EGI-CSIRT
Security Training Portfolio

EGI CSIRT

DI4R Conference Krakow / WISE meeting

www.egi.eu

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

Overview

EGI CSIRT Trainings:

Defensive: Protect your (grid-)site while under attack. (Leif Nixon)

Offensive: Scan for Vulnerabilities, attack! (Leif Nixon, Daniel Kouril)

Security tools/monitoring: install configure security monitoring in a training env.

Forensics: This VM got compromised, find out what happened. (Heiko Reese)

Role Play Training . . . Today :)

Defensive

- Developed 2011 by Leif Nixon, includes an advanced infrastructure.
- Lecture, Scoreboard, competition. Focus on Finding Leads/Reporting
- Online Version 20 participants max.
- Offline Version (1/2 day) approx 100 participants.
- Material contains Forensics tools/Docs.
- 20+ events, globally (Taipei, Australia, Europe).

Defensive, Cloud

- Developed 2014 by Heiko Reese (KIT CERT)
- Lecture
- VM images
- Task analyse the VM image, usage of snapshots
- Resolve the incident
- approx 20 Participants per event, can scale out, more trainers needed
- EGI Conf. Helsonki, HepSysman meeting UK

Offensive

- Developed 2015 by Leif Nixon.
- Pentesting in a game environment, advanced infrastructure.
- Lecture about Pentesting, typical service vulnerabilities.
- Competition.
- Extensive Introduction to a pentest toolset.
- approx 20 participants (Online Version) 1 day.
- 100+ in the offline version (1/2 day).
- 10+ events

Getting Started with Pentesting

- Excercise to introduce basic attacker techniques
- Organized as a game for the attandees
  - The first one to pass all levels wins
- Developed by Masaryk univesity, utilizing its simulation environment
  - Sandboxed environment embedding local networks
  - Users has full control over one machine, need to get access to others
  - Every user has a dedicated environment
- Performed several times at EGI events and at partners.
  - One game takes cca 4 hours (including introduction of techniques)
  - Max. number attandees 30-40

Security Tools/Monitoring

- Training Lab consisting of VMs
- Install Configure Pakiti, central logging etc
- Developed 2013
- Can take 20 trainees

RolePlay Training

- Developed 2016
- 10 - 30 Patticipants
- 3 Events (Taipei, Zürich, Krakow)
- Participants with a wide range of backgrounds