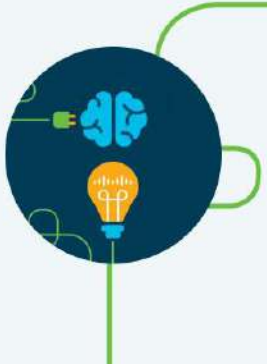
pue | academy

Workshop sobre hacking ético: ataques de ingeniería social

RAQUEL MARTÍNEZ
Technical Manager | EMEAR Cisco



Hacking Ético

Póngase en la piel de un actor de amenazas

Raquel Martínez Hernández
Europe Technical Manager

Junio 2024

Agenda

- Por qué la ciberseguridad es prioritaria
- Inteligencia Artificial y seguridad
- Afrontar el déficit de cualificaciones con educación
- Curso de Hacking Ético
- Demo
  - Ataques de Ingeniería social
  - Rockyou
    - Crunch
    - Cupp

Por qué la ciberseguridad es prioritaria

Cada nuevo lugar y método utilizado por un empleado para trabajar es un nuevo agujero en su bote salvavidas.

Cuanta más flexibilidad ofrece el trabajo híbrido, mayor es la complejidad que deben gestionar los equipos de TI. La exposición a las amenazas es enorme.

Source: Cisco Future of Secure Remote Work Report

La Ciberseguridad es crucial

- Miles de millones de personas de todo el mundo dependen de la fiabilidad, resistencia y seguridad de Internet.
- Se espera que en 2025 haya más de 40.000 millones de dispositivos conectados a Internet.
- La necesidad de seguridad es cada vez mayor y las amenazas a la ciberseguridad van en aumento.

1. Statista
2. Accenture, Triple digit increase in cyberattacks: What next?, Aug 2021
3. EmisoftThe State of Ransomware in the US: Report and Statistics 2021,

40.9 MM

Número total de dispositivos previstos para 2025 en todo el mundo, incluidos smartphones, ordenadores, portátiles y dispositivos IoT[1]

+125%

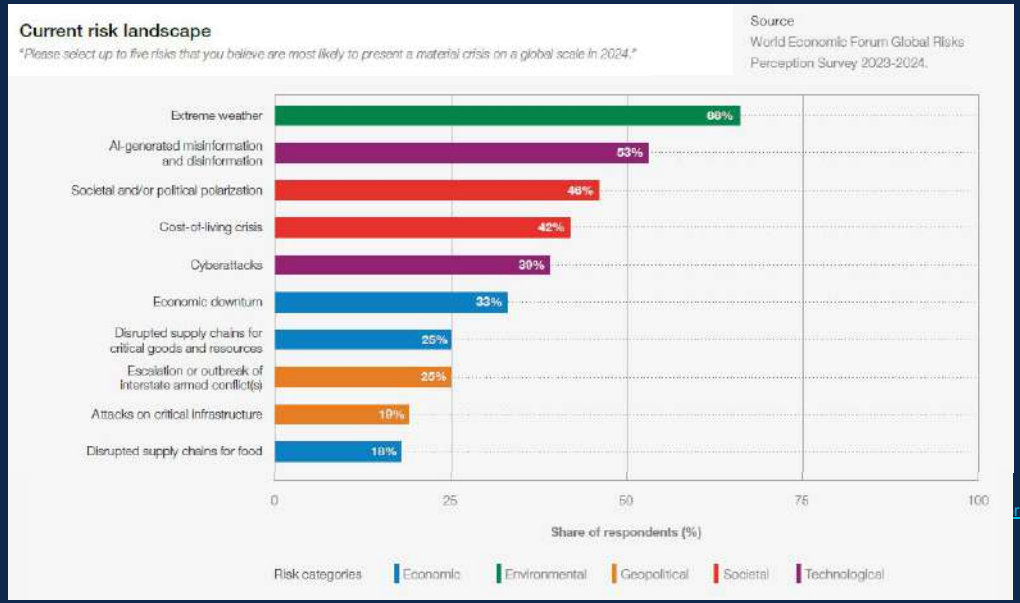
Las intrusiones informáticas notificadas aumentan un 125% anual en todo el mundo[2]

$ 623 M

Los ataques de ransomware a gobiernos estatales y municipales de EE.UU. ascendieron a más de 623 millones de dólares en 2021[3]

La ciberseguridad es una de las principales amenazas críticas globales

- Los ciberataques están en el top 5 de riesgos actualmente y ha subido 3 puestos en los últimos 2 años
- Riesgos relaciones con el uso de IA han despuntado entrando en el listado como el número 2.



Source: State of Security 2024 | Splunk

Generative AI: Friend or foe?

Who has the generative AI advantage? Respondents are split.

43%
Defenders will benefit most

12%
They will cancel each other out

45%
Adversaries will benefit most

Es como la pregunta:

¿Prefieres luchar contra un pato del tamaño de un caballo o contra 100 caballos del tamaño de un pato?

Probablemente sea más manejable centrarse en una sola amenaza, pero la IA generativa creará el escenario menos atractivo, actuando como multiplicador de fuerza para los ataques existentes.

- Kirsty Paine, CTO de campo y asesora estratégica para EMEA, Splunk

IA y Ciberseguridad

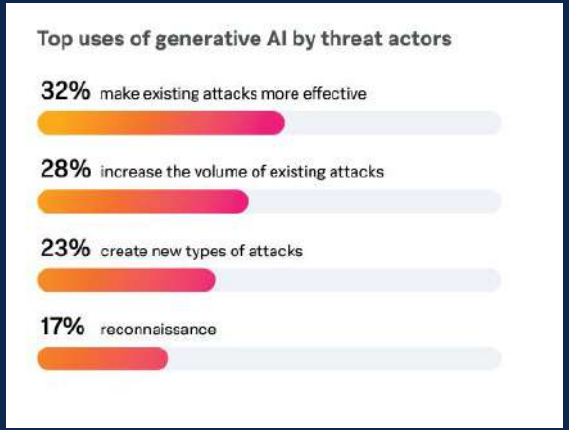
La inteligencia artificial (IA) ha revolucionado la forma en que se llevan a cabo los ciberataques, haciendo que la seguridad de la red sea más vulnerable que nunca.

El uso de la IA en los ciberataques plantea inmensos retos a las organizaciones a la hora de defenderse contra amenazas sofisticadas.
Pero también, los defensores parecen optimistas y están de acuerdo en que la IA generativa es una buena combinación para varios casos de uso de la ciberseguridad, nombrando el análisis de inteligencia de amenazas y la identificación de riesgos como las dos aplicaciones principales.

Por qué aumentarán los ciberataques por la presencia de la IA- El lado oscuro de la IA

Ventajas de la IA en Ciberataques:

- Velocidad superior: Ejecución más rápida de tareas que el humano.
- Adaptabilidad: Aprendizaje y adaptación continua.
- Incansable: Operación continua sin descansos. Los ataques son sostenidos y prolongados.
- Costo-efectivo: No requiere salario, lo que es más rentable para los ciberdelincuentes.
- Anonimato: Dificulta detección y rastreo de los hackers.
- Precisión y complejidad: Mejora constante en técnicas de ataque.



Historia del primer ataque de Vishing mediante IA

En marzo de 2021, unos delincuentes utilizaron un programa informático basado en inteligencia artificial para hacerse pasar por la voz de un director ejecutivo y exigirle una transferencia fraudulenta de 220.000 euros, en lo que los expertos en ciberdelincuencia describieron como un caso inusual de uso de inteligencia artificial en el pirateo informático.

El consejero delegado de una empresa energética con sede en el Reino Unido pensó que estaba hablando por teléfono con su jefe, el consejero delegado de la sede alemana de la empresa, quien le pidió que enviara los fondos a un proveedor húngaro. La persona que llamó dijo que la petición era urgente y ordenó al ejecutivo que pagara en el plazo de una hora, según la aseguradora de la empresa, Euler Hermes Group SA.

Deepfakes

Los piratas informáticos utilizaron programas comerciales de generación de voz para llevar a cabo el ataque. Grabó su propia voz utilizando uno de esos productos y dijo que la versión reproducida sonaba real.

El ataque de suplantación de voz en Europa es el primer ciberdelito del que tienen noticia.

Las estafas y el vishing mediante IA suponen un nuevo reto para las empresas. Las herramientas tradicionales de ciberseguridad diseñadas para mantener a los hackers alejados de las redes corporativas no pueden detectar las voces suplantadas. Los atacantes podrían utilizar grabaciones de voz disponibles públicamente para hacerse pasar por celebridades o ejecutivos.

Vídeos falsos, que podrían ser una herramienta aún más útil para los hackers. "Imagina una videollamada con la voz [de un director general], las expresiones faciales con las que estás familiarizado. Entonces no tendrías ninguna duda". Por eso, la empresa líder en seguridad empezó a trabajar en dispositivos de ciberseguridad basados en IA para poder mitigar el futuro.

Ataque DDOS con IA

- Uno de los ciberataques asistidos por IA más recientes se produjo cuando TaskRabbit, un mercado en línea para trabajadores autónomos y sus clientes, fue atacado por piratas informáticos.
- 3,75 millones de usuarios del sitio web se vieron afectados en abril de 2018 cuando sus números de la Seguridad Social y los detalles de sus cuentas bancarias fueron extraídos de sus datos de usuario. El ataque fue realizado por hackers que utilizaron una enorme botnet controlada por una IA, que utilizó máquinas esclavizadas para realizar un enorme ataque DDoS contra los servidores de TaskRabbit. El ataque fue tan drástico que todo el sitio tuvo que ser desactivado hasta que se pudiera restablecer la seguridad. Mientras tanto, lamentablemente, otros 141 millones de usuarios se vieron afectados.
- Ataque de botnet a WordPress 2019, Instagram..

¿Qué medidas pueden adoptar las organizaciones para protegerse de los ciberataques impulsados por la IA?

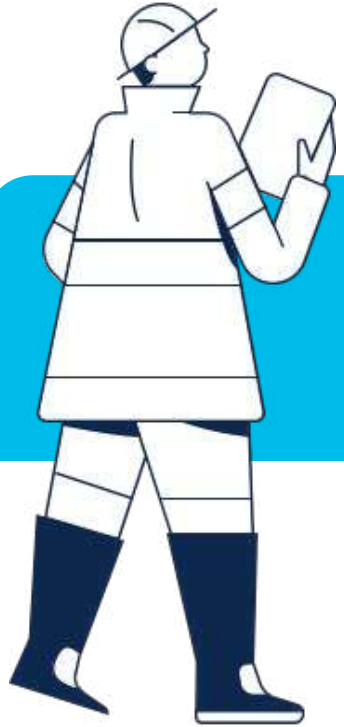
- Implantar soluciones basadas en IA: Tener la misma velocidad para detectar y responder a los ciberataques
- Formar a los empleados en las mejores prácticas de ciberseguridad
- Implementar la autenticación multifactor : puede ser una forma efectiva de evitar el acceso no autorizado a sistemas y datos.
- Actualizar y parchear periódicamente los sistemas: para evitar vulnerabilidades en el sistema.
- Tener siempre una copia de seguridad.

- Supervisar el tráfico de la red: los ataques basados en IA suelen implicar un gran tráfico, por lo que supervisar la red puede ser una forma eficaz de detectar estos ataques. Analizando el tráfico de la red en busca de anomalías y patrones que puedan indicar un ataque, las organizaciones pueden responder con rapidez y eficacia.
- Implantar el control de acceso

- Realizar auditorías de seguridad periódicas : puede ayudar a los órganos a identificar

Subsanar el déficit de cualificaciones con educación

Necesidad de mano de obra cualificada



85 millones
empleos

Desplazados por un cambio de mano de obra entre humanos y máquinas para 2025[1]

97 millones
nuevos empleos

Creados por la transformación digital para 2025[1]

1. "Future of Jobs," World Economic Forum

El déficit de cualificaciones

3.5

escasez de profesionales de la ciberseguridad en todo el mundo

Millones

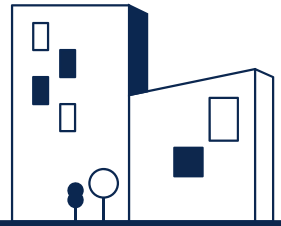
La continua falta de profesionales de la ciberseguridad amenaza el crecimiento económico.

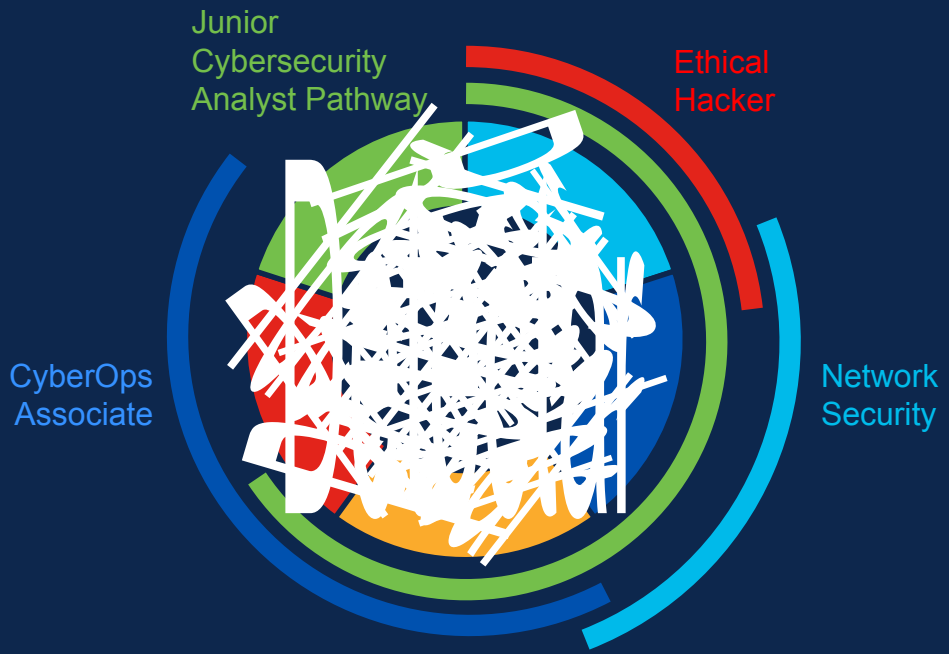
Es vital contar con profesionales que puedan liderar la ciberseguridad, probar y proteger los sistemas y formar a las personas en higiene digital.

Cybersecurity Jobs Report 2021, Cybersecurity Ventures

Los cursos se ajustan a las normas del sector

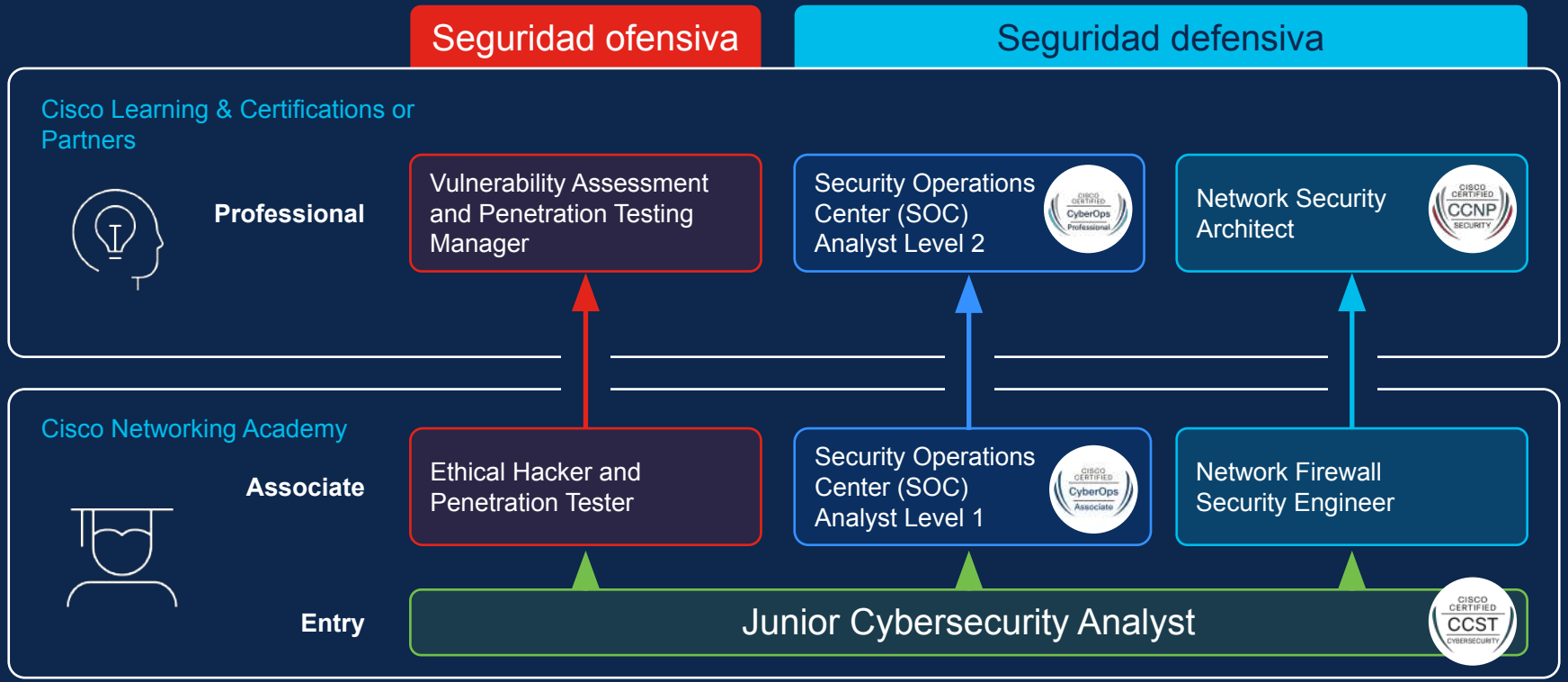
Los cursos de Cisco Networking Academy desarrollan habilidades en todas las funciones clave definidas por el Marco de Ciberseguridad del NIST.





National Institute for Standards and Technology (NIST) Cyber Security Framework Functions (v1.1)
www.nist.gov/cyberframework

Progresión profesional en ciberseguridad



Ethical Hacker Course

Ethical Hacker

Course Overview

The Ethical Hacker course prepares learners with skills to proactively discover vulnerabilities before the cybercriminals do. Learners will become proficient in the art of scoping, executing, and reporting on vulnerability assessments, while recommending mitigation strategies.

Benefits

Through the gamified narrative in the course and real-world inspired hands-on practice labs, students develop essential workforce readiness skills, laying a solid foundation in offensive security.

Prepare for Careers

- ✔ Get job-ready for Offensive Security roles such as Ethical Hacker or Penetration Tester.
- ✔ Understand the mindset and tactics of cybercriminals to strengthen your defensive security skillset.
- ✔ Gain needed skills for implementing security controls and monitoring, analyzing, and responding to current security threats.

Course Details

Target Audience: College/university students or vocational school students

Estimated Time to Completion: 70 hours

Prerequisites:
- Entry-level cybersecurity knowledge: CCST Cybersecurity certification or Cybersecurity Essentials or Junior Cybersecurity Analyst Career Path, or equivalent
- Basic programming knowledge

Course Delivery: Instructor-led and Self-paced

Learning Component Highlights:
- ✔ 10 modules and 34 labs
- ✔ 86 interactive practice activities and quizzes
- ✔ 1 final exam
- ✔ 1 skills-based assessment

Course Recognitions: Digital Badge

Recommended Next Course:
CyberOps Associate, Network Security

Requirements

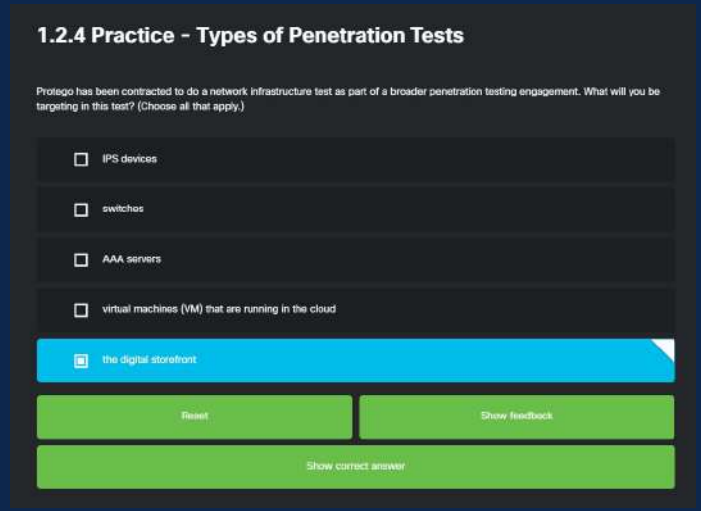
- ASC Alignment: Recommended
- Instructor Training: Recommended
- Basic Equipment: Computer and Internet
- Additional Equipment: No

skillsforall.com

Narrativa gamificada

Resumen del curso

Laboratorios prácticos y ejercicios



Resumen del curso

Entorno de laboratorio

Trayectoria del alumno

Cisco Networking Academy

Cybersecurity Essentials
Version 3.0, Instructor-Led only (70h)

Basic programming knowledge

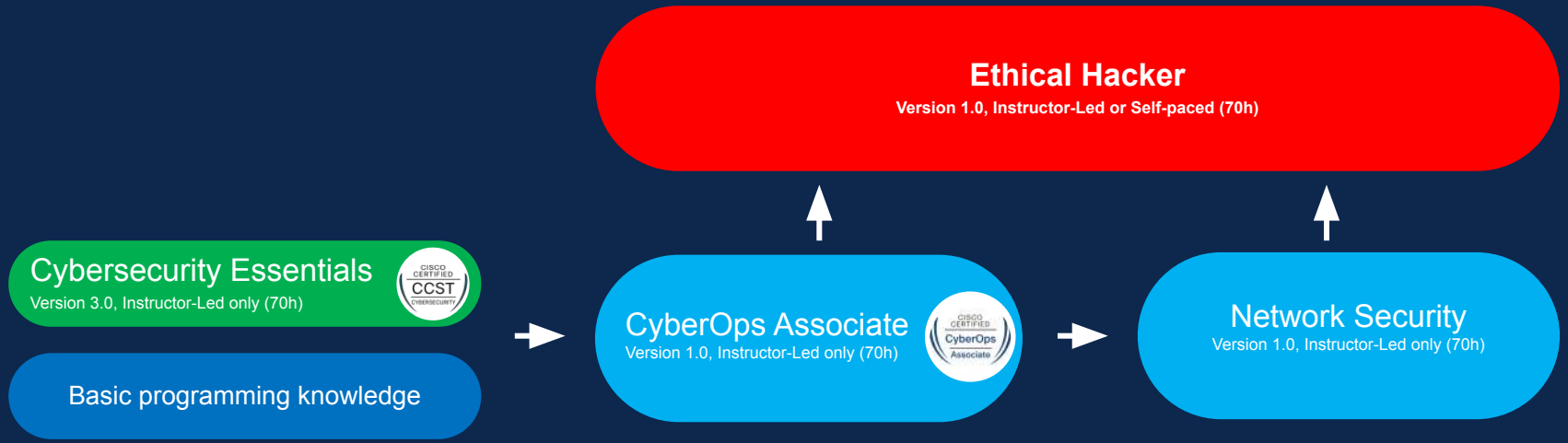
Ethical Hacker
Version 1.0, Instructor-Led or Self-paced (70h)

Trayectoria del alumno

Networking Academy

Trayectoria del alumno

Networking Academy



¡Manos a la obra!

Archivos del Taller:
http://cs.co/ethicalhackerWS24

Ataques de Ingeniería Social

Requisitos

- Kali VM
- Acceso a internet

Archivos del Taller:
http://cs.co/ethicalhackerWS24

En MV Kali – Para cambio a teclado en español
Abrir terminal en Kali setxkbmap es

Objectivos

Muchos exploits comienzan con un ataque de ingeniería social diseñado para obtener credenciales o plantar malware para crear puntos de entrada en la red objetivo. Una de las herramientas utilizadas para realizar estos ataques de ingeniería social es el Social Engineer Toolkit (SET), desarrollado por David Kennedy.

- Lanzamiento de SET y exploración del kit de herramientas
- Clonación de un sitio web para obtener credenciales de usuario
- Captura y visualización de credenciales de usuario

4.4.7 Lab - Explore the Social Engineering Toolkit - ILM

Rockyou

> I changed my password to "incorrect" so if I ever forget what it is, my computer will say "your password is incorrect"

Qué es Rockyou: Rockyou es un proveedor de medios sociales, redes sociales y aplicaciones que tenía su sede en San Francisco [California].

La filtración de datos: A Rockyou le iba muy bien hasta mediados de diciembre de 2009, cuando un hacker consiguió acceder sin autorización a la base de datos de sus cuentas.

El error: Rockyou no encriptó su base de datos, sino que la almacenó en texto simple. El hacker pudo acceder a más de 32 millones de nombres de usuario y contraseñas mediante un ataque de inyección SQL.

¿Qué hizo con los datos?
¿Venderlos?
¿Ransomware?

El Hacker simplemente subío el archivo [rockyou.txt] a internet

Rockyou

El "lado bueno" de Rockyou:

- Enseñó a las empresas a encriptar la información de las cuentas de sus usuarios. Ahora las empresas están obligadas por ley a encriptar este tipo de información para evitar que vuelvan a ocurrir sucesos como este.
- Enseñó a los usuarios a no utilizar contraseñas repetidas. Ver los 32 millones de cuentas de usuario expuestas libremente en Internet y los varios millones de usuarios que han tenido que lidiar con las secuelas es simplemente vergonzoso. Por favor, no utilices contraseñas repetidas.
- Introdujo un gran paso en la industria de la ciberseguridad. El archivo rockyou.txt es utilizado por profesionales de la ciberseguridad de todo el mundo para probar la seguridad de diferentes sistemas. Los hackers éticos utilizan este archivo para acceder a cuentas y encontrar ciertas vulnerabilidades en el sistema de un cliente.

https://www.cosmodiumcs.com/post/the-story-of-rockyou

Crunch

Cómo crear un diccionario de contraseñas con Crunch:

Crunch es un generador de listas de palabras en el que se puede especificar un conjunto de caracteres estándar o cualquier conjunto de caracteres que se vaya a utilizar para generar las listas de palabras. Las listas de palabras se crean mediante la combinación y permutación de un conjunto de caracteres. Puede determinar la cantidad de caracteres y el tamaño de la lista.
Este programa admite números y símbolos, caracteres en mayúsculas y minúsculas por separado y Unicode.

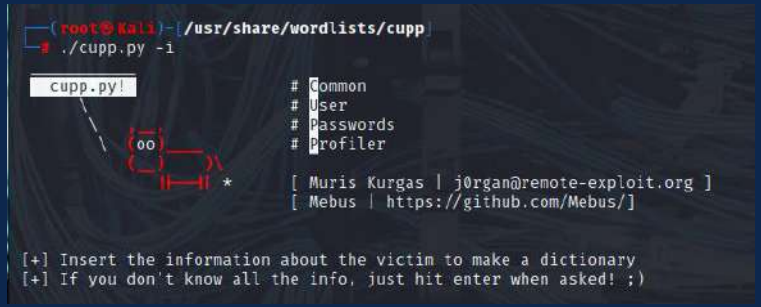
Tamaño instalado : 83 KB
Comando de instalación: sudo apt install crunch

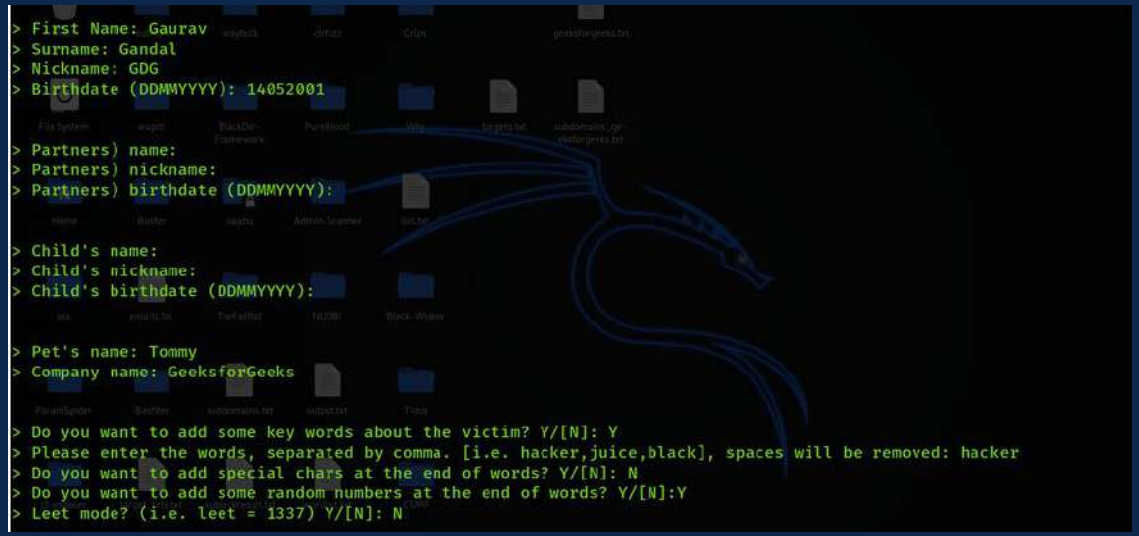
LAB

Cupp

Generar un diccionario personalizado.

Common User Passwords Profiler (CUPP) permite crear diccionarios específicos para una persona que pueden utilizarse al realizar un ataque de fuerza bruta para adivinar la credencial de inicio de sesión.





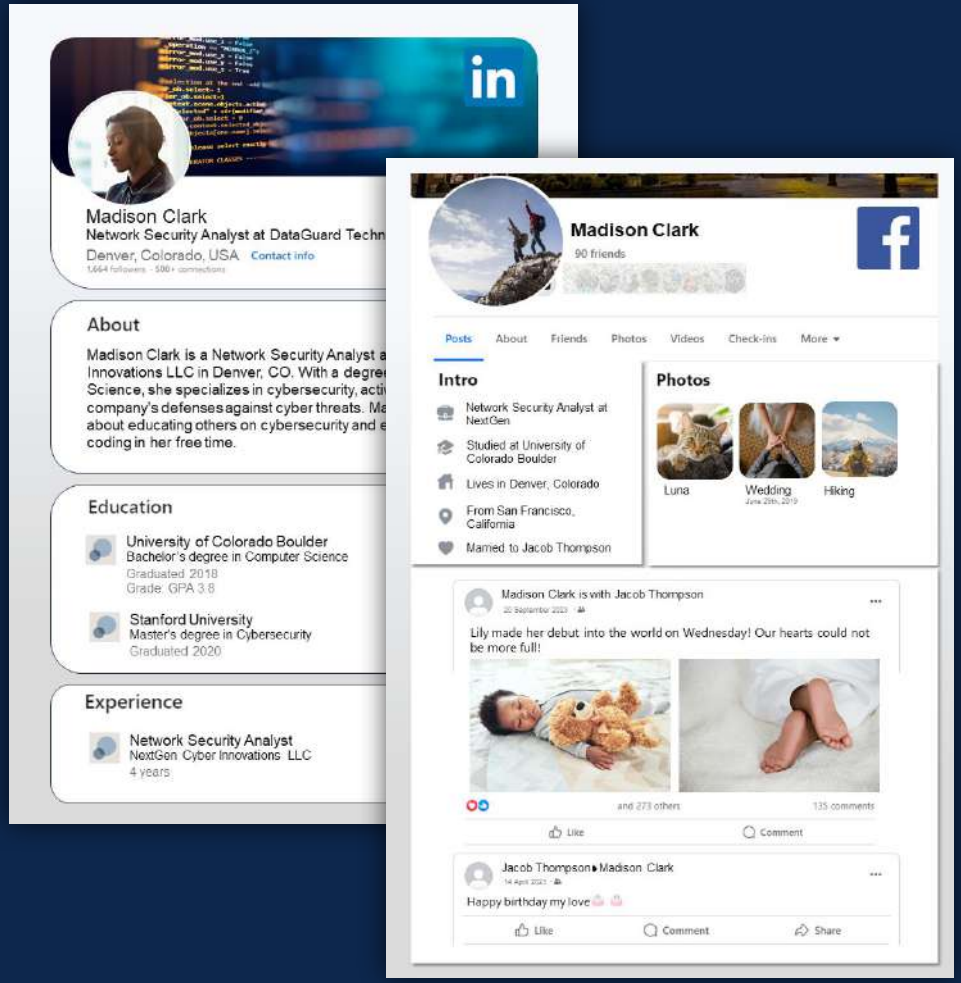
LAB

Cupp

Busca información sobre alguien en sus redes sociales y utiliza esa información para crear un diccionario e intentar entrar en sus cuentas.

Utiliza esa información en la herramienta Cupp para generar el diccionario.

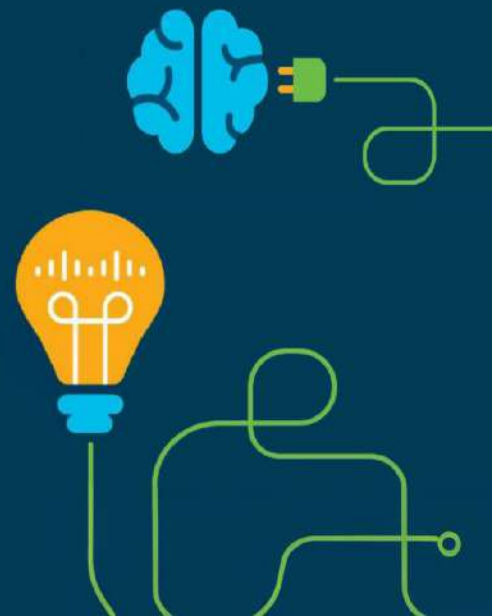
¿Podría alguien utilizar tus datos en Internet para usarlos en tu contra?



The bridge to possible

pue | academy

No te pierdas todas nuestras novedades
en nuestro perfil de LinkedIn



pue | academy

#PUEAcademyTalk

¡Muchas gracias!

para cualquier consulta, puedes dirigirte a

pueacademy@pue.es