

Experto Universitario en Ethical Hacking

Módulo 5:

Ethical Hacking

Unidad 1:

Reconocimiento Pasivo/Activo



Presentación

En esta primera Unidad del módulo, se conocerá la importancia de esta fase de reconocimiento, para la obtención de datos relevantes, de esa manera uno puede avanzar con las siguientes fases.

Aprenderán tanto las herramientas que se utilizan, así como que se obtiene a través de las mismas.



Objetivos

Que los participantes logren...

- Aprender sobre los conceptos expuestos en el mundo del Hacking.
- Conocer las herramientas y metodologías necesarias para realizar tareas de análisis de vulnerabilidades y test de penetración (Pentesting), con una filosofía enfocada en la ética profesional.
- Comprender la importancia de usar cifrado seguro en aplicaciones, abordar vulnerabilidades y potenciales ataques y amenazas, así como la correcta concientización en los usuarios.



Bloques temáticos

1. Fase de reconocimiento
2. Introducción al Footprinting
3. Information Gathering
4. Check Web Pages
5. Software Tools

Fase de Reconocimiento



Es necesario prestar atención a todos los componentes de la red, ya que los mismos serían las posibles puertas de entrada a la misma.

Así como uno puede mediante una técnica de reconocimiento, darse cuenta que para ingresar a un Router, basta un patchcord conectado en la red, también es parte del reconocimiento, chequear todos los posibles lugares, por donde pasa la información, así como también Gateways, Backups, Servidores, etc.



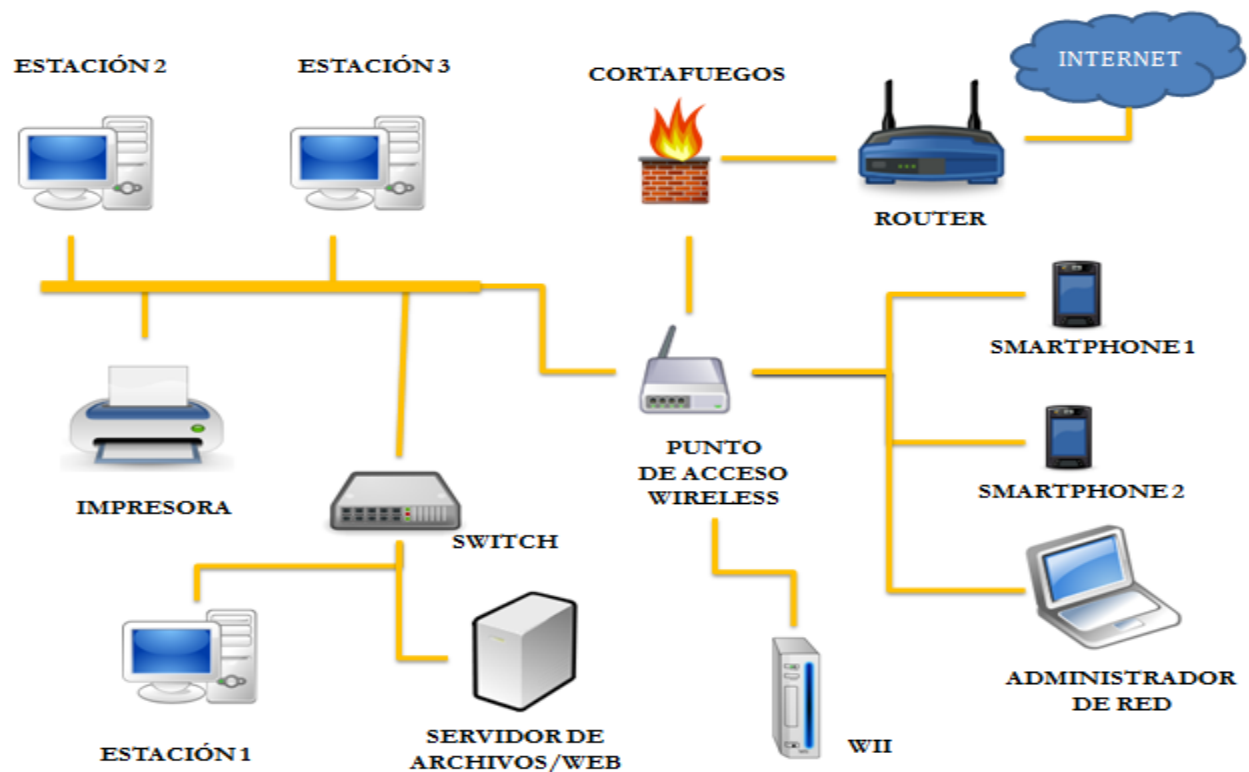
La fase de reconocimiento está compuesta por 3 etapas:

OBTENER – REUNIR – ORGANIZAR

Ejercicio 1 – Unidad 1



Si miramos con atención la gráfica a continuación, cuántos puntos posibles de ingreso/intrusión, creen que son posibles? Responder en el foro a través de un post.



En un análisis de reconocimiento de la red, no siempre es todos equipos o dispositivos, sino que pueden incluirse factores externos, como por ejemplo, una cámara IP, un sensor biométrico, un panel de acceso, hasta el router del ISP.

Introducción al Footprinting



Se refiere a la fase preparatoria donde un atacante trata de reunir la mayor cantidad de información posible sobre el objetivo de la evaluación antes de lanzar un ataque (la manera detectivesca de hacer la fase)



Tenemos 2 tipos de Footprinting:

- **PASIVO** (no detectable), por ejemplo, buscar información de una persona de forma indirecta
- **ACTIVO** (es detectable), analizar y escanear una IP

BuscarDatos.com Móvil Personas Empresas

Búsqueda de Personas

Busque a cualquier persona de Argentina a partir de un DNI, nombre y apellido, teléfono o dirección.

Búsqueda por nombre y apellido en el padrón

Búsqueda por nombre y apellido en las guías telefónicas

Búsqueda por DNI en el padrón

Búsqueda por dirección en las guías telefónicas y el padrón

NEW *** Búsqueda por dirección en las guías telefónicas *** NEW

Búsqueda por teléfono en las guías telefónicas



(Untitled) - Wireshark

Filter: (ip.addr eq 202.54.124.154 and ip.addr eq 10.10.2.28) Express

No.	Time	Source	Destination
14	5.594548	10.10.2.28	202.54.124.154

Frame 14 (886 bytes on wire, 886 bytes captured)

Ethernet II, Src: Realtek_8c:64:f4 (00:e0:4c:c5:64:f4), Dst: 202.54.124.154

Internet Protocol, Src: 10.10.2.28 (10.10.2.28), Dst: 202.54.124.154

Transmission Control Protocol, Src Port: 1544 (1544), Dst Port: 80 (80)

Hypertext Transfer Protocol

Line-based text data: application/x-www-form-urlencoded

login=shivaji&passwd=lewinsky&FormName=existing

No es ejercicio, pero piensen ¿cuál consideran que es activo o pasivo?

Visualmente se nota que el primer gráfico, es sobre un sitio para buscar datos de personas y el segundo gráfico es un analizar de tráfico (**Snifer**), que detecto un usuario y una password.

Debatir en el foro (por favor, crear un post solo y ahí contestan todos).

Information Gathering

¿QUE DATOS SE NECESITAN OBTENER PARA EMPEZAR?

Si alguno/a tiene experiencia, habrá escuchado de la famosa **biblia del reconocimiento**, donde nos indicaba cuales son los pasos más importantes de datos a obtener, hoy sigue vigente, los pasos son:

Bloques de red: a través de los mismos se pueden ver el direccionamiento Público que está siendo usado en el mismo objetivo.

Network Whois record

Queried whois.ripe.net with "-B 151.106.96.60"...

% Information related to '151.106.96.0 - 151.106.111.255'

% Abuse contact for '151.106.96.0 - 151.106.111.255' is 'abuse@hostinger.com'

inetnum: 151.106.96.0 - 151.106.111.255

EJEMPLO: análisis de una **IP** donde me expone todo el bloque de red involucrado en el Proveedor de Hosting.

Hay muchos sitios online, donde uno puede obtener esta información, lo cual siempre se recomienda de disponer de 3 o 4 sitios, para no encontrar información que sea un falso positivo.

Una manera muy interesante de encontrar estos datos, es también chequear en el sitio web del mismo proveedor o sitios que aportan datos, por ejemplo, **CENTRALOPS** es un sitio que expone mucha información de un objetivo.

DNS Records: nos entrega información relacionada a los dominios e información sobre el servicio MX (correo), importante para saber si el servidor de correo es local o a través de un proveedor externo.

DNS records

DNS query for **60.96.106.151.in-addr.arpa** returned an error from the server: **NameError**


DNS query for **2.0.0.0.5.c.9.3.c.8.1.0.0.0.4.3.5.0.1.0.0.0.8.7.4.2.0.a.2.ip6.arpa** returned an error from the server: **NameError**

name	class	type	data		time to live
pengowin.com.ar	IN	A	151.106.96.60		14400s (04:00:00)
pengowin.com.ar	IN	NS	ns1.hostinger-ar.com		86400s (1.00:00:00)
pengowin.com.ar	IN	NS	ns2.hostinger-ar.com		86400s (1.00:00:00)
pengowin.com.ar	IN	NS	ns3.hostinger-ar.com		86400s (1.00:00:00)
pengowin.com.ar	IN	NS	ns4.hostinger-ar.com		86400s (1.00:00:00)
pengowin.com.ar	IN	SOA	server:	ns1.hostinger-ar.com	86400s (1.00:00:00)
			email:	dns@hostinger.com	
			serial:	2019060300	
			refresh:	28800	
			retry:	7200	
			expire:	604800	
			minimum ttl:	86400	
pengowin.com.ar	IN	MX	preference:	10	14400s (04:00:00)
			exchange:	mx1.hostinger.com.ar	

Podremos notar que el servidor de correo es: **mx1.hostinger .com.ar**, lo cual para saber la **IP**, se puede realizar un **PING** a esa dirección.

CENTRALOPS, como podemos observar nos ofrece esta información.

Nombres Dominio: a veces puede ser que el objetivo tenga más dominios o subdominios, lo cual sería tedioso tener que probar uno por uno y hasta averiguar cuáles son, si el escenario es un BlackBox.

Subdomains -  fbi.gov

Domain

Domain Name ends with .fbi.gov X












+ Add Filter

SEARCH

145 Search results

Flags Status Code

- -

Domain	Site Title	Alexa rank	DNS A [®]
 houston.fbi.gov	 ERROR: The request could not be satisfied	7578	 143.204.47.86 - AS16509 - AMAZON-02  143.204.47.105 - AS16509 - AMAZON-02  143.204.47.41 - AS16509 - AMAZON-02  143.204.47.54 - AS16509 - AMAZON-02
 phoenix.fbi.gov	—	—	 13.227.255.25 - AS16509 - AMAZON-02  13.227.255.35 - AS16509 - AMAZON-02  13.227.255.56 - AS16509 - AMAZON-02  13.227.255.23 - AS16509 - AMAZON-02

En esta imagen, se puede observar que se buscó un sitio primario, y del mismo se desprendieron 145 resultados de varios dominios y subdominios.

Este ejemplo, fue realizado con **SPYSE.COM**.

Rango Red y Subred: este paso es especial para un **Pentest Interno**, dado que su tarea es averiguar el direccionamiento local, así como la segmentación de redes.

Con un simple uso del comando **IPCONFIG (Windows)** / **IFCONFIG (Linux)** dentro de la red o el uso de la tool de **KALI LINUX**, llamada **NETDISCOVER**, se pueden obtener estos datos.

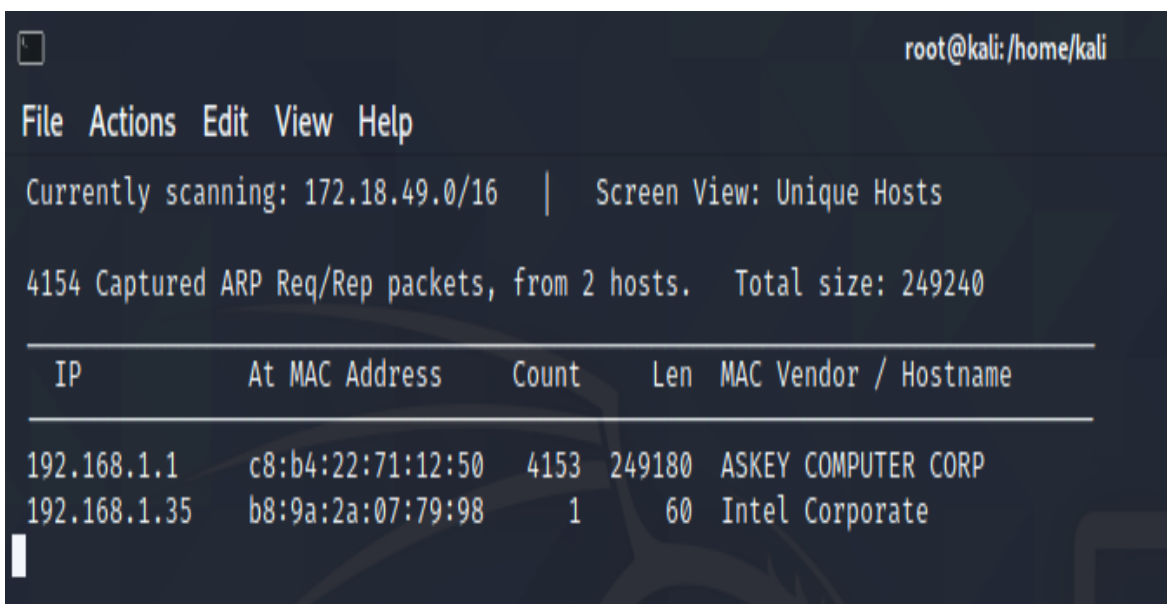
```
Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . . . : fe80::54f4:dd45:a787:fd48%23
Dirección IPv4. . . . . : 192.168.1.35
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

Direcciones IP específicas: cuando se escanea el sitio, se puede identificar los dispositivos, lo cual uno podría realizar un mapa de topología.

Maquinas Activas: se trata de los equipos que se encuentren sean accesibles o no.

Estos dos procesos, desde un **PING**, hasta el **NETDISCOVER** (tool de **Kali**), son las opciones más rápidas de uso.



```
root@kali: /home/kali

File Actions Edit View Help

Currently scanning: 172.18.49.0/16 | Screen View: Unique Hosts

4154 Captured ARP Req/Rep packets, from 2 hosts. Total size: 249240

+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+
| 192.168.1.1  | c8:b4:22:71:12:50 | 4153  | 249180 | ASKEY COMPUTER CORP   |
| 192.168.1.35 | b8:9a:2a:07:79:98 | 1      | 60    | Intel Corporate        |
+-----+-----+-----+-----+-----+
```

Puertos Abiertos y Aplicaciones: verificar servicios y aplicaciones en uso, que se encuentran escuchando en la red, tanto a nivel entrante como saliente.

Detectar SO: verificar el tipo de sistema operativo que se encuentra ejecutado en el objetivo.

Ambos puntos, la herramienta más recomendable es la tool **NMAP**, muy usada tanto para auditorías y búsquedas de dispositivos en la red, hoy dispone de scripts que facilitan distintas tareas, por ejemplo la opción “**script vuln**”, buscará vulnerabilidades en el objetivo.

```
(root@kali)~[/home/kali]
# nmap -sV -O 192.168.1.36
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-08 22:14 EST
Nmap scan report for 192.168.1.36
Host is up (0.00064s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp    open  rtsp?
2869/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:6C:01:FC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008::r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: LABORATORIO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.94 seconds
```

Info Contactos (Mails, Teléfonos, etc): para poder ser usados ante una técnica como Ingeniería Social, toda información debe ser verificada para descartar falsos positivos.

CENTRALOPS, se vuelve a utilizar, en este caso a través de información de **WHOIS**.

Domain Whois record

Queried whois.internic.net with "dom microsoft.com"...

```
Domain Name: MICROSOFT.COM
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-05-20T19:54:16Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2021-05-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1-205.AZURE-DNS.COM
Name Server: NS2-205.AZURE-DNS.NET
Name Server: NS3-205.AZURE-DNS.ORG
Name Server: NS4-205.AZURE-DNS.INFO
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-03-08T19:11:50Z <<<
```

País y ciudad donde residen los servidores: geolocalización y procesos legales en otros países, importante para no tener problemas legales, en caso de realizar un pentest en otro país, en este caso se usa una de las herramientas de **NIRSOFT**.

Major IP Addresses Blocks By Country

In this section, you can find the list of all major IP address blocks allocated for each country. For countries in europe and in the middle east, the name of the company/Internet provider that own these IP blocks is also displayed. In order to show only the major IP blocks, only IP blocks with 4096 addresses or more were added to the list. For United States, only IP blocks with 65536 addresses or more were added to the list.

Afghanistan	Albania	Algeria
American Samoa	Andorra	Angola
Antigua And Barbuda	Argentina	Armenia
Aruba	Australia	Austria
Azerbaijan	Bahamas	Bahrain
Bangladesh	Barbados	Belarus
Belgium	Belize	Benin
Bermuda	Bhutan	Bolivia
Bosnia And Herzegovina	Botswana	Brazil
Brunei Darussalam	Bulgaria	Burkina Faso
Burundi	Cambodia	Cameroon
Canada	Cape Verde	Cayman Islands

Que saber sobre los responsables del direccionamiento IP

Público

Existe el **RIR (Regional Internet Registry)** = Organización que supervisa la asignación y el registro de recursos de números de internet

Todos los dispositivos que se encuentren conectados a una red **IP** necesitan tener una **dirección IP**.

Las direcciones IP públicas y los números de sistema autónomo son recursos finitos, por ende, es necesario un manejo neutral y efectivo de estos recursos para asegurar la distribución justa e igualitaria así como para prevenir el acaparamiento.

Los recursos más utilizados relacionados con el direccionamiento son **IPv4** y **IPv6**, Sistemas Autónomos (**BGP**)

Los encargados de las bases son:

África = **AFRINIC** América Latina y Caribe = **LACNIC**

Asia = **APNIC** América = **ARIN** Europa/Oriente Medio = **RIPE NCC**



Luego cada país, dispone de una entidad local, para poder administrar entre sus empresas de comunicaciones, por ejemplo en **ARGENTINA** tenemos a **NIC**.

Estas son las bases de datos **WHOIS**, donde podemos encontrar, nombre del admin, cuando fue creado y actualizado el registro, servidores **DNS**, dominios asociados al objetivo.

Domain Whois record

Queried **whois.internic.net** with "**dom microsoft.com**"...

```
Domain Name: MICROSOFT.COM
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-05-20T19:54:16Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2021-05-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1-205.AZURE-DNS.COM
Name Server: NS2-205.AZURE-DNS.NET
Name Server: NS3-205.AZURE-DNS.ORG
Name Server: NS4-205.AZURE-DNS.INFO
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-03-08T19:11:50Z <<<
```

Mediante los datos que nos encontremos de bloques de red, se puede deducir por la máscara, que **IPs** están siendo utilizadas, tener en cuenta que es un dato muy importante localizar esas **IPs**, y sobre todo interpretarlas, por eso se reitera por Enésima vez: **DIRECCIONAMIENTO IP** es importante comprenderlo.

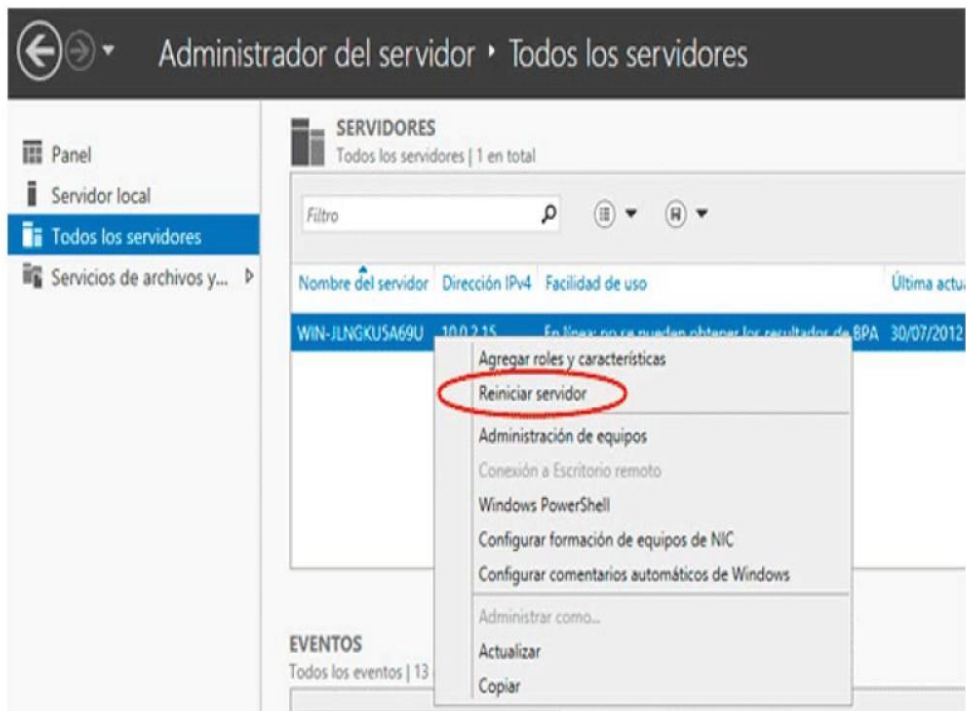
Network Whois record

Queried **whois.arin.net** with "**n 104.215.148.63**"...

```
NetRange:      104.208.0.0 - 104.215.255.255
CIDR:          104.208.0.0/13
NetName:       MSFT
NetHandle:     NET-104-208-0-0-1
Parent:        NET104 (NET-104-0-0-0-0)
NetType:       Direct Assignment
OriginAS:      AS8075
Organization:  Microsoft Corporation (MSFT)
RegDate:       2014-10-01
Updated:       2014-10-01
Ref:           https://rdap.arin.net/registry/ip/104.208.0.0
```

Otros datos a tener en cuenta en un reconocimiento:

¿Cuál es la regla de oro en los servidores???



Que necesitan estar siempre disponibles, por ende, **CUANTO MENOS SE APAGUEN O REINICIEN MEJOR**, he aquí un dato muy importante:

Si se consigue dar la fecha de **booteo** de ese servidor, puede darse cuenta que parches o protecciones no están instaladas, conclusión, es una técnica muy usada y fácil por un atacante para saber que necesita y de esa forma vulnerar el objetivo.

Otra opción es, una vez conseguido «ciertas» cantidades de datos, se podrá diagramar la posible topología de la red (esto en caso de hacer un test de penetración sin información alguna que nos brinde la empresa)

Para aclarar este punto, recuerden que tenemos 3 ambientes para trabajar, el **White Box**, la empresa nos brinda toda la información que requerimos, el **Black Box**, la empresa no nos brinda ningún tipo de información (por lo que tendríamos que arreglarnos con lo encontrado por nuestros propios medios), y el **Grey Box**, que sería que la empresa nos da cierta información, que puede ser relevante o no.

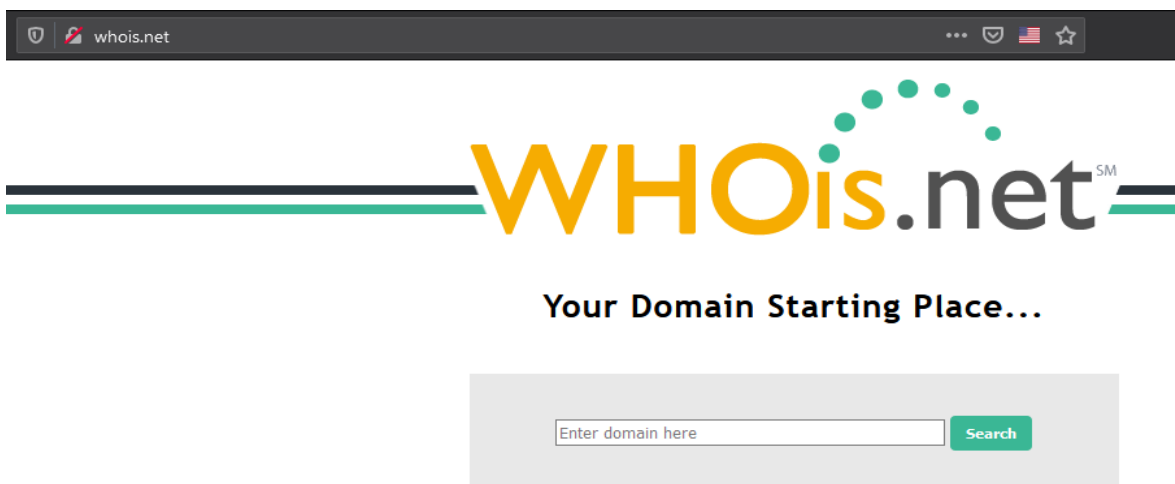
Las técnicas de reconocimiento, son muy importantes, así como di ejemplos, lo ideal es que prueben con un objetivo virtual (hay cientos de laboratorios) y recopilen toda la información posible y que entre todos los presentes veamos los ejemplos, obviamente la parte de desarrollo.

Check WEB Pages

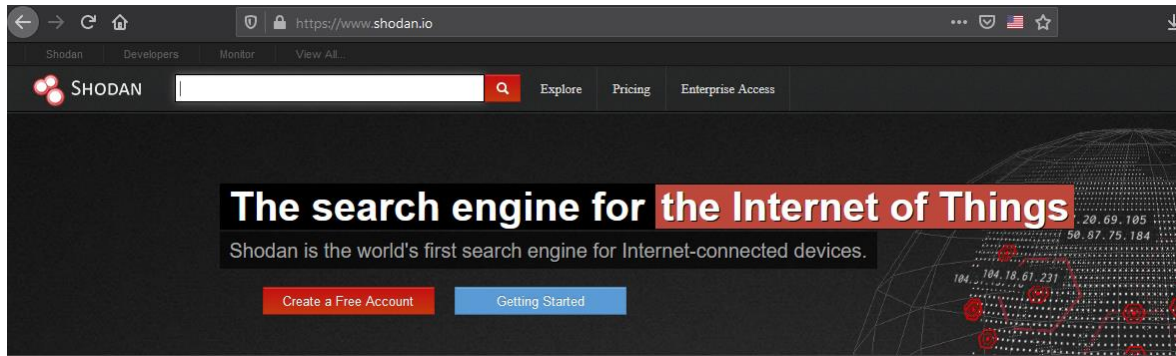
En este procedimiento, es bueno disponer de una serie de WEBS online que nos ayudaran a cumplir parte de lo que necesitamos para empezar a realizar el reconocimiento tanto activo como pasivo.

A continuación se expondrán algunos sitios recomendados que nos pueden ser útiles para poder completar la recolección de información necesaria y de esa manera poder seguir haciendo el **Pentest**.

Los sitios que exponemos, son recomendados, obviamente que pueden haber algunos mejores, es un aporte nada más.



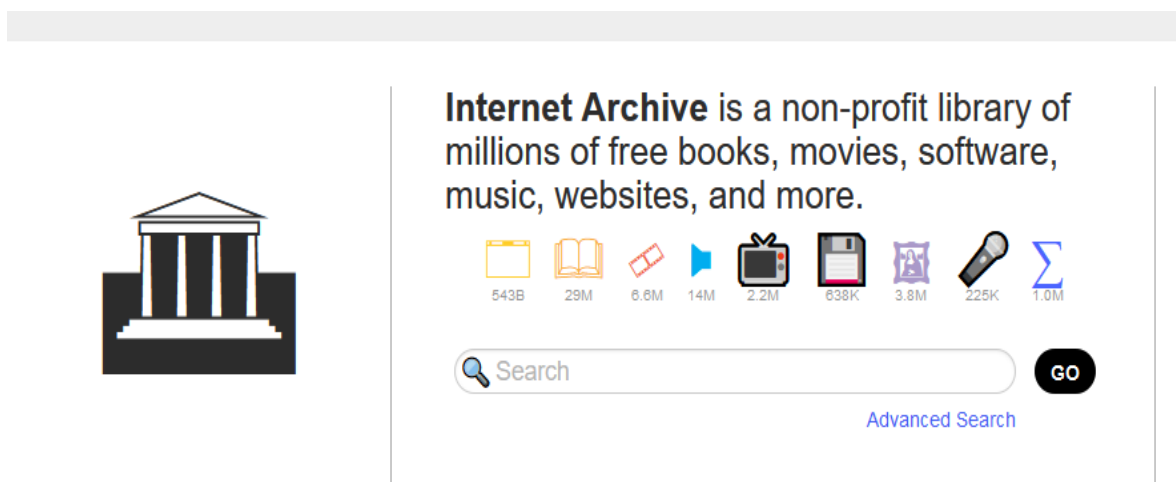
WHOIS Lookup: Identifica información de registración de un dominio internacional



SHODAN.IO (búsqueda periféricos, datos, etc) expone puertos y servicios



NETCRAFT (Búsqueda datos, DNS, etc)



ARCHIVE.ORG (Búsqueda de historiales de webs, etc)

Free online network tools

Tools

Domain Dossier

Investigate domains and IP addresses. Get registrant information, DNS records, and more—all in one report.

enter a domain or IP address

go

or [learn about yourself](#)

Domain Check

See if a domain is available for registration.

Email Dossier

Validate and troubleshoot email addresses.

Browser Mirror

See what your browser reveals about you.

Ping

See if a host is reachable.

Traceroute

Trace the network path from this server to another.

NsLookup

Look up various domain resource records with this version of the classic NsLookup utility.

AutoWhois











Get Whois records automatically for domains worldwide.

AnalyzePath



Do a simple, graphical traceroute.

CENTRALOPS (Búsqueda de datos, DNS, etc)

you get signal

- tools**
 -  **Port Forwarding Tester** -> find open ports on your connection
 -  **What Is My IP Address** -> quickly identify your external IP address
 -  **Network Location Tool** -> locate a network using Google Maps
 -  **Visual Trace Route Tool** -> plot the route to network address
 -  **Phone Number Geolocator** -> figure out who's calling
 -  **Reverse E-mail Lookup Tool** -> figure out who's e-mailing
 -  **Reverse IP Domain Check** -> find other sites on a web server
 -  **WHOIS Lookup Tool** -> check to see if a domain name is available
- other**
 -  **Links** -> visit sponsors and find other networking resources
 -  **About YouGetSignal.com** -> learn about the site and donate

NETWORK TOOLS (Búsqueda de dominios, datos, etc)

← → ↻ 🏠   <https://mxtoolbox.com>

JavaScript is disabled. Javascript is required for this site.

MX Lookup

Domain Name

[MX Lookup](#) [Solve Email Delivery Problems](#)

ABOUT MX LOOKUP

This test will list MX records for a domain in priority order. The MX lookup is done directly against the domain's authoritative name server, so changes Open Relay check and measure response time performance. You may also check each MX record (IP Address) against 105 DNS based [blacklists](#). (

MX TOOLBOX (Búsqueda de dominios, datos, etc)



[Búsqueda avanzada](#)
[Herramientas del idioma](#)

[Buscar con Google](#) [Voy a tener suerte](#)

Google.com.ar ofrecido en: [español \(Latinoamérica\)](#)

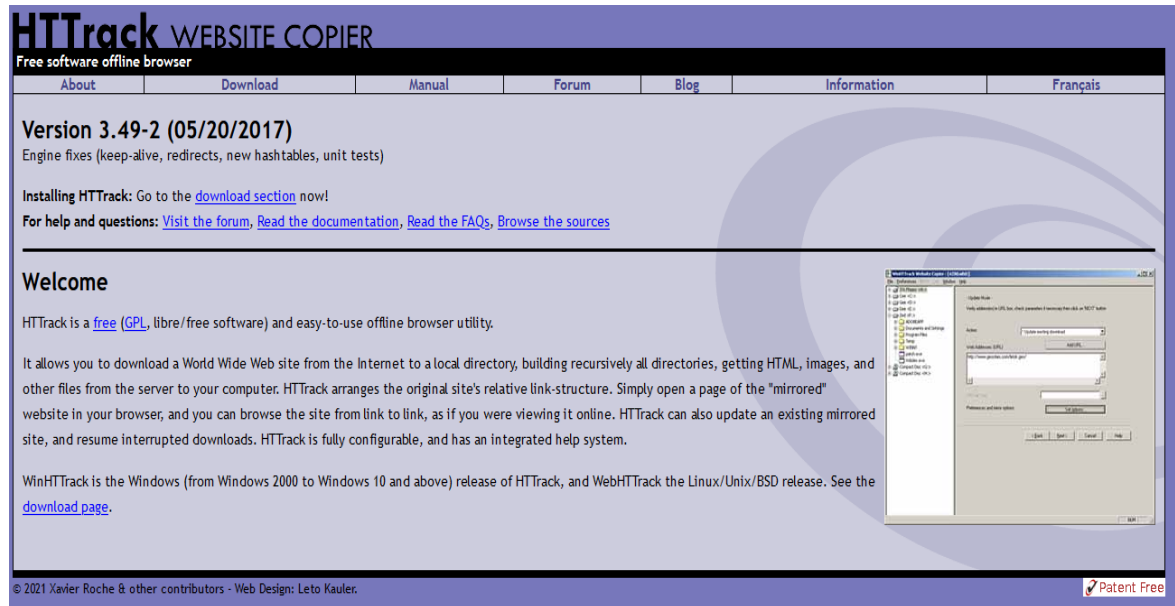
[Programas de publicidad](#) [Soluciones Empresariales](#) [Todo acerca de Google](#) [Google.com in English](#)

GOOGLE (Búsqueda de personas, datos, etc) es una de las mejores fuentes de información

También se puede utilizar : <http://www.google.com/maps>

Software Tools

Disponemos de muchas herramientas para ser usada en la recolección de datos, se expondrán a continuación algunas de las mas conocidas.



BAJADA DE WEBSITES PUBLICOS Y PRIVADOS e INTERNOS

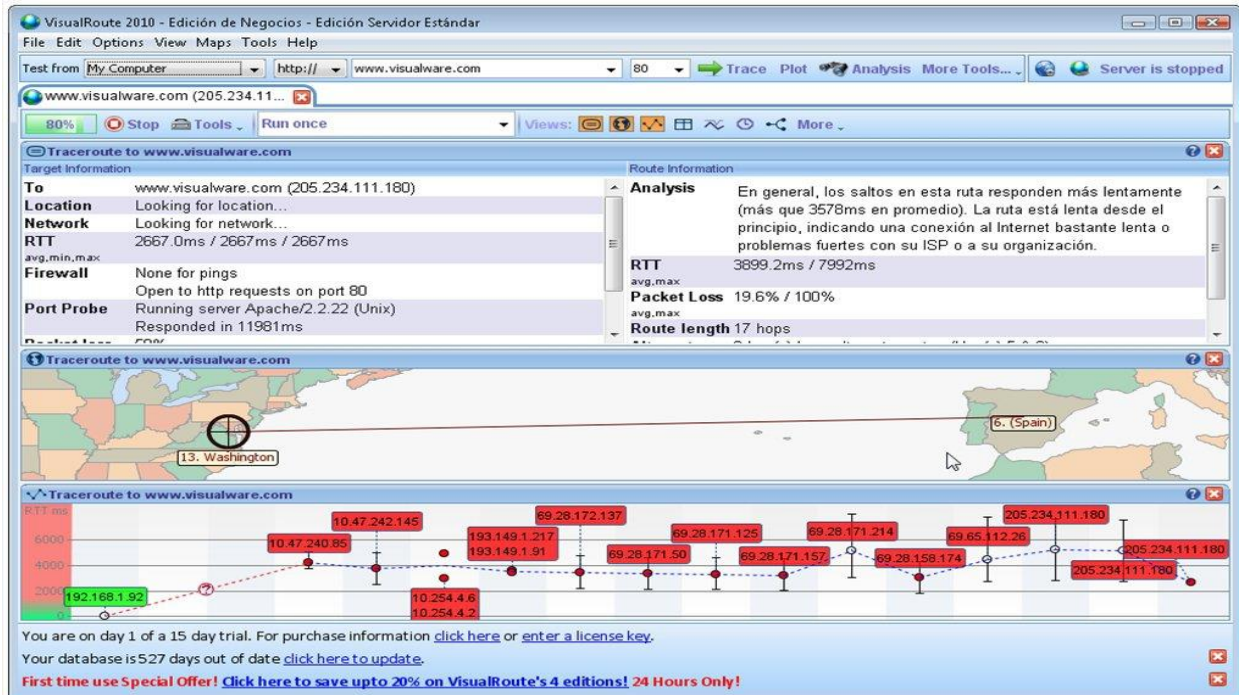
EJEMPLO: WWW.INTRUDERS.COM

[HTTP://PARTNERS.INTRUDERS.COM](http://PARTNERS.INTRUDERS.COM)

[HTTP://INTRANET.INTRUDERS.COM](http://INTRANET.INTRUDERS.COM)

Se podría utilizar el WGET o HTTrack, para copiar el sitio completo y poder ver sus ramificaciones.

Muy utilizada para bajar el sitio completo a un dispositivo, y luego analizar su información.

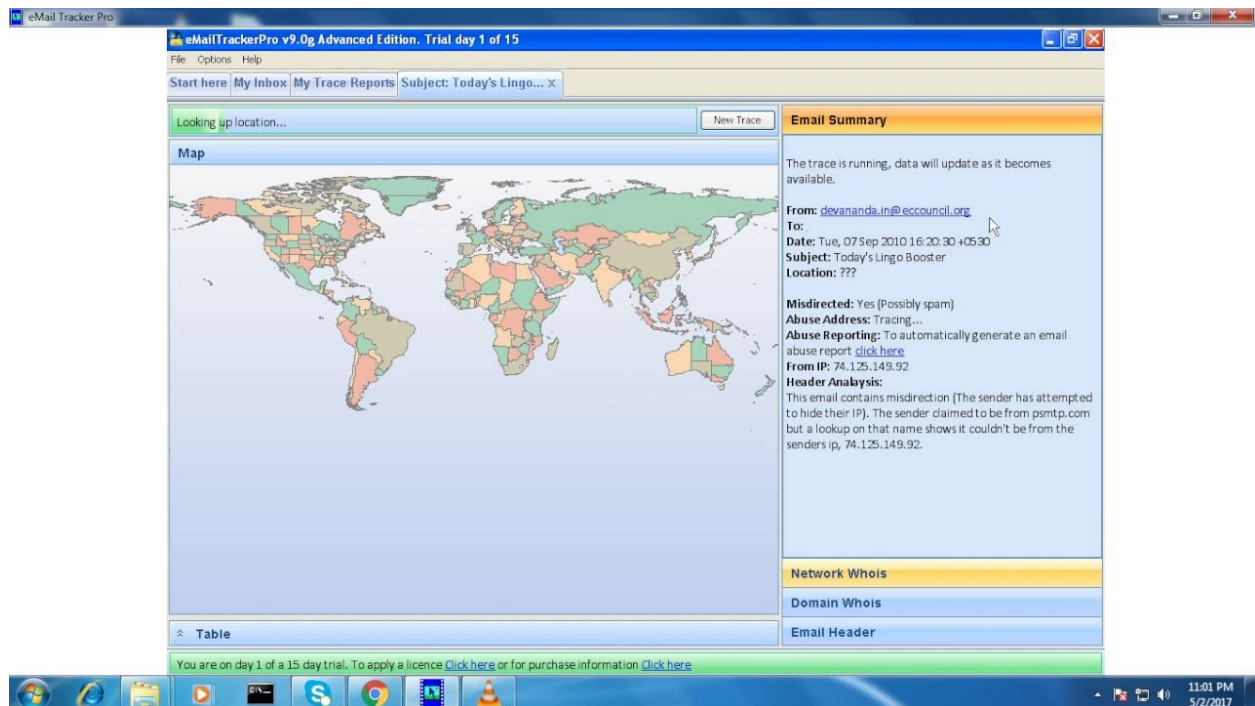


HACKING TOOLS = VISUAL ROUTE




HACKING TOOLS = MALTEGO

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
 (1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning



EMAIL TRACKER PRO


 New Scan Scans Settings About

uber.com FINISHED

Summary Browse Graph Scan Settings Log

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Domain Name	11	11	2020-06-26 01:08:56
Affiliate - Internet Name	68	72	2020-06-26 01:17:34
BGP AS Membership	11	134	2020-06-26 01:19:09
Co-Hosted Site	274	300	2020-06-25 21:23:14
Co-Hosted Site - Domain Name	140	274	2020-06-25 21:23:14
Domain Name	1	3	2020-06-26 01:24:16
IP Address	178	268	2020-06-26 01:22:46
IPv6 Address	24	24	2020-06-25 22:28:27
Internet Name	136	689	2020-06-26 01:20:39
Internet Name - Unresolved	12	50	2020-06-26 01:13:43
Netblock Membership	21	40	2020-06-26 01:17:59
Open TCP Port	277	503	2020-06-26 01:19:09

SPIDERFOOT



```
[recon-ng v4.9.3, Tim Tomes (@LaNMaSteR53)]
```

```
[75] Recon modules
[8] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules
```

```
[recon-ng][default] >
```

AYUDA PLUS: cuando uno encuentra datos de DNS, tiene que comprender para que es cada registro

Registro	Función
A	Dado un nombre devuelve la IP correspondiente
NS	Indica la dirección IP de un servidor DNS para el dominio dado. Pueden existir varios.
MX	Indica la dirección IP de un servidor de mail para el dominio dado. Pueden existir varios.
PTR	Indica el nombre correspondiente a una dirección IP dada. Sólo puede existir uno por dirección IP.
CNAME	Es un alias. Si un host tiene varios nombres se especifica uno con un registro A y el resto con CNAME, haciendo referencia al nombre en el registro A. Pueden existir varios.
SOA	Es un registro especial que provee información importante sobre la configuración de una zona en un DNS. Es básicamente utilizado para el funcionamiento interno del servicio. Sólo puede haber uno.
SPF	Es un registro especial cuya función principal es la de ayudar a combatir el SPAM. Lo que indica es qué servidores están autorizados para enviar correos para el dominio en cuestión.

CONCLUSION

La etapa de reconocimiento es importante, ofreciéndonos un panorama de algo nuevo a nuestros ojos, dándonos la posibilidad de empezar a “dibujar” lo que sería el objetivo.

Nadie es adivino de lo que podemos encontrar, pero... si estamos en condiciones de poder diagramar, dibujar, complementar, gracias a la recolección de datos realizada, a través de este método, uno podría tener una idea.

Ejercicio 2 Unidad 1



Seleccionar un sitio web y tratar de buscar información del mismo, haciendo un desarrollo de lo encontrado, REITERO: buscar información del mismo, a partir de lo encontrado en INTERNET o sea información pública.

En caso de ser necesario, se le puede solicitar al instructor un listado de sitios para poder usarlos en el reconocimiento pasivo, por ejemplo: CentralOPS, Robtex.

PD: esto no es un ataque, es chequear información que este pública en INTERNET, subirlo al foro, y abriremos debates sobre lo encontrado (por favor, no más de 3 páginas)

Cómo presentar los ejercicios de la unidad

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido_UnidadX.doc (donde apellido será el de cada uno y la "X" el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy **IMPORTANTE** que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad.

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

Los ejercicios de esta unidad no llevan calificación

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.



Bibliografía utilizada y sugerida

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU.

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México.

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España.

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU.

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learn the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU.

En caso de que los links que se exponen no funcionen, por favor avisar al instructor (es normal que un sitio pueda cambiar su URL, dominio o variables, lo cual como la unidad se prepara a principio de año podría suceder que se haya modificado)