

Criptografía y Seguridad  
Pentesting: Recopilación de Información



**Integrantes:**

- Axel Casas Espinosa 316218849
- Fernanda Garduño Ballesteros 317010316

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

#### ● Requisitos

Comenzar a familiarizarnos con la fase de recopilación para identificar nuestros posibles vectores de ataque a sistemas.

Buscamos conocer la siguiente información:

- Puntos de la red.
- DNS.
- Dirección IP.
- Nombre de dominio, así como sus datos de contacto.
- Fechas de inicio, expiración y actualización.
- Posibles rutas para acceder a este.
- Medir los retrasos de tránsito de los paquetes.
- Subdominios.
- Los puertos, estatus y servicios.

Cabe recalcar que podemos conocer mayor información la cual nos ayudará a enriquecer nuestras bases para llevar a cabo un mejor ataque .

#### ● Identificación de fuentes de información

Para poder recolectar la información anteriormente mencionada haremos uso de las siguientes herramientas:

- Virtualbox con Kali linux
- ping
- nslookup
- traceroute
- whois
- dnsrecon
- Nmap
- EtherApe
- dig
- Host
- Curl

Estas herramientas nos ayudarán con la obtención de información sin embargo es necesario un script para poder filtrar la cantidad de información que nos será brindada.

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

- Adquisición

Generamos el siguiente script en Bash:

```
#!/bin/bash
#Primero nos aseguramos de que se de un dominio a examinar.
if [ -z "$1" ]; then
    echo "Debe proporcionar un dominio como argumento."
    exit 1
fi
#Recibimos el dominio y vamos a usar whois para obtener la info
#whois nos dará información sobre el propietario del nombre de dominio, la dirección
IP, la fecha de registro, la fecha de vencimiento y otros detalles relacionados con la
administración del dominio.
whois $1 > temp.txt

#Extraer datos basicos del punto 1-4 pdf de la práctica.
echo "Analisis de $1:" >> $1.txt #Será nuestro análisis
grep -m 1 "Domain" temp.txt >> $1.txt #obtenemos el dominio
grep -m 1 "Created" temp.txt >> $1.txt #la fecha de creación
grep -m 1 "Last" temp.txt >> $1.txt #la fecha de ult. actualización
grep -m 1 "Expiration" temp.txt >> $1.txt #fecha de expiración
sed -n '/Registrant:/,/Name Servers:/ {/Name Servers:/d; p}' temp.txt >> $1.txt
#Obtenemos todos los datos de contacto
echo "" >>$1.txt

#Recibimos ahora conectividad de red
#Para obtener esta información usamos ping determinar si una dirección IP específica
está accesible en una red determinada y cuánto tiempo tarda en responder, es decir
problemas de conectividad. Envía paquetes constantemente por lo que solo puede pararse
manualmente.
echo "*****Conectividad de la red:*****" >> $1.txt
ping -c 4 $1 >> ping.txt #Limitamos el número de paquetes a enviar
cat ping.txt >> $1.txt
echo "" >>$1.txt

# Medir latencia
#Para medir la latencia usamos ping de igual forma, únicamente restringimos la
información a la cantidad de tiempo que tardó el paquete en llegar y regresar, lo
separamos en min, avg y max.
echo "*****Latencia:*****" >> $1.txt
min=$(grep "min/avg/max" ping.txt | awk '{print $4}' | cut -d '/' -f 1) #Obtenemos el
tiempo mínimo
avg=$(grep "min/avg/max" ping.txt | awk '{print $4}' | cut -d '/' -f 2) #obtenemos el
tiempo promedio
max=$(grep "min/avg/max" ping.txt | awk '{print $4}' | cut -d '/' -f 3) #obtenemos el
tiempo máximo
echo "min=$min" >> $1.txt #guardamos en el archivo de análisis
echo "avg=$avg" >> $1.txt
echo "max=$max" >> $1.txt
echo "" >>$1.txt
#Borramos nuestro archivo ping ya que no necesitamos más información de este
rm ping.txt
```

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

```
#La IP pública y sus segmentos
#Para obtener la IP usamos nslookup la cual nos permite consultar DNS para obtener
información sobre nombres de dominio específicos, como direcciones IP, registros MX y
registros de servicio (SRV).
echo "*****IP pública y sus segmentos:*****" >> $1.txt
nslookup $1 >> $1.txt
echo "" >>$1.txt

#Registros de disponibilidad
#Para este apartado usamos curl para procesar los registros disponibles
echo "***** Registros de disponibilidad *****" >> $1.txt
curl -s -o /dev/null -w "%{http_code}\n" $1 >> $1.txt
echo "" >>$1.txt

#Registro IPv4 e IPv6
#Usamos host para ver las IPs asociadas al dominio solicitado
echo "*****Registros IPv4 e IPv6*****" >> $1.txt
echo "-----IPv4-----" >> $1.txt
host -t A $1 >> $1.txt #Realizamos el tipo de consulta A para IPv4
echo "" >> $1.txt
echo "-----IPv6-----" >> $1.txt
host -t AAAA $1 >> $1.txt #Realizamos el tipo de consulta AAAA para IPv6
echo " " >> $1.txt

#Registros reversos
#Volvemos a hacer uso de Host
echo "*****Registros reversos:*****" >> $1.txt
host $1 >> $1.txt
echo " " >> $1.txt

#Ruta y los saltos para llegar al dominio
#Usaremos traceroute para rastrear la ruta que sigue un paquete de datos desde su
origen hasta su destino final. En otras palabras, veremos los nodos de red que un
paquete atraviesa mientras se mueve desde su origen hasta su destino.
echo "***** Ruta y saltos *****" >> $1.txt
traceroute $1 >> $1.txt
echo " " >> $1.txt

#Enumerar lo DNS
#Dig nos sirve para realizar consultas DNS y obtener información sobre nombres de
dominio y direcciones IP.
echo "*****Enumeración de DNS*****" >> $1.txt
echo "----Usando dig ----" >> $1.txt
dig +nocmd $1 >> $1.txt
echo " " >> $1.txt
#Para otro enfoque usamos dnsrecon la cual sirve para realizar pruebas de enumeración
y recolección de información de DNS
echo "----Usando dnsrecon ----" >> $1.txt
dnsrecon -d $1 -t std >> $1.txt
echo " " >> $1.txt

#Puertos, estados y servicios
#Usamos Nmap ya que usa un escaneo de puertos para identificar los servicios que se
ejecutan en una máquina remota, así como para determinar si hay puertos abiertos que
podrían ser explotados por atacantes.
```

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

```
echo "*****Puertos, estados y servicios*****" >> $1.txt
nmap $1 >> $1.txt

#Ya que no necesitamos más datos de este
rm temp.txt
#Desplegamos el análisis obtenido
cat $1.txt
#Descomentar en caso de no querer almacenar la info completa
#rm $1.txt
```

## ● Procesamiento

A continuación mostramos los resultados obtenidos para los dominios especificados:

### ★ Análisis de **unam.mx**:

Domain Name: unam.mx  
Created On: 1989-03-31  
Last Updated On: 2022-12-09  
Expiration Date: 2023-03-30  
Registrant:  
Name: UNAM  
City: Mexico  
State: Distrito Federal  
Country: Mexico

Administrative Contact:

Name: HECTOR BENITEZ PEREZ  
City: Mexico  
State: Ciudad de Mexico  
Country: Mexico

Technical Contact:

Name: ALEJANDRO CRUZ SANTOS  
City: Mexico  
State: Ciudad de Mexico  
Country: Mexico

Billing Contact:

Name: UNIDAD ADMINISTRATIVA DGTIC  
City: Mexico  
State: Ciudad de Mexico  
Country: Mexico

\*\*\*\*\*Conectividad de la red:\*\*\*\*\*

```
PING unam.mx (132.248.166.20) 56(84) bytes of data.
64 bytes from 132.248.166.20 (132.248.166.20): icmp_seq=1 ttl=63 time=96.2 ms
64 bytes from 132.248.166.20 (132.248.166.20): icmp_seq=2 ttl=63 time=90.5 ms
64 bytes from 132.248.166.20 (132.248.166.20): icmp_seq=3 ttl=63 time=199 ms
64 bytes from 132.248.166.20 (132.248.166.20): icmp_seq=4 ttl=63 time=92.6 ms
```

```
--- unam.mx ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
```

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

rtt min/avg/max/mdev = 90.457/119.567/199.006/45.909 ms

\*\*\*\*\*Latencia:\*\*\*\*\*

min=90.457  
avg=119.567  
max=199.006

\*\*\*\*\*IP publica y sus segmentos:\*\*\*\*\*

Server: 10.0.2.3  
Address: 10.0.2.3#53

Non-authoritative answer:

Name: unam.mx  
Address: 132.248.166.20  
Name: unam.mx  
Address: 132.248.166.17  
Name: unam.mx  
Address: 132.248.166.18  
Name: unam.mx  
Address: 132.248.166.19  
Name: unam.mx  
Address: 2001:1218:3000:180::17  
Name: unam.mx  
Address: 2001:1218:3000:180::19  
Name: unam.mx  
Address: 2001:1218:3000:180::18  
Name: unam.mx  
Address: 2001:1218:3000:180::20

\*\*\*\*\* Registros de disponibilidad \*\*\*\*\*

301

\*\*\*\*\*Registros IPv4 e IPv6\*\*\*\*\*

-----IPv4-----

unam.mx has address 132.248.166.20  
unam.mx has address 132.248.166.19  
unam.mx has address 132.248.166.18  
unam.mx has address 132.248.166.17

-----IPv6-----

unam.mx has IPv6 address 2001:1218:3000:180::19  
unam.mx has IPv6 address 2001:1218:3000:180::20  
unam.mx has IPv6 address 2001:1218:3000:180::18  
unam.mx has IPv6 address 2001:1218:3000:180::17

\*\*\*\*\*Registros reversos:\*\*\*\*\*

unam.mx has address 132.248.166.18  
unam.mx has address 132.248.166.17  
unam.mx has address 132.248.166.20  
unam.mx has address 132.248.166.19  
unam.mx has IPv6 address 2001:1218:3000:180::18  
unam.mx has IPv6 address 2001:1218:3000:180::17  
unam.mx has IPv6 address 2001:1218:3000:180::20  
unam.mx has IPv6 address 2001:1218:3000:180::19

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

unam.mx mail is handled by 0 unam-mx.mail.protection.outlook.com.

```
***** Ruta y saltos *****
traceroute to unam.mx (132.248.166.17), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.193 ms  0.156 ms  0.143 ms
 2  _gateway (192.168.0.1)  7.769 ms  12.966 ms  12.890 ms
 3  10.176.0.1 (10.176.0.1)  32.422 ms  32.397 ms  32.408 ms
 4  * * *
 5  * * *
 6  10.3.13.33 (10.3.13.33)  43.011 ms  19.614 ms  19.456 ms
 7  customer-189-216-3-40.cablevision.net.mx (189.216.3.40)  22.100 ms  20.532 ms
 32.484 ms
 8  150.189-204-152.bestelclientes.com.mx (189.204.152.150)  44.115 ms  44.089 ms
 43.989 ms
 9  45.189-204-152.bestelclientes.com.mx (189.204.152.45)  42.595 ms  42.569 ms
 42.445 ms
10  8.243.220.101 (8.243.220.101)  62.680 ms  10.3.13.33 (10.3.13.33)  32.080 ms !X
 17.482 ms !X
```

\*\*\*\*\*Enumeración de DNS\*\*\*\*\*

```
--Usando dig -----
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15530
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;unam.mx.           IN      A

;; ANSWER SECTION:
unam.mx.          5395    IN      A      132.248.166.19
unam.mx.          5395    IN      A      132.248.166.18
unam.mx.          5395    IN      A      132.248.166.20
unam.mx.          5395    IN      A      132.248.166.17

;; Query time: 4 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: dom mar 05 22:15:10 CST 2023
;; MSG SIZE rcvd: 100
```

--Usando dnsrecon -----

```
[*] std: Performing General Enumeration against: unam.mx...
[-] All nameservers failed to answer the DNSSEC query for unam.mx
[*]     SOA ns1.unam.mx 132.248.108.221
[*]     NS ns3.unam.mx 132.248.108.215
[*]     NS ns3.unam.mx 2001:1218:100:10a:108::215
[*]     NS ns2.unam.mx 132.248.204.25
[*]     NS ns4.unam.mx 132.248.204.32
[*]     NS ns4.unam.mx 2001:1218:403:203:204::32
[*]     NS ns5.unam.mx 132.248.243.37
[*]     NS ns1.unam.mx 132.248.108.221
[*]     MX unam-mx.mail.protection.outlook.com 104.47.73.10
[*]     MX unam-mx.mail.protection.outlook.com 104.47.74.10
```

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

```

[*] A unam.mx 132.248.166.17
[*] A unam.mx 132.248.166.19
[*] A unam.mx 132.248.166.20
[*] A unam.mx 132.248.166.18
[*] AAAA unam.mx 2001:1218:3000:180::18
[*] AAAA unam.mx 2001:1218:3000:180::17
[*] AAAA unam.mx 2001:1218:3000:180::20
[*] AAAA unam.mx 2001:1218:3000:180::19
[*] TXT unam.mx v=spf1 ip4:132.247.28.137 ip4:132.247.190.11 ip4:132.248.10.70
ip4:132.248.10.100 ip4:200.53.148.150 ip4:200.53.148.151 ip4:200.53.148.152
ip4:200.53.148.158 include:spf.protection.outlook.com -all
[*] TXT unam.mx
hIYSSjVawRSRgYwMB8MWcUj81pD0+HgJrP9FE1TakicPFo+ODDkmH4LevTIS9JPz9Qx5f7qBF6FvYJ0A13QPvg
==

[*] Enumerating SRV Records
[+] SRV _sip._tls.unam.mx sipdir.online.lync.com 52.112.64.203 443
[+] SRV _sip._tls.unam.mx sipdir.online.lync.com 2603:1037:0:8::b 443
[+] SRV _sip._tls.unam.mx sipdir.online.lync.com 2603:1037:0:b::b 443
[+] SRV _sip._tls.unam.mx sipdir.online.lync.com 2603:1037:0:6::b 443
[+] SRV _sip._tls.unam.mx sipdir.online.lync.com 2603:1037:0:3::b 443
[+] SRV _sip._tls.unam.mx sipdir.online.lync.com 2603:1037:0:d::f 443
[+] SRV _sip._tls.unam.mx sipdir.online.lync.com 2603:1037:0:4::b 443
[+] SRV _sip._tls.unam.mx sipdir.online.lync.com 2603:1037:0:17::c 443
[+] SRV _sip._tls.unam.mx sipdir.online.lync.com 2603:1037:0:1::b 443
[+] SRV _sipfederationtls._tcp.unam.mx sipfed.online.lync.com 52.112.70.139 5061
[+] SRV _sipfederationtls._tcp.unam.mx sipfed.online.lync.com 2603:1037:0:1::b
5061
[+] 11 Records Found

```

\*\*\*\*\*Puertos, estados y servicios\*\*\*\*\*

```

Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-05 22:15 CST
Nmap scan report for unam.mx (132.248.166.19)
Host is up (0.031s latency).

Other addresses for unam.mx (not scanned): 132.248.166.20 132.248.166.17
132.248.166.18 2001:1218:3000:180::18 2001:1218:3000:180::17 2001:1218:3000:180::20
2001:1218:3000:180::19

Not shown: 997 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
554/tcp   open  rtsp
1723/tcp  open  pptp


```

Nmap done: 1 IP address (1 host up) scanned in 2.23 seconds

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

#### ★ Análisis de **ipn.mx**:

Domain Name: ipn.mx  
Created On: 1995-04-30  
Last Updated On: 2022-04-26  
Expiration Date: 2023-04-29  
Registrant:  
Name: Instituto Politecnico Nacional  
City: No hay informacion  
State: Distrito Federal  
Country: Mexico

Administrative Contact:

Name: Contacto NIC del IPN  
City: Mexico  
State: Distrito Federal  
Country: Mexico

Technical Contact:

Name: Departamento de Conectividad del IPN  
City: Mexico  
State: Distrito Federal  
Country: Mexico

Billing Contact:

Name: Contacto NIC del IPN  
City: Mexico  
State: Distrito Federal  
Country: Mexico

\*\*\*\*\*Conectividad de la red:\*\*\*\*\*

PING ipn.mx (104.214.26.43) 56(84) bytes of data.

--- ipn.mx ping statistics ---

4 packets transmitted, 0 received, 100% packet loss, time 3054ms

\*\*\*\*\*Latencia:\*\*\*\*\*

min=  
avg=  
max=

\*\*\*\*\*IP pública y sus segmentos:\*\*\*\*\*

Server: 10.0.2.3  
Address: 10.0.2.3#53

Non-authoritative answer:

Name: ipn.mx  
Address: 104.214.26.43

\*\*\*\*\* Registros de disponibilidad \*\*\*\*\*

301

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

\*\*\*\*\*Registros IPv4 e IPv6\*\*\*\*\*

-----IPv4-----

ipn.mx has address 104.214.26.43

-----IPv6-----

ipn.mx has no AAAA record

\*\*\*\*\*Registros reversos:\*\*\*\*\*

ipn.mx has address 104.214.26.43

ipn.mx mail is handled by 0 ipn-mx.mail.protection.outlook.com.

\*\*\*\*\* Ruta y saltos \*\*\*\*\*

traceroute to ipn.mx (104.214.26.43), 30 hops max, 60 byte packets

```

1 10.0.2.2 (10.0.2.2) 1.194 ms 1.226 ms 1.146 ms
2 _gateway (192.168.0.1) 5.098 ms 4.976 ms 4.943 ms
3 10.176.0.1 (10.176.0.1) 16.686 ms 19.474 ms 19.736 ms
4 * *
5 * *
6 10.3.13.33 (10.3.13.33) 23.166 ms 27.844 ms 27.670 ms
7 customer-189-216-3-40.cablevision.net.mx (189.216.3.40) 30.698 ms 30.633 ms
30.478 ms
8 150.189-204-152.bestelclientes.com.mx (189.204.152.150) 41.403 ms 40.889 ms
40.794 ms
9 45.189-204-152.bestelclientes.com.mx (189.204.152.45) 40.559 ms 40.457 ms
34.439 ms
10 129.189-202-244.bestelclientes.com.mx (189.202.244.129) 52.874 ms 55.780 ms
55.576 ms
11 bestel.mex30-96cbe-1b.ntwk.msn.net (104.44.198.59) 58.145 ms 57.966 ms 57.897
ms
12 ae24-0.icr02.sn1.ntwk.msn.net (104.44.234.218) 83.230 ms 104.44.49.131
(104.44.49.131) 76.351 ms 72.233 ms
13 * *
14 * *
15 * *
16 * *
17 * *
18 * *
19 * *
20 * *
21 * *
22 * *
23 * *
24 * *
25 * *
26 * *
27 * *
28 * *
29 * *
30 * *
```

\*\*\*\*\*Enumeración de DNS\*\*\*\*\*

-----Usando dig -----

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41253

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

# Criptografía y Seguridad

## Pentesting: Recopilación de Información

```

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ipn.mx.                      IN      A

;; ANSWER SECTION:
ipn.mx.           3128    IN      A      104.214.26.43

;; Query time: 0 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: dom mar 05 22:19:58 CST 2023
;; MSG SIZE rcvd: 51

-----Usando dnsrecon -----
[*] std: Performing General Enumeration against: ipn.mx...
[-] All nameservers failed to answer the DNSSEC query for ipn.mx
[*]      SOA dns1.ipn.mx 148.204.103.2
[*]      NS dns1.ipn.mx 148.204.103.2
[*]      NS dns2.ipn.mx 148.204.198.2
[*]      NS dns3.ipn.mx 148.204.235.2
[*]      MX ipn-mx.mail.protection.outlook.com 104.47.73.10
[*]      MX ipn-mx.mail.protection.outlook.com 104.47.74.10
[*]      A ipn.mx 104.214.26.43
[*]      TXT ipn.mx
cisco-ci-domain-verification=307996563beb52e5dc9afeb332f03fb418c000eac99844337394ad33b
8a4280f
[*]      TXT ipn.mx v=spf1 ip4:148.204.103.190/32 ip4:148.204.103.31/32
ip4:148.204.103.9/32 ip4:148.204.103.30/32 include:_spf.google.com
include:spf.protection.outlook.com -all
[*]      TXT ipn.mx MS=ms47790906
[*]      TXT ipn.mx
o6ymFg6zAtvtZWNiR5CHl1jZCZ0l2JBs4w2KowjUovMflgCTld95BDKL0/WRaYRPVOTzTKU0YwKz5MzzXjLuk5Q
==
[*]      TXT ipn.mx
5LEGIzBjtK0WgL/wH3Rm0H/3QViSGfZqr0JyCp7dbNjwgq92KPvG/Ws3T7VVUVdfj4iMcWz1RhMDBm+FEHnvwQ
==
[*]      TXT ipn.mx j0rgi81b184ijt7ggt6c70t3ln
[*]      TXT ipn.mx
google-site-verification=4f9Y7GzioIxex65vzemp0YQivTmv4dCPNB49saWVceBk
[*]      TXT _dmarc.ipn.mx v=DMARC1; p=reject; pct=100; rua=mailto:correo@ipn.mx;
ruf=mailto:dmarc_forensic@ipn.mx; fo=1
[*] Enumerating SRV Records
[+]      SRV _sipinternaltls._tcp.ipn.mx im.ipn.mx 148.204.103.16 5061
[+]      SRV _sip._tls.ipn.mx im.ipn.mx 148.204.103.16 5061
[+]      SRV _sipfederationtls._tcp.ipn.mx im.ipn.mx 148.204.103.16 5061
[+]      SRV _autodiscover._tcp.ipn.mx correo.ipn.mx 148.204.103.31 443
[+]      SRV _autodiscover._tcp.ipn.mx correo.ipn.mx 148.204.103.30 443
[+] 5 Records Found

*****Puertos, estados y servicios*****
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-05 22:20 CST
Nmap scan report for ipn.mx (104.214.26.43)
Host is up (0.030s latency).
```

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

Not shown: 995 filtered ports

PORT STATE SERVICE

21/tcp open ftp

80/tcp open http

443/tcp open https

554/tcp open rtsp

1723/tcp open pptp

Nmap done: 1 IP address (1 host up) scanned in 7.02 seconds

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

#### ★ Análisis de **pemex.com**:

```
Domain Name: PEMEX.COM
>>> Last update of whois database: 2023-03-06T04:16:18Z <<<
Registrar Registration Expiration Date: 2023-06-20T00:00:00-0500
```

\*\*\*\*\*Conectividad de la red:\*\*\*\*\*

```
PING pemex.com (200.23.91.20) 56(84) bytes of data.
```

```
--- pemex.com ping statistics ---
```

```
4 packets transmitted, 0 received, 100% packet loss, time 3079ms
```

\*\*\*\*\*Latencia:\*\*\*\*\*

```
min=
avg=
max=
```

\*\*\*\*\*IP pública y sus segmentos:\*\*\*\*\*

```
Server: 10.0.2.3
Address: 10.0.2.3#53
```

Non-authoritative answer:

```
Name: pemex.com
Address: 200.23.91.20
```

\*\*\*\*\* Registros de disponibilidad \*\*\*\*\*

```
200
```

\*\*\*\*\*Registros IPv4 e IPv6\*\*\*\*\*

-----IPv4-----

```
pemex.com has address 200.23.91.20
```

-----IPv6-----

```
pemex.com has no AAAA record
```

\*\*\*\*\*Registros reversos:\*\*\*\*\*

```
pemex.com has address 200.23.91.20
```

```
pemex.com mail is handled by 5 pemex-com.mail.protection.outlook.com.
```

\*\*\*\*\* Ruta y saltos \*\*\*\*\*

```
traceroute to pemex.com (200.23.91.20), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.670 ms  0.526 ms  0.462 ms
 2  _gateway (192.168.0.1)  4.514 ms  4.413 ms  4.352 ms
 3  10.176.0.1 (10.176.0.1)  19.384 ms  19.312 ms  19.139 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  10.3.13.33 (10.3.13.33)  27.693 ms  27.519 ms  27.456 ms
 9  customer-189-216-3-40.cablevision.net.mx (189.216.3.40)  28.190 ms  26.241 ms
26.127 ms
10  10.3.13.33 (10.3.13.33)  43.880 ms !X  43.697 ms !X
150.189-204-152.bestelclientes.com.mx (189.204.152.150)  96.760 ms
```

# Criptografía y Seguridad

## Pentesting: Recopilación de Información

```
*****Enumeración de DNS*****
-----Usando dig -----
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36681
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;pemex.com.           IN      A

;; ANSWER SECTION:
pemex.com.        45      IN      A      200.23.91.20

;; Query time: 4 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: dom mar 05 22:16:46 CST 2023
;; MSG SIZE rcvd: 54

-----Usando dnsrecon -----
[*] std: Performing General Enumeration against: pemex.com...
[-] All nameservers failed to answer the DNSSEC query for pemex.com
[*]     SOA dns1.p07.nsone.net 198.51.44.7
[*]     SOA dns1.p07.nsone.net 2620:4d:4000:6259:7:7:0:1
[*]     NS dns1.p07.nsone.net 198.51.44.7
[*]     NS dns1.p07.nsone.net 2620:4d:4000:6259:7:7:0:1
[*]     NS dns2.p07.nsone.net 198.51.45.7
[*]     NS dns2.p07.nsone.net 2a00:edc0:6259:7:7::2
[*]     NS dns3.p07.nsone.net 198.51.44.71
[*]     NS dns3.p07.nsone.net 2620:4d:4000:6259:7:7:0:3
[*]     NS dns4.p07.nsone.net 198.51.45.71
[*]     NS dns4.p07.nsone.net 2a00:edc0:6259:7:7::4
[*]     MX pemex-com.mail.protection.outlook.com 104.47.73.138
[*]     MX pemex-com.mail.protection.outlook.com 104.47.73.10
[*]     A pemex.com 200.23.91.20
[*]     TXT pemex.com
fSHVs2u9ZSfKCv401p4gL5XJt0DUVzy3YPPQyctR1gcRmJTG0Z2tMD83rjIzSjKH7nx9he/+03ZJk8rGt2TqYA
==

[*]     TXT pemex.com MS=ms13272953
[*]     TXT pemex.com
google-site-verification=ISHwEmA3TCA5q-qRYZXLcQRahFyPg9T1p929TeHdziwhFyPg9T1p929TeHdzi
w
[*]     TXT pemex.com v=spf1 include:spf1.pemex.com include:spf2.pemex.com
include:spf.protection.outlook.com include:_spf.google.com ~all
[*]     TXT pemex.com
google-site-verification=N0byGdjkIv0Rhi6BADcsSYyETtFbWceNqR8Ebaxqw7A
[*]     TXT _dmarc.pemex.com
v=DMARC1;p=quarantine;adkim=s;aspf=s;fo=1;ri=3600;pct=100;rua=mailto:seguridad.inciden
tes@pemex.com;ruf=mailto:seguridad.incidentes@pemex.com
[*] Enumerating SRV Records
[+]     SRV _xmpp-server._tcp.pemex.com sipmx.pemex.com 200.23.91.144 5269
[+]     SRV _xmpp-server._tcp.pemex.com sipmx.pemex.com 200.188.13.145 5269
[+]     SRV _sipfederationtls._tcp.pemex.com sipfed.online.lync.com 52.112.66.11 5061
```

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

```
[+] SRV _sipfederationtls._tcp.pemex.com sipfed.online.lync.com 2603:1037:0:d::f  
5061  
[+] SRV _sipfederationtls._tcp.pemex.com sipfed.online.lync.com 2603:1037:0:3::b  
5061  
[+] SRV _sipfederationtls._tcp.pemex.com sipfed.online.lync.com 2603:1037:0:6::b  
5061  
[+] SRV _sipfederationtls._tcp.pemex.com sipfed.online.lync.com 2603:1037:0:b::b  
5061  
[+] SRV _sipfederationtls._tcp.pemex.com sipfed.online.lync.com 2603:1037:0:8::b  
5061  
[+] SRV _sipfederationtls._tcp.pemex.com sipfed.online.lync.com 2603:1037:0:1::b  
5061  
[+] SRV _sipfederationtls._tcp.pemex.com sipfed.online.lync.com 2603:1037:0:17::c  
5061  
[+] SRV _sipfederationtls._tcp.pemex.com sipfed.online.lync.com 2603:1037:0:4::b  
5061  
[+] SRV _sip._tls.pemex.com sipdir.online.lync.com 52.112.65.139 443  
[+] SRV _sip._tls.pemex.com sipdir.online.lync.com 2603:1037:0:b::b 443  
[+] SRV _autodiscover._tcp.pemex.com correo.pemex.com 200.23.91.90 443  
[+] 14 Records Found
```

\*\*\*\*\*Puertos, estados y servicios\*\*\*\*\*

Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-05 22:16 CST

Nmap scan report for pemex.com (200.23.91.20)

Host is up (0.020s latency).

rDNS record for 200.23.91.20: www.pemex.com

Not shown: 997 filtered ports

PORT	STATE	SERVICE
------	-------	---------

21/tcp	open	ftp
--------	------	-----

554/tcp	open	rtsp
---------	------	------

1723/tcp	open	pptp
----------	------	------

Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

- ★ Análisis de **www.gob.mx**: (se añade www ya que sin este no existe la página)

Domain Name: www.gob.mx  
Created On: 2002-03-01  
Last Updated On: 2023-03-01  
Expiration Date: 2024-02-28  
Registrant:  
Name: Secretaría de la Función Pública  
City: México  
State: Distrito Federal  
Country: México

Administrative Contact:

Name: Eduardo Martínez Vargas  
City: México  
State: Ciudad de México  
Country: México

Technical Contact:

Name: Eduardo Martínez Vargas  
City: México  
State: Ciudad de México  
Country: México

Billing Contact:

Name: Eduardo Martínez Vargas  
City: México  
State: Ciudad de México  
Country: México

\*\*\*\*\*Conectividad de la red:\*\*\*\*\*

```
PING www.gob.mx (23.200.40.201) 56(84) bytes of data.  
64 bytes from a23-200-40-201.deploy.static.akamaitechnologies.com (23.200.40.201):  
icmp_seq=1 ttl=63 time=58.9 ms  
64 bytes from a23-200-40-201.deploy.static.akamaitechnologies.com (23.200.40.201):  
icmp_seq=2 ttl=63 time=72.1 ms  
64 bytes from a23-200-40-201.deploy.static.akamaitechnologies.com (23.200.40.201):  
icmp_seq=3 ttl=63 time=64.2 ms  
64 bytes from a23-200-40-201.deploy.static.akamaitechnologies.com (23.200.40.201):  
icmp_seq=4 ttl=63 time=70.8 ms
```

--- www.gob.mx ping statistics ---

```
4 packets transmitted, 4 received, 0% packet loss, time 3006ms  
rtt min/avg/max/mdev = 58.883/66.488/72.052/5.297 ms
```

\*\*\*\*\*Latencia:\*\*\*\*\*

```
min=58.883  
avg=66.488  
max=72.052
```

\*\*\*\*\*IP pública y sus segmentos:\*\*\*\*\*

```
Server: 10.0.2.3  
Address: 10.0.2.3#53
```

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

Non-authoritative answer:

```
Name: www.gob.mx
Address: 23.200.40.201
Name: www.gob.mx
Address: 23.200.40.207
```

\*\*\*\*\* Registros de disponibilidad \*\*\*\*\*

301

\*\*\*\*\*Registros IPv4 e IPv6\*\*\*\*\*

-----IPv4-----

```
www.gob.mx has address 23.200.40.201
www.gob.mx has address 23.200.40.207
```

-----IPv6-----

```
www.gob.mx has no AAAA record
```

\*\*\*\*\*Registros reversos:\*\*\*\*\*

```
www.gob.mx has address 23.200.40.207
www.gob.mx has address 23.200.40.201
```

\*\*\*\*\* Ruta y saltos \*\*\*\*\*

```
traceroute to www.gob.mx (23.200.40.207), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  1.075 ms  1.075 ms  1.049 ms
 2  _gateway (192.168.0.1)  11.737 ms  11.631 ms  11.595 ms
 3  10.176.0.1 (10.176.0.1)  29.138 ms  29.097 ms  29.065 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  10.3.13.33 (10.3.13.33)  37.895 ms  37.697 ms  59.275 ms
 9  customer-189-216-3-40.cablevision.net.mx (189.216.3.40)  59.219 ms  35.781 ms
35.638 ms
10  150.189-204-152.bestelclientes.com.mx (189.204.152.150)  324.708 ms  324.512 ms
324.441 ms
11  45.189-204-152.bestelclientes.com.mx (189.204.152.45)  68.792 ms  68.624 ms
68.558 ms
12  216.171.70.209 (216.171.70.209)  324.093 ms  408.763 ms  303.173 ms
13  * * *
14  201-174-250-45.transtelco.net (201.174.250.45)  360.494 ms  360.434 ms  356.743 ms
15  201-174-17-121.transtelco.net (201.174.17.121)  356.598 ms  356.534 ms  200.092 ms
16  * * *
17  * * *
18  a23-200-40-207.deploy.static.akamaitechnologies.com (23.200.40.207)  80.671 ms
80.542 ms  80.158 ms
```

\*\*\*\*\*Enumeración de DNS\*\*\*\*\*

----Usando dig -----

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33984
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
```

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

```

;www.gob.mx.           IN      A
;; ANSWER SECTION:
www.gob.mx.          20      IN      A      23.200.40.207
www.gob.mx.          20      IN      A      23.200.40.201

;; Query time: 415 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: dom mar 05 22:32:56 CST 2023
;; MSG SIZE rcvd: 71

-----Usando dnsrecon -----
[*] std: Performing General Enumeration against: www.gob.mx...
[-] All nameservers failed to answer the DNSSEC query for www.gob.mx
[*]      SOA a20-66.akam.net 95.100.175.66
[*]      SOA a20-66.akam.net 2a02:26f0:67::42
[*]      NS a3-64.akam.net 96.7.49.64
[*]      NS a3-64.akam.net 2600:1408:1c::40
[*]      NS a7-65.akam.net 23.61.199.65
[*]      NS a7-65.akam.net 2600:1406:32::41
[*]      NS a26-67.akam.net 23.74.25.67
[*]      NS a26-67.akam.net 2600:1480:b800::43
[*]      NS a20-66.akam.net 95.100.175.66
[*]      NS a20-66.akam.net 2a02:26f0:67::42
[*]      NS a8-66.akam.net 2.16.40.66
[*]      NS a8-66.akam.net 2600:1403:a::42
[*]      NS a1-179.akam.net 193.108.91.179
[*]      NS a1-179.akam.net 2600:1401:2::b3
[*]      A www.gob.mx 23.200.40.201
[*]      A www.gob.mx 23.200.40.207
[*]      TXT www.gob.mx F5CB-F102-317B-3B51-2A29-42A3-AD10-7D03
[*]      TXT www.gob.mx 9pqb3gtylk1084922kk6h8g017fnzbn0
[*]      TXT www.gob.mx 60vqrrb0gcnj7ccvd363ddyzg0hplddr
[*]      TXT www.gob.mx
google-site-verification=2qSWKNVNb4P05xP4WF17Xr-0_IT05-5KYAgIPutXByE
[*]      TXT www.gob.mx 7GLOHC2NGG8QGB9S5A1F2GC2U0
[*] Enumerating SRV Records
[+] 0 Records Found

*****Puertos, estados y servicios*****
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-05 22:33 CST
Nmap scan report for www.gob.mx (23.200.40.201)
Host is up (0.027s latency).
Other addresses for www.gob.mx (not scanned): 23.200.40.207
rDNS record for 23.200.40.201: a23-200-40-201.deploy.static.akamaitechnologies.com
Not shown: 994 filtered ports
PORT      STATE     SERVICE
21/tcp    open      ftp
53/tcp    closed    domain
80/tcp    open      http
443/tcp   open      https
554/tcp   open      rtsp
1723/tcp  open      pptp

Nmap done: 1 IP address (1 host up) scanned in 6.17 seconds

```

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

#### ● Análisis

##### **ipn.mx**

El dominio fue creado el 30 de abril de 1995 y expira el 29 de abril de 2023.

El registrante es el Instituto Politécnico Nacional, ubicado en la Ciudad de México, México.

Los contactos 'administrativo', 'técnico' y de 'facturación' son personas afiliadas al IPN.

La dirección IP asociada al dominio es 104.214.26.43.

El resultado del traceroute muestra 30 saltos para llegar al servidor IP y algunos paquetes se perdieron en el camino.

El análisis de la disponibilidad del sitio web muestra que hay una redirección HTTP 301.

##### **unam.mx**

Fue creada en 1989 y se actualizó por última vez en diciembre de 2022. Su fecha de expiración es el 30 de marzo de 2023.

El dominio es propiedad de la propia UNAM, y tiene diferentes contactos para la gestión del registro. Héctor Benítez Pérez es el contacto administrativo, Alejandro Cruz Santos es el contacto técnico y la Unidad Administrativa DGTIC es el contacto de facturación.

La página web cuenta con una buena conectividad de red, con una latencia media de 119.567 ms y un tiempo de respuesta máximo de 199.006 ms. La dirección IP pública del servidor principal de la página web es 132.248.166.20, y tiene varias direcciones IPv6 también.

La página web tiene registros de disponibilidad y respuesta al ping, así como registros de direcciones IPv4 e IPv6 y registros inversos.

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

#### **pemex.com**

El registro de DNS muestra que el nombre de dominio pemex.com se asigna a la dirección IP 200.23.91.20. No se proporciona información adicional sobre segmentos de IP.

La disponibilidad de pemex.com tiene 200 registros, por lo que creemos que el dominio ha sido utilizado para diversos fines.

El registro de DNS indica que pemex.com tiene una dirección IPv4 200.23.91.20, pero no tiene un registro de IPv6.

También observamos que el correo electrónico de pemex.com se maneja a través de los servidores de outlook.com.

La herramienta traceroute muestra 30 saltos hacia pemex.com. Algunos saltos se ven diferentes, lo que sugiere que puede haber problemas en el camino.

#### **www.gob.com**

Fue creado el 1 de marzo de 2002. La última actualización del registro de dominio fue el 1 de marzo de 2023 y su fecha de expiración es el 28 de febrero de 2024. El registro del dominio está a nombre de la Secretaría de la Función Pública, y Eduardo Martinez Vargas figura como contacto administrativo, técnico y de facturación.

La dirección IP del sitio web es 23.200.40.201 y 23.200.40.207.

La enumeración de DNS revela que el sitio web tiene un registro A para IPv4 y no tiene un registro AAAA para IPv6.

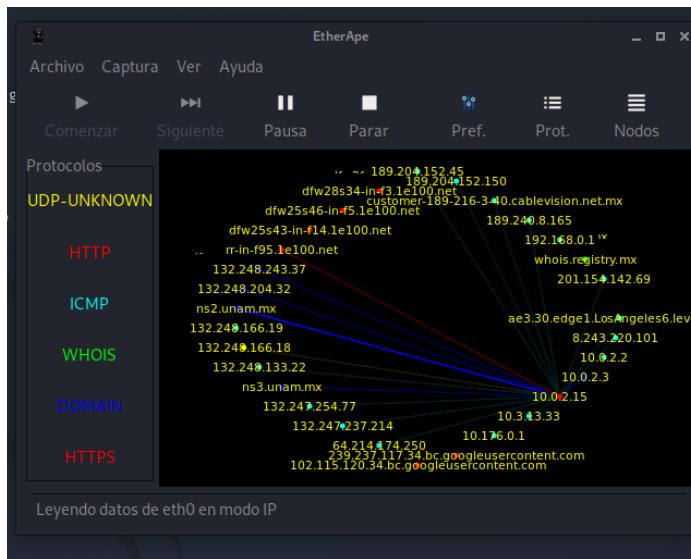
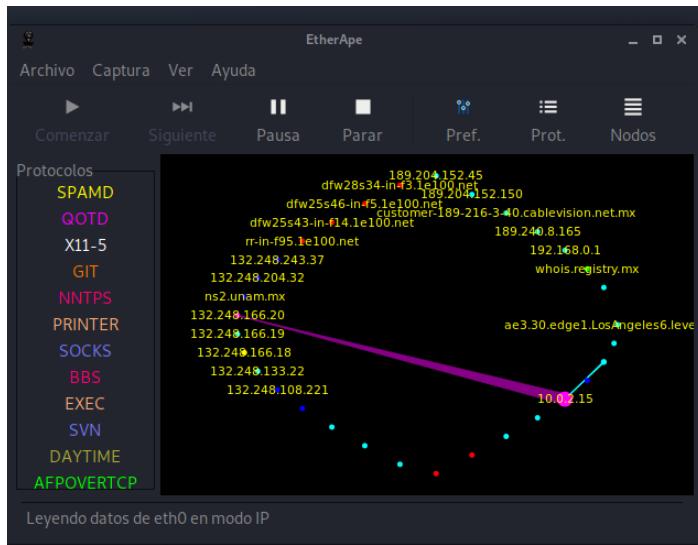
La ruta de acceso a la dirección IP se realiza a través de varios saltos, y la lista de DNS no está disponible.

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

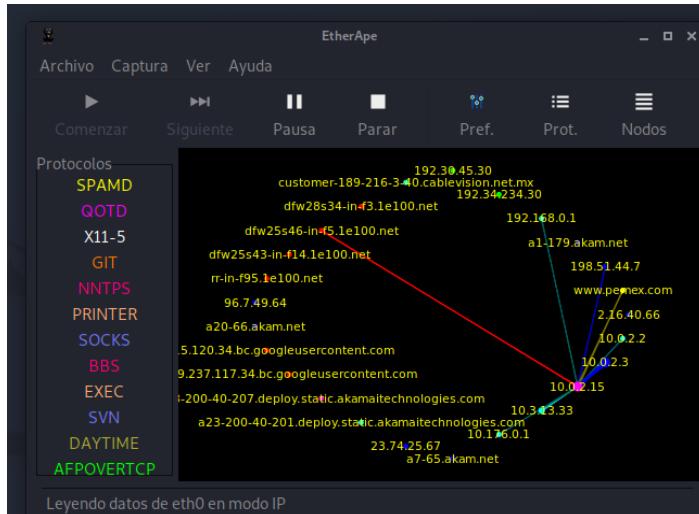
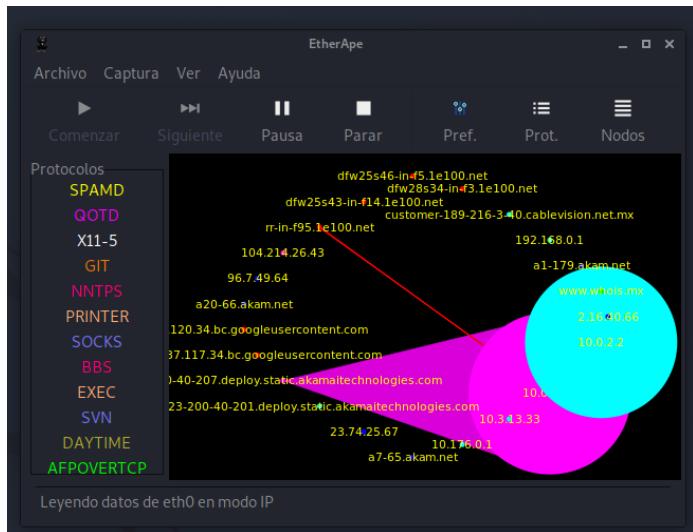
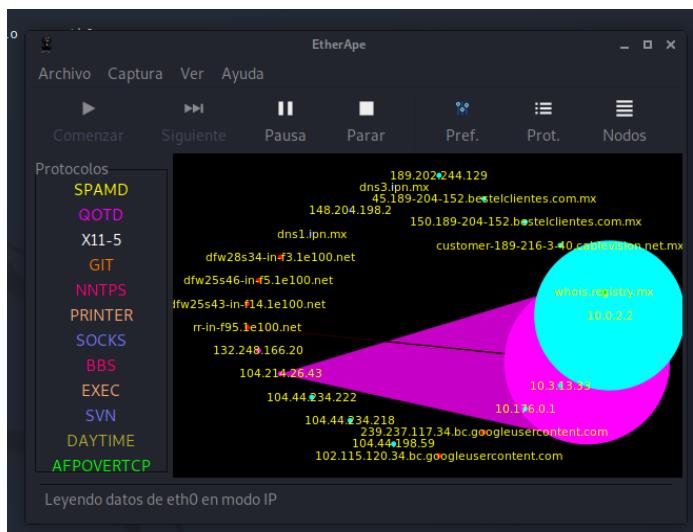
#### Etherape

A través de **Etherape** monitoreamos el estado de la red al momento de realizar las pruebas, pudimos observar cómo se fue formando una estrella de enlaces entre nuestro ordenador hacia otros sitios en la red de igual forma notamos que el tamaño de las líneas era proporcional al tráfico de datos que se estaban mandando/recibiendo el respectivo nodo.



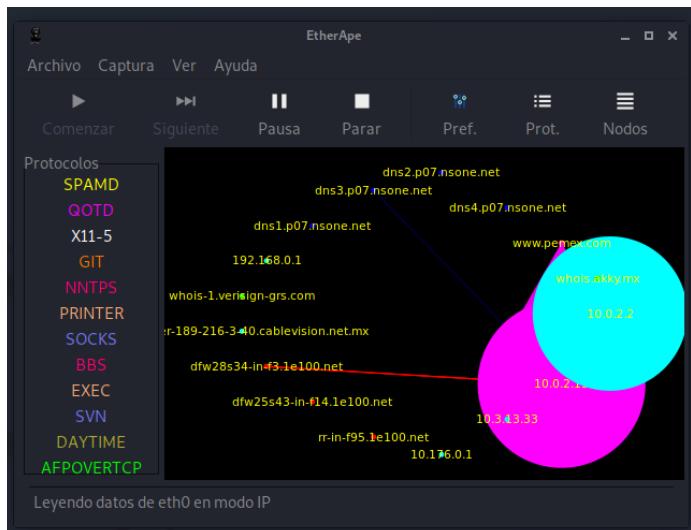
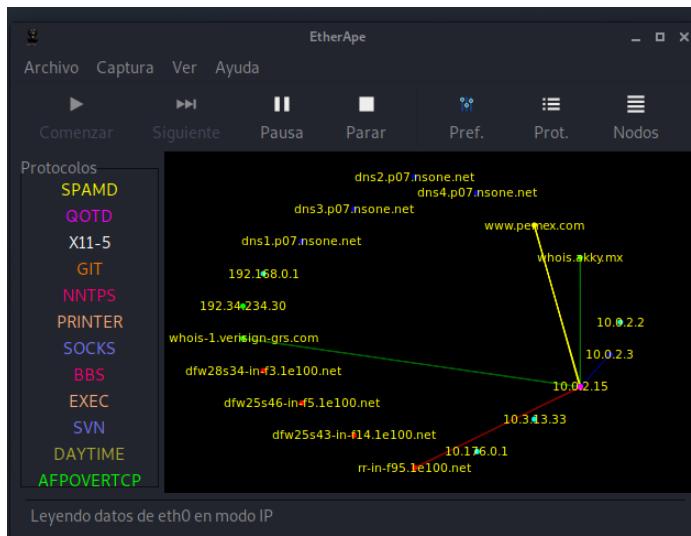
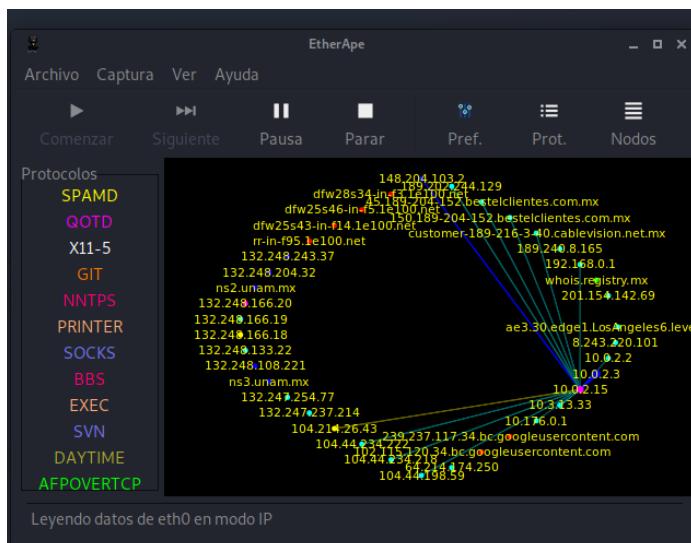
## Criptografía y Seguridad

### Pentesting: Recopilación de Información



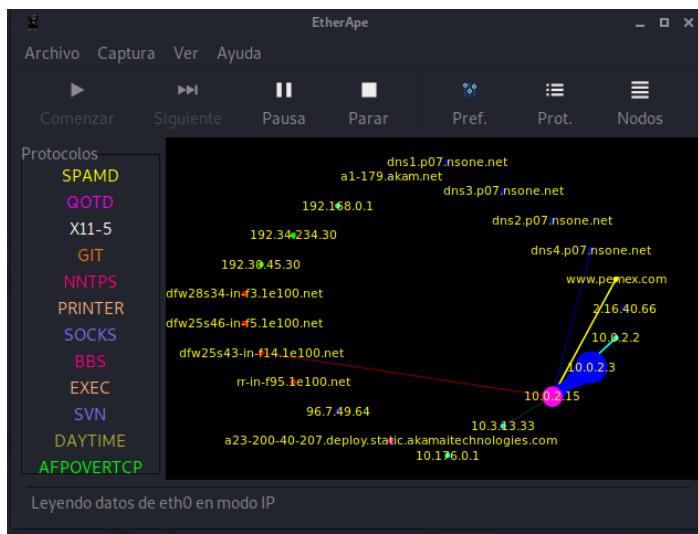
# Criptografía y Seguridad

## Pentesting: Recopilación de Información



# Criptografía y Seguridad

## Pentesting: Recopilación de Información



### ● Presentación

#### **www.gob.com**

Se puede concluir que el sitio web [www.gob.mx](http://www.gob.mx) se encuentra disponible y responde de manera rápida.

#### **ipn.mx**

No fue posible establecer conexión con el servidor a través **PING**, no está respondiendo a los paquetes de red enviados por lo que no podemos observar la latencia. Al hacer traceroute se muestra que la conexión se interrumpe en algún punto de la ruta hacia el servidor, por lo que podemos suponer que ocurre un problema en la red que impide que los paquetes lleguen al servidor. En resumen, parece que hay un problema de conectividad con el servidor.

#### **unam.mx**

El resultado muestra que la conexión al servidor de [unam.mx](http://unam.mx) es buena, con un promedio de latencia de alrededor de 119 ms, lo que indica que la conexión puede ser un poco lenta pero sigue siendo funcional. También se muestra que la dirección IP del servidor de [unam.mx](http://unam.mx) tiene tanto direcciones IPv4 como IPv6.

#### **pemex.com**

Se puede decir que la página web de Pemex está activa y tiene una dirección IP pública asignada. Sin embargo, no se pudo hacer ping al servidor, lo que indica que el servidor puede estar temporalmente inaccesible. Además, el análisis de ruta muestra que el tráfico puede pasar por varios saltos intermedios antes de llegar al servidor de Pemex y en algunos casos, el tráfico se pierde o se bloquea en saltos intermedios.

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

## PREGUNTAS

### 1. Menciona los tipos de protocolos de red

- a. **TCP/IP** (Transmission Control Protocol/Internet Protocol): es el protocolo de red más utilizado en todo el mundo y es el que rige el funcionamiento de Internet.
- b. **HTTP** (Hypertext Transfer Protocol): es el protocolo utilizado por la World Wide Web para transmitir información en forma de páginas web.
- c. **FTP** (File Transfer Protocol): Es un protocolo que permite la transferencia de archivos entre dos sistemas.
- d. **SMTP** (Simple Mail Transfer Protocol): es el protocolo utilizado para enviar correo electrónico a través de Internet.
- e. **DNS** (Domain Name System): es el protocolo que se utiliza para traducir los nombres de dominio en direcciones IP.
- f. **SSH** (Secure Shell): es un protocolo que permite conectarse de forma segura a un servidor remoto.
- g. **SNMP** (Simple Network Management Protocol): es un protocolo utilizado para administrar y supervisar dispositivos de red.
- h. **ICMP** (Internet Control Message Protocol): es un protocolo utilizado para diagnosticar problemas de red, como la comprobación de la conectividad y la detección de errores.

### 2. Respecto a tu pregunta anterior ¿Cómo funcionan? ¿Para qué sirven?

Los protocolos de red son reglas y estándares que establecen cómo se deben comunicar los dispositivos en una red. Cada protocolo tiene su propia función específica y define el formato y la secuencia de los mensajes que se envían entre los dispositivos.

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

Cada protocolo tiene un propósito específico. Algunos sirven para permitir que los dispositivos se comuniquen entre sí, mientras que otros se utilizan para administrar la red, diagnosticar problemas o transferir datos.

Por ejemplo, el protocolo TCP/IP se utiliza para la transmisión de datos a través de Internet. Este protocolo divide los datos en paquetes y los envía de manera eficiente a través de la red, asegurándose de que lleguen a su destino sin errores ni pérdida de datos.

El protocolo HTTP se utiliza para la transferencia de páginas web. Cuando un usuario introduce una dirección URL en su navegador, el navegador utiliza HTTP para solicitar la página al servidor web y luego muestra la página en el navegador del usuario.

El protocolo FTP se utiliza para transferir archivos entre dispositivos en una red. Los usuarios pueden cargar o descargar archivos de un servidor FTP utilizando un cliente FTP.

En resumen, los protocolos de red son fundamentales para el funcionamiento de cualquier red de computadoras. Cada protocolo tiene una función específica y define las reglas y estándares que se deben seguir para que los dispositivos se comuniquen de manera efectiva.

### 3. ¿Qué es un sniffer?

Un **sniffer** (también conocido como "analizador de protocolos" o "packet sniffer") es una herramienta de software o hardware que se utiliza para capturar y analizar el tráfico de red en una red de computadoras.

Un sniffer es capaz de interceptar y registrar los paquetes de datos que se transmiten a través de la red, lo que permite a los usuarios obtener información detallada sobre el tráfico de red, como la dirección IP de origen y destino, los protocolos utilizados, los puertos de origen y destino, y el contenido de los datos.

Los sniffers pueden ser utilizados para diversos fines, incluyendo:

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

Diagnóstico de problemas de red: los sniffers pueden ayudar a identificar problemas de red, como congestión, errores de configuración o fallos en los dispositivos de red.

Seguridad de la red: los sniffers pueden ser utilizados por los administradores de seguridad de red para detectar posibles intrusiones o actividades malintencionadas en la red.

Análisis de tráfico: los sniffers pueden ser utilizados para analizar el tráfico de red y obtener información útil, como los patrones de uso de la red, las tendencias de tráfico y las estadísticas de ancho de banda.

Es importante destacar que los sniffers también pueden ser utilizados con fines maliciosos, como el espionaje o la captura de contraseñas y otros datos sensibles. Por lo tanto, es fundamental utilizar herramientas de seguridad y medidas de protección adecuadas para evitar que los sniffers sean utilizados de manera indebida.

#### 4. OSINT, ¿Qué es? ¿Para qué sirve?

OSINT (Open Source Intelligence) es un término que se refiere a la recopilación y análisis de información de fuentes de acceso público, como sitios web, redes sociales, noticias y otras fuentes de información disponibles en línea.

Se utiliza para recopilar información sobre personas, organizaciones, eventos, tendencias y otros temas relevantes. Esta información puede ser utilizada para una amplia variedad de fines, incluyendo la investigación criminal, la inteligencia militar, la ciberseguridad, la investigación de mercado, la toma de decisiones empresariales y otras aplicaciones.

Es una técnica valiosa porque proporciona acceso a información que de otra manera sería difícil o costosa de obtener. Además, la información obtenida a través del OSINT es de fuentes de acceso público y, por lo tanto,

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

no viola la privacidad o los derechos legales de las personas u organizaciones.

Entre las herramientas que se utilizan para el OSINT se encuentran los motores de búsqueda avanzados, las herramientas de análisis de redes sociales, los scrapers de datos y otras herramientas de análisis de información.

Es importante destacar que también presenta algunos riesgos, como la posibilidad de que la información sea incompleta, inexacta o manipulada. Por lo tanto, es importante utilizar técnicas de análisis adecuadas y verificar la información obtenida a través del OSINT antes de tomar decisiones importantes basadas en ella.

#### 5. Investiga los 5 OSINT más usados.

- **Maltego:** Es una herramienta de inteligencia de código abierto que se utiliza para recopilar y analizar información de diversas fuentes de OSINT. Permite a los usuarios visualizar y analizar datos de diferentes fuentes, incluyendo redes sociales, bases de datos públicas y registros de dominios.
- **Shodan:** Shodan es un motor de búsqueda especializado en la búsqueda de dispositivos conectados a Internet, como cámaras web, servidores y routers. Es útil para la investigación de vulnerabilidades de seguridad en dispositivos conectados a Internet.
- **Recon-ng:** Recon-ng es una herramienta de inteligencia de código abierto que permite a los usuarios recopilar información de fuentes de OSINT utilizando técnicas de recopilación de datos automatizadas. Es útil para la recopilación de información sobre objetivos específicos en línea.
- **Nexvision:** es una herramienta que se utiliza para buscar información sobre personas y empresas en línea. Esta herramienta utiliza técnicas avanzadas de búsqueda para rastrear fuentes de información en la web, incluyendo redes sociales, foros, blogs y otras fuentes de acceso público. Nexvision también ofrece funciones de análisis de datos, lo que permite a los usuarios obtener información detallada y relevante a partir de la información obtenida.
- **Google Dorks:** son términos de búsqueda avanzados que se utilizan para buscar información específica en Google y otros motores de búsqueda. Permiten a los usuarios buscar información específica, como archivos PDF, contraseñas, números de tarjetas de crédito, y otros tipos de información que podrían ser sensibles o confidenciales.

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

#### 6. ¿Por qué el eslabón más débil de seguridad es el humano?

Porque las personas pueden cometer errores o ser engañadas por los atacantes. Aunque los sistemas de seguridad pueden ser diseñados para ser muy seguros y difíciles de penetrar, los humanos pueden proporcionar una brecha de seguridad involuntaria. Muchas personas no están al tanto de los riesgos de seguridad, no entienden cómo proteger su información y no saben cómo identificar y responder a las amenazas de seguridad. Por lo tanto, los atacantes pueden aprovechar esta falta de conocimiento para obtener acceso no autorizado a sistemas o información.

#### 7. ¿Qué acciones haces para protegerte de ciberataques?

Utilizamos contraseñas seguras y diferentes para cada cuenta en línea, y las actualizamos regularmente, además de usar antivirus, 2FA y tener cuidado al navegar por internet.

#### 8. ¿Crees que tus métodos preventivos son suficientes?

Son insuficientes, ya que, por ejemplo se hace uso de redes wifi públicas o tener mejor gestión de mis contraseñas y los sitios a los que accede.

## Criptografía y Seguridad

### Pentesting: Recopilación de Información

#### Referencias:

Universidad Nacional Autónoma de México (UNAM). (s.f.). Seguridad informática [Contenido en línea]. Recuperado el 5 de marzo de 2023, de

[https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/795/mod\\_resource/content/7/contenido/index.html](https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/795/mod_resource/content/7/contenido/index.html)

Geekflare. (s.f.). Las 21 mejores herramientas OSINT para investigaciones digitales y seguridad. [Contenido en línea]. Recuperado el 5 de marzo de 2023, de <https://geekflare.com/es/osint-tools/>

Universitat de Barcelona (UB). (2020, 5 de marzo). OSINT: qué es y técnicas más usadas [Entrada de blog]. IL3. Recuperado el 5 de marzo de 2023, de

<https://www.il3.ub.edu/blog/osint-que-es-y-tecnicas-mas-usadas/>

ICANN. (2019). What is Whois? Internet Corporation for Assigned Names and Numbers.

<https://www.icann.org/resources/pages/whois-2019-03-05-en>

Microsoft. (2022). Ping.

<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ping>

RedesZone. (2019). Cómo usar nslookup para resolver DNS en Windows.

<https://www.redeszone.net/tutoriales/internet/nslookup-resolucion-dns-windows/>

Dang, T. (2021). Curl and Bash examples. LinuxHint. [https://linuxhint.com/curl\\_bash\\_examples/](https://linuxhint.com/curl_bash_examples/)

Singh, P. (2021, March 5). Host command in Linux with examples. GeeksforGeeks.

<https://www.geeksforgeeks.org/host-command-in-linux-with-examples/>

Hernández, J. (2019, January 7). Qué es y cómo funciona el comando tracert o traceroute en Windows. RedesZone.

<https://www.redeszone.net/tutoriales/internet/que-es-comando-tracert-traceroute/>

PhoenixNAP. (2021, February 23). Linux Dig Command Examples (Domain Information Groper).

<https://phoenixnap.com/kb/linux-dig-command-examples>

Kali Linux. (s. f.). DNSRecon. Recuperado el 3 de marzo de 2023, de

<https://www.kali.org/tools/dnsrecon/>

RedesZone. (2019). Cómo utilizar Nmap para escanear puertos en Windows y Linux. Recuperado el 3 de marzo de 2023, de

<https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/>