



Captura y análisis de tráfico de red

Guillermo Román - hartek
HoneyCON 2017

Y tú, ¿qué música escuchas?



Acerca de mí

Guillermo Román Ferrero

@Guille_Hartek

- Graduado en **Ingeniería Informática** (mención TI) por UVA.
- **Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones** por la UEM.
- **Analista de Protocolos de Red y Seguridad** en Excem Technologies.
- Cofundador y coautor del blog **Follow the White Rabbit**
(<https://www.fwhibbit.es>)
 - Seguridad, privacidad y hacking ético
 - Premio Bitácoras 2016 al mejor blog de seguridad informática.





Introducción - ¿De qué va este taller?

- ¿Te has preguntado alguna vez cómo de fácil es obtener tu tráfico de red?
- De paso, ¿y cómo de fácil es extraer información del mismo?
- Existe una gran cantidad de métodos de obtención de capturas de tráfico.
- Existen tanto herramientas comerciales/gratuitas como métodos de *scripting* que nos permiten realizar un análisis de estas capturas y extraer la información.
- En este taller tendremos:
 - Una breve introducción a las razones por las que alguien podría capturar tráfico.
 - Una descripción y pequeñas demostraciones de algunos métodos de obtención de capturas.
 - Un análisis mediante herramientas de una captura de tráfico.
 - Un análisis mediante *scripts* de una captura de tráfico.

Obtención de capturas de tráfico

- Existe una gran cantidad de métodos para capturar el tráfico, tantos como razones para hacerlo.
- ¿Razones?
 - De forma lícita: Monitorización de redes, redirección a IDS/IPS mediante mirroring, análisis de protocolos, ingeniería reversa.
 - De forma ilícita: Espionaje de redes WiFi, espionaje industrial, perfilado no autorizado de usuarios, obtención de credenciales, servicio VPN maligno.



Obtención de capturas de tráfico

- Métodos usuales para la obtención de capturas de tráfico:
 - Espionaje de redes inalámbricas.
 - Intervención del cableado (*network tap*).
 - *Port mirroring*.
 - Suplantación y ataques *Man in the Middle* (*ARP spoofing*, *DNS spoofing*).
 - Punto de acceso falso (*Rogue AP*) o equivalentes en telefonía móvil.
 - Proxies y VPNs malignas.



Captura de tráfico en redes inalámbricas

- En redes sin cifrado, [el proceso es trivial](#). Toda la información viaja desprotegida en el aire.
- En redes con cifrado WEP, la información se cifra con una clave común (la de autenticación a la red). Quien la conozca, podrá descifrar el tráfico.
- En redes con cifrado WPA/2, existen técnicas para descifrar el tráfico ([KRACK](#)).



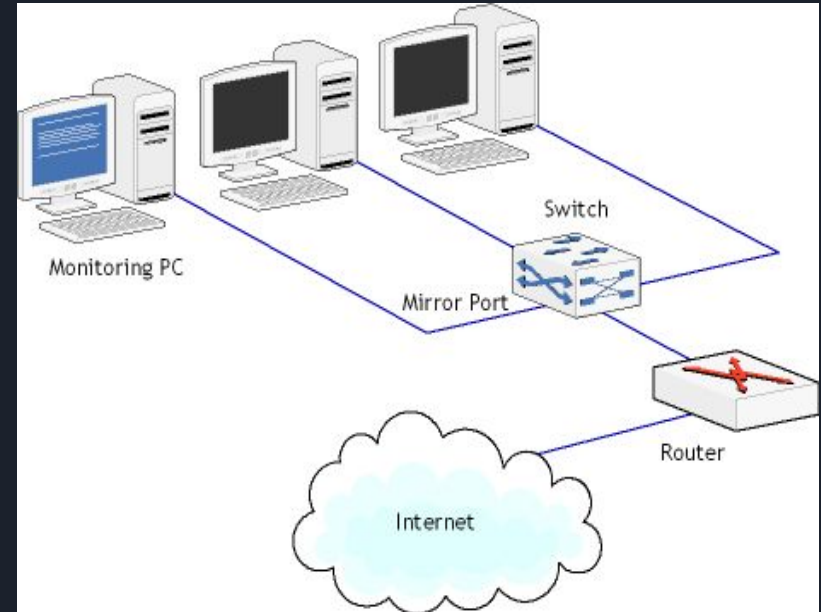
Captura de tráfico con intervención del cableado

- Se hace uso de dispositivos llamados *network tap*.
- Este dispositivo pasivo permite duplicar el tráfico que pasa por un cable de red y dirigirlo a un dispositivo a la escucha.
- Es “invisible”, dado que trabaja a nivel eléctrico (capa física).
- Muy sencillo de [fabricar de forma casera](#).
- Limita la velocidad a 100 Mbps.



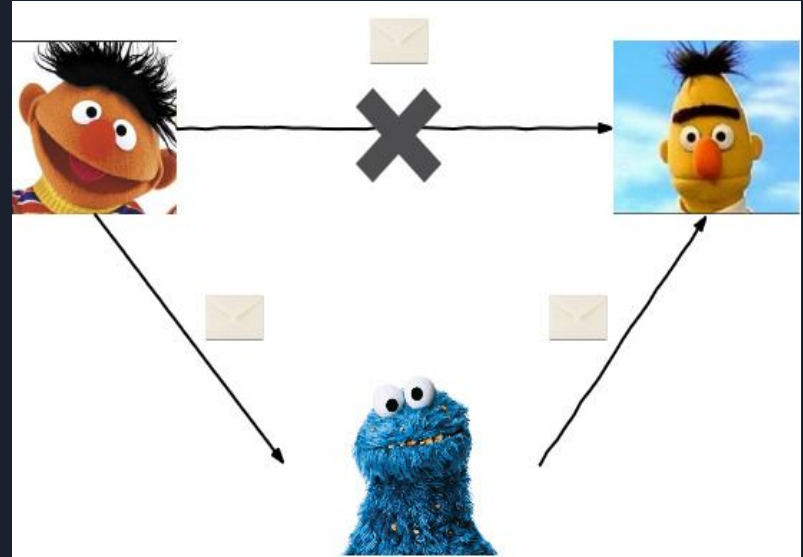
Captura de tráfico con *port mirroring*

- Se configura uno de los puertos de un *switch* de manera que repita por él los paquetes que pasen por uno o varios de sus otros puertos.
- Se tiene una copia exacta del tráfico de una red local.
- Utilizado normalmente para tareas de monitorización e implementación de sistemas IPS/IDS.



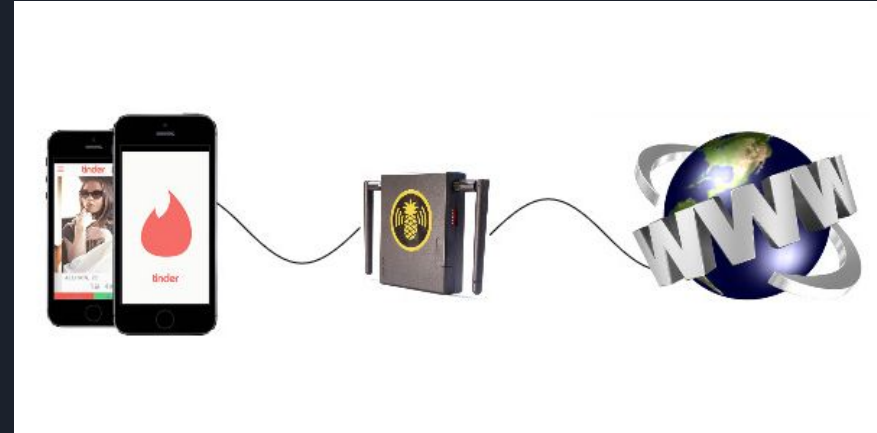
Captura de tráfico mediante suplantación y *Man in the Middle*

- Se utilizan técnicas de *hacking* de comunicaciones para suplantar otro *host* o cualquier servicio.
- Se intenta que el tráfico entre dos puntos pase por nosotros (el atacante) antes de ser reenviado al destinatario verdadero.
- Técnicas muy variadas:
 - *ARP Poisoning*.
 - *DNS Spoofing*.
 - Clonado de páginas.
 - *SSL Strip*, *Delorean*.



Captura de tráfico mediante punto de acceso falso (*Rogue AP*)


- Colocamos un punto de acceso, protegido o desprotegido, que guardará una copia de todo el tráfico que pase por él.
- Muy fácilmente fabricable mediante una Raspberry Pi o similares, o temporalmente mediante software.
- WiFi Pineapple.
- Variantes:
 - Evil Twin.
 - Equivalentes en redes móviles.



Proxies y VPNs malignas

- Un proveedor de servicio Proxy o VPN puede potencialmente guardar y analizar todo el tráfico.
- Caso parecido al punto de acceso falso.
- ¿VPNs gratuitas?
- Se han dado casos en los que un servicio VPN ha monitorizado sin permiso el tráfico de usuarios.



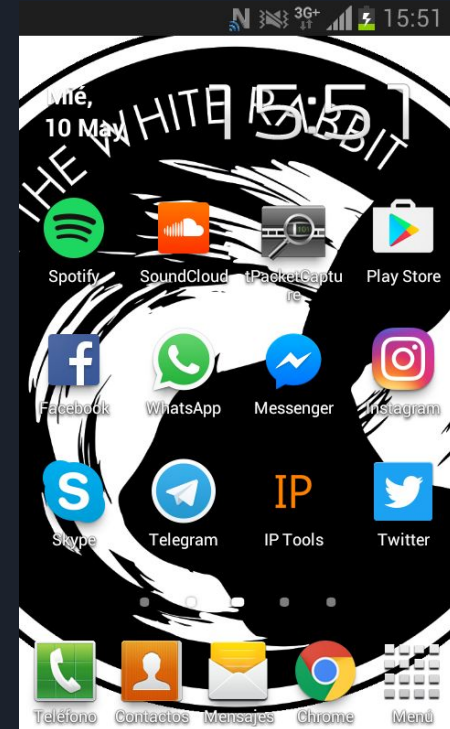


Análisis de una captura - ¿Qué pasa por mi teléfono?

- Por un teléfono móvil circula una cantidad enorme de información, **cifrada y no cifrada**.
 - Las aplicaciones que cifran mis datos, **¿cómo lo hacen?**
 - Dichas aplicaciones, ¿cifran **todos** mis datos?
 - Mis datos no cifrados, ¿son **fácilmente recuperables?**
 - Mis datos cifrados, ¿pueden aun así **revelar información?**
- En este taller aprenderemos a:
 - Enfrentarnos a una captura de red extraída de un **dispositivo móvil**.
 - Filtrar y extraer información de forma manual con **Wireshark**.
 - Filtrar y extraer información de forma manual mediante **scripts de Python**.

Análisis de una captura

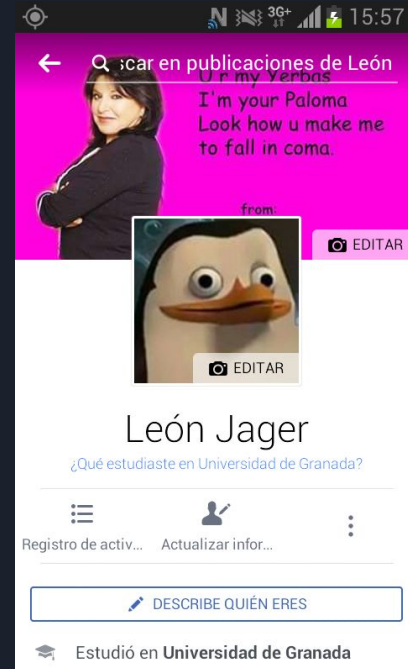
- Equipo capturado: Samsung Galaxy Ace 2.
 - Android 4.1.2.
 - Actualizado 9 Mayo 2017.
- Tarjeta prepago Orange.
- Para la captura del tráfico:
 - Aplicación TPacketCapture.
 - Punto de acceso falso.



Análisis de una captura

- Identidad falsa: León Jager Jasyp.
- Cuentas en diversos servicios y redes sociales:
 - Gmail
 - Twitter
 - Facebook
 - Instagram
 - ...
- ¿Dar mis datos? ¿Aceptar cookies?
- ¿Dar permisos? ¿Conocer mi localización?

¡¡Sí, por favor!!





Reconocimiento de aplicaciones

Las aplicaciones que se comunican con el exterior dejan siempre un rastro de tráfico, susceptible de ser analizado.

Algunos protocolos interesantes:

- *HTTP/HTTPS*: Utilizado en la mayoría de las aplicaciones. Peticiones con un destino o estructura reconocidos.
- *XMPP*: Aplicaciones de mensajería.
- *STUN*: Establecimiento de llamadas VoIP.
- *DNS*: Consulta de nombres de dominio reconocibles.

Steelcentral Packet Analyzer

Permite realizar tanto una inspección en forma de gráfico como la disección de la captura en protocolos, fuentes de tráfico, etc.

Ampliamente ligado a Wireshark

<https://www.riverbed.com/es/products/steelcentral/network-performance-management/steelcentral-packet-analyzer.html>.





Wireshark

Inspector de protocolos de red. Permite capturar y examinar las diferentes capas de red de una captura de tráfico.

Funciones interesantes: Extracción de datos HTTP (o cualquier otro protocolo), seguimiento de flujos de tráfico, rastreo de orígenes...

Windows:

<https://www.wireshark.org/#download>

Linux: Repositorios





Wireshark

GeoIP: Base de datos de MaxMind que relaciona un origen/destino de tráfico con la ciudad, país, número AS y otra información.

Nos permite relacionar una dirección IP con la empresa que la utiliza.

<https://wiki.wireshark.org/HowToUseGeoIP>

<http://dev.maxmind.com/geoip/legacy/geolite/>





Inspección HTTP con Wireshark

Localización de agentes de usuario: Permite identificar el dispositivo y algunas aplicaciones.

- `http.user_agent`

Navegación web: Páginas visitadas por el dispositivo y sin cifrar.

- `http.request.full_uri`
- `http` contains “Referer:”

Geolocalizaciones: Intercambio HTTP con la API de Google Maps (o similar).

- `http.request.full_uri` contains “maps/api”





Inspección de orígenes con Wireshark

Utilizamos el módulo de estadísticas de Wireshark para visualizar una lista de IPs con las que se encuentra tráfico. (Statistics->Endpoints).

Si hemos activado GeoIP, podremos ver la empresa que maneja dicha dirección IP y otros datos.

Podemos deducir una buena cantidad de aplicaciones utilizadas a partir de estos datos.

Protocolos interesantes: XMPP, HTTP, STUN...





Inspección de peticiones DNS con Wireshark

Las peticiones DNS nos dan muchas pistas acerca de los servicios utilizados.

Permiten además en ocasiones determinar el operador de red, apareciendo como servidor DNS el suyo.



Extracción de ficheros HTTP con Wireshark

Pueden extraerse un gran número de ficheros intercambiados mediante HTTP.

Podemos encontrar:

- Imágenes/gifs.
- Ficheros de audio y vídeo.
- Ficheros XML/JSON.
- HTML, Javascript, CSS...

File -> Export Objects -> HTTP



Análisis mediante scripting

Pueden programarse de forma fácil scripts en diversos lenguajes para proporcionar un análisis personalizado de la captura de red.

Utilizaremos [*dpkt*](#), una librería para Python escrita por Dug Song y otros contribuidores para realizar inspección a nivel de paquete.

- `pip install dpkt`



Análisis mediante scripting

Escribiremos ahora tres sencillos scripts en Python que realizarán las siguientes acciones:

- Extraer estadísticas de los diferentes protocolos de cada capa TCP/IP.
- Extraer los agentes de usuario por orden de uso.
- Extraer las resoluciones DNS de tipo A y CNAME.





Conclusiones

Respecto a la recogida de tráfico:

- Resulta sencillo, incluso trivial en algunos contextos, realizar una captura de tráfico.
- Muchos de estos métodos son invisibles (pasivos) y muy difíciles de detectar.
- Métodos que se han utilizado durante años siguen siendo igual de efectivos.

Respecto al análisis del tráfico:

- Las aplicaciones y servicios, incluso si aseguran cifrar el contenido del tráfico, pueden dejar información desprotegida.
- Puede realizarse un perfilado del usuario del dispositivo con esta información.
- Importancia de comprobar el tráfico de nuestros dispositivos en contextos de seguridad avanzados.

¿Preguntas?

¡¡Muchas gracias por venir!!