MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

# Webinar Gratuito
# Redes Inalámbricas

**Alonso Eduardo Caballero Quezada**

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

Sitio web: http://www.mile-sec.com
Correo: capacitacion@mile-sec.com

Enero 2019

# Sobre MILE-SEC

MILE-SEC
Capacitación y Consultoría en
Hacking Ético & Forense Digital

**MILESEC E.I.R.L**, es una empresa de capitales Peruanos fundada en el año 2017, netamente dedicada a brindar servicios de capacitación a empresas, instituciones, organizaciones  y profesionales, en las áreas de seguridad de la información y tecnologías de la información (T.I.), tales como; Pruebas de Penetracion, Hacking Ético, Evaluación de Vulnerabilidades, Forense de Computadoras y Forense Digital. Así mismo brinda servicios de consultorías especializadas en todas las áreas antes mencionadas.

Durante estos años ha realizado capacitaciones presenciales y consultorías tanto públicas cuanto privadas para Ecuador y Perú, en las ciudades de Lima, Cusco y Trujillo. Así mismo ha realizado capacitaciones online o virtuales.


http://www.mile-sec.com/

informes@mile-sec.com / mileseceirl@gmail.com

https://www.facebook.com/mileseceirl/

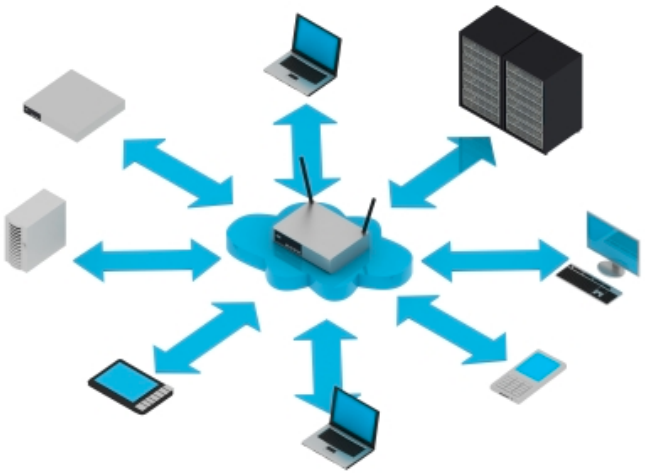
https://twitter.com/mileseceirl

https://www.linkedin.com/in/milesec/

# Temario

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

- Entender las implicaciones de las vulnerabilidades en redes inalámbricas
- Seleccionar las herramientas
- Descubrir redes inalámbricas
- Verificar por un reconocimiento global
- Escanear ondas aéreas locales
- Descubrir ataques a redes inalámbricas, y tomar medidas correctivas
- Tráfico encriptado
- Wi-Fi Protected Setup (WPS)
- Dispositivos inalámbricos falsos
- Spoofing MAC
- Problemas de seguridad física
- Estaciones de trabajo inalámbricas vulnerables
- Ajustes por defecto de configuración



# Introducción



Las redes de área local (o Wi-Fi), especialmente aquellas basadas en el estándar IEEE 802.11, está siendo más desplegadas dentro de redes en empresas y de casas. Wi-Fi ha sido atacado desde su creación, casi una década y media atrás. El estigma de una conexión Wi-Fi no segura está empezando a disminuir, pero no por ello se deberá bajar las defensas.

Wi-Fi tiene un gran valor comercial, desde la conveniencia para reducir el tiempo de despliegue de la red. Ya sea la organización permite o no acceso hacia una red inalámbrica, es probable se tenga una, por lo cual es crítico evaluar las vulnerabilidades de seguridad Wi-Fi.

Lo importante es conocer las vulnerabilidades comunes de seguridad en la red inalámbrica a evaluar, luego algunas medidas de seguridad fáciles y de bajo precio, las cuales se puedan implementar para garantizar Wi-Fi no sea un riesgo mayor para la organización.

* http://www.ieee802.org/11/

# Implicaciones de vulnerabilidades en redes inalámbricas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Wi-Fi son muy susceptibles a ataques, incluso más a las redes cableadas, si no están configuradas o desplegadas adecuadamente. Las redes inalámbricas tienen muchas vulnerabilidades, las cuales pueden permitir a un atacante apoderarse de la red, o permitir extraer información sensible.

- Perdida de acceso hacia la red, incluyendo correo electrónico, web, y otros servicios causantes de tiempo desperdiciado para la empresa
- Perdida de información sensible, incluyendo contraseñas, datos de clientes, propiedad intelectual y más
- Consecuencias de regulación y responsabilidades legales asociadas, con usuarios no autorizados ganando acceso hacia los sistemas de la empresa.

Muchas de las vulnerabilidades están en la implementación del estándar 802.11. Los APs y sistemas clientes también tienen algunas vulnerabilidades.

# Seleccionar las herramientas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Existen muy buenas y diversas herramientas para seguridad inalámbrica, ya sea para plataformas Windows o Linux

- Kismet
- Aircrack-NG
- CommView
- ElcomSoft Wireless Security Auditor
- OmniPeek

Considerar adquirir entre los tres tipos de antenas inalámbricas.

- Omnidireccional
- Semidireccional
- Direccional

* https://www.kismetwireless.net/
* http://aircrack-ng.org/
* https://www.tamos.com/products/commwifi/
* https://www.elcomsoft.com/ewsa.html
* https://www.liveaction.com/products/omnipeek/

# Descubrir redes inalámbricas



Después de tener una tarjeta inalámbrica y el software para realizar las pruebas, se está listo para empezar. La primera prueba a realizar será capturar información sobre la red inalámbrica.

# Verificar por un reconocimiento global



La primera prueba requiere únicamente la dirección MAC del AP y acceso hacia Internet. Se está probando para ver si alguien ha descubierto la señal Wi-Fi, y publicado esta información para ser vista mundialmente.

Para este propósito se puede utilizar el sitio web WIGLE.

Si el AP está listado alguien la ha descubierto, muy probablemente mediante “war-driving”, y se ha publicado la información para otros lo vean. Es necesario por lo tanto empezar a implementar medidas de seguridad tan pronto como sea posible, para evitar otros utilicen esta información en contra.


* Wigle: https://wigle.net/

# Escanear ondas aéreas locales

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Vigilar las ondas aéreas alrededor de un edificio para ver si es factible encontrar APs no autorizados o autorizados. Se busca por un SSID, el cual es el nombre de la red inalámbrica. Se se tienen redes inalámbricas múltiples y separadas, cada una podría o no tener una única SSID asociada a esta.

Se puede utilizar una herramienta para descubrir SSIDs y otra información detallada sobre los APs inalámbricos, incluyendo lo siguiente:

- Direcciones MAC
- Nombre
- Canal de radio en uso
- Nombre del proveeedor
- Si esta activa o no la encriptación
- Fortaleza de la señal RF

* Netstumbler: http://www.netstumbler.com/downloads/

# Descubrir ataques a redes inalámbricas, medidas correctivas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Diversos “hacks” maliciosos, incluyendo ataques DoS, puede ser realizados contra las redes Inalámbricas. Esto incluye forzar a los APs a revelar sus SSIDs durante el proceso de ser desasociado desde la red, y uniéndose nuevamente. Además los atacantes pueden literalmente interferir la señal RF de un AP, especialmente en sistemas 802.11b y 802.11g, y forzar a los clientes inalámbricos a reasociarse hacia un AP falso simulando al AP victima.

- Tráfico inalámbrico sin encriptar
- WEP débil y claves previamente compartidas WPA
- PINs Wi-Fi Protected Setup (WPS) factible de ser roto
- APs no autorizados
- Controles de direcciones MAC fáciles de ser evadidos
- Equipo Inalámbrico el cual es accedible físicamente
- Ajustes de configuración por defecto

* https://www.wifipineapple.com/

# Tráfico encriptado



El tráfico inalámbrico puede ser capturado directamente de las ondas aéreas, haciendo a estos medios de comunicación susceptibles a interceptación. A menos el tráfico esté encriptado, será enviado y recibido en texto claro como en una red cableada. En la cima de esto, los protocolos para la encriptación 802.11, Wired Equivalent Privacy (WEP), y Wi-Fi Protected Access (WPA), cada una teniendo sus propias debilidades, lo cual permite a los atacantes romper sus claves de encriptación, y desencriptar tráfico capturado.

Para romper WEP un atacante únicamente necesita capturar una gran cantidad de tráfico, pudiendo demandar esto minutos o días. Capturar los suficientes IVs para romper la clave WEP.

Para romper WPA y WPA2 PSK, se debe esperar por el cliente se autentique con el AP. Más rápido sería forzar el proceso de autenticación, enviando un paquete de desautenticación hacia la dirección de difusión. Luego de capturar los paquetes pertinentes, se puede intentar romper la clave previamente compartida utilizando un buen diccionario.

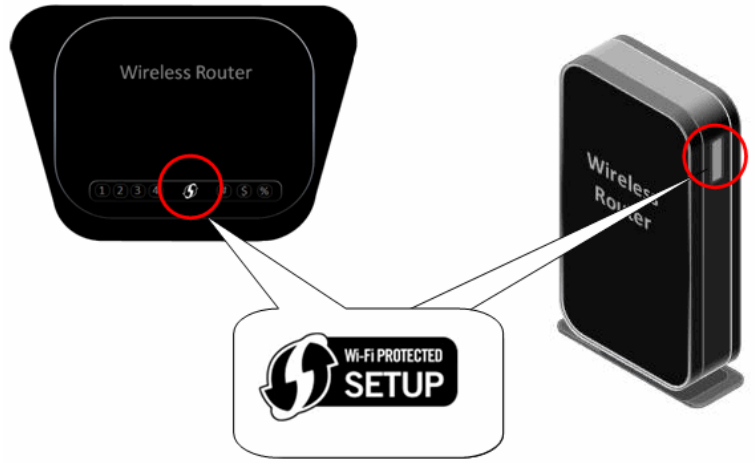
# Wi-Fi Protected Setup (WPS)



Es un estándar inalámbrico el cual permite conectividad simple hacia un AP inalámbrico “Seguro”. El problema con WPS es la implementación de PINs registrados, lo cual hace fácil conectarse hacia una inalámbrica, y puede facilitar los ataques sobre muchas claves previamente compartidas WPA/WPA2, utilizadas para bloquear todo el sitema.

WPS esta destinado a consumidores en redes inalámbricas de casa.

Los ataques son relativamente sencillos utilizando herramientas de fuente abierta. Este procedimiento podría demandar desde algunos minutos hasta horas. Aunque esto depende mucho también del escenario en evaluación.




* https://code.google.com/archive/p/reaver-wps/

# Dispositivos inalámbricos falsos

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Se debe vigilar por APs  no autorizados y clientes inalámbricos adjuntados hacia la red, y ejecutándose en modo ad-hoc.

También, educar a los usuarios sobre el uso seguro del Wi-Fi cuando estén fuera de una oficina. Comunicar los peligros de conectarse hacia redes Wi-Fi desconocidas, y recordárselo en periodos consistentes.

- SSIDs comunes, incluyendo aquellos populares por defecto como linksys, y Wi-Fi público gratuito
- Direcciones MAC no pertenecientes a la red. Buscar por los primeros tres bytes de la dirección MAC, los cuales especifican el nombre del proveedor.
- Señales de radio débiles, lo cual puede indicar un AP oculto, adyacente, o incluso fuera del edificio.
- Comunicaciones a través de diferentes canales de radio, diferentes a los utilizados para la red del trabajo
- Degradación en el rendimiento de la red para cualquier cliente Wi-Fi

# Spoofing MAC



Una defensa común para las redes inalámbricas, es aplicar controles en las direcciones MAC (Media Access Control). Aquí es donde se configura la AP, para permitir únicamente a clientes inalámbricos con direcciones MAC conocidas, se conecten hacia la red. Consecuentemente, un ataque muy común contra las redes inalámbricas es suplantar las direcciones MAC.

Los atacantes maliciosos pueden fácilmente falsificar las direcciones MAC en Linux, utilizando por ejemplo el comando “ifconfig”, en Windows también se pueden utilizar algunos programas. Sin embargo, como WEP y WPA, los controles basados en direcciones MAC son otra capa de protección y mejor a nada en absoluto. Si alguien falsifica una de las direcciones MAC, la única manera de detectar un comportamiento malicioso es a través de una concientización contextual, mediante la detección de la misma dirección MAC utilizada en dos lugares de la WLAN, lo cual puede ser complicado.

# Problemas de seguridad física

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Diversas vulnerabilidades de seguridad física pueden generar robo físico, la reconfiguración de dispositivos inalámbricos, y captura de información confidencial. Se debe buscar por las siguientes vulnerabilidades en seguridad cuando se prueben los sistemas:

- APs montadas fuera del edificio y públicamente factibles de accederse.
- Antenas pobremente montadas, o tipos incorrectos de antenas, la difusión muy fuerte de la señal, y por lo tanto sea factible de ser accedida por el público. Se debe visualizar la fortaleza de la señal.

Estos inconvenientes son frecuentemente pasados por alto, debido a instalaciones presurosas, planificación inadecuada, o ausencia de conocimiento técnico, pero esto se volverá en contra de la empresa.

# Estaciones de trabajo inalámbricas vulnerables

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Las estaciones de trabajo tales como laptops basadas en Windows, tienen muchas vulnerabilidades en seguridad, desde contraseñas débiles hasta agujeros de seguridad sin parchar, para el almacenamiento de claves de encriptación WEP y WPA localmente.

Muchas de las bien conocidas vulnerabilidades en el cliente inalámbrico, han sido parchadas por sus respectivos proveedores, pero nunca se sabe si los sistemas inalámbricos están ejecutando las últimas (y usualmente más seguras) versiones de los sistemas operativos, software del cliente inalámbrico y otras aplicaciones de software.

Ademas se sugiere utilizar en el cliente inalámbrico, un software para analizar la red, de tal manera se puedan buscar por vulnerabilidades en los clientes inalámbricos, realizando escaneos autenticados utilizando herramientas para evaluar vulnerabilidades, como Nessus, OpenVAs, Nexpose, etc.

* https://nvd.nist.gov/vuln/search

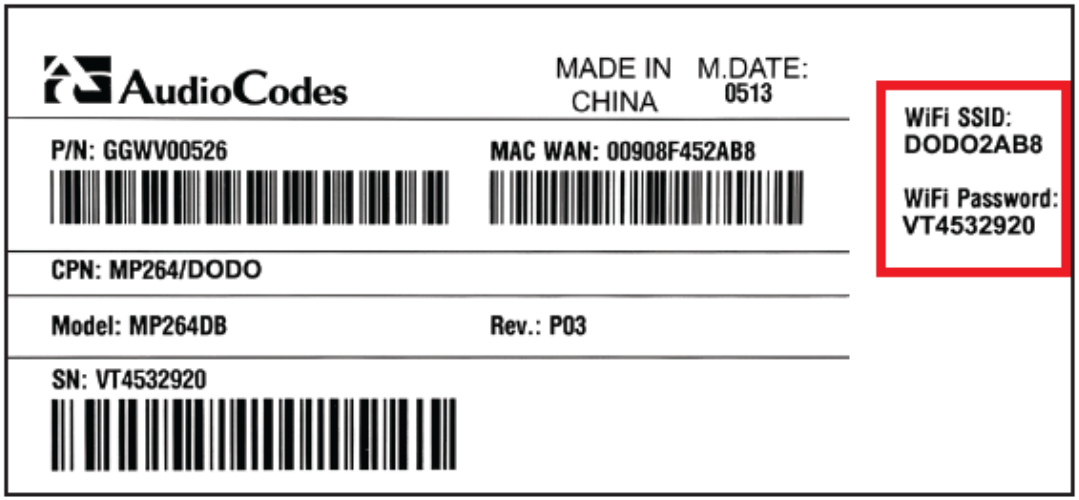
# Ajustes por defecto de configuración



Similar a las estaciones de trabajo, los APs pueden tener muchas vulnerabilidades conocidas. Aquellas más comunes son los SSIDs por defecto y contraseñas de administrador.

Aquellas más específicas ocurren únicamente sobre ciertas versiones de hardware y software, las cuales generalmente son publicadas en bases de datos sobre vulnerabilidades, y sitios webs de los proveedores.

Muchos sistemas inlámbricos tienen aún WEP y WPA deshabilitado por defecto también.



MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

# Webinar Gratuito
# Redes Inalámbricas

**Alonso Eduardo Caballero Quezada**

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

Sitio web: http://www.mile-sec.com
Correo: capacitacion@mile-sec.com

Enero 2019