Cymetrics

紅隊勇者的證照冒險攻略

Cymetrics Security Research Engineer
楊士賢 Ken Yang

Cymetrics

楊士賢 Ken Yang

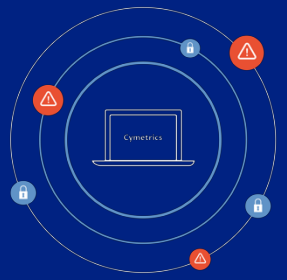
Security Research Engineer @ Cymetrics

- 擁有 20+ 張專業證照
- 揭露 30+ CVEs

👉 https://linktr.ee/4hsienyang

Start Proactive Cyber Defense Today

漸進式資安評估

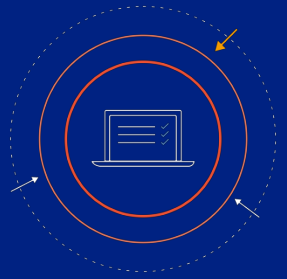


外部攻擊面管理
EASM

Cymetrics EASM 簡化了網路安全監控，消弭了持續監督的低效率。我們的 EASM 評估不具侵入性，提供即時、全面的資安審查。

弱點評估
VAS

Cymetrics VAS 提供自動化的漏洞評估服務，用戶可快速獲得測試結果。我們精心挑選測試項目，結合滲透測試經驗，增強評估的深度和有效性。



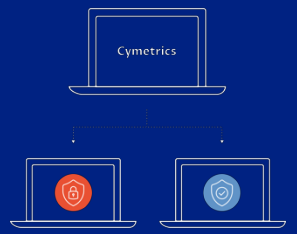
滲透測試
PTS

Cymetrics VAS 提供自動化的漏洞評估服務，用戶可快速獲得測試結果。我們精心挑選測試項目，結合滲透測試經驗，增強評估的深度和有效性。

全方位資安服務

紅隊演練
Red Teaming

結合最新攻防技術，模擬 APT 攻擊，測試應用與網路架構弱點，確保系統安全。透過實戰模擬與多層滲透測試，提升企業對抗網路威脅能力。



第三方網路風險管理
TPRM

透過我們的服務，加強您的第三方網路風險管理流程。透過 TPRM API，將風險管理整合到您現有的公司系統中，以提升效率。

Web3 資安風險評估
Web3 Security Solutions

透過滲透測試與智能合約審計，挖掘漏洞並保障 Web3 安全，涵蓋應用、API、錢包完整性、智能合約與權限控制，全方位保護您的 Web3 業務。

關於 Cymetrics AI 紅隊演練

專業認證

我們團隊持有 ISO 42001主導稽核員認證，專精於 AI 系統治理，以及符合倫理和負責任的 AI 原則。

LLM 專業知識

透過我們深厚的 LLM 系統設計和架構專業知識，將能全面了解 LLM 特殊漏洞。

自動化檢測工具

利用我們的檢測工具 Vulcan 和全面的測試案例庫，隨選即用或預設排程，進行完整的 AI 風險檢測。

無縫整合

輕鬆配置路徑和 API 密鑰，與您的 LLM 端點無縫整合。

實用見解

我們將提供詳細報告和專家建議，展示所發現的漏洞和可改善的建議，幫助您的團隊迅速緩解 AI 風險。

打造一個 AI 韌性的生態系

藉由 Cymetrics 進階的平台和服務，包括 AI 紅隊演練、弱點評估和滲透測試，進一步提升您生態系統的韌性。

Cymetrics

Cymetrics

●團隊之紅隊演練檢測人員應具備專業要求，至少需具備下列證照至少 X 張。

– CEH(EC-Council Certified Ethical Hacker)。

– CPENT(EC-Council Certified Penetration Tester)。

– CompTIA PenTest+。

– CPSA(The

– OSCP(Offe

– 其他資安

●紅隊演練檢測人員

具備 CPENT、CPSA 或 OSCP 等證照，同時有多年相關工作經歷，具備專業駭客思維與能力，能模擬各式滲透攻擊以發掘系統或網路中潛在威脅。此項為演練優先情境之需求人員，建議紅隊團隊應具備至少三張以上專業證照。

Cymetrics

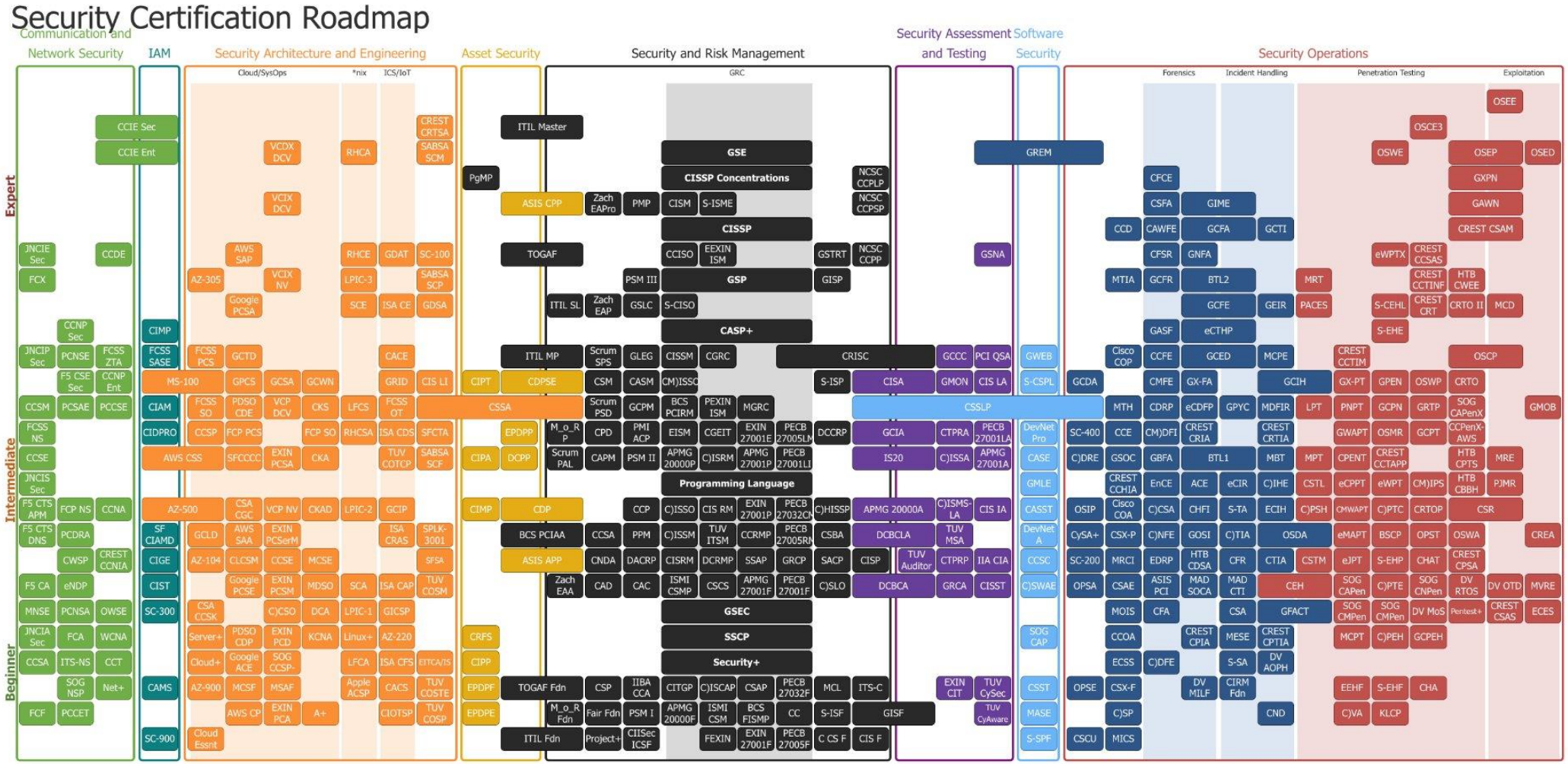
資通安全專業證照清單

日期：114年1月24日修正公布

序	發證機構(單位)	管理類(22)	技術類(89)
1.	已簽署國際認證論壇(International Accreditation Forum, IAF)多邊相互承認協議(ISO/IEC 27006範圍)之認證機構(含TAF)所認證之資訊安全管理系統驗證機構、稽核員驗證或註冊之國際專業機構[1]	1. ISO/IEC 27001:2013 Information Security Management System (ISMS) Auditor/Lead Auditor (請於114年10月31日前完成轉版) 2. ISO/IEC 27001:2022 Information Security Management System (ISMS) Auditor/Lead Auditor 3. ISO 22301 Business Continuity Management System (BCMS) Auditor/Lead Auditor 4. ISO/IEC 27701:2019 Privacy Information Management System Lead Auditor	

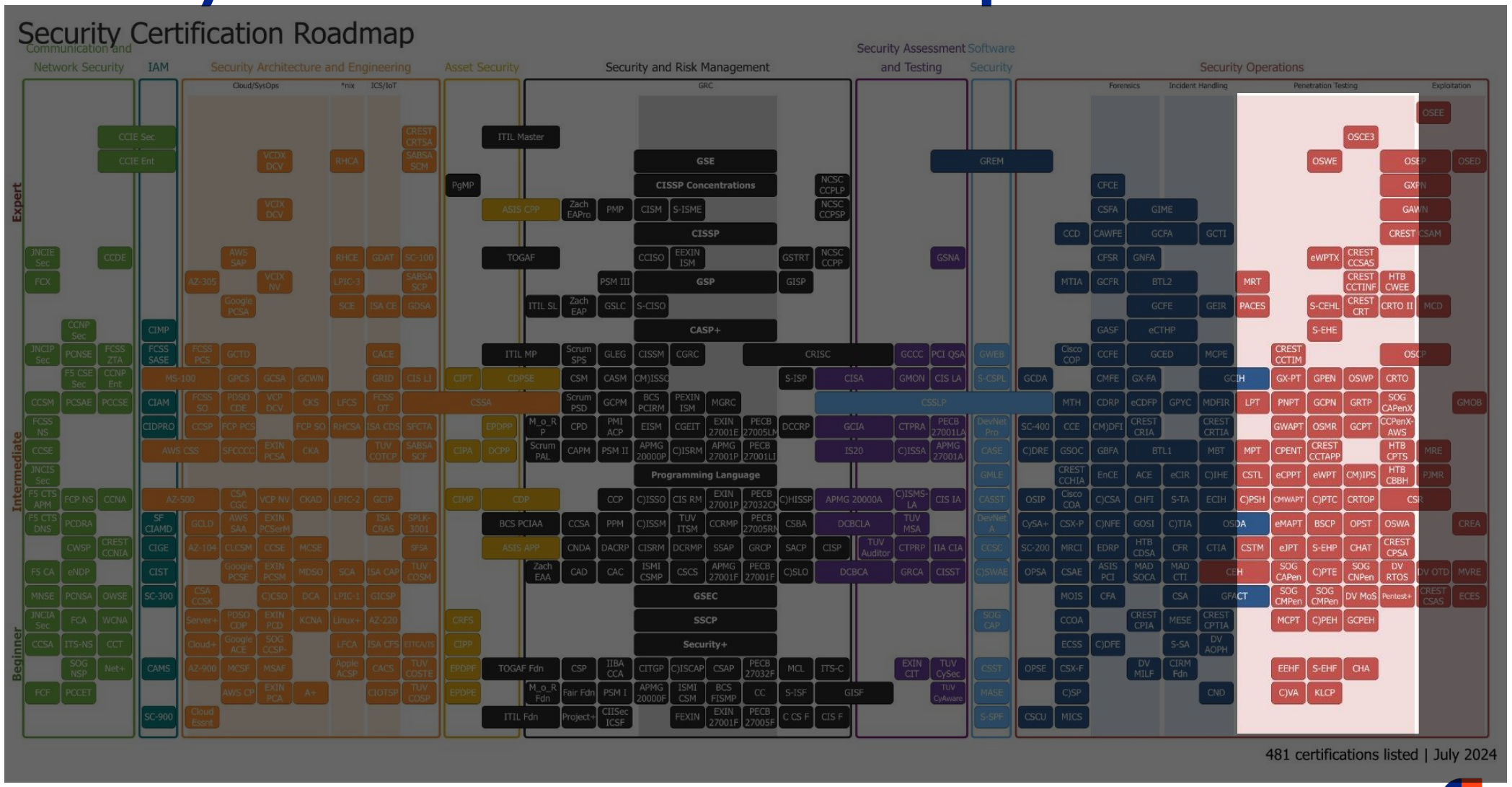
Cymetrics

Security Certification Roadmap



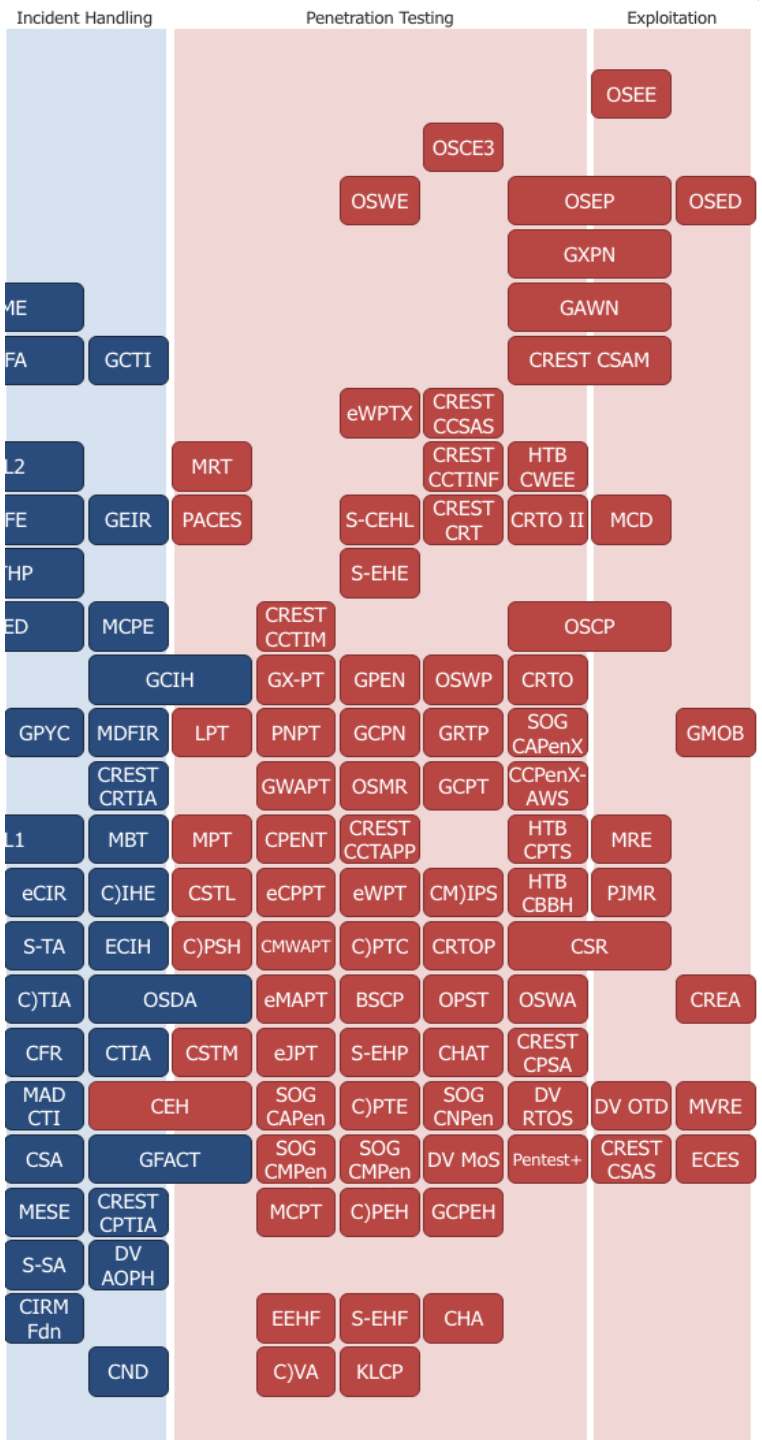
Cymetrics

Security Certification Roadmap



Cymetrics

Security Certification Roadmap



Cymetrics

Security Certification Roadmap

Level 1

Cymetrics

Security Certification Roadmap

Level 2

EC-Council LPT LICENSED PENETRATION TESTER MASTER CERTIFIED

GIAC PENETRATION GPEN TESTER

OFFENSIVE security OSCP

Level 1

EC-Council CEH CERTIFIED

CREST CPSA PRACTITIONER

CompTIA PenTest+ CERTIFIED

Cymetrics

Security Certification Roadmap

Level 3

Level 2

Level 1

Cymetrics

Cymetrics


E-COMMERCE CONSU
INTERNATIONAL COUNCIL
EC-Council
Offsec™
The Path to a Secure Future™

Cymetrics

選擇題

實作題

Cymetrics

eLearnSecurity - eJPT

Exam Objectives

The eJPT evaluates an individual's skills across various domains and objectives, certifying their mastery and understanding.

Assessment Methodologies (25%)

- Locate endpoints on a network
- Identify open ports and services on a target
- Identify operating system of a target
- Extract company information from public sources
- Gather email addresses from public sources
- Gather technical information from public sources
- Identify vulnerabilities in services
- Evaluate information and criticality or impact of vulnerabilities

Host and Networking Auditing (25%)

- Compile information from files on target
- Enumerate network information from files on target
- Enumerate system information on target
- Gather user account information on target
- Transfer files to and from target
- Gather hash/password information from target

Host and Network Penetration Testing (35%)

- Identify and modify exploits
- Conduct exploitation with metasploit
- Demonstrate pivoting by adding a route and by port forwarding
- Conduct brute-force password attacks and hash cracking

Web Application Penetration Testing (15%)

- Identify vulnerabilities in web applications
- Locate hidden file and directories
- Conduct brute-force login attack
- Conduct web application reconnaissance

https://security.ine.com/certifications/ejpt-certification/

Cymetrics

The SecOps Group - CNPen

Exam Syllabus

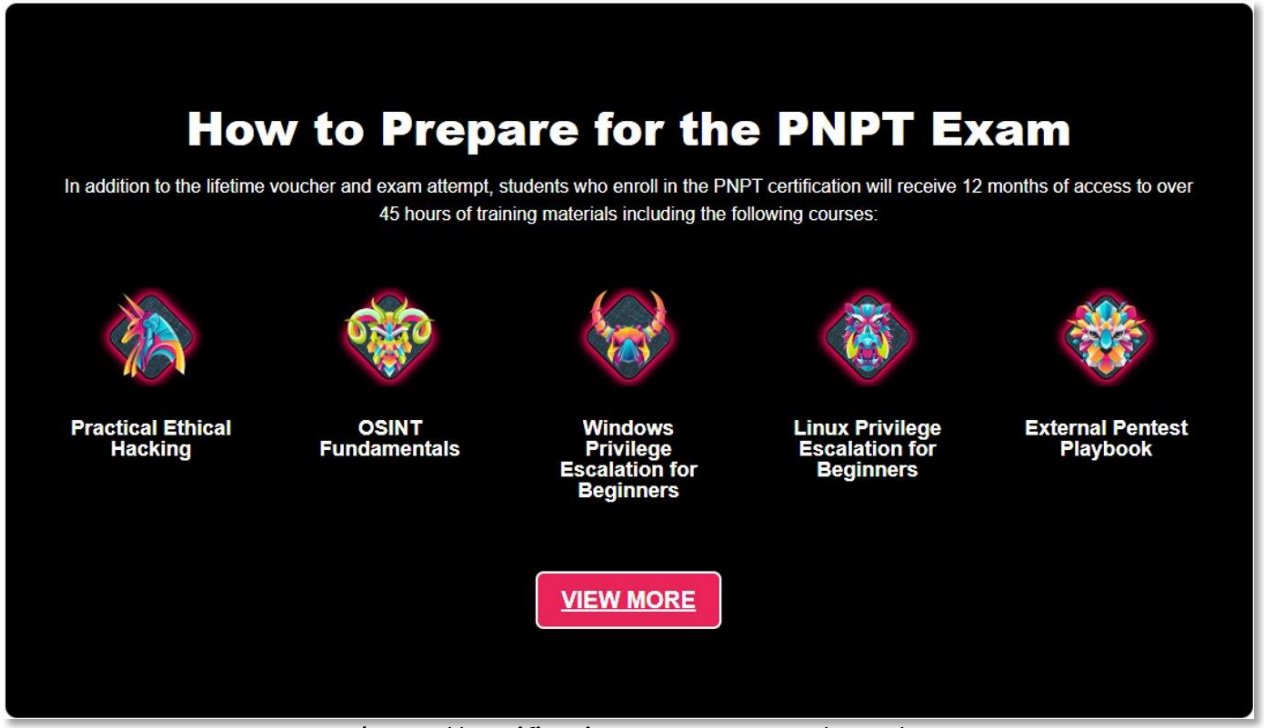
The exam will cover the following topics:

- Common OSINT Techniques
- Network Mapping And Target Identification
- Brute-Force Attacks
- Vulnerability Identification And Exploitation Using Common Hacking Tools
- Application Server Flaws
- Insecure Protocols
- *Nix Vulnerabilities
- Insecure File Permissions
- Security Misconfigurations Leading To Privilege Escalation Attacks
- Windows Active Directory Attacks (On-Premise)
- OS Credential Dumping And Replay
- Kerberoasting; Golden And Silver Tickets
- Password Attacks And Password Cracking
- Administrative Shares Exploitation
- Persistence Techniques
- Lateral Movements
- Common Security Weaknesses Affecting Cloud Services

https://secops.group/product/certified-network-pentester/

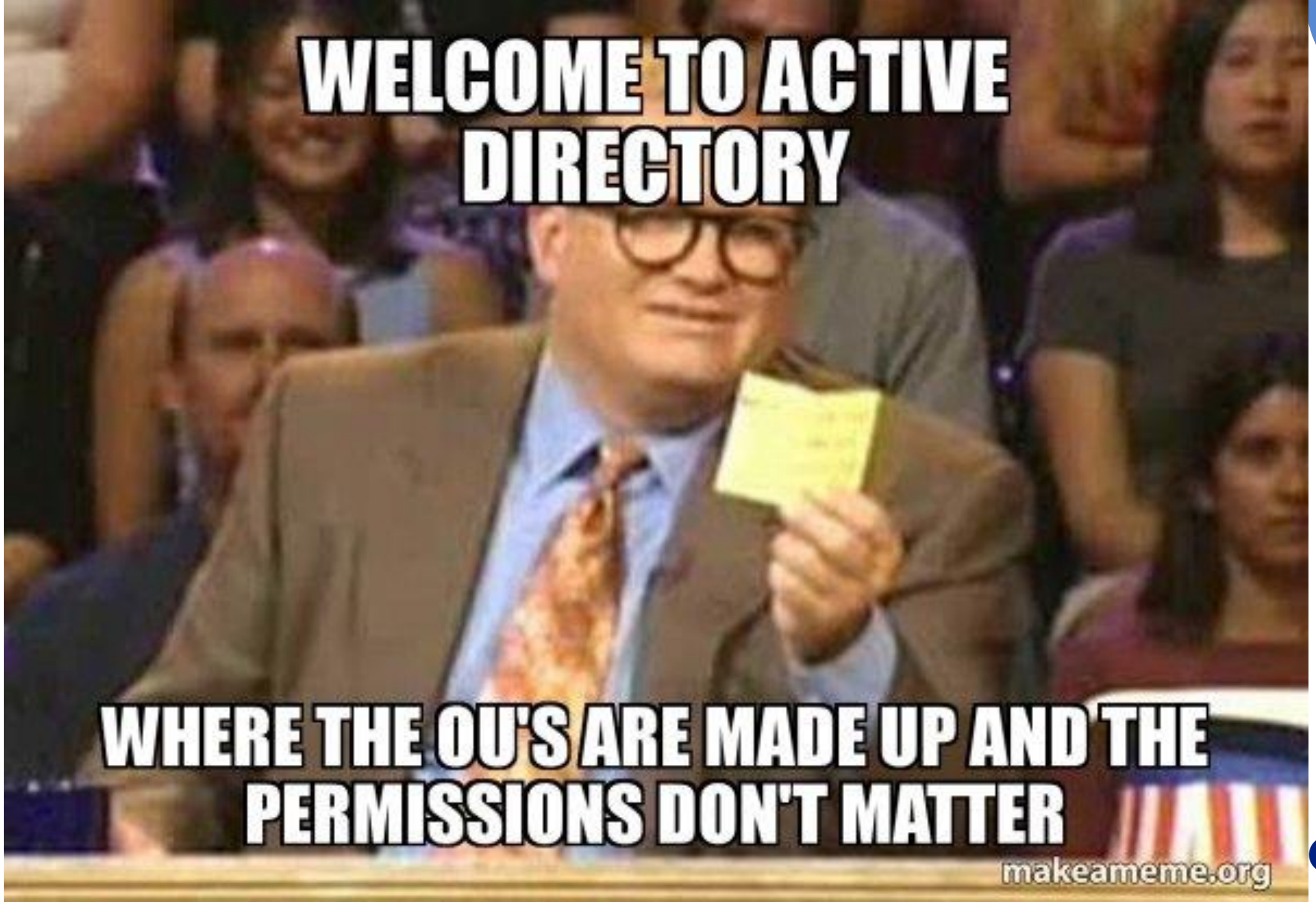
Cymetrics

TCM Security - PNPT



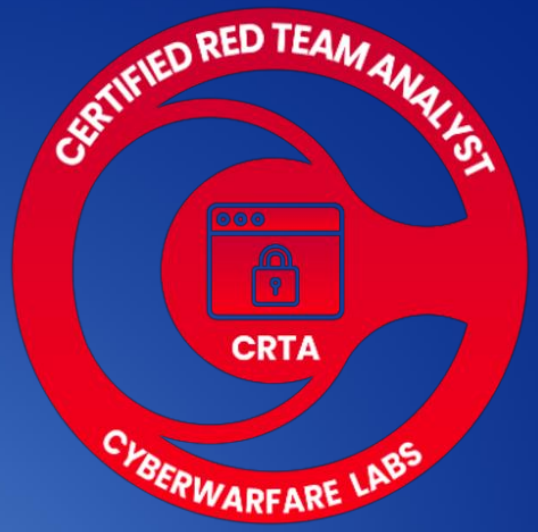
https://certifications.tcm-sec.com/pnpt/

Cymetrics


WELCOME TO ACTIVE DIRECTORY
WHERE THE OU'S ARE MADE UP AND THE PERMISSIONS DON'T MATTER
makeameme.org

Cymetrics

CyberWarFare Labs - CRTA



The courses contents are divided across 5 sections listed below:

Introduction to Red Teaming

- What is Red Teaming?
- Red Team Attack Lifecycle (Phases)
- Red Team Infrastructure (Nomenclature)
- Enterprise Environment Overview
- Technologies Exploitation in Red Teaming (Web, Network, Cloud)

Red Team Lab setup

- Virtual Environment Setup & Configuration
- Setting up Attacker Machine
- External Red Team Lab Setup
- Network Pivoting Setup
- Internal Red Team Lab Setup (Active Directory Setup)

External Offensive Operations

- External Infrastructure Overview
- Enumerating & Mapping External exposed assets
- Externally exposed service exploitation
- Exploitation (Web & Network based)
- Post-Exploitation (Web & Network based)

Internal Offensive Operations

- Internal Infrastructure Overview
- Enumerating & Mapping Internal assets
- Infrastructure Enumeration (Active Directory Environment)
- Bypassing Network Segmentation (Firewalls)
- Active Directory Phases Exploitation (Initial Recon to Domain Admin)

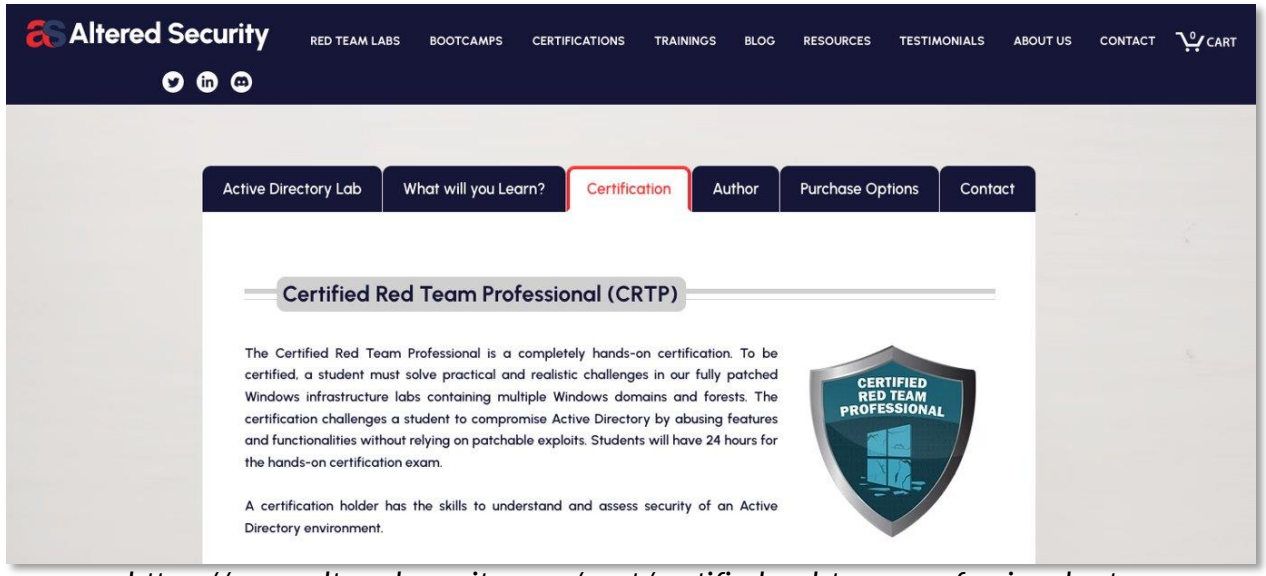
Practical Case Study (Hands-on Lab)

- Accessing the Lab
- Lab Architecture
- Mapping the Lab with MITRE ATT&CK Framework
- External Red Teaming
- Internal Red Teaming
- Utilizing LOLBAS for stealth persistence & Data Exfiltration
- Preparing for Examination

https://cyberwarfare.live/product/red-team-analyst-crta/

Cymetrics

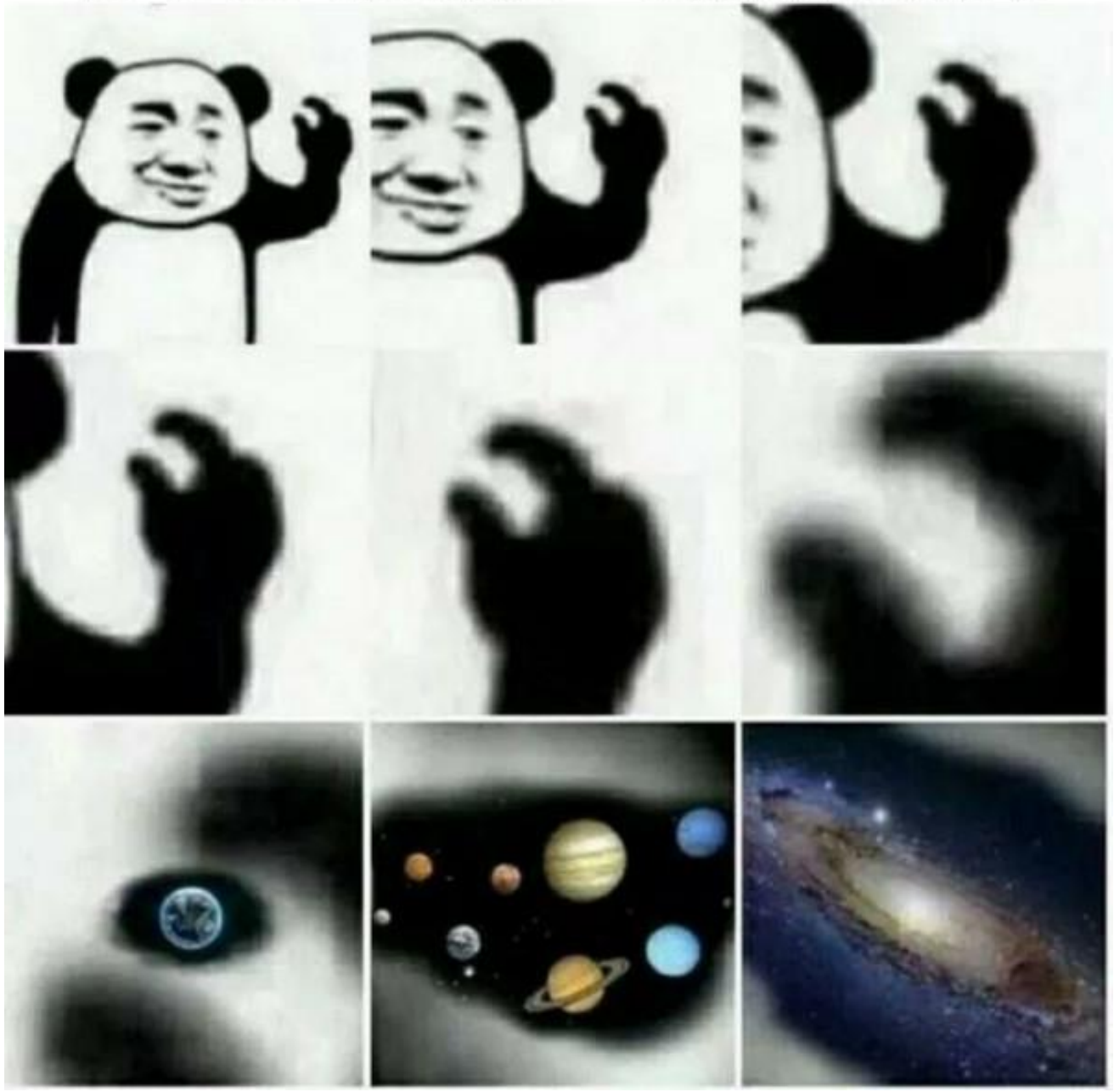
Altered Security - CRTP



https://www.alteredsecurity.com/post/certified-red-team-professional-crtp

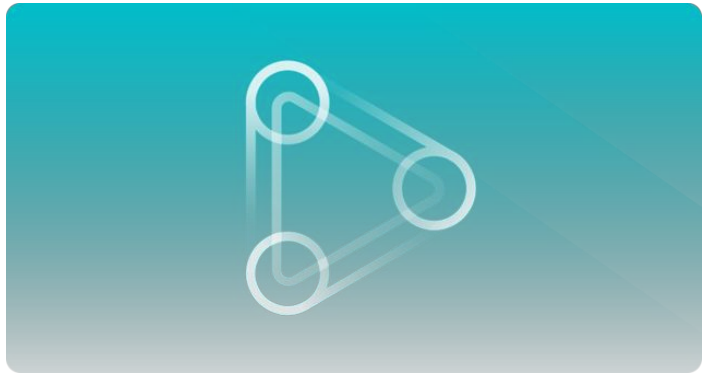
Cymetrics

學習只要花一點點時間



Cymetrics

OffSec Proving Grounds Labs



Proving Grounds Practice

$199 USD/Year
or $19 USD/Month

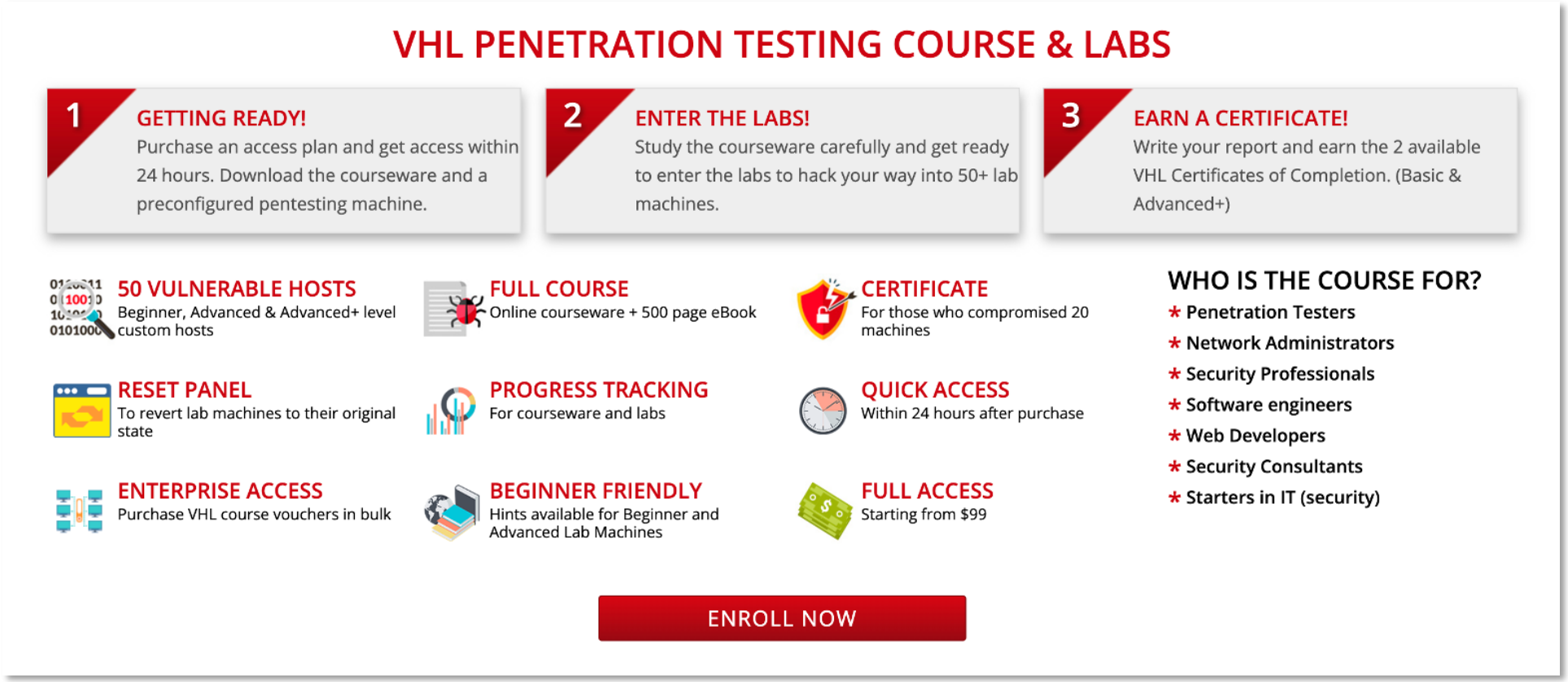
Proving Grounds Play

Free, 3hr/day

https://www.offsec.com/labs/individual/

Cymetrics

Virtual Hacking Labs



https://www.virtualhackinglabs.com/

Cymetrics

Virtual Hacking Labs

> 20 Lab Machines
(Beginner or Advanced)

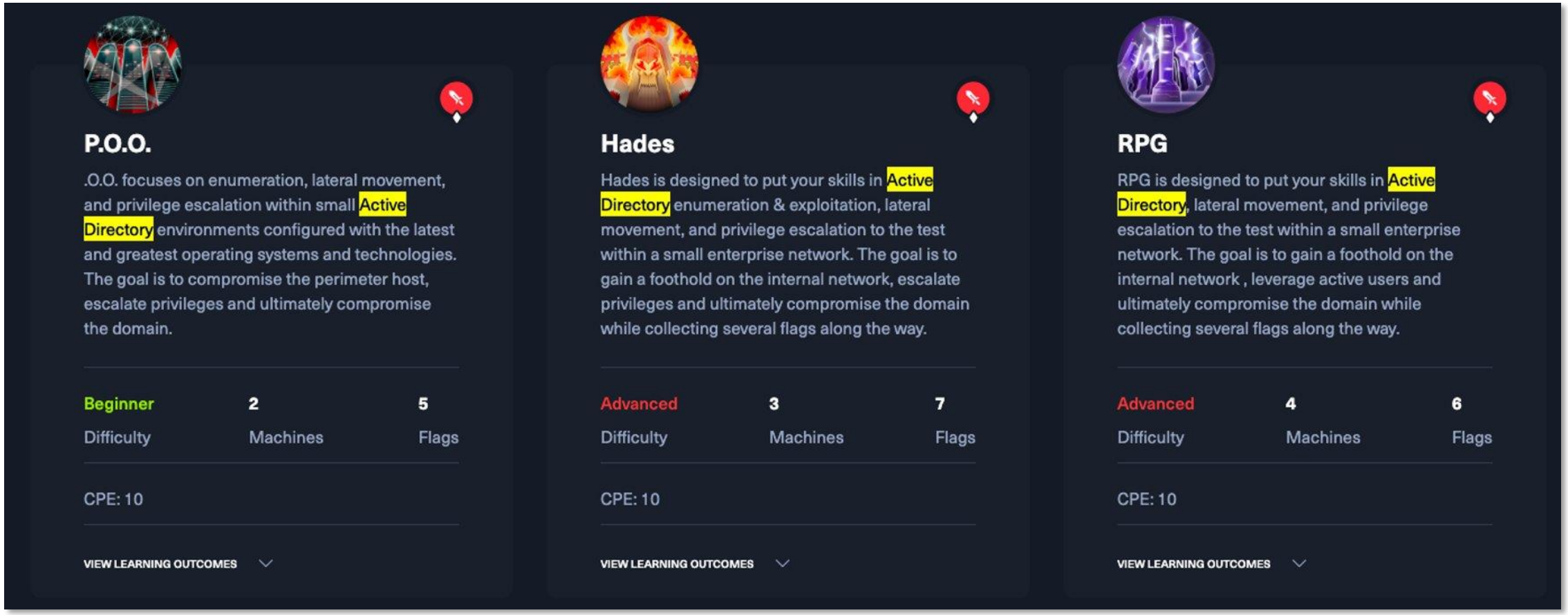
> 10 Lab Machines
(Advanced +)

> 10 Lab Machines
& 2 Network Labs

https://www.virtualhackinglabs.com/

Cymetrics

Hack The Box - Pro Labs



https://www.hackthebox.com/hacker/pro-labs

Cymetrics

Hack The Box - Certifications

https://academy.hackthebox.com/preview/certifications

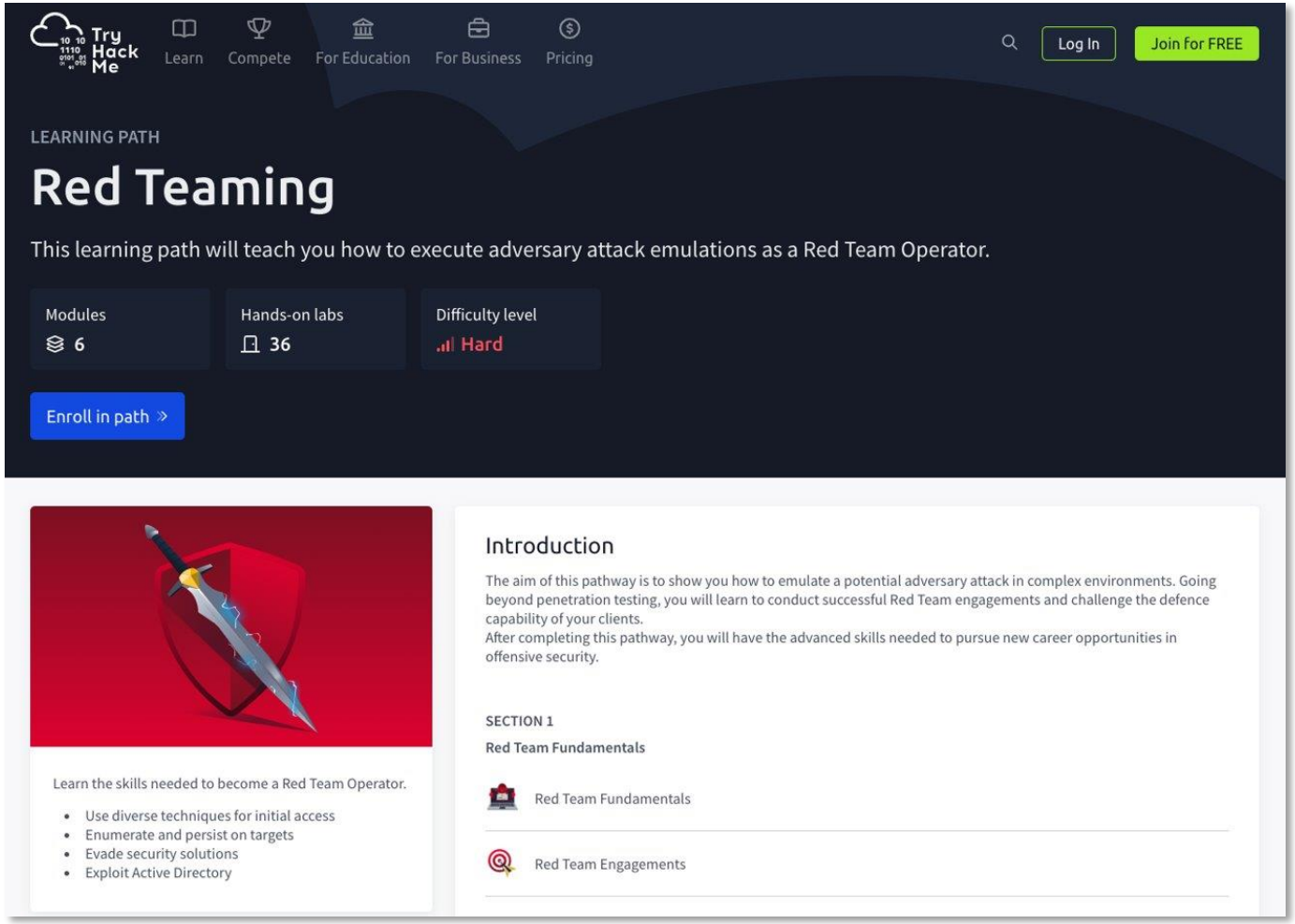
Cymetrics

Hack The Box - Certifications

https://academy.hackthebox.com/preview/certifications

Cymetrics

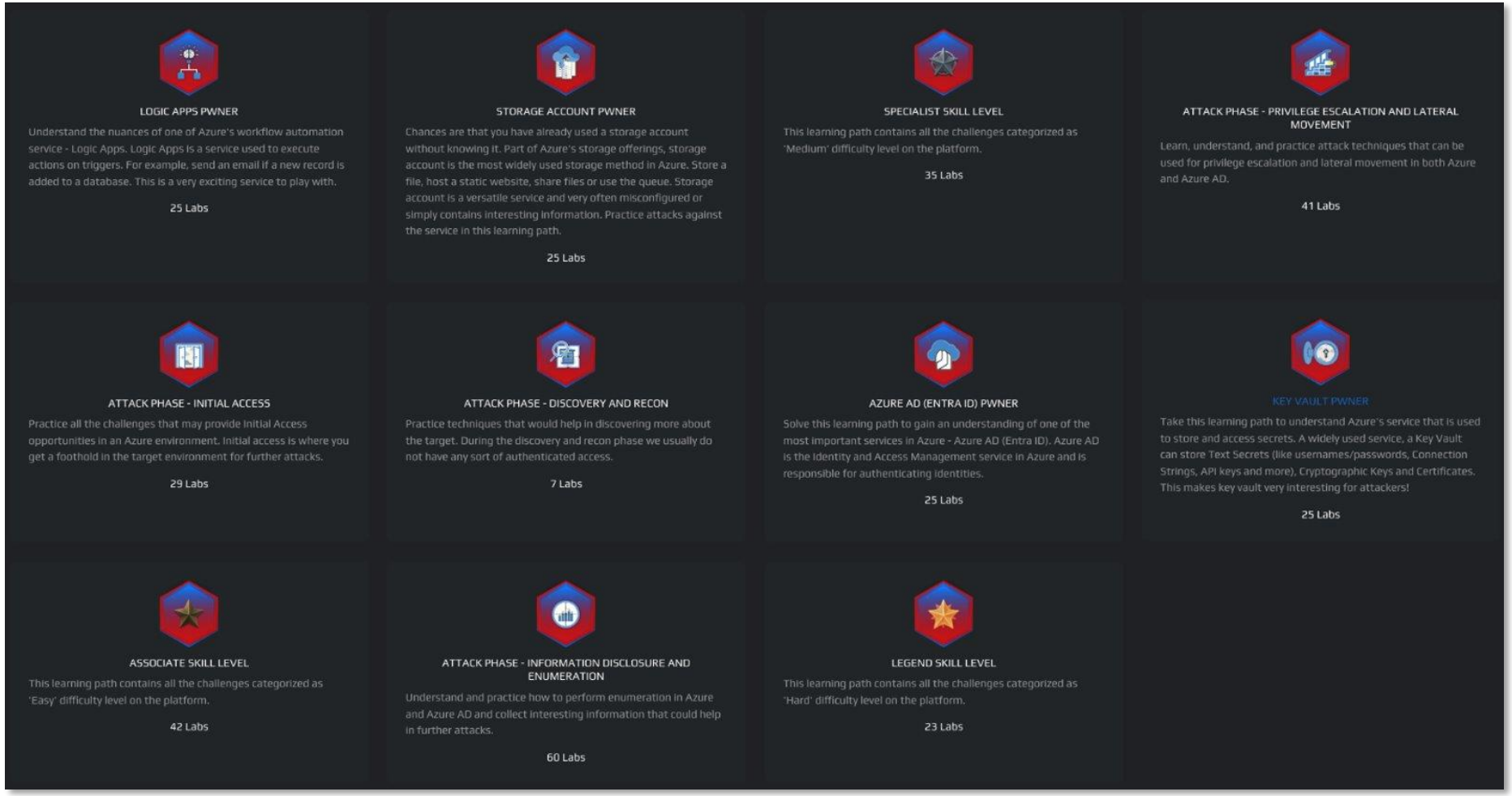
TryHackMe - Red Teaming Training



https://tryhackme.com/path/outline/redteaming

Cymetrics

Altered Security Red Labs Platform



https://redlabs.enterprisesecurity.io/

Cymetrics

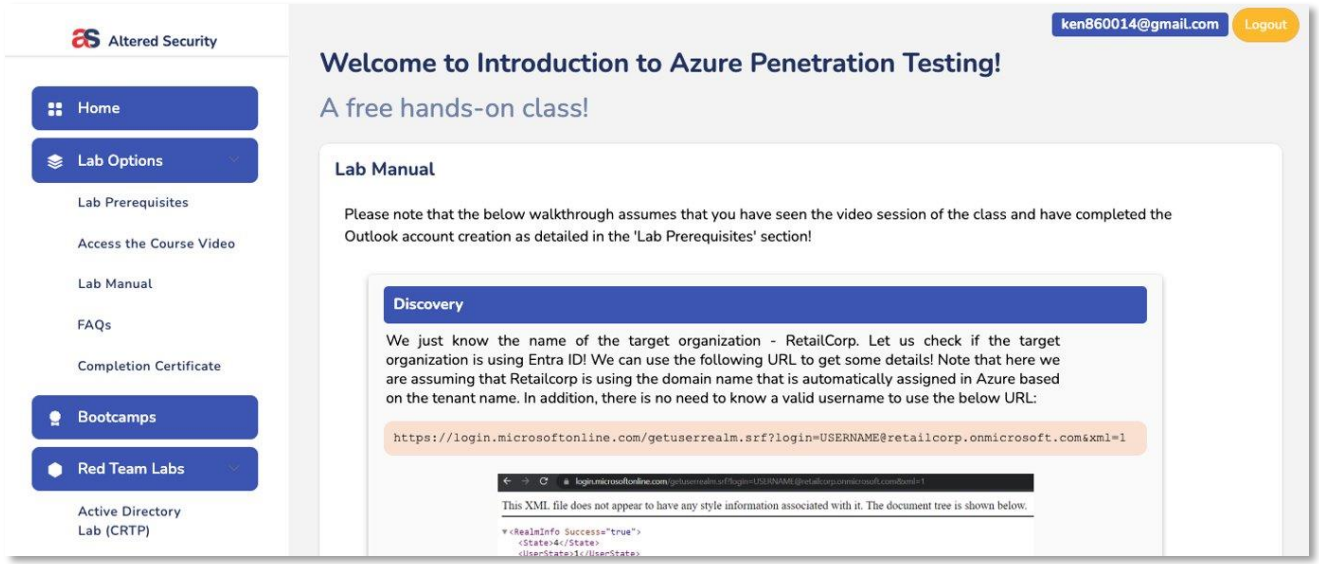
Altered Security Red Labs Platform

Cymetrics

Altered Security Red Labs Platform

Azure Penetration Testing

Azure Red Teaming



https://azure.enterprisesecurity.io/

Cymetrics

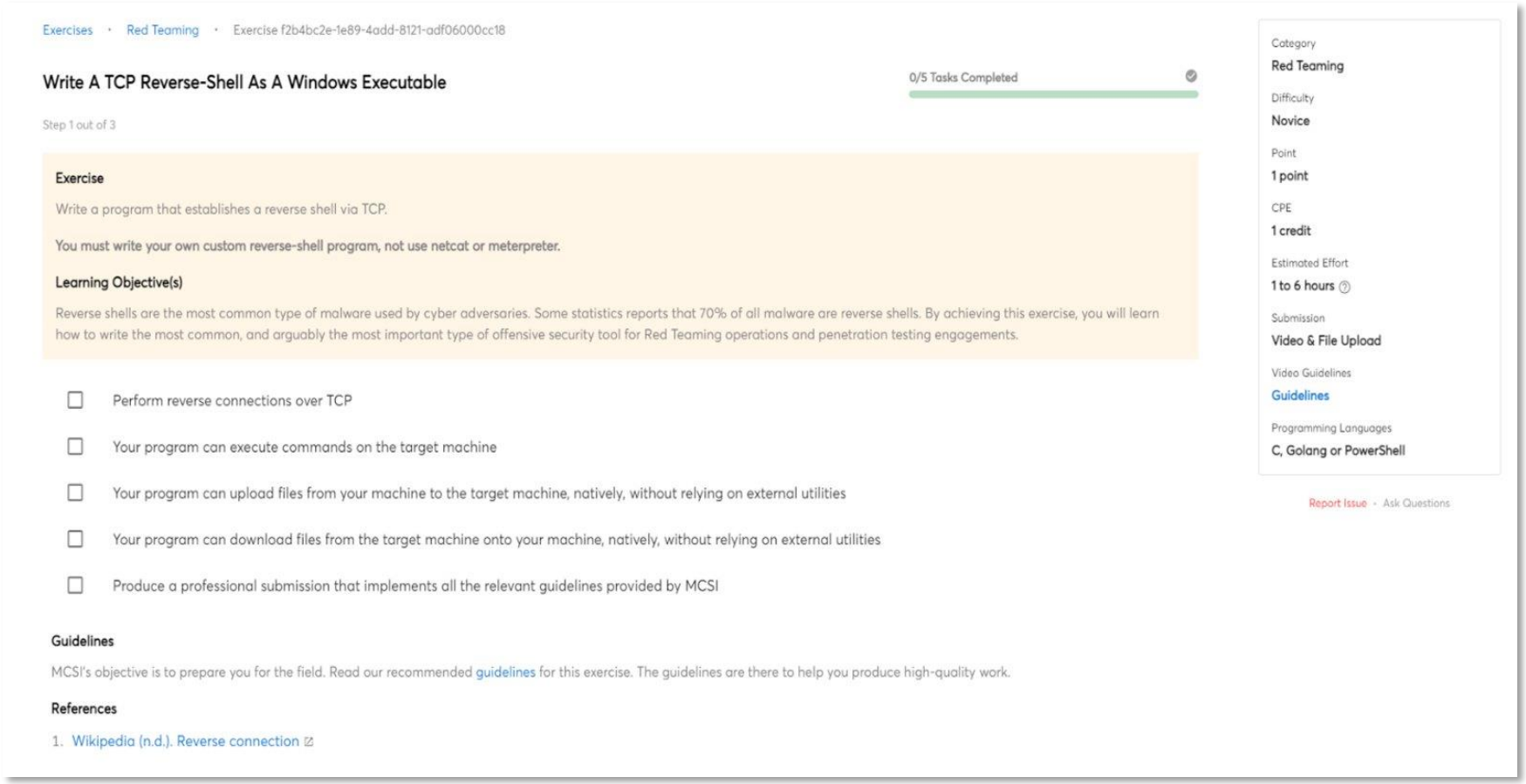
Mossé Cyber Security Institute - MRT

	CERTIFICATE LEVEL	CURRICULUM COMPLETION REQUIREMENT	SCENARIOS COMPLETION REQUIREMENT
MCSI Red Team Learner	Level 1	0%	0%
MCSI Novice Red Teamer	Level 2	20%	0%
MCSI Red Team Practitioner	Level 3	50%	25%
MCSI Senior Red Team Practitioner	Level 4	70%	50%
MCSI Certified Principal Red Team Practitioner	Level 5	80%	75%
MCSI Certified Expert Red Team Practitioner	Level 6	95%	100%

https://www.mosse-institute.com/certifications/mrt-certified-red-teamer.html

Cymetrics

Mossé Cyber Security Institute - MRT



Exercises · Red Teaming · Exercise f2b4bc2e-1e89-4add-8121-adf06000cc18

Write A TCP Reverse-Shell As A Windows Executable

0/5 Tasks Completed

Step 1 out of 3

Exercise

Write a program that establishes a reverse shell via TCP.

You must write your own custom reverse-shell program, not use netcat or meterpreter.

Learning Objective(s)

Reverse shells are the most common type of malware used by cyber adversaries. Some statistics reports that 70% of all malware are reverse shells. By achieving this exercise, you will learn how to write the most common, and arguably the most important type of offensive security tool for Red Teaming operations and penetration testing engagements.

- [ ] Perform reverse connections over TCP
- [ ] Your program can execute commands on the target machine
- [ ] Your program can upload files from your machine to the target machine, natively, without relying on external utilities
- [ ] Your program can download files from the target machine onto your machine, natively, without relying on external utilities
- [ ] Produce a professional submission that implements all the relevant guidelines provided by MCSI

Guidelines

MCSI's objective is to prepare you for the field. Read our recommended guidelines for this exercise. The guidelines are there to help you produce high-quality work.

References

1. Wikipedia (n.d.). Reverse connection

Category
Red Teaming

Difficulty
Novice

Point
1 point

CPE
1 credit

Estimated Effort
1 to 6 hours

Submission
Video & File Upload

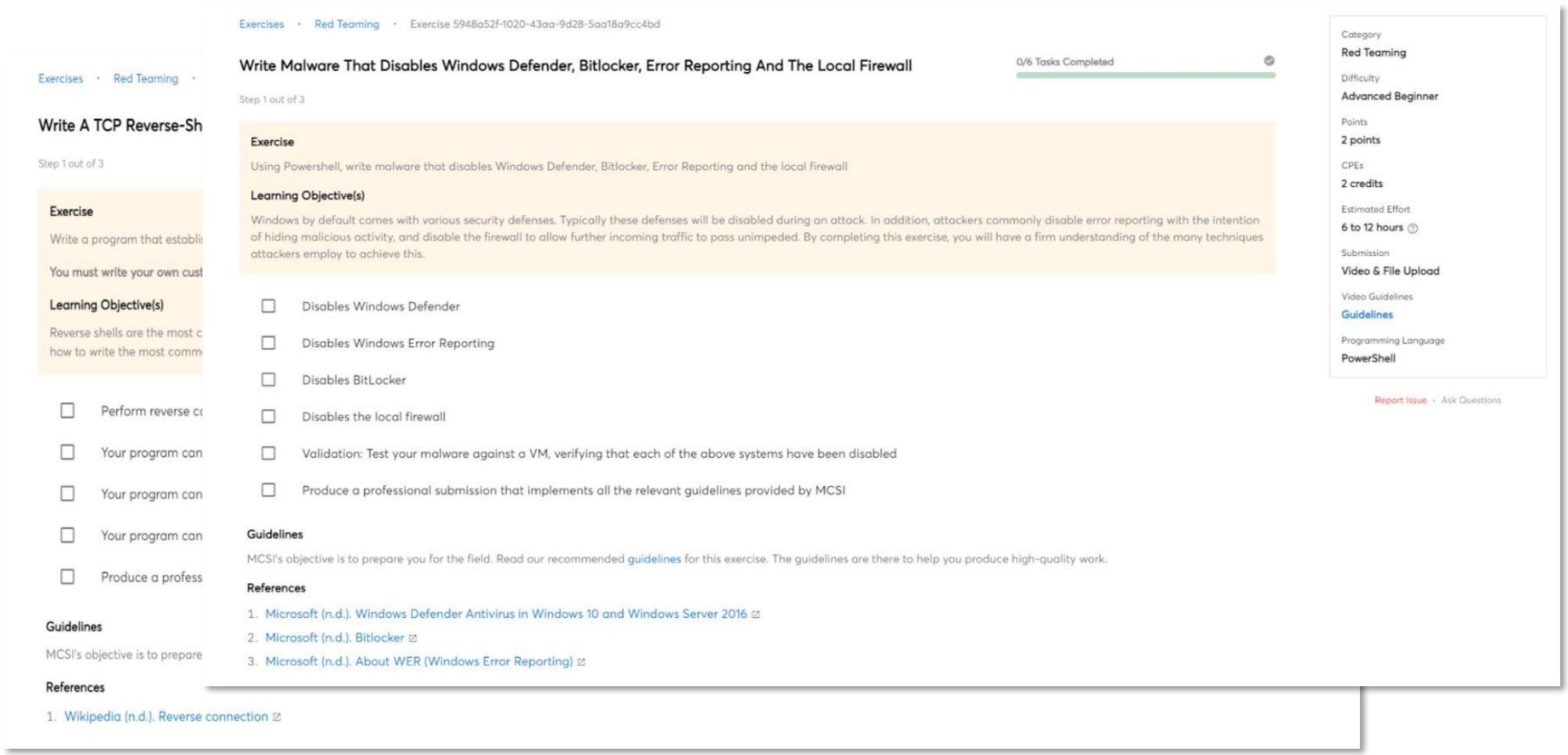
Video Guidelines
Guidelines

Programming Languages
C, Golang or PowerShell

Report Issue · Ask Questions

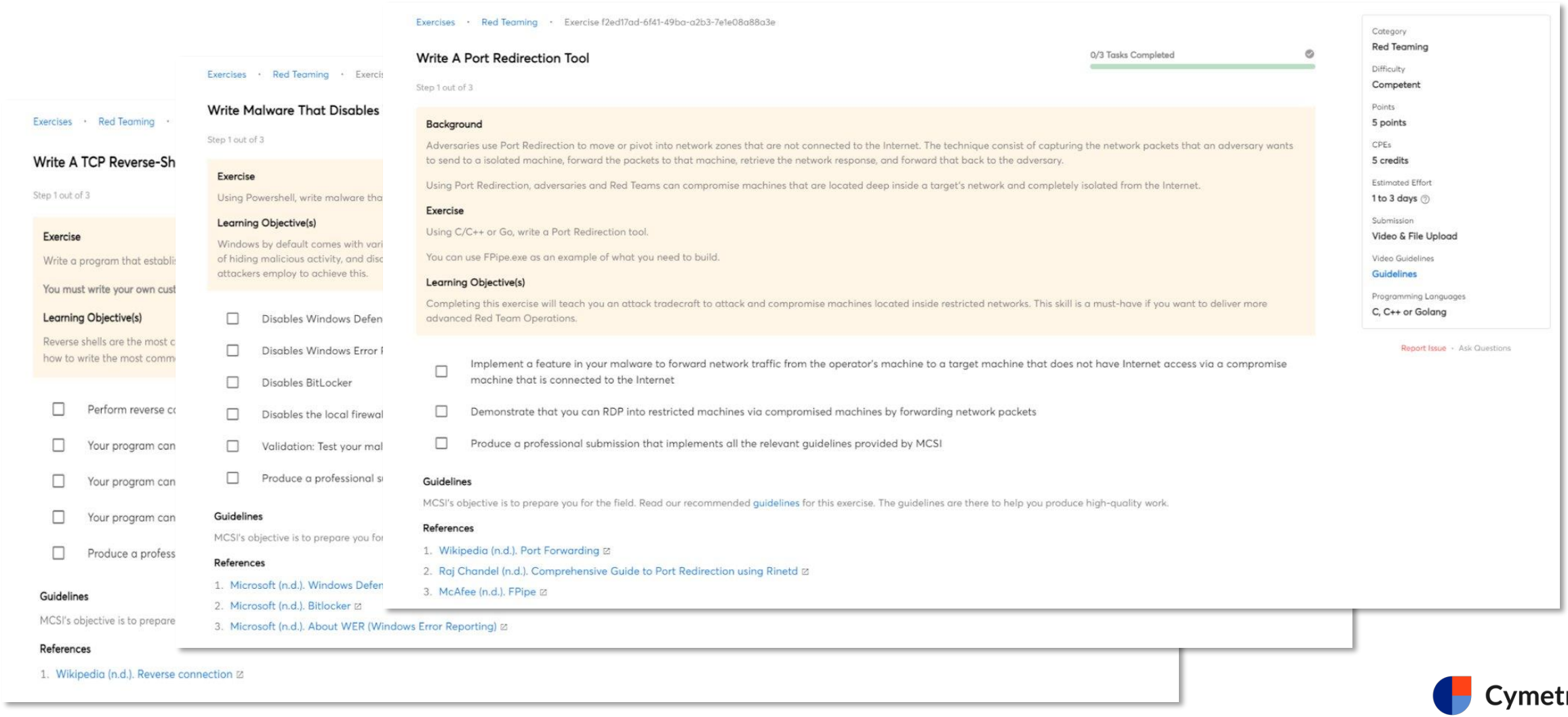
Cymetrics

Mossé Cyber Security Institute - MRT



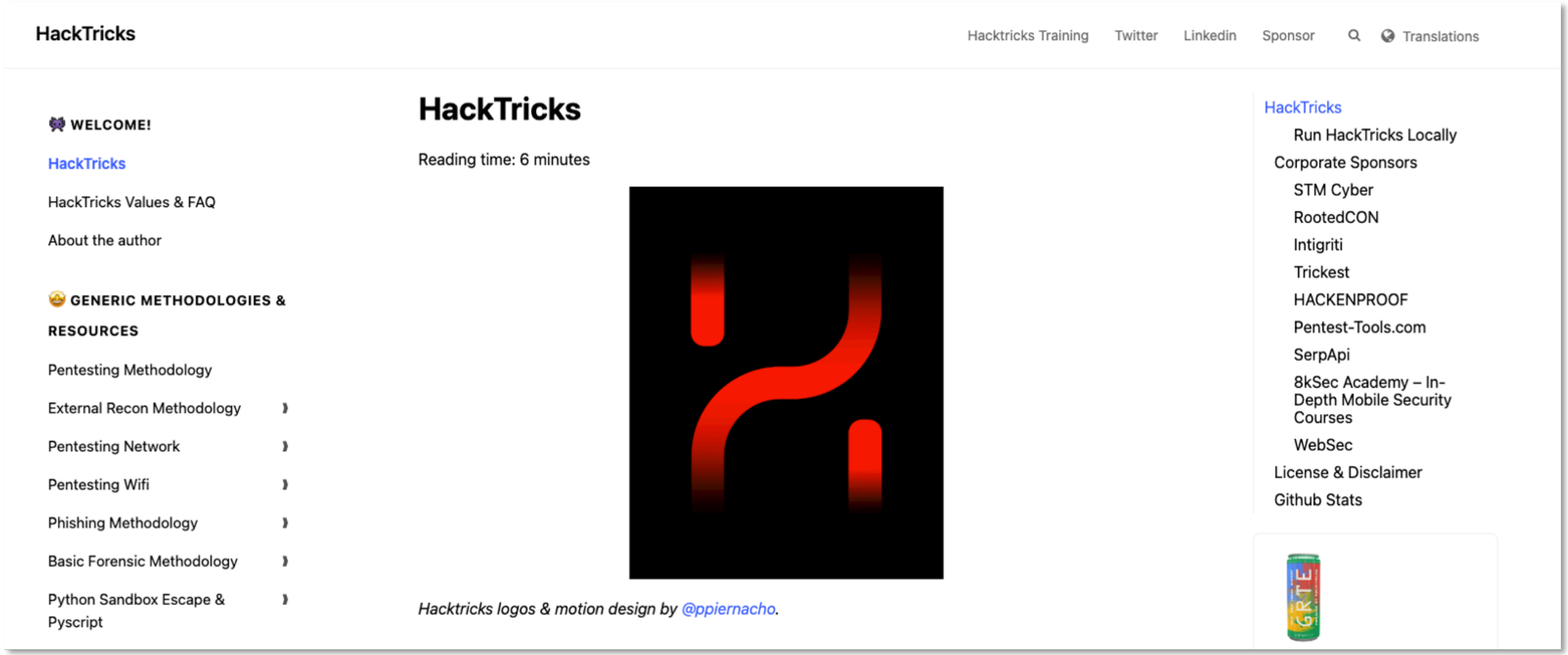
Cymetrics

Mossé Cyber Security Institute - MRT



Cymetrics

HackTricks



https://book.hacktricks.wiki/en/index.html

Cymetrics

Cymetrics

HackTricks Training

ARTA

ARTE

GRTA

GRTE

AzRTA

AzRTE

https://training.hacktricks.xyz/

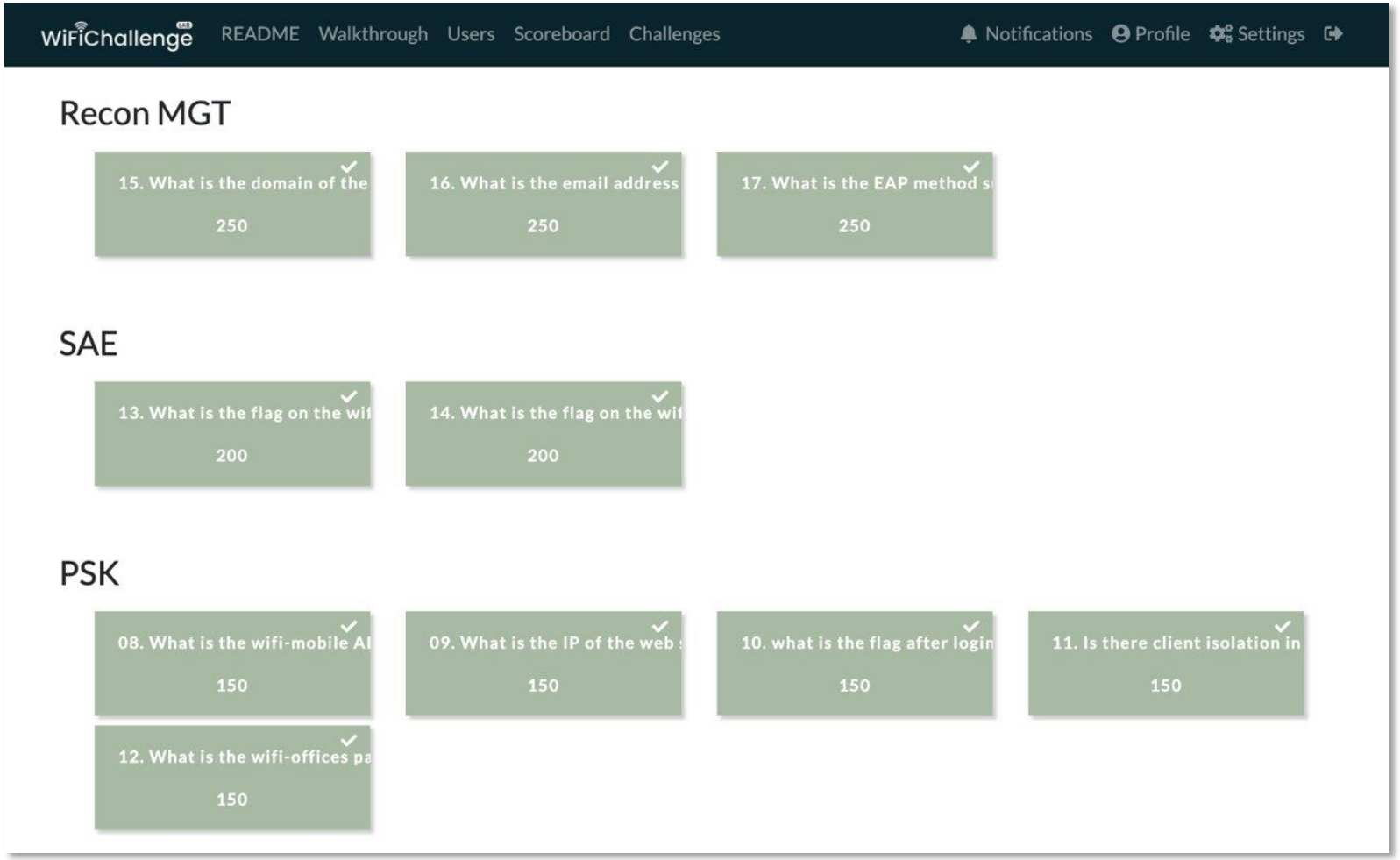
Cymetrics

FREE Wi-Fi

$$\int_{-2}^{2} \left(x^3 \cos \frac{x}{2} + \frac{1}{2} \right) \sqrt{4 - x^2}\, dx$$

The Wi-Fi password is the first 10 digits of the answer.

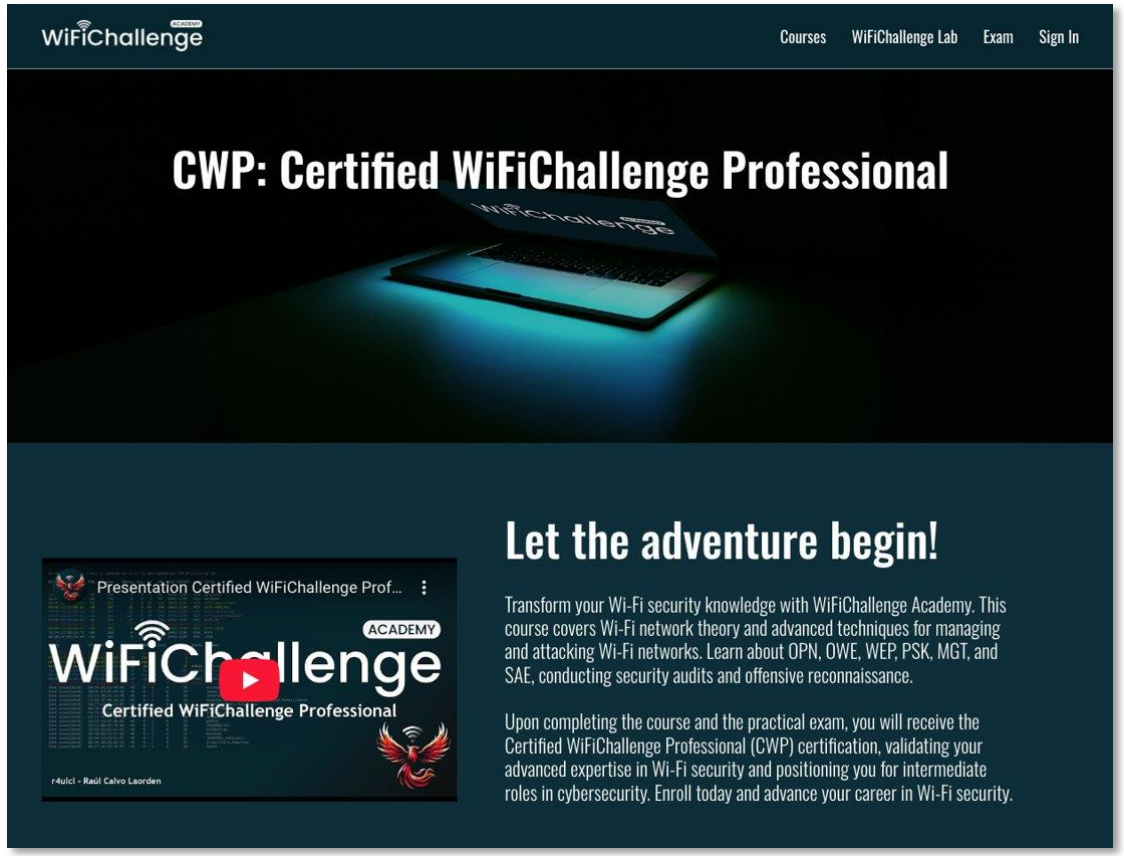
WiFiChallenge Lab



https://lab.wifichallenge.com/

Cymetrics

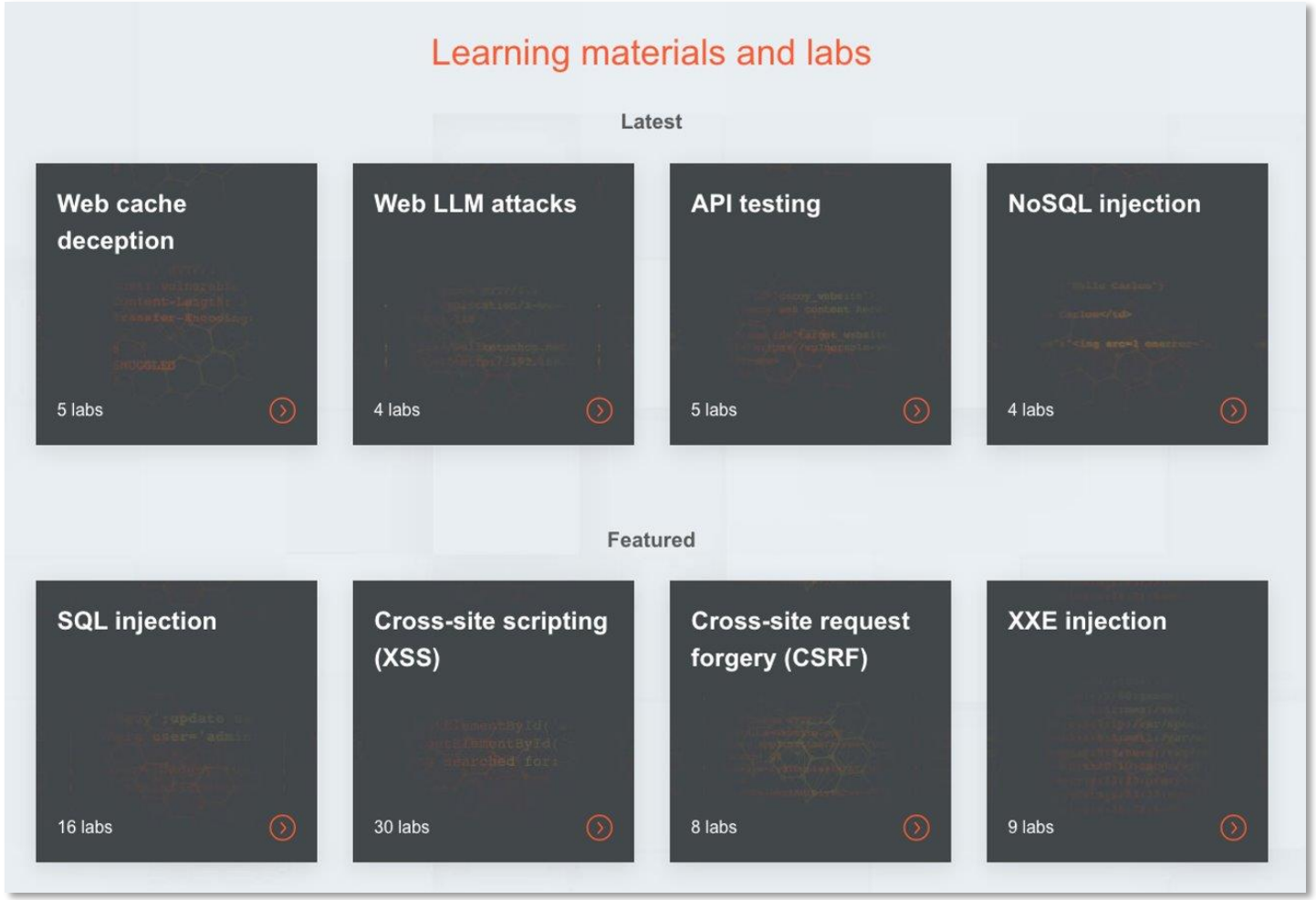
WiFiChallenge Academy



https://academy.wifichallenge.com/

Cymetrics

Web Security Academy (PortSwigger)



https://portswigger.net/web-security

Cymetrics

Web Security Academy (PortSwigger)

What is a Burp Suite Certified Practitioner?

The Burp Suite Certified Practitioner (BSCP) is an official certification for web security professionals, from the makers of Burp Suite. Becoming a Burp Suite Certified Practitioner demonstrates a deep knowledge of web security vulnerabilities, the correct mindset to exploit them, and of course, the Burp Suite skills needed to carry this out.

Why become a Burp Suite Certified Practitioner?

Successfully passing the Burp Suite Certified Practitioner exam indicates a high-level proficiency in web security testing. It is aimed at penetration testers, and the organizations that employ them.

Prove your proficiency

- Demonstrate a deep knowledge of the latest vulnerability classes and how to exploit them.
- Showcase your skills with Burp Suite Professional.
- Prove your hacking ability to employers and the community.

LEARN MORE

Upskill your team

- Prove the proficiency of your testing team to potential clients.
- Easily identify the best new talent to join your team.
- Develop your team's expertise with knowledge of the latest vulnerability classes and how to exploit them.

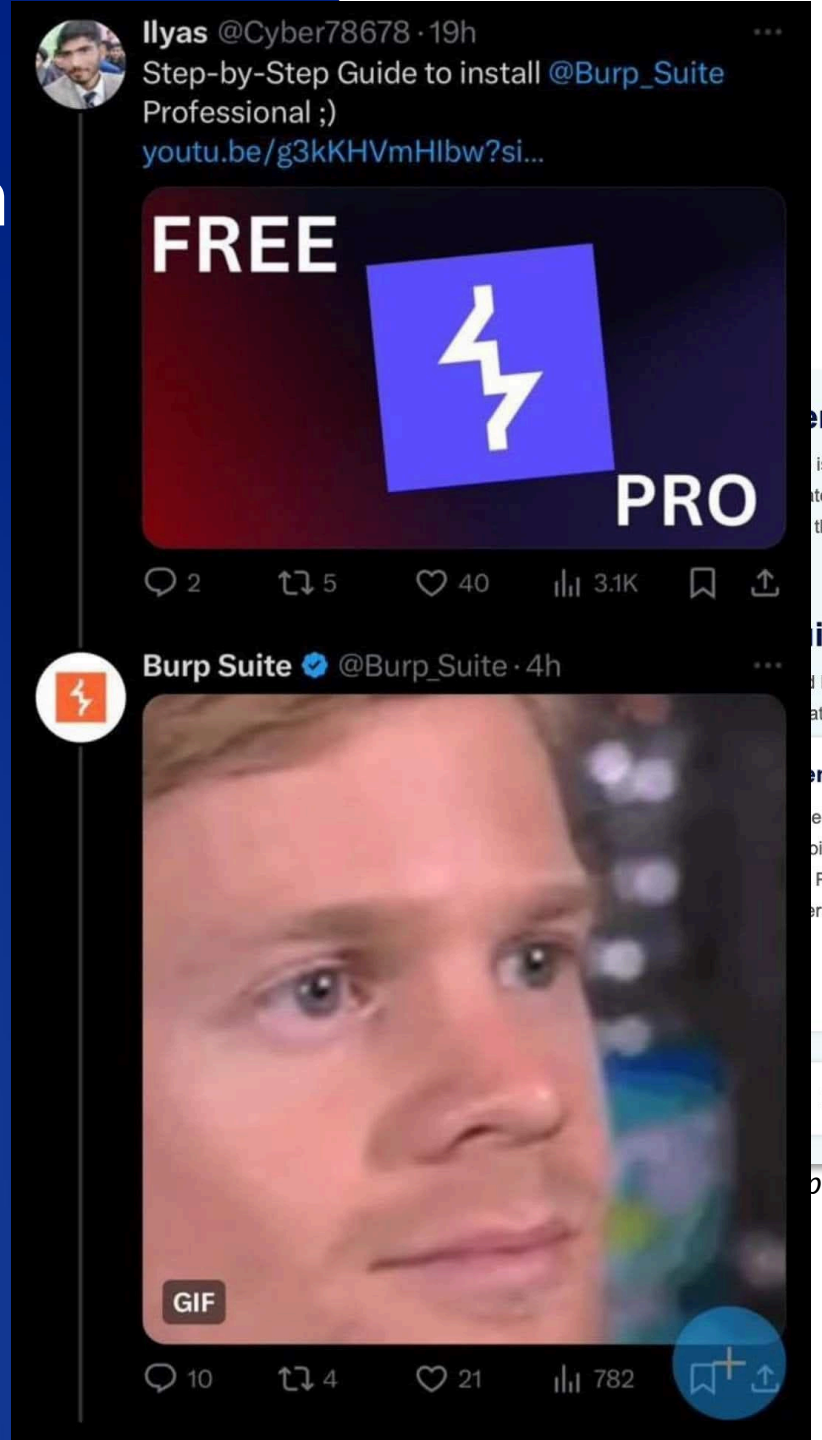
LEARN MORE

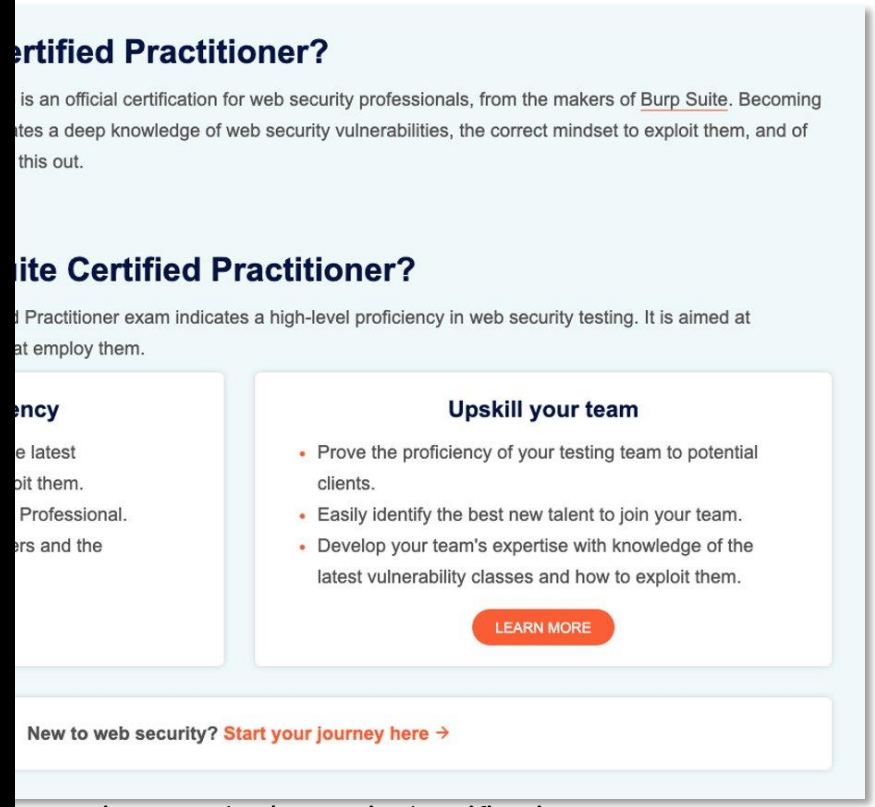
New to web security? Start your journey here →

https://portswigger.net/web-security/certification

Cymetrics

Web Security Aca
(PortSwigger)





portswigger.net/web-security/certification

Cymetrics

Summarize

紅隊大佬

想成為紅隊仔

資安萌新

Cymetrics

Summarize

資安證照這麼多

我真的需要嗎？

Cymetrics

Cymetrics

C230 展攤

CYBERSEC 2025
臺灣資安大會

4/15-4/17
臺北南港展覽二館

車用互聯網、紅隊演練、Web3

Cymetrics
全方位資安論壇
等你來聽!

Car Security 論壇

Project D:
左握方向盤，右打 CarPlay

Cyber Talent 論壇

紅隊勇者的證照冒險攻略

Web3 安全論壇

AI 驅動的智慧合約漏洞檢測

OneSavie Lab 特別講者 *(Cymetrics* 合作夥伴*)*

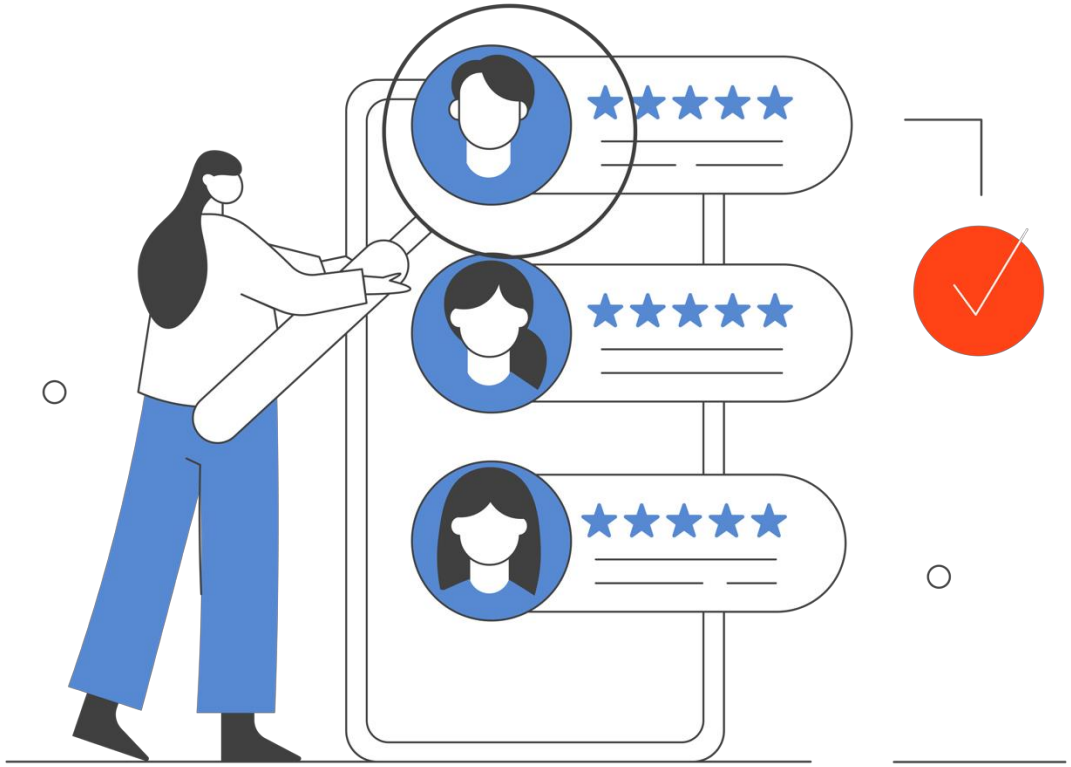
Cymetrics

We are Hiring!!!

- Senior Security Engineer (RedTeam, Pentest)
- Security Engineering Intern
- Associate Software Backend Engineer
- Project Manager
- Product Manager

Cake

Cymetrics



Cymetrics

Cymetrics

凡聽完演講後，
持 Cymetrics 貼紙至
Cymetrics 攤位(C230)

即可獲得
神秘小禮物！

數量有限 送完為止