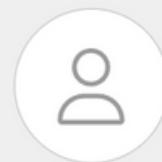


# Report esercizi svolti durante la settimana

1) corso di 6h introduzione alla cybersecurity



This badge was issued to [Saverio Giangiuli](#) on February 22, 2024  
[View celebrations](#)

Your badge must be made public in  
order to share your badge.

Share



## Introduction to Cybersecurity

Issued by [Cisco](#)

Cisco verifies the earner of this badge successfully completed the Introduction to Cybersecurity course. The holder of this student-level credential has introductory knowledge of cybersecurity, including the global implications of cyber threats on industries, and why cybersecurity is a growing profession. They understand vulnerabilities and threat detection and defense. They also have insight into opportunities available with pursuing cybersecurity certifications.

[Learn more](#)

### Skills

Cyber Best Practices

Cybersecurity

Network Vulnerabilities

Privacy And Data Confidentiality

Threat Detection

## 2) corso azure, concetti fondamentali



TROFEO

Concetti fondamentali di Microsoft Azure: Descrivere  
i concetti di base

Data di completamento 23/2/2024

# 2) stanze gratuite tryhackme svolte

## linux fundamentals



### Linux Fundamentals Part 1

Embark on the journey of learning the fundamentals of Linux. Learn to run some of the first essential commands on an interactive terminal.



### Linux Fundamentals Part 2

Continue your learning Linux journey with part two. You will be learning how to log in to a Linux machine using SSH, how to advance your commands, file system interaction.



### Linux Fundamentals Part 3

Power-up your Linux skills and get hands-on with some common utilities that you are likely to use day-to-day!

## windows fundamentals



### Windows Fundamentals 1

In part 1 of the Windows Fundamentals module, we'll start our journey learning about the Windows desktop, the NTFS file system, UAC, the Control Panel, and more..



### Windows Fundamentals 2

In part 2 of the Windows Fundamentals module, discover more about System Configuration, UAC Settings, Resource Monitoring, the Windows Registry and more..



### Windows Fundamentals 3

In part 3 of the Windows Fundamentals module, learn about the built-in Microsoft tools that help keep the device secure, such as Windows Updates, Windows Security, BitLocker, and more...

## introduction to pentesting



### Pentesting Fundamentals

Learn the important ethics and methodologies behind every pentest.



### Principles of Security

Learn the principles of information security that secures data and protects systems from abuse

## pentesting fundamentals



### Pentesting Fundamentals

Learn the important ethics and methodologies behind every pentest.

cybersecurity

framework

penetration testing

ethics



Info

# stanza OWASP fatta fino al task 18

7380



## OWASP Top 10

Learn about and exploit each of the OWASP Top 10 vulnerabilities; the 10 most critical web security risks.

Start AttackBox Awards Help

67%

Task 1 Introduction

Task 2 Accessing machines

Task 3 [Severity 1] Injection

Task 4 [Severity 1] OS Command Injection

Task 5 [Severity 1] Command Injection Practical

Task 6 [Severity 2] Broken Authentication

Task 7 [Severity 2] Broken Authentication Practical

Task 8 [Severity 3] Sensitive Data Exposure (Introduction)

Task 9 [Severity 3] Sensitive Data Exposure (Supporting Material 1)

Task 10 [Severity 3] Sensitive Data Exposure (Supporting Material 2)

Task 11 [Severity 3] Sensitive Data Exposure (Challenge)

Task 12 [Severity 4] XML External Entity

Task 13 [Severity 4] XML External Entity - eXtensible Markup Language

Task 14 [Severity 4] XML External Entity - DTD

Task 15 [Severity 4] XML External Entity - XXE Payload


Task 16 [Severity 4] XML External Entity - Exploiting

Task 17 [Severity 5] Broken Access Control

Task 18 [Severity 5] Broken Access Control (IDOR Challenge)

Task 19 [Severity 6] Security Misconfiguration

# CTF Easy Peasy




## Easy Peasy

Practice using tools such as Nmap and GoBuster to locate a hidden directory to get initial access to a vulnerable machin...

nmap gobuster steganography cronjob

Easy

nmap




## Nmap

An in depth look at scanning with Nmap, a powerful network scanning tool.

beginner nmap scanning theory

Easy

hydra



## Hydra


Learn about and use Hydra, a fast network logon cracker, to bruteforce and obtain a website's credentials.

hydra bruteforce

Easy

# stanze extra

## CTF guidata con video mr.robot




### Mr Robot CTF

Based on the Mr. Robot show, can you root this box?

mrrobot root beginner Medium

## CTF guidata RootMe




### RootMe

A ctf for beginners, can you root me?

security web linux privilege-escalation Easy

## CTF guidata Blue




### Blue

Deploy & hack into a Windows machine, leveraging common misconfigurations issues.

windows eternal blue MS17-010 CVE2017-0144 Easy

## CTF guidata Vulniversity



### Vulniversity

Learn about active recon, web app attacks and privilege escalation.

recon privesc webappsec video Easy