12. Exercise: Cooperation with Law Enforcement Agencies (Advising in Cyber Crime Cases)

Main Objective	To explain a CERT's role in advising in a cyber-crime case and the basis for its effective cooperation with an LEA.	
Targeted Audience	Technical and management CERT staff	
Total Duration	4 hours, 25 minutes	
Time Schedule	Introduction to the exercise	10 min.
	Task 1: Identification and reporting a cyber crime	60 min.
	Task 2: CERT advises an incident reporter in a cyber crime case	60 min.
	Task 3: CERT advises an LEA in a cyber crime case	60 min.
	Task 4: CERT prepares training for an LEA	60 min.
	Summary of the exercise	15 min.
Frequency	At least yearly	

12.1 GENERAL DESCRIPTION

In this exercise the students will learn when and how CERT members cooperate with an Law Enforcement Agencies (LEA). In particular, the objectives of the exercise are to:

- practice the identification of cases of cyber-crimes;
- make students aware of differences between the legal systems of various countries and the consequences of these differences;
- explain the legal aspects of CERT work;
- practice writing instructions regarding the reporting of a cyber-crime to an LEA;
- provide information on how to advise a reporter or LEA in a cyber-crime case; and
- develop ideas for training that will be useful for an LEA.

The trainer should have organizational and technical knowledge concerning legal procedures relating to IT crime and abuse, and should be familiar with the most significant differences between the laws of particular countries.

As it is very important for all CERT members to know about cooperation with an LEA, this exercise is aimed at both technical and management staff.

In its basic form the exercise lasts about three hours. As this exercise is designed to develop the skills of incident handlers in communicating with other parties and in exchanging formal, legal information which could have important consequences, it is recommended that this exercise be conducted often – at least yearly.

12.2 EXERCISE COURSE

The course of this exercise is as follows. All discussions should be moderated by the trainer.

12.3 Introduction to the exercise

At the beginning, introduce students to the exercise, providing them with information on how long the exercise is and what its main parts are.

12.3.1 Task 1 Identifying and reporting cyber crimes

Ask the students to read the list of short descriptions of different Internet security incidents including: breaking netiquette rules (based on *Netiquette Guidelines* RFC 1855 [2]) and cyber-crimes (based on [5]). Then ask them:

- Which incidents they consider to be cyber-crimes?
- To try to name identified cyber-crimes (ie, computer intrusion, phishing, etc); and
- Where they would report them?

1.	Reposting a personal message to a mailing group	
2.	Multiple login attempts by an unauthorised user	Password guessing
3.	Discovering the weak points of a computer system by scanning	
4.	Observing and recording network traffic (wiretapping)	Sniffing
5.	Attempting unauthorized remote or local access to someone's computer	
6.	Sending mails with abusive content	
7.	Attempting to use an unknown exploit	
8.	Forwarding or re-posting a message received with word changes	
9.	Selling or installing copies of unlicensed commercial software or other copyright protected materials	Copyright piracy
10.	Attempt to acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication	Phishing
11.	A successful compromise of a system or application by exploiting vulnerabilities	Computer intrusion
12.	Using someone's FTP site to deposit materials which somebody else	

	wants other people to pick up	
13.	Including, or inserting into a system, software intended for a harmful purpose	Malware
14.	Limiting the availability of someone's computer resources by sending lots of packets	DoS attacks
15.	Sending large amounts of unsolicited mails to people	Spam

When students have finished, explain briefly (1) the main differences in the classification of Internet incidents (cyber-crime?) in different countries, and (2) where to report a cybercrime, as follows:

Comment: *Differences in legal systems of different countries*

Explain the main differences between the various classes and types of cyber-crimes. Point out that various Internet-related incidents are considered and treated differently in different countries. For this purpose you can use the *Handbook of Legislative Procedures of Computer and Network Misuse*[15]. If the group of students is multi-national, present some examples of the main differences in the legal systems of the countries they represent. If the students come from the same country, you can focus more on the cyber law of their own country and highlight the differences with the laws of some other countries you choose.

Comment: *Where to report a cyber-crime?*

Explain that while 'breaking netiquette rules' is typically reported to the ISP, Internet-related crime, like any other crime, should be reported to the appropriate law enforcement investigative authorities of the country. Depending on the country and on the source and scope of the crime, it can be reported at local, national or international levels. However, in most European countries, regardless of the source of an Internet-related crime (ie, whether the attack launched from inside or outside the country), it should be reported first to the nearest police unit.

12.4 Task 2 CERT advises an incident reporter in a cyber-crime case

Explain to students the general aspects of the legal framework in which a CERT exists[16] and its role in a cyber-crime case. Basically, when an incident is reported to a CERT and it needs to be reported to an LEA, the main role of the CERT is to:

- help the victim by advising him where and how to report the crime, and
- help and assist the LEAs in the investigation.

[15] *RFC 1855 - Netiquette Guidelines, http://datatracker.ietf.org/doc/rfc1855/*

[16] *Reporting Computer, Internet-Related, or Intellectual Property Crime, http://www.justice.gov/criminal/cybercrime/reporting.html#C4*

After this short explanation, ask students to consider three different types of incidents, as follows:

- A report from a user who states that e-mails with viruses are being received from a particular address. (The reporter suspects that they are being sent on purpose). The reporter requests the CERT's help and provides the details of his mailbox (login and password) to have it checked.
- A report from a server administrator at a University, whose web server (IP given) has become the target of a massive DDoS attack. The number of connections from attacking hosts exceeded 35,000 in the first few days, but on that day, boosted attacks had been occurring four times a day for 2 to 3.5 hours each time, with more than 130,000 connections (as recorded in the firewall logs). The total number of attacking hosts was likely to be more than 1,000. They had already blocked about 450 of the attacking networks. In most cases, the attacks originated from the network in France, Netherlands and Germany.
- A report from a bank which has been informed that there is a website hosted by some other company that is involved in a phishing scheme to obtain personal account information from customers of the bank.

Next, split the students into a few groups and ask them to write separate instructions for the victims of these incidents, including their explanations on how to report the incidents to LEA.

When the groups are ready, a representative of each group presents its instructions. During each presentation the trainer makes notes with his or her comments. After all the presentations have been made, the trainer presents his comments and explains what information was missing from the instructions. In particular, the instructions should explain to the incident reporter:

- how to collect data related to each incident; and
- how to restore the systems involved, ie, what data has to be secured for the purpose of legal investigation and how to do it.

Also the instructions should contain information on what kind of data related to the incident should be provided to the ISP, police or the LEA, such as:

- information about the owner's IP address;
- information about the domain name of the owner (concerning personal data protection issues); and
- information confirming or denying the fact of a network connection (eg, using the netflow data). Some data could also concern old events (eg, events more than 2 years old) – it will provide a chance to address data retention aspects of the case.

Optionally, present a kind of template instruction. (It can either be presented on the blackboard or displayed). The template instruction should include a description of the kind of information about a cyber-crime that should be included and an explanation about how to properly secure traces of evidence. If any LEA templates (in 'fill-in' form) are available, the trainer can present these as well.

This task could end with a short explanation on how an LEA investigates cyber-crime cases, how long it takes to start the proceedings, how long can investigation take, etc. The trainer can talk about some successful or unsuccessful past cases.

12.5 Task 3 CERT advises LEA in a cyber-crime case

Then ask the students to imagine how an effective cooperation with an LEA would take place.

Ask the students what kind of aspects should be addressed in an effective cooperation with an LEA. These would include:

- educational activities (the CERT trains the LEA);
- cooperation on the basis of the realization of the outsourced expertise's of cyber-crime; and
- consultations when the CERT receives a request from the LEA regarding a suspected cyber-crime.

Ask the students to think about what advice a CERT could give when it receives a call from an LEA regarding a case of suspected cyber-crime. (Provide a few examples of cybercrimes.)

For example, what would the students do in the case of:

  - a denial of service attack,
  - phishing, or
  - cyber defamation?

- What kind of information should the LEA provide them with?
- How could they identify the source of the crime?
- What could they advise the LEA?

The students should ask about the IP addresses (source and destination, static or dynamic), data and time of crime (with time zones), e-mail addresses, and service ports (source, destination).

For more information see also RFC 3227[17]

[17] *RFC 3227 - Guidelines for Evidence Collection and Archiving, http://www.faqs.org/rfcs/rfc3227.html*

12.6 Task 4 CERT prepares training for LEA

Ask the students to think about proposals for CERT training for an LEA. This training should contain advice about:

- What data should be contained in an official letter from an LEA to a CERT to help obtain requested information:
  - obligatory information
  - optional information

  for individual incidents?
- How long is data concerning IP addresses assignments stored?
- What kind of information should the LEA forward to internet service providers?
- What additional data could be useful (for example, translations of addresses)?
- What data should internet service providers provide for the LEA?
- How to identify the owner of an IP address?
- How to identify the owner of a domain?
- How to identify the owner of an e-mail address?

Below are some examples of questions from an LEA.

- LEA asks you to establish the owner of an e-mail address.
- LEA sends yo2u a letter without the return address.
- LEA asks questions without authorisation or the appropriate signature.
- LEA asks for the list of log entries that could help to identify users connecting to the Internet using computer of IP address xxxx.
- LEA asks to identify the user that was assigned IP address xxxxx in a specific period of time a few years ago.
- LEA asks for log entries containing a list of all connections established on a particular day.

Students should think about proposals for CERT training an LEA to reduce the number of such questions.

12.7 Summary of the exercise

Now it is the time for the exercise summary. Encourage students to exchange their opinions, ask questions, and give their feedback about the exercise.

12.8 EVALUATION METRICS

Evaluating the results of this exercise, the trainer should take into consideration the following aspects:

- Did the students properly recognize cyber-crimes?
- Are the instructions about how to collect data related to an incident clear and concrete enough?
- Are the instructions about how to report an incident to an LEA clear?
- Are students able to collect the proper data about IP addresses and domain owners?

12.9 REFERENCES

1. Handbook of Legislative Procedures of Computer and Network Misuse
2. http://ec.europa.eu/information_society/eeurope/2005/doc/all_about/csirt_handbook_v1.pdf
3. RFC 1855 - Netiquette Guidelines, http://datatracker.ietf.org/doc/rfc1855/
4. Reporting Computer, Internet-Related, or Intellectual Property Crime, http://www.justice.gov/criminal/cybercrime/reporting.html#C4
5. CERT Handbook, csirt_handbook_v1.pdf [page 7]
6. Incident classification developed within eCSIRT.net project,
7. http://www.ecsirt.net/cec/service/documents/wp4-pub-userguide-v10.html#HEAD7
8. RFC 3227 - Guidelines for Evidence Collection and Archiving, http://www.faqs.org/rfcs/rfc3227.html