European Cyber Security Challenge

Dr. Dimitrios Patsos, Chief Technology Officer

CISSP, CISM, C|EH, C|HFI, CCDA, CCSE, SCCISP

Agenda

- Basics and History of the Competition
- Structure of Challenges & Skills
- Challenges Overview

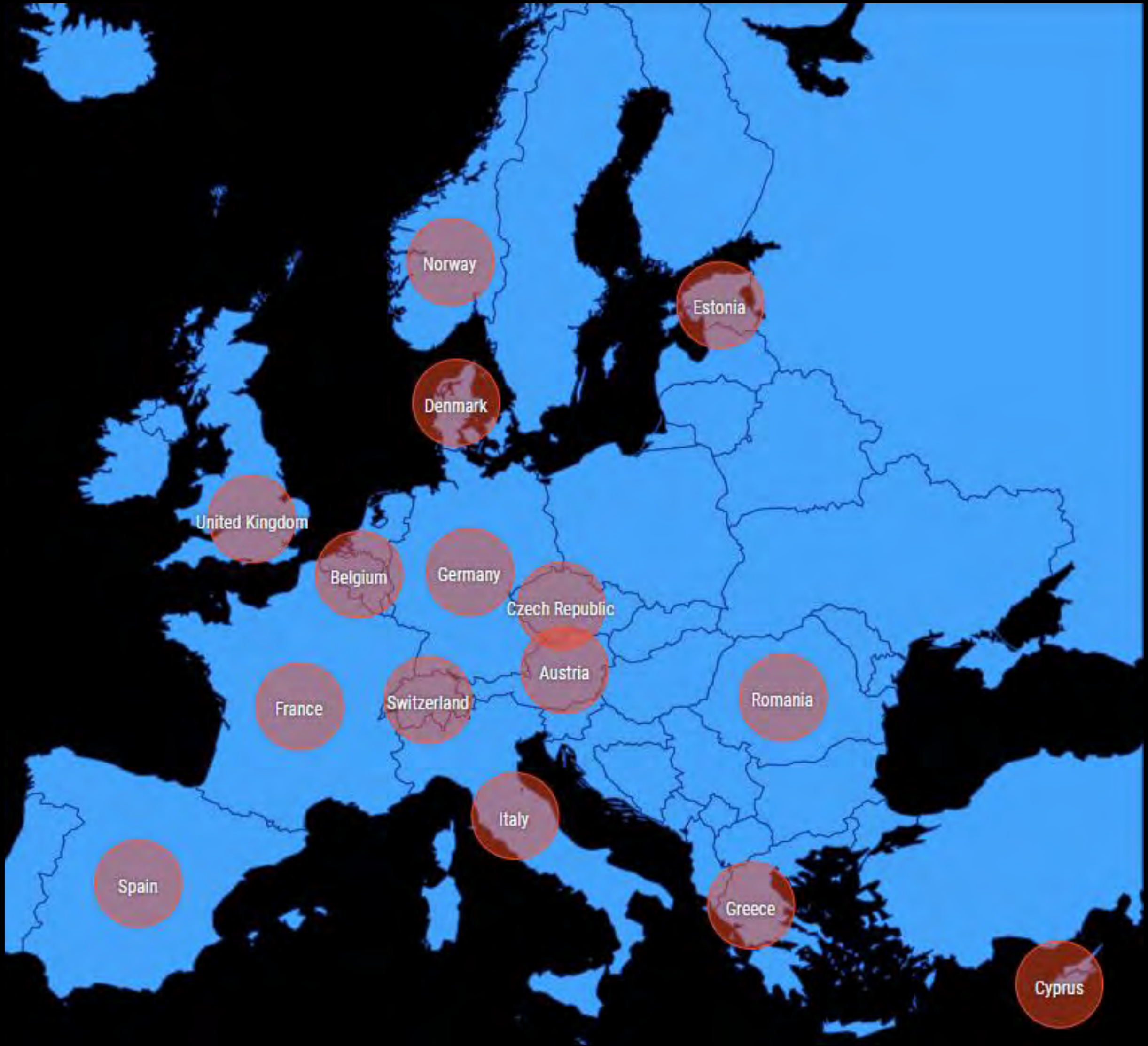
What ECSC is about

- It **is acknowledged** that there is a growing need for **IT security professionals** worldwide
- To mitigate **this shortage**, many countries launch **National Cyber Security Competitions**
- The **aim** of these competitions are:
  - Find **new** and **young talents** in **cyber security**
  - **Encourage** young people to **pursue a career** in **cyber security**
- The **European Cyber Security Challenge – ECSC** adds a **Pan-European layer** on these **National Competitions**

The Basics

- It is an initiative of the **European Commission** supported by **ENISA**
- **Annually**, the competition brings together **young talents** from **European Countries** to have fun and **compete in cyber security**
- The goal of **ECSC** is to place **Cyber Security** at the **service of humankind**
- **Promoting:**
  - **An open, safe and secure cyberspace**
  - **A peaceful society with democratic values**
  - **Free and critical thinking**
- A **Cyber Security championship**

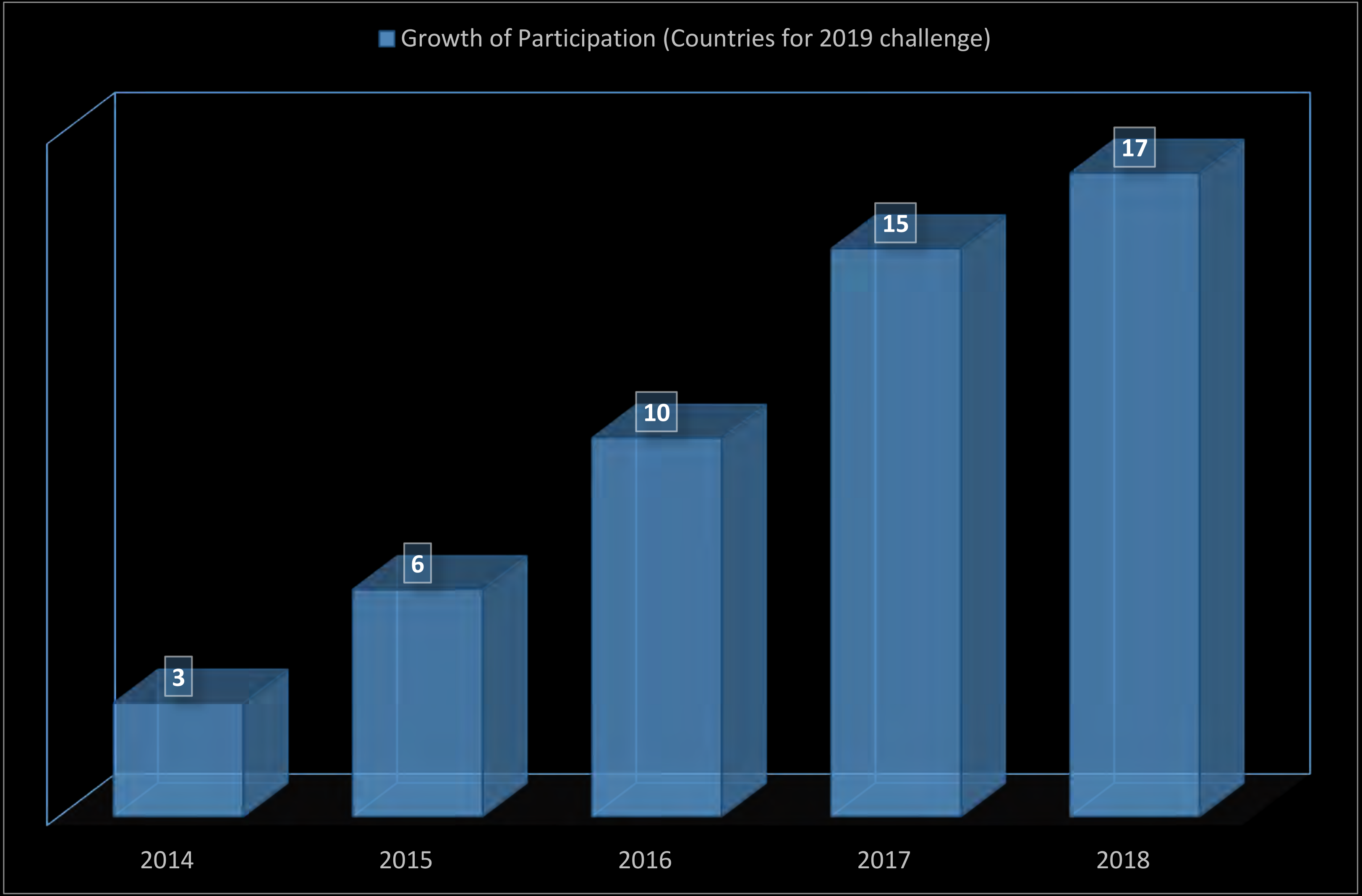
Participation of European Countries



Ireland, Lichtenstein, Luxembourg, Netherlands & Poland participate for the 1st time

Participation of countries in 2018

Growth of Participation in Numbers

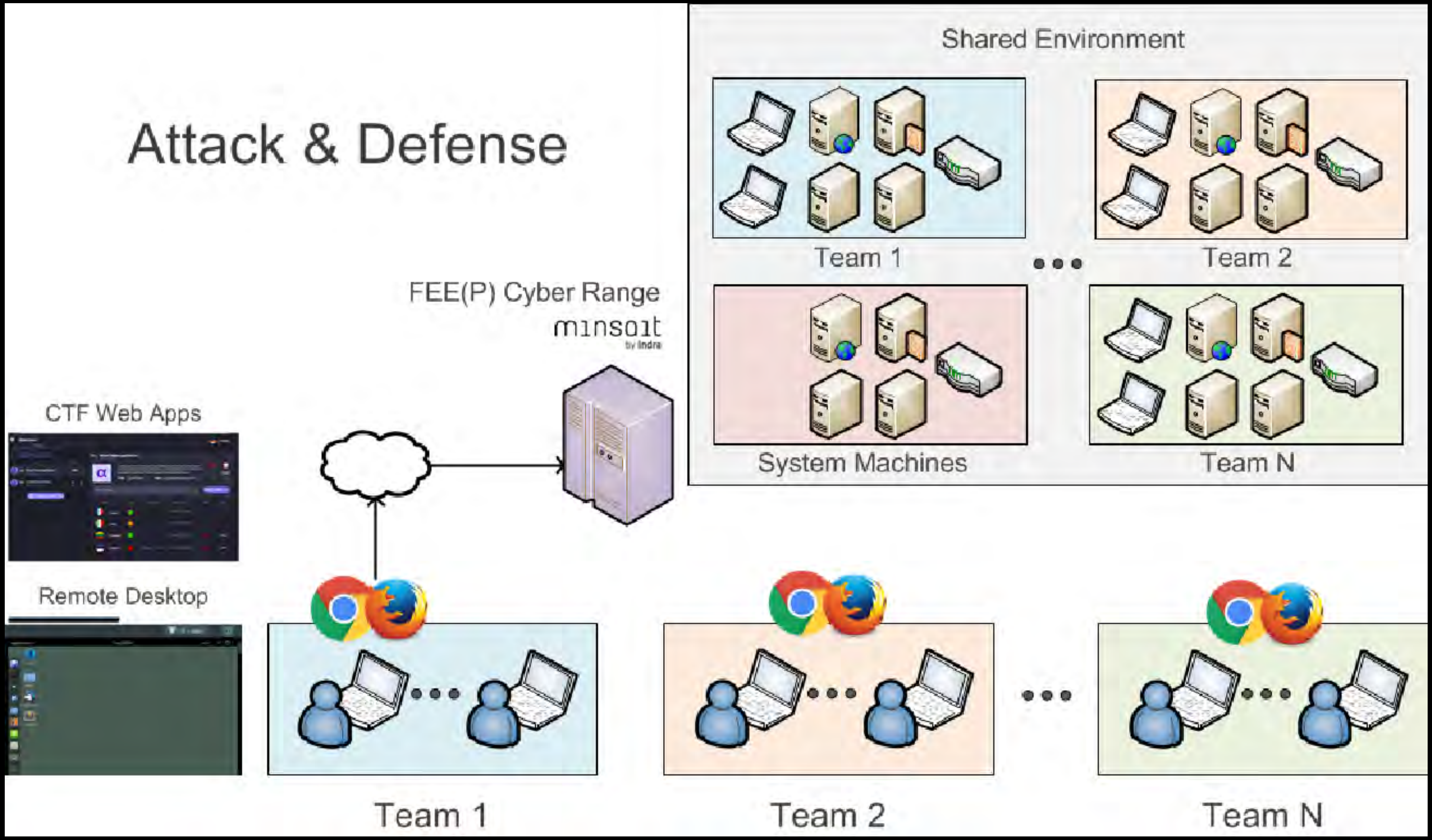


Structure

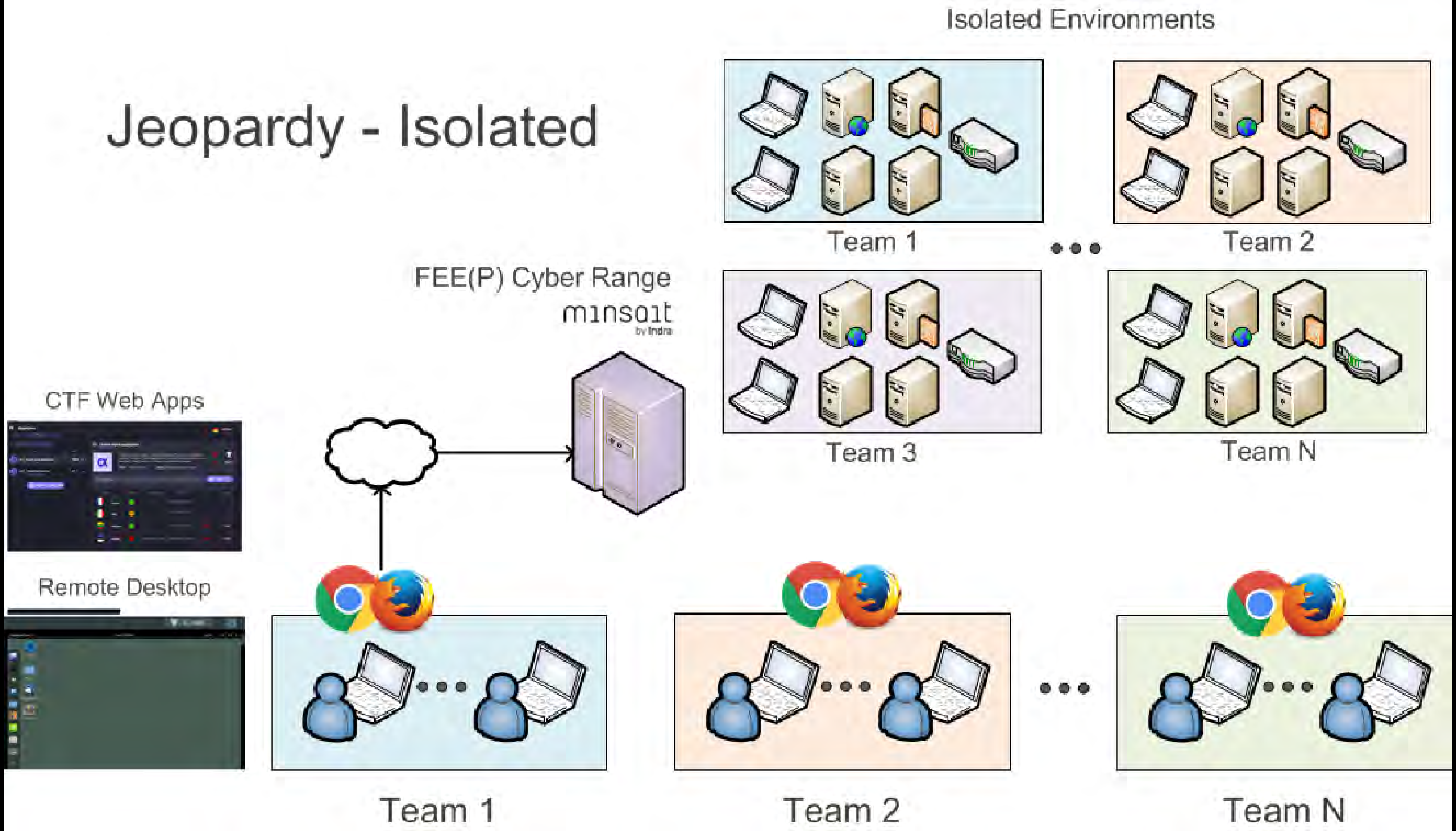
Overview

- It will be based on the **educational exercise Capture-The-Flag (CTF),** which gives the participants experience in:
    - **Securing** a **machine** or an **application**
    - **Conducting** and **reacting** to **attacks** found in the **real world**
- Challenges will include:
    - **Reverse engineering, network sniffing, protocol analysis**
    - **System administration, programming, cryptoanalysis**
    - **Web security, forensics, mobile security**
- In both styles: (a) **attack/defense** and (b) **Jeopardy**

CTF: Attack and Defense



CTF: Jeopardy



Skills

Operating Systems	Forensic Analysis	Web Hacking	Crypto Puzzles
Malware Analysis	Reverse Engineering	Social Engineering	Mobile Security
Esteganography	Database Security	Code Analysis	Cryptography
Secure Programming	Penetration Testing	Network Security	Miscellaneous

The Challenges

Types of Challenges

For ECSC 2018, 36 challenges were provided that belong to the following technical fields:

Unix privilege escalation	Forensic Traffic Analysis
Forensic Image Analysis	Memory Dump Analysis
Android mobile	Packet capture analysis
Password attack / Hash stealing	Steganography
Password attack / Brute-forcing	Node analysis
Crypto	Cryptanalysis
Exploit development	Post-incident forensics on Linux
Hardware	Post-incident forensics on Windows
Combination network / reversing	CTF

95% or more of the above were solved.

Objectives of Challenges

Most of the challenges require knowledge of methodologies and vulnerabilities in accordance with the OWASP Top 10 project:

(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A5) Broken Access Control
(A6) Security Misconfiguration
(A8) Insecure Deserialization
(A9) Using Components with Known Vulnerabilities

Moreover, many concepts refer to well-known technologies, as well as crypto-currencies. Attack vectors vary depending on the type of the challenge (crypto, web, mobile, etc.) and contestants need to identify these in a timely manner in order to proceed.

Following the Trail

Unix privilege escalation challenge. Estimated time to complete: 4 hours. Difficulty: Hard

Image Intelligence - Scenario #1

Forensic Image Analysis challenge. Estimated time to complete: 1 hour. Difficulty: Easy

Do Androids Dream?

Android mobile challenge. Estimated time to complete: 4 hours. Difficulty: Medium

Beneath the Waves

Password attack / Hash stealing challenge. Estimated time to complete: 4 hours. Difficulty: Hard

Unscrambling the Message #1 - Source

Crypto challenge. Estimated time to complete: 3 hours. Difficulty: Medium

Unscrambling the Message #2 - Binary

Crypto challenge. Estimated time to complete: 3 hours. Difficulty: Medium

Proving your Skills #1 - Smashing the Stack

Exploit development challenge. Estimated time to complete: 3 hours. Difficulty: Medium

Vigenère Cipher Cracking

Crypto challenge. Estimated time to complete: 3 hours. Difficulty: Medium

Hardware Manipulation #1

Hardware challenge. Estimated time to complete: 3 hours. Difficulty: Medium

ADACOM CYBER SECURITY

Curious Service

Combination of network/ reversing challenge. Estimated time to complete: 3 hours. Difficulty: Hard

Image Intelligence - Scenario #2

Forensic Image Analysis challenge. Estimated time to complete: 1 hour. Difficulty: Easy

ADACOM
CYBER SECURITY

KnowYourBrand - Forensic Analysis

Forensic challenge. Estimated time to complete: 4 hours. Difficulty: Medium

KnowYourBrand - Traffic Analysis

Forensic traffic analysis challenge. Estimated time to complete: 2 hours. Difficulty: Easy

KnowYourBrand - Blockchain Analysis

Memory Dump Analysis challenge. Estimated time to complete: 3 hours. Difficulty: Medium

KnowYourBrand - TreasurePro

Packet capture analysis challenge. Estimated time to complete: 2 hours. Difficulty: Easy

KnowYourBrand - Data Leakage

Packet capture analysis, steganography challenge. Estimated time to complete: 2 hours. Difficulty: Easy

KnowYourBrand - RSA Analysis

Packet capture analysis / cryptanalysis challenge. Estimated time to complete: 3 hours. Difficulty: Medium

Game of Dorms

Password attack / Bruteforcing challenge. Estimated time to complete: 1 hour. Difficulty: Easy

Forest for the Trees

Node analysis challenge. Estimated time to complete: 2 hours. Difficulty: Easy

Lost in Transmission

Packet capture analysis challenge. Estimated time to complete: 3 hours. Difficulty: Medium

Ma Baker

Cryptanalysis challenge. Estimated time to complete: 3 hours. Difficulty: Medium

ADACOM
CYBER SECURITY

Ma Baker Returns

Cryptanalysis challenge. Estimated time to complete: 3 hours. Difficulty: Hard

Byte Queen

Cryptanalysis challenge. Estimated time to complete: 2 hours. Difficulty: Easy

Abyssinium Forensics - Linux

Post-incident forensics on Linux challenge. Estimated time to complete: 6 hours. Difficulty: Hard

Abyssinium Forensics - Windows

Post-incident forensics on Windows challenge. Estimated time to complete: 6 hours. Difficulty: Hard

Bob's Encrypted Email

Cryptanalysis challenge. Estimated time to complete: 1 hour. Difficulty: Easy

Analyzing BC4

Cryptanalysis challenge. Estimated time to complete: 1 hour. Difficulty: Easy

Online Banking OTP Token

Cryptanalysis challenge. Estimated time to complete: 2 hours. Difficulty: Medium

Old Cryptogram

Cryptanalysis challenge. Estimated time to complete: 1 hour. Difficulty: Easy

Congo

CTF challenge. Estimated time to complete: 3 hours. Difficulty: Medium

ADACOM
CYBER SECURITY

Domotica

CTF challenge. Estimated time to complete: 1 hour. Difficulty: Easy

Irony

CTF challenge. Estimated time to complete: 2 hours. Difficulty: Easy

Patient0

CTF challenge. Estimated time to complete: 3 hours. Difficulty: Medium

Untrackable

CTF challenge. Estimated time to complete: 2 hours. Difficulty: Easy

VelvetTrail

CTF challenge. Estimated time to complete: 4 hours. Difficulty: Hard

The Device

Hardware challenge. Estimated time to complete: 3 hours. Difficulty: Medium

ADACOM CYBER SECURITY

Bonus: Bandstand

Physical challenge. Objectives:

1. Bypass electronic access control
2. Disarm an intruder alarm using a number sequence challenge
3. Bypass some combination locks
4. Solve some hidden riddles which will be exposed by use of a UV torch
5. Using teamwork, disarm a device (wire cutting challenge)

Needed skills?

Participants must be of age 14-25.

Participants should be cybersecurity enthusiasts, amateurs or professionals.

Due to the nature of the challenges, participants need to possess skills in various cybersecurity domains, such as cryptography, forensics, mobile security, web application penetration testing, reverse engineering, etc.

Team members should have presentation and teamwork skills, apart from technical skills.

Questions ?

CYPRUS
CYBER SECURITY
CHALLENGE

GOOD LUCK TEAM CYPRUS

ADACOM
CYBER SECURITY

Thanks for Watching !

United Kingdom
London
88 Wood Street,
Barbican EC2V 7RS,
+44 (0) 20 3287 8026

Greece
Athens
25 Kreontos Street,
104 42,
+30 210 5193700

Serbia
Belgrade
Omladinskih Brigada 90v,
11070 Airport City,
+381 11 3219425

Cyprus
Nicosia
Lapithou 11
2410
+357 99 318516