UNIVERSIDAD
DE GRANADA

ATAQUE ‘MAN IN THE MIDDLE’

Elena Mª Gómez Ríos
Nazaret Román Guerrero
Guillermo Sandoval Schmidt

ÍNDICE

SWAP · ATAQUE ‘MAN IN THE MIDDLE’

INTRODUCCIÓN

ATAQUE ‘MAN IN THE MIDDLE’

INTRODUCCIÓN

SWAP · ATAQUE ‘MAN IN THE MIDDLE’

¿QUÉ ES?

La base principal del ataque es interceptar la comunicación entre un cliente-cliente o un cliente-servidor sin que se percaten del ataque, para sustraer o modificar la información interceptada.

SOFTWARE UTILIZADO

ATAQUE ‘MAN IN THE MIDDLE’

SOFTWARE UTILIZADO

SWAP · ATAQUE ‘MAN IN THE MIDDLE’

Para la demo, nosotros hemos utilizado Kali Linux, ya que cuenta con las aplicaciones como Ettercap para realizar de manera sencilla y rápida un ataque MITM.

WireShark, mitmAP, Bettercap, MITMProxy, Evilgrade, Hamster o Ferret

DEFENSA ANTE ATAQUES MITM

ATAQUE ‘MAN IN THE MIDDLE’

DEFENSA ANTE ATAQUES MITM

SWAP · ATAQUE ‘MAN IN THE MIDDLE’

Claves públicas y claves secretas

Mantener actualizado el software

Utilizar técnicas biométricas

No utilizar redes públicas, utilizar redes privadas

Evitar descargar software sospechoso (Malware)

Usar canales seguros (HTTPS)

MITM FAMOSOS

ATAQUE ‘MAN IN THE MIDDLE’

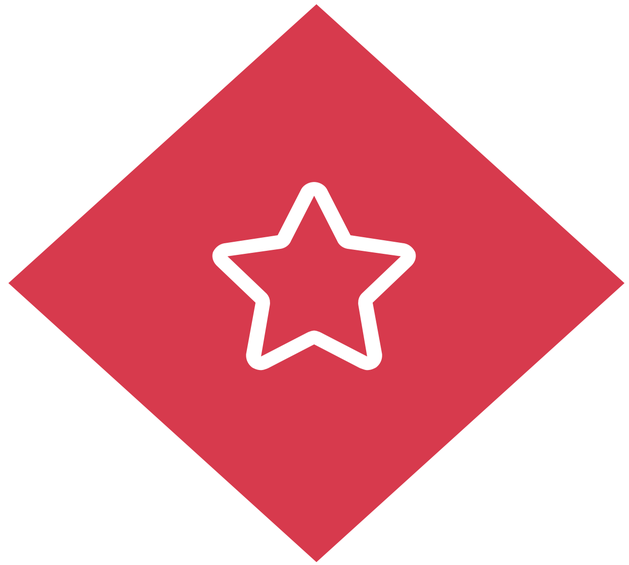
MITM FAMOSOS

SWAP · ATAQUE ‘MAN IN THE MIDDLE’

En 2016, una joven española estafó 6.500€ a una empresa al cambiar el número de cuenta del destinatario de una transferencia de la misma.

En 2015, 49 personas eran detenidas en Europa por estafar 6.000.000€ a bancos europeos utilizando el mismo método anteriormente citado.

Quizás uno de los casos más conocidos de ataque MITM y que fue destapado por Edward Snowden, fue el perpetrado por la Agencia Nacional de Seguridad Estadounidense, que simulaba los servicios de búsqueda de Google para recolectar datos de los usuarios.

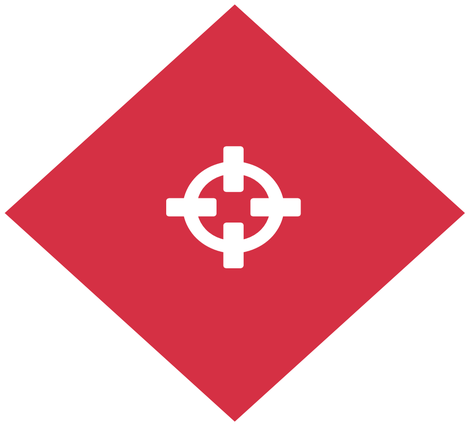


DEMOSTRACIÓN

ATAQUE ‘MAN IN THE MIDDLE’

DEMOSTRACIÓN

SWAP · ATAQUE ‘MAN IN THE MIDDLE’



Veamos un ejemplo...

BIBLIOGRAFÍA

ATAQUE ‘MAN IN THE MIDDLE’

BIBLIOGRAFÍA

SWAP · ATAQUE ‘MAN IN THE MIDDLE’

- https://en.wikipedia.org/wiki/Man-in-the-middle_attack
- https://en.wikipedia.org/wiki/Entropy_(information_theory)
- http://www.cursodehackers.com/ManInTheMiddle.html
- https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html
- https://www.cnet.com/news/nsa-disguised-itself-as-google-to-spy-say-reports/
- https://nakedsecurity.sophos.com/es/2015/06/11/49-busted-in-europe-for-man-in-the-middle-bank-attacks/
- https://navarra.elespanol.com/articulo/sucesos/detenida-pamplona-joven-19-anos-estafar-6-500-euros-empresa/20160513113625041253.html

GRACIAS POR SU ATENCIÓN

Repositorios

https://github.com/ElenaMGR/SWAP
https://github.com/nazaretrogue/SWAP
https://github.com/Gsandoval96/SWAP-UGR