EU CyberSecurity challenge

Cosmin Ciobanu| Expert in NIS

Athens | 21.08.2015

European Union Agency for Network and Information Security

ENISA CERT training

- ENISA CERT training and exercise material was introduced in 2008, from 2012 till now it was complemented with new scenarios containing essential material for success in the CERT community and in the field of information security.

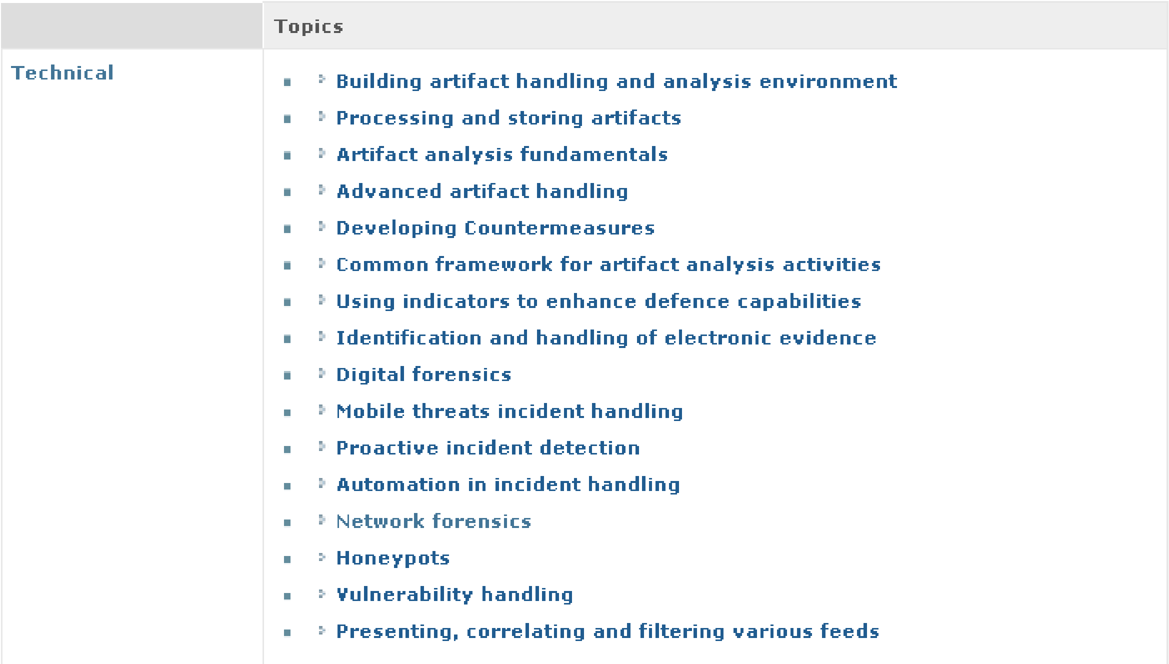
- At the moment there are over 36 different training scenarios and counting

Training Courses

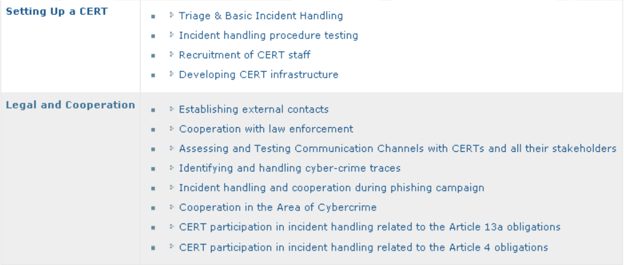
Training Resources

http://www.enisa.europa.eu/activities/cert/training/

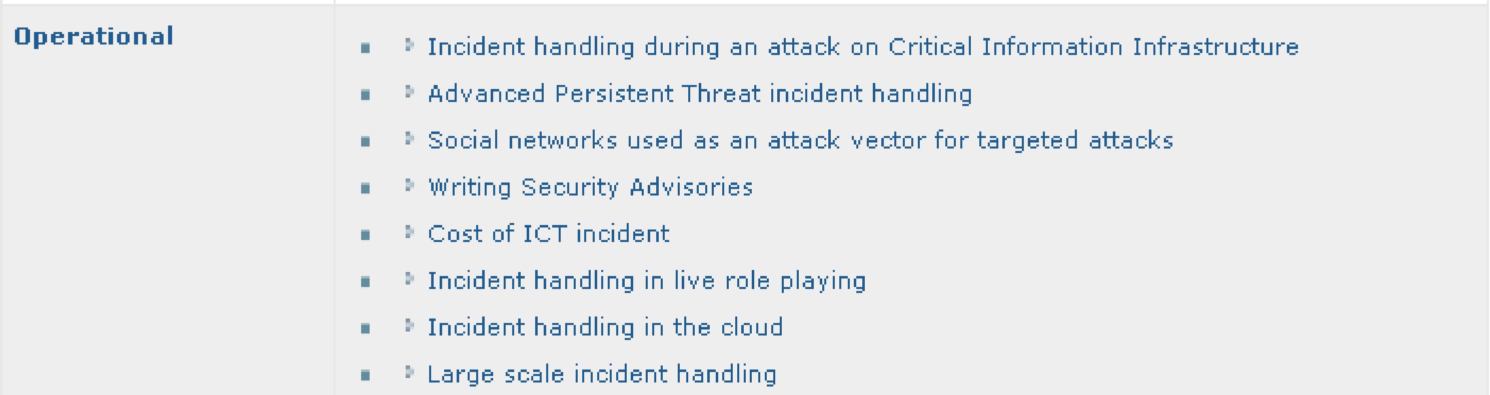
ENISA CERT training scenarios



	Topics
Technical	Building artifact handling and analysis environment Processing and storing artifacts Artifact analysis fundamentals Advanced artifact handling Developing Countermeasures Common framework for artifact analysis activities Using indicators to enhance defence capabilities Identification and handling of electronic evidence Digital forensics Mobile threats incident handling Proactive incident detection Automation in incident handling Network forensics Honeypots Vulnerability handling Presenting, correlating and filtering various feeds



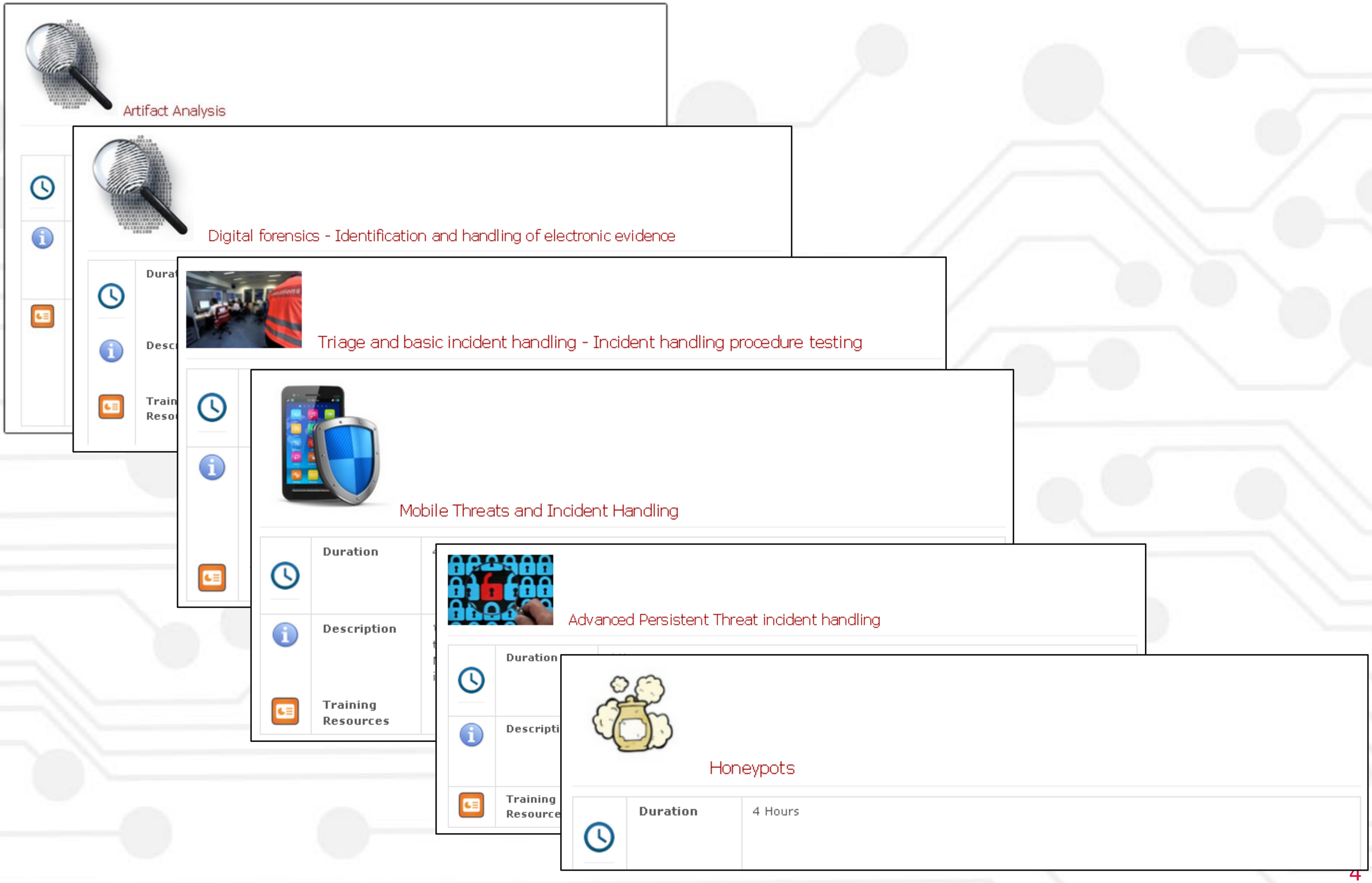
Setting Up a CERT	Triage & Basic Incident Handling Incident handling procedure testing Recruitment of CERT staff Developing CERT infrastructure
Legal and Cooperation	Establishing external contacts Cooperation with law enforcement Assessing and Testing Communication Channels with CERTs and all their stakeholders Identifying and handling cyber-crime traces Incident handling and cooperation during phishing campaign Cooperation in the Area of Cybercrime CERT participation in incident handling related to the Article 13a obligations CERT participation in incident handling related to the Article 4 obligations



Operational	Incident handling during an attack on Critical Information Infrastructure Advanced Persistent Threat incident handling Social networks used as an attack vector for targeted attacks Writing Security Advisories Cost of ICT incident Incident handling in live role playing Incident handling in the cloud Large scale incident handling

http://www.enisa.europa.eu/activities/cert/training/training-resources

ENISA CERT training courses



Artifact Analysis

Digital forensics - Identification and handling of electronic evidence

Durat

Desc

Train
Reso

Triage and basic incident handling - Incident handling procedure testing

Mobile Threats and Incident Handling

Duration

Description

Training
Resources

Advanced Persistent Threat incident handling

Duration

Descripti

Training
Resource

Honeypots

Duration	4 Hours

http://www.enisa.europa.eu/activities/cert/training/courses

Intro to CTF

Capture the flag (CTFs):
CTFs are competitions which combine many Information Security topics into small measurable exercises.
The answers submitted by the participants are called **flags**.
Each flag yields a particular number of points.
Most of the times a flag looks like:
e48e13207341b6bffb7fb1622282247b
ctf{flag_hash_goes_here}

CAPTURE THE FLAG

PRESS SPACE TO START

PRESS I FOR INSRCUCTIONS

Short term goals:

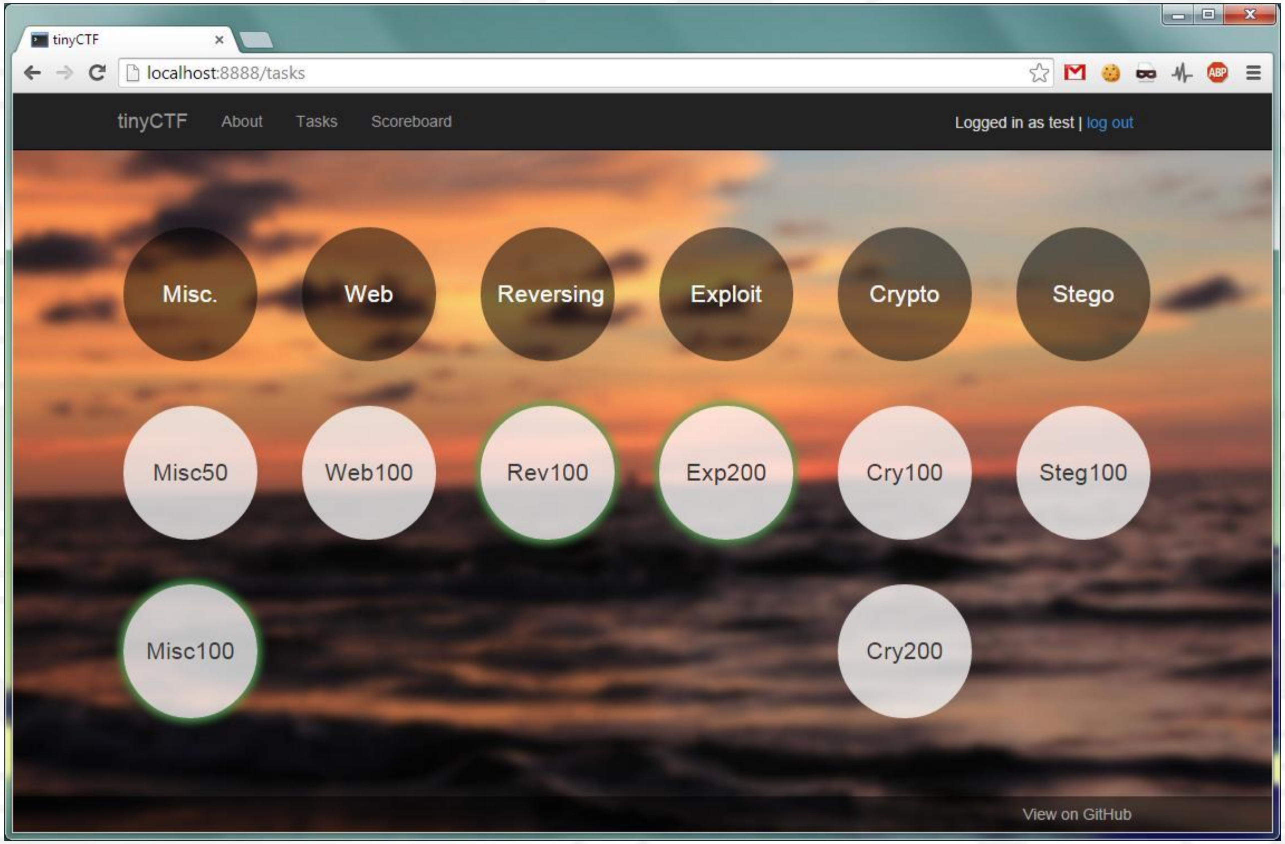
- Get as many flags as possible (Solve as many challenges as possible.
- Win prizes ☺

Long term goals:

- Learn new skills.
- Improve and refresh your current skills on the topic.
- Develop team work and collaboration abilities.

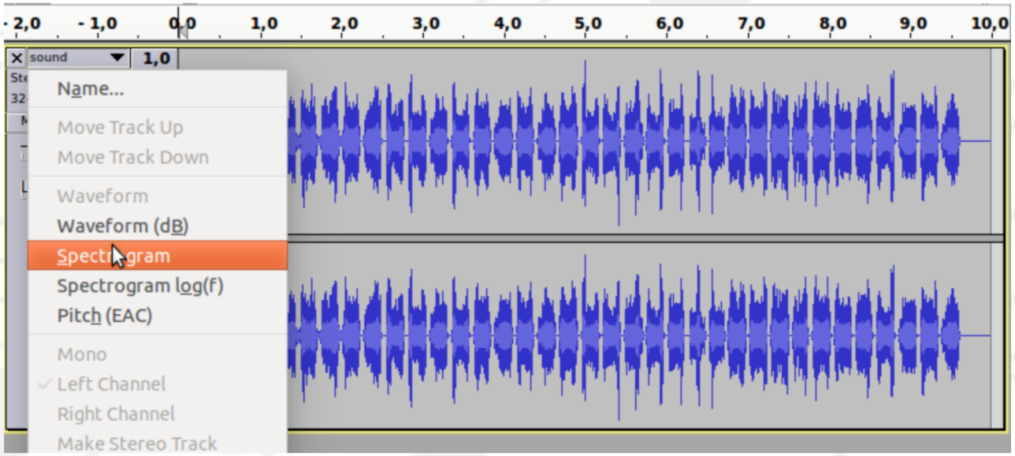
CTF challenges

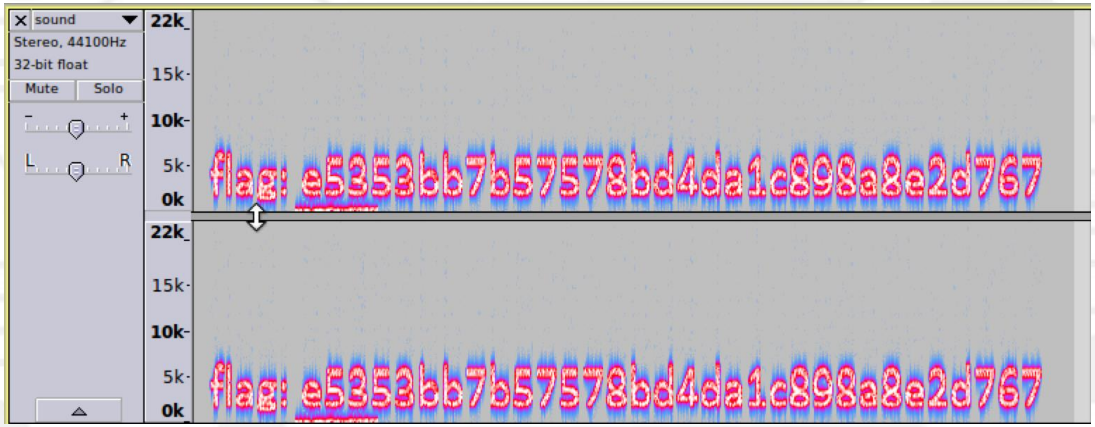
TinyCTF platform:



Example of a stego challenge

You have one file.wav and you have to find the flag:





flag: e5353bb7b57578bd4da1c898a8e2d767

flag: e5353bb7b57578bd4da1c898a8e2d767

European Cyber Security Challenge

Cyber Security Challenge UK
Cyber Security Challenge
GERMANY
AUSTRIA
CYBER SECURITY
CHALLENGE
cyber camp
SWISS CYBER STORM
ROMANIA
CYBER SECURITY
CHALLENGE

Objectives & goals:

- Nowadays there is a shortage of IT Security professionals
- The ECSC is trying to address this gap by organizing a CTF (capture the flag) competition for young cyber talents and for encourage them to pursue a career in cyber security
- An important aspect of the competition is the Pan-European participation.
- The top cyber talents from each country meet to network and collaborate and finally compete against each other to determine which country has the best cyber talents.

Scope:

- Teams from EU member states can participate.
- The participants are from 14 – 30 years old
- The participants are not subject matter experts (They don`t have special security certifications CEH,OCSP, CISSP, GIAC etc).

European Cyber Security Challenge

- ENISA is facilitating the preparations & organization of the ECSC.
- In 2015 there are 6 countries participating: UK, DE, AT, ES, RO, CH
- In each participating country the national competition is taking place.
- The finalists from national competitions will participate in the final competition that will take place in October 21./22., KKL Lucerne, Switzerland

National competitions:
http://www.verbotengut.at/
http://www.cybersecuritychallenge.de
http://www.cybersecuritychallenge.ro
https://cybercamp.es/
http://challenge.swisscyberstorm.com
http://cybersecuritychallenge.org.uk/
Main event:
http://www.europeancybersecuritychallenge.eu/