Webinar Gratuito

Atacar Redes WPA con Kali Linux

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: http://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 1 de Octubre del 2020

Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures Pen Testing, Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist y OSEH.

Instructor y expositor en OWASP Perú, PERUHACK, 8.8 Lucky Perú. Cuenta con más de 17 años de experiencia y desde hace 13 años labora como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

https://twitter.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

http://www.reydes.com

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

reydes@gmail.com

WPA

WPA (Wifi Protected Access) se presenta como una solución temporal de la Wi-Fi Alliance para asegurar las redes inalámbricas, luego de conocerse la debilidad de WEP.

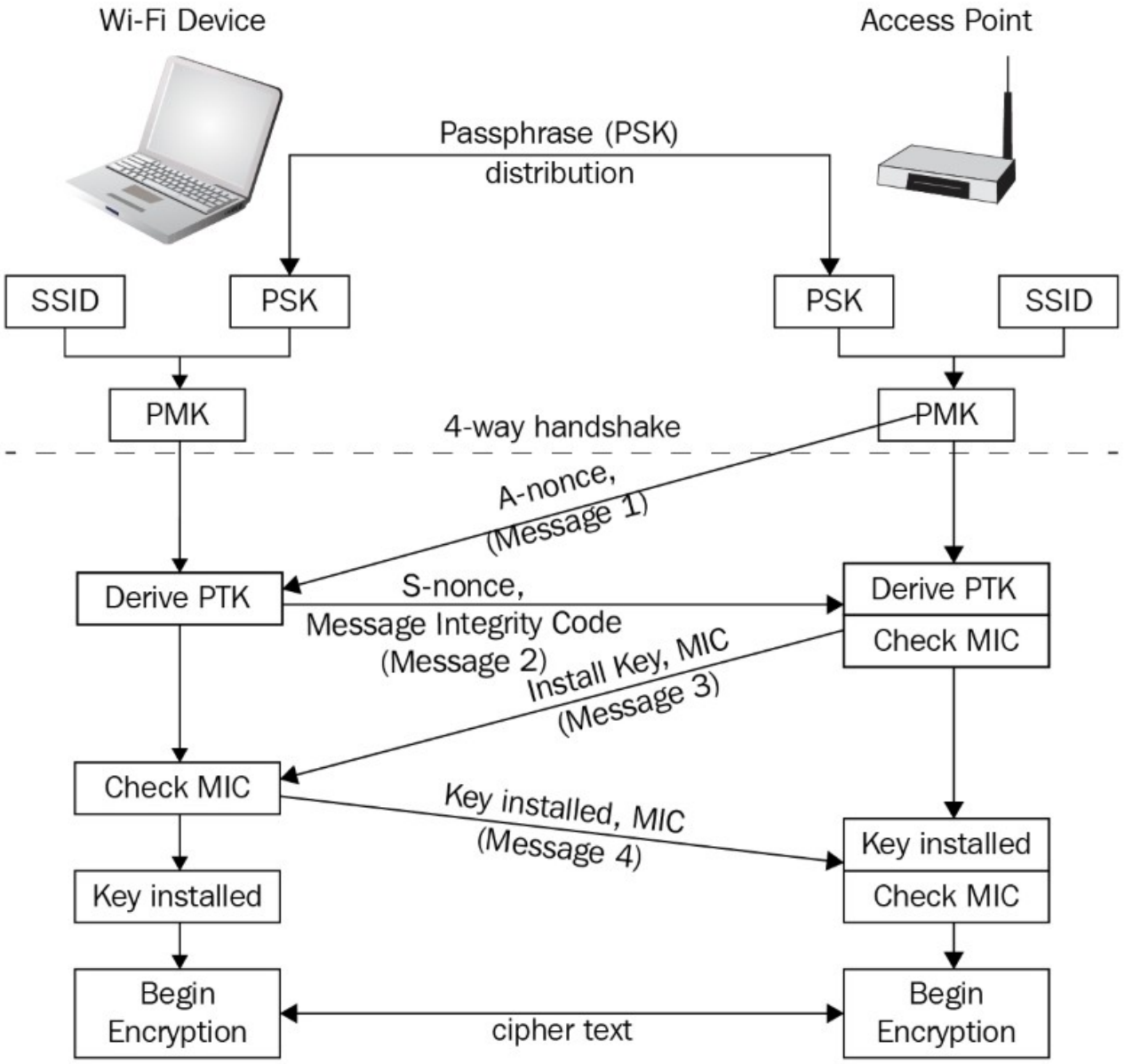
Tanto WPA como WPA2 soportan el protocolo 802.1x para la autenticación en escenarios empresariales, y la autenticación a través de llave compartida PSK, (Pre Shared Key).

WPA y WPA2 difieren principalmente en el algoritmo empleado de encriptación. WPA se basa en el algoritmo TKIP para las comunicaciones, el cual se basa en RC4, mientras WPA2 utiliza CCMP.

Otra diferencia es el algoritmo utilizado para el control de la integridad del mensaje. WPA utiliza Michael, mientras WPA2 implementa una versión mejorada de MIC.

* IEEE 802.11: https://standards.ieee.org/standard/802_11-2007.html
* Wifi Protected Access: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

WPA (Cont.)


Wi-Fi Device
Access Point
Passphrase (PSK)
distribution
SSID
PSK
PSK
SSID
PMK
4-way handshake
PMK
A-nonce,
(Message 1)
Derive PTK
S-nonce,
Message Integrity Code
(Message 2)
Derive PTK
Check MIC
Install Key, MIC
(Message 3)
Check MIC
Key installed, MIC
(Message 4)
Key installed
Check MIC
Key installed
Begin
Encryption
cipher text
Begin
Encryption

Atacar WPA

El cliente y el punto de acceso negocian una política de seguridad a seguir, la primera fase de autenticación. La importancia de este proceso radica en cliente se conecta hacia la red sin haber iniciado el proceso de autenticación, no siendo el tráfico aún encriptado, lo cual permite realizar un ataque de desauntenticación. Provocando el cliente inicie un nuevo proceso de autenticación y asociación.

Fundamentalmente para atacar una red WPA-PSK, se intentará de capturar el intercambio de número aleatorios. Una vez conocidos estos, además del SSID y las direcciones MAC tanto del cliente como del punto de acceso de la red, obtener la clave o secreto compartido utilizado.

Una vez obtenida la clave compartida, será factible conectarse hacia la red inalámbrica.

Aircrack-NG

Aircrack-ng es una suite completa de herramientas para evaluar la seguridad de redes WiFi.

Se enfoca en diferentes áreas de la seguridad WiFi:

- **Vigilancia:** Captura de paquetes y exportar datos hacia archivos de texto para procesamiento posterior, mediante herramientas de terceros.
- **Atacar:** Retransmitir ataques, desautenticación, puntos de acceso falso, y otros mediante inyección de paquetes.
- **Pruebas:** Verificar tarjetas WiFiy capacidades del controlador (captura de inyección)
- **Romper:** WEP y WPA PSK (WPA 1 y 2)

Todas las herramientas son en línea de comandos , lo cual permite scripting. Funciona principalmente en Linux, pero también Windows, OS X, FreeBSD, OpenBSD, NetBSD, como también Solaris e incluso eComStation 2.

* aircrack-ng: https://www.aircrack-ng.org/

Curso

Curso Hacking con Kali Linux 2020

Domingos 4, 11, 18 y 25 de Octubre del 2020. De 9:00 am a 12:15 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Presentación

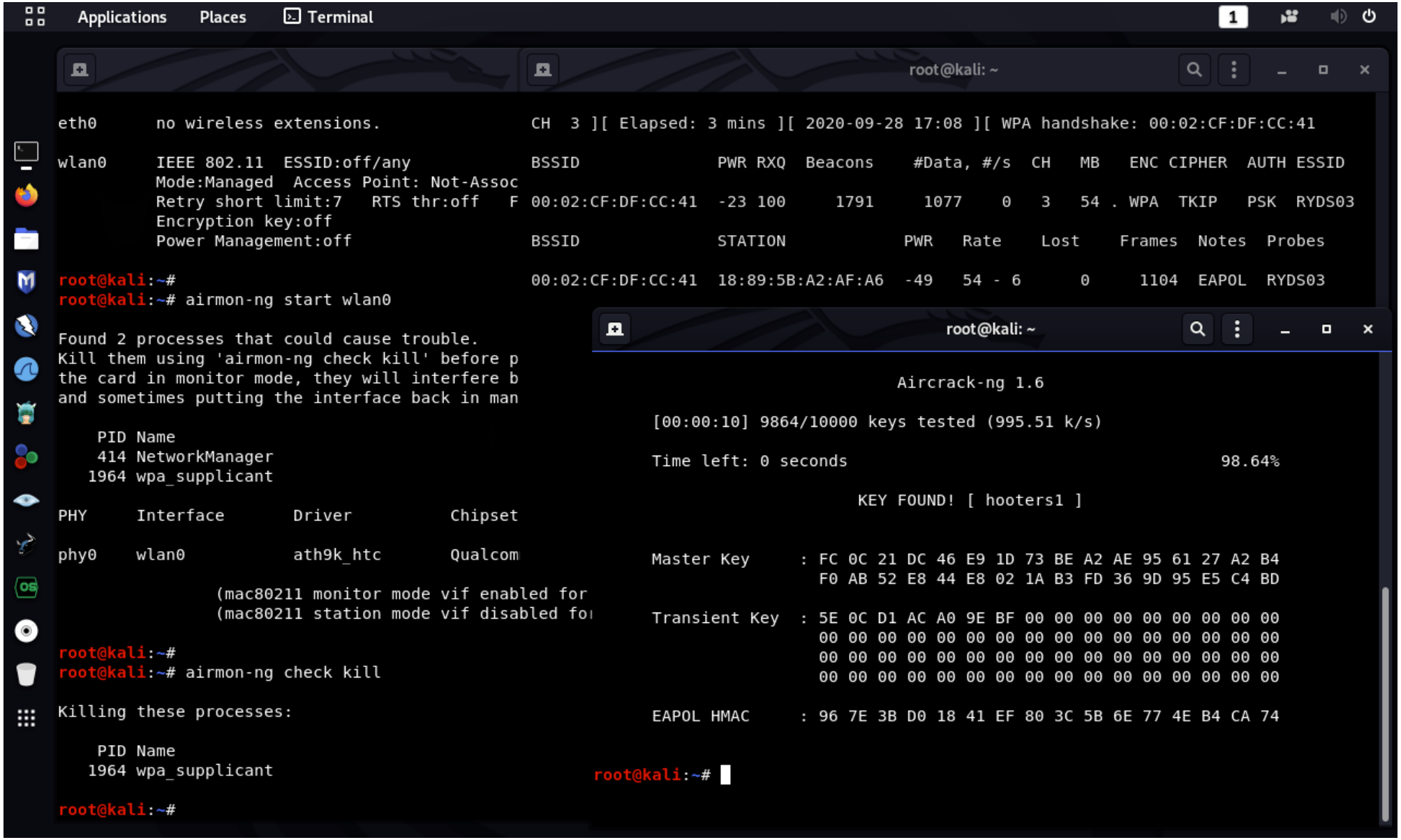
Kali Linux es una distribución basada en GNU/Linux Debian, diseñada para realizar auditorias de seguridad y pruebas de penetración avanzadas. Kali Linux contiene cientos de herramientas destinadas a diversas tareas en seguridad de la información, tales como pruebas de penetración, investigación de seguridad, forense digital e ingeniería inversa. Kali Linux incluye más de 600 herramientas para pruebas de penetración, es libre, tiene un árbol GIT open source, cumple con FHS, tiene un amplio soporte para dispositivos inalámbricos, incluye un kernel parchado para inyección, es desarrollado en un entorno seguro, sus repositorios y paquetes están firmados con GPG, tiene soporte para múltiples lenguajes, incluye soporte para ARMEL, y ARMHF, además de ser completamente personalizable.

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OSEH. Ha sido instructor en el OWASP LATAM Tour Lima, Perú del año 2014, expositor en el 0x11 OWASP Perú Chapter Meeting 2016 y OWASP LATAM at Home

Información: http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

e-mail: reydes@gmail.com Sitio web: http://www.reydes.com

Demostraciones



Cursos Virtuales Disponibles en Video

Curso Virtual de Hacking Ético
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web
http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense
http://www.reydes.com/d/?q=Curso_de_Informatica_Forense

Curso Virtual Hacking con Kali Linux
http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso Virtual OSINT - Open Source Intelligence
http://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes
http://www.reydes.com/d/?q=Curso_Forense_de_Redes

Y todos los cursos virtuales:

http://www.reydes.com/d/?q=cursos

Más Contenidos

Videos de 60 webinars gratuitos

http://www.reydes.com/d/?q=videos

Diapositivas de los webinars gratuitos

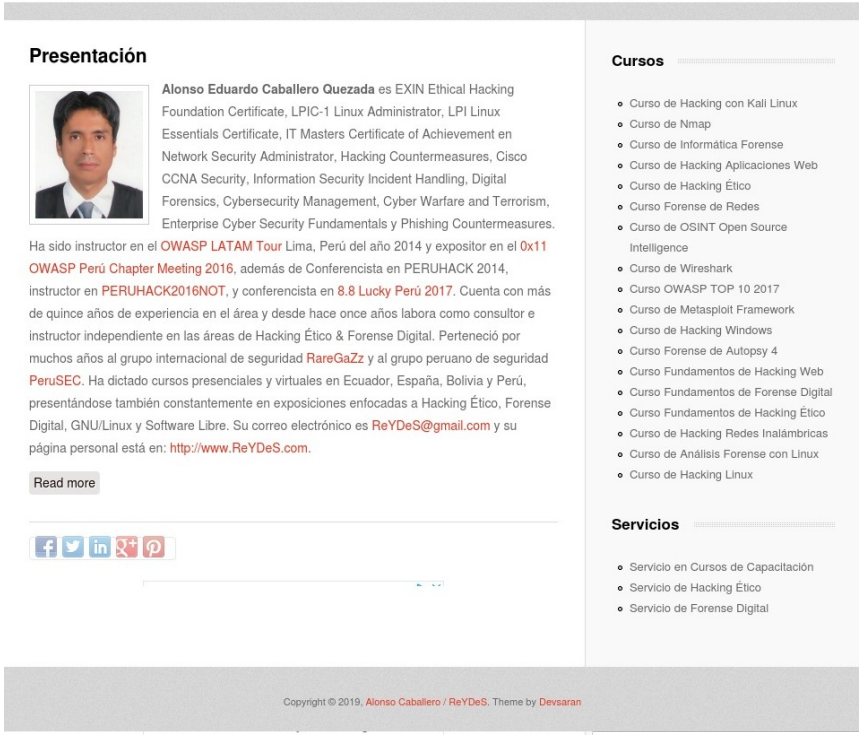
http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

http://www.reydes.com/d/?q=node/2

Blog sobre temas de mi interés.

http://www.reydes.com/d/?q=blog/1



Webinar Gratuito

Atacar Redes WPA con Kali Linux

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: http://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 1 de Octubre del 2020