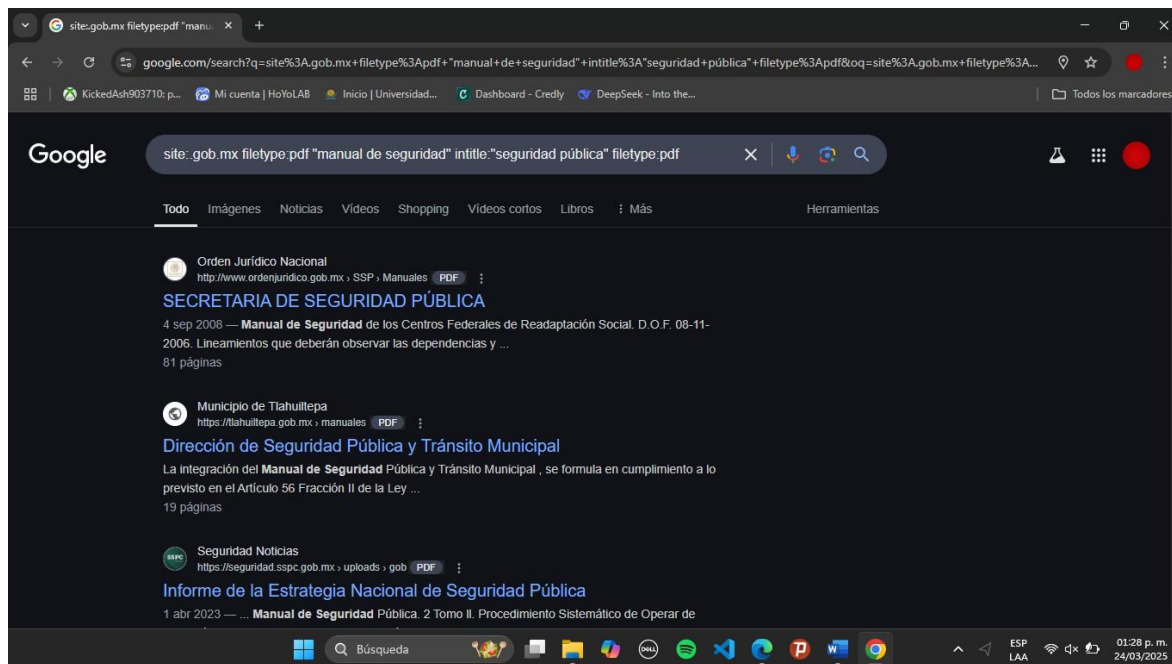
ID: 1' OR '1'='1  
 First name: admin  
 Surname: admin  
  
 ID: 1' OR '1'='1  
 First name: Gordon  
 Surname: Brown  
  
 ID: 1' OR '1'='1  
 First name: Hack  
 Surname: Me  
  
 ID: 1' OR '1'='1  
 First name: Pablo  
 Surname: Picasso  
  
 ID: 1' OR '1'='1  
 First name: Bob  
 Surname: Smith

**More Information**

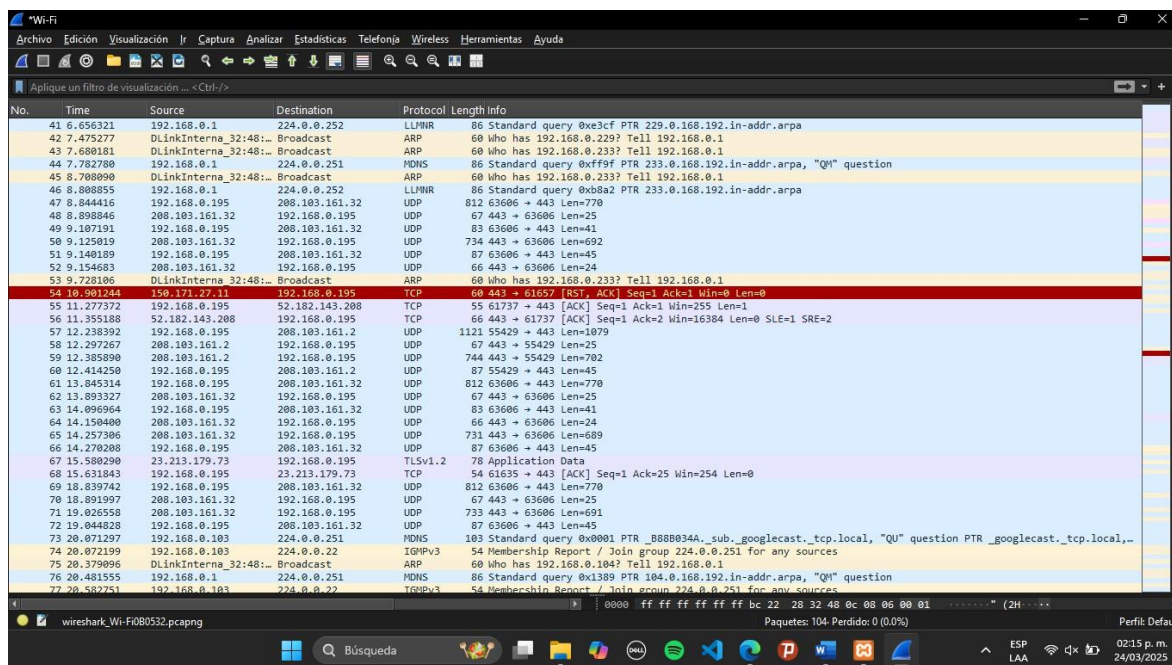
- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)



Google Dorks



## WireShark



## Masscan

```
franco@FrancoPC:~/masscan$ sudo masscan 192.168.0.101 -p80
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-03-24 20:27:02 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
franco@FrancoPC:~/masscan$ sudo masscan 192.168.0.101 -p0-65535
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-03-24 20:27:47 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
rate: 0.10-kpps, 1.87% done, 0:10:36 remaining, found=0
```

## Nmap

```
franco@FrancoPC:~$ sudo nmap -p- 192.168.0.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-24 14:54 CST
Nmap scan report for realme-GT3-240W (192.168.0.101)
Host is up (0.0092s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
46888/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.19 seconds
```

## Shodan

The screenshot shows the Shodan search results page for the query "Mexico country:MX city:Mérida". The page displays 3 total results. The top organizations listed are Wistarip S de RL de CV (2 results) and IP Matrix, S.A. de C.V. (1 result). The main result shown is for IP 201.174.171.90, which is a RouterOS CCR2116-12G-4S+ with service 78. The page also includes a "Product Spotlight" for Shodan Monitor and a search bar at the top.

Shodan search results for "Mexico country:MX city:Mérida".

**TOTAL RESULTS:** 3

**TOP ORGANIZATIONS:**

- Wistarip S de RL de CV: 2
- IP Matrix, S.A. de C.V.: 1

**Product Spotlight:** Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#).

**201.174.171.90**

201-174-171-90.transleic.com

**SNMP:**

- Uptime: 3203549100
- Description: RouterOS CCR2116-12G-4S+
- Service: 78
- Versions: 1, 3
- Name: Borda-TTCO
- Engineid Format: text
- Contact: nazarlo@wistarip.mx
- Engine Boots: 0
- Engineid Data: 00003a8c04
- Enterprise: 14988
- Objectid: 1.3.6.1.4.1.14988.1
- Engine Time: 0:00:...

**190.93.89.253**

dynamus-190-93-89-253