Seguridad Informática

Tema 4 – Ataques a redes IP y protocolos

Bloque II – Ataques y contramedidas

Universidad Rey Juan Carlos

Antonio González Pardo **antonio.gpardo@urjc.es**

14/02/2023

Índice

- Introducción y recordatorios.
- ARP Poisoning, ARP Spoofing y Man in the Middle.
- TCP Hijacking.
- Ataques en la capa de aplicación.
- Ataques Denial of Service (DoS).

Índice

- **Introducción y recordatorios.**
- ARP Poisoning, ARP Spoofing y Man in the Middle.
- TCP Hijacking.
- Ataques en la capa de aplicación.
- Ataques Denial of Service (DoS).

Introducción y recordatorios

Universidad Rey Juan Carlos

- Nos centraremos en ataques a diferentes protocolos de redes TCP/IP.
- Existen otros tipos de ataques/contramedidas relacionados con el *perímetro* de la red (firewalls, DMZ, …).
- Antes de comenzar es recomendable repasar algunos elementos esenciales de redes.

Introducción y recordatorios

Universidad Rey Juan Carlos

- Una familia de protocolos de Internet es el conjunto de protocolos que son implementados por la pila de protocolos sobre los que se fundamenta Internet, y que permiten la transmisión de datos entre las redes de ordenadores.

- Hay dos protocolos importantes: TCP e IP.

- TCP/IP es el modelo que sostiene Internet y que permite la comunicación entre equipos independientemente del sistema operativo o de las redes en las que están los equipos.

Introducción y recordatorios

- Además del modelo TCP/IP existe el modelo OSI.
- Es el modelo para la Interconexión de Sistemas Abiertos (*Open System Interconection*)
- Contiene 7 capas, y cada una cumple funciones específicas necesarias para comunicar dos sistemas.
- Cada capa se apoya en la capa anterior, realiza su función y ofrece un servicio a la capa superior.

Introducción y recordatorios

- Aplicación: proporciona servicios utilizados por las aplicaciones.
- Presentación: define el formato de los datos que se van a intercambiar entre las aplicaciones.
- Sesión: proporciona mecanismos para controlar el diálogo entre las aplicaciones.
- Transporte: permite intercambiar datos entre sistemas dividiendo en mensaje en varios fragmentos.
- Red: se encarga de definir el camino que seguirán los datos.
- Enlace de datos: se ocupa del direccionamiento físico dentro de la topología de la red.
- Física: controla las señales por donde viajarán los datos.

Introducción y recordatorios

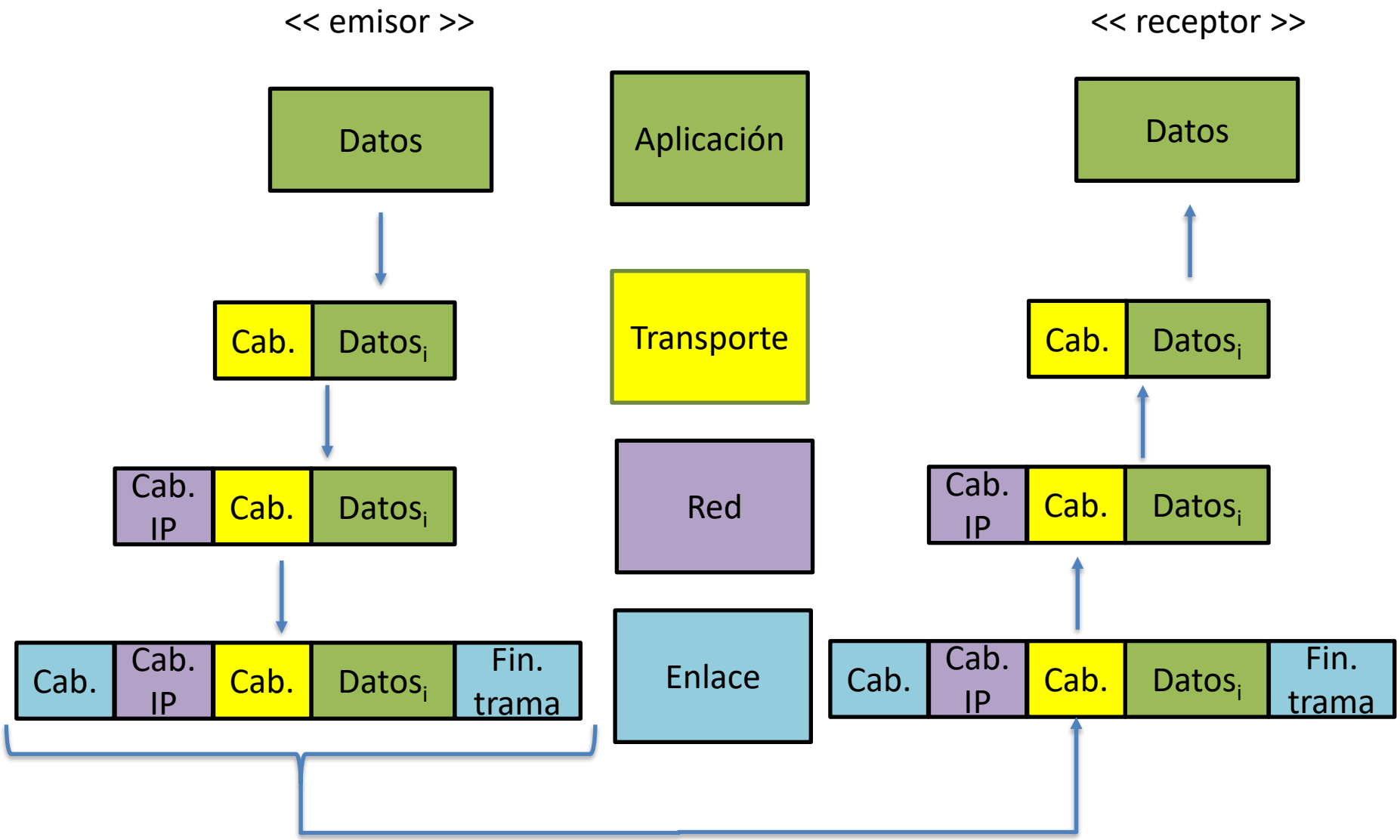
- Aplicación: maneja protocolos de alto nivel que permiten la representación de los datos, codificación y control del diálogo.
- Transporte: se establece la conexión lógica entre el host transmisor y el receptor. Estos protocolos segmentan los datos en el origen para que las capas inferiores realicen el envío.
- Nivel de Red: seleccionar la mejor ruta para transmitir los paquetes por la red.
- Nivel de Enlace de Datos: realiza el direccionamiento físico de los paquetes.
- Acceso a la red: se controla el enlace físico con los medios de la red.

Introducción y recordatorios

Universidad Rey Juan Carlos

Introducción y recordatorios

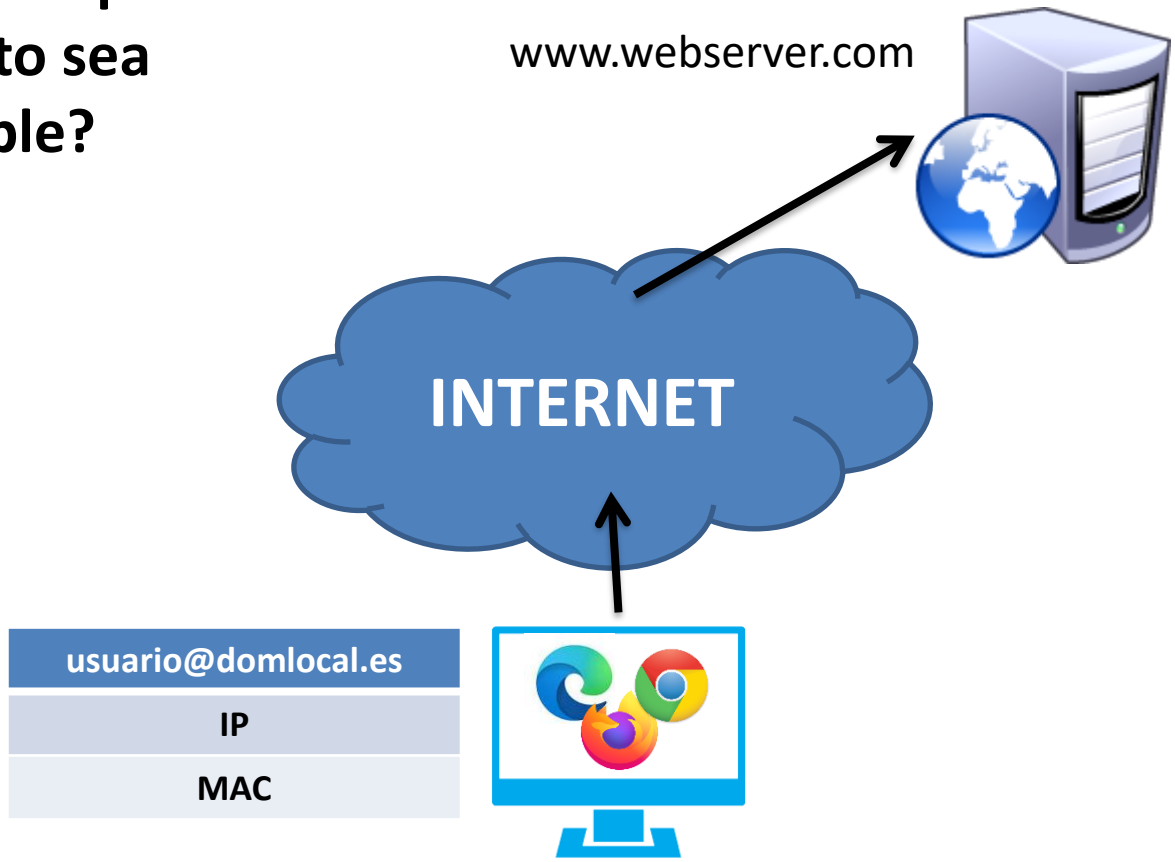
Universidad Rey Juan Carlos



Introducción y recordatorios

Universidad Rey Juan Carlos

¿Qué ocurre para que esto sea posible?



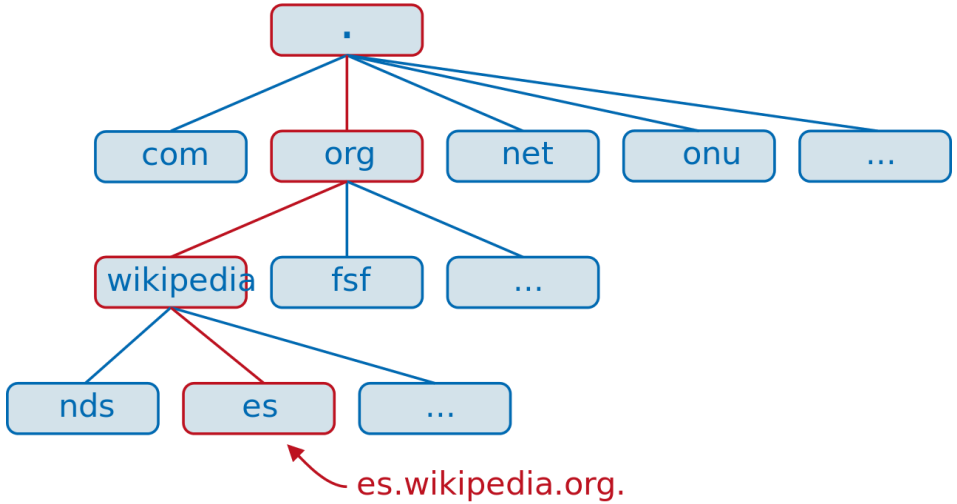
Introducción y recordatorios

Universidad Rey Juan Carlos

- La realidad es que existen cuatro protocolos diferentes que se necesitan ejecutar:
  - DNS: Domain Name System
  - ARP: Address Resolution Protocol
  - TCP/IP: Protocolo de Control de Transmisión / Protocolo de Internet
  - ICMP: Internet Control Message Protocol

DNS (Domain Name System)

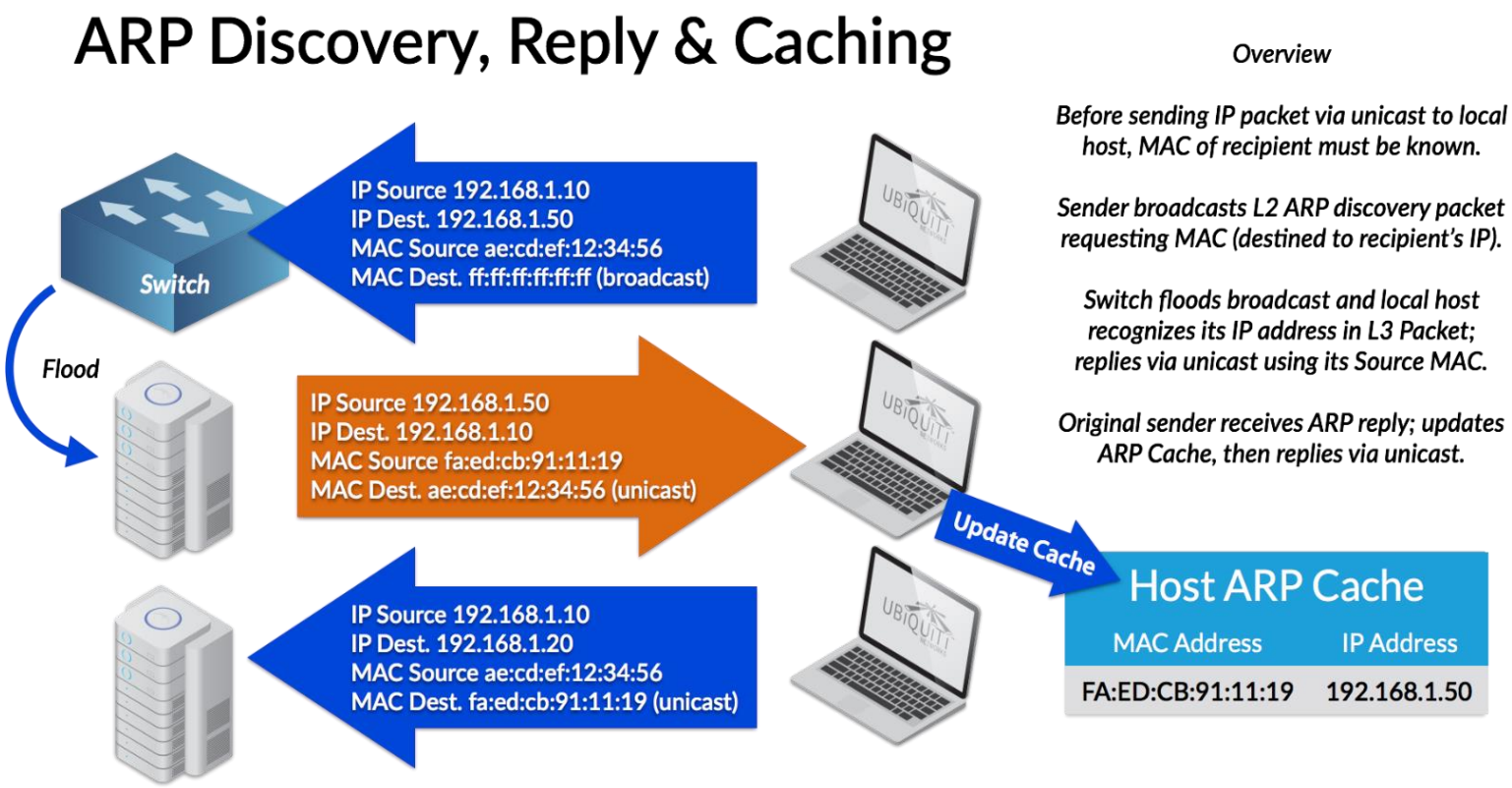
- Se encarga de “traducir” el nombre de un dominio a una dirección IP.
- Funcionamiento:
  - El cliente envía una petición DNS a su servidor DNS.
  - Si el servidor tiene la respuesta manda la contestación. Si no la tienen, pueden reenviar la petición a otro servidor.



ARP (Address Resolution Protocol)

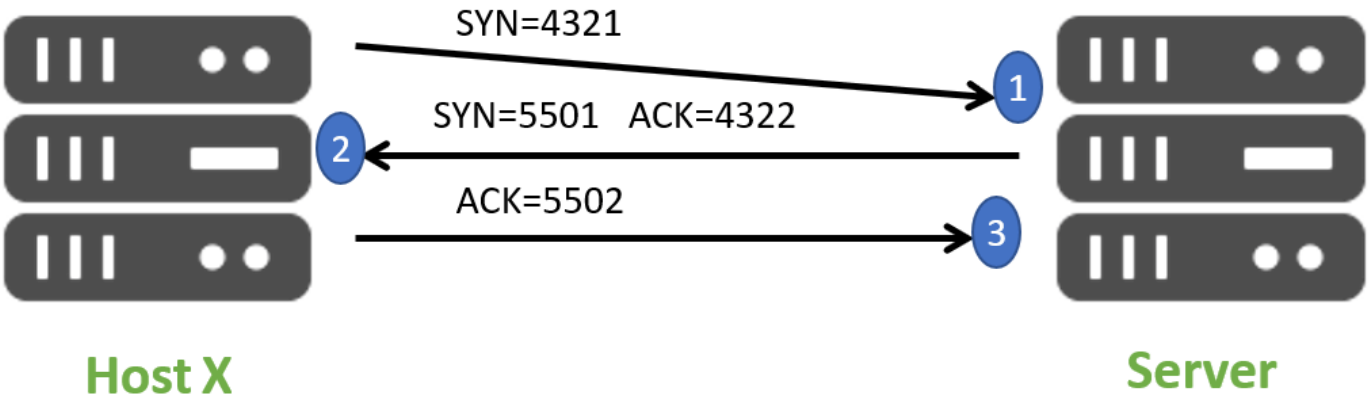
- Protocolo de comunicación usado para encontrar la dirección de hardware (MAC) que se corresponde con una determinada dirección IP.
- Funcionamiento:
  - Se envía un ARP Request a la dirección de broadcast, con la IP que queremos consultar.
  - La máquina espera que le llegue ARP Reply con la dirección que le corresponde.
  - Finalmente se actualiza la caché ARP.

Universidad Rey Juan Carlos



Protocolo TCP/IP

- Tiene el sistema three-way handshake usado para establecer la conexión entre el cliente y el servidor.
- Sirve para sincronizar y asegurarnos la recepción de paquetes.

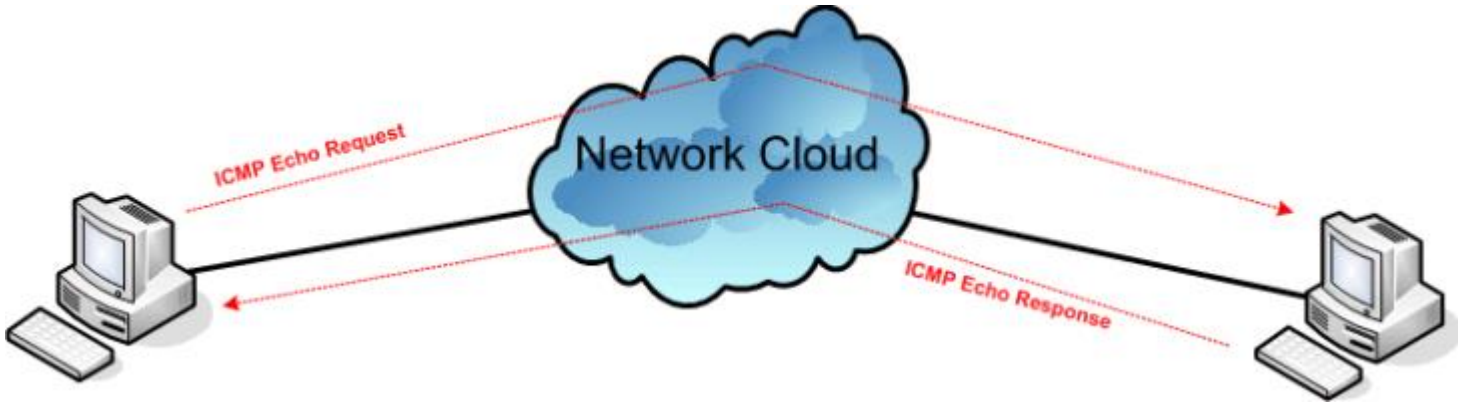


ICMP (Internet Control Message Protocol)

- Protocolo usado para enviar mensajes de error e información operativa:
  - Un host no puede ser localizado
  - Un servicio no está disponible
  - El tiempo de vida de un paquete ha expirado
- Tipos de mensaje:
  - Echo Reply
  - Destination Unreachable
  - Echo Request
  - Redirect
  - Time exceeded
  - ….

Introducción y recordatorios

- Protocolo ICMP



Sniffing

Universidad Rey Juan Carlos

- La mayor parte de los ataques que se pueden realizar, tienen como base la misma técnica → *sniffing.*
- *Sniffing* consiste supervisar los diferentes paquetes que circulan por una red en tiempo real.
- Se recogen tanto los datos de entrada como de salida.
- No es un ataque.
- Sólo es necesario usar un *sniffer* que active el modo promiscuo de la tarjeta de red: por ejemplo Wireshark.

Sniffing

Universidad Rey Juan Carlos

- En un principio, un *sniffer* no es maligno.
- Es algo muy utilizado por los administradores de sistemas para monitorización de la red.
- Permiten diagnosticar problemas y evaluar el rendimiento.
- Se puede usar para intentar identificar el consumo del ancho de banda.

Sniffing

Universidad Rey Juan Carlos

- Usos legítimos:
  - **Ingenieros de red**: pueden usar los sniffers para optimizar la estructura de la red y mejorar la eficiencia y/o velocidad.
  - **Administradores del sistema**: se pueden llegar a identificar cuellos de botella.
  - **Empresas**: permite conocer qué sitios visitan los empleados, o si están descargando algo que no deben.
  - **Profesionales de la seguridad**: para ellos es fundamental identificar tráfico inusual.
- Usos delictivos:
  - Acceso a las credenciales de inicio de sesión, datos bancarios, …

Índice

- Introducción y recordatorios.
- **ARP Poisoning, ARP Spoofing y Man in the Middle.**
- TCP Hijacking.
- Ataques en la capa de aplicación.
- Ataques Denial of Service (DoS).

ARP Poisoning, ARP Spoofing y MitM

- La pila de protocolos TCP/IP se basa en:
  - Identificadores: los campos de las cabeceras que se añaden en cada capa.
  - Protocolos, que permiten:
    - traducir estos identificadores
    - de manera transparente a los usuarios y aplicaciones.

Nombre de dominio → Dirección IP → Dirección MAC.

- Para simplificar el uso, se diseñaron protocolos dinámicos.

- Las técnicas de poisoning se basan en utilizar estos protocolos **dinámicos** de manera que el atacante "envenena" la traducción empleada por la víctima introduciendo información falsa.

ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

- Caso práctico:

SOROA Catalina Nilda Ascasubi 4637 2309 7256
" Diaz Alberto
AVelazquez PquePosadas 3956 2336 4435
" Manuel Ruperto Ascasubi 4637 2304 1760
SOROCHIELLO Valles Eduardo
Gambetta 1169a 2355 1169
SOROKINS Pancirer Adriana Nurit
EAcevedo 1494 2400 1073
" Pancirer Jorge Daniel
PantaleonSotelo 3960 2336 5032
Sorondo Alberto Av18deJulio 1263 2901 2459
2902 3342
SORONDO Amaro Marcelo Sebastian
FJMuñoz 3235bis 2628 9099
" Angel M AvJBelloni 5850 2222 4676
Sorondo Bordigoni Alberto Luis
Av18deJulio 1263 2902 6095
SORONDO Bordigoni Maria de Rosario
Sonia AvELopez 4889 2613 5836
" Fernando LaCumparsita 1339 2908 1188
" Garcia Celestina BrJBatlleyO 3900 2215 2411
" Gutierrez Miguel Angel
Durazno 1967 2410 8566
" Imperial Maria Laura
CerroLargo 1521 2402 5800
" Lanusse Miguel Alejandro
Defensa 1968 2408 1843
" Lastra Isabel Mini 809 2901 7110
" Naguila Teresa Av18deJulio 878 2903 2437
SORONDO Noya Andres Ignacio
Caigua 1346 2203 5457
" Perez Noelia Fernanda
Colonia 2119 2402 2269
" Peyre Ana Maria Andes 1417 2908 4927
" Rebollo Gabriela Porongos 2860 2200 4873
" Rosa Marina Duarte de
Orinoco 5159 2619 1743
SOROZABAL Charle Martha
Ceres 4178 2222 8201
" Mena Dorbal Jose Dunant 4303 2215 3145
" Silvera Evaristo Esp
CnelJArenas 926 2357 9235
SORRENTI Belgica Mensez de
DrBKoch 4086 2203 9682 2216 1554

SOSA Aceved
MMenendezyF
" Acosta Alb
GralTAparicio
" Acosta Carl
PCosio 2150
SOSA Acosta
AvDFCrespo
SOSA Acosta
HFGomez 44
" Acosta Gra
" Acosta Kar
GralTAparicio
" Acosta Ma
VMacKenna
" Acosta Ro
" Acosta Wa
MDelRRamo
" Acuña Jos
" Acuña Luc
Marsella 27
SOSA Acuña
" Acuña Ma
NNPiaggio
" Acuña Ma
" Acuña Na
PsjeMangar
" Adelina N
" Adolfo PF
" Adriana B
Proyect17M
" Aghazaria
VVeneto 10
" Aguilar Da
Tacuabe 45
" Aguilar Ga
" Aguilar Ro
CnoChacarita
" Aguilera Fe
PdreJBonmesa
" Aguirre Gre
" Aguirre Mar
" Aguirre Rosa
CnoLaPaloma 1
SOSA Aguirreg
GralHornos 551
Esther

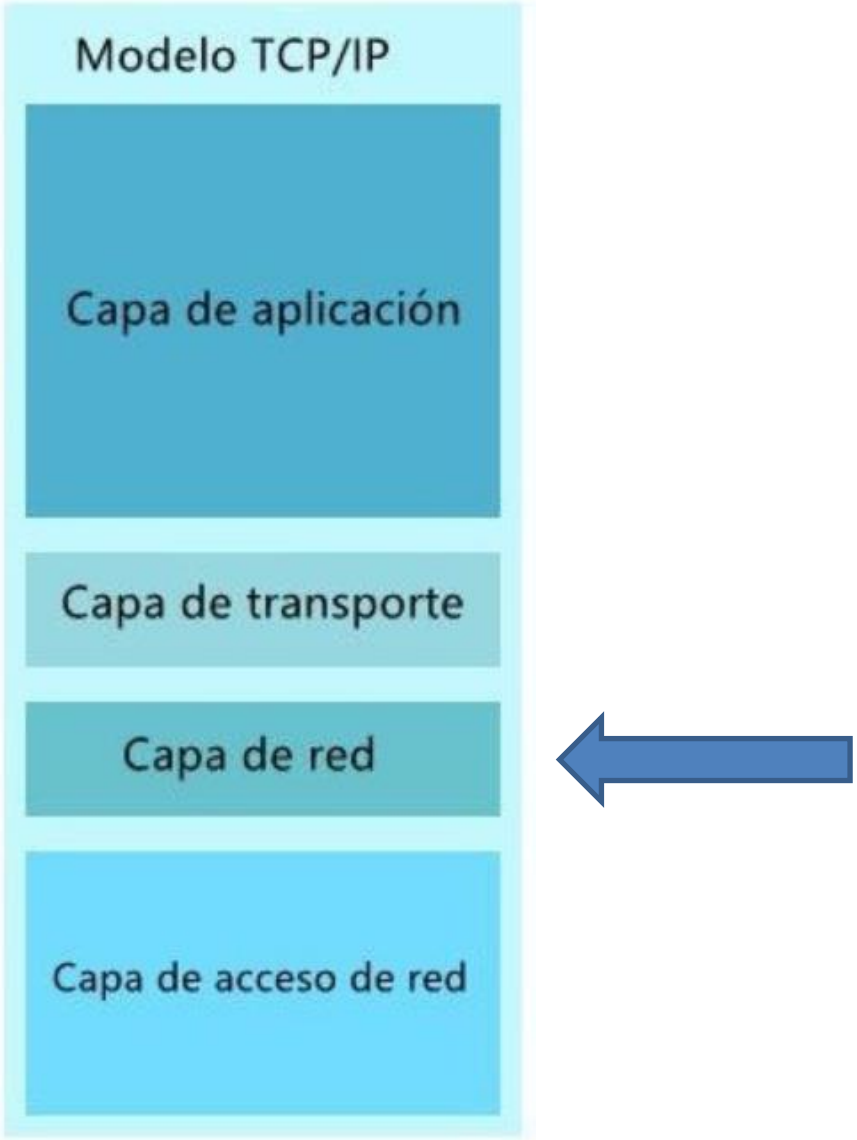
- ¿Qué haríamos si queremos conocer un teléfono que no está en la guía?
  - Preguntar.

ARP Poisoning, ARP Spoofing y MitM

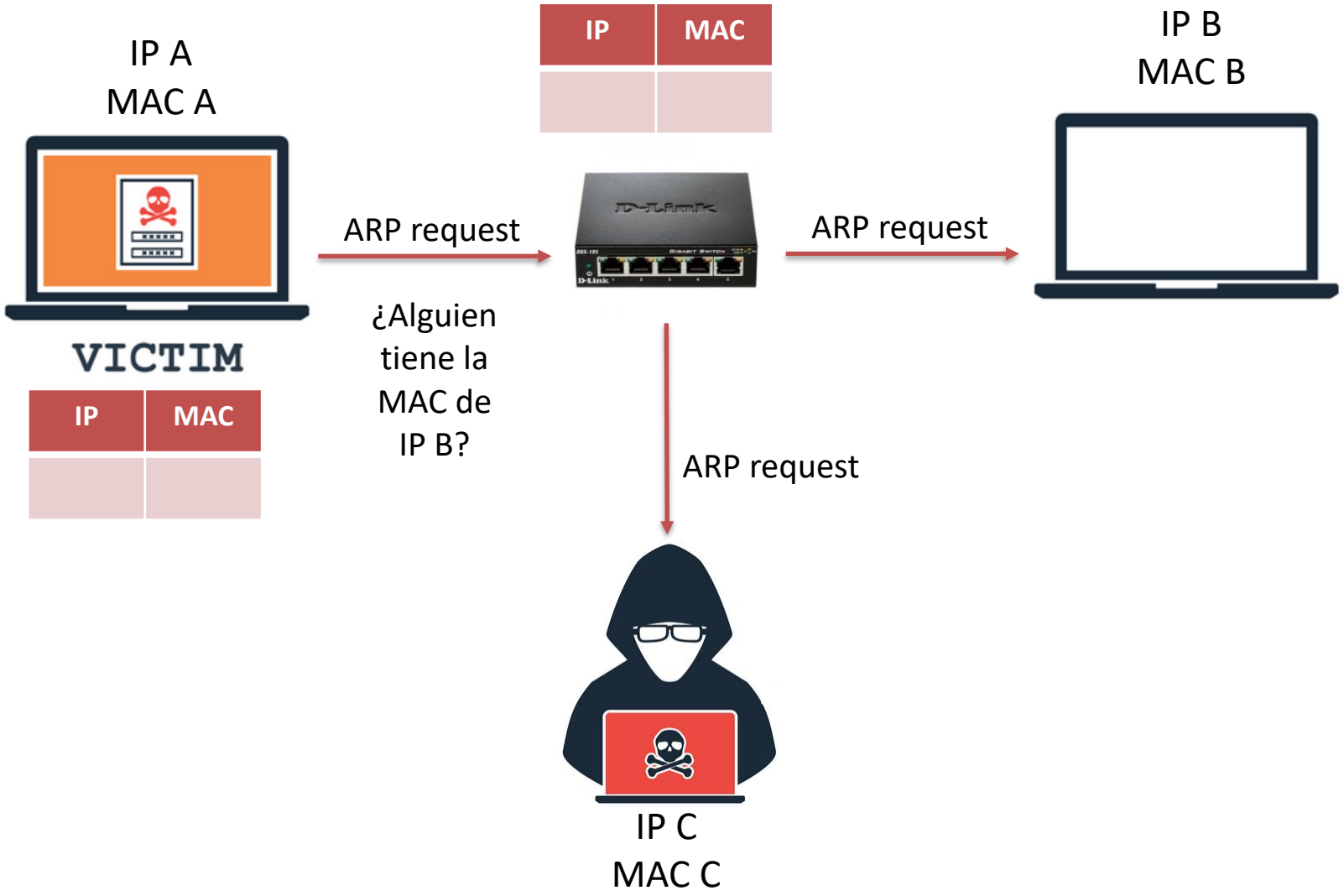
- Esto es lo que hace el protocolo ARP pero en lugar de traducir Nombre ↔ Teléfono, traduce: IP ↔ MAC.
  - Este protocolo se definió para entornos 100% confiables, por lo que no se "sospecha" de ninguna respuesta de tipo ARP Reply.
  - Las definiciones de la funcionalidad del protocolo establecían que cualquiera que tuviera la respuesta podría ofrecerla, y por tanto el solicitante debería aceptarla.
- Enviando tramas ARP Reply falsas, el atacante consigue envenenar las cachés ARP de sus víctimas.
  - Como se trata de un protocolo dinámico, estas tramas se tendrán que enviar periódicamente para mantener el engaño.

ARP Poisoning, ARP Spoofing y MitM

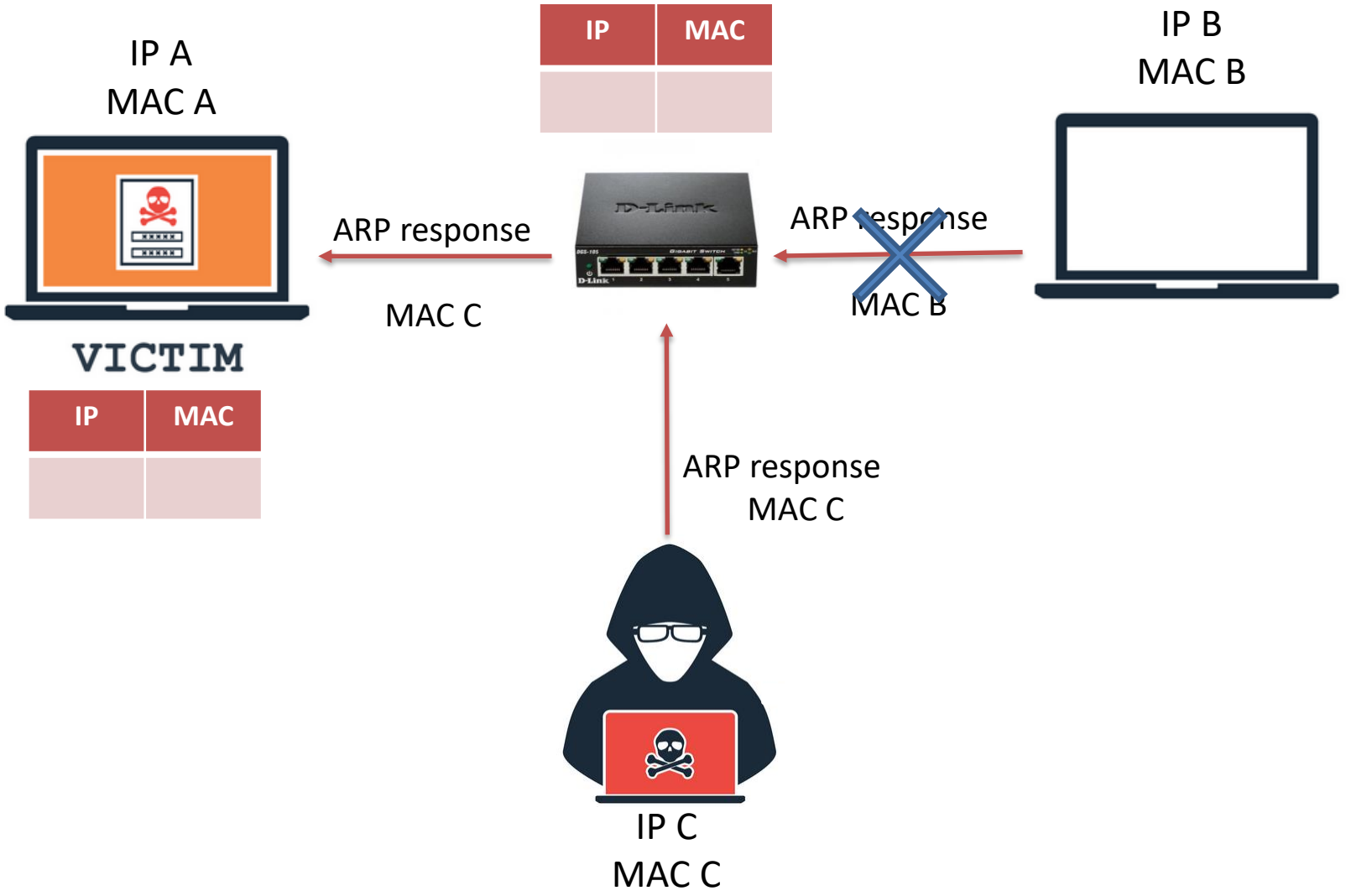
Universidad Rey Juan Carlos



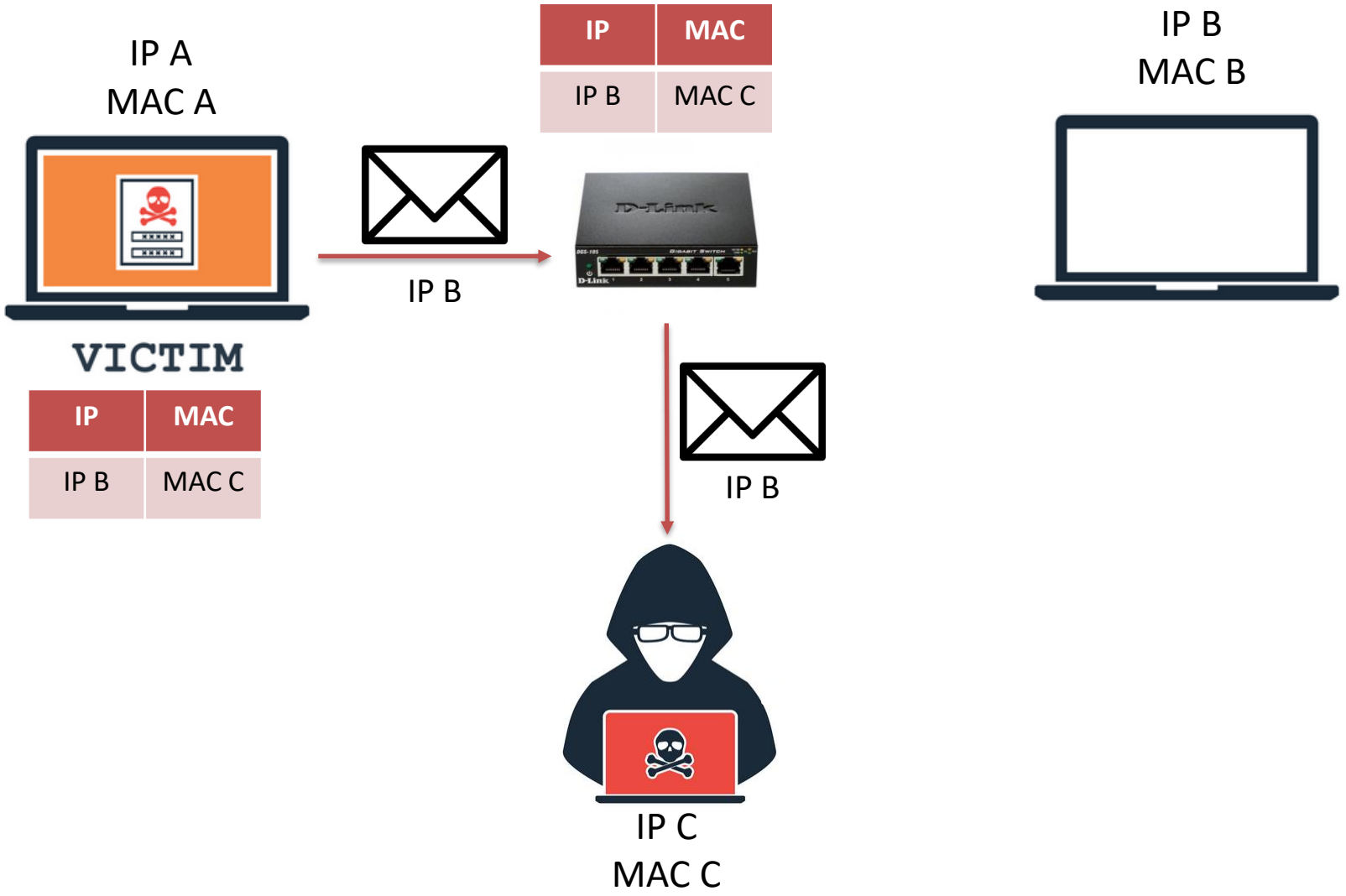
Ejemplo Ataque #1



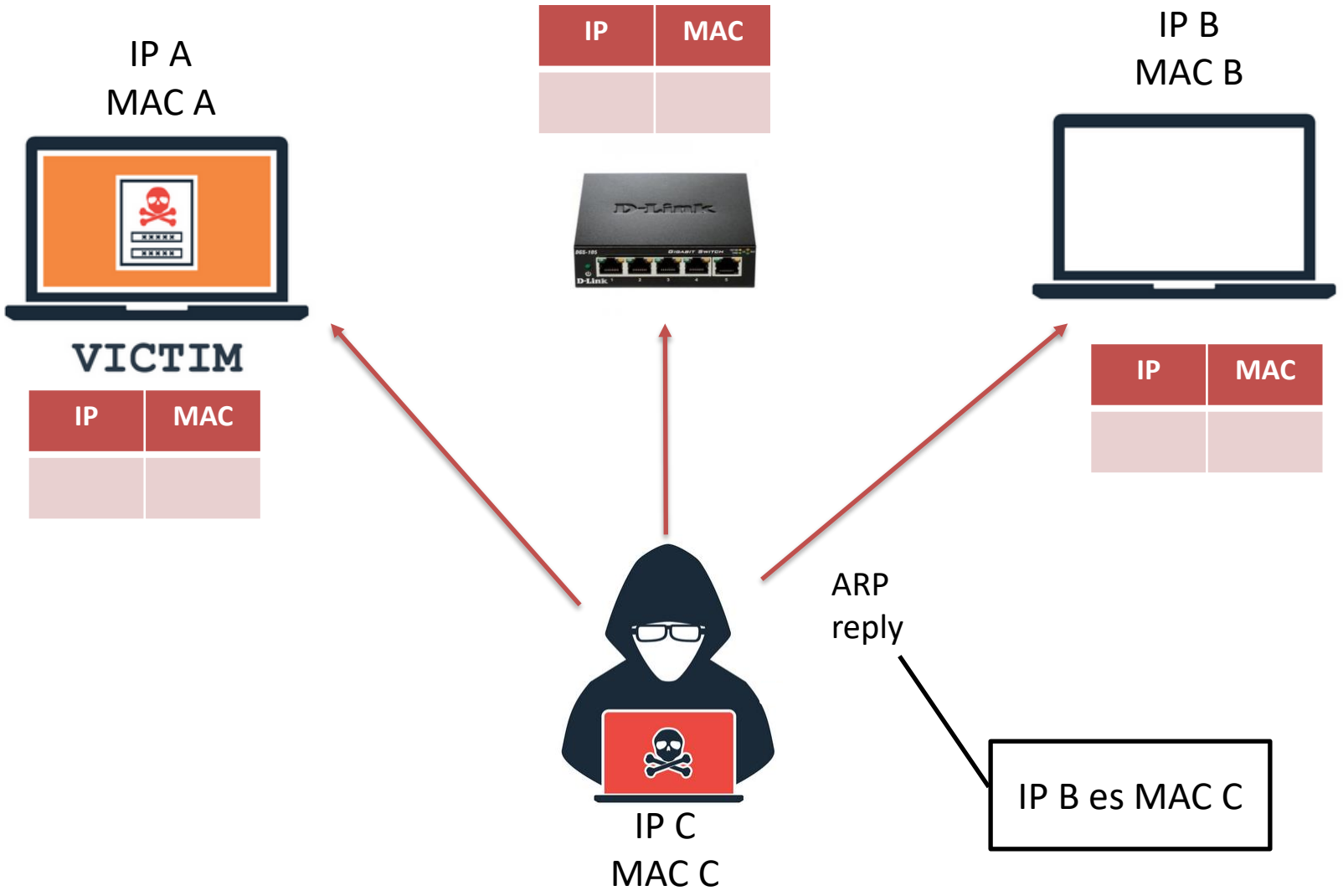
Ejemplo Ataque #1



Ejemplo Ataque #1



Ejemplo Ataque #2



Ejemplo Ataque #2

IP A
MAC A

VICTIM

IP	MAC
IP B	MAC C

IP	MAC
IP B	MAC C

IP B
MAC B

IP	MAC
IP B	MAC C

IP C
MAC C

ARP Poisoning, ARP Spoofing y MitM

- El ataque #1 es más difícil de detectar en la red, pero por el contrario el impacto es mucho menor.

- El ataque #2 tiene la ventaja de que afecta a un mayor número de víctimas, el problema es que genera una gran cantidad de tráfico en la red y es más fácil de detectar.

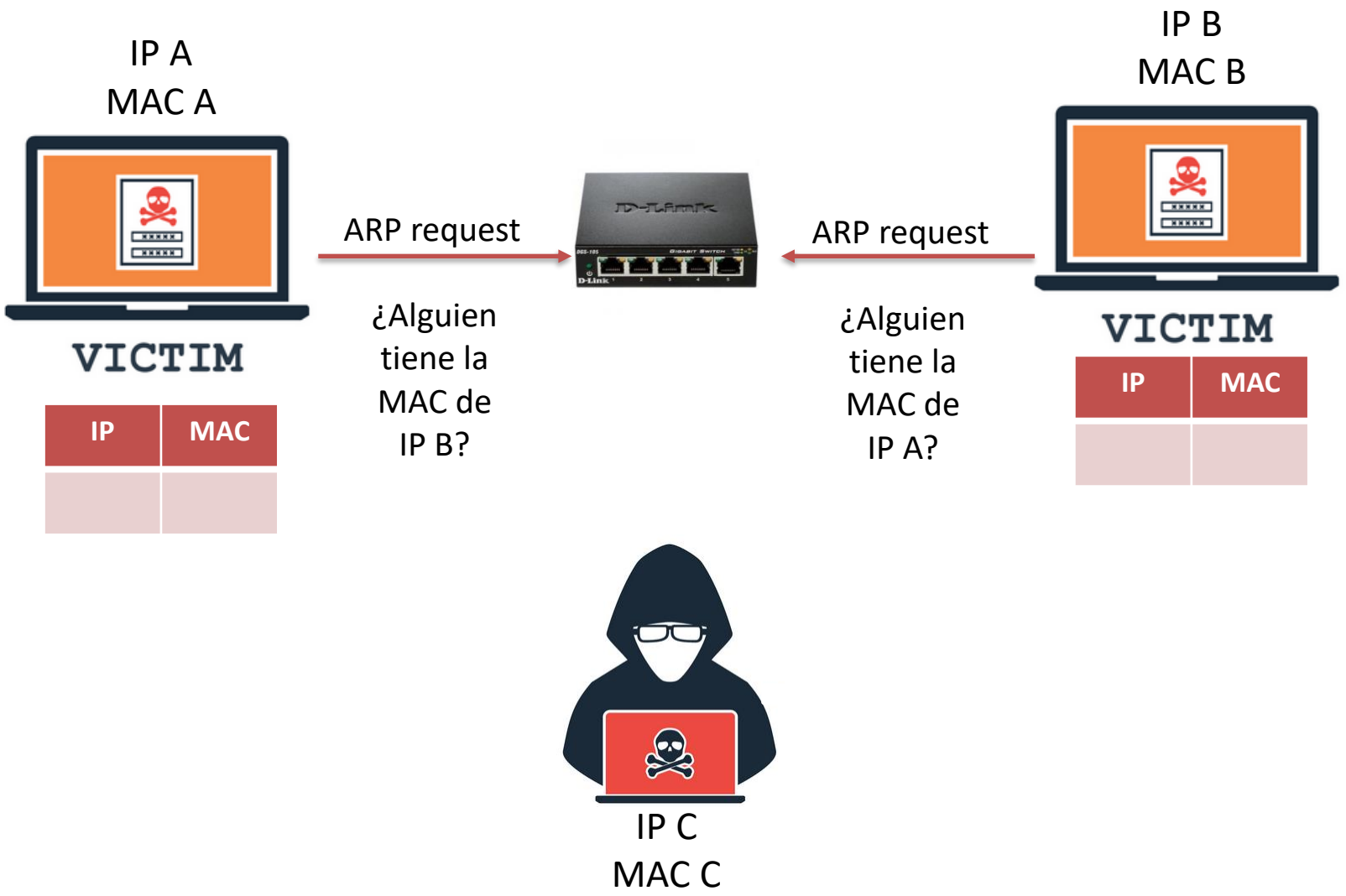
ARP Poisoning, ARP Spoofing y MitM

- Una vez que se tienen las tablas ARP envenenadas, ¿qué más podemos hacer?
  - Ataques de Man-in-the-Middle (*MiTM attacks*)
    - Es el ataque más común. El atacante asocia su MAC con la puerta de enlace de la víctima.
  - Ataques de Denegación de Servicio (*DoS attacks*)
    - Se podría realizar este ataque para que muchos dispositivos asocien la MAC de la víctima con la MAC de la puerta de enlace.
  - Secuestros de sesión (*Session Hijacking*)
    - Es parecido al MiTM pero aquí el atacante busca el número de secuencia TCP o la cookie de una web, para suplantar la identidad de la víctima.

ARP Poisoning, ARP Spoofing y MitM

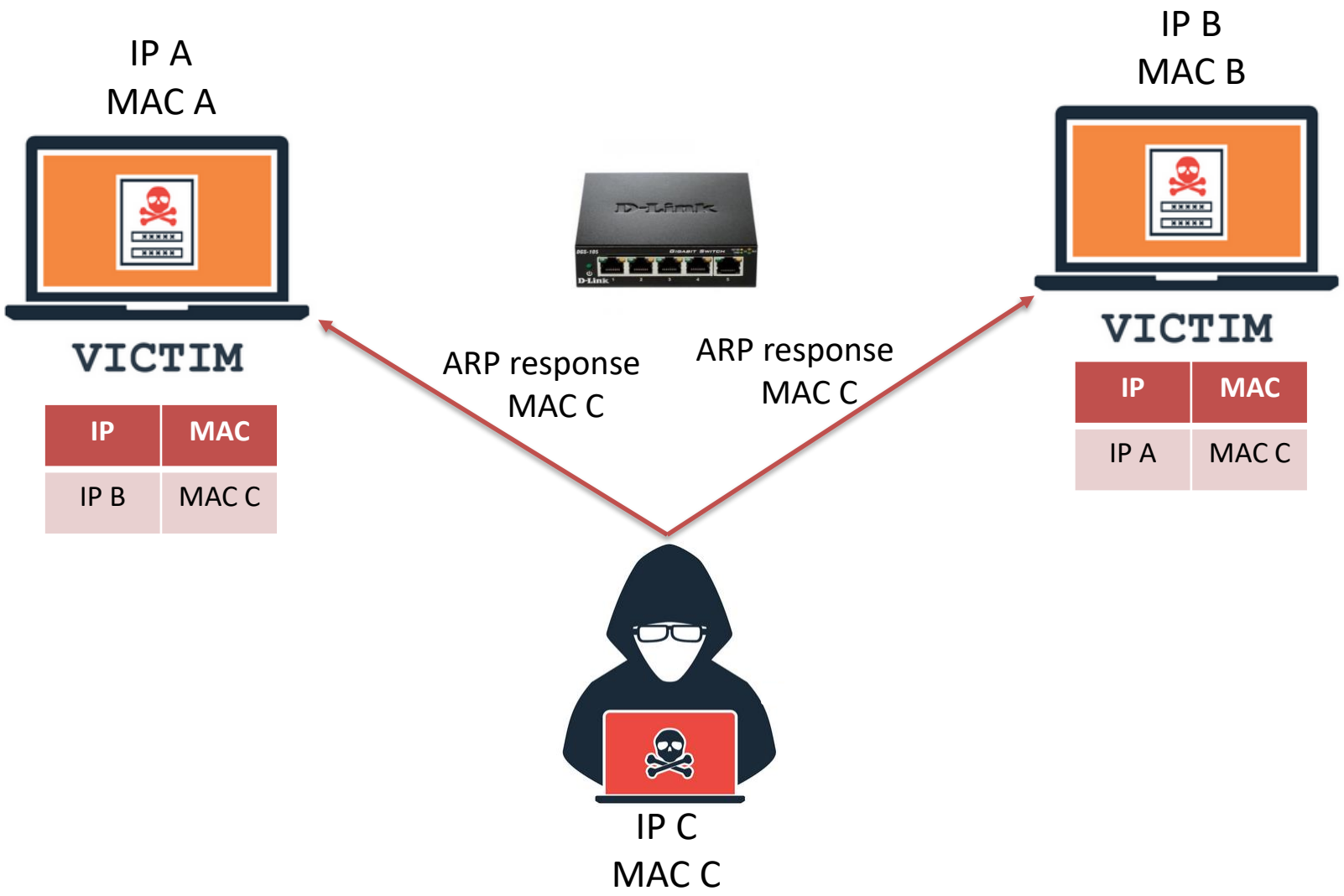
- El envenenamiento de la caché ARP suele utilizarse para suplantar la identidad de la víctima: ARP Spoofing.
  - Los ataques de spoofing siempre implican suplantación de identidad a diferentes niveles.
- Por ejemplo, se pueden interceptar/modificar todas las comunicaciones entre dos equipos que se encuentren en el mismo segmento de red que el atacante (o entre un equipo y su puerta de enlace).
  - Este ataque se suele denominar Man in the Middle (MitM).

ARP Poisoning, ARP Spoofing y MitM

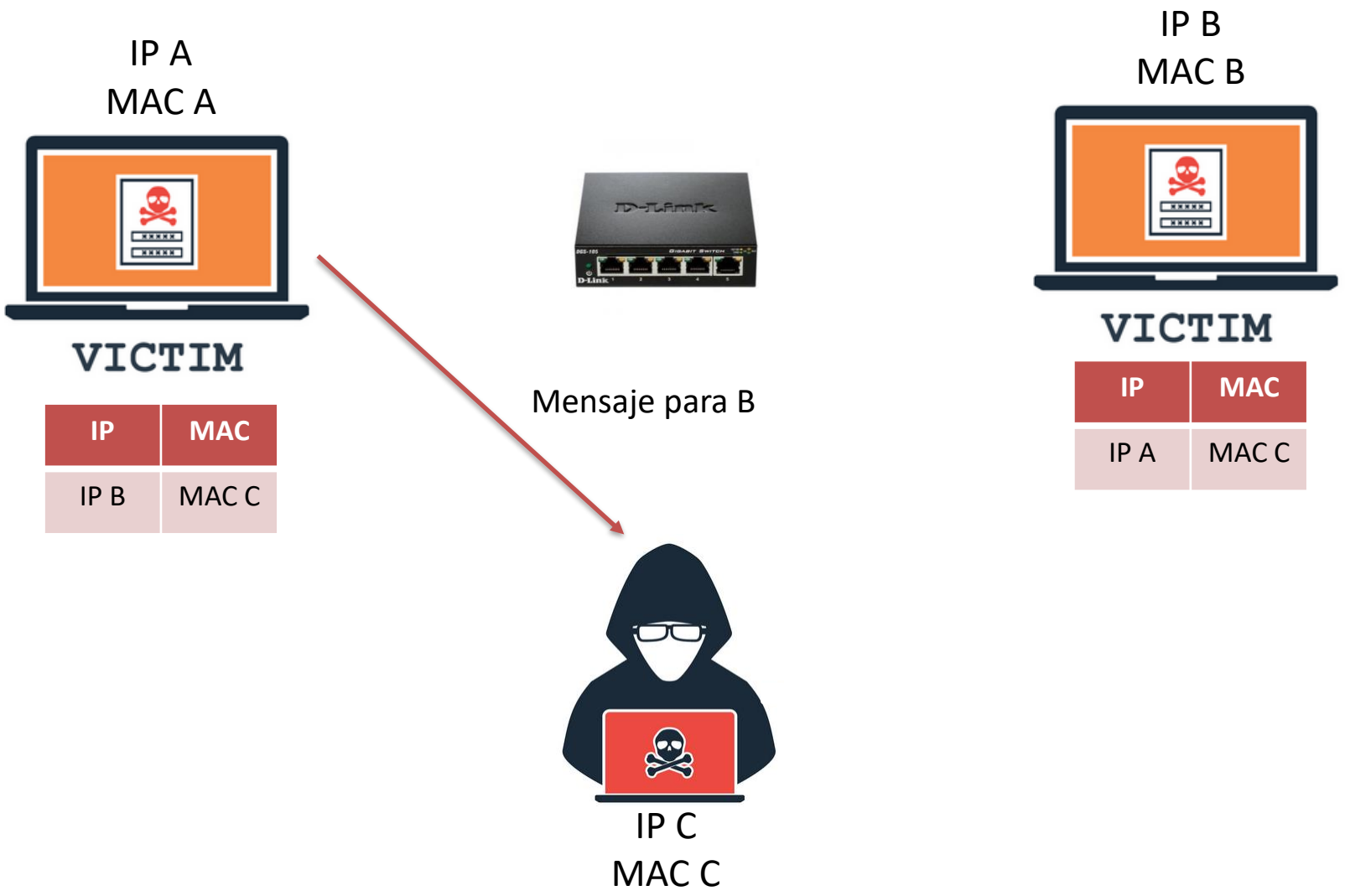


ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos



ARP Poisoning, ARP Spoofing y MitM



IP	MAC
IP B	MAC C

IP	MAC
IP A	MAC C

ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

IP A
MAC A

VICTIM

IP	MAC
IP B	MAC C

Mensaje para B

IP B
MAC B

VICTIM

IP	MAC
IP A	MAC C

IP C
MAC C

ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

IP A
MAC A

VICTIM

IP	MAC
IP B	MAC C

IP B
MAC B

VICTIM

IP	MAC
IP A	MAC C

Respuesta para A

IP C
MAC C

ARP Poisoning, ARP Spoofing y MitM

Universidad Rey Juan Carlos

IP A
MAC A

VICTIM

IP	MAC
IP B	MAC C

IP B
MAC B

VICTIM

IP	MAC
IP A	MAC C

Respuesta
para A

IP C
MAC C

ARP Poisoning, ARP Spoofing y MitM

- Para que el ataque sea efectivo es necesario:
  - Que el atacante tenga visibilidad de las víctimas, o al menos una de ellas y el router (problema del ***insider***).
  - Que el envenenamiento se mantenga en el tiempo. Por lo que el atacante tiene que mandar de manera periódica *ARP Reply* falsas para que esa información esté siempre en las tablas ARPs de las víctimas.
  - El atacante ofrezca buena respuesta para que no haya interrupciones en la comunicación.

Contramedidas

- Tablas ARP estáticas (mucho trabajo admin).
- Implementando el protocolo de configuración dinámica de host (DHCP). Con DHCP Snooping el Switch analiza todo el tráfico que pasa por él ("sabe" en que puerto (camino) se hacen las comunicaciones).
- Herramientas específicas:
  - ARPwatch. Envía una notificación al administrador de la red, cuando una entrada ARP cambia.
  - ReverseARP. Si RARP devuelve más de una dirección IP para una MAC dada, significa que esa MAC ha sido clonada.

Índice

- Introducción y recordatorios.
- ARP Poisoning, ARP Spoofing y Man in the Middle.
- **TCP Hijacking.**
- Ataques en la capa de aplicación.
- Ataques Denial of Service (DoS).

TCP Hijacking

Universidad Rey Juan Carlos

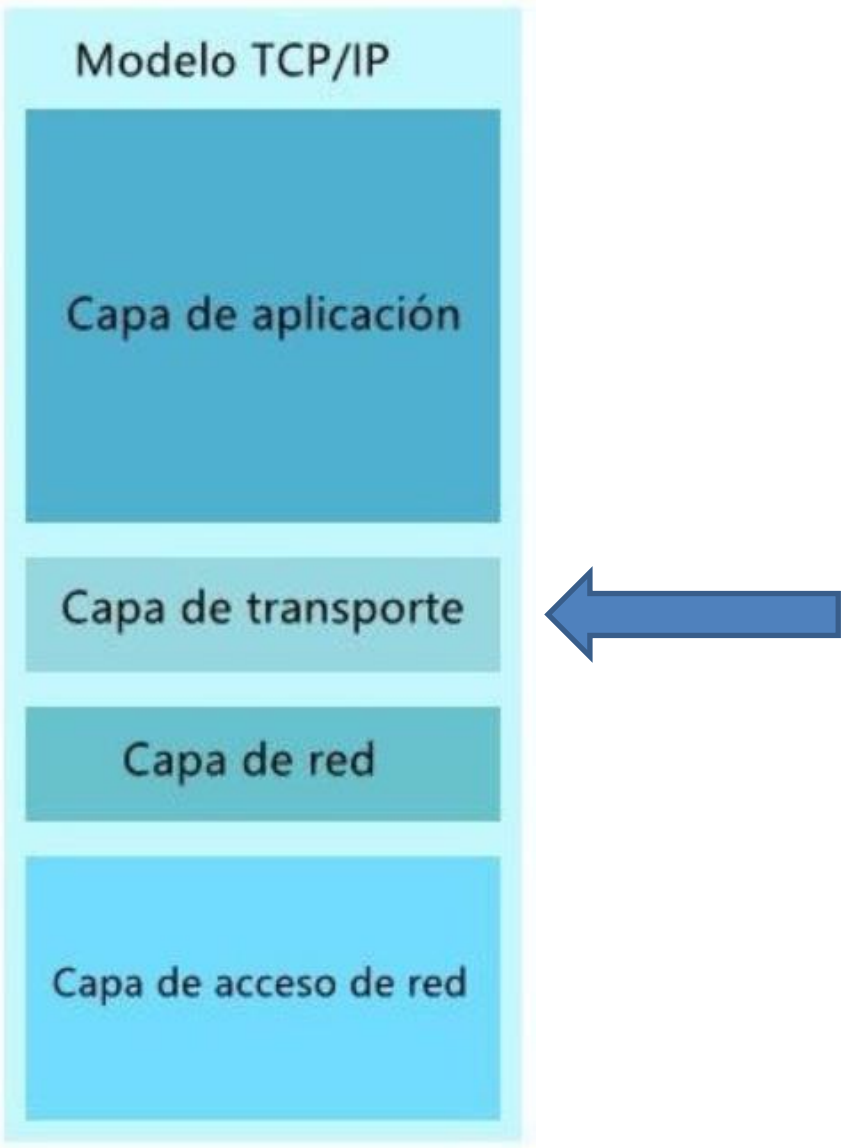
- En muchos casos mediante una combinación de sniffing, envenenamiento ARP y MitM, se puede conseguir el login y la password de un usuario para una determinada aplicación o servicio.

- En el caso del TCP hijacking, lo que se pretende es secuestrar la sesión a un nivel más alto.

- Es decir, tomar el control de la comunicación establecida una vez que el usuario ya ha introducido su login y su password.

TCP Hijacking

Universidad Rey Juan Carlos



TCP Hijacking

Universidad Rey Juan Carlos

- La principal diferencia con respecto a un Spoofing, es que en este último se suplanta una identidad desde el principio.

- En el TCP Hijacking, una vez que el usuario se ha logueado, el atacante se adueña de la sesión y actúa como si fuera el usuario legítimo, pero lo hace porque no puede suplantar al usuario completamente e iniciar la comunicación en el momento que lo desee.

TCP Hijacking

Universidad Rey Juan Carlos

- Las comunicaciones TCP/IP se realizan intercambiando paquetes.
  - La seguridad de una sesión TCP/IP se basa en los números de secuencia intercambiados en cada paquete y los ACKs.
  - Con UDP el secuestro es inmediato, ya que ni siquiera se utilizan estos números.

- TCP no provee de mecanismos que permitan comprobar a los extremos de la comunicación la identidad real del otro, en última instancia sólo se puede confiar en el par dirección MAC-dirección IP.

TCP Hijacking

Universidad Rey Juan Carlos

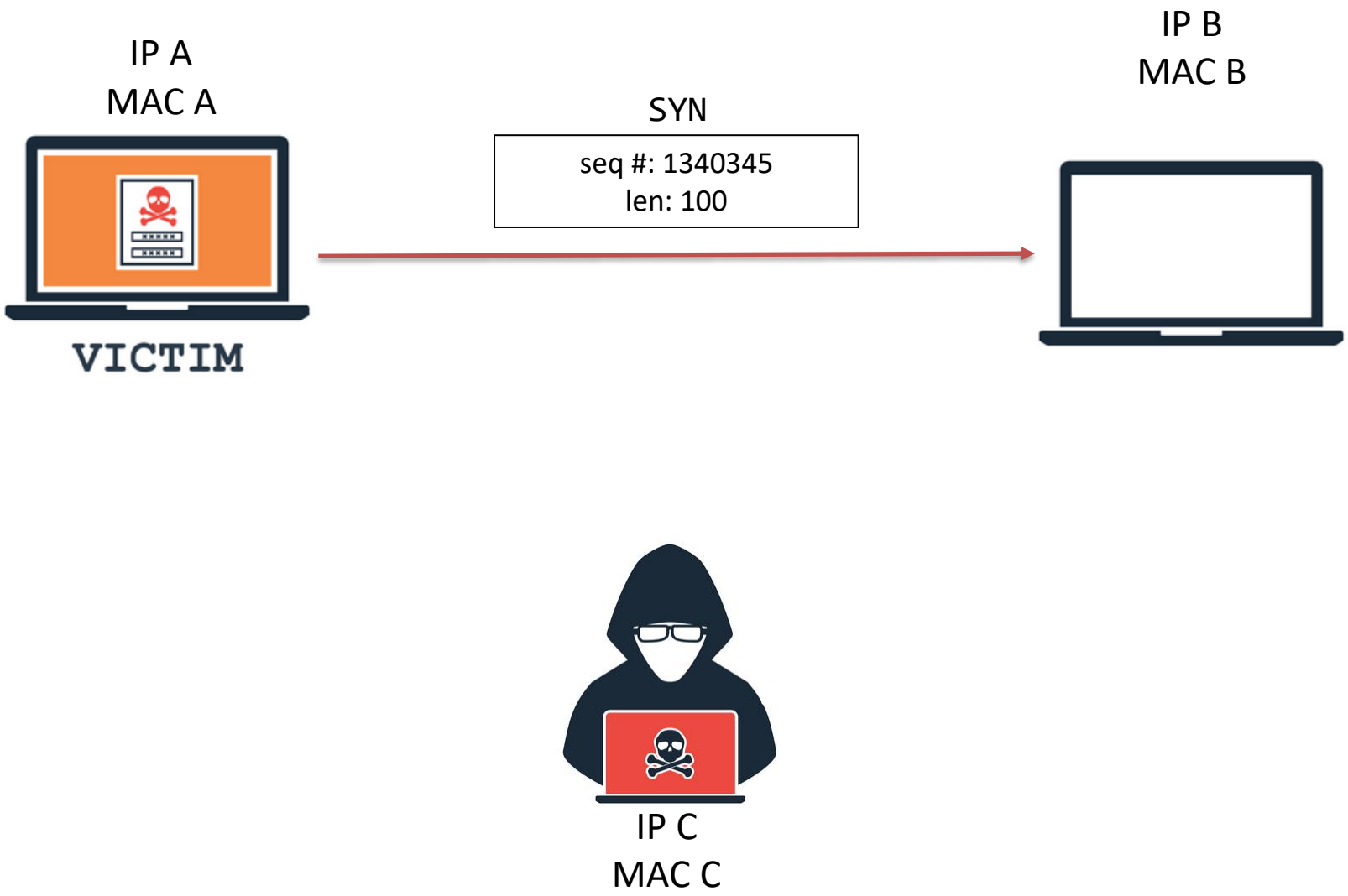
- Una conexión TCP esta definida únicamente por cuatro parámetros:
  - La dirección IP del emisor (el que inicia la conexión).
  - La dirección IP del receptor (el que recibe la conexión).
  - El puerto TCP del emisor.
  - El puerto TCP del receptor.
- Todos los paquetes llevan dos números que los identifican y que permiten decidir a su receptor si los acepta o no:
  - SEQ (32 bits): este número de secuencia se inicializa aleatoriamente y luego se incrementa en el número de bytes enviados, en los paquetes de datos, y en uno, en los paquetes de control.
  - ACK, que no es más que el valor del número de secuencia siguiente que se espera recibir.

TCP Hijacking

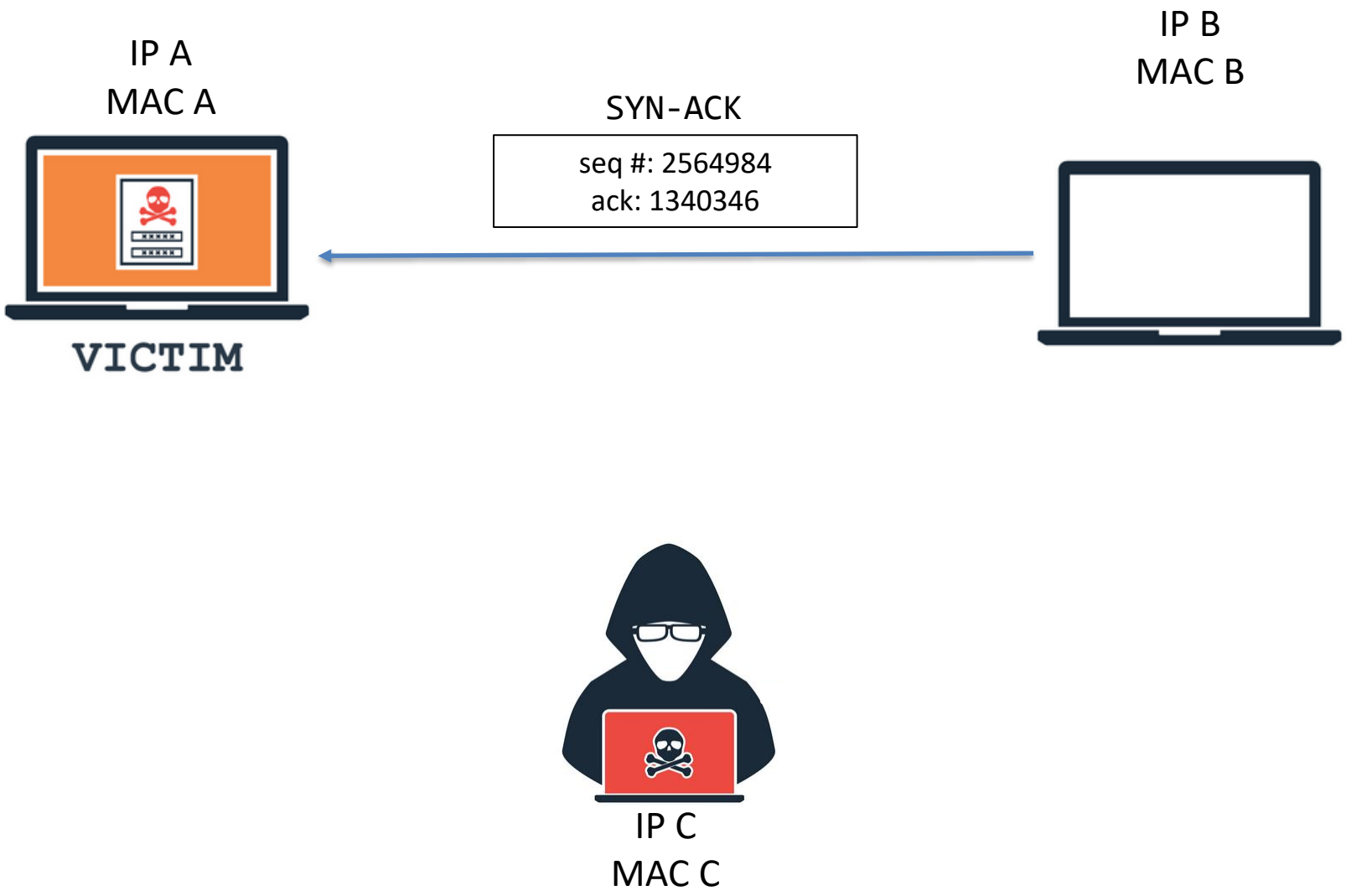
Universidad Rey Juan Carlos

- Para realizar el secuestro de sesión el atacante:
  1. Monitoriza el tráfico TCP entre los equipos que van a mantener la sesión que se desea secuestrar (normalmente con un sniffer).
  2. Espera a que los dos extremos de la comunicación negocien el inicio de sesión y el tamaño de la ventana.
  3. Cuando la sesión ya está establecida, se utilizan los número de secuencia interceptados.
  4. Haciendo spoofing/MitM a la víctima, el atacante envía datos al otro extremo de la comunicación con el número de secuencia y ACK que corresponda.
     - Cuando la víctima los envía, se rechazarán porque ya no corresponden esos parámetros.
  5. La sesión secuestrada
     - La víctima ha perdido la capacidad de comunicarse con el otro extremo y pensará que por algún motivo le han cerrado su sesión, mientras que es el atacante quien tiene el control de la sesión.

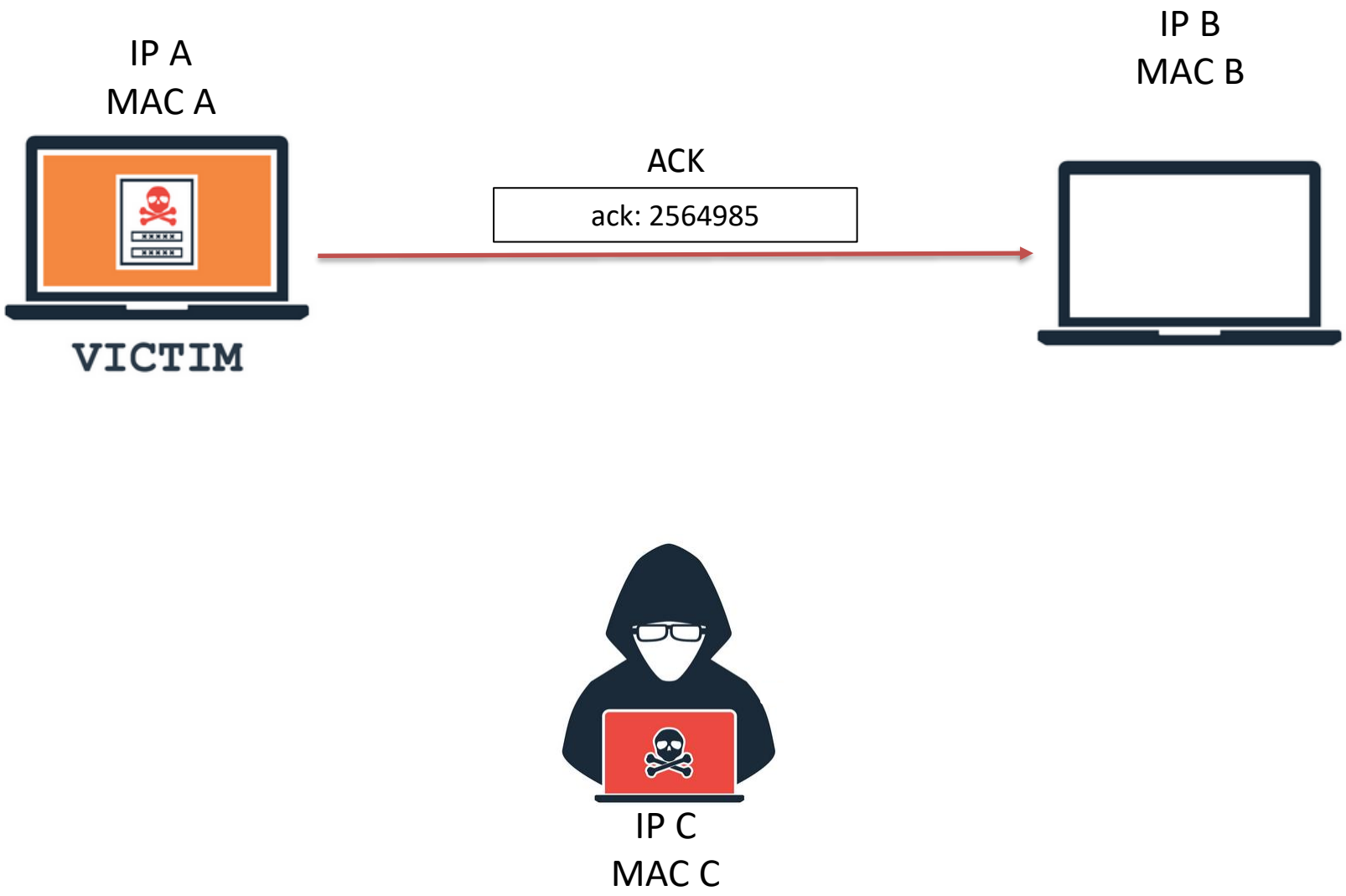
TCP Hijacking



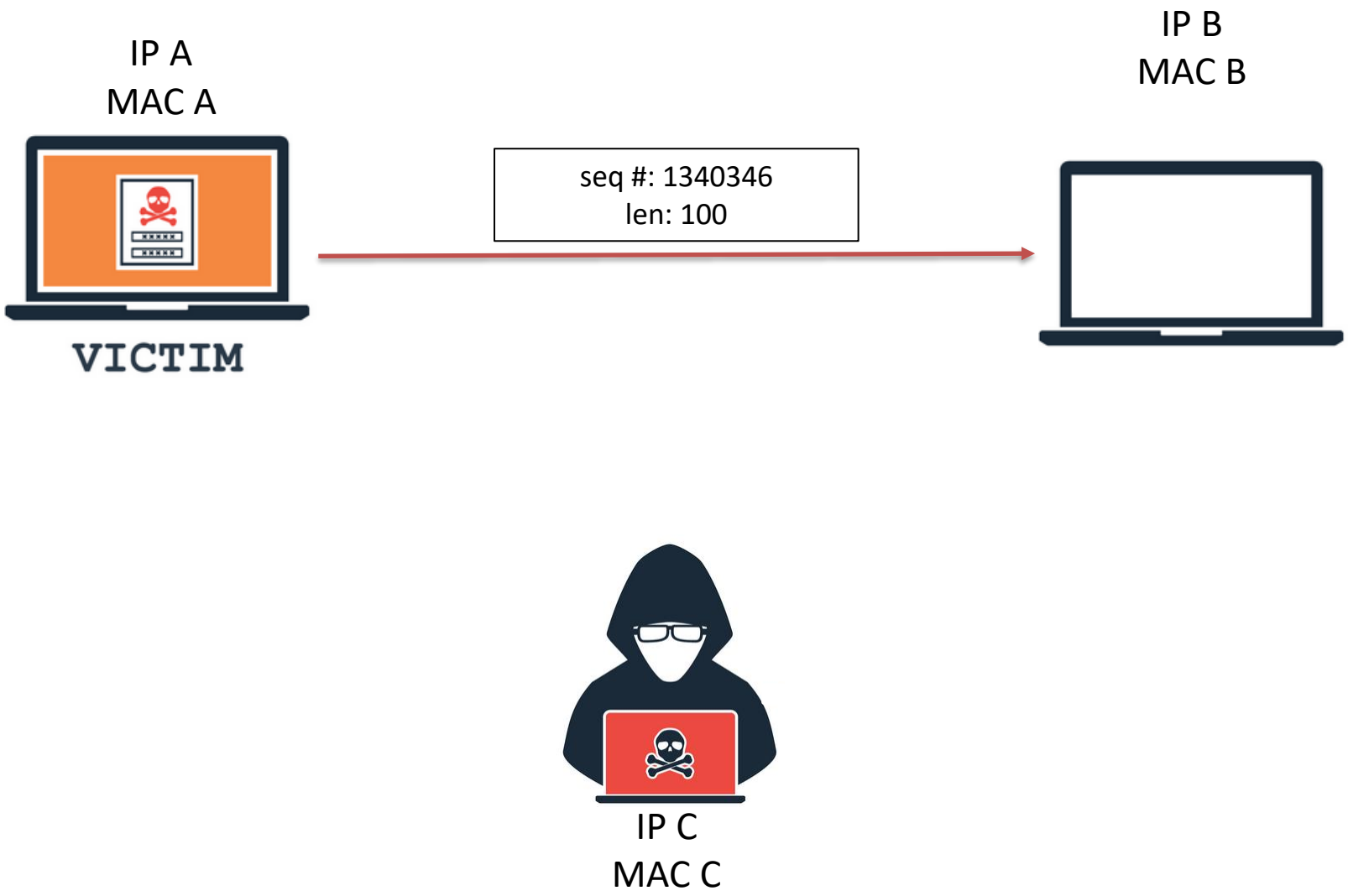
TCP Hijacking



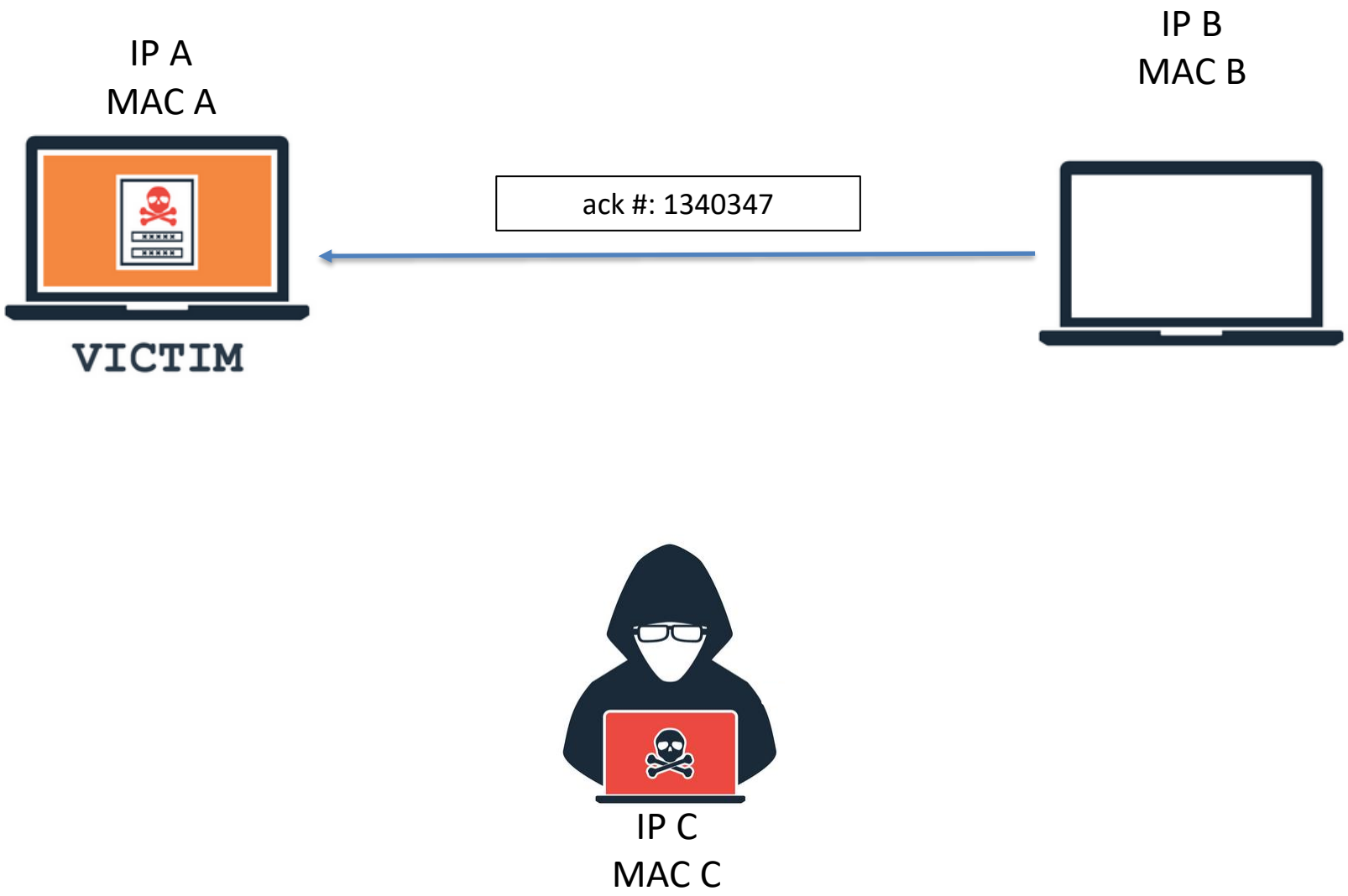
TCP Hijacking



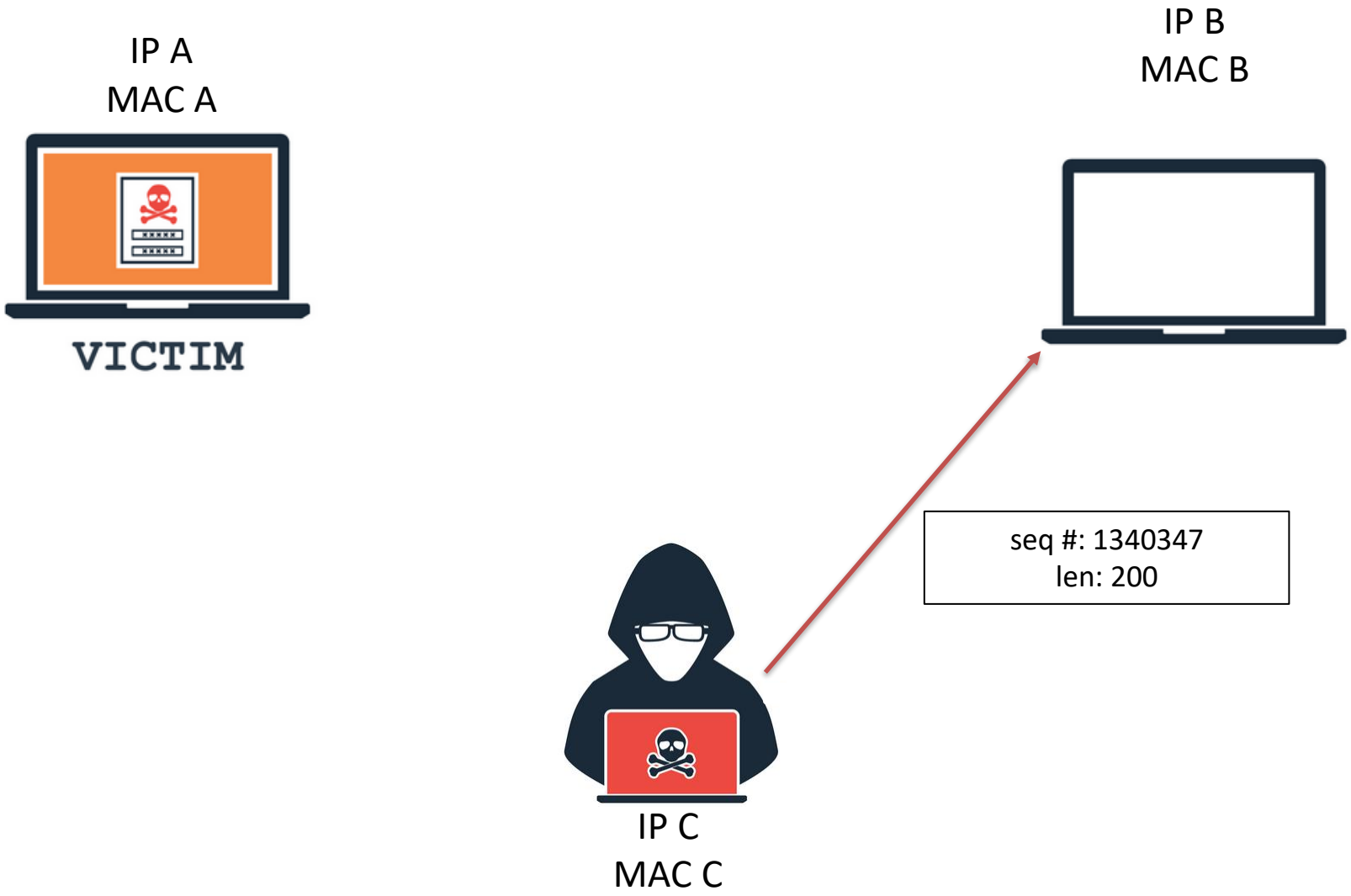
TCP Hijacking



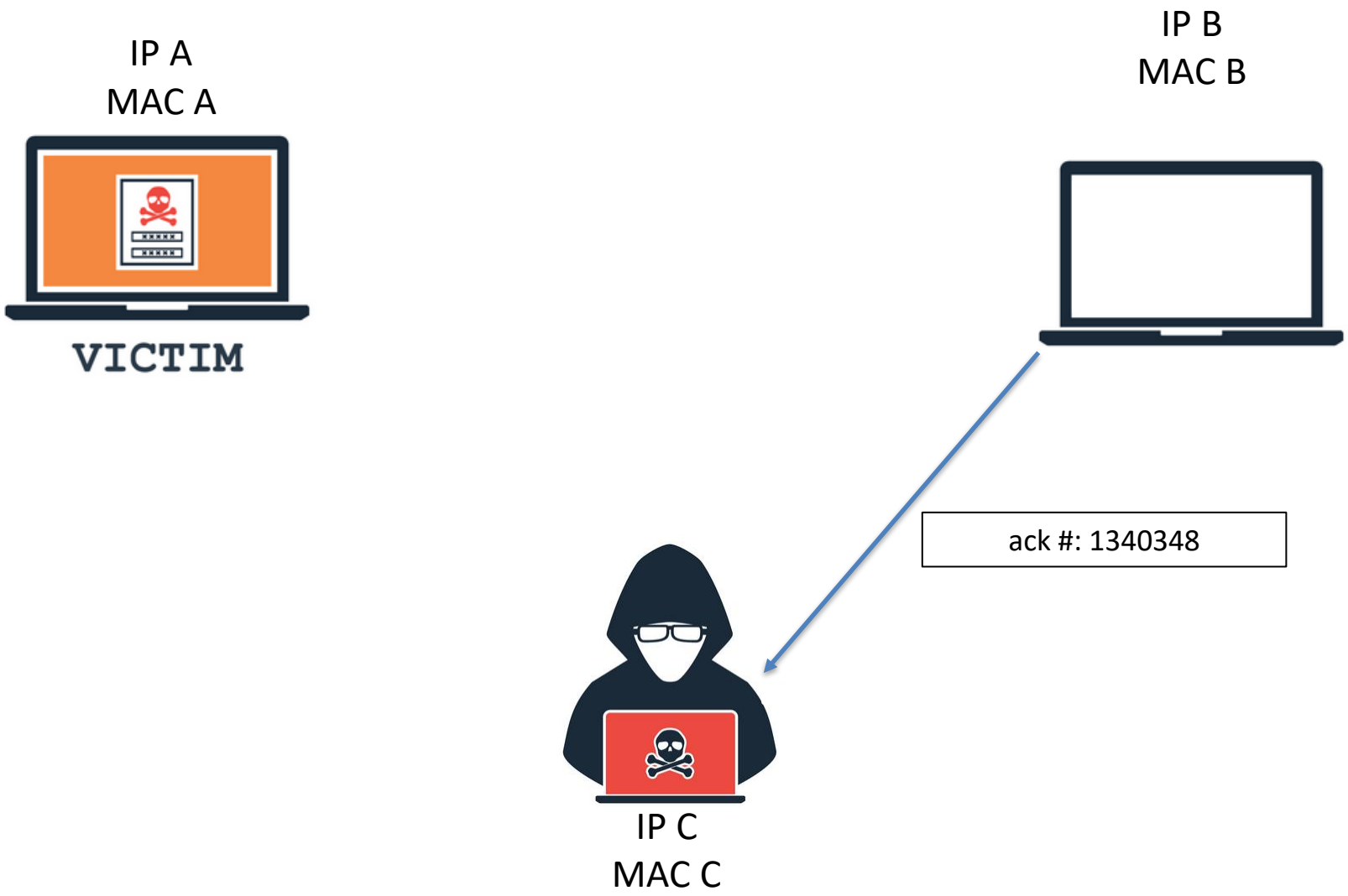
TCP Hijacking



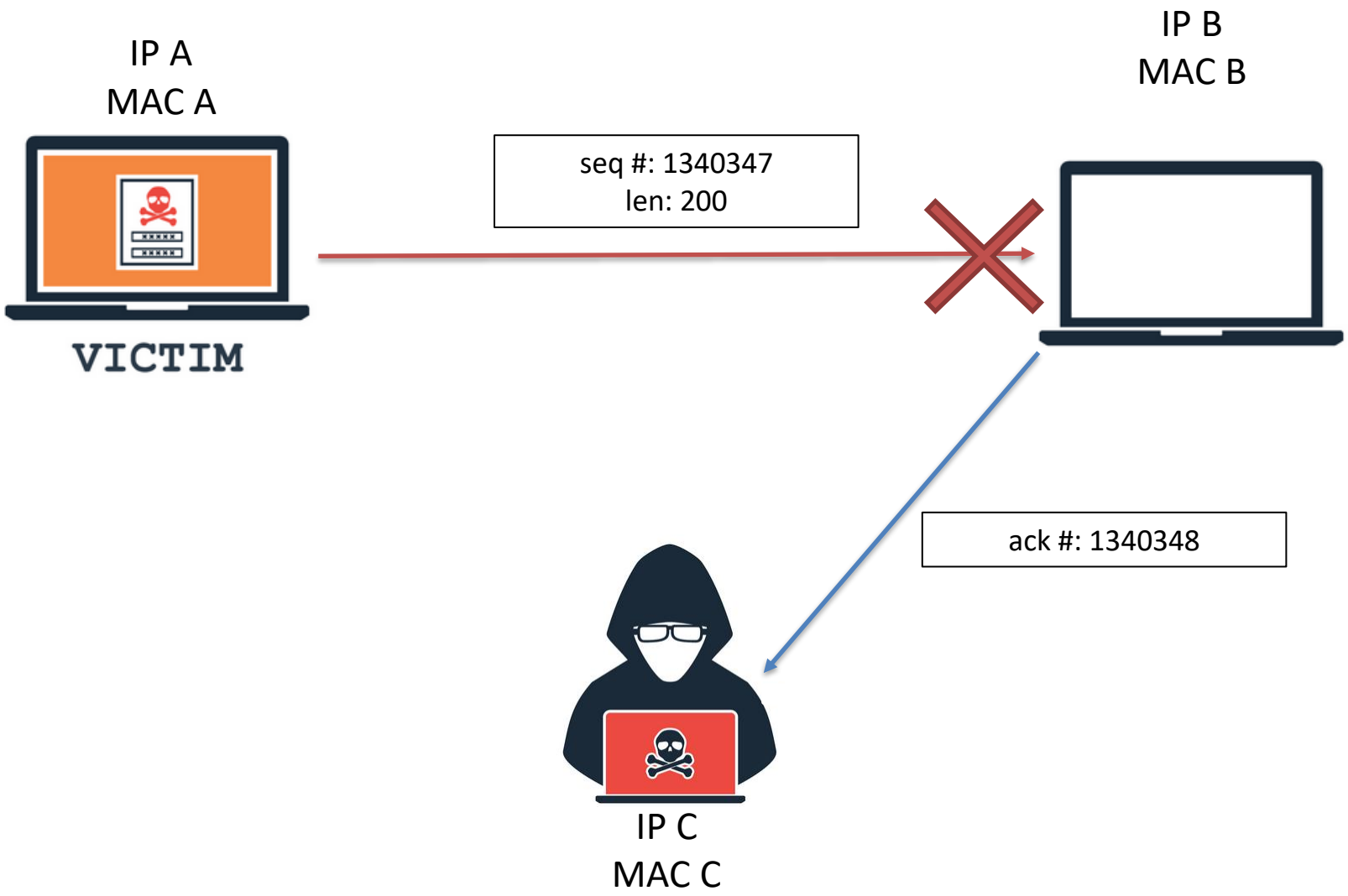
TCP Hijacking



TCP Hijacking



TCP Hijacking



TCP Hijacking

Universidad Rey Juan Carlos

- Si el atacante no puede espiar las comunicaciones entre los dos extremos de la sesión, el secuestro debe hacerse a ciegas y es mucho más complicado.

- Se basan en la predicción de los números de secuencia, que si se han inicializado de manera aleatoria (en teoría) no es tan sencillo.

- En la práctica no es tan aleatoria. Se resetea periódicamente y construye con una fórmula no muy compleja y casi determinista.
  - Se puede averiguar estudiando los sistemas off-line

TCP Hijacking

Universidad Rey Juan Carlos

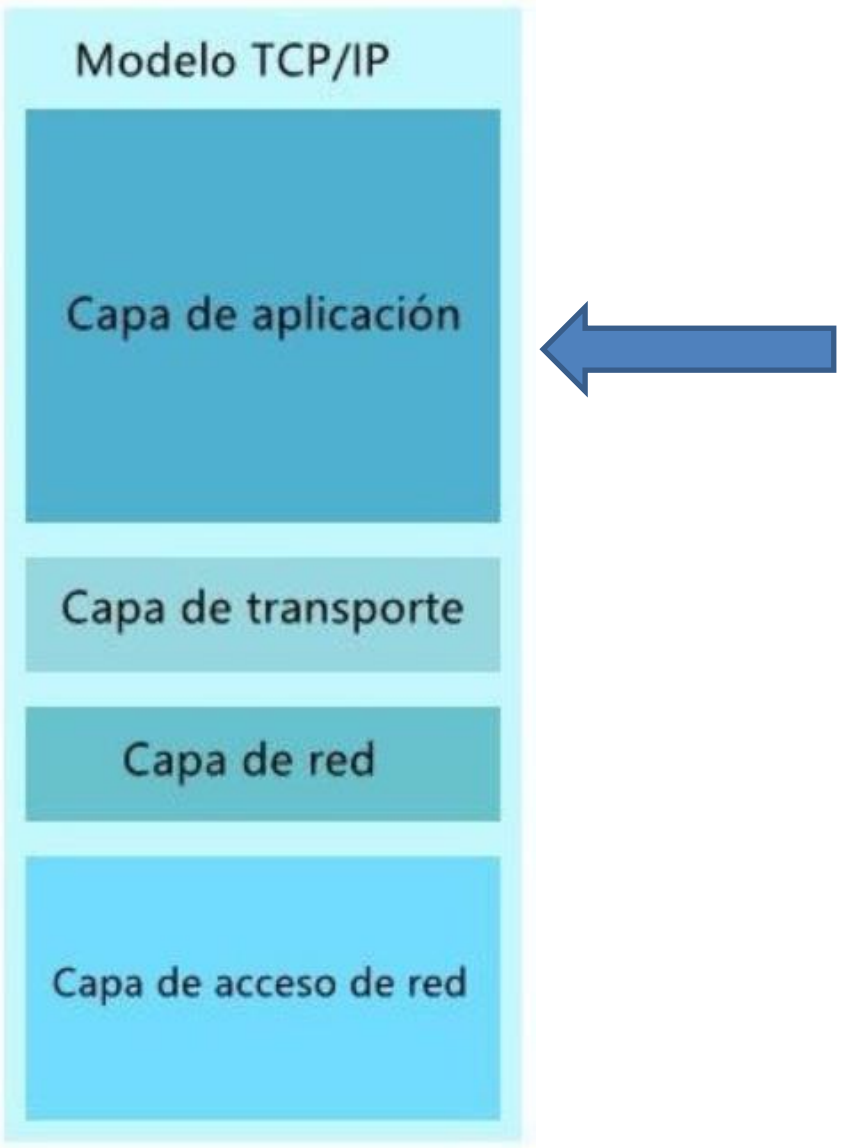
- En la actualidad es un tipo de ataque que está muy en desuso.

- Se puede obtener la misma información con otro tipo de ataques, como son los Cross-site scripting.

Índice

- Introducción y recordatorios.
- ARP Poisoning, ARP Spoofing y Man in the Middle.
- TCP Hijacking.
- **Ataques en la capa de aplicación.**
- Ataques Denial of Service (DoS).

Ataques en la capa de aplicación



Ataques en la capa de aplicación

- La capa de aplicación es la más cercana al usuario final, y por tanto proporciona a los atacantes mayor superficie de ataque.

- Existe una gran variedad de ataques dentro de esta capa pero nos centraremos en los siguientes:
  - Rogue DHCP.
  - DNS Poisoning.
  - Typosquatting.
  - Ataques de denegación de servicio (DoS).

Rogue DHCP

Universidad Rey Juan Carlos

- El objetivo de este ataque no es el MitM que hemos visto hasta ahora*.
- Esta técnica se basa en la implementación de un servidor DHCP falso.

(*) El TCP hijacking no es un MitM

Rogue DHCP

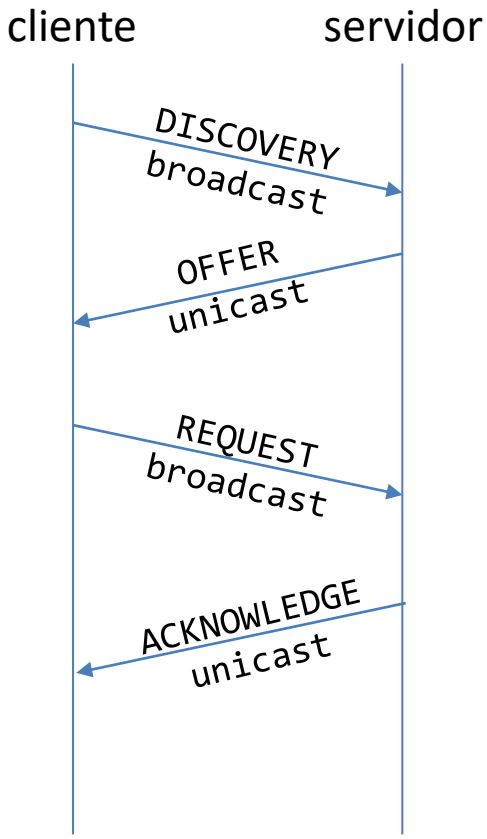
Universidad Rey Juan Carlos

- DHCP es un protocolo que sirve para asignar una dirección IP a una máquina, de manera automática, así como la configuración completa a nivel TCP/IP.
- Es un protocolo muy utilizado ya que simplifica el esfuerzo de administración.
- El problema radica en que la funcionalidad del protocolo es un poco anárquica.

Rogue DHCP

Universidad Rey Juan Carlos

1. El cliente envía un DISCOVERY para que el servidor DHCP le asigne una dirección IP y otros parámetros (la máscara de red, el servidor DNS… etc.)
2. El servidor responde con un OFFER en el que proporciona esa información.
3. El cliente selecciona los parámetros que le interesan y solicita esos datos con un REQUEST.
4. Para terminar, el servidor responde con un ACK para indicar que los parámetros que finalmente se han asignado.



Rogue DHCP

Universidad Rey Juan Carlos

- En este entorno, ¿cómo se comportaría la red si hubiera dos servidores DHCP?
- El cliente “hará caso” a aquel paquete que llegue antes.

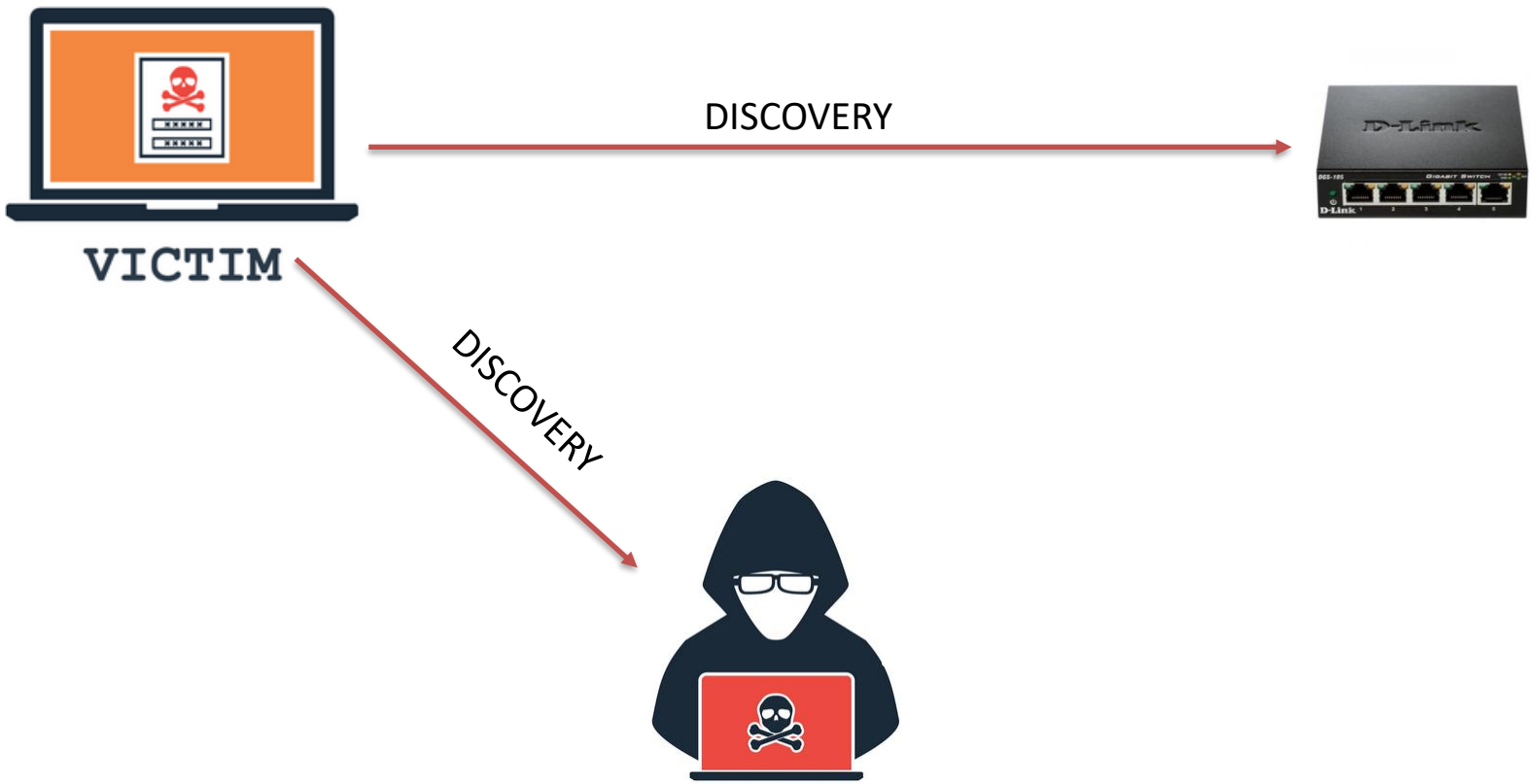
- Un ataque simple consiste en implementar un servidor DHCP falso.
- Cuando un cliente envía un DISCOVERY, el servidor falso responderá con el OFFER… pero también lo hará el servidor real.

Rogue DHCP

Universidad Rey Juan Carlos

- El problema que puede tener un atacante es que puede no conocer tanto el rango de direcciones IP que se están asignando, como las direcciones que ya están asignadas.
- Por lo que podría haber un conflicto entre las direcciones que daría el servidor falso y el real.
- La solución se conoce como *DHCP ACK injection*.

Rogue DHCP

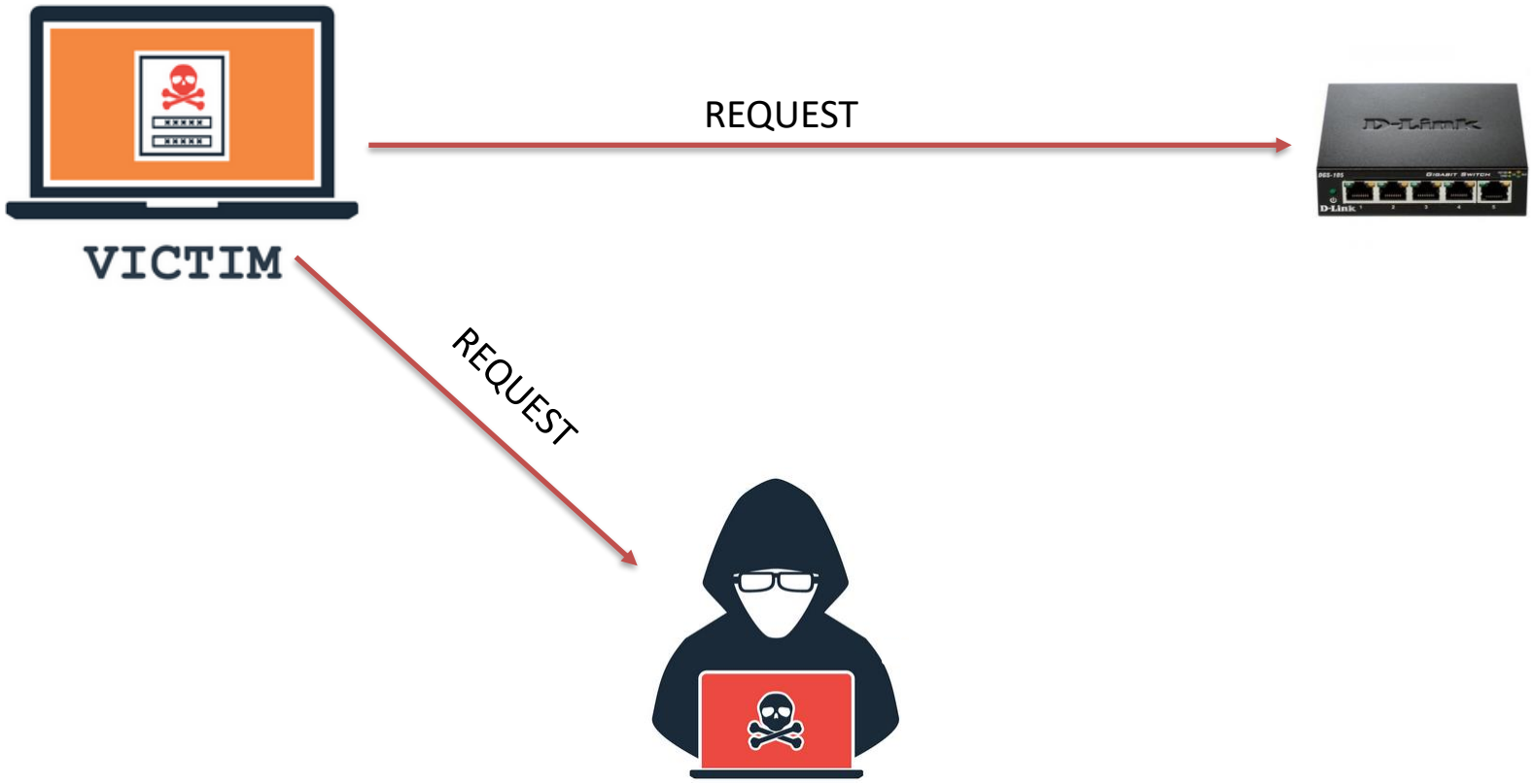


Rogue DHCP

VICTIM

OFFER

Rogue DHCP



Rogue DHCP

VICTIM

ACK

Rogue DHCP

Universidad Rey Juan Carlos

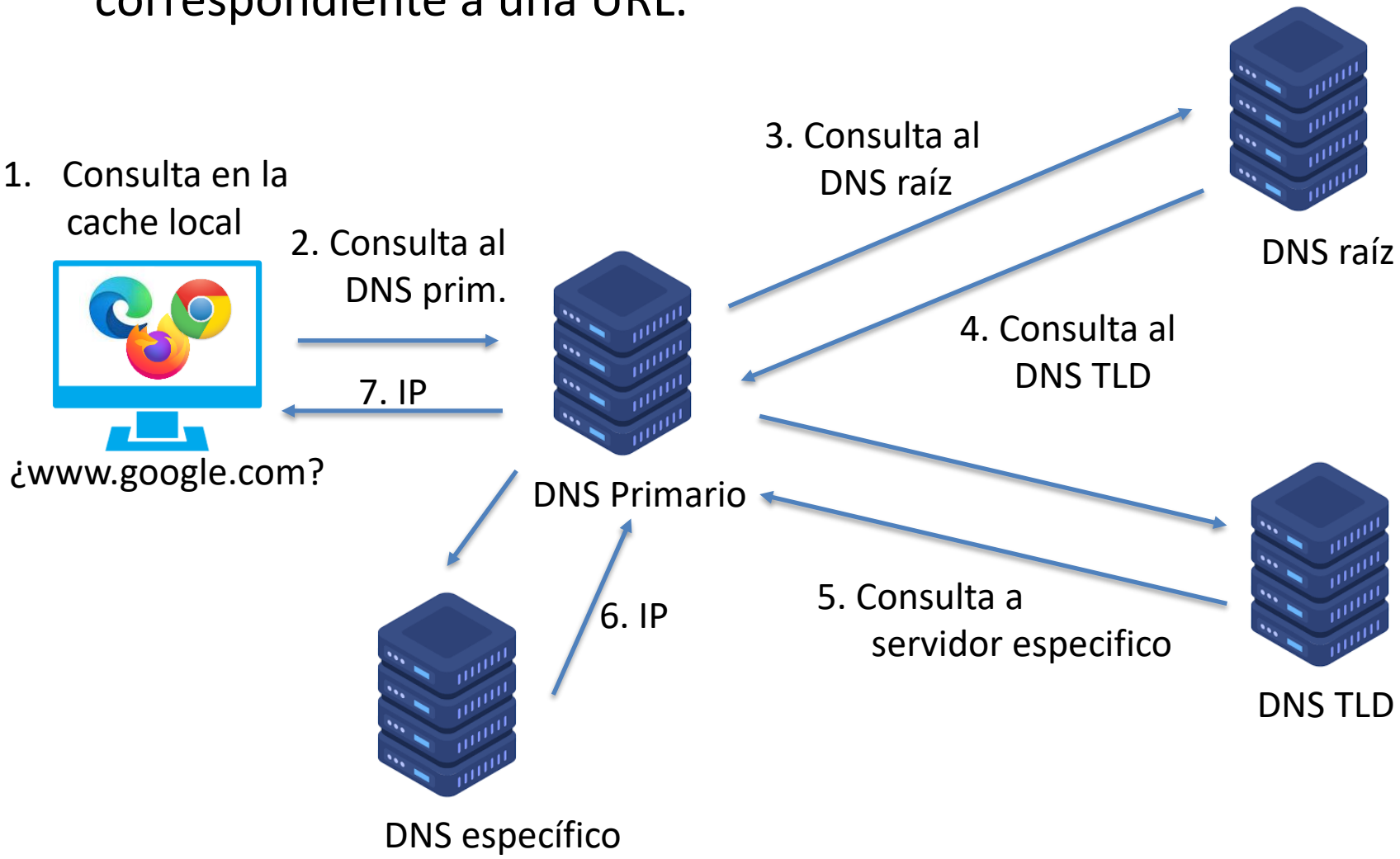
- Una ventaja de este ataque es que no se necesita conocer el rango de direcciones IP válidas ni qué direcciones están libres o no.

- Simplemente hay que esperar a que se mande el REQUEST y ya conocer el rango de direcciones y detalles de la red.

DNS Poisoning

Universidad Rey Juan Carlos

- DNS es un protocolo encargado de obtener la dirección IP correspondiente a una URL.



DNS Poisoning

Universidad Rey Juan Carlos

- DNS Poisoning es un ciberataque que permite redirigir el tráfico de una página web legítima hacia una falsa.

- El ataque se puede hacer de diferentes maneras:
  - Infectando el equipo de la víctima. La idea es que el usuario acceda a una URL que contiene el código malicioso que se ejecuta e infecta la máquina cambiando su configuración.
  - Con un ataque de MitM. El atacante se posiciona entre la víctima y el servidor DNS.
  - Con un DNS server hijack. Puede ser que el router tenga una mala configuración, o tenga alguna vulnerabilidad. Esto permitiría al atacante acceder la configuración del router y cambiar las direcciones de los DNS.

DNS Poisoning

- Con un ataque de MitM.

DNS Primario

Web maliciosa

1. ¿Quién es www.urjc.es?

2. IP a web maliciosa

DNS Poisoning

Universidad Rey Juan Carlos

- DNS server hijack.

DNS Primario

1. Consulta en la cache local

2. Consulta al DNS falso

DNS falso

3. IP a web maliciosa

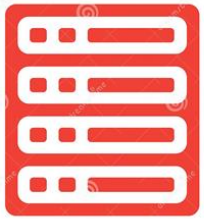
Web maliciosa

DNS Poisoning

Universidad Rey Juan Carlos

- ¿Cómo podría un atacante “introducir” un DNS falso en la red?

DNS Primario



DNS falso

- Spoofing
- Usando Rogue DHCP

DNS Poisoning

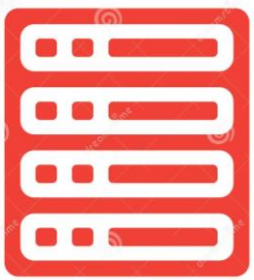
DNS Primario

1. Consulta en la cache local

Web maliciosa

2. Consulta al DNS falso

3. IP a web maliciosa



DNS falso

DNS Poisoning

- El ataque típico consiste en montar un sitio web falso similar a otro oficial.
- De esta manera, el atacante podría obtener las credenciales de la víctima, sin que ésta lo sepa.
- Otro ataque, es el de alojar en la web falsa algún tipo de *exploit* para que cuando la víctima entre en la web, sea vulnerado.

DNS Poisoning

Universidad Rey Juan Carlos

- Algunos riesgos a los que se enfrenta una víctima de DNS poisoning:
  - **Robo de datos**: el atacante puede recrear la página web de entidades bancarias (por ejemplo) de tal manera que contraseñas, información personal o información bancaria, quedan comprometidas.
  - **Infección por malware**: la víctima puede ser redirigida a una web que contenga malware como spyware, keyloggers, gusanos, etc.
  - **Paralización de las actualizaciones** de seguridad: si los sitios suplantados incluyen proveedores de seguridad, las actualizaciones legítimas no se llevarán a cabo y el equipo puede estar expuesto a otras amenazas.
  - **Censura**: se puede modificar el DNS para asegurarse de que sólo se visitan ciertos sitios web aprobados.

Typosquatting

Universidad Rey Juan Carlos

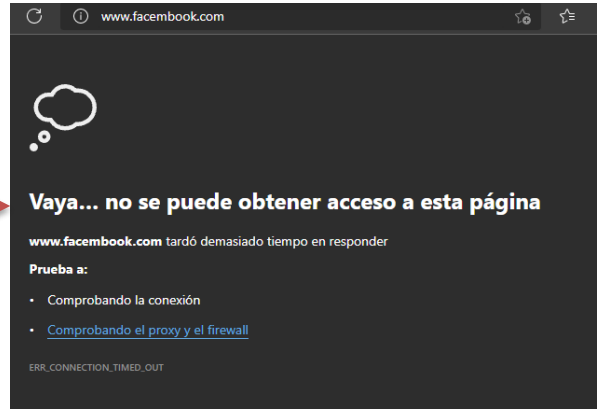
- Consiste en aprovecharse de la probabilidad de que un usuario acceda a una página diferente a la que pensaba visitar por equivocarse al escribir la URL.

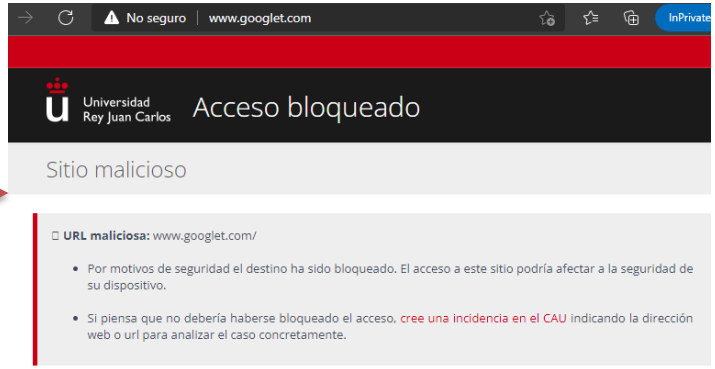
- En este caso el ataque aprovecha los errores tipográficos que los usuarios cometemos al teclear los nombres de dominio.

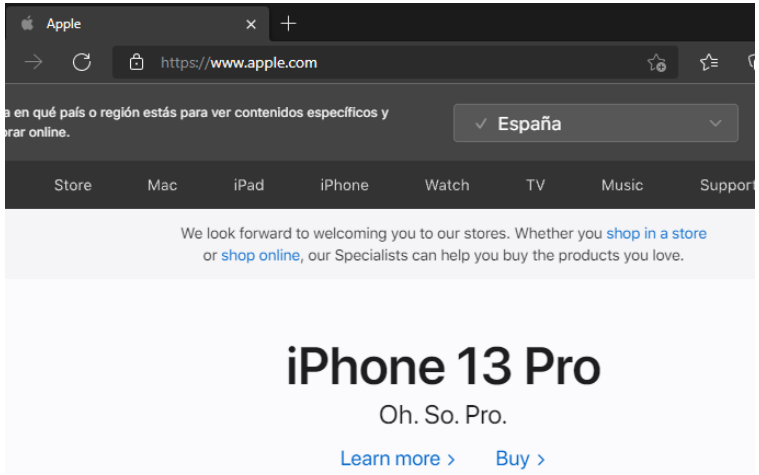
Typosquatting

Universidad Rey Juan Carlos

- Algunos ejemplos podrían ser:
  - www.facembook.com
  - www.googlet.com
  - www.micrososft.com
  - www.twiter.com
  - www.appl.com







Typosquatting

Universidad Rey Juan Carlos

- Por lo general, las grandes compañías suelen comprar los dominios que son similares al principal.
- Sin embargo es complicado abarcar todas las posibilidades.
- Esto es utilizado por los atacantes para crear páginas fraudulentas y obtener información de las víctimas.
- El atacante podría esperar el fallo humano, o intentar por medio del spam, que alguien acceda a su web.

Índice

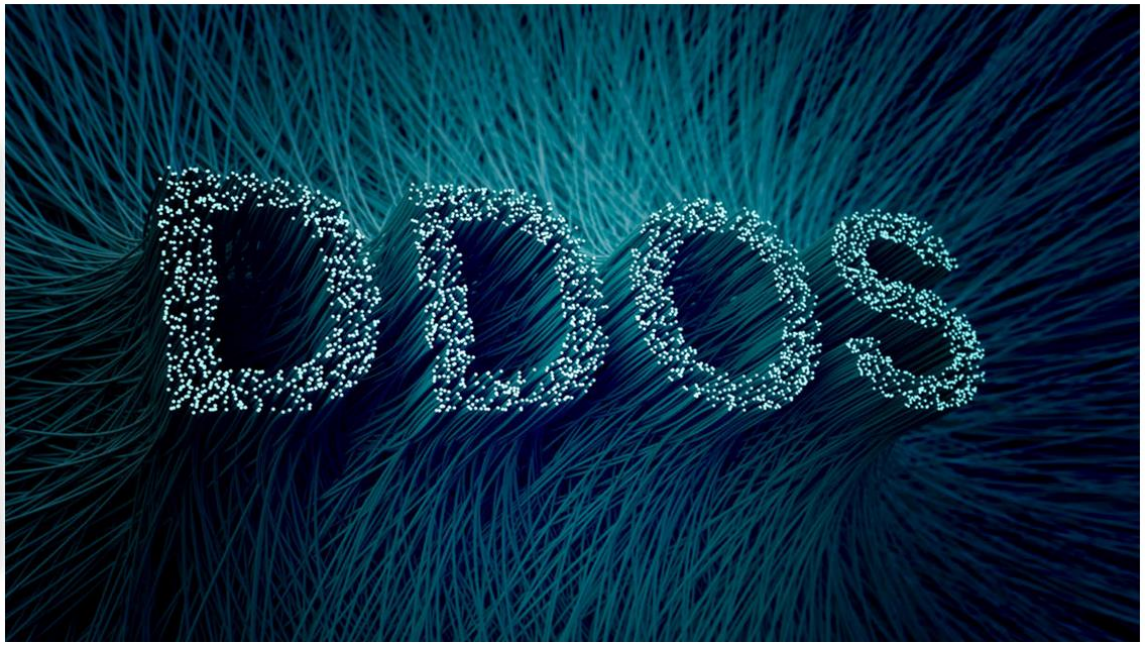
- Introducción y recordatorios.
- ARP Poisoning, ARP Spoofing y Man in the Middle.
- TCP Hijacking.
- Ataques en la capa de aplicación.
- **Ataques Denial of Service (DoS).**

Denegación de Servicio

Universidad Rey Juan Carlos

Máximo histórico de ataques DDos en el mundo el último trimestre de 2021

El número total de ataques DDoS durante el cuarto y último trimestre del año 2021 fue de 86.710, una cifra registrada 4,5 veces superior a la del mismo periodo del año 2020, y que supone un aumento del 52% en comparación con el trimestre inmediatamente anterior.



M.A.M.
23 FEB 2022

La Denegación de Servicio (DoS) es uno de los ataques más frecuentes y que más impacto tienen en la sociedad.

Denegación de Servicio

Universidad Rey Juan Carlos

- La idea de estos ataques consiste en saturar un equipo con el objetivo de evitar el uso legítimo de la red, de los sistemas o de las aplicaciones.

- Para conseguir esto se pretende agotar ciertos recursos como:
  - Las redes -> ancho de banda
  - Los sistemas -> sw. y estructuras de datos para la gestión de la red
  - Las aplicaciones -> contra una web que requiera autenticación.

Denegación de Servicio

- Existen dos grandes grupos de ataques DoS dependiendo de la capa en la que se utilizan.

- De esta manera tenemos:
  - Ataques a la capa de transporte.
    - Inundaciones por ping.
    - Inundaciones mediante SYN.
    - Inundaciones por UDP.
  - Ataques a la capa de aplicación.
    - Inundaciones por HTTP.

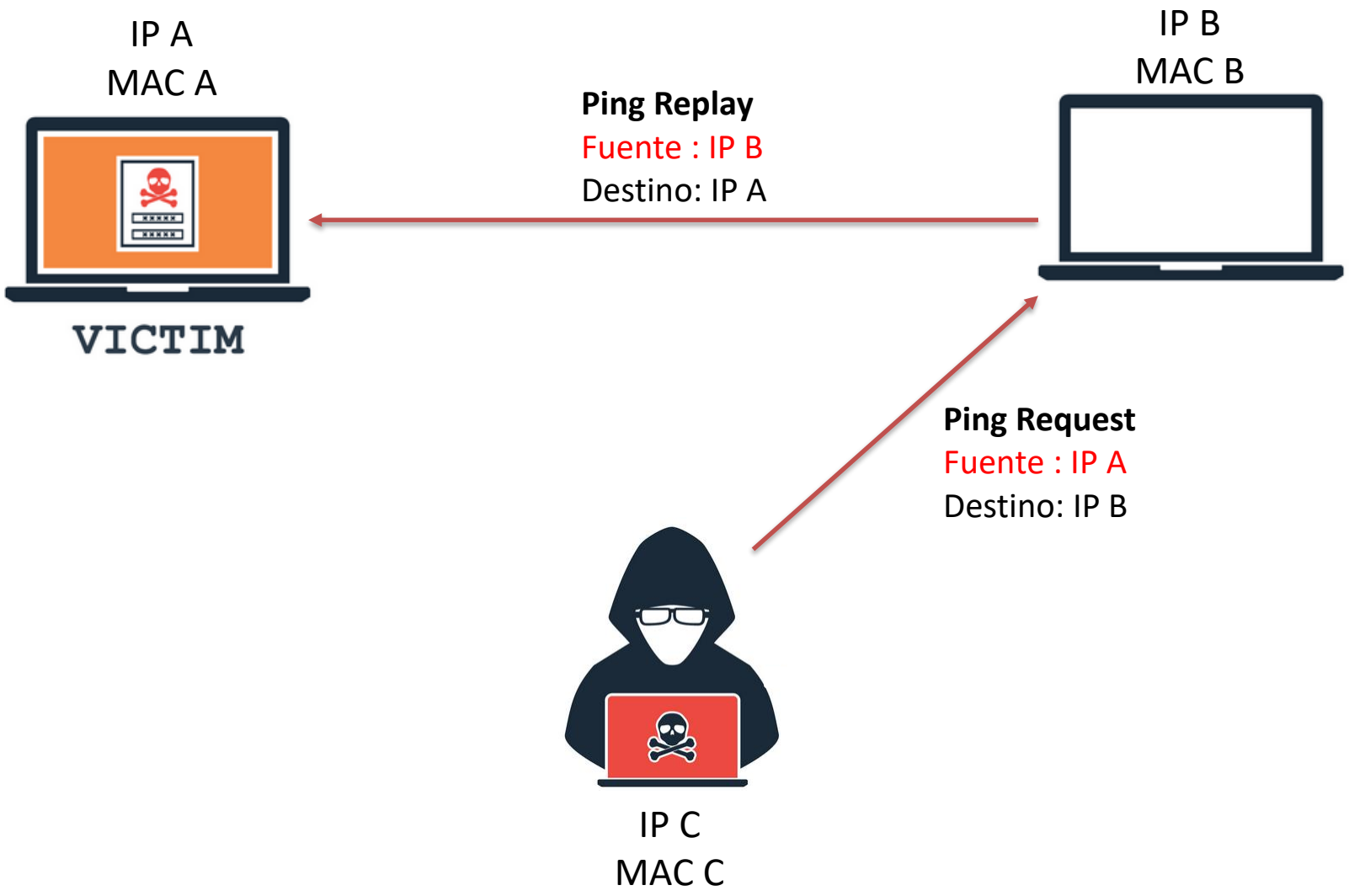
Denegación de Servicio

El DoS clásico: Inundación por ping (ping flood attack)

- Es un ataque contra recursos de red, en concreto intenta saturar el ancho de banda.
  1. Al hacer un ping contra un host este nos dedica una fracción de su tiempo para contestar.
  2. Cuantos más ping hagamos, más tiempo le tendremos ocupado,
  3. y por tanto menos tiempo puede dedicar a otras cosas.

- Para evitar que el atacante sea detectable, y que el ordenador del atacante también se bloquee debido a las respuestas, es necesario falsear de la dirección origen.
- Es decir hay que construir un paquete de datos similar al que se genera al hacer un ping, pero con una IP origen falsa.

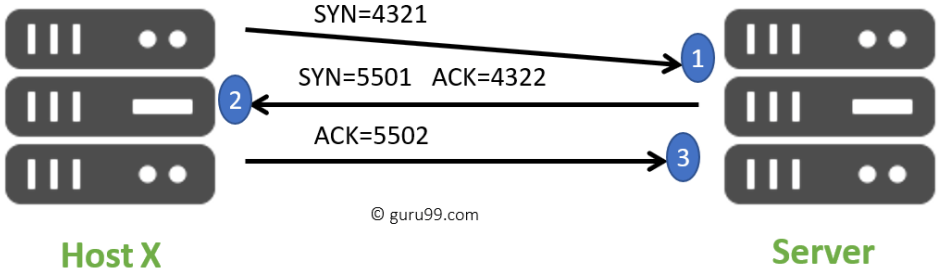
Denegación de Servicio



Denegación de Servicio

DoS mediante SYN Spoofing (Ataque a la tabla de conexiones TCP)

- Es un ataque contra los procesos del SO que gestionan las peticiones de conexión TCP (recursos de sistema).
- El atacante genera muchas señales SYN con direcciones fuente falsas.
- La víctima almacena cada una en la tabla TCP connections y envía la señal SYN-ACK a dichas direcciones.
- Como esas direcciones nunca enviaron nada:
  - Si de verdad existen, envían un RST y la tabla elimina esa petición.
  - Pero si no existen, no responden con ACK, y por tanto la tabla no se vacía.
- Cuando la tabla esta llena no se atienden más peticiones TCP… aunque las peticiones sean legítimas.



Denegación de Servicio

Universidad Rey Juan Carlos

DoS mediante ataque al puerto de diagnóstico con UDP (UDP flood attack)

- Se utilizan paquetes UDP dirigidos contra algún puerto.
- Generalmente los servidores tienen activado el servicio de eco para diagnósticos, en el puerto 7.
- Si un servidor recibe un paquete UDP destinado a ese puerto y el servicio está activado, entonces responderá con un paquete UDP y el servidor pierde el tiempo.

Denegación de Servicio

Universidad Rey Juan Carlos

- La ventaja (o problema) de los ataques anteriores es que son fácilmente detectables.
- Sin embargo existen otros ataques que son más complicados de detectar.
- Es el caso de las inundaciones por HTTP.
- De las cuales hay diferentes tipos.

Denegación de Servicio

Universidad Rey Juan Carlos

Fragmentación HTTP

- En este ataque, se estable una conexión HTTP válida.
- La clave está en dividir todo el tráfico de datos en pequeños fragmentos y enviarlos lo más lento posible para que no de *timeout.*

- Esto obliga al servidor a mantener sesiones activas por largos períodos de tiempo, por lo que si el número de conexiones también es alto, se agotarán los recursos asignados a la tabla de conexiones.

Denegación de Servicio

Número excesivo de conexiones HTTP

- Consiste en generar muchas conexiones HTTP contra un servidor.
- En este caso lo que se hace es realizar peticiones específicas que buscan maximizar el tiempo de procesamiento por parte del servidor.
- Un ejemplo: solicitud de archivos de gran tamaño.
- Otro ejemplo: usando el estándar HTTP, un atacante puede pedir un número arbitrario de veces el mismo fragmento de un archivo y cada petición se puede mandar en una sesión diferente, solicitando hasta 1 Gb (por petición).

Denegación de Servicio

Universidad Rey Juan Carlos

Número excesivo de peticiones en una sesión

- Variante del caso anterior, en el que se realizan varias peticiones dentro de la misma sesión HTTP.

Peticiones múltiples en una sola sesión

- Se crean múltiples peticiones HTTP que no se envían de manera individual, sino que se genera un único paquete con todas ellas.
- Se genera un alto número de peticiones con una baja tasa de envío de paquetes.

Denegación de Servicio

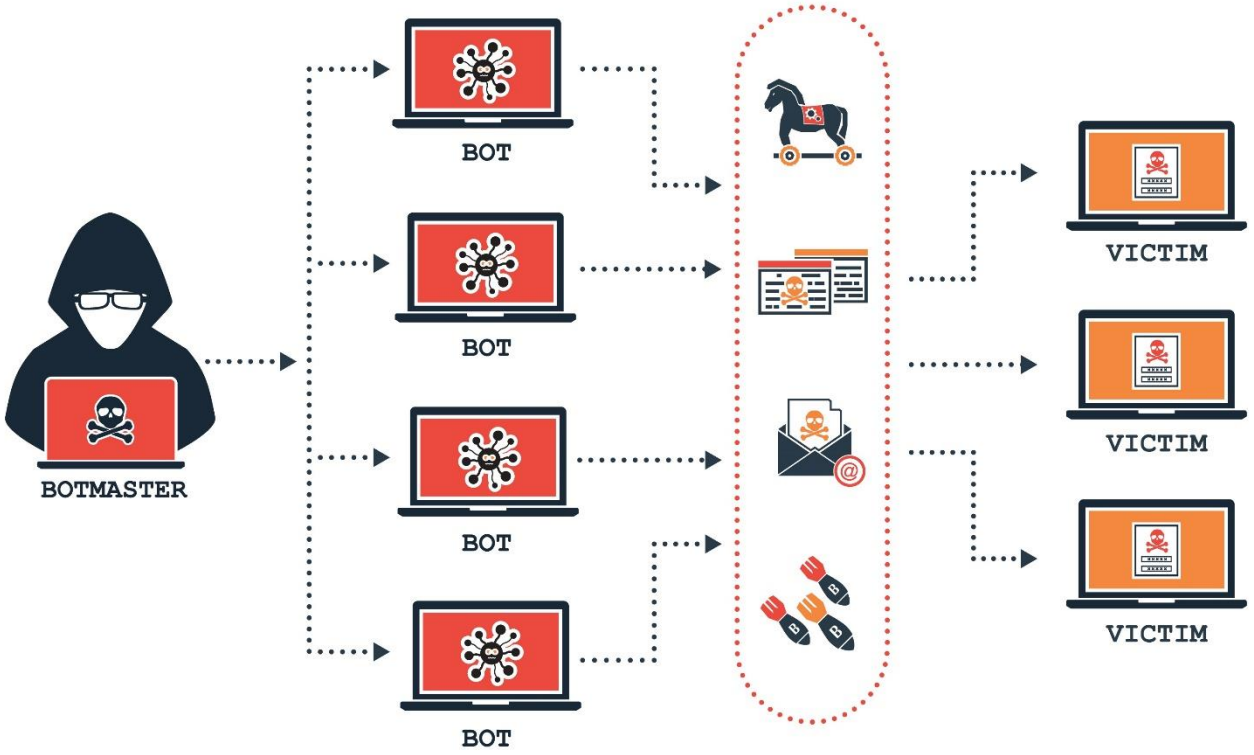
Universidad Rey Juan Carlos

- Estos ataques logran el daño deseado cuando realmente son capaces de agotar los recursos de la víctima.
- Pero esto es muy difícil utilizando un único equipo.
- Los atacantes normalmente utilizan técnicas para poder usar más equipos:
  - DoS distribuido (DDoS).
  - Ataques por reflexión.
  - Ataques con amplificación .

Denegación de Servicio

Universidad Rey Juan Carlos

DoS Distribuido (Distributed DoS, DDoS)



Denegación de Servicio

DoS Distribuido (Distributed DoS, DDoS)

- El atacante primero debe lograr acceso a un equipo o a una red.
- A continuación, utiliza algún malware que le permita controlarlo.
  - dicho equipo se denomina zombi.
  - dicha red se denomina botnet.
- Normalmente se agrupan varios zombis bajo un controlador (handler) creando una jerarquía.
- Para comunicarse con los controladores
  - Antes se desarrollaban programas específicos.
  - Hoy en día, los atacantes se comunican con los controladores mediante servidores de HTTP o IRC.
  - Además se incluyen mecanismos criptográficos para evitar que un análisis de la red los pueda detectar.

Denegación de Servicio

Universidad Rey Juan Carlos

- Una botnet se podría construir con un ataque por malware.
- Aunque también podríamos alquilarla en la Deep web.

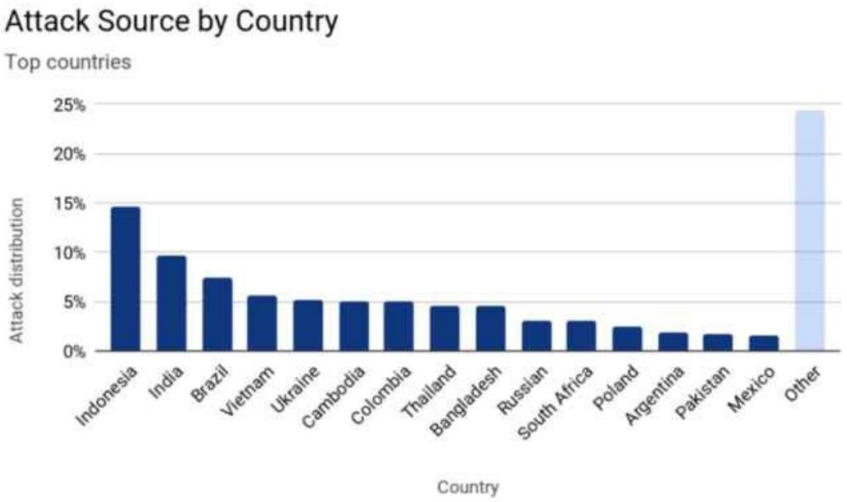
- En los últimos años estas botnets están compuestas no solo por ordenadores y equipos sino por dispositivos IoT.
- Muchos comerciantes no tienen la seguridad del dispositivo incorporada en el producto.
- Hay muchos clientes que no se preocupan por la seguridad y dejan configuraciones por defecto.
- Mirai: malware que escanea internet en busca de dispositivos IoT basados en Linux que están desprotegidos, o tienen configuraciones por defecto. Una vez detectados, los infecta para controlarlos.

Denegación de Servicio

- Ejemplos de ataques DDoS:
  - Navidades de 2014. Dos ataques de este tipo tumbaron PlayStation Network y Xbox Live. Por lo que los usuarios no pudieron jugar durante las navidades.
  - En Octubre de 2016 se realizó un ataque muy significativo de DDoS. En lugar de atacar un servidor, o plataforma, este ataque se enfocó a los servidores de la empresa Dyn.
    - Dyn es un proveedor de DNS muy importante.
    - El resultado del ataque: se cayeron servicios como Twitter, Reddit, Spotify, Paypal, PlayStation Network o la CNN.

Denegación de Servicio

- A finales de verano del 2021, se reportó el mayor ataque DDoS de la historia.
- Este ataque utilizaba una botnet Mirai que en cuestión de segundos fue capaz de lanzar más de 330 millones de solicitudes.
- Esto implica una tasa de 17,2 millones de rps (*request per second*)



Denegación de Servicio

Universidad Rey Juan Carlos

- También tenemos la botnet de **Meris**.
- Esta botnet ha conseguido batir el record anterior 2 veces a finales del año 2021.
- El rps conseguido es 21,8 millones, y utilizó 250.000 dispositivos.
- Países que han sido atacados: Rusia (afectó a instituciones financieras), Reino Unido, Estados Unidos, Nueva Zelanda (bloqueó el acceso a los bancos principales del país durante 3 días)

Denegación de Servicio

- Finalmente otro ejemplo de ataque DDoS volumétrico (en función de la cantidad de datos solicitados).

- En Junio de 2020, Amazon AWS informó que había lidiado con el que sería el mayor ataque DDoS volumétrico hasta el momento.

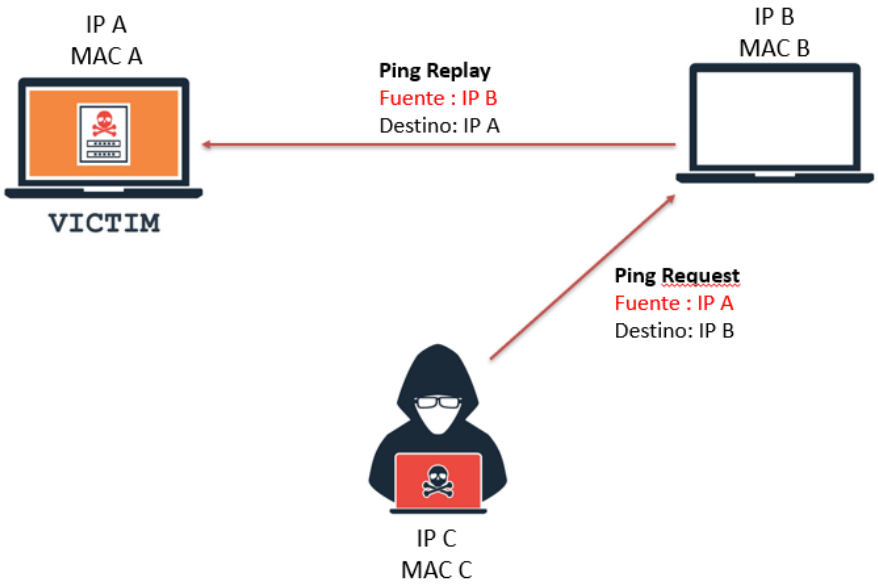
- Según Amazon el ataque fue de 2,3 Tbps.
- Los ataques de este tipo suelen ser de 500 Gbps.

- Otro ataque importante lo sufrió GitHub en 2018 y soportó 1,3 Tbps.

Denegación de Servicio

Ataque DDoS por reflexión

- Es un tipo de ataque con intermediario que refleja la acción contra la víctima.
- A veces, se crea un bucle de tráfico entre intermediario y la víctima.
- Ataque por intermediario:



Denegación de Servicio

Universidad Rey Juan Carlos

Ataque DDoS por reflexión

- Es un tipo de ataque con intermediario que refleja la acción contra la víctima.
- A veces, se crea un bucle de tráfico entre intermediario y la víctima.
- Ataque por intermediario:
  - El atacante envía paquetes de petición a un servicio pero con la dirección de la víctima.
  - Se suelen seleccionar servicios que generen un gran volumen de tráfico porque todo ese volumen va a parar a la víctima.
    - Ventaja 1: Si puede ser, el atacante enviará todo ese tráfico contra la victima.
    - Ventaja 2: Si no, el ataque estará camuflado entre tanto volumen.

Denegación de Servicio

- Una petición DNS es un paquete UDP de 60 bytes, pero la respuesta es otro paquete UDP de 512 bytes (máximo).
  - Utilizar servidores DNS que respondan con registros grandes como intermediarios.
- Pero además, DNS ha ampliado a 4000 bytes la respuesta para incluir características como IPv6, seguridad, etc.
- Secuencia del ataque:
  - El atacante crea un serie de peticiones DNS con la dirección de la víctima, y las dirige a los servidores DNS seleccionados.
  - Estos responden a la víctima con un tráfico mucho mayor que el empleado para atacarla.

Denegación de Servicio

Universidad Rey Juan Carlos

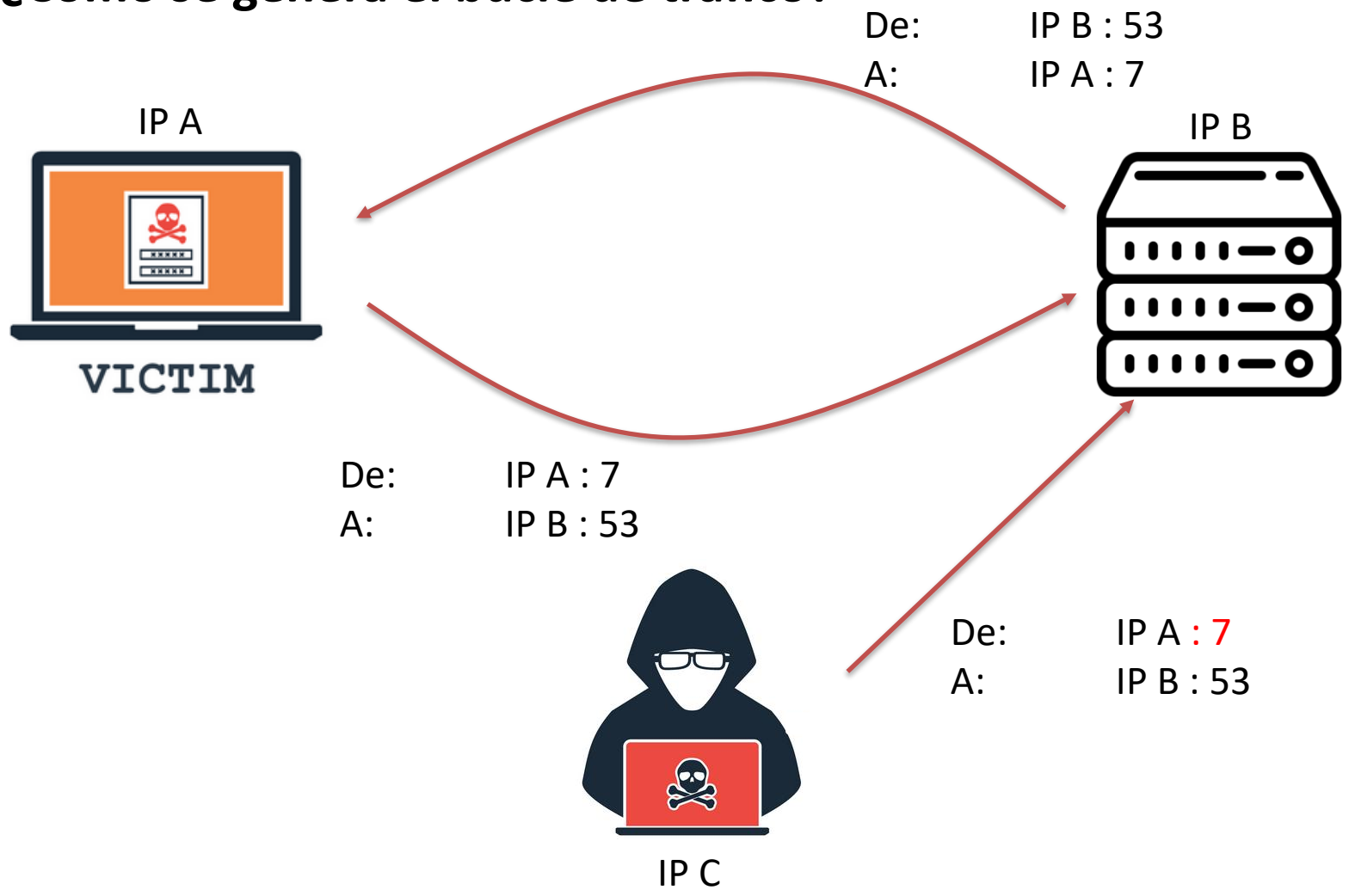
¿Cómo se genera el bucle de tráfico?

- Si la víctima tiene el servicio de *echo* activado, puede entrar en un bucle con el servidor DNS intermediario.
- Recordar que:
  - DNS viaja sobre UDP, igual que el servicio de *echo*
  - El puerto de servicio de diagnóstico mediante *echo* es el 7
  - El puerto para servir nombres de dominio es el 53

Denegación de Servicio

Universidad Rey Juan Carlos

¿Cómo se genera el bucle de tráfico?



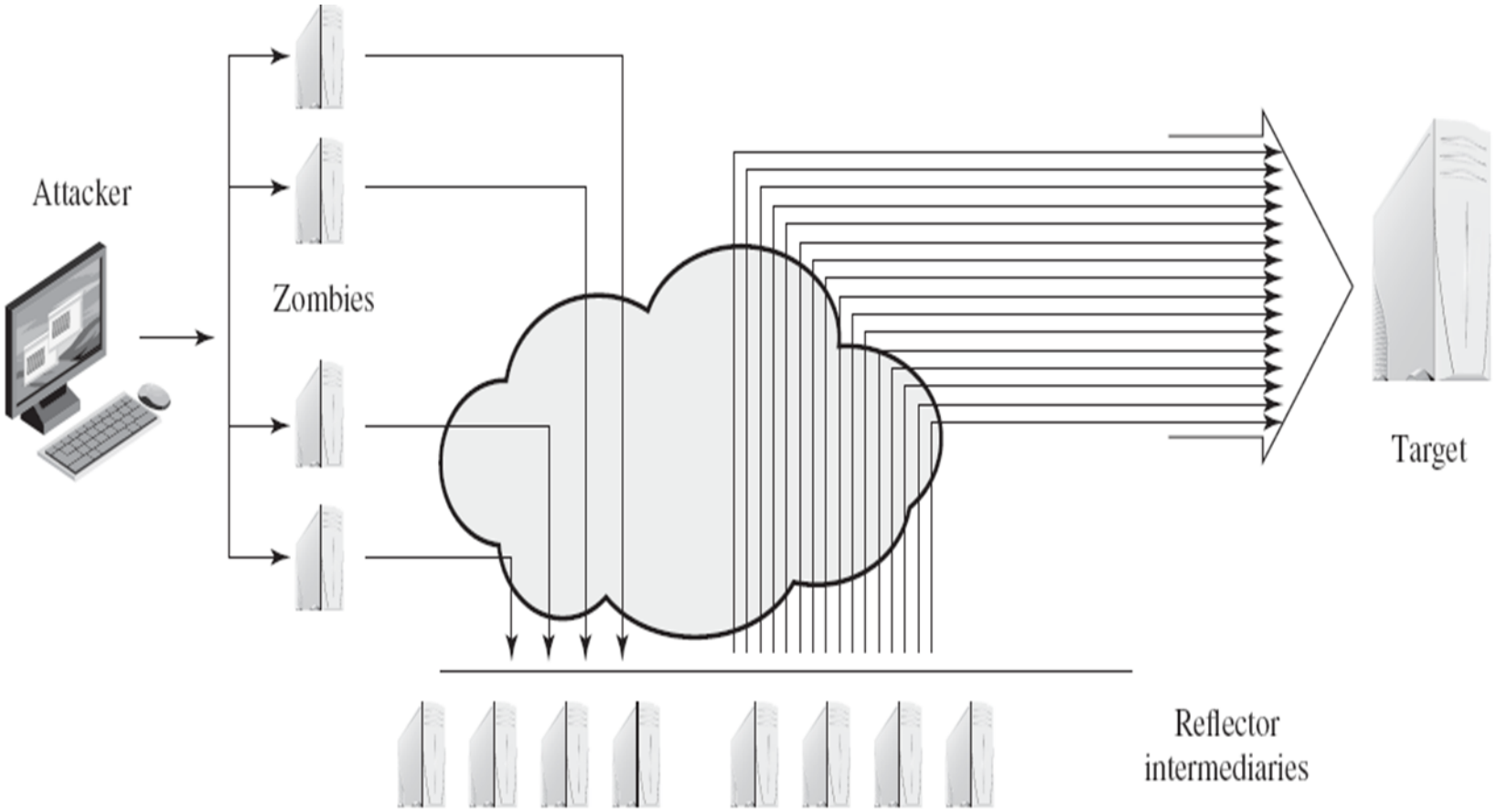
Ataque DDoS por amplificación

- Es similar al de reflexión pero se utilizan muchos intermediarios.

- Un modo habitual es dirigir la petición inicial a la dirección de broadcast de alguna red.
  - Todos los hosts de dicha red responderán.

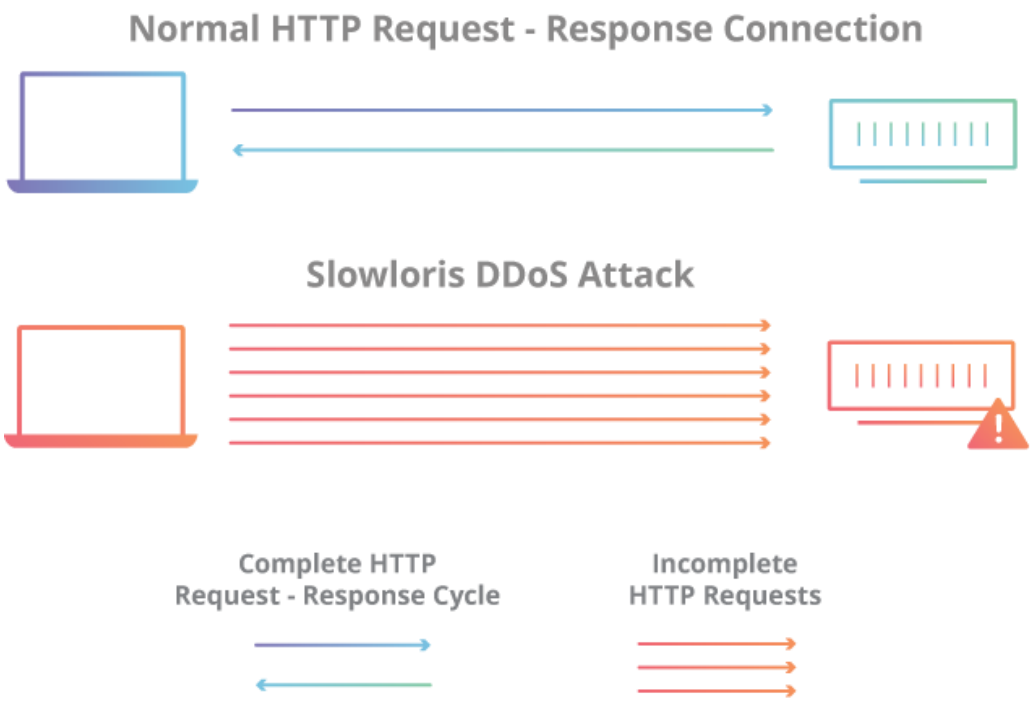
- Ejemplos:
  - Smurf : mediante un ping (ICMP)
  - Fraggle : mediante el servicio de eco (UDP)

Denegación de Servicio



Denegación de Servicio

Una herramienta de ataque es *Slowloris*



Denegación de Servicio

- En el ataque con Slowloris se utilizan peticiones HTTP parciales.
- El atacante abre múltiples conexiones con el servidor por las que manda las cabeceras de las peticiones HTTP.
- El servidor abrirá un thread por cada petición, para cerrarla una vez que la petición se haya respondido. Y si una petición tarda mucho, saltará un timeout y se cerrará el thread.
- El atacante seguirá enviando peticiones parciales en esas conexiones para evitar que se cierren por timeout
- El servidor no es capaz de liberar esos threads. Cuando todos los threads disponibles se estén usando, se creará el DoS.