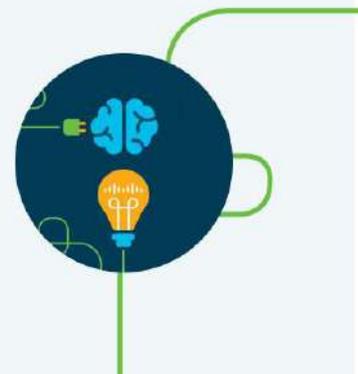




RAQUEL MARTÍNEZ

Technical Manager | EMEAR Cisco

Workshop sobre hacking ético: ataques de ingeniería social





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.

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.

40.9 MM

Número total de dispositivos previstos para 2025 en todo el mundo, incluidos smartphones, ordenadores, portátiles y dispositivos IoT¹

+125%

Las intrusiones informáticas notificadas aumentan un 125% anual en todo el mundo²

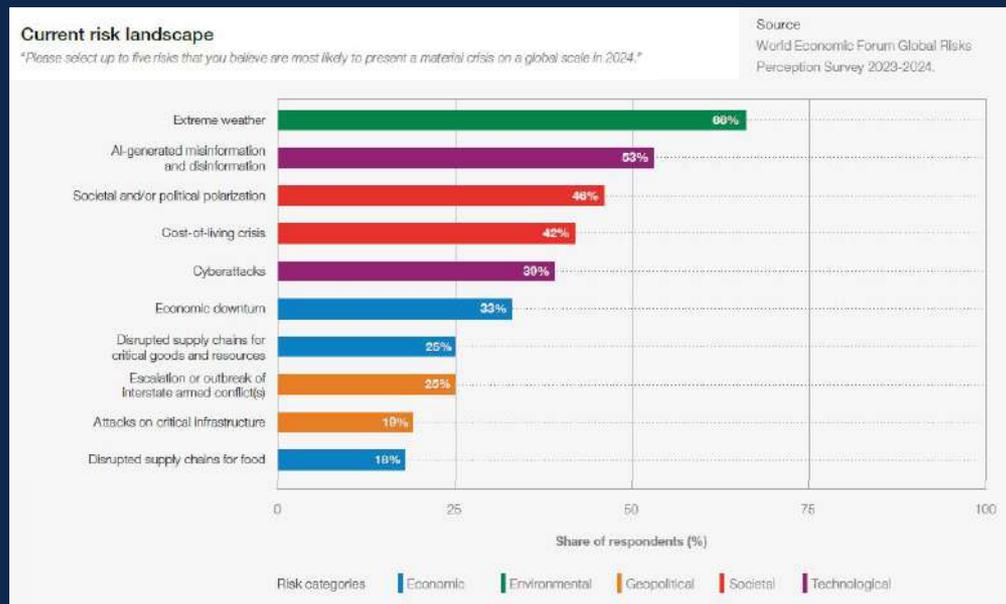
\$ 623 M

Los ataques de ransomware a gobiernos estatales y municipales de EE.UU. ascendieron a más de 623 millones de dólares en 2021³

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,](#)

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.



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

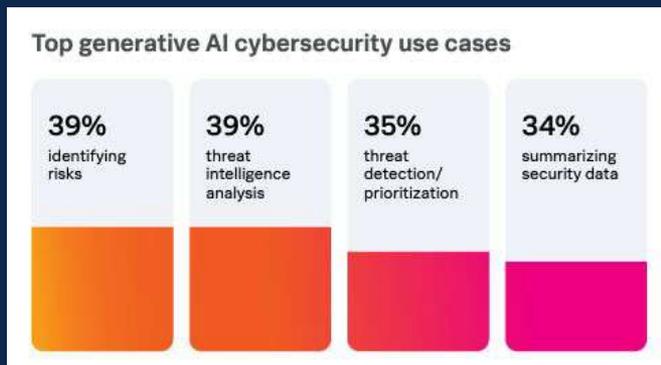
IA y Ciberseguridad

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.

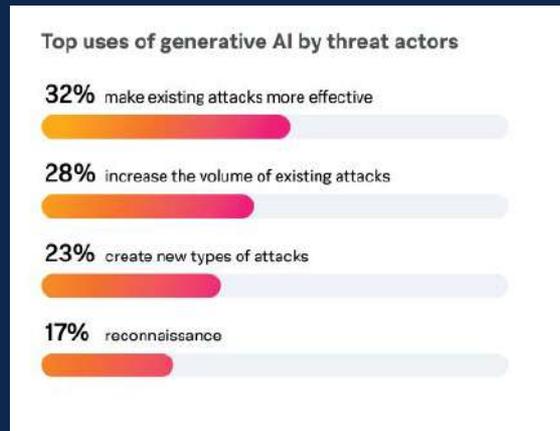
Pero también, los defensores parecen optimistas y están de acuerdo en que la IA generativa es una buena combinación para varios casos de uso de la ciberseguridad, nombrando el análisis de inteligencia de amenazas y la identificación de riesgos como las dos aplicaciones principales.



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?

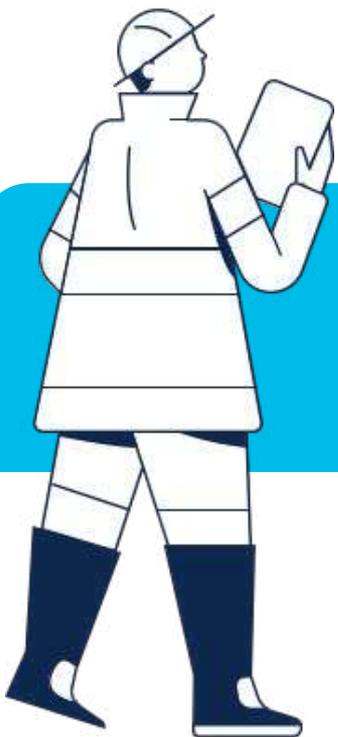
- Implantar soluciones basadas en IA: Tener la misma velocidad para detectar y responder a los ciberataques
- Formar a los empleados en las mejores prácticas de ciberseguridad
- Implementar la autenticación multifactor : puede ser una forma efectiva de evitar el acceso no autorizado a sistemas y datos.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

- 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 2025¹



97 millones
nuevos empleos

Creados por la transformación digital para 2025¹

El déficit de cualificaciones

3.5

escasez de profesionales de la
ciberseguridad en todo el mundo

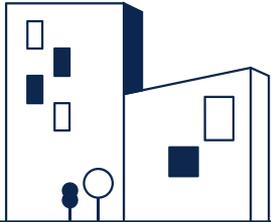
Millones

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

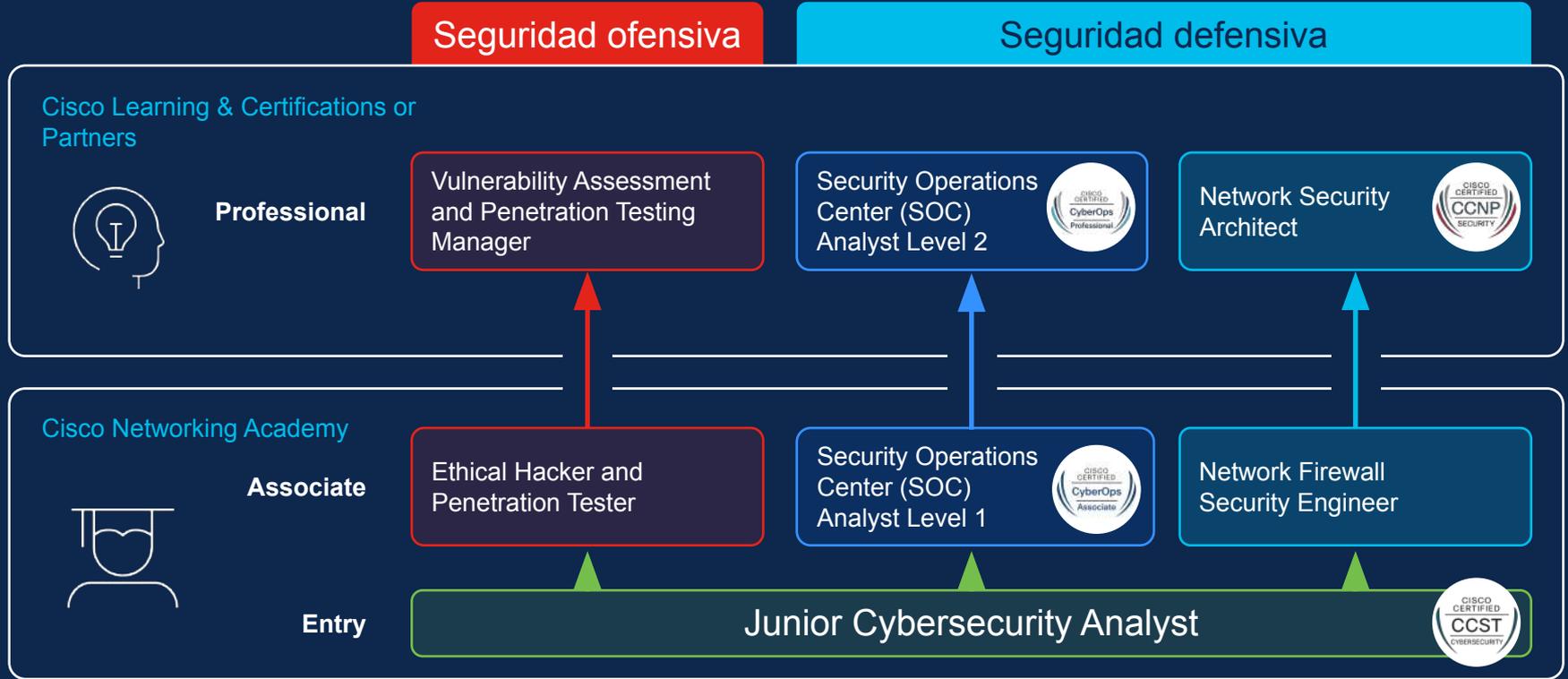
Es vital contar con profesionales que puedan liderar la ciberseguridad, probar y proteger los sistemas y formar a las personas en higiene digital.

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.



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

Narrativa gamificada



Offering the best in penetration testing and security assessment services.

Founded
2009 in San Francisco, CA by a group of cybersecurity professionals who had previously worked for the U.S. Department of Defense. Privately owned.

Employees
75 including a dedicated team of ethical hackers and cybersecurity analysts

Revenue
\$37 Million annually

Services
Security assessments, cybersecurity risk assessment, disaster recovery planning, user training and testing

Offices
Headquarters in San Francisco, CA. Branch offices in London and Singapore.

Protego Security Solutions employs a team of highly-skilled and certified cybersecurity professionals. In addition to penetration testing, we provide made-to-order cybersecurity training to our clients. Because of this focus on training and learning, we highly value promising entry-level candidates who can grow professionally in our supportive mentored environment.

Our Mission
At Protego Security Solutions (PSS), we are committed to helping our clients secure their networks, systems, and applications against cyber threats. Every business has a right to be secure. Our teams of ethical hackers and security experts are dedicated to identifying vulnerabilities, mitigating risks, and providing comprehensive solutions to protect our clients' digital assets.

Our Services

- Penetration Testing
- Vulnerability Assessment
- Network Security Testing
- Website Security Testing
- Mobile Application Security Testing
- Social Engineering Testing
- Cybersecurity Consulting
- User Security Training

Protego Personnel Certifications

- Infosec Institute Certified Penetration Tester (CPT)
- CompTIA PenTest+
- Certified Information Security Managers (CISM)
- Certified Information Systems Security Professionals (CISSP)
- Certified Ethical Hacker (CEH)
- Certified Expert Penetration Tester (CEPT)
- Global Information Assurance Certification (GIAC) Penetration Tester (GPEN)
- And many others.

Accreditations

- PCI Qualified Security Assessor ("QSA")
- HITRUST CSF
- Council of Registered Ethical Security Testers (CREST)
- ISO 27001
- CHECK Service Provider

About Us
At Protego, we believe in each other. We value the contributions of all employees and create a people-first culture of inclusion. We are proud to engage with our Bay Area community, and we are committed to continued growth and leadership in the gaming industry.



Matt Willis
CEO, Founder



Janice Katz
V.P. Finance



Fernando Gomes
V.P. Technology



Alex Prevost
Director, Customer Engagement



Our mission is to push the boundaries of creativity and innovation in the gaming industry to the next level. Our quest is to create immersive engaging gaming experiences that captivate players and inspire them to explore rich new worlds, conquer new challenges, and take off on exciting adventures.

As a company, we are dedicated to fostering a culture of collaboration, excellence, and inclusivity. We value the contributions of every team member. We are proud to be based in San Francisco, a hub of innovation and creativity, and we are excited to continue to grow and expand our reach in the years to come.



Elizabeth deGray
Creative Director & CEO



William A. Hurst
Technical Director



Alphonse Luis Silva
V.P. Marketing & Sales

Living on island time since 2012
Privately Owned

75 developers, programmers, graphic designers, content creators
\$30 Million Annual Revenue
Games for Windows, MacOS, Linux, and all major gaming platforms
+ tee shirts, coffee mugs, posters, and other swag

Just a few awards...



- 2013 Most Promising New Video Game Enterprise, International Association Video Game Traders (IAVGT)
- 2013 Runner Up, Games World Magazine best games of the year
- 2015 3rd Place, Games World Magazine best games of the year
- 2019 European Gamers Alliance Outstanding New Game
- 2020 Celtic Fog Warriors Union best of 2020



Resumen del curso

Laboratorios prácticos y ejercicios

1.2.3 Environmental Considerations

There are, of course, a number of different types of penetration tests. Often they are contained in the overall scope of a penetration test; however, they can also be performed as individual tests as well.

The following is a list of some of the most common environmental considerations for the types of penetration tests below:

Network Infrastructure Tests **Application-Based Tests** **Penetration Testing to the Cloud**

Network Infrastructure Tests

Testing of the network infrastructure can mean a few things. For the purposes of this course, we say it is focused on evaluating the security posture of the actual network infrastructure and how it is able to help defend against attacks. The others include the wireless, intrusion, tunnels, and supporting infrastructure, such as authentication, authorization, and accounting (AAA) servers and firewalls. A penetration test on wireless infrastructure may sometimes be included in the scope of a network infrastructure test. However, additional types of tests beyond a wired network assessment would be performed. For instance, a wireless security tester would attempt to connect with a network to the wireless network either by bypassing security mechanisms or breaking the cryptographic methods used to secure the traffic. Testing the wireless infrastructure helps an organization to determine weaknesses in the wireless equipment as well as the equipment. It often includes a detailed test map of the signal environment.

NOTE: Many penetration testers find the physical aspect of testing to be the most fun because they are essentially being paid to break into the facility of a target. This type of test can help expose any weaknesses in the physical perimeter, as well as any security mechanisms that are in place, such as guards, gates, and fencing. The result should be an assessment of the external/physical security controls. The majority of corporations today start with some level of social engineering attack. This could be a phone call, an email, a website, an SMS message, and so on. It is important to test how your employees handle these types of situations. This type of test is often omitted from the scope of a penetration testing engagement mainly because it primarily involves being caught. Instead of the technology, in most cases, management does not agree with this type of approach. However, it is important to get a high-level view of the client about interests. The result of a social engineering test should be to assess the security awareness program to that you can enhance it. It should not be to identify individual employees for the test. One of the tests that we talk about more in a later module is the Social-Engineer Toolkit (SET), created by Dave Kennedy. This is a great tool for performing social engineering testing campaigns.



TIP: Bug bounty programs enable security assessors and penetration testers to get recognition (and often monetary compensation) for finding vulnerabilities in websites, applications, or any other types of systems. Companies like Microsoft, Apple, and Cisco and some government institutions such as the UK's Department of Defense (DOD) are big security programs to reward security professionals when they find vulnerabilities in their systems. Many security companies, such as HackerOne, Bugcrowd, Bright, and Synack, provide platforms for businesses and security professionals to participate in bug bounty programs. These programs are different from traditional penetration testing engagements but have a similar goal: finding security vulnerabilities to allow the organization to fix them before malicious attackers are able to exploit such vulnerabilities. These include different bug bounty SaaS and resources in my GitHub repository at: <https://github.com/0x00sec/0x00sec/blob/master/README.md>

When talking about penetration testing methods, you are likely to hear the terms unknown-environment (previously known as black-box), known-environment (previously known as white-box), and partially known environment (previously known as gray-box) testing. These terms are used to describe the perspective from which the testing is performed, as well as the amount of information that is provided to the tester.

Unknown-Environment Test **Known-Environment Test** **Partially Known Environment Test**

Unknown-Environment Test

In an unknown-environment penetration test, the tester is typically provided only a very limited amount of information. For instance, the tester may be provided only the domain names and IP addresses that are in scope for a particular target. The idea of this type of information is to have the tester start out with the perspective that an external attacker might have. Typically, an attacker would first determine a target and then begin to gather information about the target, using public information, and gain more and more information to use in attacks. The tester would not have prior knowledge of the target's organization and infrastructure. Another aspect of unknown-environment testing is that sometimes this network support personnel of the target may not be given information about security when the test is taking place. This allows for a defense exercise to take place as well, and to simulate the basis of a target preparing for the test and not giving a real-world view of how the security posture really looks.

1.2.4 Practice - Types of Penetration Tests

Protego has been contracted to do a network infrastructure test as part of a broader penetration testing engagement. What will you be targeting in this test? (Choose all that apply.)

- IPS devices
- switches
- AAA servers
- virtual machines (VM) that are running in the cloud

the digital storefront

Reset

Show feedback

Show correct answer

1.3.6 Lab - Deploy a Pre-Built Kali Linux Virtual Machine (VM)



Prerequisite: Security Solutions Test

Kali is a great tool! We are providing you with a working version of it that you can use to start your hands-on practice penetration testing techniques. The Kali Linux version that I am giving you contains all of the full tools and scripts, otherwise, download images that you can install on virtual testing target systems. I encourage you to use the available targets and other subjects that you have permission to view, such as your home network. Be careful though, Kali provides some very powerful tools!

Find you need to install and run the virtual machine, and from the lab target!

In this lab, you will complete the following objectives:

- Part 1: Deploying a Customized Kali Linux VM on AMD or Intel Chip-based Computer
- Part 2: Deploying a Customized Kali Linux VM on ARM M1/M2 based MacOS Computer
- Part 3: Exploring Linux

Lab - Deploy a Pre-Built Kali Linux Virtual Machine (VM)

Select play to watch a demonstration of the lab.

Video - Deploy a Pre-Built Kali Linux Virtual Machine (VM)

Part 1: Deploying a Customized Kali Linux VM on AMD or Intel Chip-based Computer

Part 2: Deploying a Customized Kali Linux VM on ARM M1/M2 based MacOS Computer

Part 3: Exploring Linux

Please answer the following questions after you have completed the lab.

Skills Check

You have just downloaded and installed VirtualBox or UTM. What do you do next? (Select all that apply.)

- You need to update the install files to the latest version.
- You need to download and import the Kali VM file in VirtualBox or UTM.
- There may be an issue with the installation. You may need to install VirtualBox or UTM.
- You must use VirtualBox or UTM to connect to the virtual machine on the labging website.

Submit

Show feedback

Lab Survey

Please let us about your experience with the lab by indicating your level of agreement with the following statements.

I had feedback about the lab's content with this lab.

Please select an option

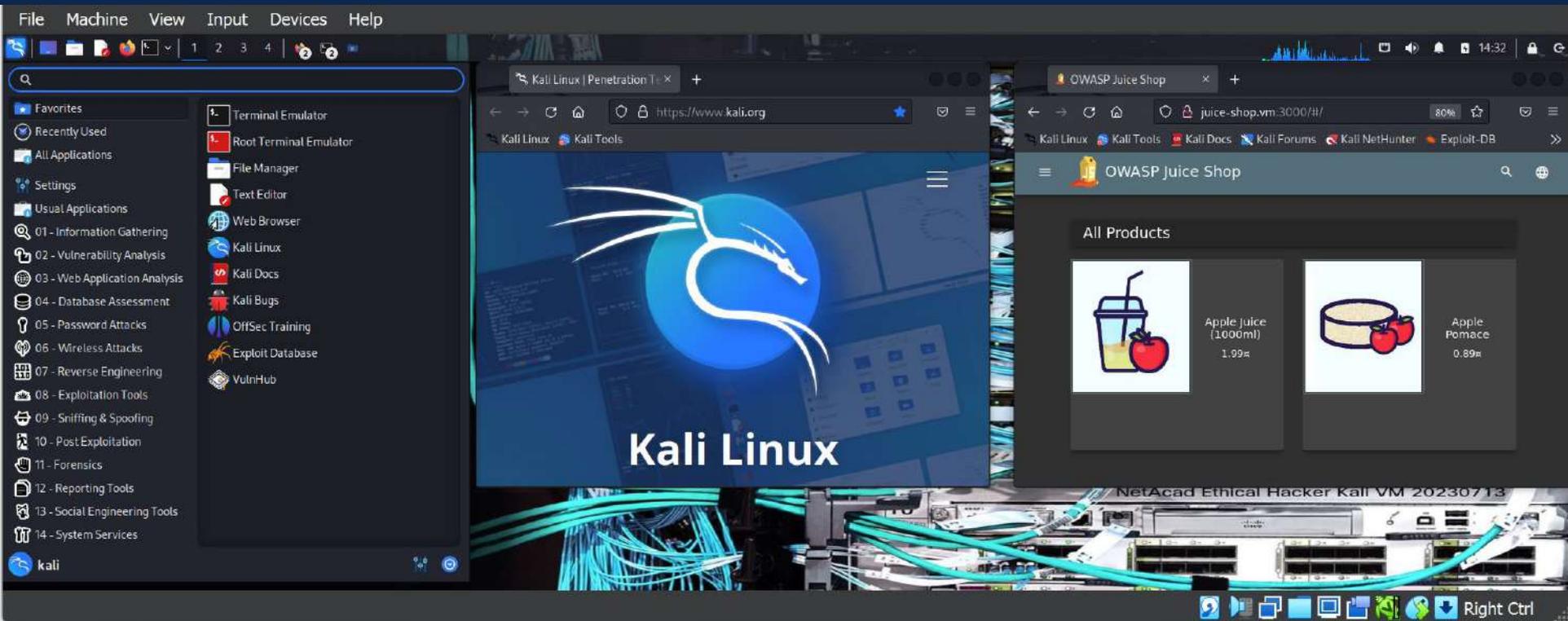
Completing this lab was a good use of my time.

Please select an option

Submit

Show feedback

Entorno de laboratorio



Trayectoria del alumno

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

Cybersecurity Essentials

Version 3.0, Instructor-Led only (70h)



Basic programming knowledge



CyberOps Associate

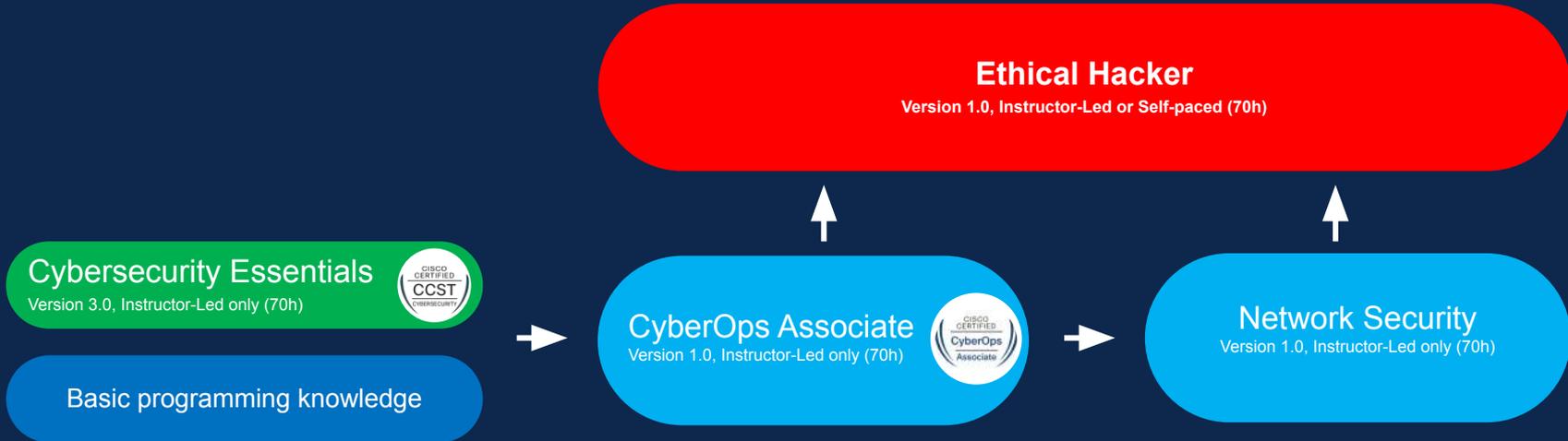
Version 1.0, Instructor-Led only (70h)



Ethical Hacker

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

Trayectoria del alumno



¡Manos a la obra!

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



Ataques de Ingeniería Social

Requisitos

- Kali VM
- Acceso a internet

Objetivos

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

Archivos del Taller:

<http://cs.co/ethicalhackerWS24>

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

4.4.7 Lab - Explore the Social
Engineering Toolkit - ILM

LAB

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
subió 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>

The image shows the Rockyou logo, which consists of the word "rockyou" in a lowercase, white, sans-serif font. The logo is centered within a solid teal rectangular background.

Crunch

Cómo crear un diccionario de contraseñas con

Crunch, 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`



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.

```
(root@kali) ~ | /usr/share/wordlists/cupp |
# ./cupp.py -i

cupp.py!
# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)
```

```
> First Name: Gaurav
> Surname: Gandal
> Nickname: GDG
> Birthdate (DDMMYYYY): 14052001

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name: Tommy
> Company name: GeeksforGeeks

> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: hacker
> Do you want to add special chars at the end of words? Y/[N]: N
> Do you want to add some random numbers at the end of words? Y/[N]: Y
> Leet mode? (i.e. Leet = 1337) Y/[N]: N
```

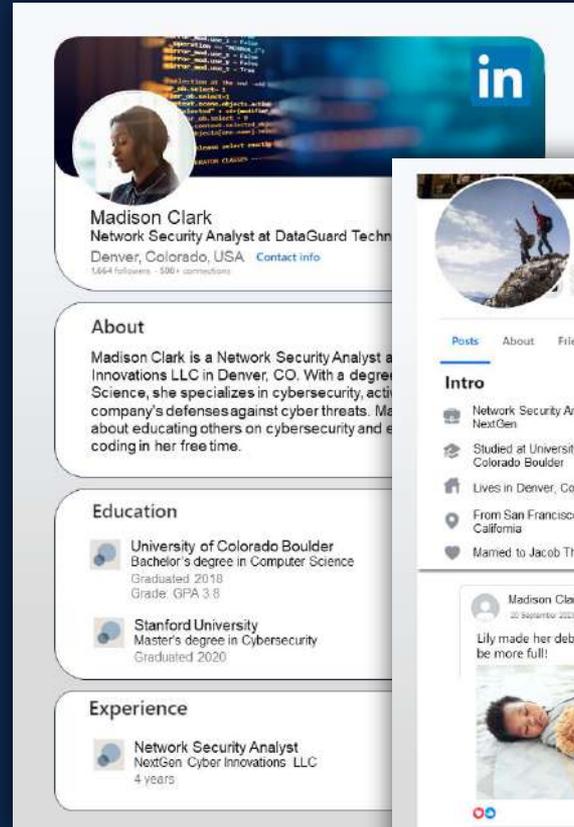
LAB

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?



LinkedIn profile of Madison Clark, Network Security Analyst at DataGuard Tech. The profile includes a cover image with code, a profile picture, and sections for About, Education, and Experience.

Madison Clark
Network Security Analyst at DataGuard Tech
Denver, Colorado, USA [Contact info](#)
1,664 followers · 500+ connections

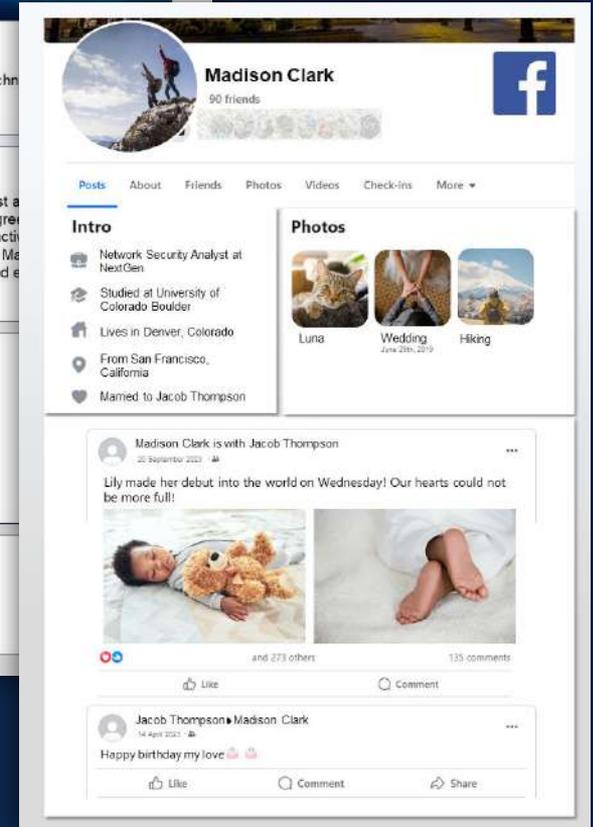
About
Madison Clark is a Network Security Analyst at Innovations LLC in Denver, CO. With a degree in Computer Science, she specializes in cybersecurity, acting as a key player in the company's defenses against cyber threats. Madison is also about educating others on cybersecurity and ethical hacking in her free time.

Education

- University of Colorado Boulder**
Bachelor's degree in Computer Science
Graduated 2018
Grade: GPA 3.8
- Stanford University**
Master's degree in Cybersecurity
Graduated 2020

Experience

- Network Security Analyst**
NextGen Cyber Innovations LLC
4 years



Facebook profile of Madison Clark, Network Security Analyst at NextGen. The profile includes a cover image, a profile picture, and sections for Intro, Photos, and a recent post.

Madison Clark
90 friends

Intro

- Network Security Analyst at NextGen
- Studied at University of Colorado Boulder
- Lives in Denver, Colorado
- From San Francisco, California
- Mmarried to Jacob Thompson

Photos

- Luna
- Wedding (July 25th, 2019)
- Hiking

Madison Clark is with Jacob Thompson
20 September 2023 · 44

Lily made her debut into the world on Wednesday! Our hearts could not be more full!

and 273 others · 135 comments

Jacob Thompson • Madison Clark
14 April 2023

Happy birthday my love 🎂🎉



The bridge to possible

No te pierdas todas nuestras novedades
en nuestro perfil de LinkedIn



¡Muchas gracias!

para cualquier consulta, puedes dirigirte a
pueacademy@pue.es