



紅隊勇者的證照冒險攻略

Cymetrics Security Research Engineer

楊士賢 Ken Yang

楊士賢 Ken Yang

Security Research Engineer @ Cymetrics

★ 擁有 20+ 張專業證照

★ 揭露 30+ CVEs

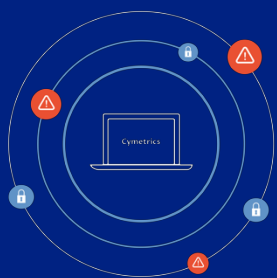
👉 <https://linktr.ee/4hsienyang>



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

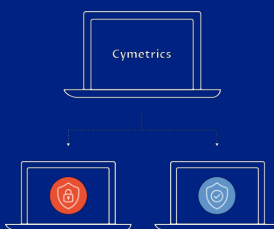
Cymetrics VAS 提供自動化的漏洞評估服務，用戶可快速獲得測試結果。我們精心挑選測試項目，結合滲透測試經驗，增強評估的深度和有效性。

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

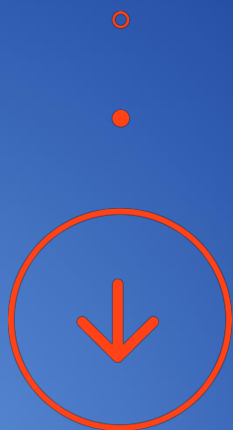
透過我們的服務，加強您的第三方網路風險管理流程。透過 TPRM API，將風險管理整合到您現有的公司系統中，以提升效率。



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。



通靈大賽開始

紅
隊

日
常

- 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。

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	

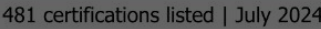
這些酷酷的證照



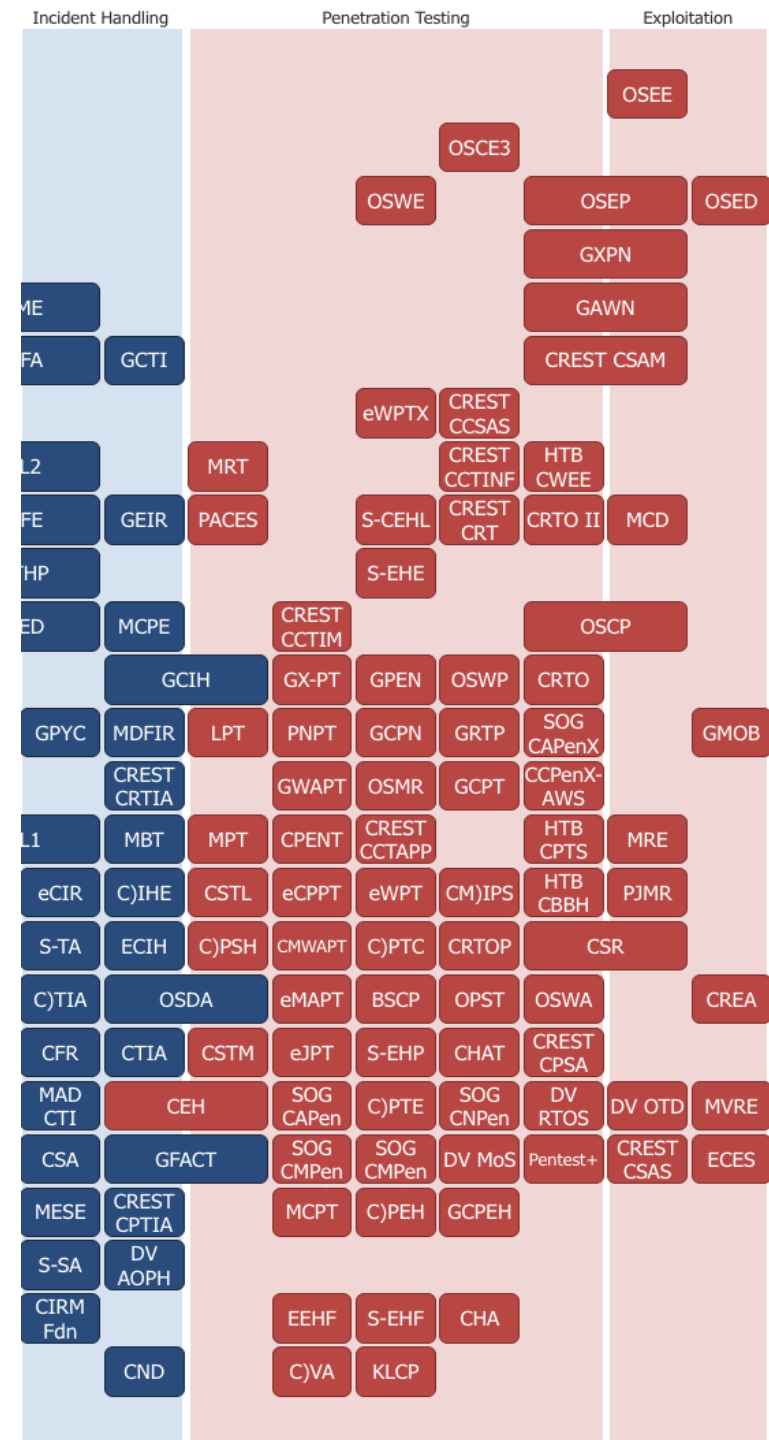
真的好想好想要



Cymetrics



Security Certification Roadmap



Security Certification Roadmap



Level 1



Security Certification Roadmap



Level 2



Level 1



Security Certification Roadmap



Level 3



Level 2



Level 1





JAKE-CLARK.TUMBLR



E-commerce Council



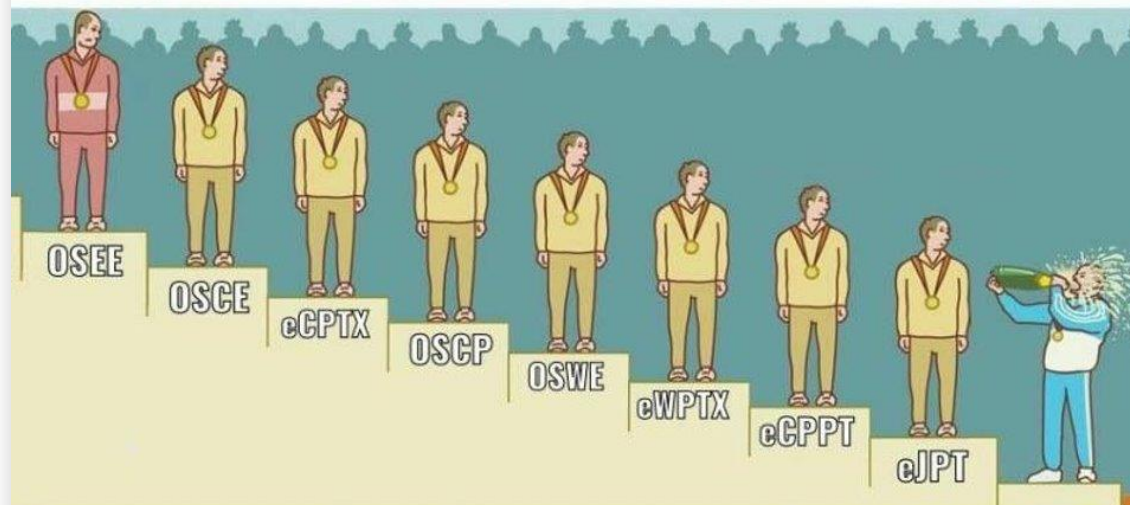
Softsec™
The Path to a Secure Future™



選擇題



實作題



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/>

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/>

TCM Security - PNPT



How to Prepare for the PNPT Exam

In addition to the lifetime voucher and exam attempt, students who enroll in the PNPT certification will receive 12 months of access to over 45 hours of training materials including the following courses:



Practical Ethical
Hacking



OSINT
Fundamentals



Windows
Privilege
Escalation for
Beginners



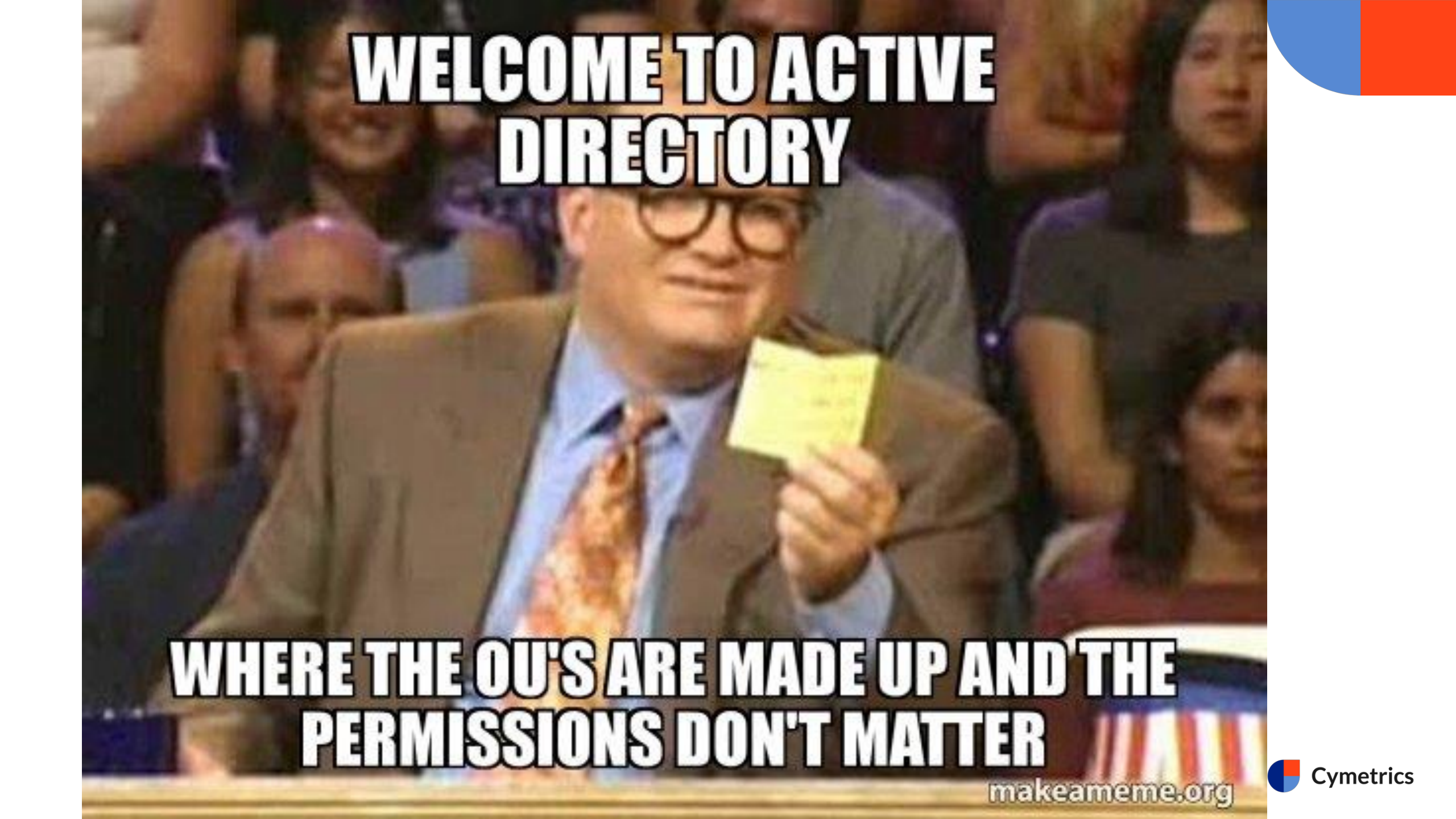
Linux Privilege
Escalation for
Beginners



External Pentest
Playbook

[VIEW MORE](#)

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

A man in a brown suit, blue shirt, and patterned tie, wearing glasses, is holding a yellow sticky note. He is in the foreground, looking slightly to the right. In the background, a crowd of people is visible, some looking towards the camera. The image is a meme with text overlaid.

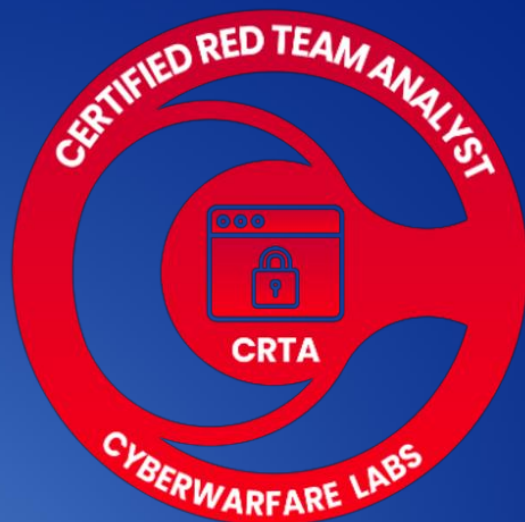
**WELCOME TO ACTIVE
DIRECTORY**

**WHERE THE OU'S ARE MADE UP AND THE
PERMISSIONS DON'T MATTER**

makeameme.org

CyberWarFare Labs

- CRTA

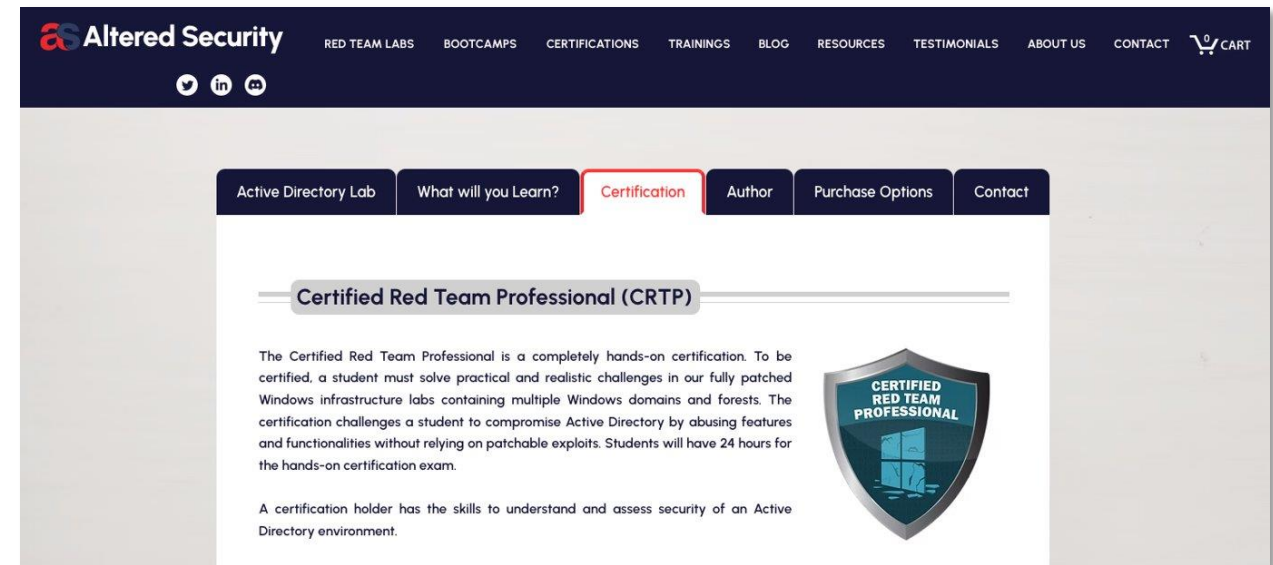


The courses contents are divided across 5 sections listed below:

Section	Topics
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

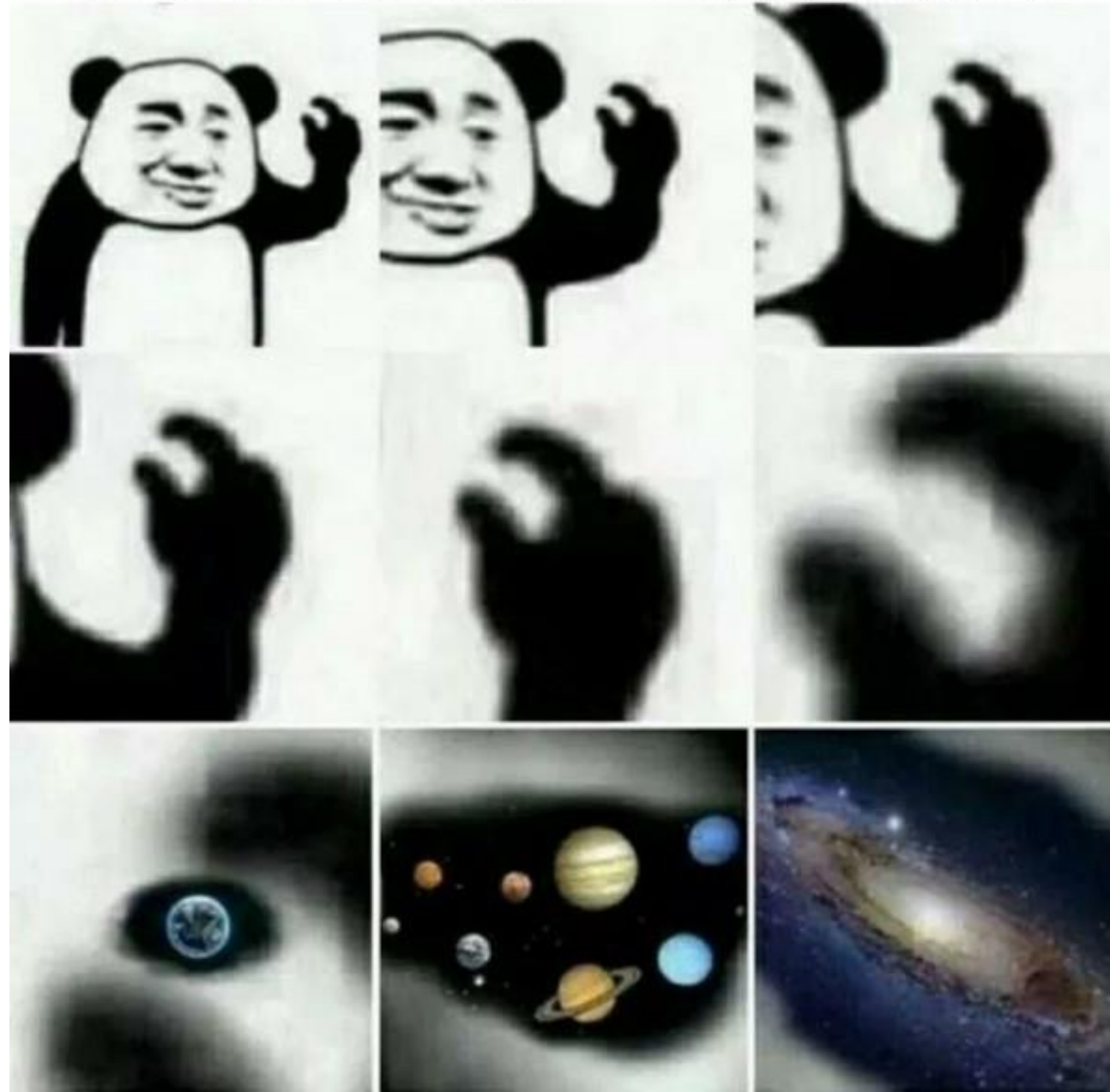
<https://cyberwarfare.live/product/red-team-analyst-crt/>

Altered Security - CRTP

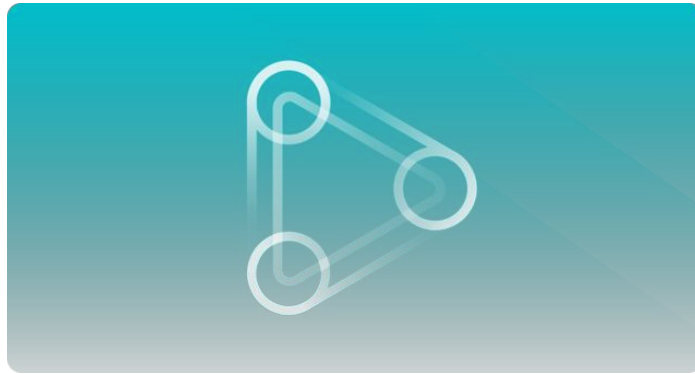


<https://www.alteredsecurity.com/post/certified-red-team-professional-crtp>

學習只要花一點點時間

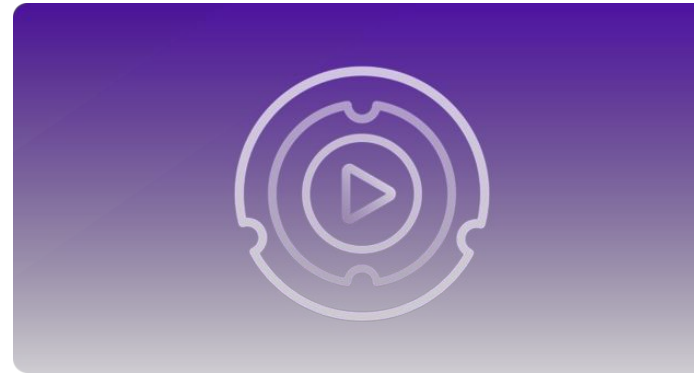


OffSec Proving Grounds Labs



Proving Grounds Practice

*\$199 USD/Year
or \$19 USD/Month*



Proving Grounds Play

Free, 3hr/day

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

Virtual Hacking Labs

VHL PENETRATION TESTING COURSE & LABS

1

GETTING READY!

Purchase an access plan and get access within 24 hours. Download the courseware and a preconfigured pentesting machine.

2

ENTER THE LABS!

Study the courseware carefully and get ready to enter the labs to hack your way into 50+ lab machines.

3

EARN A CERTIFICATE!

Write your report and earn the 2 available VHL Certificates of Completion. (Basic & Advanced+)



50 VULNERABLE HOSTS

Beginner, Advanced & Advanced+ level custom hosts



FULL COURSE

Online courseware + 500 page eBook



CERTIFICATE

For those who compromised 20 machines



RESET PANEL

To revert lab machines to their original state



PROGRESS TRACKING

For courseware and labs



QUICK ACCESS

Within 24 hours after purchase



ENTERPRISE ACCESS

Purchase VHL course vouchers in bulk



BEGINNER FRIENDLY

Hints available for Beginner and Advanced Lab Machines



FULL ACCESS

Starting from \$99

WHO IS THE COURSE FOR?

- * Penetration Testers
- * Network Administrators
- * Security Professionals
- * Software engineers
- * Web Developers
- * Security Consultants
- * Starters in IT (security)

ENROLL NOW

<https://www.virtualhackinglabs.com/>

Virtual Hacking Labs



> 20 Lab Machines
(Beginner or Advanced)



> 10 Lab Machines
(Advanced +)



> 10 Lab Machines
& 2 Network Labs

Hack The Box - Pro Labs



P.O.O.

.O.O. focuses on enumeration, lateral movement, and privilege escalation within small **Active Directory** environments configured with the latest and greatest operating systems and technologies. The goal is to compromise the perimeter host, escalate privileges and ultimately compromise the domain.

Beginner	2	5
Difficulty	Machines	Flags

CPE: 10

VIEW LEARNING OUTCOMES ▾



Hades

Hades is designed to put your skills in **Active Directory** enumeration & exploitation, lateral movement, and privilege escalation to the test within a small enterprise network. The goal is to gain a foothold on the internal network, escalate privileges and ultimately compromise the domain while collecting several flags along the way.

Advanced	3	7
Difficulty	Machines	Flags

CPE: 10

VIEW LEARNING OUTCOMES ▾



RPG

RPG is designed to put your skills in **Active Directory**, lateral movement, and privilege escalation to the test within a small enterprise network. The goal is to gain a foothold on the internal network , leverage active users and ultimately compromise the domain while collecting several flags along the way.

Advanced	4	6
Difficulty	Machines	Flags

CPE: 10

VIEW LEARNING OUTCOMES ▾

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

Hack The Box - Certifications



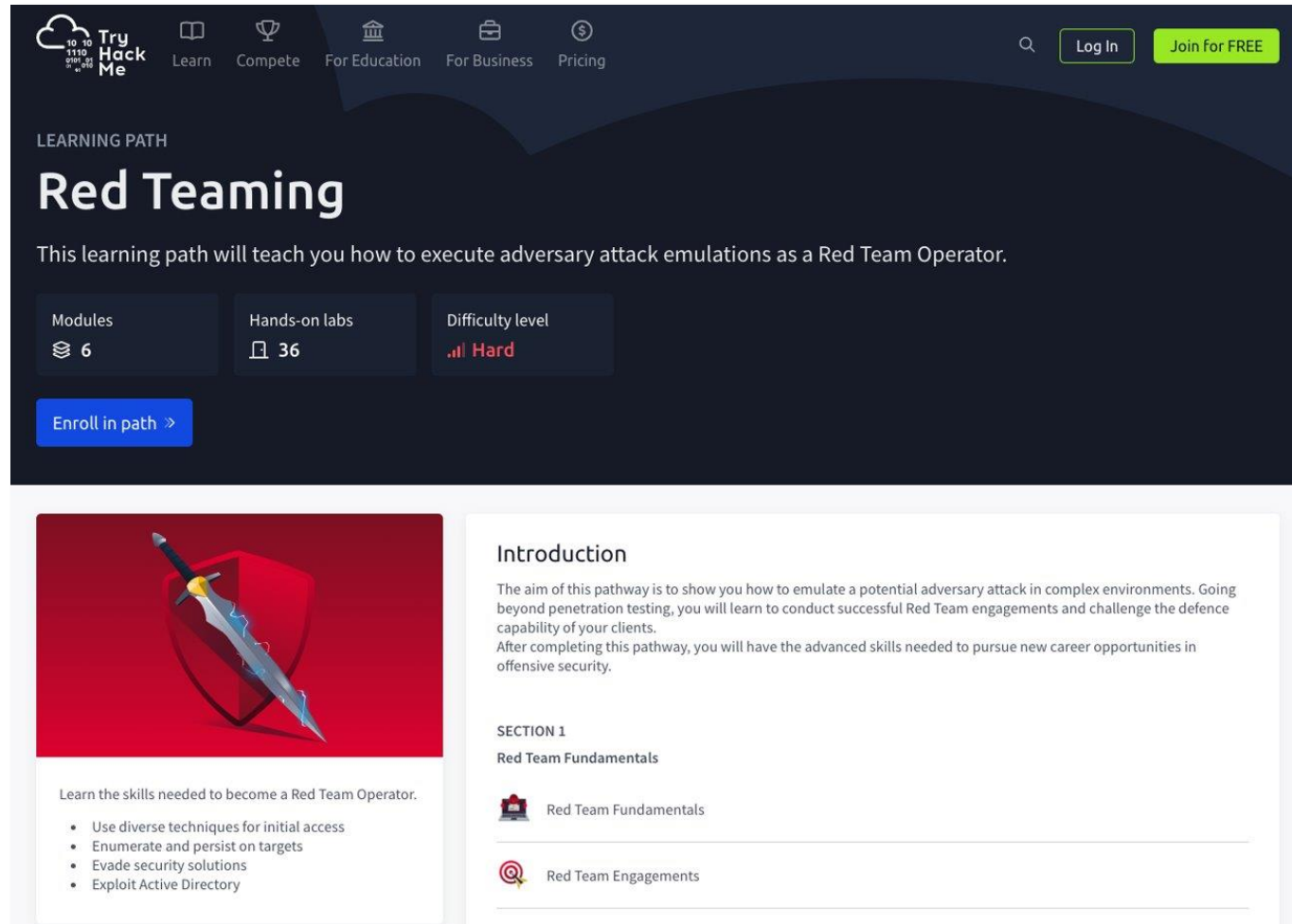
<https://academy.hackthebox.com/preview/certifications>

Hack The Box - Certifications



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

TryHackMe - Red Teaming Training



The screenshot shows the TryHackMe website interface for the Red Teaming learning path. The top navigation bar includes the TryHackMe logo, links for Learn, Compete, For Education, For Business, and Pricing, a search icon, and buttons for Log In and Join for FREE. The main section is titled 'LEARNING PATH' and 'Red Teaming'. Below the title, a description states: 'This learning path will teach you how to execute adversary attack emulations as a Red Team Operator.' Three statistics are displayed: Modules (6), Hands-on labs (36), and Difficulty level (Hard). An 'Enroll in path' button is present. The lower section features a red graphic with a sword and a shield, followed by an 'Introduction' paragraph and a list of skills. The 'SECTION 1' section lists 'Red Team Fundamentals' and 'Red Team Engagements'.

TryHackMe

Learn Compete For Education For Business Pricing

Log In Join for FREE

LEARNING PATH

Red Teaming

This learning path will teach you how to execute adversary attack emulations as a Red Team Operator.

Modules 6

Hands-on labs 36

Difficulty level **Hard**

Enroll in path »



Learn the skills needed to become a Red Team Operator.

- Use diverse techniques for initial access
- Enumerate and persist on targets
- Evade security solutions
- Exploit Active Directory

Introduction

The aim of this pathway is to show you how to emulate a potential adversary attack in complex environments. Going beyond penetration testing, you will learn to conduct successful Red Team engagements and challenge the defence capability of your clients. After completing this pathway, you will have the advanced skills needed to pursue new career opportunities in offensive security.

SECTION 1

Red Team Fundamentals

- Red Team Fundamentals

Red Team Engagements

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

Altered Security Red Labs Platform

 LOGIC APPS PWNER Understand the nuances of one of Azure's workflow automation service - Logic Apps. Logic Apps is a service used to execute actions on triggers. For example, send an email if a new record is added to a database. This is a very exciting service to play with. 25 Labs	 STORAGE ACCOUNT PWNER Chances are that you have already used a storage account without knowing it. Part of Azure's storage offerings, storage account is the most widely used storage method in Azure. Store a file, host a static website, share files or use the queue. Storage account is a versatile service and very often misconfigured or simply contains interesting information. Practice attacks against the service in this learning path. 25 Labs	 SPECIALIST SKILL LEVEL This learning path contains all the challenges categorized as 'Medium' difficulty level on the platform. 35 Labs	 ATTACK PHASE - PRIVILEGE ESCALATION AND LATERAL MOVEMENT Learn, understand, and practice attack techniques that can be used for privilege escalation and lateral movement in both Azure and Azure AD. 41 Labs
 ATTACK PHASE - INITIAL ACCESS Practice all the challenges that may provide Initial Access opportunities in an Azure environment. Initial access is where you get a foothold in the target environment for further attacks. 29 Labs	 ATTACK PHASE - DISCOVERY AND RECON Practice techniques that would help in discovering more about the target. During the discovery and recon phase we usually do not have any sort of authenticated access. 7 Labs	 AZURE AD (ENTRA ID) PWNER Solve this learning path to gain an understanding of one of the most important services in Azure - Azure AD (Entra ID). Azure AD is the Identity and Access Management service in Azure and is responsible for authenticating identities. 25 Labs	 KEY VAULT PWNER Take this learning path to understand Azure's service that is used to store and access secrets. A widely used service, a Key Vault can store Text Secrets (like usernames/passwords, Connection Strings, API keys and more), Cryptographic Keys and Certificates. This makes key vault very interesting for attackers! 25 Labs
 ASSOCIATE SKILL LEVEL This learning path contains all the challenges categorized as 'Easy' difficulty level on the platform. 42 Labs	 ATTACK PHASE - INFORMATION DISCLOSURE AND ENUMERATION Understand and practice how to perform enumeration in Azure and Azure AD and collect interesting information that could help in further attacks. 60 Labs	 LEGEND SKILL LEVEL This learning path contains all the challenges categorized as 'Hard' difficulty level on the platform. 23 Labs	

<https://redlabs.enterprisesecurity.io/>

Altered Security Red Labs Platform



Altered Security Red Labs Platform

Azure Penetration Testing

Azure Red Teaming

The screenshot displays the Altered Security Red Labs Platform interface. On the left is a navigation sidebar with the following items: Home, Lab Options (selected), Lab Prerequisites, Access the Course Video, Lab Manual, FAQs, Completion Certificate, Bootcamps, and Red Team Labs. Below these are 'Active Directory' and 'Lab (CRTP)'. The main content area is titled 'Welcome to Introduction to Azure Penetration Testing!' and 'A free hands-on class!'. It includes a 'Lab Manual' section with a 'Discovery' subsection. The text in the 'Discovery' section explains that the walkthrough assumes the user has completed the 'Lab Prerequisites' section and provides a URL to check if a target organization is using Entra ID. Below the text is a screenshot of a web browser showing an XML response from a Microsoft login endpoint.

Altered Security

ken860014@gmail.com Logout

Welcome to Introduction to Azure Penetration Testing!

A free hands-on class!

Lab Manual

Please note that the below walkthrough assumes that you have seen the video session of the class and have completed the Outlook account creation as detailed in the 'Lab Prerequisites' section!

Discovery

We just know the name of the target organization - RetailCorp. Let us check if the target organization is using Entra ID! We can use the following URL to get some details! Note that here we are assuming that Retailcorp is using the domain name that is automatically assigned in Azure based on the tenant name. In addition, there is no need to know a valid username to use the below URL:

```
https://login.microsoftonline.com/getuserrealm.srf?login=USERNAME@retailcorp.onmicrosoft.com&xml=1
```

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<RealInfo Success="true">
  <StateId:State>
    <UserState:UserState>
```

<https://azure.enterprisesecurity.io/>

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>

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](#)

Mossé Cyber Security Institute - MRT

Exercises · Red Teaming · Exercise 5948a52f-1020-43aa-9d28-5aa18a9cc4bd

Write A TCP Reverse-Sh

Step 1 out of 3

Exercise

Write a program that establi

You must write your own cust

Learning Objective(s)

Reverse shells are the most c

how to write the most comm

☐ Perform reverse c

☐ Your program can

☐ Your program can

☐ Your program can

☐ Produce a profess

Guidelines

MCSI's objective is to prepare

References

1. [Wikipedia \(n.d.\). Reverse connection](#)

Exercises · Red Teaming · Exercise 5948a52f-1020-43aa-9d28-5aa18a9cc4bd

Write Malware That Disables Windows Defender, Bitlocker, Error Reporting And The Local Firewall

0/6 Tasks Completed

Step 1 out of 3

Exercise

Using Powershell, write malware that disables Windows Defender, Bitlocker, Error Reporting and the local firewall

Learning Objective(s)

Windows by default comes with various security defenses. Typically these defenses will be disabled during an attack. In addition, attackers commonly disable error reporting with the intention of hiding malicious activity, and disable the firewall to allow further incoming traffic to pass unimpeded. By completing this exercise, you will have a firm understanding of the many techniques attackers employ to achieve this.

☐ Disables Windows Defender

☐ Disables Windows Error Reporting

☐ Disables BitLocker

☐ Disables the local firewall

☐ Validation: Test your malware against a VM, verifying that each of the above systems have been disabled

☐ 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. [Microsoft \(n.d.\). Windows Defender Antivirus in Windows 10 and Windows Server 2016](#)

2. [Microsoft \(n.d.\). Bitlocker](#)

3. [Microsoft \(n.d.\). About WER \(Windows Error Reporting\)](#)

Category

Red Teaming

Difficulty

Advanced Beginner

Points

2 points

CPEs

2 credits

Estimated Effort

6 to 12 hours

Submission

Video & File Upload

Video Guidelines

[Guidelines](#)

Programming Language

PowerShell

[Report Issue](#) · [Ask Questions](#)

Mossé Cyber Security Institute - MRT

Exercises · Red Teaming · Exercise f2ed17ad-6f41-49ba-a2b3-7e1e08a88a3e

0/3 Tasks Completed

Category
Red Teaming

Difficulty
Competent

Points
5 points

CPEs
5 credits

Estimated Effort
1 to 3 days

Submission
Video & File Upload

Video Guidelines
[Guidelines](#)

Programming Languages
C, C++ or Golang

[Report Issue](#) · [Ask Questions](#)

Exercises · Red Teaming · Exercise f2ed17ad-6f41-49ba-a2b3-7e1e08a88a3e

Step 1 out of 3

Write A Port Redirection Tool

Background

Adversaries use Port Redirection to move or pivot into network zones that are not connected to the Internet. The technique consist of capturing the network packets that an adversary wants to send to a isolated machine, forward the packets to that machine, retrieve the network response, and forward that back to the adversary.

Using Port Redirection, adversaries and Red Teams can compromise machines that are located deep inside a target's network and completely isolated from the Internet.

Exercise

Using C/C++ or Go, write a Port Redirection tool.

You can use FPipe.exe as an example of what you need to build.

Learning Objective(s)

Completing this exercise will teach you an attack tradecraft to attack and compromise machines located inside restricted networks. This skill is a must-have if you want to deliver more advanced Red Team Operations.

☐ Implement a feature in your malware to forward network traffic from the operator's machine to a target machine that does not have Internet access via a compromise machine that is connected to the Internet

☐ Demonstrate that you can RDP into restricted machines via compromised machines by forwarding network packets

☐ 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 \(n.d.\). Port Forwarding](#)
2. [Raj Chandel \(n.d.\). Comprehensive Guide to Port Redirection using Rinetd](#)
3. [McAfee \(n.d.\). FPipe](#)

Exercises · Red Teaming · Exercise f2ed17ad-6f41-49ba-a2b3-7e1e08a88a3e

Step 1 out of 3

Write Malware That Disables Windows Defenses

Exercise

Using Powershell, write malware that disables Windows Defenses.

Learning Objective(s)

Windows by default comes with various security features that help protect the system from malicious activity, and attackers employ to achieve this.

☐ Disables Windows Defender

☐ Disables Windows Error Reporting

☐ Disables BitLocker

☐ Disables the local firewall

☐ Validation: Test your malware

☐ Produce a professional submission

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. [Microsoft \(n.d.\). Windows Defender](#)
2. [Microsoft \(n.d.\). Bitlocker](#)
3. [Microsoft \(n.d.\). About WER \(Windows Error Reporting\)](#)

Exercises · Red Teaming · Exercise f2ed17ad-6f41-49ba-a2b3-7e1e08a88a3e

Step 1 out of 3

Write A TCP Reverse-Shell

Exercise

Write a program that establishes a reverse shell connection to a target machine.

You must write your own custom code.

Learning Objective(s)

Reverse shells are the most common technique used by attackers to maintain access to a compromised machine. How to write the most common reverse shell.

☐ Perform reverse connection

☐ Your program can connect to a target machine

☐ Your program can execute commands on the target machine

☐ Your program can maintain a persistent connection

☐ Produce a professional submission

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](#)

HackTricks

HackTricks

Reading time: 6 minutes



Hacktricks logos & motion design by [@ppiernacho](#).

WELCOME!

[HackTricks](#)

HackTricks Values & FAQ

About the author

GENERIC METHODOLOGIES & RESOURCES

- Pentesting Methodology
- External Recon Methodology ›
- Pentesting Network ›
- Pentesting Wifi ›
- Phishing Methodology ›
- Basic Forensic Methodology ›
- Python Sandbox Escape & Pyscript ›

[HackTricks](#)

- Run HackTricks Locally
- Corporate Sponsors
 - STM Cyber
 - RootedCON
 - Intigriti
 - Trickest
 - HACKENPROOF
 - Pentest-Tools.com
 - SerpApi
 - 8kSec Academy – In-Depth Mobile Security Courses
 - WebSec
- License & Disclaimer
- Github Stats



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

A close-up photograph of a white and brown cat's face. The cat has large, wide-open eyes and a slightly open mouth, giving it a surprised or excited expression. The background is dark and out of focus.

雲端服務

那麼厲害

HackTricks Training



ARTA



ARTE



GRTA



GRTE



AzRTA



AzRTE

<https://training.hacktricks.xyz/>

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

WiFiChallenge

README Walkthrough Users Scoreboard Challenges

Notifications Profile Settings

Recon MGT

15. What is the domain of the ✓
250

16. What is the email address ✓
250

17. What is the EAP method s ✓
250

SAE

13. What is the flag on the wifi ✓
200

14. What is the flag on the wifi ✓
200

PSK

08. What is the wifi-mobile Al ✓
150

09. What is the IP of the web ✓
150

10. what is the flag after login ✓
150

11. Is there client isolation in ✓
150

12. What is the wifi-offices pa ✓
150

<https://lab.wifichallenge.com/>

WiFiChallenge Academy



WiFiChallenge Academy

Courses WiFiChallenge Lab Exam Sign In

CWP: Certified WiFiChallenge Professional

Let the adventure begin!

Transform your Wi-Fi security knowledge with WiFiChallenge Academy. This course covers Wi-Fi network theory and advanced techniques for managing and attacking Wi-Fi networks. Learn about OPN, OWE, WEP, PSK, MGT, and SAE, conducting security audits and offensive reconnaissance.

Upon completing the course and the practical exam, you will receive the Certified WiFiChallenge Professional (CWP) certification, validating your advanced expertise in Wi-Fi security and positioning you for intermediate roles in cybersecurity. Enroll today and advance your career in Wi-Fi security.

Thumbnail for the CWP course presentation, showing the title 'Presentation Certified WiFiChallenge Prof...' and the WiFiChallenge Academy logo.

<https://academy.wifichallenge.com/>

Web Security Academy (PortSwigger)

Learning materials and labs

Latest

- Web cache deception**
5 labs
- Web LLM attacks**
4 labs
- API testing**
5 labs
- NoSQL injection**
4 labs

Featured

- SQL injection**
16 labs
- Cross-site scripting (XSS)**
30 labs
- Cross-site request forgery (CSRF)**
8 labs
- XXE injection**
9 labs

<https://portswigger.net/web-security>

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>

Web Security Aca (PortSwigger)



Certified Practitioner?

is an official certification for web security professionals, from the makers of [Burp Suite](#). Becoming a Certified Practitioner requires a deep knowledge of web security vulnerabilities, the correct mindset to exploit them, and of how to put this out.

Burp Suite Certified Practitioner?

The Certified Practitioner exam indicates a high-level proficiency in web security testing. It is aimed at professionals who can help organizations protect themselves from cyber threats.

Agency

the latest
to exploit them.
Professional.
ers and the

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](#) →

portswigger.net/web-security/certification

Summarize



紅隊大佬



想成為紅隊仔



資安萌新



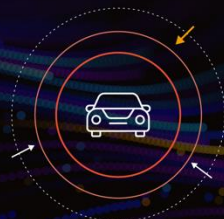
Summarize

資安證照這麼多

我真的需要嗎？

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

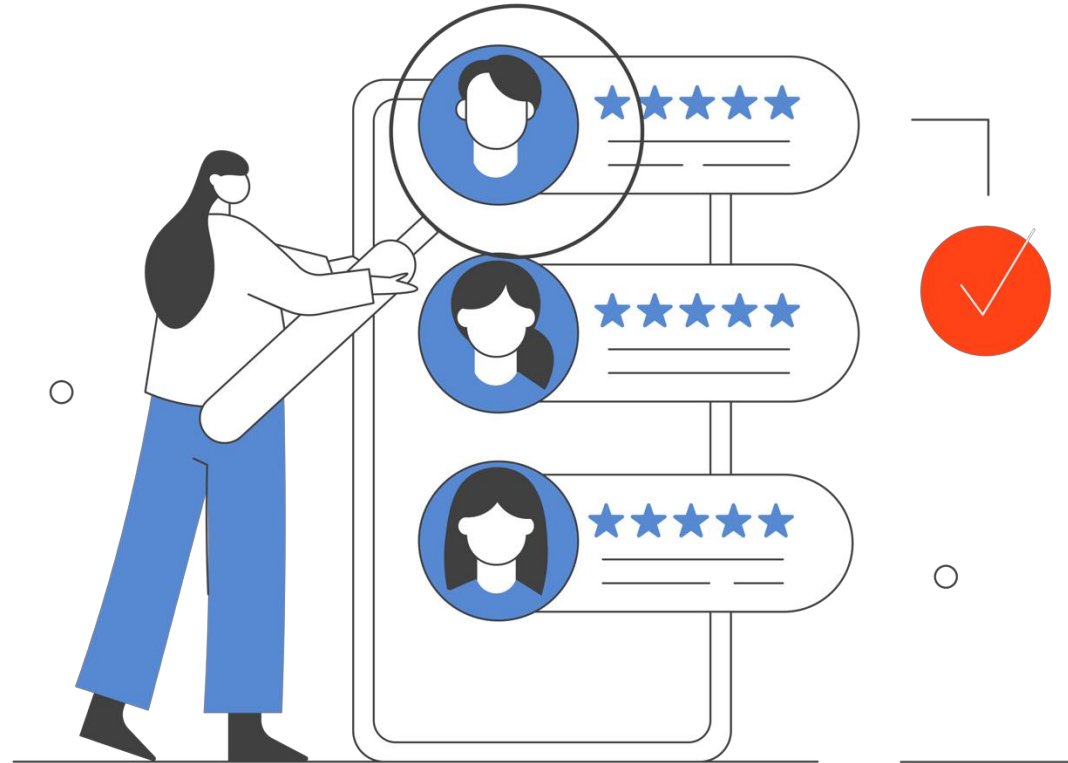
OneSavie Lab 特別講者 (Cymetrics 合作夥伴)

We are Hiring!!!

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



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

