

BIENVENIDOS al Taller de NMap

Los datos del Router Wifi para hacer las prácticas y el material necesario es:

Nombre WIFI: CRONSEC

CONTRASEÑA: HACKMADRID%27

Página Material:

192.168.1.10:8080/wordpress/

contacto@rodolfolopez.es rodolfolopez.es

Taller NMap



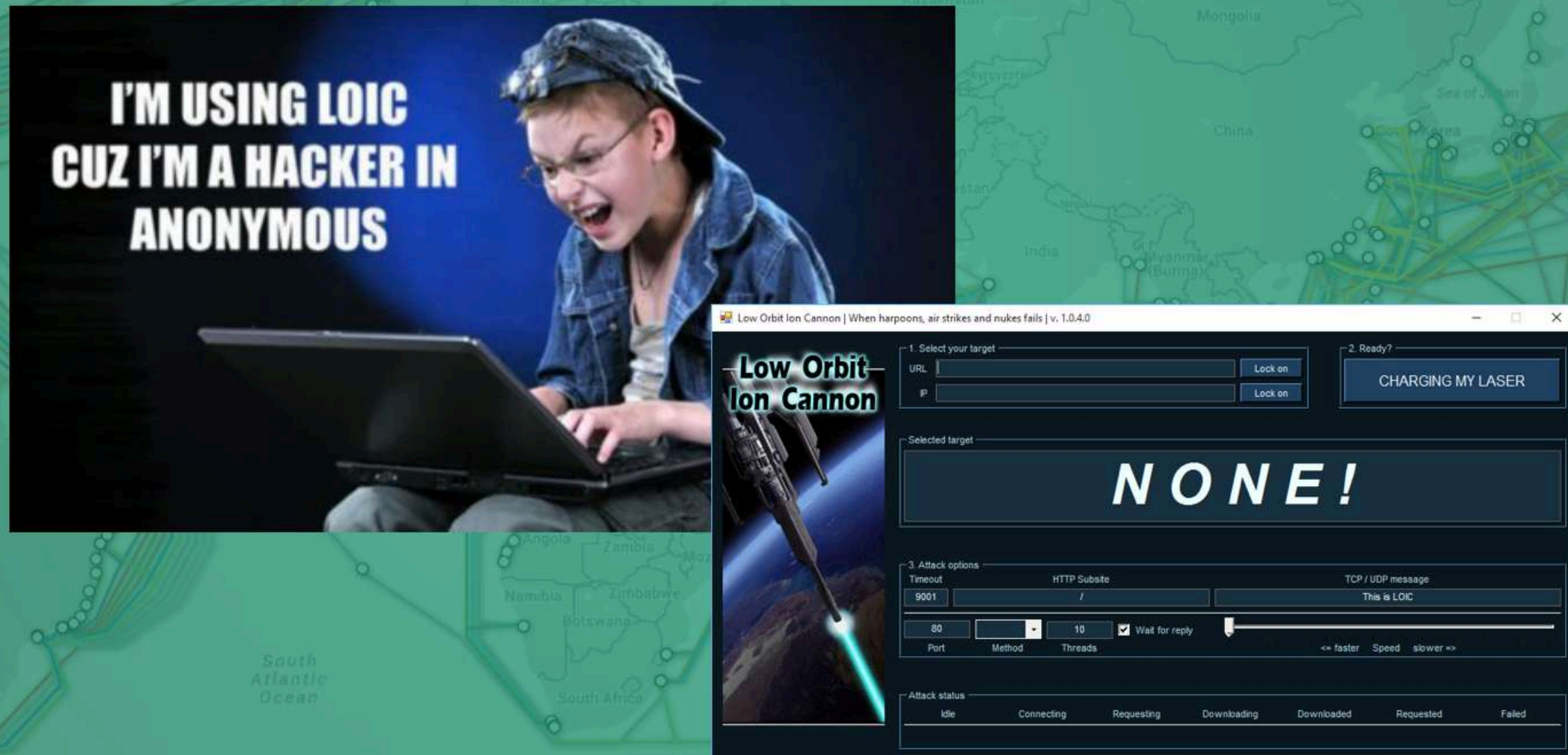
Rodolfo Miguel López
rodolfolopez.es
CronSec.com

contacto@rodolfolopez.es

rodolfolopez.es

Taller NMap [No ScriptKiddies]

Se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que **no tiene intención de aprender.**



contacto@rodolfolopez.es rodolfolopez.es

“ Lo primordial no es saber usar la herramienta sino saber lo que queremos conseguir con cualquier herramienta a tu disposición.”

Taller NMap [Glosario]

- **Host** : El término host o anfitrión se usa en informática para referirse a las computadoras u otros dispositivos conectados a una red.
- **Protocolo** : Sistema de reglas que permiten que dos o más entidades se comuniquen entre ellas.
- **Puerto**: Es una interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos. Puede ser física o por software también llamada lógica.
- **Servicio** : Son programas que proporcionan una utilidad por ejemplo: DNS, DHCP, FTP
- **OSI** : Open System Interconnection es un modelo de referencia creado por la ISO, International Organization for Standardization.

Taller NMap [Glosario]

- **Gui** : Graphic User Interface es un programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos.
- **Cli**: Permite a los usuarios dar instrucciones a algún programa informático por medio de una línea de texto simple.
- **Flag** : Funciones o opciones específicas que se pueden activar y desactivar en un Segmento TCP.
- **MAC** : Identificador de 48 bits para identificar de forma única la tarjeta de red. [6d:5d:62:5f:d0:43]
- **Dirección IP** : Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red de un dispositivo que utilice el protocolo IP (Internet Protocol). [192.168.1.1]

Taller NMap [Glosario]

- **Ping** : Es una utilidad de diagnóstico en redes de computadoras que comprueba el estado de la comunicación del host local con uno o varios equipos remotos de una red IP por medio del envío de paquetes ICMP.
- **ARP**: Es un protocolo de resolución de direcciones, responsable de encontrar la dirección de hardware **MAC** que corresponde a una determinada **dirección IP**.
- **Spoofing**: Técnica a través de la cual se consigue falsificar los datos en una comunicación.

Las metodologías de Pentesting o pruebas de penetración son una serie de recomendaciones para llevar a cabo una prueba de intrusión.

Hay muchas metodologías y cada Pentester usa la que mas le gusta.

Pero a grandes rasgos casi todas tienen una serie de fases que suelen ser las siguientes:

- Fase de reconocimiento: Recopilación de la información por ej: OSINT
- **Fase de escaneo: Escaneo de puertos y servicios para buscar vectores de ataque.**
- Fase de enumeración: Obtención de datos, usuarios, equipos, servicios...
- Fase de acceso: Explotación de vulnerabilidades.
- Fase de mantenimiento de acceso o persistencia: Mantener durante el mayor tiempo el acceso a los sistemas comprometidos.

Taller NMap

[Modelo OSI]

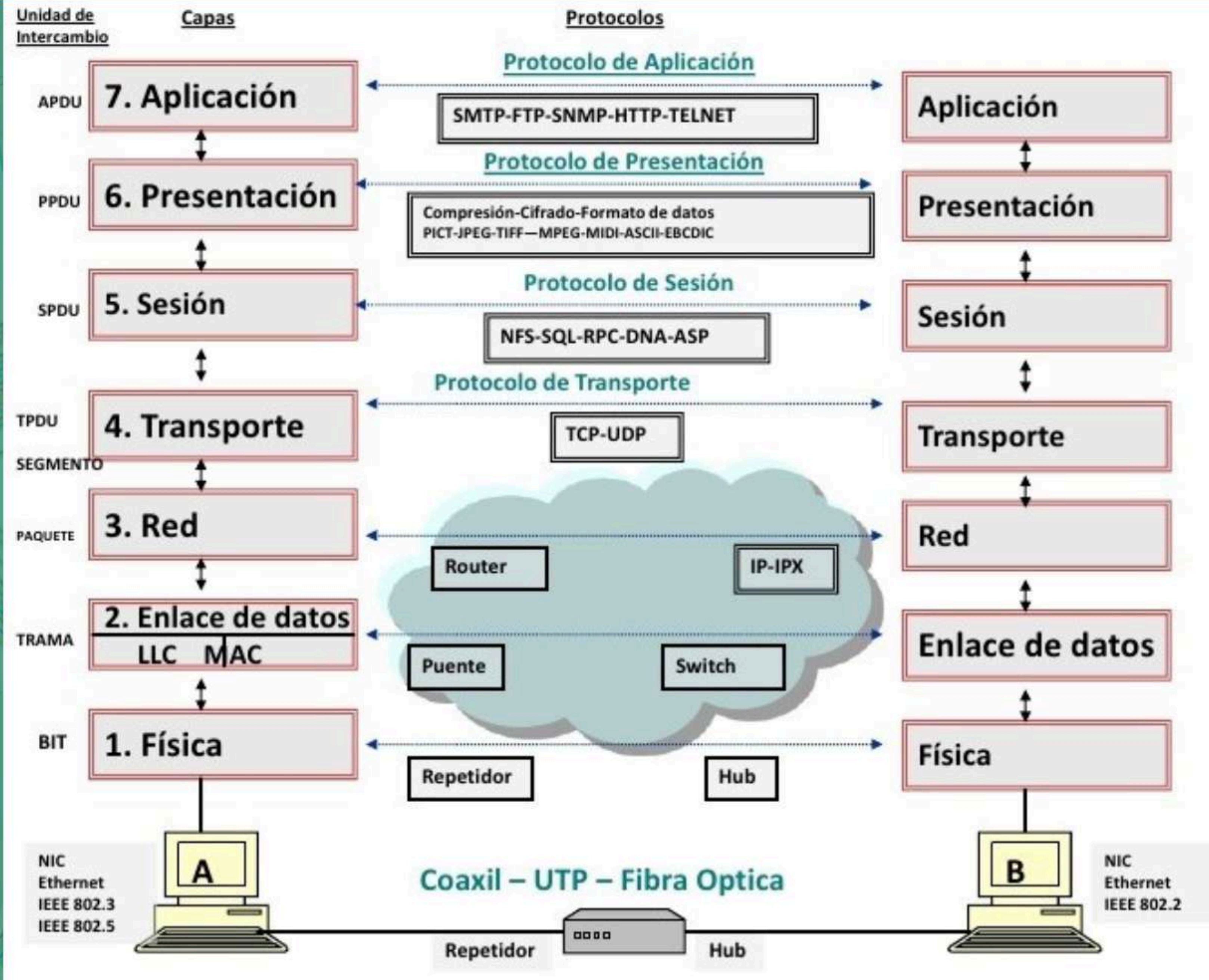


Space Invaders National Championship

1980

contacto@rodolfolopez.es rodolfolopez.es

Taller NMap [Modelo OSI]



Taller NMap

[Modelo TCP/IP vs OSI]

OSI Model vs. TCP/IP Model

OSI Reference Model

Application - Identifying and establishing the availability of intended communication partner and whether there are sufficient resources

Presentation - Data translation, encryption, code formatting

Session - Setting up, managing and tearing down sessions. Keeps application's data separate

Segment

Transport - Provides end-to-end transport services - establishes logical connections between hosts. Connection-oriented or connectionless data transfer.

packet

Network - Manages logical addressing and path determination

frame

Data Link - Provides physical transmission of data, handles error notification, flow control and network topology. Split into two sub layers (LLC and MAC)

bits

Physical - Specifies electrical, mechanical, procedural and functional requirements for activating, maintaining and deactivating a physical link.

Protocol Data Units (PDUs)

TCP/IP Model Protocol Suite

Process/Application layer

FTP - TCP file transfer service – port 20-21

Telnet - Terminal emulation program – port 23

TFTP - UDP file transfer – port 69

SMTP - Send email service – port 25

DHCP - Assigns IP addresses to hosts – ports 67 and 68

DNS - Resolves FQDNs to IP addresses – port 53

Host-to-Host layer

TCP - Connection-oriented protocol, provides reliable connections (acknowledgments, flow control, windowing)

UDP - Connectionless protocol, low overhead but unreliable

Internet layer

IP - connectionless protocol, provides network addressing and routing

ARP - finds MAC addresses from known IPs

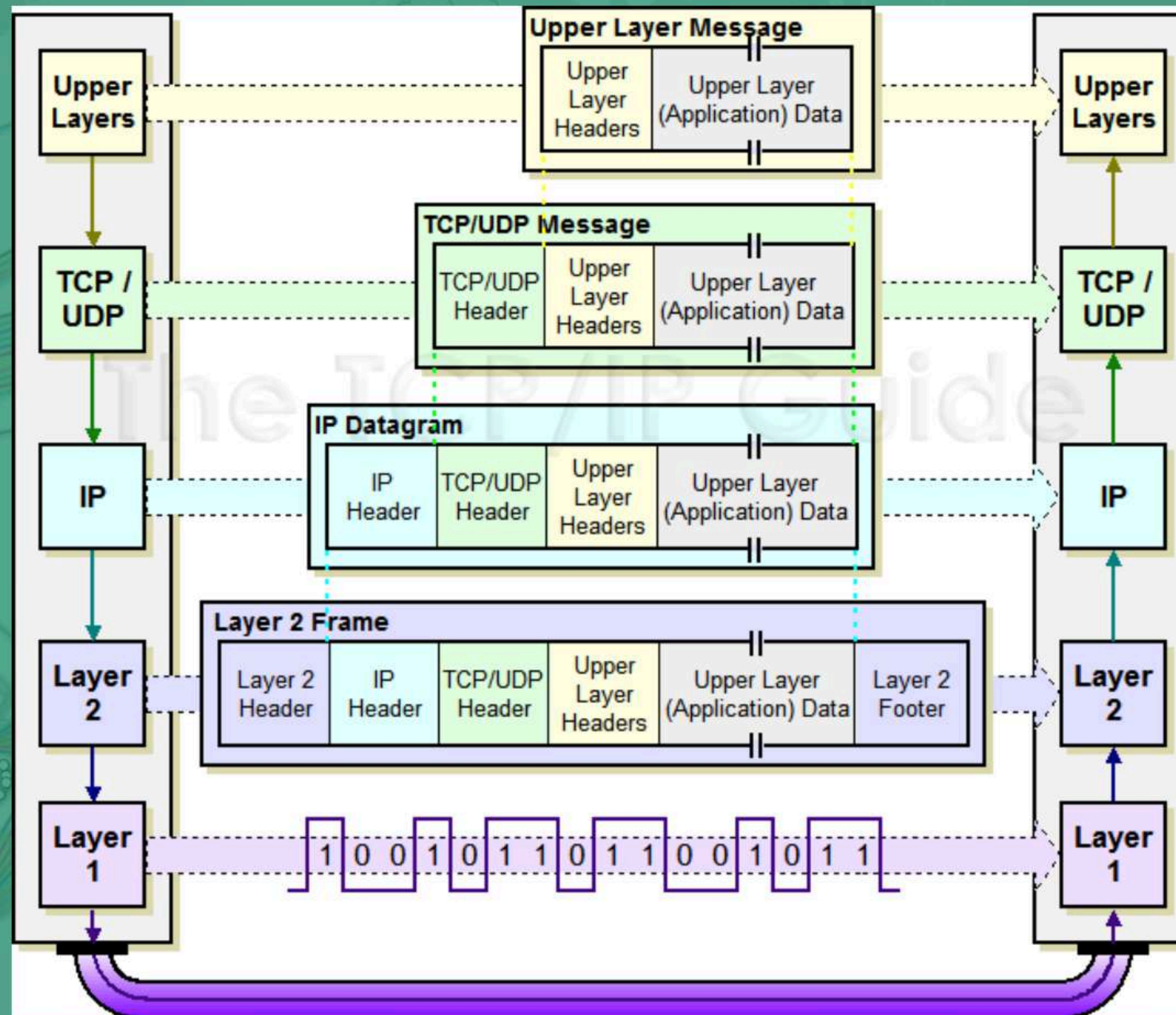
RARP - finds IPs from known MAC addresses

ICMP - provides diagnostics, used by ping and traceroute

Network Access

Taller NMap

[Capas de información]

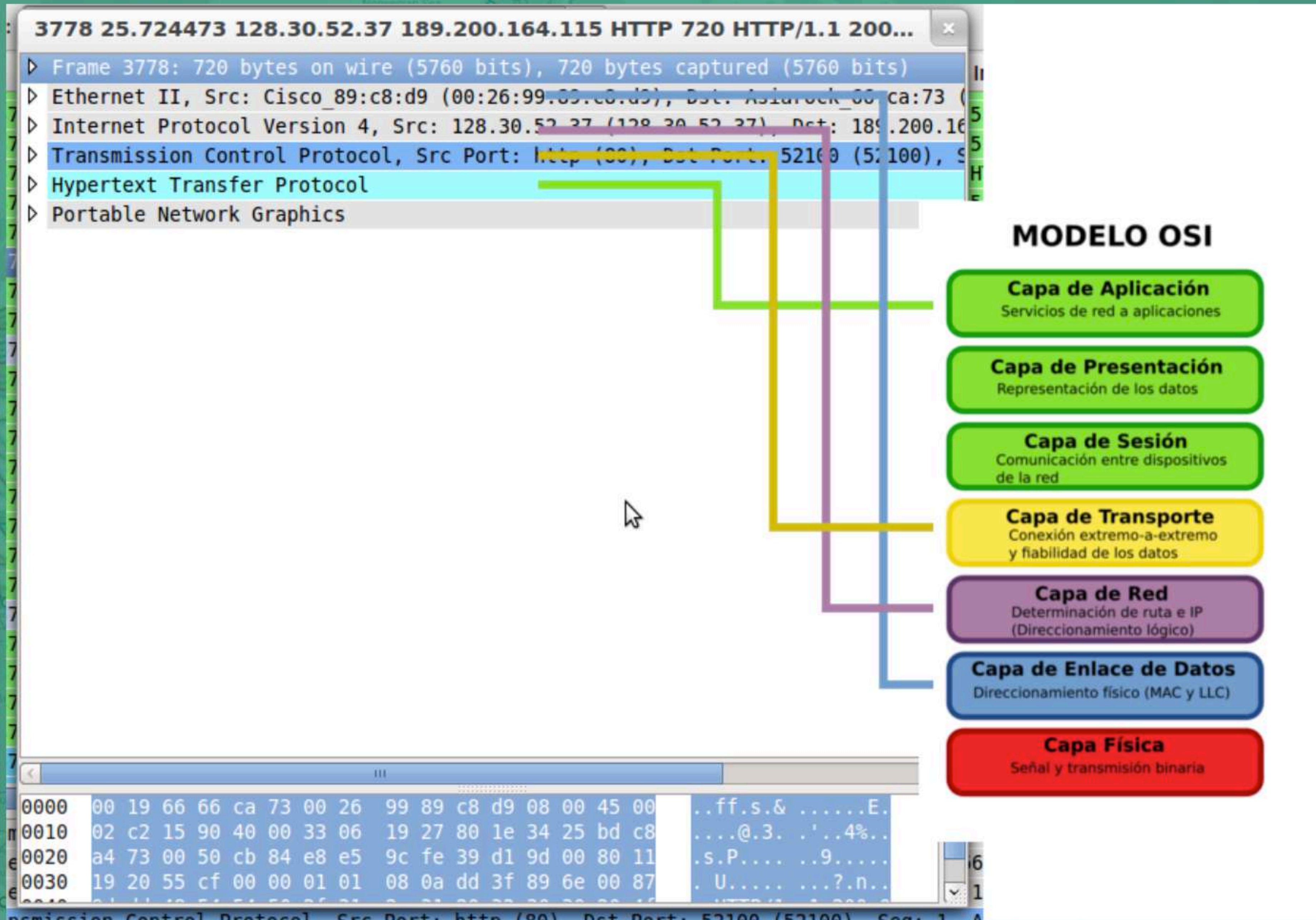


El protocolo TCP/IP es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red.

TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

Taller NMap

[TCP/IP vs OSI]



Taller NMap [Protocolo TCP]

TCP: Transmission Control Protocol es uno de los protocolos fundamentales en redes se utiliza para crear "conexiones" entre equipos/hosts a través de las cuales pueden enviarse un flujo de datos, el protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

Segmento TCP

Offsets	Octeto	0								1								2								3							
Octeto	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Puerto de origen																Puerto de destino															
4	32	Número de secuencia																															
8	64	Número de acuse de recibo (si ACK es establecido)																															
12	96	Longitud de Cabecera				Reservado				N S	C W R	E C E	U R G	A C K	P S H	R S T	S Y N	F I N	Tamaño de Ventana														
16	128	Suma de verificación																Puntero urgente (si URG es establecido)															
20	160	Opciones (Si la Longitud de Cabecera > 5, relleno al final con "0" bytes si es necesario)																															
...																															

Taller NMap [Protocolo UDP]

UDP: Es un protocolo del nivel de transporte basado en el intercambio de datagramas, permite el envío de información a través de la red sin que se haya establecido previamente una conexión, no tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción.

El protocolo UDP se utiliza por ejemplo cuando se necesita transmitir voz o vídeo y resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

Segmento UDP

+	Bits 0 - 15	16 - 31
0	Puerto origen	Puerto destino
32	Longitud del Mensaje	Suma de verificación
64	Datos	

Taller NMap [Protocolo TCP]

Banderas/Flags TCP

Aunque hay más flags o banderas las que vamos a ver son las principales, las demás se utilizan para control de tráfico.

Segmento TCP

Offsets	Octeto	0								1								2								3							
Octeto	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Puerto de origen																Puerto de destino															
4	32	Número de secuencia																															
8	64	Número de acuse de recibo (si ACK es establecido)																															
12	96	Longitud de Cabecera				Reservado				N S	C W R	E C E	U R G	A C K	P S H	R S T	S Y N	F I N	Tamaño de Ventana														
16	128	Suma de verificación																Puntero urgente (si URG es establecido)															
20	160	Opciones (Si la Longitud de Cabecera > 5, relleno al final con "0" bytes si es necesario)																															
...																															

Taller NMap [Protocolo TCP]

Offsets	Octeto	0								1								2								3							
Octeto	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Puerto de origen																Puerto de destino															
4	32	Número de secuencia																															
8	64	Número de acuse de recibo (si ACK es establecido)																															
12	96	Longitud de Cabecera				Reservado				N S	C W R	E C E	U R G	A C K	P S H	R S T	S Y N	F I N	Tamaño de Ventana														
16	128	Suma de verificación																Puntero urgente (si URG es establecido)															
20	160	Opciones (Si la Longitud de Cabecera > 5, relleno al final con "0" bytes si es necesario)																															
...																															

- **SYN** : (Synchronizese) Se utiliza para iniciar una conexión.
- **ACK** : (Acknowledgement) Confirma la conexión
- **RST** : (Reset) Se Utiliza para reiniciar una conexión, por motivos diversos.
- **FIN** : (Finalize) Se utiliza para finalizar la conexión.
- **PSH** : (Push) Se utiliza para forzar el enviado inmediato de los datos tan pronto como sea posible.
- **URG** : (Urgent) Se dispone de datos urgentes que enviar

Taller NMap [Protocolo TCP]

```

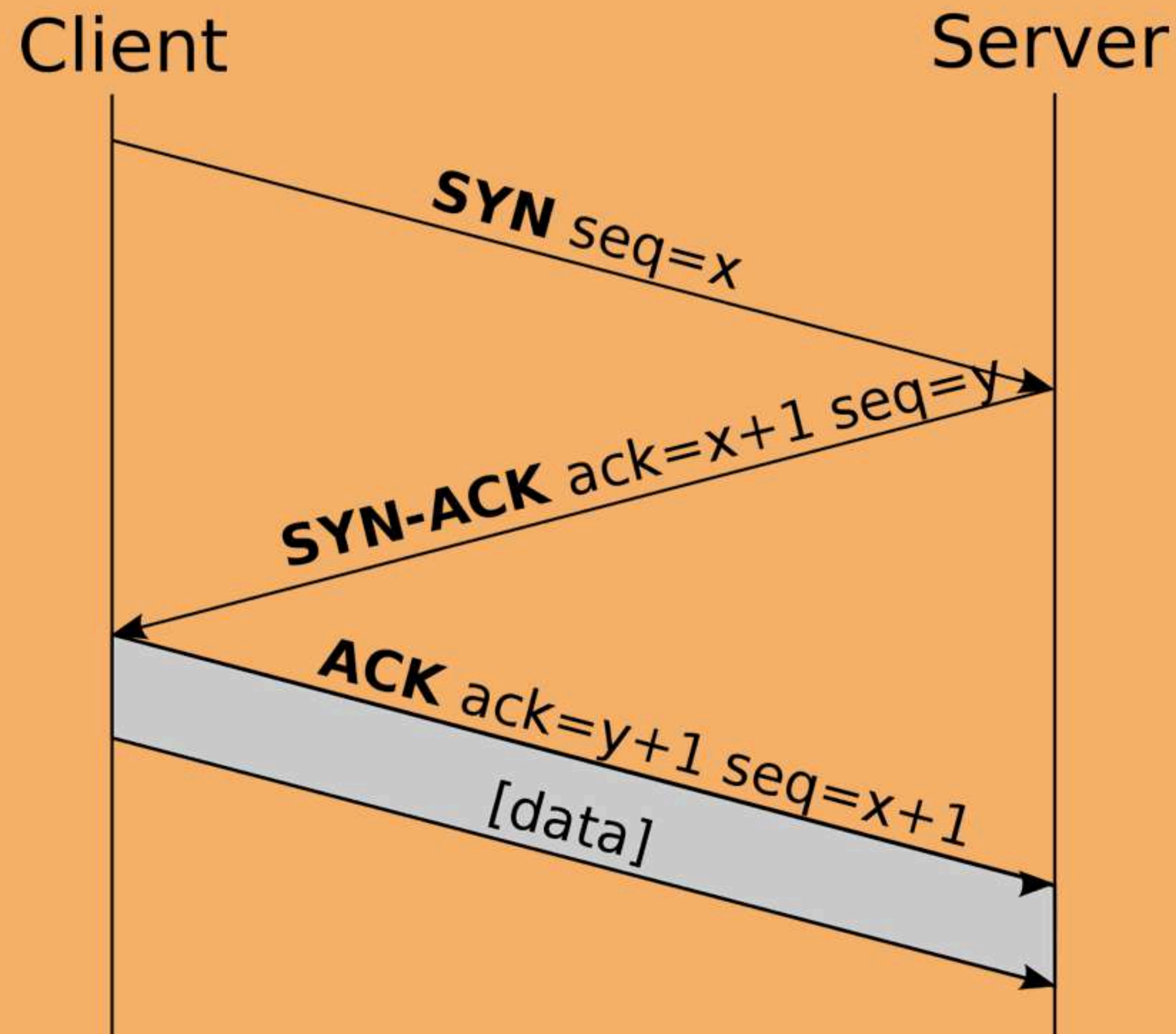
Transmission Control Protocol, Src Port: 63865 (63865), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 717
  Source Port: 63865 (63865)
  Destination Port: 80 (80)
  [Stream index: 31]
  [TCP Segment Len: 717]
  Sequence number: 1      (relative sequence number)
  [Next sequence number: 718      (relative sequence number)]
  Acknowledgment number: 1      (relative ack number)
  Header Length: 32 bytes
  ▾ .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
  Window size value: 4117
  [Calculated window size: 131744]
  [Window size scaling factor: 32]
  ▸ Checksum: 0x8772 [validation disabled]

0000  74 d4 35 45 ca e0 68 5b 35 94 80 af 08 00 45 00  t.5E..h[ 5.....E.
0010  03 01 96 62 40 00 40 06 00 00 c0 a8 01 d8 c0 a8  ...b@.@. ....
0020  01 56 f9 79 00 50 57 6d a2 ce 9e 18 be cf 80 18  .V.y.PWm .....
0030  10 15 87 72 00 00 01 01 08 0a 20 45 fd 66 52 89  ...r.... .. E.fR.
0040  ce 52 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31  .RGET / HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e  ..Host: 192.168.
0060  31 2e 38 36 0d 0a 41 63 63 65 70 74 3a 20 74 65  1.86..Ac cept: te
0070  78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74  xt/html, applicat
0080  69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70  ion/xhtm l+xml,ap
0090  70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d  plicatio n/xml;q=
00a0  30 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 43  0.9,*/*; q=0.8..C
00b0  6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d  onnectio n: keep-
00c0  61 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 5f  alive..C ookie: _
```


Taller NMap [Protocolo TCP]

Las conexiones TCP se componen de tres etapas:

1. establecimiento de conexión.



I AM HERE...



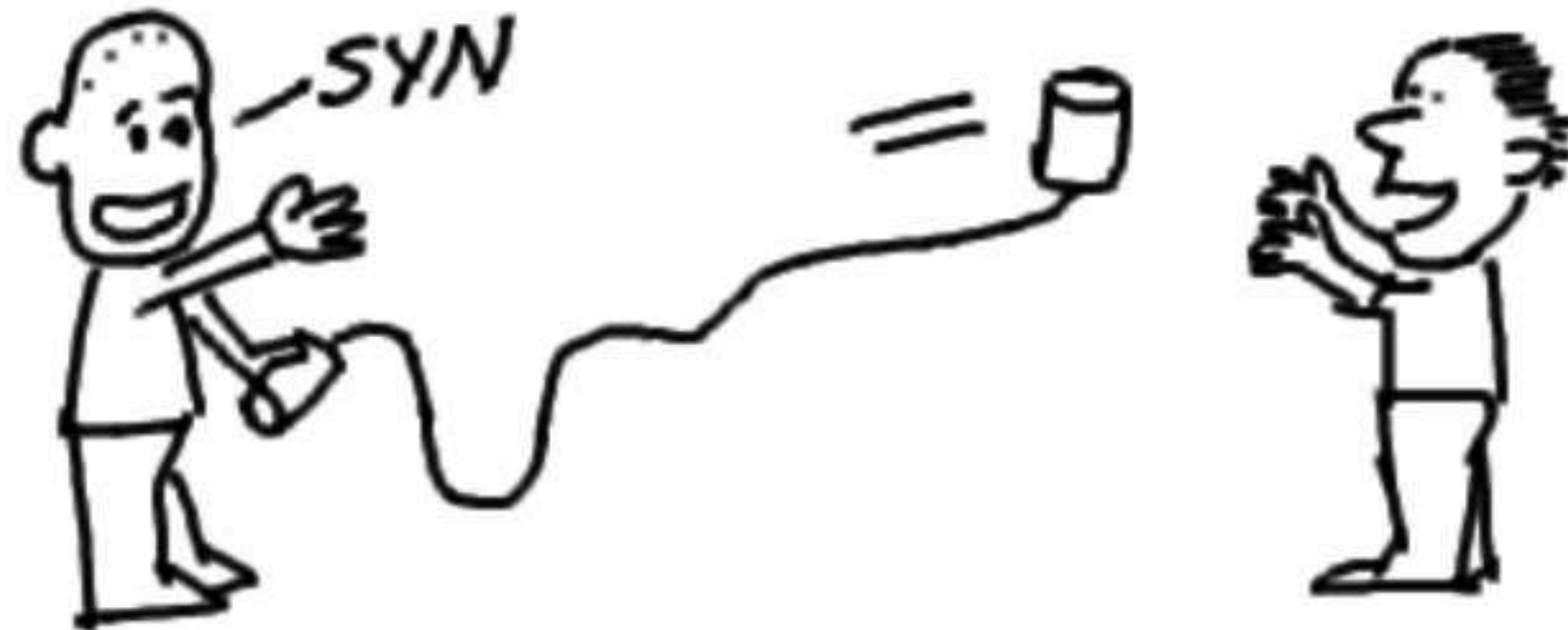
...JUST BUILDING...



...MY LAYER 1



-SYN



SYN-ACK



-ACK



WE ARE SO GEEKS

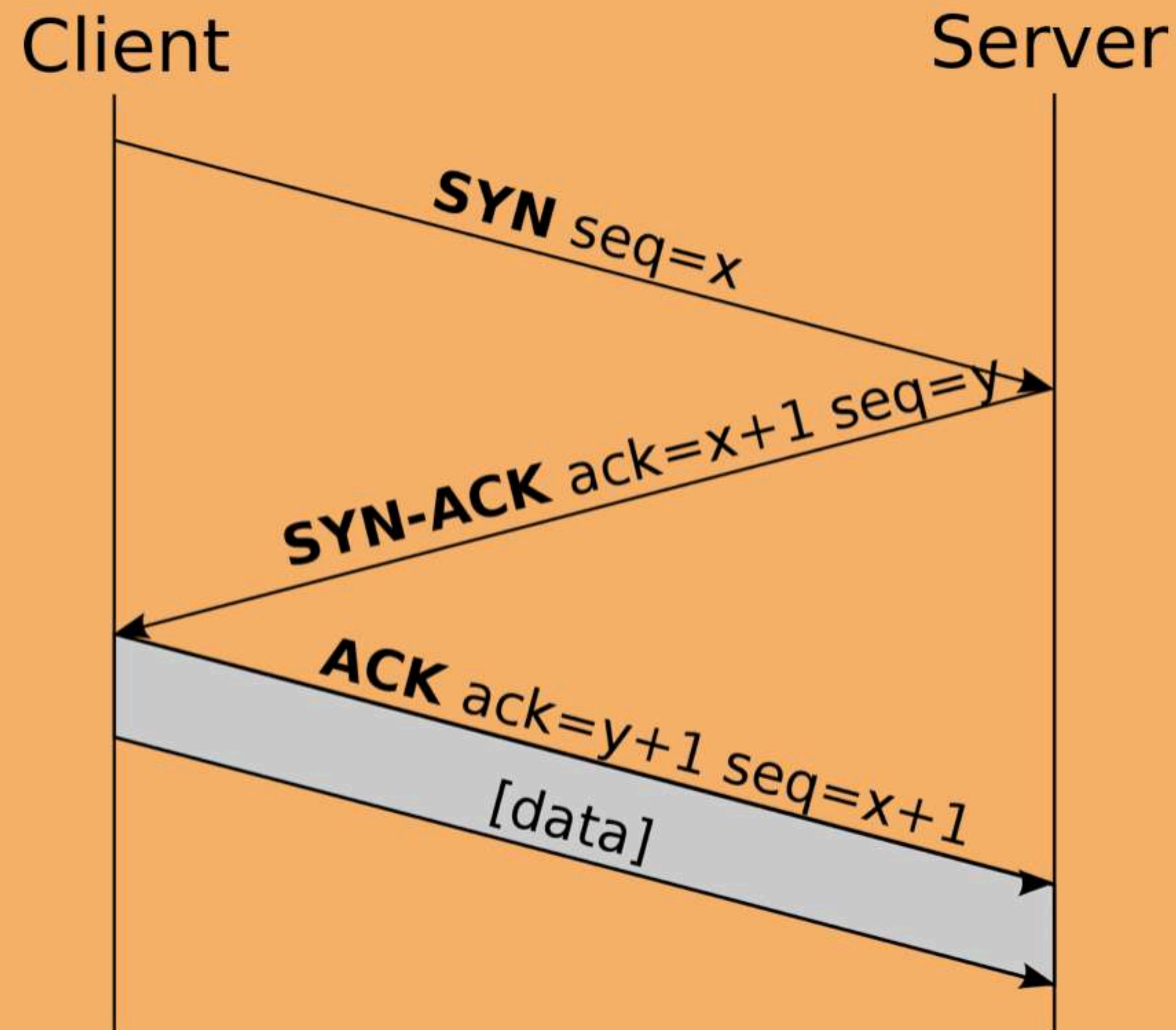


TOTALLY



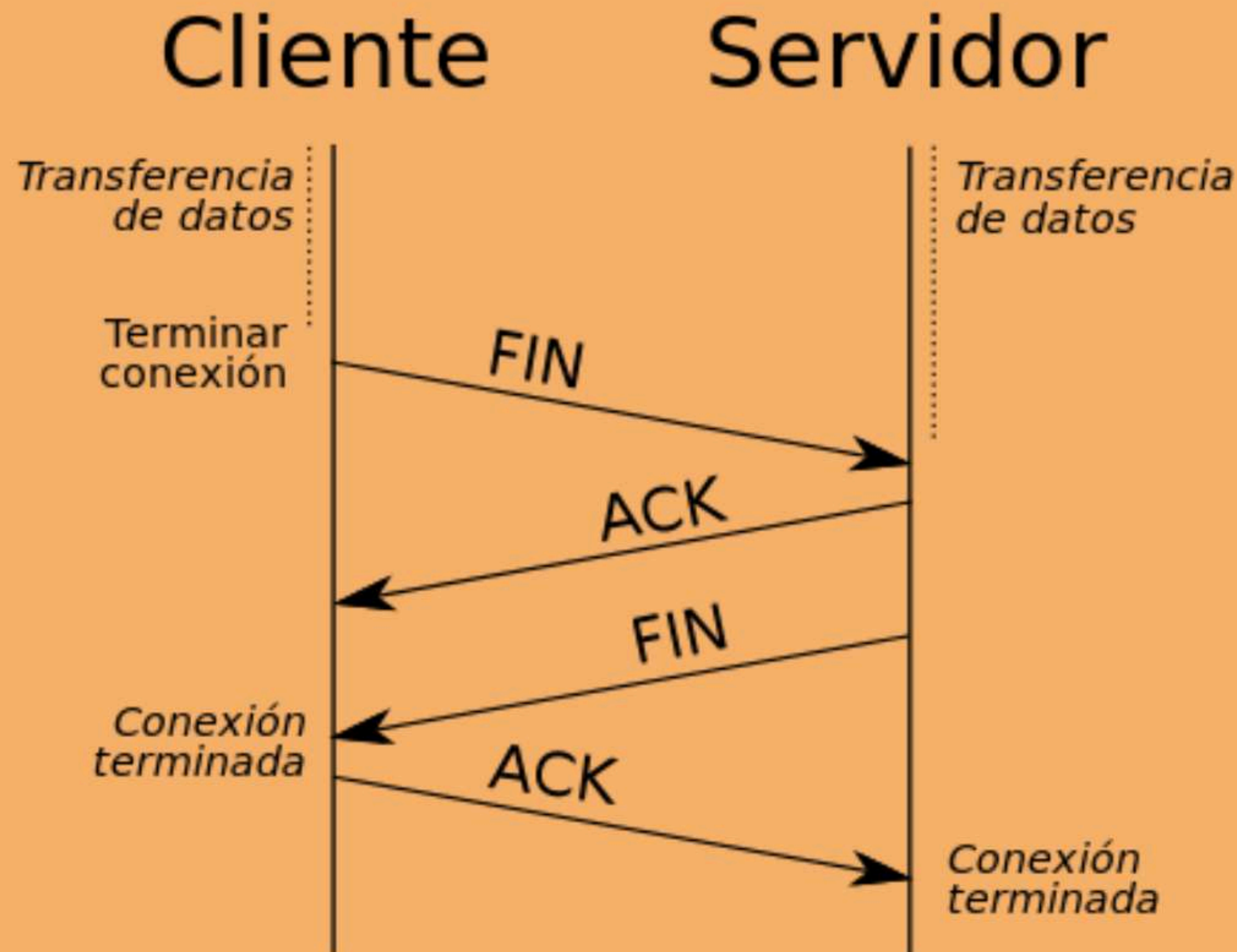
Taller NMap [Protocolo TCP]

Las conexiones TCP se componen de tres etapas:
2. transferencia de datos.



Taller NMap [Protocolo TCP]

Las conexiones TCP se componen de tres etapas:
3. fin de la conexión.



Un puerto suele estar numerado para de esta forma poder identificar la aplicación que lo usa. Decidir a qué programa entregará los datos recibidos. Esta asignación de puertos permite a una máquina establecer simultáneamente diversas conexiones con máquinas distintas, ya que todos los segmentos que se reciben tienen la misma dirección, pero van dirigidos a puertos diferentes.

- **Puertos conocidos 0 - 1023** : Son puertos reservados para el sistema operativo y usados por "protocolos bien conocidos"
- **Puertos Registrados 1024-49151**: Pueden ser usados por cualquier aplicación.
- **Puertos dinámicos/privados 49152 a 65535** : Son denominados dinámicos o privados porque normalmente se asignan de forma dinámica a las aplicaciones de clientes al iniciarse la conexión.

Taller NMap [Protocolo ICMP]

Internet Control Message Protocol es un sub protocolo de control y notificación de errores del Protocolo de Internet (IP)

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta ping y traceroute, que envían mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese host y cantidad de hosts por los que pasa.

Paquete ICMP

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Tipo = 0								Código = 0								Checksum															
Identificador																Número de secuencia															
Datos :::																															

IP: (Internet Protocol) provee un servicio de datagramas no fiable (también llamado del "mejor esfuerzo": lo hará lo mejor posible, pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP

VOY A BUSCAR TODAS



LAS WEBS VULNERABLES



Taller NMap

[NMap y ZenMap]



nmap.org

contacto@rodolfolopez.es

rodolfolopez.es

Nmap es un programa de código abierto que sirve para efectuar análisis de puertos. Fue creado originalmente para Linux aunque actualmente es multiplataforma. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.

Que podemos hacer con NMap

- Descubrimiento de hosts.
- Identifica puertos abiertos y servicios.
- Determinar qué sistema operativo y versión utiliza.
- Obtiene información del hardware y del equipo. MAC, IP, Nombre Equipo, etc...
- Dispone de una colección de SCRIPTS par hacer muchas más cosas:

Algunas categorías de scripts:

- **Auth:** Scripts que gestionan procesos de autenticación.
- **Broadcast:** Orientado a la obtención de información por medio de peticiones Broadcast.
- **Brute:** Scripts destinados a la auditoría de contraseñas por medio de fuerza bruta.
- **Discovery:** Scripts para el descubrimiento de equipos.
- **Dos:** Scripts relacionados con ataques tipo DoS.
- **Exploit:** Scripts que explotan vulnerabilidades conocidas.

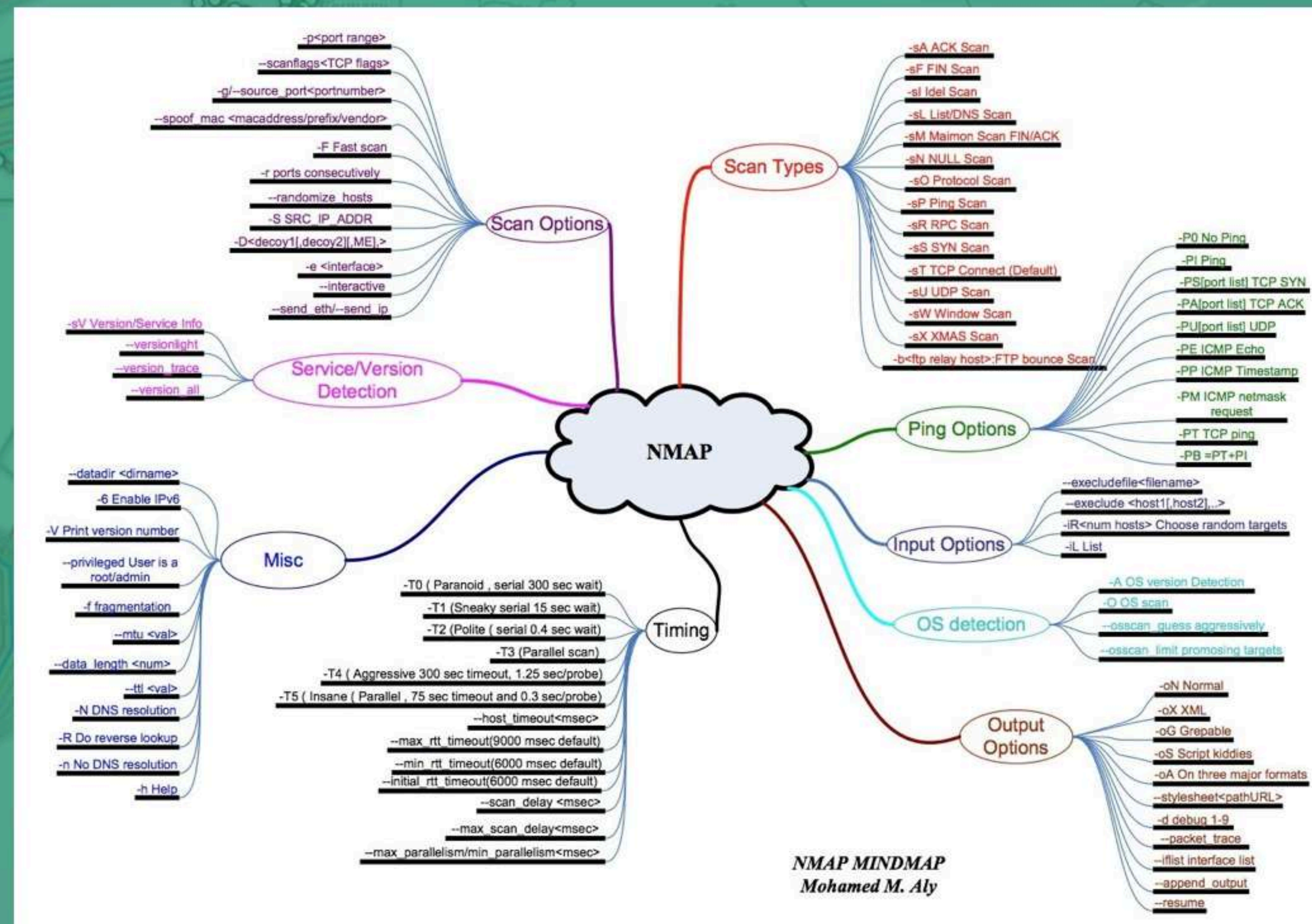
En la actualidad NMap Dispone de 585 Scripts y 132 Librerías

Ver todos los Scripts con su explicación:

<https://nmap.org/nsedoc/>

Taller NMap [Comandos NMap]

Aquí les voy a presentar algunas opciones pero la lista completa la tienen en la documentación y con el comando `man nmap` .
La mayoría de comandos necesitan permisos de administrador del sistema.



Taller NMap [ZenMap]

The image displays two windows from the Zenmap application. The main window, titled 'Zenmap', shows a scan profile named 'Intense Scan' targeting 'scanme.nmap.org'. The command line is set to 'nmap -T Aggressive -A -v scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net'. The 'Hosts' tab is active, showing a list of hosts: scanme.nmap.org, 171.67.22.3, 10.0.0.10, wap.yuma.net, and zardoz.yuma.net. The 'Host Status' section for scanme.nmap.org shows it is 'up' with 3 open ports and 2 closed ports. The 'Addresses' section shows IPv4: 205.217.153.62. The 'Hostnames' section shows 'scanme.nmap.org - PTR'. The 'Operating System' section shows 'Linux 2.6.20-1 (Fedora Core 5)' with 100% accuracy. The 'Profile Editor' window is open, showing the 'Command' tab with the command 'nmap -sF -sV -T Sneaky -6 -O <target>'. The 'Scan options' section shows 'TCP scan' set to 'FIN scan', 'Special scans' set to 'None', and 'Timing' set to 'Sneaky'. The 'Advanced' section shows 'Services version detection' and 'Operating system detection' checked, and 'Maximum Retries' set to 1.

Zenmap Window:

- Menu: Scan, Tools, Profile, Help
- Buttons: New Scan, Command Wizard, Save Scan, Open Scan, Report a bug, Help
- Target: .10 wap.yuma.net zardoz.yuma.net
- Profile: Intense Scan
- Command: nmap -T Aggressive -A -v scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net
- Hosts: scanme.nmap.org, 171.67.22.3, 10.0.0.10, wap.yuma.net, zardoz.yuma.net
- Host Status: up, Open ports: 3, Filtered ports: 0, Closed ports: 2, Scanned ports: 5, Up time: 3916956, Last boot: Sat Oct 27 10:38:07 2007
- Addresses: IPv4: 205.217.153.62, IPv6: , MAC:
- Hostnames: Name - Type: scanme.nmap.org - PTR
- Operating System: Name: Linux 2.6.20-1 (Fedora Core 5), Accuracy: 100%

Profile Editor Window:

- Command: nmap -sF -sV -T Sneaky -6 -O <target>
- Scan options: TCP scan: FIN scan, Special scans: None, Timing: Sneaky
- Advanced: ☐ FTP bounce attack, ☐ Idle Scan (Zombie), ☒ Services version detection, ☒ Operating system detection, ☐ Disable reverse DNS resolution, ☒ IPv6 support, ☐ Maximum Retries: 1

Comandos Iniciales

nmap	ayuda
nmap -h	ayuda breve
man nmap	ayuda completa para salir q

La sintaxis inicial de NMap es

nmap [Tipo(s) de análisis] [Opciones] [Objetivos]

Taller NMap [Usando NMap]

ESPECIFICACIÓN DE OBJETIVO

Para decidir un objetivo a escanear con **NMap** podemos hacerlo de diferentes maneras.

- `nmap scanme.nmap.org` ----> Web
- `nmap 192.168.1.1` ----> ip
- `nmap 192.168.1.1/24` ----> Rango CIDR
- `nmap 192.168.1.1-50` ----> Rango

Otras opciones

`-iL <archivo_entrada>`: Lee una lista de sistemas/redes del archivo.

`nmap -iL ips.txt`

`--exclude <sist1[,sist2][,sist3],...>`: Excluye ciertos sistemas o redes

`nmap --exclude 192.168.1.50 192.168.1.1-254`

Taller NMap [Usando NMap]

DESCUBRIMIENTO DE HOSTS

A través de estas opciones puedes hacer un sondeo de los host que están en tu red , este puede ser un paso previo a los siguientes análisis.

- sL: Sondeo de lista - Simplemente lista los objetivos a analizar haciendo Resolución DNS inversa
- sP: Sondeo Ping - Sólo determina si el objetivo está vivo

Ejemplo:

```
nmap -sP 192.168.1.1
```


TACTICAS DE ANÁLISIS

Puedes especificarle diferentes formas de analizar puertos jugando con los diferentes Flags TCP dependiendo del objetivo y de la información conseguir, del nivel de ruido que quieras generar , etc...

TCP SYN scan es tal vez la técnica de escaneo más básica y utilizada. Consiste en iniciar una sesión TCP, enviando el flag SYN, y examinar la respuesta del servidor (SYN-ACK) pero no terminar de enviar nunca el paquete TCP con el flag ACK. De esta forma la sesión nunca se establece y no queda rastro de nuestra conexión.

-sS/sT/sA/sW/sM: Análisis TCP SYN/Connect()/ACK/Window/Maimon

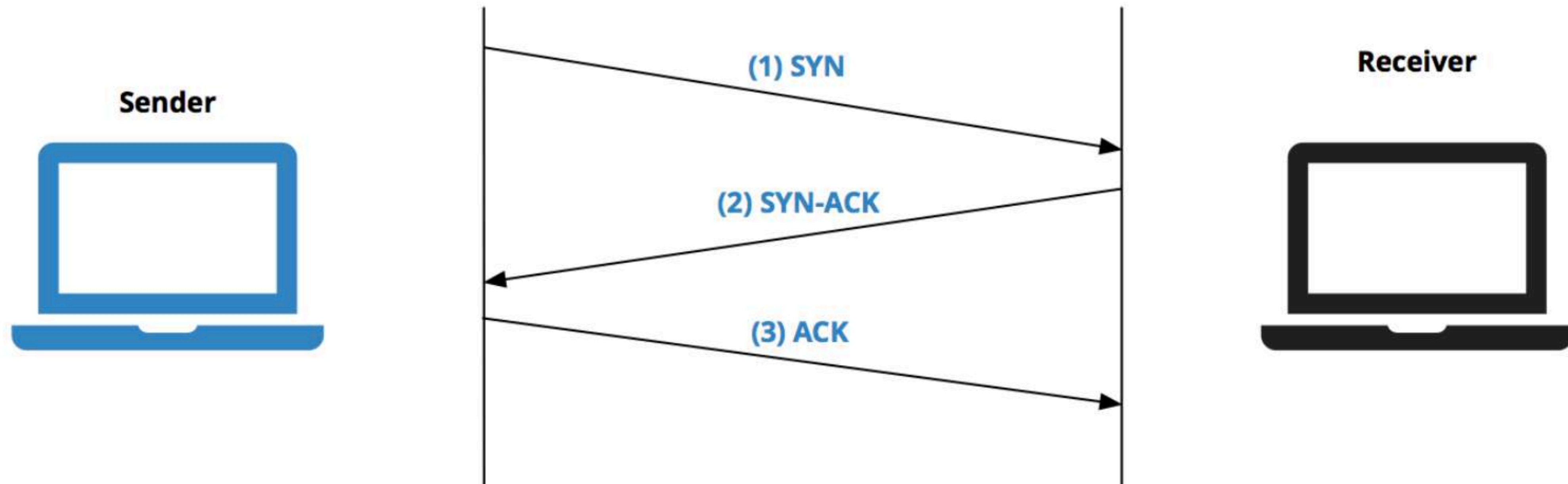
-sN/sF/sX: Análisis TCP Null, FIN, y Xmas

Ejemplo de TCP SYN scan

```
nmap -sS -sV -P0 192.168.1.1
```


Taller NMap

[Usando NMap]



Taller NMap [Usando NMap]

ESPECIFICACION DE PUERTOS Y ORDEN DE ANÁLISIS

A través de estas Opciones puedes decirle a NMap que puerto quieres analizar

Probar un único puerto. Por ejemplo el 443: -p443

Probar un rango de puertos. Por ejemplo desde el 20 hasta el 22 (inclusive): -p20-22

Probar un conjunto de puertos. Por ejemplo 80 y 443 (se separan con coma): -p80,443

Probar todos los puertos. del 0 al 65535: -p1-65535

Otras opciones:

-p: Especifica el puerto a analizar.

-F: Rápido - Analizar sólo los puertos listados en el archivo nmap-services. Los más comunes.

-r: Analizar los puertos secuencialmente, no al azar.

ejemplo:

```
nmap -F 192.168.1.1
```


Taller NMap [Usando NMap]

Estados de los puertos:

Abierto: existe una aplicación en la máquina objetivo que está a la escucha de nuevas conexiones o paquetes TCP o UDP. Muestra un servicio disponible para ser usado en la red.

Cerrado: es un puerto alcanzable, pero no existe una aplicación a la escucha en él.

Filtrado: Nmap no ha recibido respuestas a las sondas enviadas hacia un puerto. Suele significar que una herramienta intermedia (generalmente cortafuegos, sondas IDS/IPS, otros elementos de la red, o cualquier otro tipo de filtro) está bloqueando dicho puerto, respondiendo con poca o ninguna información (en ocasiones con un ICMP de tipo "destino inalcanzable").

No filtrado: Solo aparece tras un análisis de tipo ACK (ver 3.2.5). Es un puerto alcanzable, pero no es posible determinar si está abierto o cerrado.

Estados de los puertos:

Abierto | filtrado: En este caso, NMap no ha sido capaz de determinar si el puerto está abierto o filtrado debido a falta de respuestas, bien porque están siendo eliminadas por algún tipo de filtro de paquetes o Sonda.

Cerrado | filtrado: Solo se obtiene tras un escaneo de tipo Idle. En este caso Nmap no ha sido capaz de determinar si el puerto está cerrado o filtrado.

DETECCION DE SERVICIO/VERSIÓN

A través de estas Opciones, Nmap trata de determinar la aplicación o servicio que está escuchando en cada puerto y su versión.

la carpeta donde se guardan la relación de puertos y servicios conocidos se encuentra en esta ruta:

/usr/local/share/nmap/nmap-services

-sV: Sondear puertos abiertos, para obtener información del servicio/versión

--version-intensity <nivel>: Fijar de 0 (ligero) a 9 (probar todas las sondas)

--version-light: Limitar a las sondas más probables (intensidad 2)

--version-all: Utilizar todas las sondas (intensidad 9)

--version-trace: Presentar actividad detallada del análisis (para depurar)

Ejemplo escaneo de servicios.

```
nmap -sS -sV -P0 192.168.1.1
```


DETECCIÓN DE SISTEMA OPERATIVO

Con las siguientes opciones intenta según las huellas TCP/IP adivinar cuál es el sistema operativo del Host.

Otras Opciones

- O: Activar la detección del sistema operativo (SO)
- osscan-limit: Limitar la detección de SO a objetivos prometedores
- osscan-guess: Adivinar el Sistema Operativo de la forma más agresiva

Ejemplo

```
nmap -sS -O -P0 192.168.1.1
```


Taller NMap [Usando NMap]

TEMPORIZADO Y RENDIMIENTO:

Escaneo paranoico

El modo paranoico es el más sigiloso de todos. Trata de no dejar rastro alguno del escaneo. Es el indicado al momento de escanear una víctima.

Para correr un escaneo "paranoico" utilizar la opción -T0.

Por ejemplo:

```
nmap -sS -T0 -P0 192.168.1.1
```

-T[0-5]: Seleccionar plantilla de temporizado (los números altos son mas rápidos)

- * **0: paranoid**
- * **1: sneaky**
- * **2: polite**
- * **3: normal (Por defecto)**
- * **4: aggressive**
- * **5: insane**

El escaneo "insano" (-T5) es el más agresivo de todos y asume que se dispone de una red ultra rápida, o se desea sacrificar algo de precisión a cambio de velocidad. Por otro lado sería ético sólo utilizarlo contra nuestros propios servidores (para no saturar redes, interfaces ni hosts ajenos)

EVASION Y FALSIFICACION PARA CORTAFUEGOS/IDS

Para Evadir los sistemas de control de red podemos usar algunos parámetros, los más usados son la fragmentación , el análisis con señuelos haciéndonos pasar por otro equipo o el MAC Spoofing ocultando nuestra mac Original.

Otras opciones

- f : fragmentar paquetes
- D: d1,d2 encubrir análisis con señuelos
- S: ip falsear dirección origen
- g: source falsear puerto origen
- randomize-hosts: orden de equipos a analizar
- spoof-mac mac: cambiar MAC de origen

Ejemplo

```
nmap -f 192.168.1.1
```


SALIDA

Para poder analizar todos estos datos, hacer informes podemos guardar la salida de todos los datos que nos proporciona NMap a un archivo en el formato deseado

Opciones

-oN/-oX/-oS/-oG <file>: Guardar el sondeo en formato normal, XML, s| <rlpt kllddi3 (n3n3b4n4n4), y Grepeable (para usar con grep), respectivamente, al archivo indicado.

Ejemplo:

```
nmap -sX -A 192.168.1.1-255 -oN scanresult.txt
```


MISCELANEA

Otras opciones de forma complementaria con los escaneos

Opciones

-6: Habilitar análisis IPv6

-A: Habilita la detección de SO y de versión

Ejemplo:

```
nmap -sS -A 192.168.1.1
```


Nmap Scan Types

Scan Type	Description
TCP SYN	Send a SYN packet to each port and wait for an ACK
TCP connect	Open a connection to each port.
FIN	Send a FIN packet and wait for a RST, which means the port is closed.
XMAS	Send a packet with the FIN, URG, and PUSH flags set and wait for a RST, which means the port is closed
NULL	Send a packet with the FIN, URG, and PUSH flags set to zero and wait for a RST, which means the port is closed.
UDP	Send a 0 byte UDP packet to each port and wait for an ICMP port unreachable message.
IP Protocol	Send a raw IP protocol header packet without any protocol headers and wait for an ICMP protocol unavailable message.
Idle scan	Uses a side channel to send a TCP port scan. (I.E. Broadcast node)
ACK Scan	Send an ACK packet to the port and wait for and RST packet.
RPC scan	Floods all open TCP and UDP ports with null RPC packets to determine if it is an RPC port.

Taller NMap [Usando NMap]

Scan Type	Syntax	Example
TCP SYN Scan	-sS	nmap -sS 10.20.3.100
TCP Connect Scan	-sT	nmap -sT 10.20.3.100
Fin Scan	-sF	nmap -sF 10.20.3.100
XMAS Scan	-sX	nmap -sX 10.20.3.100
Null Scan	-sN	nmap -sN 10.20.3.100
Ping Scan	-sP	nmap -sP 10.20.3.100
Version Detection	-sV	nmap -sV 10.20.3.100
UDP Scan	-sU	nmap -sU 10.20.3.100
IP Protocol Scan	-sO	nmap -sO 10.20.3.100
ACK Scan	-sA	nmap -sA 10.20.3.100
Windows Scan	-sW	nmap -sW 10.20.3.100
List Scan	-sL	nmap -sL 10.20.3.100

Otras herramientas Interesantes para usar junto a NMap

- **Nsearch** : Buscador de scripts NMap
- **hping3** : Conjunto de Utilidades para enviar paquetes tcp entre otras opciones
- **TcpDump** : Ayuda a ver tráfico TCP Sniffer
- **Wireshark** : Analizador de tráfico

Taller NMap

[Usando NMap]

Gracias a todos por
asistir y los esperamos
en otra ocasión en la
Comunidad de
HACKMADRID%27

contacto@rodolfolopez.es

rodolfolopez.es

Taller NMap



Rodolfo Miguel López
rodolfolopez.es
CronSec.com

contacto@rodolfolopez.es

rodolfolopez.es