EXTRACTO GRATUITO - 2 CAPÍTULOS COMPLETOS DE 22

El Mapa: Fundamentos de Ciberseguridad

El plan de 90 días y cómo elegir tu camino: dos capítulos completos de la guía, para que empieces hoy.

por Eduardo Solís

Ingeniero de seguridad con más de 5 años defendiendo infraestructura Fortune 500 y global - WAF, CDN, superficie de ataque y gestión de vulnerabilidades. Pasé de Costa Rica a la primera línea del mundo enterprise. Este es el mapa que me hubiera gustado tener.

linkedin.com/in/edusolis

Por qué escribí esto

No crecí con un camino claro hacia la ciberseguridad. Empecé en Costa Rica, aprendí por mi cuenta cómo funcionan de verdad los sistemas, y me abrí paso hasta la primera línea de la seguridad enterprise - arquitectando protección en Akamai (una de las empresas que mantiene online y segura una porción enorme de internet), liderando superficie de ataque y gestión de vulnerabilidades para clientes globales, y defendiendo infraestructura Fortune 500.

Nadie me entregó una hoja de ruta. La construí por las malas - con fundamentos, repeticiones, y muchas noches rompiendo cosas en un laboratorio hasta que por fin tenían sentido.

Esta guía es esa hoja de ruta, ordenada y estructurada para que no tengas que andar dando vueltas. No te va a convertir en experto de la noche a la mañana. Pero si de verdad haces el trabajo que hay adentro, vas a construir la base sobre la que se sostiene todo lo demás en este campo.

Si te sirve, me encantaría saberlo - y si quieres avanzar más rápido, acompaño como mentor a personas que recorren exactamente este camino. Más sobre eso al final.

- Eduardo Solís

Contenido

Este extracto trae completos los dos capítulos marcados. El resto del índice es lo que contiene la guía completa.

Cómo usar esta guía

- Lee para entender primero, no para memorizar.
- Al final de cada capítulo, completa las acciones de estudio.
- Toma tus propias notas en lenguaje simple.
- Vuelve a los mismos temas con más profundidad después de armar tu laboratorio.

21. Un plan de aprendizaje de 90 días

La mayoría mejora más rápido con estructura. El plan de abajo no es el único camino válido, pero es una secuencia fuerte para principiantes porque construye desde los fundamentos de computación hacia el razonamiento de seguridad y la práctica.

- Días 1-30: lógica, Python básico, Linux básico, Windows básico, vocabulario de redes, DNS, HTTP y herramientas del navegador.
- Días 31-60: TLS, seguridad web básica, conceptos OWASP, autenticación, logging, capturas de paquetes y automatización simple con Python.
- Días 61-90: gestión de vulnerabilidades, fundamentos de nube, conceptos de SIEM/logs, flujo de respuesta a incidentes y uno o dos proyectos de portafolio.

> *Un plan estructurado funciona. Pero un mentor que ya recorrió este camino puede comprimir meses en semanas - manteniéndote enfocado en lo que de verdad importa y fuera de los hoyos que estancan a la mayoría de los principiantes.*

Por qué importa este capítulo

La clave es la constancia. Dos horas enfocadas cada día suelen ganarle a un atracón de fin de semana.

Ritmo sugerido de 12 semanas

- Semanas 1-2: lógica, Python básico, shell básico
- Semanas 3-4: fundamentos de Linux y Windows
- Semanas 5-6: redes, DNS, HTTP
- Semanas 7-8: TLS, autenticación, seguridad web básica
- Semanas 9-10: logs, detección, respuesta a incidentes
- Semanas 11-12: gestión de vulnerabilidades, nube, un proyecto de portafolio

ACCIONES DE ESTUDIO

- Bloquea tus semanas de estudio en el calendario y lleva un tracker visible.
- Revisa y ajusta cada 2 semanas en vez de esperar la perfección.

22. Cómo elegir un camino en ciberseguridad

La ciberseguridad no es un solo trabajo. Diferentes roles enfatizan diferentes partes de la base. Saber esto temprano te ayuda a estudiar con propósito.

- SOC / Detección / IR: logging fuerte, redes, visibilidad de endpoint y habilidades de investigación.
- Seguridad en la nube: IAM, redes de nube, infraestructura, políticas, automatización y arquitectura.
- Seguridad de aplicaciones: programación, SDLC, seguridad web, APIs y modelado de amenazas.
- Ingeniería de seguridad: sistemas, automatización, arquitectura, tooling, confiabilidad y controles.
- Gestión de vulnerabilidades / reducción de superficie de ataque: contexto de activos, exposición, escaneo, priorización, remediación, comunicación.
- Arquitectura de seguridad / roles de soluciones: entendimiento amplio, comunicación con

clientes, trade-offs y traducir riesgo en controles prácticos.

> *No tienes que resolver esto solo. Una conversación con alguien que ha trabajado en varios de estos caminos puede ahorrarte meses de adivinar - es una de las cosas más comunes que la gente me trae en la mentoría.*

Por qué importa este capítulo

No necesitas elegir tu camino para siempre de inmediato. Construye fundamentos amplios primero, luego especialízate según el trabajo que de verdad te energiza.

ACCIONES DE ESTUDIO

- Lee algunas descripciones de roles y resalta las expectativas técnicas que se repiten.
- Elige un camino para explorar más a fondo los próximos 60 días.

Lo que acabás de leer es el final

El plan de 90 días te dice QUÉ estudiar y en qué orden. Los 20 capítulos anteriores son el CÓMO: los fundamentos que hacen que ese plan se pueda cumplir de verdad, explicados por alguien que los usa todos los días defendiendo infraestructura real.

La guía completa - 22 capítulos, 66 acciones de estudio

- Parte I - Base: lógica, programación, sistemas operativos y redes.
- Parte II - Internet de verdad: DNS, HTTP/TLS, APIs, CDNs, proxies y caché.
- Parte III - Seguridad: identidad, criptografía, controles, ataques, seguridad web y de APIs, gestión de vulnerabilidades, logging y detección, nube.
- Parte IV - Práctica: herramientas, laboratorio en casa y proyectos de portafolio.
- Apéndice: glosario y consejos finales.

La guía completa (ES + EN) viene incluida en el Torvex Academy. No se paga por secretos: no existen. Se paga estructura, feedback real y rendición de cuentas - el trabajo de llevarte.

Tu siguiente paso

Ahora tienes los fundamentos que la mayoría se salta. La diferencia entre quienes entran a la ciberseguridad - y siguen subiendo - normalmente no es talento. Es dirección, retroalimentación y no perder meses en las cosas equivocadas.

En eso ayudo.

-> Sesión de Estrategia de Carrera

Una sesión 1:1 enfocada donde mapeamos dónde estás, a dónde quieres llegar, y tus próximos 90 días exactos. Te vas con una hoja de ruta personalizada.

-> Mentoría 1:1

Acompañamiento continuo para personas serias sobre pasar de los fundamentos a su primer rol - y de ahí a senior y enterprise.

Ya sea que estés tratando de conseguir tu primer trabajo o subir a un rol internacional, yo recorrí el camino - y puedo ayudarte a recorrerlo más rápido.

Agenda una llamada o escríbeme

Agenda: cal.com/torvex/career-strategy

Email: eduardo@torvexsecurity.com

LinkedIn: linkedin.com/in/edusolis

Glosario de términos imprescindibles

Superficie de ataque
El conjunto total de sistemas, interfaces y rutas de confianza alcanzables que un atacante podría atacar.

Botnet
Un grupo de dispositivos comprometidos controlados para realizar acciones maliciosas o abusivas coordinadas.

Exploit
Un método o ruta de código usada para aprovechar una debilidad.

Mínimo privilegio
Dar solo el acceso requerido, nada más.

Parche
Una actualización de software que corrige errores, debilidades o problemas de estabilidad.

Segmentación
Separar sistemas o tráfico para reducir la exposición y el radio de impacto.

Telemetría
Datos observables emitidos por sistemas, aplicaciones, identidades o redes.

Modelo de amenazas
Una forma estructurada de pensar quién puede atacar, qué puede atacar y cómo.

Consejo final para quien aprende

- Estudia en capas: concepto, observación, experimentación segura, explicación, luego automatización.
- Toma notas con tus propias palabras. Copiar texto se siente productivo, pero explicar es lo que construye maestría.
- Arma proyectos simples, honestos y bien documentados.
- Cuando te atasques, vuelve a los fundamentos: qué es el sistema, cuál es el comportamiento esperado, qué cambió y qué evidencia tengo?
- Los fundamentos sólidos se acumulan. No apures lo básico.

Una frase para recordar
La ciberseguridad se vuelve más fácil cuando dejas de tratarla como una bolsa de trucos aislados y empiezas a tratarla como el estudio de cómo los sistemas reales funcionan, fallan y se defienden.