# Bootcamp Full Stack CyberSecurity Keepcoding

https://keepcoding.io/nuestros-bootcamps/bootcamp-en-ciberseguridad/

## Evaluaciones de los casos prácticos

Formadores Bootcamp: https://keepcoding.io/sobre-nosotros/profesores/

## Módulo 1. Introducción a la Ciberseguridad

Evaluación:

Buenos días Marcos,

En primer lugar felicitarte por el trabajo realizado e indicarte que la práctica es **APTA**. Te he puesto algunos comentario en el documento, pero has conseguido realizar todos los ejercicios y documentarlos perfectamente.

Como recomendación te indicaría un par de cosas. En primer lugar siempre esta bien incluir un índice y un pequeño informe ejecutivo del resultado de la auditoria. Como las conclusiones que incluiste pero al principio del informe.

Y por otra parte la sección de recomendaciones esta muy bien pero yo la incluiría debajo de cada vulnerabilidad. SQL Injection y posteriormente sus posibles soluciones, y así están agrupadas junto a su vulnerabilidad.

Pero de nuevo, muy buen trabajo.

Saludos,
Carlos Cilleruelo Rodríguez
Alpha Security

## Módulo 2. Cryptography

Evaluación:

Hola Marcos,

Te envío el feedback sobre tu práctica de Criptografía:

Ejercicio 1. Repeating-key XOR

El ataque se basa en análisi de frecuencia y no fuerza bruta. El cálculo de posibles combinaciones tampoco es correcto. Una clave de 10 bytes tiene 256**10 y no 10**256.

La explicación del código sí que usa el método correcto de encontrar la clave, byte por byte, usando análisi de frecuencia.

Ejercicio 2. CTR bit-flipping

Buena explicación del ataque de bit-flipping.

Ejercicio 3. Autenticación

Has identificado correctamente que se trata de un problema de autenticación, en este caso tanto un hmac como GCM funciona, pero al estar usando CTR, GCM sería la solución más lógica.

Ejercicio 4.

El problema está en la generación del nonce, en el hecho de que sólo se genera una vez y se reutiliza para todas las encriptaciones.

Ejercicio 5 y 6.

Has identificado los dos problemas correctamente. Pbkdf es una buena opción. Y has reconocido el problema con el algoritmo 'None' aunque no lo has mencionado en el ejercicio 5, sí que lo solucionas en el 6.

Ejercicio 7.

Correcto, http es inseguro para un servidor de autenticación, y se debería usar siempre HTTPS.

Ejercicio 8.

La seguridad de https depende de los CAs guardados en el sistema. Y si el sistema ha sido comprometido, entonces la seguridad de SSL también. El problema más grande sería que el atacante haya introducido en el ordenador su propio CA, para generar certificados inválidos.

Considero tu práctica APTA. Pregúntame si hay alguna duda sobre el feedback.
Buena suerte con el resto del bootcamp :)

Sergi

## Módulo 3. Information Gathering | OSINT

Evaluación:

Hola Marcos,

La nota de tu práctica es APTO.

Muy buen trabajo, muy completo y con buen formato. Has utilizado muchas herramientas vistas en clase y de la forma correcta, y has ido comentando detalladamente los pasos que has realizado.

Buen descubrimiento de los activos de la organización y muy buen análisis de vulnerabilidades, comprobando también si la información es falso positivo o no, y describiendo las vulnerabilidades que encuentras.

Muy buen análisis OSINT, muy interesante toda la información que obtienes.
Creo que a veces pecas de dar demasiados detalles, por ejemplo, cuando realizas el análisis con nmap sería suficiente si indicas el último comando que has usado y no los intermedios que dan menos información.

Para el futuro, intenta poner también alguna captura de pantalla. Personalmente, yo utilizo Shift + Tecla de Windows + S.

Los objetivos de la práctica los has cumplido y creo que entiendes como recopilar información de un objetivo y realizar un informe de inteligencia. Se nota que estás interesado y trabajas bien, de nuevo, fantástico trabajo.

Un saludo,
Alvaro Schuller

## Módulo 4. Pentesting

Evaluación:

Hola Marcos,

Has hecho un gran trabajo resolviendo ambas máquinas y generando la documentación. A continuación te dejo algún comentario:

- No se había solicitado en el ejercicio, pero se podría poner un apartado de resumen ejecutivo con un resumen de las vulnerabilidades identificadas en cada máquina.
- Muy bien detallado y trabajado el apartado de la remediación. Normalmente suele quedar un poco olvidado pero es lo más importante para las empresas cuando entregas un informe.
- Se ve un gran dominio de Metasploit en la explotación de muchas de las vulnerabilidades.

Enhorabuena por el trabajo realizado, se puede apreciar todos los conocimientos que has adquirido ;)

Un saludo,
Roberto López.

## Módulo 5. Blue Team

Evaluación:

**Buenas Marcos, enhorabuena por el trabajo ya que me parece que esta muy bien documentado y has alcanzado todos los objetivos en el mismo incluso los opcionales como el honeypot. Solo quiero decirte que me ha gustado mucho tu trabajo.**

**Enhorabuena.**

Apto

Un saludo

Nacho Alonso

# Módulo 7. Malware Analysis

Buenas tardes Marcos, te escribo para comunicarte que tu práctica final de módulo de malware está APTA.

El ejercicio de análisis de malware es de un gran nivel, de hecho el informe es prácticamente el de un profesional. Has investigado las diferentes familias que se asocian al ransomware, sus alias, otros ficheros del mismo tipo visto, los grupos criminales asociados a este malware, está todo muy bien estructurado, has sacado mucho provecho a las herramientas dadas. De hecho, están todos los datos e IOCs muy claros. Por poner algo a mejorar a futuro, sería una sección al final donde haya un resumen ejecutivo donde en 2 párrafos hagas un resumen de todas las acciones realizadas por el malware y el alcance sufrido, aunque es una mera mejora a futuro.

En cuanto al ejercicio de reglas Yara, mi intención era que tuvierais un acercamiento real a la detección de malware usando el framework de Yara, pero tu me has hecho un ejercicio que bien podría ser un proyecto final del bootcamp. Has creado un detector malware estático basado en reglas yaras, has conseguido 107 muestras con una tasa de detección del 87%. Una maravilla, otro nivel sinceramente.

Por tanto, sólo me queda decirte que enhorabuena, tu práctica es un 10!!

Espero que estes disfrutando del bootcamp y sobre todo, que estes aprendiendo!

Un saludo,

Adrián