Ataques Man-in-the-Middle

Grupo 1:

David Cabezas Berrido

dxabezas@correo.ugr.es

Patricia Córdoba Hidalgo

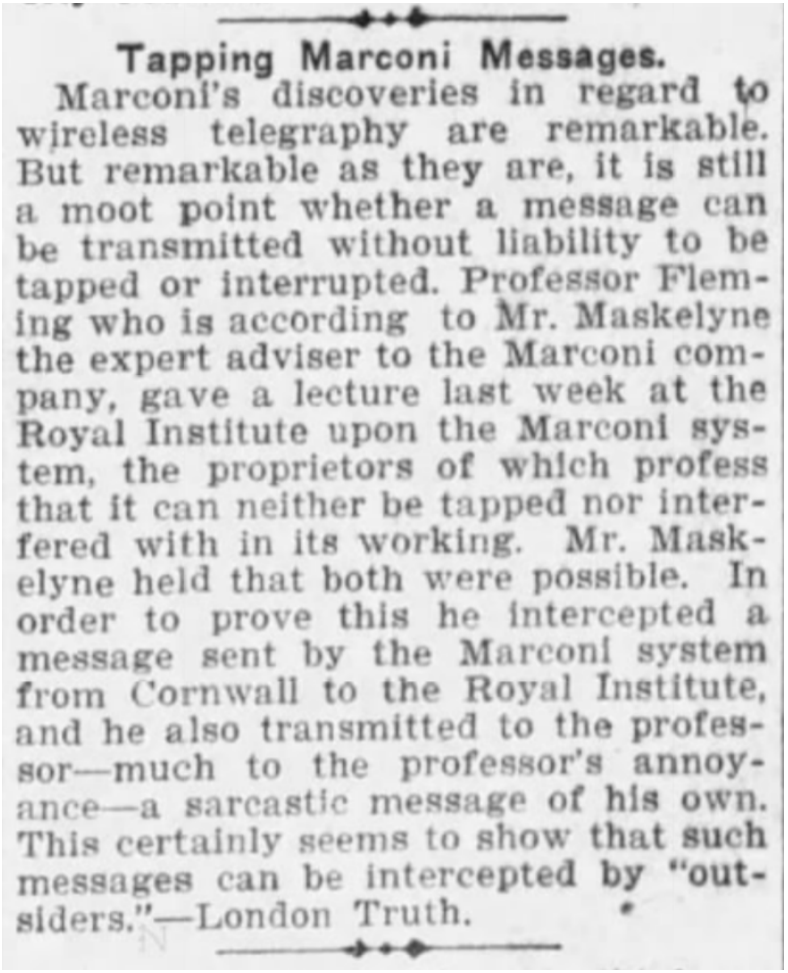
patriciacorhid@correo.ugr.es

Contenido

Contenido

Motivación

Vamos a presentar uno de los ciberataques más comunes en la historia y en la actualidad. Al igual que con otros tipos de ciberataques, conviene estar informado sobre las distintas formas en las que se manifiesta y saber cómo protegerse de él.



Tapping Marconi Messages.

Marconi's discoveries in regard to wireless telegraphy are remarkable. But remarkable as they are, it is still a moot point whether a message can be transmitted without liability to be tapped or interrupted. Professor Fleming who is according to Mr. Maskelyne the expert adviser to the Marconi company, gave a lecture last week at the Royal Institute upon the Marconi system, the proprietors of which profess that it can neither be tapped nor interfered with in its working. Mr. Maskelyne held that both were possible. In order to prove this he intercepted a message sent by the Marconi system from Cornwall to the Royal Institute, and he also transmitted to the professor—much to the professor's annoyance—a sarcastic message of his own. This certainly seems to show that such messages can be intercepted by "outsiders."—London Truth.

Figura: Recorte de periódico: Austin-American Statesman, 17 de julio de 1903.

NSA disguised itself as Google to spy, say reports

If a recently leaked document is any indication, the US National Security Agency -- or its UK counterpart -- appears to have put on a Google suit to gather intelligence.

Figura: Caso Snowden. Se descubrió que la NSA se hacía pasar por Google para robar información.

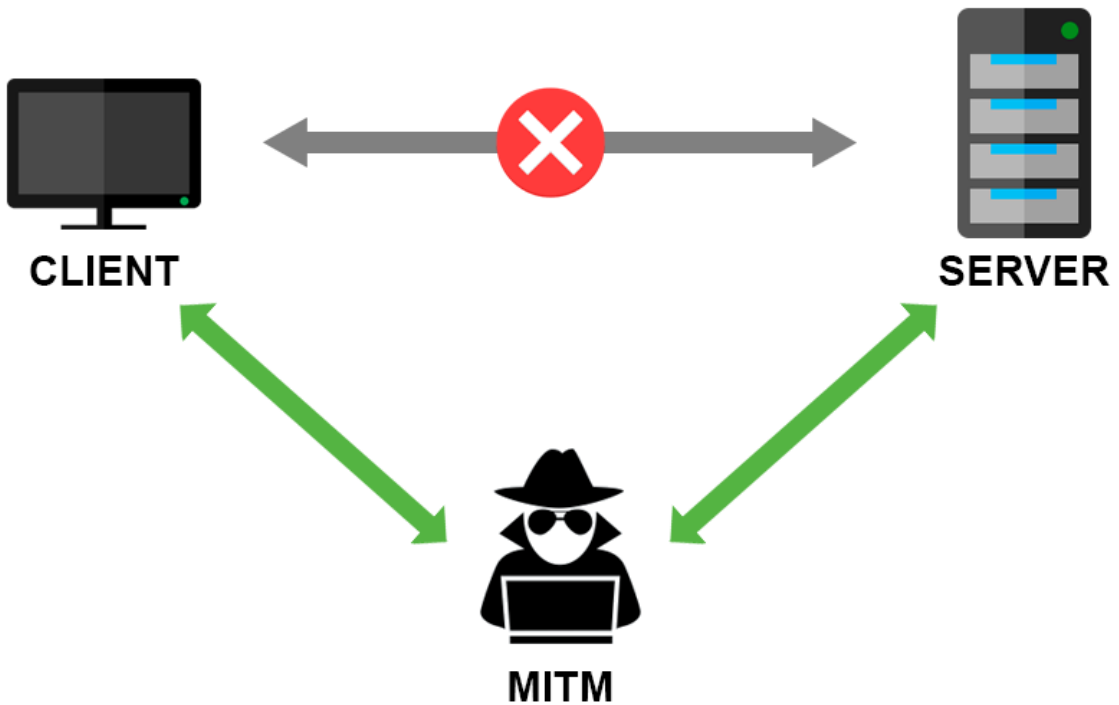
'Fraudsters hacked emails to my solicitor and stole £340,000 from my property sale'

Figura: Robo del pago de una vivienda.

Contenido

Descripción

Los ataques (MITM) son una clase de ciberataques en los que un individuo (el atacante) logra infiltrarse en una comunicación entre dos partes legítimas, de forma que ambas partes ignoran su presencia.



Ejemplo

1. Bob (cliente) quiere conectarse a la web del banco (servidor) para hacer una transferencia de 500€ a la cuenta XXX.

2. Alice (atacante) intercepta la conexión y conduce a Bob a una réplica de la web del banco creada por ella.

3. Bob introduce sus credenciales, que son recibidos por Alice.

4. Alice se conecta a la aplicación del web con los credenciales de Bob.

5. Bob rellena el formulario (falso) para realizar la transferencia.

Ejemplo

6. Alice recibe el formulario y rellena uno (real) para enviar 5000€ a la cuenta YYY, registrada como Bob en la aplicación.

7. Cuando Alice recibe el siguiente mensaje del banco: “Hola Bob, para confirmar su transferencia de 5000€ al número de cuenta YYY, sume los dígitos 1, 2 y 7 de su código secreto e introduzca el resultado”.

8. Alice envía a Bob a través de la aplicación falsa el mensaje: “Hola Bob, para confirmar su transferencia de 500€ al número de cuenta XXX, sume los dígitos 1, 2 y 7 de su código secreto e introduzca el resultado”.

9. Bob envía a Alice la respuesta de seguridad, que Alice utilizará para robarle 5000€.

Inconveniente

Este ataque requiere de un papel muy activo del atacante para que las víctimas no se percaten del engaño.

Si sólo queremos acceder a la información, se puede reenviar a las víctimas de forma automática. Si queremos alterarla, el proceso es menos automatizable.

Inconveniente

Este ataque requiere de un papel muy activo del atacante para que las víctimas no se percaten del engaño.

Si sólo queremos acceder a la información, se puede reenviar a las víctimas de forma automática. Si queremos alterarla, el proceso es menos automatizable.

Contenido

ARP Cache Poisoning

Un atacante envía a los integrantes de la comunicación mensajes en los que indique que la dirección IP del otro integrante corresponde con la dirección física del atacante.

El atacante se infiltra en la conversación haciéndose pasar por ambas víctimas y recibiendo los mensajes que vayan destinados a cualquiera de las víctimas desde la otra.

DNS Cache Poisoning

Un atacante se infiltra en la comunicación entre un usuario y un servidor DNS, para proporcionarle al usuario una entrada DNS falsa que conduce a una página creada por el atacante.

Figura: Esquema de DNS Cache Poisoning. Artículo "A Review of Man-in-the-Middle Attacks", Figura 5.

HTTPS Spoofing

El atacante elabora un página HTTPS con dominio similar y contenido idéntico al de otra página a la que quiere acceder una de sus víctimas.

Por ejemplo, si visitamos el enlace https://www.xn–80ak6aa92e.com veremos que el dominio que aparece en la barra de navegación se asemeja a https://www.apple.com, mientras que el contenido es totalmente distinto y ambas páginas utilizan HTTPS.

Normalmente se utiliza el Phishing para hacer que la víctima haga click en uno de estos enlaces engañosos.

Wi-Fi Eavesdropping

Los atacantes pueden interceptar el tráfico en redes públicas o inseguras, o incluso crear una red WiFi para ver todo el tráfico que circula por ella. Si un usuario escribe sus credenciales, contraseñas, cuentas bancarias o cualquier tipo de información sensible en esa red, el atacante puede robarlas y usarlas en su beneficio.

Session Hijacking

El atacante puede hacerse con la cookie que contiene información relativa a la sesión que se crea al iniciar la comunicación con un servidor web. Así, éste será capaz de navegar por dicha web haciéndose pasar por el usuario.

Contenido

Simulación de ataque MITM con ARP Cache Poisoning

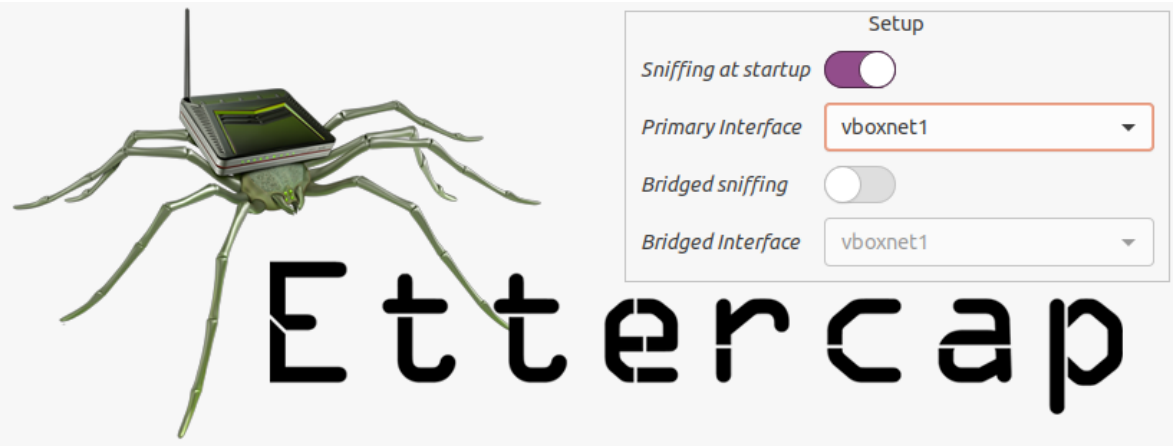
Seguimos el tutorial de: https://www.youtube.com/watch?v=fbXu8EX0hsI.
Tenemos las siguientes máquinas en la red `vboxnet1`.

Host	IP	MAC
Atacante	192.168.57.1	0a:00:27:00:00:01
Cliente	192.168.57.3	08:00:27:01:3a:c8
Servidor	192.168.57.4	08:00:27:6c:b7:f2

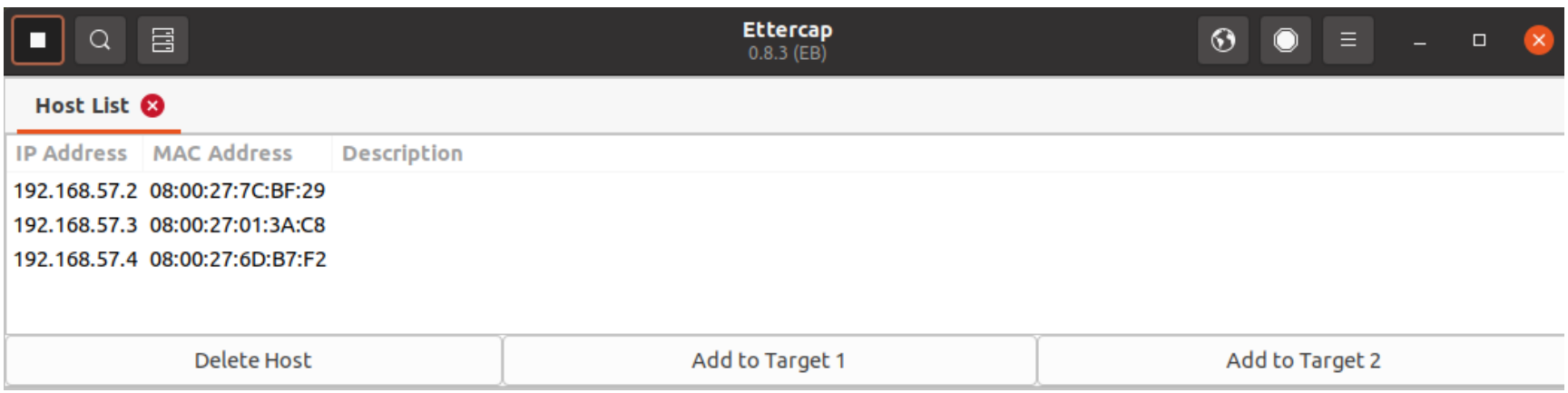
Tenemos que activar la redirección de paquetes en la máquina atacante.
Podemos lograr esto ejecutando la orden

```
sudo sysctl -w net.ipv4.ip_forward=1
```

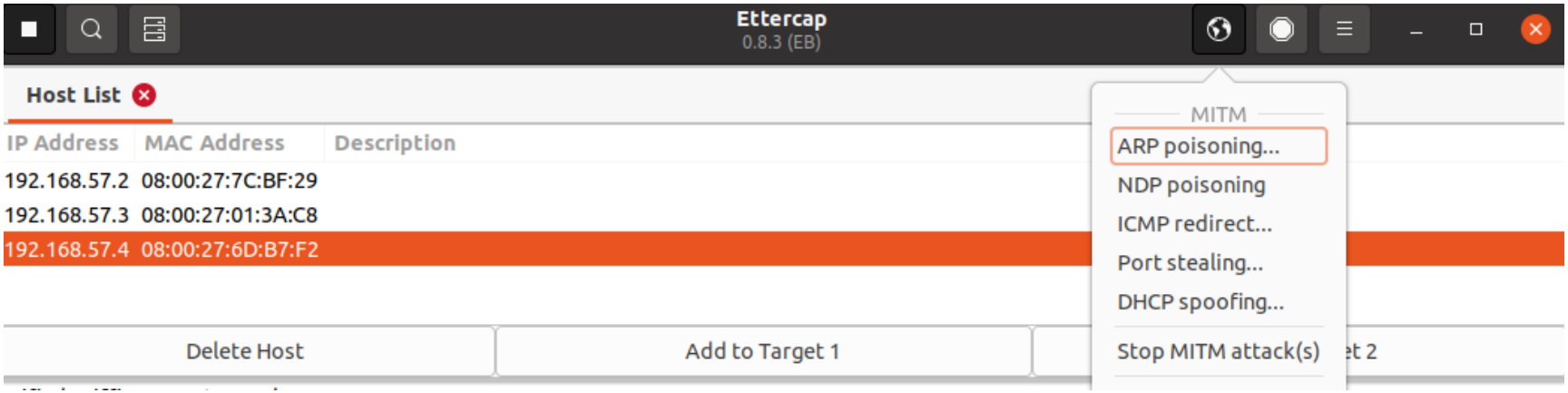
Abrimos Ettercap y seleccionamos la interfaz `vboxnet1`.



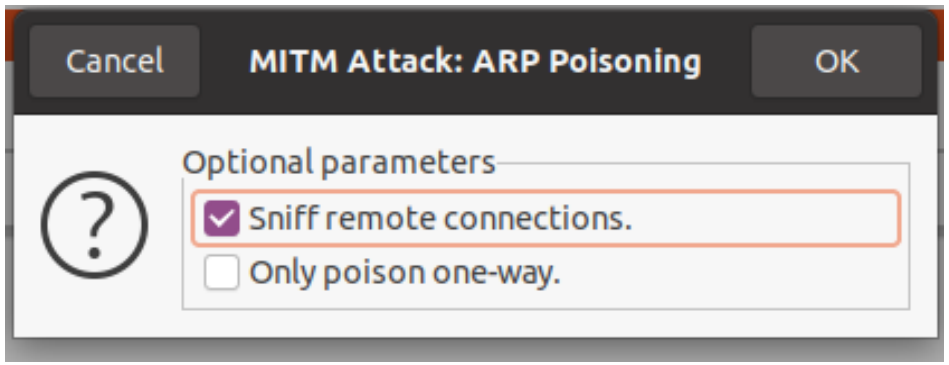
Pulsamos *Scan for hosts* (la lupa) y luego *Hosts List*.



Añadimos 192.168.57.3 (cliente) a Target 1 y 192.168.57.4 (servidor) a Target 2.
Luego pulsamos ARP poisoning en el menú MITM.



Marcamos Sniff remote connections en la ventana emergente que aparece.



Análisis con Wireshark

El atacante envenena la caché de ARP de las víctimas.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	0a:00:27:00:00:01	PcsCompu_01:3a:c8	ARP	42	192.168.57.4 is at 0a:00:27:00:00:01
2	0.000055607	0a:00:27:00:00:01	PcsCompu_6d:b7:f2	ARP	42	192.168.57.3 is at 0a:00:27:00:00:01
3	10.010320904	0a:00:27:00:00:01	PcsCompu_01:3a:c8	ARP	42	192.168.57.4 is at 0a:00:27:00:00:01
4	10.010376009	0a:00:27:00:00:01	PcsCompu_6d:b7:f2	ARP	42	192.168.57.3 is at 0a:00:27:00:00:01

Cuando el cliente hace curl al servidor, obtenemos

7	22.244376349	192.168.57.3	192.168.57.4	TCP
8	22.246721940	192.168.57.3	192.168.57.4	TCP
9	22.247178067	192.168.57.4	192.168.57.3	TCP
10	22.254785765	192.168.57.4	192.168.57.3	TCP
11	22.255176773	192.168.57.3	192.168.57.4	TCP
12	22.255444466	192.168.57.3	192.168.57.4	HTTP
13	22.262782256	192.168.57.3	192.168.57.4	TCP
14	22.262952093	192.168.57.3	192.168.57.4	TCP
15	22.263251390	192.168.57.4	192.168.57.3	TCP
16	22.263828784	192.168.57.4	192.168.57.3	HTTP
17	22.270842201	192.168.57.4	192.168.57.3	TCP
18	22.271018585	192.168.57.4	192.168.57.3	TCP
19	22.271202578	192.168.57.3	192.168.57.4	TCP
20	22.276114728	192.168.57.3	192.168.57.4	TCP
21	22.278912837	192.168.57.3	192.168.57.4	TCP
22	22.279054353	192.168.57.3	192.168.57.4	TCP
23	22.279460501	192.168.57.4	192.168.57.3	TCP
24	22.286886829	192.168.57.4	192.168.57.3	TCP
25	22.287282723	192.168.57.3	192.168.57.4	TCP
26	22.294844833	192.168.57.3	192.168.57.4	TCP

El SYN del cliente al servidor se envía en dos paquetes, pasando por el atacante.

```
  7 22.244376349 192.168.57.3     192.168.57.4     TCP      74 43054 → 80 [SYN] Seq=0 Win=64240
  8 22.246721940 192.168.57.3     192.168.57.4     TCP      74 [TCP Out-Of-Order] 43054 → 80 [S
Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface vboxnet1, id 0
Ethernet II, Src: PcsCompu_01:3a:c8 (08:00:27:01:3a:c8), Dst: 0a:00:27:00:00:01 (0a:00:27:00:00:01)
Internet Protocol Version 4, Src: 192.168.57.3, Dst: 192.168.57.4
Transmission Control Protocol, Src Port: 43054, Dst Port: 80, Seq: 0, Len: 0
```

Las direcciones IP son engañosas. En las direcciones físicas observamos que el atacante hace de intermediario.

```
  7 22.244376349 192.168.57.3     192.168.57.4     TCP      74 43054 → 80 [SYN] Seq=0 Win=64240
  8 22.246721940 192.168.57.3     192.168.57.4     TCP      74 [TCP Out-Of-Order] 43054 → 80 [S
Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface vboxnet1, id 0
Ethernet II, Src: 0a:00:27:00:00:01 (0a:00:27:00:00:01), Dst: PcsCompu_6d:b7:f2 (08:00:27:6d:b7:f2)
Internet Protocol Version 4, Src: 192.168.57.3, Dst: 192.168.57.4
Transmission Control Protocol, Src Port: 43054, Dst Port: 80, Seq: 0, Len: 0
```

Lo mismo ocurre con cada paquete del proceso de comunicación.

```
 16 22.263828784 192.168.57.4  192.168.57.3  HTTP     351 HTTP/1.1 200 OK  (text/html)
 17 22.270842201 192.168.57.4  192.168.57.3  TCP       66 80 → 43054 [ACK] Seq=1 Ack=77 Wi
 18 22.271018585 192.168.57.4  192.168.57.3  TCP      351 [TCP Retransmission] 80 → 43054
Frame 16: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface vboxnet1, id 0
Ethernet II, Src: PcsCompu_6d:b7:f2 (08:00:27:6d:b7:f2), Dst: 0a:00:27:00:00:01 (0a:00:27:00:00:01)
Internet Protocol Version 4, Src: 192.168.57.4, Dst: 192.168.57.3
Transmission Control Protocol, Src Port: 80, Dst Port: 43054, Seq: 1, Ack: 77, Len: 285
```

En partircular, la respuesta del servidor pasa por el atacante.

```
 16 22.263828784 192.168.57.4  192.168.57.3  HTTP     351 HTTP/1.1 200 OK  (text/html)
 17 22.270842201 192.168.57.4  192.168.57.3  TCP       66 80 → 43054 [ACK] Seq=1 Ack=77 Wi
 18 22.271018585 192.168.57.4  192.168.57.3  TCP      351 [TCP Retransmission] 80 → 43054
Frame 18: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface vboxnet1, id 0
Ethernet II, Src: 0a:00:27:00:00:01 (0a:00:27:00:00:01), Dst: PcsCompu_01:3a:c8 (08:00:27:01:3a:c8)
Internet Protocol Version 4, Src: 192.168.57.4, Dst: 192.168.57.3
Transmission Control Protocol, Src Port: 80, Dst Port: 43054, Seq: 1, Ack: 77, Len: 285
```

Contenido

Conclusiones

Esperamos haber concienciado sobre la facilidad con la que se puede ser víctima de este tipo de ataques, así como de la gravedad que pueden llegar a tener.

A continuación, ofrecemos una serie de consejos y buenas prácticas para prevenir o percatarse de estos ataques.

Consejos y buenas prácticas

- Evitar el uso de redes Wi-Fi públicas y sin contraseña.
- Evitar hacer logins desde redes públicas como las de cafeterías o bibliotecas.
- Evitar navegar en sitios web que no utilicen protocolo HTTPS.
- Usar varios factores de autenticación.

Consejos y buenas prácticas

- Utilizar algún protocolo de cifrado y firma para intercambiar mensajes importantes.
- Cerrar la sesión en páginas antes de cerrarlas.
- Seguir el principio de confianza cero: No aceptar conexiones hasta verificar su procedencia.

Indicios de que estamos siendo víctimas de un ataque MITM

- Experimentamos retrasos en la comunicación, o desconexiones inesperadas.
- Aparecen direcciones extrañas en nuestra barra de navegación.
- Tenemos conexiones a sitios desconocidos.

Cómo actuar caso de sospecha

- Monitorizar la actividad de red con Wireshark o similares.
- Inspeccionar las conexiones actuales.
- Usar un network sniffer (una herramienta para espiar tráfico) de forma defensiva.
- Buscar software malicioso en nuestro equipo.

Contenido

Bibliografía

Ataque MTIM en demostración de Marconi.

1. https://havocshield.com/2020/07/cybersecurity-history-the-very-first-man-in-the-middle-attack.
2. https://www.bbc.com/mundo/noticias/2016/05/160523_primer_hacker_caballero_victoriano_marconi_fleming_maskelyne_finde_dv.

Ejemplos notables.

4. Escándalo de la NSA: https://www.cnet.com/news/nsa-disguised-itself-as-google-to-spy-say-reports.
5. Estafa a la familia Lupton: https://www.conveyancingassociation.org.uk/fraudsters-hacked-emails-to-my-solicitor-and-stole-340000-from-my-property-sale-a-case-study-from-ca-affiliate-members-lawyer-checker.

Bibliografía

Ataque MITM: Explicación y tipos.

6. What is a MITM Attack, Detection and Prevention Tips: https://www.varonis.com/blog/man-in-the-middle-attack.
7. A Review of Man-in-the-Middle Attacks: https://arxiv.org/pdf/1504.02115.pdf.
8. Punycode alert: https://github.com/yabirgb/punycodeAlert.

Cifrado y firma para evitar ataques MITM.

9. Asignatura Seguridad y Protección de Sistemas Informáticos. Apuntes del profesor Francisco Miguel García Olmedo.

Bibliografía

Simulación.

10. Redirección de paquetes: https://www.garron.me/es/gnu-linux/habilitar-ip-forward-linux-ubuntu.html.
11. Tutorial YouTube: https://www.youtube.com/watch?v=fbXu8EX0hsI.

Consejos para evitar ser víctimas del ataque.

12. What is a MITM Attack, Detection and Prevention Tips: https://www.varonis.com/blog/man-in-the-middle-attack.
13. Zero Trust: https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html.