# 8. Exercise: Establishing External Contacts

| | | |
|---|---|---|
| Main Objective | To enhance students' skills in establishing contacts with other CERTs, administrators of ISPs, and other parties responsible for the mitigation of security incidents in their networks around the globe. | |
| Targeted Audience | This exercise is primarily targeted at new and future employees of CERTs. It requires an understanding of Internet attacks and communication skills. The students should be also good in written and spoken English. | |
| Total Duration | Session One: 1 hour, 10 minutes | |
| | Session Two: 50 minutes | |
| | Note: Students are required to spend additional time on monitoring the mailboxes and responding to e-mails between the sessions. | |
| Time Schedule | ***Session One*** | |
| | Introduction | 10 min. |
| | ***Task 1***: Preparatory research | 30 min. |
| | ***Task 2***: Creating the letters | 30 min. |
| | ***Session Two*** | |
| | ***Task 3***: Review | 30 min. |
| | Summary to the exercise | 20 min. |
| Frequency | Once per team member | |

## 8.1 GENERAL DESCRIPTION

The communication and exchange of information is one of the crucial aspects of CERT work. The more effectively information is shared and exchanged between interested parties, the faster security incidents can be mitigated and less damage occurs. Thus, it is very important to have at hand, and know how to use, sources of contact information, networks of contacts and other channels for the distribution and sharing of data.

The goal of this exercise is to enhance students' skills in establishing contacts with other CERTs, administrators of ISPs, and other parties responsible for the mitigation of security incidents in their networks around the globe. The students will be asked to identify and contact proper authorities about real incidents. After finishing the exercise, the students should be able to establish and develop networks of contacts faster and more effectively.

In order to conduct the exercise you need to secure logs from a security system such as a firewall, IDS/IPS, honeypot, netflow from darknets, etc. The logs should include attack descriptions (or the attack type must be easily identifiable), timestamps including time-zone and source IP addresses. If needed, any data about the targeted host can be anonymized. The logs must not be more than five days old.

Alternatively, you may use spam e-mails as long as you know precisely how to identify the source of the message and explain to the students where to look for the offending host.

The students will also need to access and use their business e-mail accounts. It is recommended that PGP/GPG is available for these accounts.

The students should be also able to make international phone calls when necessary.

Before you start the exercise, split the logs into as many parts as the number of students taking the exercise. While doing so, try to make sure that information about sources does not overlap for different students – in other words, no two students should receive information about the same hosts.

Planning the exercise: Note that the exercise is conducted in two sessions, the second one scheduled for two or more working days after the first one. Plan your and the students' time, and book the rooms, etc, accordingly.

## 8.2 EXERCISE COURSE

**Session One**

## 8.3 Introduction

Distribute logs to the students – send them by e-mail or post them on a web page for download. Ask each student to choose between three and five attacks with distinct sources from their logs. Preferably, these sources should be distributed geographically.

### 8.3.1 Task 1 Preparatory research

Ask the students to identify a responsible party (IPS, CERT, etc) that should be able to coordinate. They will find instructions for this in their book. Allow 20-30 minutes for the research. Review the findings, and ask students how they found the contacts and their reasons for choosing them.

### 8.3.2 Task 2 Creating the letters

Ask students to prepare the correspondence. Each e-mail should contain:

- an introduction - this part should include identification of the team on whose behalf the students are working);
- a description of the problem;
- evidence; and
- a request for action.

Allow 20-30 minutes for this part of the exercise. Review the contents, and then let the students send their e-mails.

Pay attention to the tone of the reports. While they should contain a clear request for action, it should not be demanding. CERT should not put itself into a role that might discourage

administrators from cooperating, especially where there is no formal relationship between the CERT and the business or ISP in question.

Ask students to monitor their mailboxes regularly and to reply if needed. Inform the students about the time of the second session, which should be held at least two working days ahead in order to allow enough time for replies.

**Session Two**

### 8.3.3 Task 3 Review

Ask the students to identify a responsible party (IPS, CERT, etc) who should be able to coordinate. Then Ask each student to report on his or her results:

- How many replies did he or she get (with reference to the number of e-mails sent)?
- Was more information exchanged than in the initial e-mail?
- Was the attack mitigated?

## *8.4 Summary of the exercise*

If replies were received, discuss different reactions and what triggered them. If some students were significantly more successful than others, how were their reports different?

If no replies were received, ask the students to discuss the possible reasons why:

- The e-mail did not reach the responsible person (incorrect data published or wrong sources used);
- The e-mail was filtered out;
- The problem was treated with low priority and queued;
- The ISP / CERT does not act appropriately on abuse from its network; and/or
- Other reasons.

Optionally, ask students to call parties who did not respond in a timely manner. Use information found in *whois* databases and on web pages (call centres?). Take time differences into consideration!

## *8.5 EVALUATION METRICS*

You can use the following factors to evaluate the exercise:

- How many reports successfully reached intended recipients?
- In how many cases was positive feedback received?
- How many incidents were successfully mitigated?

When preparing for the exercise, make sure you can measure these numbers as precisely as possible. Use positive examples to motivate students, explain what could be fixed in cases of failure. Explain that no feedback does not necessarily mean unresolved incidents and that even skilled and experienced incident handlers are not able to guarantee success in resolution

in all circumstances. Some negative factors beyond the control of the handler, impacting incident resolution, are:

- unresponsive administrators;
- lack of proper laws and regulations;
- lack of technical means to react beyond own network; and
- inert enforcement of the law.