Tipos de ataques .Como actúan los piratas informáticos

SWAP

Juan Manuel López Castro
Ignacio Pineda Mochón

1. Ataque Informático

1. Ataque Informático

Un ciberataque es un método por el cual un individuo,mediante un sistema informático, intenta tomar el control , desestabilizar o dañar otro sistema informático

2.Tipos de ataques informáticos

2.Tipos de ataques informáticos

1. Cartoneo
2. DoS
    2.1. Ping Flood
3. ARP Spoofing
4. Escaneo de Puertos
    4.1. Formas de limitar la informacion dada en los puertos
5. Man-In-The-Middle
6. Ataques de secuencia TCP
    6.1. Cómo prevenirlos

Cartoneo

Cartoneo

-Sencillo

-Astuto

-Eficaz

DoS

-Causa que un servicio o recurso sea inaccesible

-Provoca la pérdida de la conectividad con la red por el consumo del ancho de banda

-Se generan mediante la saturación de los puertos

-Hace que el servidor se sobrecargue y no pueda prestar servicio

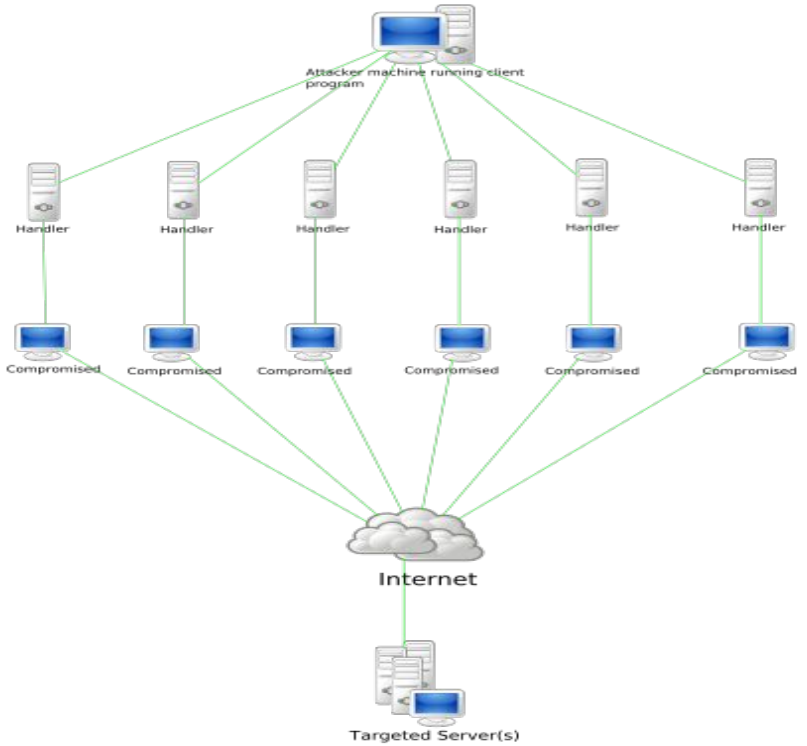
DoS

-Causa que un servicio o recurso sea inaccesible

-Provoca la pérdida de la conectividad con la red por el consumo del ancho de banda

-Se generan mediante la saturación de los puertos

-Hace que el servidor se sobrecargue y no pueda prestar servici



DoS

Los síntomas de sufrir un ataque de denegación de servicio son:

- Rendimiento de la red inusualmente lento (abrir archivos o acceder a sitios web)
- Indisponibilidad de un sitio web en particular
- Incapacidad para acceder a cualquier sitio web

Ping de la Muerte

Ping de la Muerte

-Ping

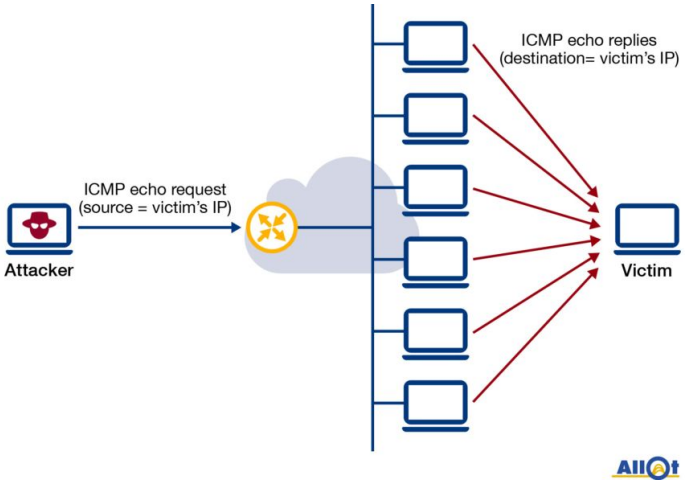
-ICMP > 64B

-Fragmentar paquete

-"Explota" en destino (buffer)

Ping Flooding

Ping Flooding



-Ping

-Múltiples paquetes ICMP

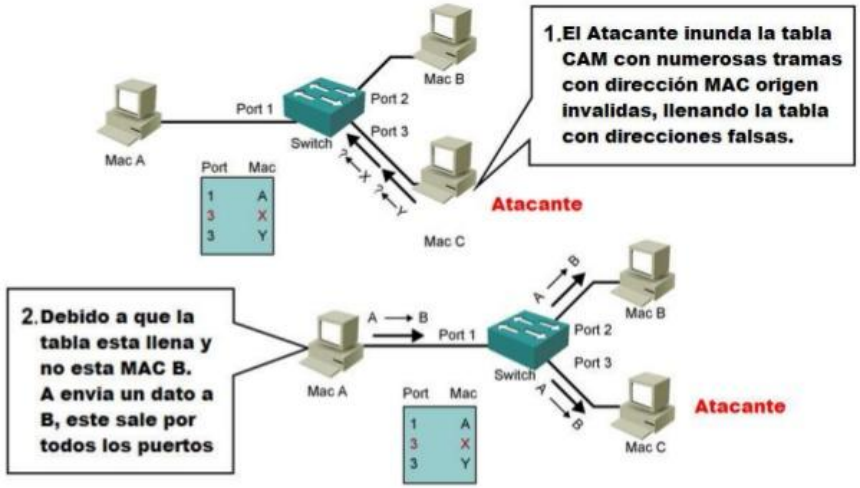
-Dificultad recepción

-Ancho de Banda

-Delegar/ordenar ataque

ARP Spoofing

ARP Spoofing



-Inundación MAC

-Múltiples paquetes + MACs diferentes

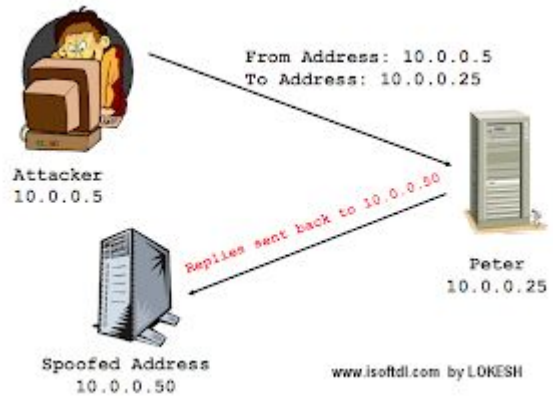
-Memoria llena

-Apertura fallida (como HUB)

-Recepción y análisis paquetes

ARP Spoofing

ARP Spoofing



-IP Spoofing

-IP falsa

-Ocultar identidad

-Falsificar identidad

-Acceso restringido

-No es posible el TCP “Handshake”

Escaneo De Puertos

-Es utilizada para descubrir los servicio expuestos a posibles ataques.

-Un escaneo de puertos ayuda al atacante a encontrar los puertos que están disponibles

-Puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos

-Nmap es una herramienta que ofrece esta utilidad , y está disponible para Linux y Windows

Escaneo De Puertos

-Es utilizada para descubrir los servicio expuestos a posibles ataques.

-Un escaneo de puertos ayuda al atacante a encontrar los puertos que están disponibles

-Puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos

-Nmap es una herramienta que ofrece esta utilidad , y está disponible para Linux y Windows

Escaneo De Puertos

Formas de limitar la información dada por los puertos:

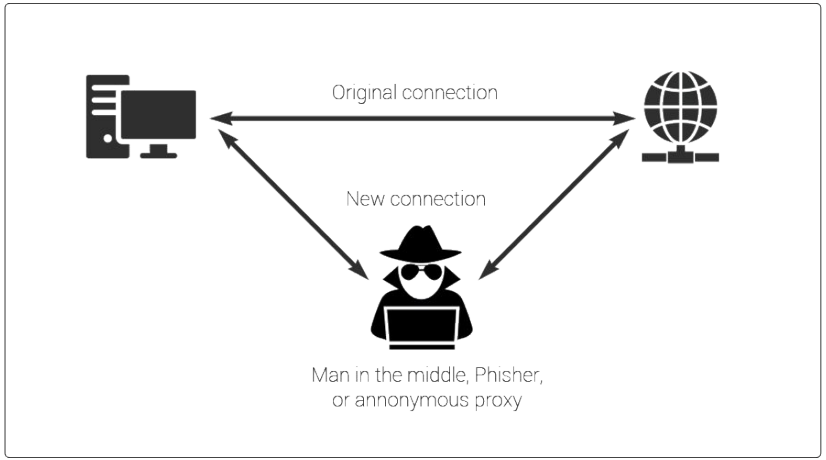
-Cerrar los servicios innecesarios en los sistemas destino

- Utilizar PortSentry, que detecta las solicitudes de conexión en una serie de puertos

-Se puede seleccionar qué puertos escuchara y la cantidad de solicitudes no válidas

Man-In-The-Middle

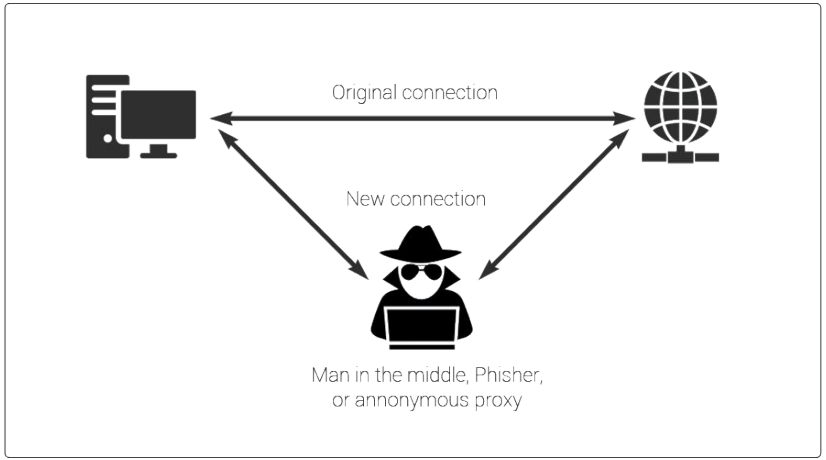
Man-In-The-Middle



-LAN

-Internet

Man-In-The-Middle



-LAN

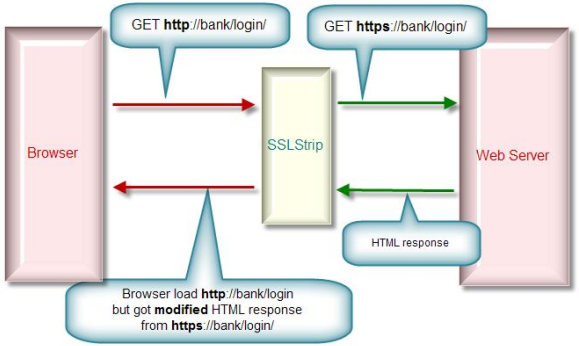
-Envenenar tabla ARP

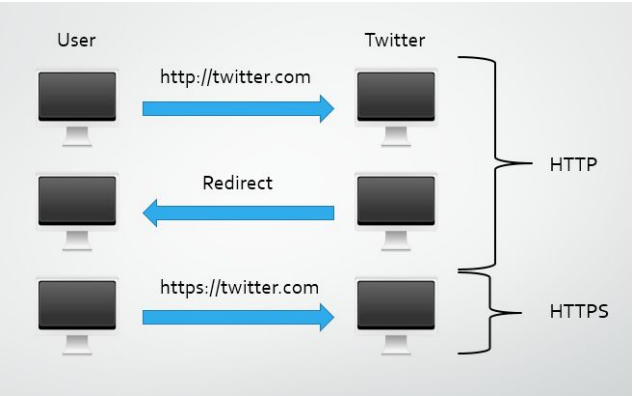
-Gateway falso

-Obtener información

-Inyectar script

Man-In-The-Middle





-Cifrado

-SSLStrip

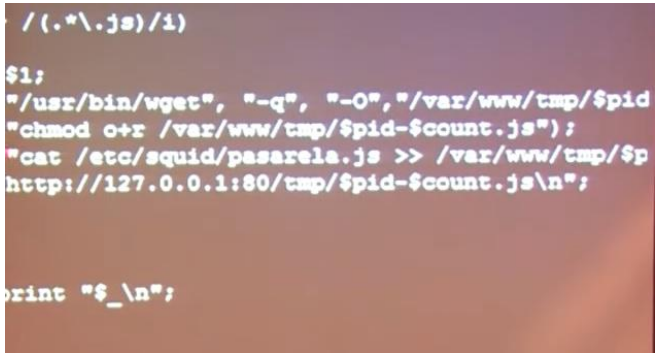
-Cambiar HTTPs por HTTP entre victima y atacante

-Navegador impide: HSTS

-SSLStrip2

-Caducar entradas HSTS ↠ 1 petición HTTP

Man-In-The-Middle



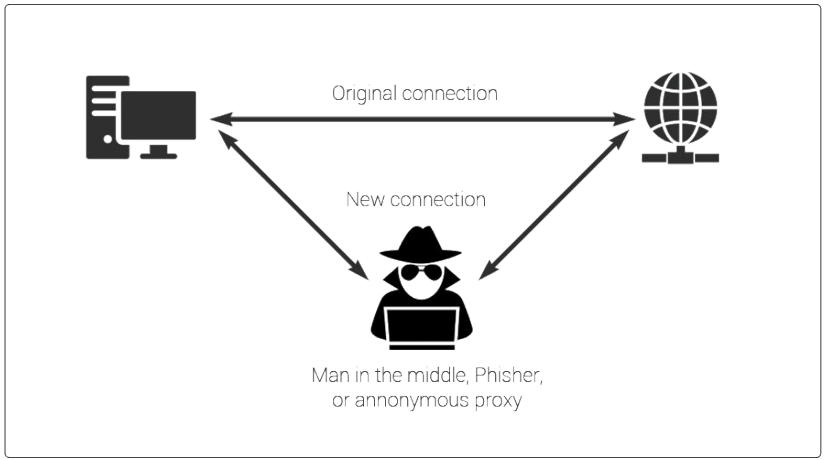
-Troyano

-JavaScript modificado

-Extensión Navegador

-WiFi falsa

Man-In-The-Middle



-Internet

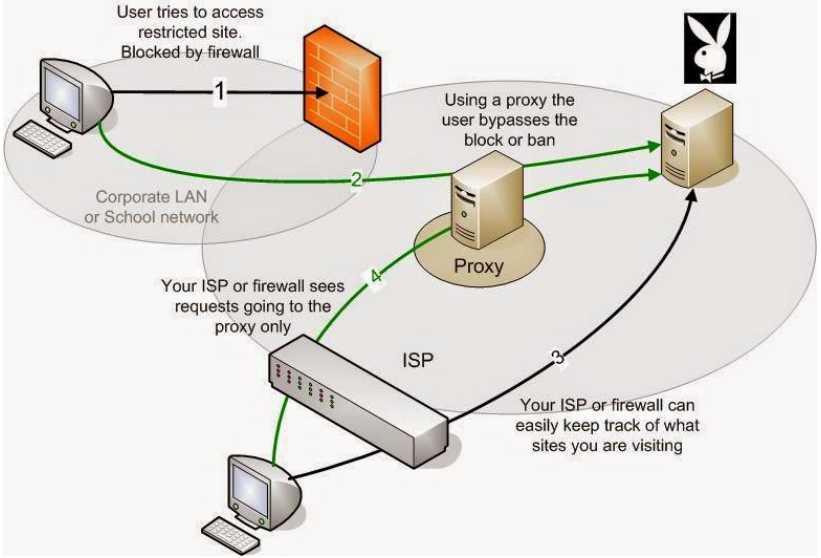
-DoubleDirect

-ICMP redirect

-DNS falso

-WEB falsa (propia)

Man-In-The-Middle



-Proxy

-Conexión anónima

-Hackear Hackers

-Obtener información

-Inyectar scripts

Ataque de secuencia TCP

-Es un intento de predecir el número de secuencia utilizado para identificar los paquetes en TCP

-El atacante monitoriza el flujo de datos entre dos host

-Tumba el host que no le interesa y prepara un paquete TCP “falso” con el número de secuencia esperado

-El paquete entregado puede servir para :

-Obtener acceso a la comunicación

-Entregar una carga maliciosa

Ataque de secuencia TCP

-Es un intento de predecir el número de secuencia utilizado para identificar los paquetes en TCP

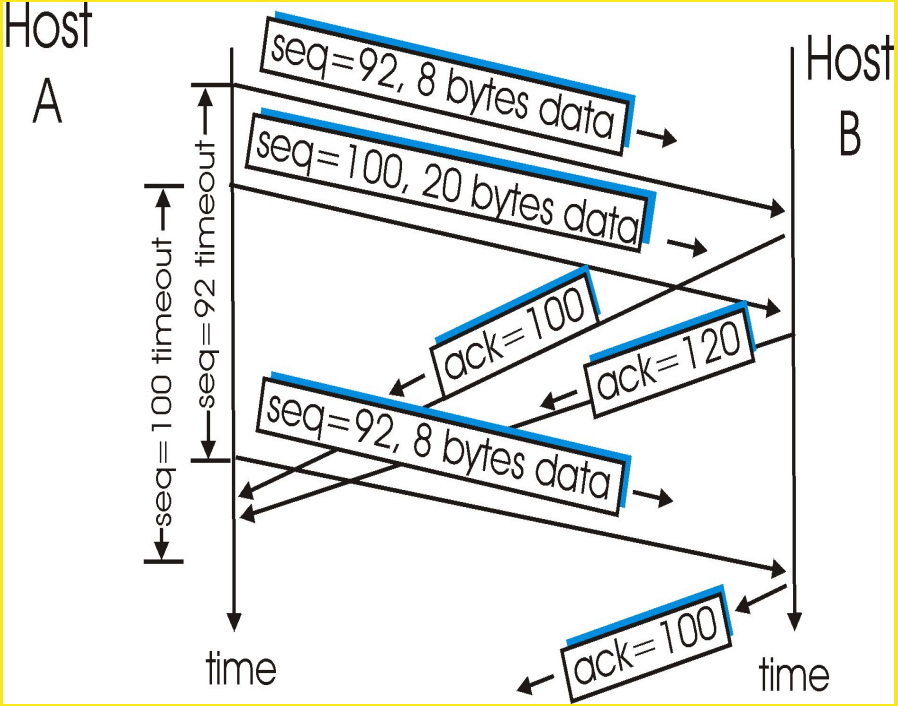
-El atacante monitoriza el flujo de datos entre dos host

-Tumba el host que no le interesa y prepara un paquete TCP “falso” con el número de secuencia esperado

-El paquete entregado puede servir para :

-Obtener acceso a la comunicación

-Entregar una carga maliciosa



Ataque de secuencia TCP

Como prevenir estos ataques:

Ataque de secuencia TCP

Como prevenir estos ataques:

-Información como difernecia de tiempo o informacion de capas bajas de protocolos

-Configurar un router o un firewall para no permitir que entren paquetes de una fuente externa , con Ip interna

CASOS REALES

ZIMPERIUM. Industry Leadership Products Solutions

devices:
Google, Facebook, Twitter, Hotmail, Live.com, Naver.com (Korean) and others. Since the attack is happening on the IPs that the user access – it does not necessarily mean that the attacker had visibility to encrypted traffic that some of the above services are enforcing. We identified attacks across 31 countries, outlined below:

- Serbia
- Australia
- Iraq
- Kazakhstan
- Poland
- Indonesia
- Israel
- Latvia
- Finland
- Mexico
- Egypt
- United Kingdom
- Austria
- Colombia
- Greece
- Brazil
- Canada
- France
- Algeria
- Russian Federation
- Switzerland
- Italy
- Germany
- Spain
- Saudi Arabia
- Netherlands
- India
- Malta

Ledger es una cartera de criptomonedas en formato hardware que soporta varias divisas, entre ellas las populares Bitcoin y Ethereum. Días atrás se halló en ese dispositivo una **vulnerabilidad que abre la puerta a ataques de tipo *man-in-the-middle***, pudiendo los atacantes robar el dinero de la víctima.

La empresa reconoció la existencia del fallo de seguridad el pasado 3 febrero, del cual se publicó un documento PDF en DocDroid. Mediante su explotación, un actor malicioso podría **suministrar a los clientes direcciones de recibo falsas, desviando así el dinero enviado por la víctima** hacia las carteras de los atacantes en lugar del verdadero destinatario. El investigador que descubrió el problema no se ha identificado.

El ataque DDoS más grande registrado que afectó a sitios como Twitter, Spotify, Netflix, GitHub y Amazon

in noticias by claudia morales 24 octubre, 2016 0 comments

El 21 de octubre, la compañía DYN de gestión de rendimiento de Internet con sede en New Hampshire sufrió el ataque DDoS más grande registrado hasta el momento.

Los ataques fueron tres, en una sucesión relativamente rápida, siendo el último mitigado fácilmente. Se orientaron a la infraestructura DNS gestionado de la compañía. Esto causó la inaccesibilidad temporal de muchos sitios web y servicios en línea como Twitter, Spotify, Netflix, Amazon, GitHub, PayPal, Etsy, entre otros.

Lo que dice Dyn acerca de los ataques

"En este momento sabemos que fue un ataque sofisticado y altamente distribuido que involucró 10s millones de direcciones IP. Estamos llevando a cabo un análisis de las causas y análisis forense, e informar lo que sabemosmane

La Fatal Mirai

De acuerdo a Flashpoint, las redes de bots Mirai que se utilizaron en el ataque contra el Dyn "fueron botnets separadas y distintas" de las que se utilizaron para ejecutar los ataques DDoS contra el blog de Brian Krebs, y el servicio francés de internet OVH.

"A principios de este mes, 'Anna_Senpai," el hacker que opera la gran botnet Mirai utilizado en el Krebs DDoS, liberó el código fuente de Mirai en línea. Desde esta versión, otros cibercriminales han utilizado el malware para crear sus propias redes de bots con el fin de lanzar ataques DDoS".

Mirai aumenta fácilmente infectando dispositivos en su mayoría routers, DVR o cámaras WebIP, servidores Linux y dispositivos IoT funcionando con Busybox. Si sus propietarios no toman medidas para protegerlos, van a terminar infectados nuevamente en cuestión de minutos.

Desafortunadamente, algunos de estos dispositivos no pueden ser protegidos como deberían por causa de contraseñas codificadas, y el hecho de que sus fabricantes no hicieron posible su actualización.

Por el momento, la solución a este problema en particular todavía no está claro, aunque algunas propuestas en boca, incluyen la opción de "hackear e vuelta" para ganar el control de los dispositivos comprometidos. A medida que el número de dispositivos del IoT comprometidos se eleva, esta opción es seriamente considerada.

Bibliografía

http://martra.uadla.com/como-hacer-un-man-in-the-middle-con-sslstrip-asi-se-roban-las-contrasenas/

https://hipertextual.com/archivo/2014/06/ataque-man-in-the-middle/

http://www.ebankingnews.com/noticias/que-es-man-in-the-browser-el-nuevo-tipo-de-troyano-que-ataca-a-la-banca-006263

https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/

https://blog.zimperium.com/doubledirect-zimperium-discovers-full-duplex-icmp-redirect-attacks-in-the-wild/

https://www.youtube.com/watch?v=wjTjzXKpCWw

https://es.wikipedia.org/