RolePlay Training

Sven Gabriel, (Nikhef/EGI-CSIRT) / Ian Neilson (STFC/EGI-CSIRT)

EGI-CSIRT — Operational Security

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

Introduction

Earlier Trainings:

Defensive: Protect your grid-site while under attack.

Offensive: Scan for Vulnerabilities, attack!

Training Site: set-up Security tools.

Forensics: This VM got compromised, find out what happened.

Why something different

Pro:
Fun! building tech stuff is always fun

Con:
Focusing on technology (forensics, monitoring tools etc) requires an advanced lab, can only cover few details. (time constraints) All participants should have a similar background,

difficult to get a full picture with just tech experts.

RolePlay

Goal:
Handling a simulated real-life incident affecting new technology, get all affected parties involved on a high level.

Expected Results
Putting the Incident Response Procedures to a test, identify potential gaps.

Larger range of the Target Audience
Members/Future Members of Security/Admin Teams, Management, Press-, Legal Contacts

Gedankenexperiment

Motivation: What if?:

- . . . a certain technology gets deployed/widely used in the Infrastructure. Will we be able to deal with an atacker abusing this technology.
- Get into other's people's shoes, Working together, understand better the problems/tasks of the other players.
- Communication: talk to Users, Sites, VOs, Management is crucial in Incident Response in a distributed Infrastructure. Easier when all are in one room.

What is a RolePlay

RolePlay:

- Characters
- Capabilities, duties
- Interactions, communications
- Script/Story

What is a RolePlay

RolePlay:

- Characters
- Capabilities, duties
- Interactions, communications
- Script/Story

What is a RolePlay

RolePlay:

- Characters
- Capabilities, duties
- Interactions, communications
- Script/Story

What is a RolePlay

RolePlay:

- Characters
- Capabilities, duties
- Interactions, communications
- Script/Story

Set-Up

Schedule:

- RolePlay is organized in 4 Phases (+ Recovery from the incident, Evaluation)
- In each Phase the teams receive a brief description of the latest developments plus high level tasks related to their role.
- Timing: 10 Minutes to work on the task, + 20 minutes to communicate/discus the results/decisions taken.
- At the beginning of the Phases a Broadcast message is displayed, to make sure everyone has the same background information
- Start: Set the scene, Introduce Roles, Units, short description of the scenario
- Build teams, Assign Roles/Characters.

Start with Phase line alpha . . .

Characters

The Characters

The Roles

Roles and Players:

- 3 Sites (ONE, TWO, THREE), varying size, advanceness of management / monitoriug tools
- NGI Security Officer/Manager
- VO, Manager, Security Contact, Users.
- Organisation (University) Manager, IdP Admin, is part of a Federation (BigFed)
- Federation Operator (Hannah, Alessandra)
- EGI-CSIRT
- . . . more players if needed

Story

Compromised Identity Provider

Compromised Idp

Scenario:
The VO Aperture Science has build a competitive environment. Currently there is one very attractive position to be filled, the user with the best publication will get the job.
2 interesting individuals are in the race, James Herbert B. spend the past months at Neumayer Station where he found the proof for a controversely discussed theory. The theoretical calculations are based on a dataset he stored in the Grid.
The other being Glados, an ethically challenged contemporary with an obsession of spy movies from the last millennium, not really a friend of James

1st Phase

And then ...:

User James Herbert B contacts Site-ONE, that he can not access his files, in fact the whole StorageResourceManager seems dead.

Exercise

Checkpoint 1:

1st Phase

And then ...:

User James Herbert B contacts Site-ONE, that he can not access his files, in fact the whole StorageResourceManager seems dead.

EGI-CSIRT Broadcast 1

Recipients: All Sites, NGI-Security Officers, Operations, VO-Security

Heads Up: Sites reported suspicious activity related to the Identities Dr, No and James Herbert B. Both Identities belong to VO-Aperture Science. In addition sites should check for connections from 178.20.55.0/24, containing TOR exit nodes.
All sites are urged to check for glibc vulnerability on **all** systems.
Recipients: VO-Security: Could you give us more information about th

EGI-CSIRT Broadcast 2

Recipients: All Sites, NGI-Security Officers, Operations, VO-Security

We have sufficient evidence that the IDs James Herbert B and Dr. No are compromised. We have put these IDs in the argus based Central Suspension framework. Note that this might require manual intervention by the sites to take effect.
All sites are requested to suspend: James Herbert B. and Dr. No
Another bit of information that is missing is the IdP, by now its not to which the IdP the problematic IDs belong to. Sites are asked to check their SP logs for metadata that could give a hint to the IdP.

EGI-CSIRT Broadcast 3

Recipients: All Sites, NGI-Security Officers, Operations, VO-Security

VO Aperture Science has multiple malicious Ids. Its yet not clear how they got set-up in first place and how they entered the VO.

EGI-CSIRT Broadcast 4

Recipients: All Sites, NGI-Security Officers, Operations, VO-Security

All entities please provide a close out report, focus on what was missing during incident recognition/response. What is needed to recover from this incident? What would you do to prevent this from happening again.

Final Phase

Debriefing:

- If you were involved in such an incident, what would you miss (Back-ground Information, Tools, Communication Endpoints)
- What would be the steps to prevent such an incident.
- How could one monitor for this type of incidents?