11. Exercise: Incident Handling in Live Role Playing

Main Objective	The exercise simulates a real-life incident, involving many parties with conflicts of interests, different mindsets and legal frameworks, etc. With the introduction of such aspects as vulnerability handling, responsible disclosure and company security management, it helps the students to understand why incident handling is, in many cases, a complex task and what kinds of technical and social skills are required for this job.	
Targeted Audience	This exercise is primarily targeted at future members of CERTs. It requires almost no technical knowledge, just a basic understanding of terms such as VPN and how the Internet works.	
Total Duration	2 hours, 30 minutes	
Time Schedule	Introduction to the exercise	10 min.
	Task: Role-playing game	120 min.
	Summary of the exercise	20 min.
Frequency	Once per team member	

11.1 GENERAL DESCRIPTION

This exercise is designed to introduce the students to the many different layers and aspects of incident handling, including but not limited to:

- Interaction with end users;
- Interaction with administrators;
- Vulnerability handling; and
- Talking to the management.

It should help them to get into other people's shoes, understand their needs and expectations during the incident handling process, and improve their communications with other actors.

The exercise is in the form of a role-playing game where you will act as the game master. The students will start with a basic script and role descriptions. From there, they will develop the characters themselves while trying to achieve individual goals.

In order to conduct the exercise, you need a room large enough to arrange seating in the form of a round-table for all the students. You also need a copy of the personal role description (included in this book) for each participant.

You should consider getting acquainted with the roles beforehand and assigning them to people according to their personalities and future work as closely as possible. Consequently, if the exercise is used as a part of a longer, multi-day training session, it should be scheduled

towards the end of the course. This will ensure that the students will already be familiar with each other and with the trainer.

11.2 EXERCISE COURSE

The course of the role-playing game is as follows. Your role is to moderate the game.

11.3 Introduction to the exercise

There are seven key roles in this exercise. If needed, you may introduce more characters, eg, a police officer, but unless you plan for them to really interact a lot, it is better if you play those characters occasionally.

Hand out role descriptions to the students. Each one should receive only his or her role description and should not be able to see a role belonging to somebody else.

Some key facts are included in the individual role descriptions, so make sure you read them carefully. Also, read the scenario, which is for your eyes only, to get the overall picture of the initial setting.

11.3.1 Task Role-playing Game

Vulnerability disclosure is perhaps the most controversial aspect of the vulnerability handling process. You should mention, however, that various discussions are underway but that so far no agreement has been reached on standards or processes in this area [8, p.133].

As the moderator or 'game master', you may give additional information (even something you make up on your own, if you want) to one or all the players, stop time, reverse or fast-forward it, etc. Basically, you are omnipotent. Your job is to use these powers to make sure everyone gets his or her pieces of information when the time comes. It is up to you and the students how the story develops. Will the hacker get the money or go to jail? Will Alice finish her project? Give the students as much flexibility as possible; let them make mistakes. Intervene when the story is heading towards a dead end or when you think it is time to introduce new facts or characters. Make sure that everyone plays just his role – avoid situations when someone starts telling others what they might or should do (that is, unless it's the boss telling his employee what to do, of course). The characters can meet face-to-face, make phone calls, send e-mails, etc. However, it must always be clear who exchanges information with whom and what pieces of it. Do not allow anyone to use information he learned only from overhearing other conversations in the play.

Finish the game when the end is obvious or predictable and you do not see any value from further play. Let the students discuss their observations (see 'evaluation') and give your comments. The exercise should take circa 150 minutes (10 minutes preparation and explanation, 120 minutes role-play with a short break, 20 minutes discussion).

Scenario (this is for you only):

Alice is a designer in a marketing company called Ads-R-Us, one of the best in the country, which services large and well-known businesses. She is working remotely on an important

project which is due in a few days. It is Saturday morning and she is trying to access some files on a company server using her VPN software. She can access the server alright, but the files she left there on Friday evening are missing. The administrator on duty will discover that somebody had accessed the server from Alice's account last night and apparently erased the project files of all the users from the file server. Since Alice's account is a regular user account without sufficient privileges to access or modify other user's data, there seems to be big trouble in the offing. Later during the day, the administrator will receive a threatening phone call from a self-proclaimed hacker.

Suggested first contacts:

Alice → Charlie

Kevin → Ernest

Suggested contacts at some point of the game:

Charlie → Ernest

Ernest → Winston

Ernest → Patrick

Ernest → Steve

Roles (copy these pages and hand out, to each student, his or her role description):

ALICE – You are a junior designer at Ads-R-Us, a leading marketing company in the country, servicing large and well-known businesses. You know you do a good job and you are expecting a promotion any day now. If not, there are plenty of opportunities for good graphic designers, just like the one you received in the e-mail yesterday! For the past three weeks you have been working on an outdoor campaign for the biggest national newspaper and the project is due in a few days time. As you are tight on time, you need to work remotely, this time during the weekend. On a Saturday morning you open your laptop and log in to your company's intranet to get the files you left there the previous evening. Hmmm… the folder is empty and so are several others where files from the previous projects should be. The weekend seems to have started off worse than you had imagined.

CHARLIE – You are a network engineer looking after the company network of Ads-R-Us, a leading marketing company in the country, servicing large and well-known businesses. The company provides its employees with the opportunity to work remotely, especially after hours. You even use the cutting-edge operating system facilitating group work called Munix. The company policy is to not to allow any documents to be kept on laptops because of the risk of theft and the potential loss of intellectual property. Instead, secure access is provided to the company's intranet via VPN software, also provided by Munix. As the employees may use the service 24/7, there always has to be someone answering calls about missing passwords, software configuration, etc. The weekend has just started and this time it is you who is looking at another potentially boring day on duty. Oh, by the way, should any security issues arise, you are advised to seek backup from your colleagues on a CERT team which the company decided to keep for some reasons beyond your understanding.

ERNEST - You are an employee of Ads-R-Us, a leading marketing company in the country, servicing large and well-known businesses. Actually, you are one of the network administrators to whom the role of a CERT officer in the company has been delegated as part of your duties. You keep in touch with your ISP and the vendors of your most critical business applications, ie, Munix, the providers of a great OS that facilitates group work and VPN software to access it, and Office Painters, the authors of the designer's software suite.

WINSTON – You are the CEO of Ads-R-Us, a leading marketing company in the country, servicing large and well-known businesses. Since you are quite busy with your own job, you tend to rely on trusted employees to get most of the work done rather then getting yourself too involved. You also value spending days off with your family without being too distracted. And there you go, it is just another Saturday morning, a perfect time to sit back in the garden with your daughter's birthday party scheduled for the evening.

KEVIN – You are a first-grade student and very keen on computer security and software 'pentesting' (penetration testing). Recently, you laid your hands on a popular operating system Munix, used in many companies for project sharing. It did not take too long until you realized that a especially crafted document launched from a user's account can give you administrative rights allowing you to access and modify all of a users' files. You contacted Munix – the vendor – about the flow and asked for a little compensation for your efforts before you would tell them all the details. Maybe you did not sound very convincing, or maybe it was just their policy, but they rejected you. You decided to try out what you had discovered and looked through a list of companies that use the software on the Munix webpage. It started with Ads-R-Us, a leading marketing company in the country, servicing large and well-known businesses. You browsed to their webpage. Now you would just need the credentials of any user that accesses the system. Why not send a fake job offer to a few of those listed in the 'Our team' section? A little key-logging would surely go unnoticed! Once in possession of the content of some apparently classified projects, you decided to go one step further and remove it from the server. It might be that they would be willing to pay to have it back? Hmmm… they even advertise that they have a CERT in their company, so when you call them they should understand the consequences.

STEVE – You are a software developer at Munix, the developer of an operating system of the same name. The Munix is a great product, facilitating group work and remote work from anywhere. You even include a free VPN server and client in the bundle. As a part of your duties, you are responsible for responding to security questions. Not long ago you were contacted by a person claiming to have found a serious bug allowing for privilege escalation. While this sounded important, he did not say very much and asked for quite large sum of money for the details. Since company policy does not permit payment for bug reports, and especially not one as large as two-month's salary for an average employee, you offered him a credit in the security advisory if one were produced as a consequence of his report. He just laughed at you and hung up. Following your procedures, you started the internal process of bug hunting and it turned out that there indeed may be an issue. However, until the root cause of the problem and some fix or workaround was found, you decided not to raise a red flag and not to inform the customers.

PATRICK – You are a full-time CERT officer at one of the biggest ISPs in your country. It is Saturday morning and you are on duty this weekend.

Possible changes:

If you feel comfortable with the exercise, you may consider adding some tweaks to the scenario:

- Time pressure – tell Alice that her quarterly bonus depends on finishing the project on time. She should escalate the pressure on the technicians and CERT officers and consequently they should talk to the software vendor about patches. Or maybe they have ideas for workarounds? And what about the file backups?
- Communication problems – it is weekend, so maybe not all the characters can be reached easily? How does that affect the decisions? Put some of the characters, such as the vendor or the boss, in a different time zone.

11.4 Summary of the exercise

Allow the students to describe how they felt during the exercise. What kinds of problems did they have when they tried to get their job done? Sum up and say that these are the kinds of problems they might have during regular 'incident handling'.

11.5 EVALUATION METRICS

To evaluate the outcome and the performance of the exercise, ask:

- What could have been done better?
- Did they identify the technical problems?
- Did the CERT find out about the Trojan that Alice received?
- Did the commercial company CERT cooperate with the ISP?
- Did they have similar interests?
- How did the CERT get along with the rest of the network department?