5. Exercise: Vulnerability Handling

Main Objective	To provide a practical overview of the vulnerability handling process and how vulnerabilities reported to a CERT team should be handled. Also, to provide some hands-on experience with difficult situations that may arise through the role of coordinator.	
Targeted Audience	Managers and incident handlers	
Total Duration	3 hours, 10 minutes [optionally 4 hours, 10 minutes]	
Time Schedule	Introduction to the exercise	20 min.
	Task 1: Responsibilities of a CERT team in a vulnerability	30 min.
	Task 2: Vulnerability disclosure – advantages and disadvantages	30 min.
	Task 3: Designing a vulnerability disclosure policy	45 min.
	Task 4: Introducing CERT coordination in a vulnerability	45 min.
	Task 5: Identification of vulnerability handling phases	[30
	Task 6: Coordination of single and multiple vendor cases [optional]	[30 min.]
	Summary of the exercise	20 min.
Frequency	It is recommended that this exercise be performed when a CERT team is being set up and when there is a significant personnel change within a CERT team. As not many CERTs have a full vulnerability handling service, it should be performed each time a team decides to introduce this service or recognizes that it is treated by its constituency as a provider of this service.	

5.1 GENERAL DESCRIPTION

The objective of the exercise is to provide a practical overview of the vulnerability handling process and how vulnerabilities reported to a CERT team should be handled. Students will learn:

- Who the key players are, and the main phases of the vulnerability handling process;
- The main responsibilities of a CERT team involved in a vulnerability case;
- How to design a vulnerability disclosure policy suitable for their CERT; and
- How to deal with difficult situations that may arise through their role as a coordinator.

This exercise, in particular, will focus on giving some starting points (also for reading and discussion) to be prepared for handling unexpected and challenging problems that may arise when a vulnerability is reported to a CERT team. It is also intended to highlight the issues to be considered by a CERT in communicating and in resolving vulnerability cases.

In practice, vulnerability handling requires technical knowledge of vulnerabilities and some incident handling experience, as well as familiarity with social engineering techniques, high-level communication practices and risk management skills.

5.2 EXERCISE COURSE

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

5.3 Introduction to the exercise

At the beginning, introduce the students to the exercise, providing them with information on how long the exercise will take and what its main parts are. During this part, provide the students with some general information about the vulnerability handling process as described below.

Generally, the vulnerability handling process includes:

- analysis of a reported vulnerability (ie, technical verification of a suspected vulnerability and identification of the means for exploiting it);
- vulnerability repairing (ie, installing patches to limit or prevent the exploitation); and
- response coordination (ie, developing a vulnerability disclosure strategy)[2].

A *vulnerability case* that involves CERT in the coordinating role, assumes two parties, such as an external non-affiliated evaluator who discovers a novel software failure and a software vendor responsible for the product concerned[3].

[2] *CERT services.* http://www.cert.org/CERTs/services.html

[3] *Laakso M, Takanen A, Röning J,* The Vulnerability Process: a tiger team approach to resolving vulnerability cases*, in*

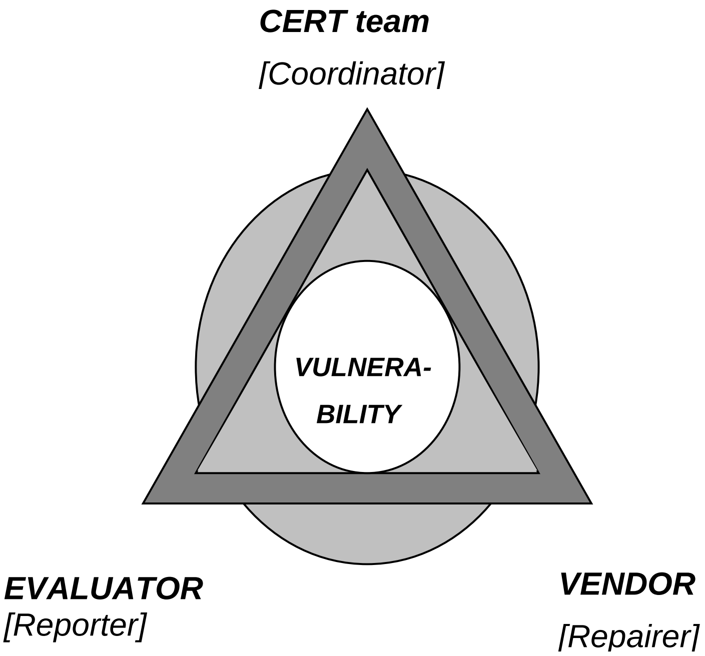

Figure 1: Three main actors and their roles in the vulnerability process

For these three main actors (see Fig 1), the vulnerability process assumes the following roles:

- **Evaluator** (*reporting* role), who reports the vulnerability discovered to a vendor or a CERT team;
- **Vendor** (*repairing* role), who is responsible for fixing the vulnerability (eg, by a patch); and
- **CERT team** (*coordinating* role), which establishes and maintains the communication link between the reporter and the repairer. The CERT team's role is to advise on how to resolve a vulnerability case.

5.3.1 Task 1 Discussion: Responsibilities of a CERT team in a vulnerability case

At the beginning, sketch a typical vulnerability case as follows:

After vulnerability is reported to a CERT team, the evaluator is asked to provide details about the identified vulnerability. Once this has been received, the CERT team asks the vendor to provide information about how their products are affected by the vulnerability reported. The vendor is then responsible for assessing the impact and severity of the vulnerability (ie, who could be affected and how) and for preparing a patch. He can also quantify the costs and benefits of vulnerability disclosure. After the patch is ready, both an evaluator and a CERT team can evaluate the final fix.

Next, ask students to identify a CERT's main responsibilities and activities in a vulnerability case, keeping in mind that a CERT team acts as an independent coordination centre. In particular ask them:

- (a) What responsibilities do they have as coordinator towards the vendor?
- (b) What responsibilities do they have towards the vulnerability reporter?

Moderate the discussion, record the students' ideas on the whiteboard, and (if needed) complete the list provided by the students with the following information regarding the CERT's activities and responsibilities:

- Providing efficient communication between all involved parties (also using the CERT's existing security contacts);
- Providing vulnerability verification;
- Evaluating the vulnerability assessment impact provided by the vendor;
- Independent identification of the scope of a vulnerability;
- Analysing the interests of all parties involved;
- Considering the advantages and disadvantages of disclosure;
- Determining when to disclose the vulnerability;
- Evaluating the final vulnerability fix; and
- Developing an appropriate strategy for disclosure.

5.3.2 Task 2 Discussion: Vulnerability disclosure – advantages and disadvantages

Vulnerability disclosure is perhaps the most controversial aspect of the vulnerability handling process. You should mention that various discussions are underway, but so far there is no agreement upon standards or processes in this area [8, page 133]. Also, there is no standard policy on how to deal with vulnerability once it has been found, eg, should it be kept a secret or be publicly disclosed? Therefore, before making any decisions, it is necessary to consider different aspects of disclosing information about a vulnerability, such as:

- Why, who, or what information should be disclosed?
- When or where should the vulnerability be disclosed?
- What factors influence the timing of disclosure?

You should stress here that there is a real dispute regarding *whether* and *why* a vulnerability should be disclosed [4]and ask students to think why this is so. Ask students to think about any

[4] *Laakso M, Takanen A, Röning J,* Introducing constructive vulnerability disclosures*, in proceedings of the 13th FIRST Conference on Computer Security Incident Handling. Toulouse*

pros and cons of full disclosure of a vulnerability and to write down their ideas in their work book.

- Advantages: Some advocate that disclosure stimulates vendors to fix vulnerabilities. Some also believe that the release of the details of a vulnerability motivates other vendors to make more tests of their software and make it more secure. Furthermore, some claim that there is only a small chance (about 8%) that the same vulnerability will be identified independently by malicious hackers and 'white hat' hackers.
- Disadvantages: Others think that disclosure significantly increases the risk of exploitation, with all the consequences that could involve, eg, the loss of millions of visitors (eg, the DoS attack on Yahoo's site in 2000). The problem also concerns the quality of the patch - particularly if developed under severe time pressure - which can be insufficient to prevent the exploitation. But even the best patch protects only customers who keep their software up to date and less security-conscious users will still at risk of being attacked by malicious hackers.

5.3.3 Task 3 Designing a vulnerability disclosure policy

Begin with a general discussion about vulnerability disclosure policies. Ask the students

- What does 'responsible vulnerability disclosure' mean to them?

Next, split the students in a few groups and ask them to develop a general vulnerability disclosure policy they believe proper for their CERT. When the groups are ready, everybody should discuss what should be the main parts of a vulnerability handling policy. Issues addressed in their policies should include (a) and (b).

Give an example of so-called grace periods (ie, the amount of time given to the affected vendor to develop a security update before the details are published) which are different for different CERTs. When CERT/CC, for example, is notified about a potential vulnerability, it contacts the software vendor and gives it a 45-day period to develop a patch[5]. After that time, that CERT makes the information public. However, the goal of CERT/CC policy is 'to balance the need of the public to be informed of security vulnerabilities with the vendors' need for time to respond effectively. The final determination of a publication schedule is always based on the best interests of the community overall'.

Stress that, as each vulnerability case is unique, it may require a quite different management policy. Also, since there are various actors and interests in the vulnerability process, there are therefore also different viewpoints regarding the disclosure of the vulnerability.

Next, present some real examples of vulnerability handling and disclosure policies. Details of the viewpoints regarding each of the roles in the vulnerability process can be found in[6]

[5] *CERT-CC* The CERT Coordination Center Vulnerability Disclosure Policy http://www.cert.org/kb/vul_disclosure.html

[6] *Rain Forest Puppy* Full Disclosure Policy (RFPolicy) v2.0

(RFPolicy – reporter's perspective), (CISCO policy - vendor's perspective)[7] and (CERT/CC policy – coordinator perspective), which are also discussed in references. Discuss with the students the aspects of these policies they find acceptable or unacceptable for their constituency. It is important to present the vulnerability handling process from different points of view. This will give the students information about the complexity of the process as well as allow them to understand controversial issues relating to this process.

Emphasize that developing a vulnerability disclosure policy, and handling and management strategies are tricky tasks that require careful analysis based on real-case scenarios, best practice policies, privacy laws, and vendors' policies.

5.3.4 Task 4 Role-playing game: Introducing CERT coordination in a vulnerability case

During the role-playing game students firstly receive a case-study, a story about vulnerability handling related by you or described in a brief by you and read by students. Then the initial scenario of a game is presented.

You should pay attention to the following rules during the role-playing game. (You should also get the students familiar with them.)

- A game leader is the trainer.
- A game leader has an absolute power to shape, modify and adjust a game scenario, eg:
  - can stop an action and introduce new factors and new conditions;
  - can rewind an action to change factors or conditions or actions already performed; and
  - can accelerate an action to avoid valueless activities.
- All students must fit their actions to what the trainer has decided.
- Students can communicate during a role-playing game only as players, not as students. (For example, they are not allowed to comment on an action unless the trainer changes it.)
- A main purpose for the trainer is to achieve the goals of the exercises.

Now you tell the story about how vulnerability should not be handled. (You can name it 'One Day at Black Hat'.) You can also give the students the story in a written form.

'Lynn was initially represented at the conference by noted cyber law attorney Jennifer Granick. The lawsuit filed by Cisco and ISS was settled with a permanent injunction against both Lynn and Black Hat preventing further disclosure of information on the exploit.' [9]

Now you start a game. It has obligatory and optional players:

[7] *CISCO* CISCO Security Vulnerability Policy
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Obligatory players are:

- the hacker,
- the large ISP, and
- CERT (two possibilities: CERT inside ISP, CERT outside ISP).

Optional players are (when there is too many students for one obligatory group, but too few for two):

- vendor of vulnerable hardware,
- law enforcement, and
- ‘vulnerability auction’ company - like WabiSabiLabi [10].

Try to fit the roles to the students. 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 it should be scheduled towards the end of the course. This way the students will be able to become more familiar with each other and with the trainer.

5.3.5 Game scenario:

The hacker reports a very serious remote administration vulnerability in a hardware device of a large ISP to a CERT and wants money and credit on the ISP's webpage for providing the details. The vulnerability is easily exploitable and renders hardware useless without hard/hand reboot. Initial direct contact between the hacker and the ISP has failed – the ISP feels threatened and is willing to prosecute the hacker.

You explain the task:

The ISP's main goals are to prevent any disclosure and to get the details of the vulnerability. If the CERT is located inside the ISP, care should be taken to show how difficult internal company relations can be –CERT v PR, network engineers v management, and so on. Students should be split into small groups. It is recommended that each player is represented by one student. The goal is to resolve the incident in a manner satisfactory to all. The trainer is responsible for moderating the discussion.

Initiate the game. Involve all students in it as soon as possible; then let them improvise. They should contact each other – the best option in a role-playing game is to stage phone calls – and discuss a topic and move the case towards a solution.

It is important that they use only the information dedicated for each role. ‘Phone tapping’ is forbidden.

5.3.6 Task 5 Identification of vulnerability handling phases [optional, if needed or there is a special interest from the students]

During this post role-playing activity, students given the task of identifying as many activities and processes as possible. This is achieved through a brain-storming session with the trainer as a group leader. Afterwards, the whole group is divided into three parts and each of them must assess how important the particular processes are for the group. A factor which makes groups different is that they represent, during the assessment, the different vulnerability handling players: vendors, vulnerability researcher (evaluator) and a CERT team. This should produce different results and make students aware how differently the vulnerability handling process looks like from different perspectives and interests.

5.3.7 Task 6 Coordination of a single and multiple vendor case [optional, if needed or there is a special interest from the students]

Ask the students to think about aspects that differ in various real cases of vulnerability.

The possible variants of vulnerability cases can differ both in terms of the number of actors and the roles of each actor, as well as the different kinds of sources of a vulnerability report; it may be a white-hat hacker, a malicious hacker, a security professional, or an internal group in a company. There can also be multiple vendors or subcontractors involved in a single case. If more than one vendor is affected, who releases an advisory? Should an advisory be internal or public? Each activity taken should be accompanied by a careful risk management plan and should be documented at each stage of the vulnerability process.

Now, focus on one aspect, ie, a vulnerability case that involves multiple vendors. Ask the students to think about possible complications, both general and those from the point of view of a CERT team acting as a coordinator.

When students are ready with their ideas, mention that over 60% of software vulnerabilities affect customers of multiple vendors. Multiple vendors add complexity to the original model concerning a monopolist vendor in two ways: (1) first, competition among vendors may lead to a competitive effort in shortening the patching time. This may or may not be a good thing. (2) Second, the earliest disclosure may be set by either CERT or one of the vendors. This may mean that the disclosure policy of the CERT might become somewhat irrelevant.

5.4 Summary of the exercise

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

It should be taken into account that communication in a vulnerability case may concern different actors with potentially conflicting roles. For example, the goal of an *evaluator* could be getting some benefits or credits from a vendor in return for providing details of a failure discovered. The goal of a *vendor* will be to minimize the cost of disclosure. In any case, CERT should aim at balancing the interests of the parties in determining when to publicly disclose.

CERT teams have already proved to be invaluable for tackling complicated vulnerability processes, thanks to the effective identification of multi-vendor cases and the building of test laboratories, as well as the reduction of communication overheads [4]. And, although different cases may require different response solutions, the CERT goals should be always the same: (1) focus on repairing a vulnerability as fast as possible to prevent a situation which could escalate to a crisis, (2) responsible disclosure that mitigates the vulnerability, and (3) a strategy that optimally satisfies the interest of all involved parties.

Individual vulnerability cases may however require different response strategies. Appropriate strategies should be developed, based on knowledge of cases already resolved and existing best practices [2]. Direct students to resources they may find interesting or which could provide them with more details about the vulnerability handling process.

5.5 EVALUATION METRICS

To evaluate the outcome and performance of the exercise, the trainer answers the following questions:

- Did the students identify the most important responsibilities of a CERT team in a vulnerability case?
- Did the students recognize the most important advantages and disadvantages of vulnerability disclosure?
- Did the students fail to address any obvious issues in their vulnerability policy?
- If any aspect of a real vulnerability policy was found unacceptable by a student, was there good reasoning behind it?
- How engaged were all sides in the role-playing scenario?
- Did the students identify the most problematic issues in the coordination of a multiple vendor case?

5.6 REFERENCES

1. CERT services. http://www.cert.org/CERTs/services.html (2008)
2. Shepherd S A, *Vulnerability Disclosure: How Do We Define Responsible Disclosure*? SANS, GIAC SEC Practical (2003)
3. https://www2.sans.org/reading_room/whitepapers/threats/932.php
4. Laakso M, Takanen A, Röning J, *The Vulnerability Process: a tiger team approach to resolving vulnerability cases*, in proceedings of the 11th FIRST Conference on Computer Security Incident Handling and Response. Brisbane (1999)
5. Rain Forest Puppy *Full Disclosure Policy (RFPolicy) v2.0*
6. http://www.wiretrip.net/p/libwhisker.html (2008)
7. CISCO *CISCO Security Vulnerability Policy* http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

8. CERT-CC *The CERT Coordination Center Vulnerability Disclosure Policy* http://www.cert.org/kb/vul_disclosure.html (2008)
9. Laakso M, Takanen A, Röning J, *Introducing constructive vulnerability disclosures*, in proceedings of the 13th FIRST Conference on Computer Security Incident Handling. Toulouse (2001)
10. Killcrece G, Kossakowski K P, Ruefle R, Zajicek M, *State of the Practice of Computer Security Incident Response Teams* (CERTs), *Technical Report* CMU/SEI-2003-TR-001 (2003)
11. Micheal Lynn case story. http://en.wikipedia.org/wiki/Michael_Lynn
12. WabiSabiLabi, http://www.wslabi.com/

Further reading:

Vulnerability disclosure policies:

– Descriptive list of publications regarding different incident response steps and processes can be found in [8] (Appendix B, pages 149-153)

Ethical issues: paying for vulnerability discovery or not?

– *Offering a bounty for security bugs*, available at http://news.cnet.com/Offering-a-bounty-for-security-bugs/2100-7350_3-5802411.html

– Zero Day Initiative, http://www.zerodayinitiative.com/advisories/disclosure_policy/

– *Bug Finders: should they be paid?* available at http://www.wired.com/science/discoveries/news/2002/08/54450?currentPage=2

– Microsoft approach, available at http://blogs.zdnet.com/security/?p=130