Federated AAI meets reality, Security Incident Handling Role Play in DI4R

Sven Gabriel, (Nikhef/EGI-CSIRT)

EGI-CSIRT Role-Play Training

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

Introduction

Authors/Contributors:

- David Groep Nikhef
- Ian Neilson STFC/RAL
- Hannah Short (CERN)
- Sven Gabriel (Nikhef/EGI-CSIRT)
- more to come . . .

Schedule

- 11:30 – 11:45 Refresher: Federated Identity Management
- 11:45 – 12:00 Assurance and Federation
- 12:15 – 12:30 Scenario / The Characters / Pick Roles
- 12:30 – 12:45 Phase alpha: Get used to your Role, finish Phase alpha Task-card.
- 12:45 – 13:00 Phase Bravo: Incident slowly starts.
- 13:00 – 14:00 **Lunch Break**
- 14:00 – 14:20 Phase Charly: Incident spreads out, coordination needed.
- 14:20 – 14:40 Phase Delta: More noise is added from external players.
- 14:40 – 15:00 Phase Echo: Contain the incident.
- 15:00 – 15:30 Evaluation.

Story

Introduction

Introduction

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 :)

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

RolePlay

Why a roleplay:

- Address range of Specialists with different background.
- Handling a simulated real-life incident affecting new technology, get all affected parties involved on a high level.
- Members/Future Members of Security/Admin Teams, Management, Press-, Legal Contacts

Expected Results

- Putting the Incident Response Procedures to a test, identify potential gaps.
- Get into other peoples shoes – by working together we can better understand the different priorities of the other players.
- Planning for implementation – modeling in a roleplay helps to identify potential problems.

Gedankenexperiment

- . . . a certain technology gets deployed/widely used in the Infrastructure. Will we be able to deal with an attacker abusing this technology.
- Roles:
  - Infrastructure: Security Officer (NGI),3 Resource centers (different levels)
  - VO Aperture Science (Manager, Users)
  - Organisation (university of Lapuda) running an Identity Provider (Manager, Admin)
  - Federation BigFed, Federation Operator
  - Jornalist, Infrastructure Media Relations
  - Lawyer, Legal contact.

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, + 5 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 . . .

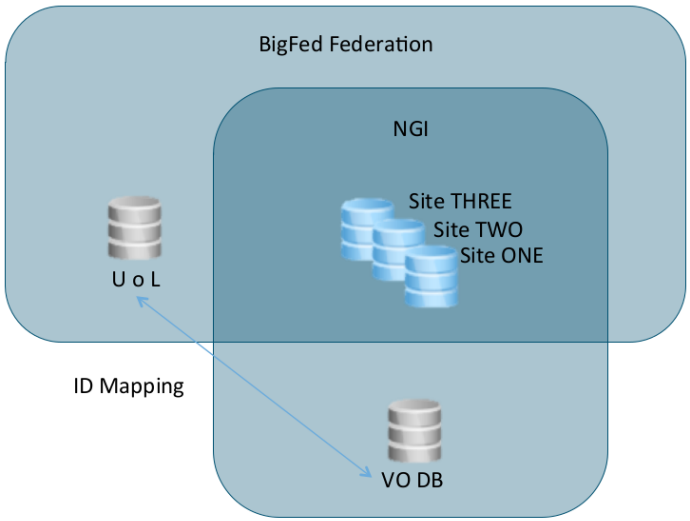
Characters

The Characters

Introduction

Scenario / Identity Management:

- VO registration requests are sent to the VO by the IdP via mail.
- Users are identified by eduPersonPrincipleName
- Known users can log in to NGI sites using Federated Access



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 controversially 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

Phase alpha

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:
Phase line alpha tasks completed/discussed

EGI-CSIRT Broadcast 1

Phase alpha, Recipients: All Sites, NGI-Security Officers, Operations,

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 the identities James Herbert B. and Dr. No?
What is their home organisation?

EGI-CSIRT Broadcast 2

Phase Bravo, Recipients: All Sites, NGI-Security Officers, Operations,

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

Phase Charly, Recipients: All Sites, NGI-Security Officers, Operations

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

Phase Delta, Recipients: All Sites, NGI-Security Officers, Operations,

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?
- What would be the role of your CERT in SIRTFI?