Criptografía y Seguridad 2025-2

Profesor: José de Jesús Galaviz Casas
Ayudante: Diana Berenice Hérnandez Alonso
Ayudante Laboratorio: María Ximena Lezama Hernández

Practica 01 - Pentesting: Recopilación de Información

No. de Cuenta
318229687
318309877

11 de Marzo del 2025

Desarrollo

- **Requisitos.**

  El objetivo del pentesting consiste en encontrar vulnerabilidades (o fallos) de un sistema a través de una simulación de un ataque de software o hardware. En esta práctica, nos centraremos en la primer fase, que es la fase de reconocimiento (recopilación de información), y abundaremos un poco en las fase de escaneo de vulnerabilidades y generaremos propuestas para la fase de explotación (no se realizara ningún ataque o simulación de ataque)[1].

  Para estos objetivos, necesitamos definir claramente:

  El problema (objetivo) a resolver. El cual es identificar el tipo de herramientas que se necesitan para obtener la información para realizar un escaneo (análisis) de vulnerabilidades en los dominios: unam.mx, pemex.com, gob.mx e ipn.mx.

  Para ese propósito, **el tipo de información que necesitamos** recopilar son datos específicos que nos permitan entender su infraestructura y posibles puntos débiles, nos centraremos en obtener los siguientes:

  1. Nombre del dominio.
  2. Cuando fue creado, actualizado y fecha de expiración.
  3. Nombre de la organización a la que pertenece y datos sobre esta (País, estado, ciudad, calle y código postal)
  4. Nombres del personal, email y teléfonos de contacto.
  5. Comprobación de la conectividad de la red.
  6. Medición de la latencia.
  7. La IP pública y sus segmentos.
  8. Registro de la disponibilidad.
  9. Registros IPv4 e IPv6.
  10. Registros reversos.
  11. La ruta y los saltos para llegar al dominio.
  12. Enumeración de las DNS.
  13. Puertos, estados y servicios.

  Todo esta información con el **propósito** de entender la estructura organizacional para posibles ataques de ingeniería social (puntos 2, 3 y 4), identificar puntos de entrada potenciales (puntos 7, 9, 10, 12 y 13), detectar configuraciones incorrectas en DNS y servidores (puntos 7, 9, 10 y 12), evaluar la disponibilidad y rendimiento de los servicios (puntos 5, 6 y 8), descubrir la topología

de red para planificar posibles rutas de ataque (punto 11), y analizar los servicios expuestos para identificar versiones potencialmente vulnerables (punto 13).

- **Identificación de fuentes de información**

  Para la recopilación de toda esta información, usaremos un conjunto de herramientas especializadas de Kali Linux que nos permiten realizar diferentes tipos de escaneos y análisis:

  - **Ping**: Utilizaremos este comando para probar rápidamente varios puntos de la red, lo cual sirve para diagnosticar problemas de conectividad, controlar el rendimiento de la red y comprobar la disponibilidad del servidor, lo cual una primera visión sobre el estado de los servicios [2].
  - **Nslookup**: Esta herramienta nos ayudará a determinar si el DNS está resolviendo correctamente los nombres y las direcciones IP. Además, fue hecho pensado para las consultas de direcciones IPv4 e IPv6 [3].
  - **Whois**: Utilizaremos este servicio para determinar el propietario de un nombre de dominio o una dirección IP en Internet. Además, se puede ver cuándo expirará el dominio, cuál es el estado de la transferencia, a quién contactar en caso de abuso y qué servidores de nombres se están utilizando [4].
  - **Traceroute**: Esta herramienta sirve para mostrar posibles rutas y medir los retrasos de tránsito de los paquetes, lo que hace es trazar la ruta que hace un paquete entrante que viene desde un host o punto de red hasta el ordenador que lo solicito [5].
  - **Findomain**: Es una herramienta que sirve para enumerar los subdominios asociados con nuestros objetivos. Como se señala en la descripción de la práctica, aunque es potente, no siempre enumera todos los subdominios disponibles, así que se usa **subfinder** y **sublist3r** para complementarlos.
  - **Dnsrecon**: Esta herramienta sirve dar un escaneo y enumeración DNS, la cual permite realizar diferentes tareas, como enumeración de registros estándar para un dominio definido (A, NS, SOA y MX). Se usa **dnsmap** para complementar.
  - **Nmap**: Utilizaremos esta herramienta para sacar la mayor cantidad de información posible y datos sobre estas instituciones. Como para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características [6].
  - **EtherApe**: Esta herramienta nos permitirá monitorear nuestra propia red durante el proceso de recopilación de información. Su objetivo es observar todo el tráfico que se genera al momento de hacer estas peticiones.

- **Adquisición.**

  En primer lugar, para ejecutar el script se debe proporcionar un dominio o una dirección IP como argumento: `./pruebap.sh <dominio/IP>`; también si es la primera vez que se ejecuta el script desde que se prendió la VM, se debe introducir la contraseña del usuario para poder darle permisos especiales a Etherape. Una vez que se le haya proporcionado dicha información, el script se encargará de verificar que el argumento sea correcto y validar que si quiera exista el dominio haciendo uso de `host`, en caso de no serlo, termina la ejecución. Después de estos pasos, se irá creando el archivo de texto donde se escribirá la información que necesitamos.

  En segundo plano se ejecutará Etherape para poder visualizar el tráfico de red del argumento. Después se hará uso de `whois` para obtener la información del dominio (aunque varía según el argumento), además de que se filtran la mayoría de comentarios irrelevantes. Con `ping` se medirá la latencia disponibilidad y se extraerá el porcentaje de pérdida de paquetes, limitamos la ejecución a 10 pings para que el proceso no sea largo.

  `nslookup` hace uso de `-query=A` para obtener las direcciones `IPv4` y hace uso de `-query=AAAA` para obtener las direcciones `IPv6`. `traceroute` solo muestra los primeros 10 saltos hacia el dominio, aunque si somos honestos, no muestra nada más que `****` pero probablemente se debe a que hay de por medio algún firewall o un problema en el router. Se usa `findomain`, se complementa con `subfinder` para detectar los subdominios relacionados al argumento y con `sublist3r` para ver las certificaciones SSL; aunque este último llega a tener problemas al momento de ejecutarse, por lo que mostrará resultados después de varios intentos. Hacemos uso de `dnsmap` para obtener las direcciones IP de los subdominios. Los registros DNS los obtenemos con `dnsrecon` y filtramos la información de los registros estándar. También se buscan los registros PTR para cada IP asociada al argumento, en este caso se usa `host` para hacer una consulta inversa ya que hacemos uso de la IP y queremos verificar el dominio asociado. Finalmente se ejecuta `nmap` para escanear y detectar los servicios abiertos del argumento, sin ping previo y analizar los primeros 1000 puertos.

  Vale la pena mencionar que en la mayoría de los subdominios todas las pruebas son satisfactorias, pero en algunos casos como en `pemex.com` con `whois`, la información obtenida es más completa que la que se obtenía en `gob.mx`.

1. **unam.mx**

   - **Procedimientos**

```
Analisis de: unam.mx
----------------------------------------
[WHOIS Information]

Domain Name:       unam.mx

Created On:        1989-03-31
Expiration Date:   2025-03-30
Last Updated On:   2024-03-27
Registrar:         AKKY ONLINE SOLUTIONS, S.A. DE C.V.
URL:               http://www.akky.mx
Whois TCP URI:     whois.akky.mx
Whois Web URL:     http://www.akky.mx/herramientas/whois.jsf

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

Name Servers:
   DNS:            ns3.unam.mx       132.248.108.215,
                                     2001:1218:100:10a:108:0:0:215
   DNS:            ns4.unam.mx       132.248.204.32,
                                     2001:1218:403:203:204:0:0:32
----------------------------------------
[Prueba de conectividad (Ping)]
PING unam.mx (132.248.166.19) 56(84) bytes of data.
64 bytes from 132.248.166.19: icmp_seq=1 ttl=255 time=55.3 ms
64 bytes from 132.248.166.19: icmp_seq=2 ttl=255 time=43.4 ms
64 bytes from 132.248.166.19: icmp_seq=3 ttl=255 time=27.0 ms
64 bytes from 132.248.166.19: icmp_seq=4 ttl=255 time=28.4 ms
64 bytes from 132.248.166.19: icmp_seq=5 ttl=255 time=30.8 ms
64 bytes from 132.248.166.19: icmp_seq=6 ttl=255 time=14.3 ms
64 bytes from 132.248.166.19: icmp_seq=7 ttl=255 time=22.5 ms
64 bytes from 132.248.166.19: icmp_seq=8 ttl=255 time=19.7 ms
64 bytes from 132.248.166.19: icmp_seq=9 ttl=255 time=24.6 ms
64 bytes from 132.248.166.19: icmp_seq=10 ttl=255 time=11.5 ms

--- unam.mx ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9076ms
rtt min/avg/max/mdev = 11.472/27.739/55.273/12.489 ms
----------------------------------------
[Registros DNS (IPv4 e IPv6 - Nslookup)]
Address:        10.0.2.3#53
Name:   unam.mx
Address: 132.248.166.20
Name:   unam.mx
Address: 132.248.166.17
Name:   unam.mx
Address: 132.248.166.19
Name:   unam.mx
Address: 132.248.166.18
Address:        10.0.2.3#53
Name:   unam.mx
```

```
Address: 2001:1218:3000:180::17
Name:    unam.mx
Address: 2001:1218:3000:180::18
Name:    unam.mx
Address: 2001:1218:3000:180::19
Name:    unam.mx
Address: 2001:1218:3000:180::20
----------------------------------------
[TRACEROUTE (primeros 10 saltos)]
traceroute to unam.mx (132.248.166.18), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.516 ms  0.582 ms  0.552 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
...
----------------------------------------
[Subdominios detectados]
www.distancia.acatlan.unam.mx
registro-coas.acatlan.unam.mx
webnom.dgp.unam.mx
morfologia.enp.unam.mx
coco.astroscu.unam.mx
hiena.astroscu.unam.mx
labvs.matem.unam.mx
cerberos.acatlan.unam.mx
av.arq.unam.mx
ve9.astros-dist.unam.mx
ecu.odonto.unam.mx
ve70.arq-dist.unam.mx
geografia.posgrado.unam.mx
...
----------------------------------------
[DNSMAP - Subdominios Detectados]
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for unam.mx using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests
```

```
blog.unam.mx
IP address #1: 132.247.174.18

bq.unam.mx
IP address #1: 132.248.55.100

dc.unam.mx
IP address #1: 132.247.70.123

ed.unam.mx
IP address #1: 132.248.48.16

email.unam.mx
IP address #1: 132.248.194.217

eventos.unam.mx
IP address #1: 132.247.22.53

fa.unam.mx
IP address #1: 132.248.43.17

...

[+] 25 (sub)domains and 27 IP address(es) found
[+] completion time: 116 second(s)
----------------------------------------
[Escaneo DNS con dnsrecon]
[*]      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 ns5.unam.mx 132.248.243.37
[*]      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 ns1.unam.mx 132.248.108.221
[*]      MX unam-mx.mail.protection.outlook.com 52.101.194.19
[*]      MX unam-mx.mail.protection.outlook.com 52.101.9.17
```

```
[*]       MX unam-mx.mail.protection.outlook.com 52.101.10.2
[*]       MX unam-mx.mail.protection.outlook.com 52.101.194.0
...
-------------------------------------------
[Resoluci n inversa (PTR)]
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:
...
-------------------------------------------
[Escaneo de Puertos con Nmap]
Ejecutando escaneo Nmap (versi n limitada para evitar bloqueos)...
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  REASON         VERSION
80/tcp  open  http     syn-ack ttl 64 Apache httpd 2.4.51 ((Unix))
443/tcp open  ssl/http syn-ack ttl 64 nginx 1.27.2
```

Figura 1: Etherape durante la ejecución de *whois*

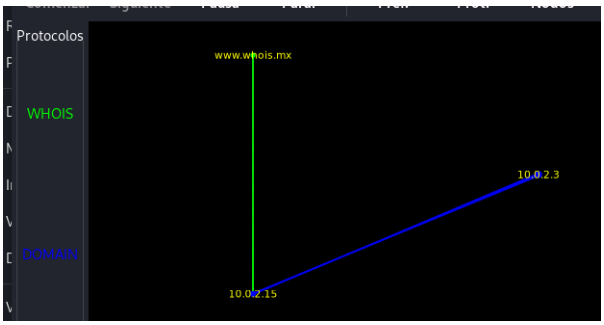


Figura 2: Etherape durante la ejecución de *ping* (1)

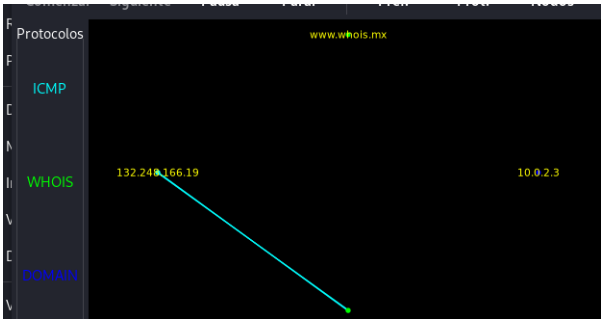


Figura 3: Etherape durante la ejecución de *ping* (2)

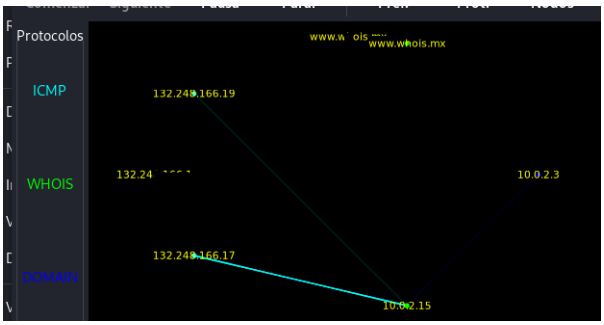


Figura 4: Etherape durante la ejecución de *traceroute* (1)

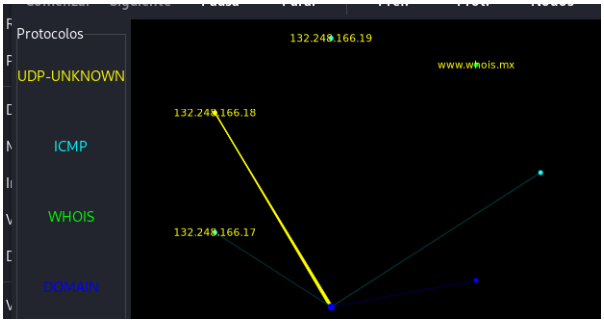


Figura 5: Etherape durante la ejecución de *traceroute* (2)

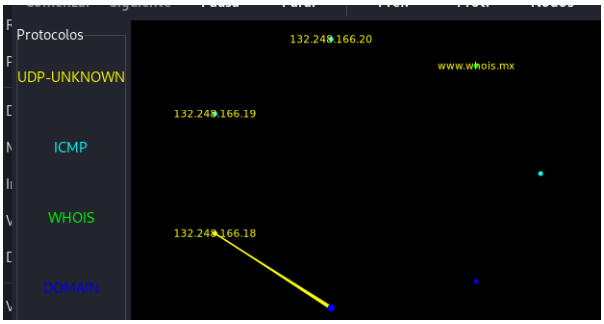


Figura 6: Etherape durante la ejecución de *findomain* (1)

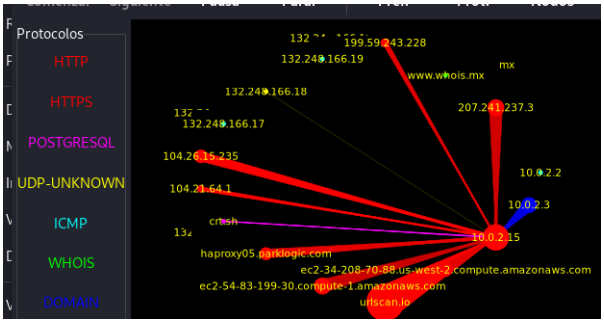


Figura 7: Etherape durante la ejecución de *subfinder* (2)

Figura 8: Etherape durante la ejecución de *sublist3r* (3)

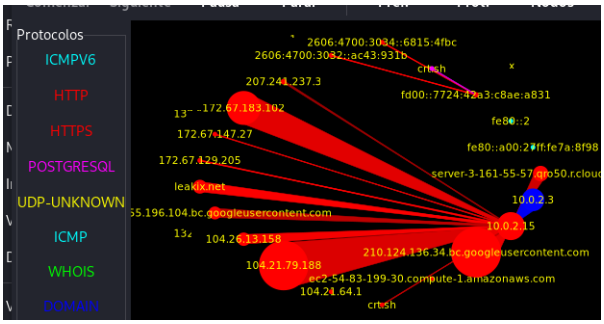


Figura 9: Etherape mostrando resultados de subdominios (4)

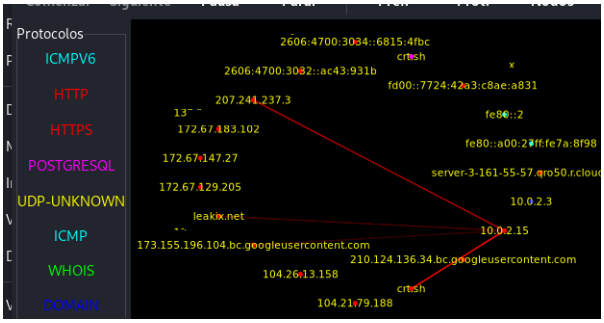


Figura 10: Etherape durante la ejecución de *dnsmap* (1)

Figura 11: Etherape durante la ejecución de *dnsmap* (2)

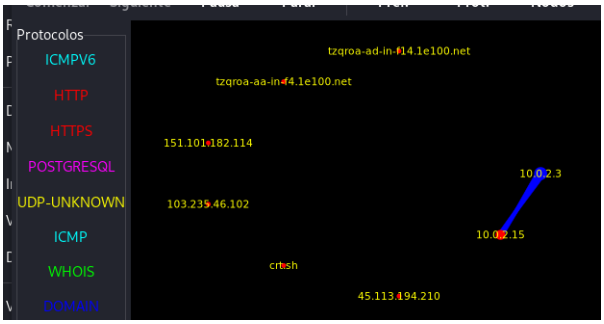


Figura 12: Etherape durante la ejecución de *dnsrecon* (3)

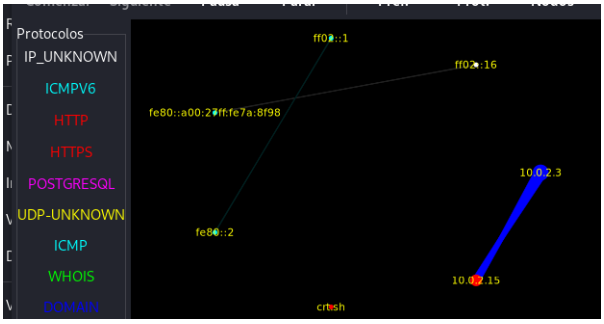


Figura 13: Etherape finalizando análisis DNS (4)

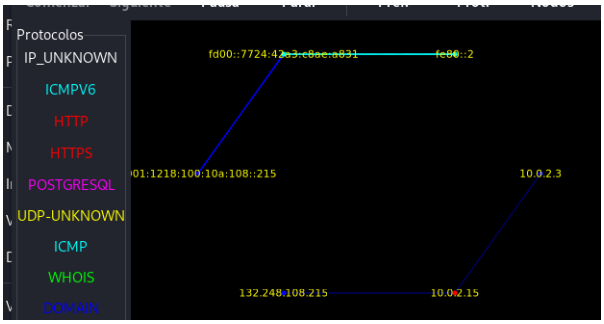


Figura 14: Etherape durante la ejecución de *nmap* (1)

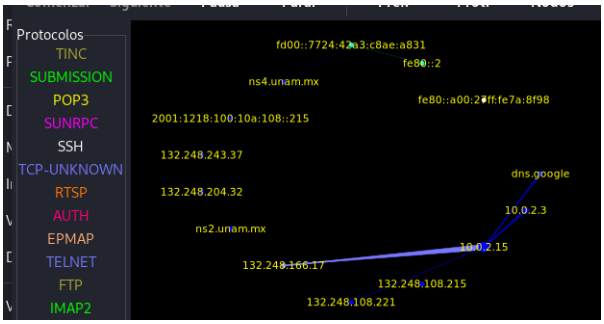
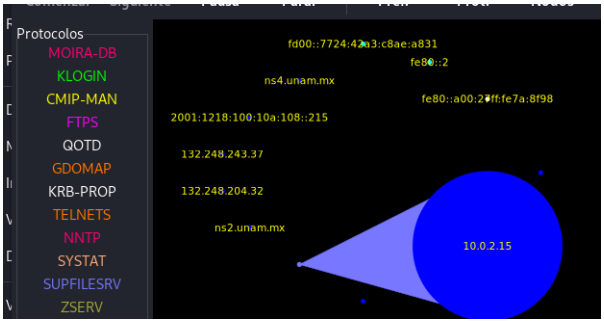


Figura 15: Etherape finalizando escaneo de puertos con *nmap* (2)



- **Análisis**

  Whois muestra que el dominio está próximo a expirar (30 de marzo, 2025), lo que representa un riesgo si no existe un proceso automatizado de renovación.

  Los registros de DNSSEC DS no fueron detectadas (no imprimió nada), lo que sugiere que podría no estar implementada o que whois ya no funciona para detectarlas.

Los resultados del traceroute muestran que después del primer salto, todos los demás aparecen como "*", lo que significa que el dispositivo no ha podido responder a las solicitudes antes de que se supere el tiempo especificado, aunque también pueden indicar que hay pérdida de paquetes. El hecho de que aparesca en todo los saltos el "*"puede significar varias cosas: El firewall o los dispositivos de seguridad del ordenador de destino bloquean la solicitud de traceroute, o/y hay problema con la ruta de retorno desde el equipo de destino o/y hay un posible problema de conexión en la dirección de destino [7].

NOTA: Lo mismo ocurre con todos los demás dominios analizados `pemex.com`, `ipn.mx` y `gob.mx`.

Entre los subdomios, no se encontró ninguno que destacara por su falta de seguridad, había algunos que simplemente no terminaban de cargar u otros que solo mostraban una linea imprimida (`https://extranet.dgire.unam.mx/`) u otros que simplemente no se podía acceder porque el navegador no lo permitía por su completa falta de protección (tal vez por configuraciones SSL/TLS inadecuadas).

dnsmap reveló 25 subdominios y 27 direcciones IP asociadas al dominio principal, lo que proporciona un mapa de la infraestructura de la universidad. Entre los subdominios se encuentran los del Instituto de Biología de la UNAM (`https://ib.unam.mx/`), la pagina a la Educación a Distancia (`https://ib.unam.mx/`), el más interesante, el del correo de la unam (`email.unam.mx`) que no logramos que cargara algo pero consideramos puede dar información de los sitios de la UNAM, en particular su infraestructura, lo cual con la suficiente paciencia y tiempo nos podría revelar algo.

Por último, según los resultados de nmap, se detectaron dos puertos en estado .ªbierto": el puerto 80/tcp ejecutando Apache httpd 2.4.51 en Unix y el puerto 443/tcp ejecutando nginx 1.27.2. Los otros 998 puertos escaneados aparecen como "filtrado", lo que significa que Nmap no puede determinar si estos puertos están abiertos porque hay algo impidiendo que las sondas alcancen el puerto. El filtrado puede provenir de un dispositivo de cortafuegos dedicado, de las reglas de un enrutador, o por una aplicación de cortafuegos instalada en el propio equipo. Como los puertos en estado "filtrado"proporcionan muy poca información y ralentizan drásticamente los escaneos debido a que Nmap debe reintentar varias veces cuando no recibe respuesta se sabe que esto tiende a frustrar a los atacantes [8].

- **Presentación**

  De acuerdo con esta pagina sobre dominios caducados [9], cuando un dominio expira, pasa por un periodo de gracia donde solo el propietario original puede renovarlo, seguido potencialmente por una subasta. Si la UNAM no renovara a tiempo este dominio, podría quedar disponible para ciberatacantes, quienes podrían aprovecharse del tráfico del dominio para phishing (ataque que intenta robar dinero o identidad) o distribución de malware dirigido a estudiantes y personal universitario.

  Investigando, encontramos que DNSSEC son las iniciales de Domain Name System Security Extensions, y es una forma de verificar la integridad de los datos de DNS y su origen. La ausencia de ellos podría (como ya lo habiamos mencioando) significar que whois no es capaz de obtenerlos, pero también puede significar que la pagina es vulnerable a .[en]venenamiento de DNS", este tipo de ataque ocurre cuando un atacante introduce información falsa en una caché DNS, haciendo que las consultas devuelvan respuestas incorrectas y dirijan a los usuarios a sitios web maliciosos. Como los solucionadores DNS normalmente no pueden verificar los datos en sus cachés, esta información incorrecta permanecerá hasta que expire el tiempo de vida (TTL) o se elimine manualmente [10].

2. **pemex.com**

- **Procedimientos**

```
Analisis de: pemex.com
----------------------------------------
[WHOIS Information]
   Domain Name: PEMEX.COM
   Registry Domain ID: 231477_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.akky.mx
   Registrar URL: http://www.akky.mx
   Updated Date: 2025-01-07T16:57:36Z
   Creation Date: 1995-06-22T04:00:00Z
   Registry Expiry Date: 2026-06-21T04:00:00Z
   Registrar: Akky Online Solutions, S.A. de C.V.
   Registrar IANA ID: 1705
   Registrar Abuse Contact Email: abuso@akky.mx
   Registrar Abuse Contact Phone: +52 (01) 81 8864-2625
   Domain Status: clientTransferProhibited
                  https://icann.org/epp#clientTransferProhibited
   Name Server: A1-68.AKAM.NET
   Name Server: A12-66.AKAM.NET
   Name Server: A18-66.AKAM.NET
   Name Server: A20-67.AKAM.NET
   Name Server: A5-66.AKAM.NET
   DNSSEC: signedDelegation
   DNSSEC DS Data: 39446 13 2
                   EABEADF50908BDB290C08C7230EEB988224FCD1C
                   6205B0374172228BD0B74E23

Registrant Email: https://www.akky.mx/WhoisContact
Registry Admin ID: Redacted for Privacy (Redactado por Privacidad)
Admin Email: https://www.akky.mx/WhoisContact
Registry Tech ID: Redacted for Privacy (Redactado por Privacidad)
Tech Email: https://www.akky.mx/WhoisContact
----------------------------------------
[Prueba de conectividad (Ping)]
PING pemex.com (200.23.91.20) 56(84) bytes of data.
```

```
--- pemex.com ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9213ms

P rdida de paquetes: 100%
----------------------------------------
[Registros DNS (IPv4 e IPv6 - Nslookup)]
Address:        10.0.2.3#53
Name:   pemex.com
Address: 200.23.91.20
Address:        10.0.2.3#53
----------------------------------------
[TRACEROUTE (primeros 10 saltos)]
traceroute to pemex.com (200.23.91.20), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.262 ms  0.299 ms  0.373 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
...
----------------------------------------
[Subdominios detectados]
ptq.pemex.com
ddiligencias.pemex.com
dataroom-aiatg.pemex.com
pep.pemex.com
sasipa.ref.pemex.com
limscpgs-d.pemex.com
tramites.franquicia.pemex.com
dipc.pemex.com
vpnautmex.pemex.com
pce.pemex.com
www.siiamobile.pemex.com
www.cp-mex1.pemex.com
blog.pemex.com
amcgdl.pemex.com
vwtutappp008.un.pemex.com
...
----------------------------------------
```

```
[DNSMAP - Subdominios Detectados]
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for pemex.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

blog.pemex.com
IP address #1: 200.23.91.78

blogs.pemex.com
IP address #1: 200.23.91.26

ca.pemex.com
IP address #1: 200.23.91.62

email.pemex.com
IPv6 address #1: 2801:c4:98::c817:5b05

email.pemex.com
IP address #1: 200.23.91.5

eventos.pemex.com
IP address #1: 200.23.91.34

ir.pemex.com
IP address #1: 200.23.91.94

owa.pemex.com
IPv6 address #1: 2603:1036:311:823::2
IPv6 address #2: 2603:1036:311:c03::2
IPv6 address #3: 2603:1036:311:822::2
IPv6 address #4: 2603:1036:311:1002::2

owa.pemex.com
IP address #1: 40.99.247.18
IP address #2: 40.99.249.66
IP address #3: 40.99.247.34
IP address #4: 52.96.47.82
```

```
...
----------------------------------------
[Escaneo DNS con dnsrecon]
[*]      SOA a1-68.akam.net 193.108.91.68
[*]      SOA a1-68.akam.net 2600:1401:2::44
[*]      NS a20-67.akam.net 95.100.175.67
[*]      NS a20-67.akam.net 2a02:26f0:67::43
[*]      NS a1-68.akam.net 193.108.91.68
[*]      NS a1-68.akam.net 2600:1401:2::44
[*]      NS a7-64.akam.net 23.61.199.64
[*]      NS a7-64.akam.net 2600:1406:32::40
[*]      NS a18-66.akam.net 95.101.36.66
[*]      NS a18-66.akam.net 2600:1480:4800::42
[*]      NS a5-66.akam.net 95.100.168.66
[*]      NS a5-66.akam.net 2600:1480:b000::42
[*]      NS a12-66.akam.net 184.26.160.66
[*]      NS a12-66.akam.net 2600:1480:f000::42
[*]      MX pemex-com.mail.protection.outlook.com 52.101.9.14
[*]      MX pemex-com.mail.protection.outlook.com 52.101.42.16
[*]      MX pemex-com.mail.protection.outlook.com 52.101.8.51
[*]      MX pemex-com.mail.protection.outlook.com 52.101.42.4
[*]      A pemex.com 200.23.91.20
...
----------------------------------------
[Resoluci n inversa (PTR)]
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:
...
----------------------------------------
[Escaneo de Puertos con Nmap]
Ejecutando escaneo Nmap (versi n limitada para evitar bloqueos)...
Not shown: 1000 filtered tcp ports (no-response)
```

Figura 16: Etherape durante la ejecución de *whois*

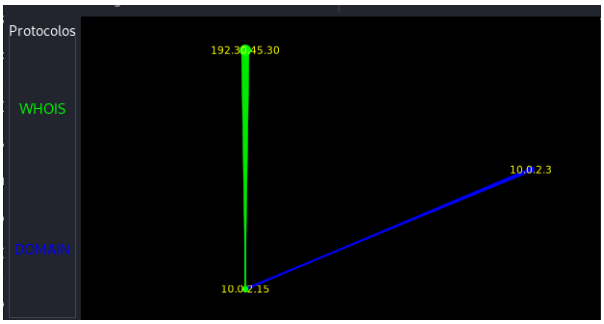


Figura 17: Etherape durante la ejecución de *ping*

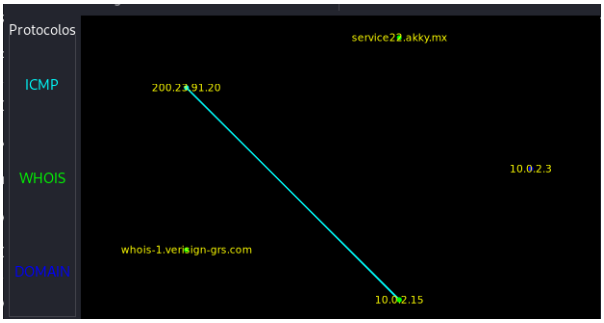


Figura 18: Etherape durante la ejecución de *traceroute* (1)

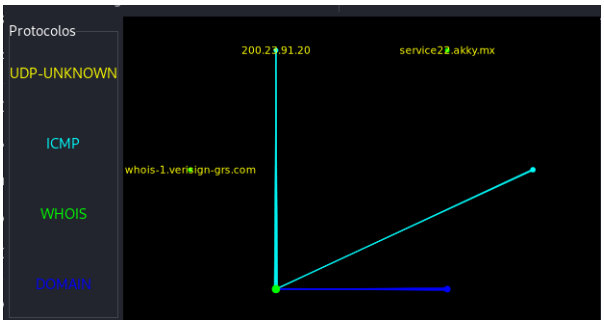


Figura 19: Etherape durante la ejecución de *traceroute* (2)

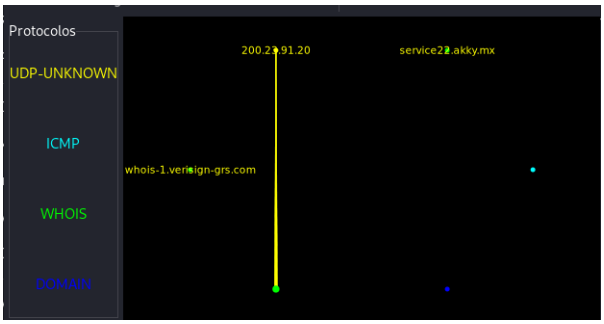


Figura 20: Etherape durante la ejecución de *findomain* (1)

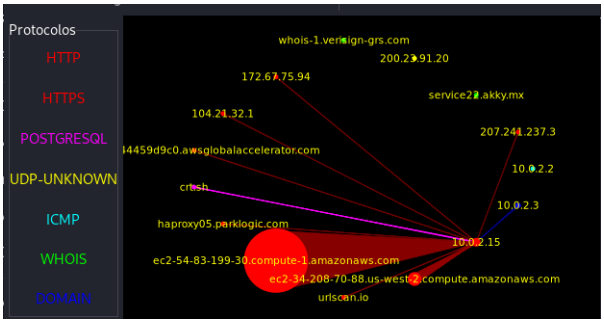


Figura 21: Etherape durante la ejecución de *subfinder* (2)

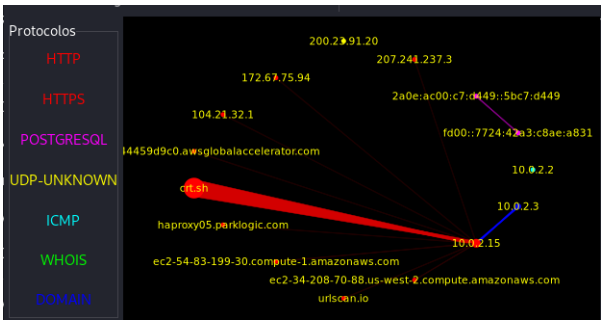


Figura 22: Etherape durante la ejecución de *dnsmap* (1)

Figura 23: Etherape durante la ejecución de *dnsmap* (2)

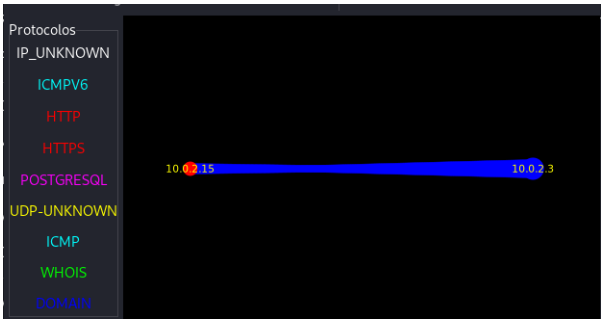


Figura 24: Etherape durante la ejecución de *dnsrecon* (3)

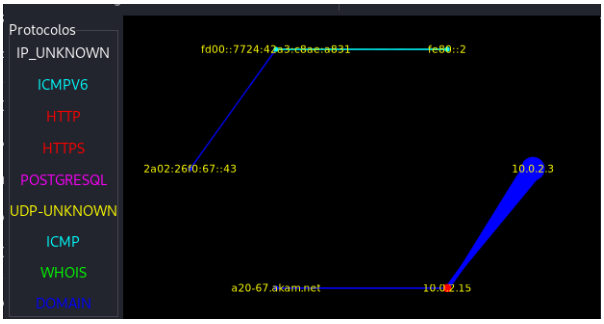


Figura 25: Etherape durante la ejecución de *nmap* (1)

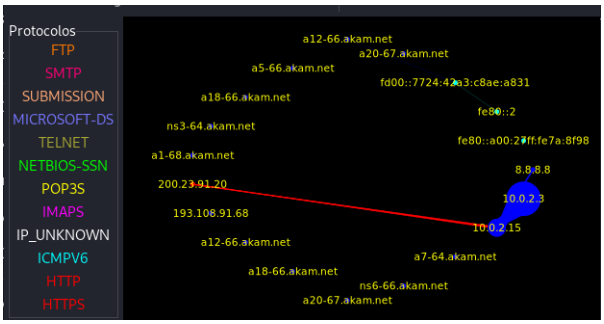


Figura 26: Etherape durante la ejecución de *nmap* (2)

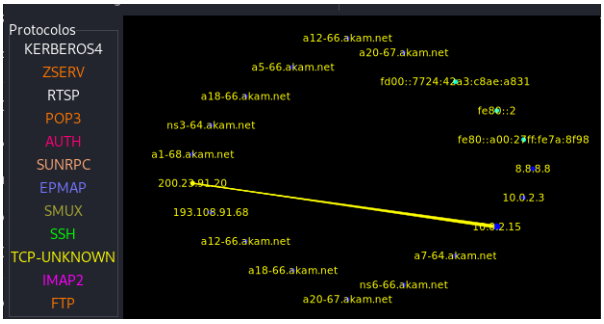


Figura 27: Etherape finalizando escaneo de puertos con *nmap* (3)

- **Análisis**

  Los registros whois indican que el dominio pemex.com tiene implementado DNSSEC ("DNSSEC: signedDelegation"), mostrando incluso datos DS específicos, lo que representa una capa de seguridad adicional que no se encontró en unam.mx. Además, como se menciona en la Presentación de unam.mx, esto lo haría menos vulnerable a ataques de envenenamiento de DNS.

Los resultados del traceroute muestran el mismo comportamiento que se observó con unam.mx, con todos los saltos después del primero apareciendo como "*", lo que refuerza la teoría de que existe un firewall o dispositivo de seguridad bloqueando estas solicitudes [7].

Una diferencia con unam.mx es el resultado del ping, que muestra un 100 % de pérdida de paquetes. Esto significa que si algún punto de la ruta no es compatible con ICMP, habrá una pérdida del 100 %, ya sea por diseño o por pérdida real [11]. También puede ser que el propio servidor bloquea los pings (firewall) o algo en la ruta (su firewall, firewall del proveedor o grupos de seguridad de proveedores de nube similares) bloquea las solicitudes de respuesta de eco ping/ICMP [12].

El análisis de puertos con nmap mostró todos los 1000 puertos escaneados en estado "filtrado", a diferencia de unam.mx donde los puertos 80 y 443 estaban abiertos. Esta configuración extremadamente restrictiva proporciona una superficie de ataque mínima y dificulta enormemente cualquier intento de reconocimiento de los servicios que pudieran estar ejecutándose en el servidor.

- **Presentación**

  El análisis de nmap no reveló puertos accesibles, mostrando todos los 1000 puertos escaneados como "filtrados". Esta configuración indica la presencia de firewalls o sistemas similares que están bloqueando activamente cualquier intento de reconocimiento (a diferencia de `unam.mx`), lo cual significa que esta bastante protegido el dominio. En general tiene mucha información protegida, como en whois que regresa muchos datos con Redacted for Privacy (Redactado por Privacidad)". Lo cual limita los ataques por ingeniería social.

  Si tuviéramos que atacar, nos concentraríamos en los subdominios, con la esperanza de encontrar alguno con configuraciones de seguridad menos rigurosas que el dominio principal (por ejemplo: `https://miicut.pemex.com/`).

3. **gob.mx**

- **Procedimientos**

```
Analisis de: gob.mx
----------------------------------------
[WHOIS Information]

Domain Name:       gob.mx

Created On:        1991-02-28
Expiration Date:   2025-02-27
Last Updated On:   2024-04-14
Registrar:         Registry .MX
URL:               http://www.registry.mx

Registrant:
   Name:           Network Information Center, S.A. de C.V.
   City:           Monterrey
   State:          Nuevo Leon
   Country:        Mexico

Administrative Contact:
   Name:           Network Information Center, S.A. de C.V.
   City:           Monterrey
   State:          Nuevo Leon
   Country:        Mexico

Technical Contact:
   Name:           Network Information Center, S.A. de C.V.
   City:           Monterrey
   State:          Nuevo Leon
   Country:        Mexico

Billing Contact:
   Name:           Network Information Center, S.A. de C.V.
   City:           Monterrey
   State:          Nuevo Leon
   Country:        Mexico
```

```
Name Servers:
   DNS:            m.mx-ns.mx       200.94.176.1
   DNS:            e.mx-ns.mx       189.201.244.1
   DNS:            x.mx-ns.mx       201.131.252.1
   DNS:            i.mx-ns.mx       207.248.68.1
   DNS:            c.mx-ns.mx       192.100.224.1,
                                    2001:1258:0:0:0:0:0:1
   DNS:            o.mx-ns.mx       200.23.1.1
...
-----------------------------------------
[Subdominios detectados]
backend-sigpada.agn.gob.mx
webdisk.acuna.gob.mx
comunidadescolar.aefcm.gob.mx
www.investigacionmercadosalud.adyt.gob.mx
cpcalendars.aguaprieta.gob.mx
mail.acancehyucatan2427.gob.mx
www.crm.acatic.gob.mx
api.acatlandeperezfigueroa.gob.mx
ns1.aguilillamichoacan.gob.mx
agenda-ciudadana.gob.mx
rocky.agua.gob.mx
declaragspdn.aguascalientes.gob.mx
webmail.acatlandejuarez.gob.mx
matrix.cienciadatos.adyt.gob.mx
...
-----------------------------------------
[DNSMAP - Subdominios Detectados]

archivos.gob.mx
IPv6 address #1: 2606:4700:3030::ac43:b384
IPv6 address #2: 2606:4700:3036::6815:3373

archivos.gob.mx
IP address #1: 104.21.51.115
IP address #2: 172.67.179.132
```

```
beta.gob.mx
IP address #1: 207.249.106.11

csg.gob.mx
IP address #1: 201.98.60.185

dh.gob.mx
IP address #1: 162.241.252.14

nl.gob.mx
IP address #1: 52.44.182.199
IP address #2: 52.1.53.61

pa.gob.mx
IP address #1: 187.174.198.80

prueba.gob.mx
IP address #1: 200.94.181.10
IP address #2: 200.94.181.11
IP address #3: 200.94.181.9

qr.gob.mx
IP address #1: 148.235.148.85

servicios.gob.mx
IP address #1: 189.247.197.90
IP address #2: 189.247.197.83
...
```

Figura 28: Etherape durante la ejecución de *whois*

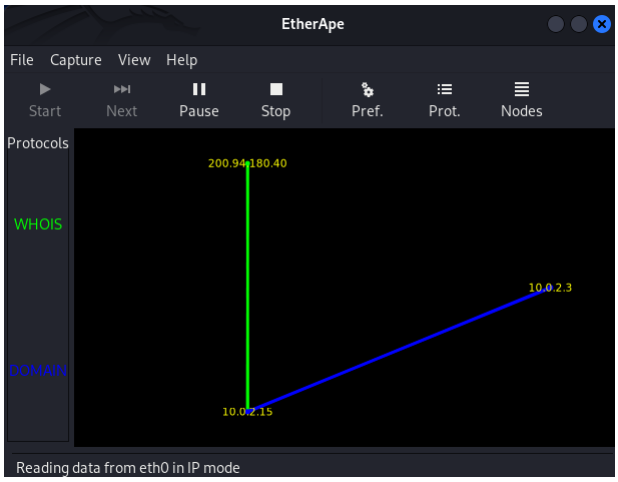


Figura 29: Etherape durante la ejecución de *findomain*

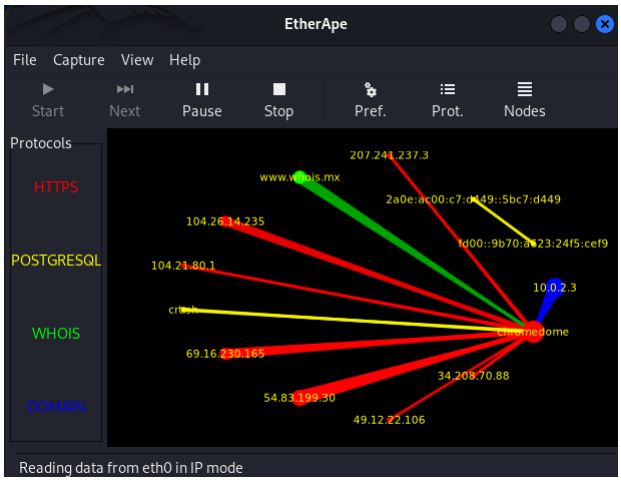


Figura 30: Etherape durante la ejecución de *subfinder*

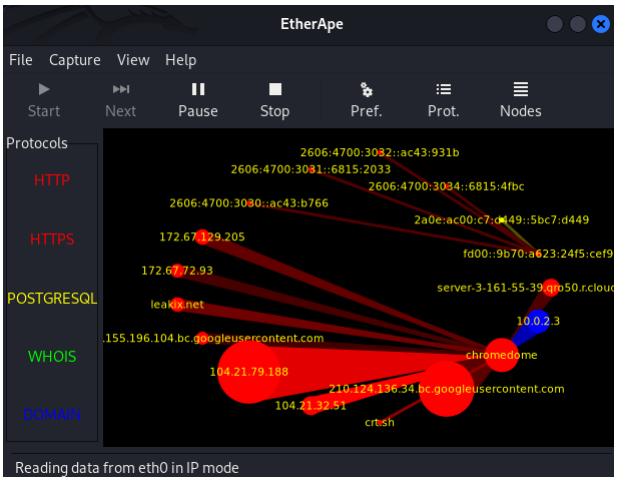
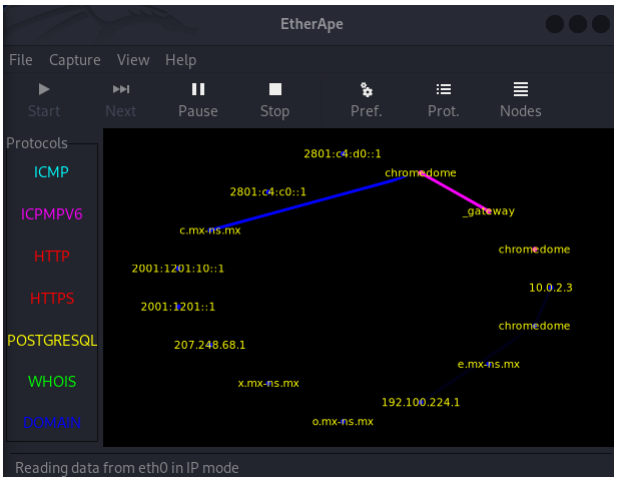


Figura 31: Etherape durante la ejecución de *dnsmap*



- **Análisis**

  `whois` muestra que el dominio expiró el 27 de Febrero de 2025, lo que significa que se corre riesgo de ser borrado o alguien más tome el control. Se puede detectar problemas con algunos subdominios relacionados a sistemas de pagos y validación de documentos, por ejemplo, `correo.aduanas.gob.mx` y `declaranet.ahome.gob.mx`. El uso de `whois` y `sublist3r` no detectó alguna implementación de DNSSEC, por lo que el dominio es vulnerable a que se intercepten datos.

- **Presentación**

  Cómo se mencionó en el apartado anterior, el servicio de `correo.aduanas.gob.mx`, puede ser objetivo de phishing, por lo que se puede enviar correos maliciosos para obtener la información de los contactos y/o usuarios. Mientras que el servicio `declaranet.ahome.gob.mx`,

puede exponer datos sensibles en base a las declaraciones patrimoniales, por lo que se pueden interceptar y aprovecharlas para conocer a más objetivos, aunque eso es un caso en general, ya que como no se cuenta con DNSSEC, se se pueden interceptar y redirigir todas las solicitudes de `gob.mx`[13]. Además, la cantidad de los subdominios también puede indicar que alguno ya esté en desuso, por lo que se podría tomar el control de algunos que ya no estén monitoreados y usarlos para otro fin. Sería aplicar **DNS Spoofing**.[14]

4. **ipn.mx**

- **Procedimientos**

```
Analisis de: ipn.mx
----------------------------------------
[WHOIS Information]

Domain Name:        ipn.mx

Created On:         1995-04-30
Expiration Date:    2025-04-29
Last Updated On:    2024-04-26
Registrar:          AKKY ONLINE SOLUTIONS, S.A. DE C.V.
URL:                http://www.akky.mx
Whois TCP URI:      whois.akky.mx
Whois Web URL:      http://www.akky.mx/herramientas/whois.jsf

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

Name Servers:
   DNS:            dns2.ipn.mx       148.204.198.2
   DNS:            dns3.ipn.mx       148.204.235.2
   DNS:            dns1.ipn.mx       148.204.103.2
...
----------------------------------------
[Subdominios detectados]
www.investigacion.ipn.mx
comunicaciondirecta.ipn.mx
www.becarvoe.ipn.mx
www.redcalidadaire.upiita.ipn.mx
www.sseeis.esimecu.ipn.mx
www.sepi.esiaz.ipn.mx
udidb.ciidiroaxaca.ipn.mx
cm-dcyc2.ipn.mx
cvdrmazatlan.ipn.mx
dzmanage.ipn.mx
megm.ciecas.ipn.mx
sse.ipn.mx
estructura.upiig.ipn.mx
core.ipn.mx
www.almacenamiento.dev.ipn.mx
becas.cofaa.ipn.mx
www.inventario.upev.ipn.mx
repamina.ipn.mx
datosabiertos.ipn.mx
builds.infra.dae.ipn.mx
azul.cicimar.ipn.mx
ciidirmich.ipn.mx
system.cics-sto.ipn.mx
tesla.cda.ipn.mx
cecyt12.ipn.mx
matedu.cicata.ipn.mx
www.monitoreo.cic.ipn.mx
www.aulasvirtuales.utecv.esiatic.ipn.mx
```

```
gaceta.cecuallende.ipn.mx
cinea2011.ipn.mx
www.virtual.cicimar.ipn.mx
...
----------------------------------------
[DNSMAP - Subdominios Detectados]

backup.ipn.mx
IP address #1: 148.204.189.219

controller.ipn.mx
IP address #1: 148.204.2.251
IP address #2: 10.204.15.5
[+] warning: internal IP address disclosed
IP address #3: 148.204.2.253
IP address #4: 148.204.150.188
IP address #5: 148.204.150.187
IP address #6: 148.204.150.189
IP address #7: 10.204.15.66
[+] warning: internal IP address disclosed
IP address #8: 10.200.3.252
[+] warning: internal IP address disclosed
IP address #9: 10.204.15.6
[+] warning: internal IP address disclosed
IP address #10: 10.204.15.65
[+] warning: internal IP address disclosed
IP address #11: 148.204.252.251
IP address #12: 148.204.252.250
IP address #13: 10.204.15.67
[+] warning: internal IP address disclosed
IP address #14: 10.204.15.4
[+] warning: internal IP address disclosed
IP address #15: 10.204.15.68
[+] warning: internal IP address disclosed

home.ipn.mx
IP address #1: 148.204.103.231
...
```

Figura 32: Etherape durante la ejecución de *whois*

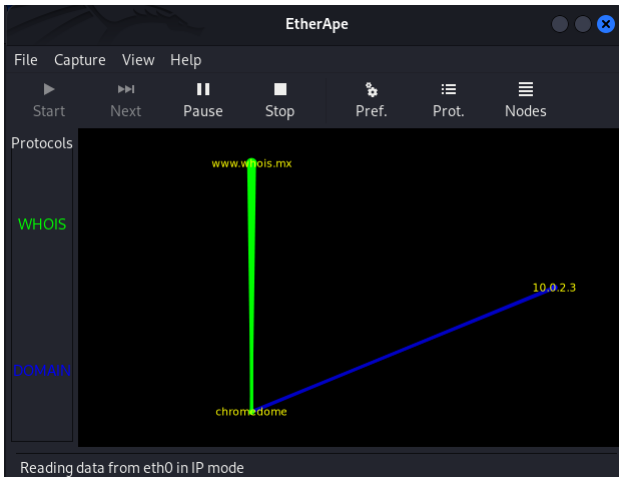


Figura 33: Etherape durante la ejecución de *ping*

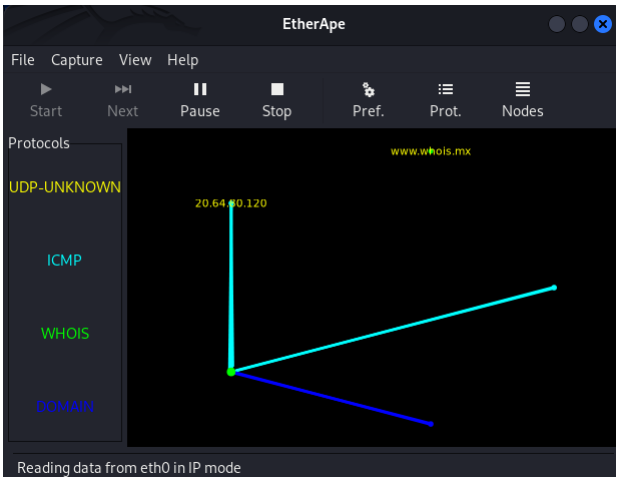


Figura 34: Etherape durante la ejecución de *findomain*

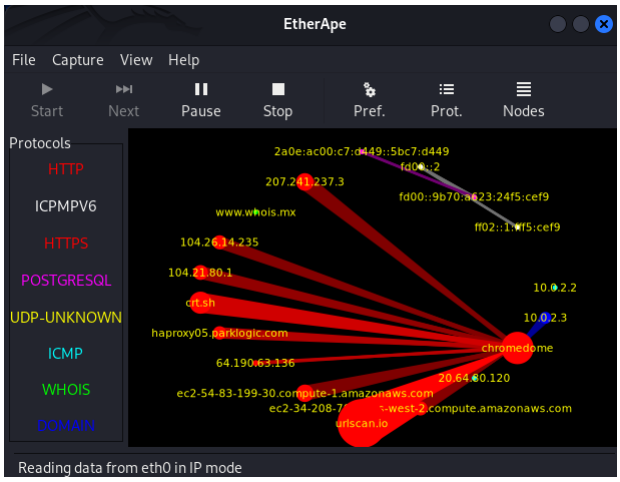


Figura 35: Etherape durante la ejecución de *subfinder*

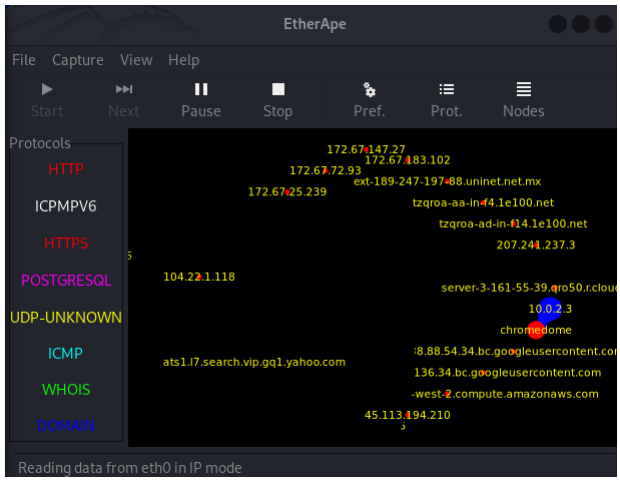


Figura 36: Etherape durante la ejecución de *nsmap*

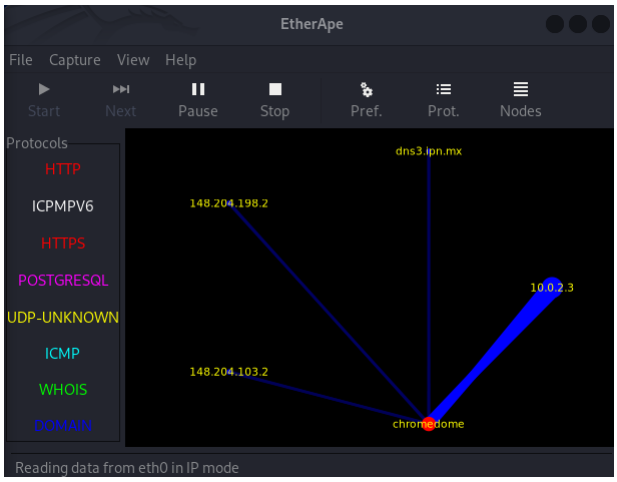
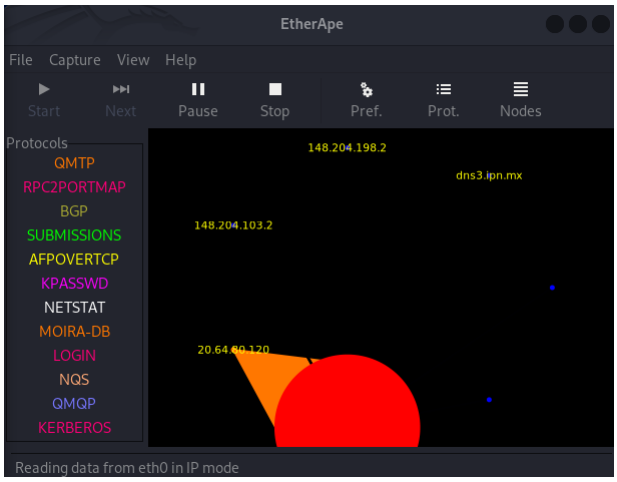


Figura 37: Etherape durante la ejecución de *nmap*



- **Análisis**

  `whois` muestra que el dominio está próximo a expirar el 29 de Abril de 2025, lo que representa un riesgo si no existe un proceso automatizado de renovación. Se puede detectar problemas con algunos subdominios relacionados a servicios administrativos, por ejemplo, `imap.correo.cofaa.ipn.mx` y `saes.cecyt9.ipn.mx`. El uso de `whois` y `sublist3r` tampoco detectó alguna implementación de DNSSEC, por lo que el dominio también es vulnerable a que se intercepten datos. Con `nmap` se pudo identificar que se tienen abiertos los puertos 80 y 443, que son puertos estándar para `HTTP` y `HTTPS` respectivamente. [15]

- **Presentación**

  El servicio de `imap.correo.cofaa.ipn.mx` es vulnerable a ataques de fuerza, por lo que una vez que se logre una infiltración, se pueden enviar correos electrónicos maliciosos para obtener información del alumnado y el profesorado. Por su lado, `saes.cecyt9.ipn.mx` puede tener fugas de información si las consultas no están bien protegidas. Como no se cuenta con DNSSEC, se pueden interceptar y redirigir todas las solicitudes de `ipn.mx` para darles otro uso. Que los puertos mencionados en la sección anterior estén abiertos nos da más razón para aprovechar la falta de DNSSEC y la intercepción de información.

Preguntas

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

   - **Protocolo de transferencia de hipertexto (HTTP)**
   - **Protocolo de transferencia de hipertexto seguro (HTTPS)**
   - **Protocolo de configuración dinámica de host (DHCP)**
   - **Protocolo de datagrama de usuario (UDP)**
   - **Protocolo de seguridad de la capa de transporte (TLS)**
   - **Protocolo de sistema de nombres de dominio (DNS)**[16]

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

   - El **Protocolo de transferencia de hipertexto (HTTP)** permite la transferencia de documentos de tipo *Hipertexto* haciendo uso del lenguaje de programación HTML y de sus enlaces internos para acceder a otros documentos.[16]
   - El **Protocolo de transferencia de hipertexto seguro (HTTPS)** a diferencia de **HTTP**, encripta los documentos, haciendo que sea un poco más segura su transferencia.[17]
   - El **Protocolo de configuración dinámica de host (DHCP)** permite que los dispositivos obtengan una configuración de red de forma automática. Cuenta con una fácil administración y la asignación evita colisiones pero la falta de seguridad cuando se trata de redes inalámbricas.[16]
   - El **Protocolo de datagrama de usuario (UDP)** es una alternativa más rápida al **DHCP** pero es menos fiable al momento de transportar información. Se suele utilizar en servicios de transmisión de vídeo y de videojuegos.[17]
   - El **Protocolo de seguridad de la capa de transporte (TLS)** ayuda a la encriptación de **HTTPS**.[17]
   - El **Protocolo de sistema de nombres de dominio (DNS)** transforma las direcciones **IP** en nombres más fáciles de usar, es decir, las traduce para la lectura humana.[16]

3. **¿Qué es un sniffer?** Es una herramienta tanto de software cómo de hardware (routers, por ejemplo) que permite a un usuario supervisar el tráfico en Internet en tiempo real y capturar todo el tráfico de datos que entra y salen de sus dispositivo. Pueden detectar, capturar e inspeccionar grandes consumos de ancho de banda en los datos que viajan a través de la red. También puede emplearse para realizar ataques de espionaje.[18]

4. **OSINT, ¿Qué es?, ¿Para qué sirve?** También conocida como *Inteligencia de Código Abierto*, es el proceso de recopilación y análisis de información de fuentes públicas, tales como redes sociales,

registros gubernamentales y directorios electrónicos, sirve para evaluar amenazas, tomar decisiones o responder preguntas específicas. Ayuda mucho a medir e identificar riesgos y vulnerabilidades en sistemas de tecnología informática. [19]

5. **Investiga los 5 OSINT más usados.**

   - **Maltego.** Se usa para la minería de datos en tiempo real, además de que proporciona representaciones gráficas de patrones y conexiones de datos. También perfila y rastrea las actividades en línea de las personas.
   - **Spiderfoot.** Se usa para la integración de fuentes de datos para obtener información cómo direcciones de correo electrónico, números telefónicos, direcciones IP, subdominios, etc.
   - **Shodan.** Se usa como un motor de búsqueda para dispositivos conectados a Internet que también puede proporcionar información sobre metados y puertos abiertos.
   - **Babel X.** Se usa como herramienta de búsqueda en la World Wide Web y la dark web.
   - **Metasploit.** Se usa para hacer pruebas de penetración para identificar vulnerabilidades se seguridad en redes, sistemas y aplicaciones. [19]

6. **Investiga 5 softwares no mencionados en la práctica que sirvan para el análisis de comunicaciones.**

   - **Wireshark.** Analiza el tráfico de red que permite capturar y examinar paquetes en tiempo real. [20]
   - **Tcpdump.** Captura y analiza tráfico de red desde la linea de comandos.[21]
   - **Masscan.** Otra alternativa a Wireshark y Masccan.[22]
   - **Zmap.** Es unscáner de red de alto rendimiento diseñado para escanear Internet en segundo.[23]
   - **MTR (My Traceroute).** Combina traceroute y ping para analizar la ruta y latencia de paquetes en la red.[24]

7. **¿Qué es la ingeniería social?** La ingeniería social es una técnica de manipulación que aprovecha el error humano para obtener información privada, acceso a sistemas u objetos de alto valor. Algunos lo denominan cómo ”piratería humana”. [25]

8. **¿Por qué el eslabón más débil de seguridad son las personas?** Porque son la primer puerta de acceso de los ciberdelincuentes además de que todos, si no la mayoría son susceptibles a la ingeniería social.

9. **¿Qué acciones haces para protegerte de ciberataques?** Cuando estoy fuera de casa, intento sólo usar mis datos móviles para no tener que acceder a redes públicas, sólo ingreso a paginas web con protocolos de trasferencia de hipertexto seguro ’https’, además de **jamás** ingresar información

privada a paginas que para usar sus servicios mínimos me la piden. Todavía no creo cuenta para la pagina web del banco al que estoy asociada ni realizo compras en linea (en Mercado libre, amazon, etc.) ingresando los datos de mi tarjeta, prefiero usar efectivo (en oxxo).

10. **¿Crees que tus métodos preventivos son suficientes?** No del todo, porque incluso si no quiero usar redes públicas, en mi vida diaria no siempre puedo darme el lujo de solo usar datos móviles, aunque he estado buscando VPN's (aunque todavía no me decido). E incluso si entro a paginas "seguras", eso no las hace completamente confiables, todavía son vulnerables a ciberataques que ponen mi información en riesgo.

Referencias

[1] OpenWebinars. Fases del pentesting: pasos para asegurar tus sistemas. [Online]. Available: https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

[2] Hostinger. Cómo usar el comando ping en linux: Tutorial para principiantes. [Online]. Available: https://www.hostinger.com/es/tutoriales/comando-ping-linux

[3] IONOS. nslookup: herramienta de consulta para dns. [Online]. Available: https://www.ionos.mx/digitalguide/servidores/herramientas/nslookup/

[4] One.com. ¿qué es whois? [Online]. Available: https://help.one.com/hc/es/articles/115005595885--Qu%C3%A9-es-WHOIS

[5] Xataka. Tracert y traceroute: qué es, cómo funciona y cómo se utiliza. [Online]. Available: https://www.xataka.com/basics/tracert-traceroute-que-como-funciona-como-se-utiliza

[6] Nmap.org. Guía de referencia de nmap. [Online]. Available: https://nmap.org/man/es/index.html

[7] Hostinger. (2023) Comando traceroute: Qué es y cómo usarlo. [Online]. Available: https://www.hostinger.com/es/tutoriales/comando-traceroute

[8] G. Lyon. (2023) Fundamentos sobre el escaneo de puertos. [Online]. Available: https://nmap.org/man/es/man-port-scanning-basics.html

[9] Arsys. (2023) Guía completa sobre expired domains o dominios caducados. [Online]. Available: https://www.arsys.es/blog/guia-completa-sobre-expired-domains-o-dominios-caducados#tree-3

[10] Cloudflare. (2023) ¿qué es el envenenamiento de caché dns? [Online]. Available: https://www.cloudflare.com/es-es/learning/dns/dns-cache-poisoning/

[11] eRGX and JerryChang. (2022) 100 % ping loss from jetson nano. NVIDIA Developer Forums. [Online]. Available: https://forums.developer.nvidia.com/t/100-ping-loss-from-jetson-nano/243659/5

[12] D.M. and M. Hampton. (2023) Ping: 100 % packet loss, can't ping to server. ServerFault. [Online]. Available: https://serverfault.com/questions/1126899/ping-100-packet-loss-cant-ping-to-server

[13] T. Khan and M. Goodwin. What is dnssec (dns security extensions)? [Online]. Available: https://www.ibm.com/think/topics/dnssec

[14] Kaspersky. What is spoofing – definition and explanation. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/spoofing

[15] D. Gitlan. Puerto 80 (http) vs puerto 443 (https): Explicación de las principales diferencias. [Online]. Available: https://www.ssldragon.com/es/blog/port-80-vs-port-443/

[16] E. Limones. (2021) Protocolo de red: Qué es, tipos y características. [Online]. Available: https://openwebinars.net/blog/protocolo-de-red-que-es-tipos-y-caracteristicas/

[17] Cloudflare. What is a protocolo? [Online]. Available: https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-protocol/

[18] A. Academy, "¿qué es un sniffer?" [Online]. Available: https://www.avast.com/es-es/c-sniffer

[19] IBM. ¿qué es osint? [Online]. Available: https://www.ibm.com/mx-es/topics/osint

[20] K. Linux. Wireshark. [Online]. Available: https://www.kali.org/tools/wireshark/

[21] ——. Tcpdump. [Online]. Available: https://www.kali.org/tools/tcpdump/

[22] ——. Masscan. [Online]. Available: https://www.kali.org/tools/masscan/

[23] ZMap. The zmap project. [Online]. Available: https://zmap.io

[24] Cloudflare. ¿qué es mtr? [Online]. Available: https://www.cloudflare.com/es-es/learning/network-layer/what-is-mtr/

[25] IBM. ¿qué es la ingeniería social? [Online]. Available: https://www.ibm.com/mx-es/topics/social-engineering