1. Exercise: Triage and Basic Incident Handling

Main Objective	This exercise provides students with experience of real-life incident reports, their ambiguity and complexity. After finishing the exercise they should understand what to focus on during initial analysis, how different factors may affect priorities and how to communicate with reporters as well as third parties. During the exercise, they will apply a given classification scheme to incidents – the purpose of this part of the exercise is to work on the consistent classification of disputable cases (eg, worm v scanning) across team members and possibly to suggest a clearer, more unambiguous classification scheme for the team.	
Targeted Audience	The exercise is aimed at incident handlers at any level of experience. It requires a good understanding of Internet topology and services.	
Total Duration	2 hours, 25 minutes	
Time Schedule	Introduction to the exercise	10 min.
	Task 1-9: Incident report analysis, classification and prioritization	60 min.
	Discussion	60 min.
	Exercise summary and wrap-up	15 min.
Frequency	Once a year for new team members or members reassigned to incident response. This exercise can be used with real reports as an intra-team exercise for all incident handlers in a CERT. In this case, the goal is to make sure there is a consistency between the classification and prioritization of reports by different team members.	

1.1 GENERAL DESCRIPTION

The exercise simulates the initial phases of incident handling with 10 real-life incident reports. These phases include:

- verification of the report (did the incident actually occur?);
- interpretation (what actually happened?);
- determination of the scope of incident (what are the actual and possible consequences for your constituency and others?);

- classification; and
- prioritization (based on the previous factors).

The students will try to complete these phases for each of the reports. Discrepancies between their results will then be discussed.

Before conducting the exercise, read through all the reports and key answers. If students come from an already established team or teams, ask them to provide the classification scheme they use in everyday work. You may decide to use those schemes rather than the ones suggested in the exercises, but it is important that all students use the same scheme as it provides common ground for a discussion. You may also consider using real-life examples from your own experience instead of some of the cases provided in the student's book. The guidelines on anonymising data for the purposes of this exercise are as follows:

- 10/8 are networks located in Utopia
- 10.187/16 are networks of Utopia NREN
- .ut is Utopia's top-level domain

They were consequently used in the reports included on the Virtual Image.

1.2 EXERCISE COURSE

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

1.2.1 Introduction to the exercise

Divide students in small groups (2-3 people). Ask them to open the Thunderbird mail client contained on the Virtual Image. There are nine incident reports in the Inbox. The toolset contains guidelines for the students as well as the proposed classification scheme[1]:

[1] *This classification was developed during the eCSIRT.net project on CERT cooperation and common statistics. More information can be found at http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6*

Incident Class (mandatory input field)	**Incident Type** (optional but desired input field)	**Description / Examples**
Abusive Content	Spam	'Unsolicited bulk e-mail', which means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having an identical content.
	Harassment	Discrediting, or discrimination against, somebody (ie, cyberstalking)
	Child/Sexual/Violence/...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kinds of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...).
	Sniffing	Observing and recording network traffic (wiretapping).
	Social Engineering	Gathering information from a human being in a non-technical way (eg, lies, tricks, bribes, or threats).

Intrusion Attempts	Exploiting known Vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as a CVE name (eg, buffer overflow, backdoors, cross side scripting, etc).
	Login Attempts	Multiple login attempts (Guessing or cracking passwords, brute force).
	New Attack Signature	An attempt using an unknown exploit.
Intrusions	Privileged Account Compromise	A successful compromise of a system or application (service). This could have been caused remotely by a known or a new vulnerability, but also by an unauthorized local access.
	Unprivileged Account Compromise	
	Application Compromise	
Availability	DoS	In this kind of an attack, a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYS-a, PING-flooding or E-mail bombing (DDoS: TFN, Trinity, etc). However, availability can also be affected by local actions (eg, destruction, disruption of power supply, etc).
	DDoS	
	Sabotage	
Information Security	Unauthorised access to information	Besides the local abuse of data and systems, information security can be endangered by a successful account or application compromise. Furthermore, attacks that intercept and access information during transmission (wiretapping, spoofing or hijacking) are possible.
	Unauthorised modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes, including profit-making ventures (eg, the use of email to

		participate in illegal chain letters for profit or pyramid schemes).
	Copyright	Selling or installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
Other	All incidents which don't fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indication that the classification scheme needs to be revised.

Ask the students to analyse the reports, to describe the situation and the possible ways in which it may be mitigated, and to apply the classification scheme and prioritize incidents, giving them 'priority ranks' of 1, 2 or 3, with 1 as the top priority.

Allow 60-75 minutes for resolution. During that time, make sure you are available to answer any questions which may arise. Do not give hints and clues yourself – answer fully and correctly only when asked.

1.3 Keys to the exercise

1.3.1 Task 1 UKSUtopia Inspections

This may seem like a regular spam report. On closer analysis it turns out that apparently somebody at *control@ministry.gov.ut* sent a message to a mailing list informing co-workers about some scheduled maintenance. One of the addresses bounced and the bounce message was reported as spam. Clearly, this is a misunderstanding and the report is void.

1.3.2 Task 2 Abuse: 10.187.137.4

The report speaks about a DDoS attack in which a host from the constituency of Utopia CERT takes part. The first thing to do should be to determine whether the address was spoofed or if we are dealing with a real problem in our network. Since the logs come from a web server and show full HTTP requests, TCP connection must have been established and communication was bi-directional. In such a case, IP spoofing would require the hackers to hijack BGP prefixes of the network which is probably too much effort when botnets are readily available. In any case the suggested follow-up is to check flows and the state of the machine in question.

1.3.3 Task 3 [SpamCop (http://www.company.ut/) id:3091085703]3-4 June-Workshops for Managers

This is a regular spam complaint forwarded via the SpamCop service. The complaint reaches Utopia CERT because the website advertised in the e-mail is within your constituency. Possible follow-up depends on legal situation of spam in a given country. In some cases, even when the sending of bulk commercial e-mails is prohibited by law, each message must be individually reported by its recipient to appropriate authorities which effectively makes the law unenforceable. In such cases the role of the CERT is minimal and is limited to advising users and possibly registering the report for statistical purposes.

1.3.4 Task 4 [CERTPT #56817] Unauthorized access attempt registered

This is a report from another CERT, containing logs of unauthorized login attempts. Within the proposed classification scheme it may be suggested that these kinds of brute-force attempts, which fit logically as 'login attempts', may be signs of worm activity. This is okay if you are confident that this is typical worm behaviour (eg, known wide-spread infections with similar patterns having occurred recently) and the same classification is used consistently within the team.

Note that the logs do not concern Utopia CERT directly. Instead, the hosts listed are from a different provider in Utopia, so the Utopia CERT will play the role as coordinator. Moreover, *.internetdsl.* in hostnames suggests dynamic addressing so it would be vital to provide the ISP with full logs along with timestamps. Lack of the address of the attacked host could be a problem if the timestamps are not synchronized and also in the case of NAT. Note that all timestamps are in GMT, so time-zone offset must be taken into account.

1.3.5 Task 5 Incident 10.187.21.203

This is a report from an automated monitoring and reporting system which notifies you about scanning activity from one of the hosts in your constituency. Notice that the scans are concentrated around well known ports used by worms (TCP 135, 137, 139 and 445). This may not necessarily indicate worm activity (possibly multiple infections at the same time), so again arguments can be raised for both the 'scanning' and 'worm' classification of the activity.

1.3.6 Task 6 [SpamCop (http://www.bigoil.ut/cgi-bin/internet.exe/portal/ep/home.do?tabId=0) id:3120641650]----BIGOIL CO. Search (Immediate Part-Time JOB for …

At first sight this looks just like another spam report related to a 'spamvertised' (advertised by Spam messages) website of a company located in Utopia. In reality this is a financial scam similar to Nigerian scams, where the name, brand and a website of an existing and reputable company are abused in a fictional story of some shady business. Suggested classification is 'fraud', because 'social engineering' relates more to reconnaissance and gathering information useful for further attack.

1.3.7 Task 7 Incident 10.187.108.39

Another report from an automated system. This time, along with scanning patterns, some descriptions of IDS signatures are provided. The same kind of attack across multiple hosts in a subnet makes it likely to be related to the activity of a worm such as MSBlaster of lovSan (these worms were targeting port 135 tcp).

1.3.8 Task 8 Bank Phish Site [211889] - Please Reply ((NOTE - THIS SITE(s) HAS BEEN UP SINCE 3/07. WE HAVE SENT 4 NOTICES TO SHUT IT DOWN - PLEASE DO SO))

A phishing case where the site is apparently using fast-flux technology to make it harder to shut it down. Several copies are reported to exist in Utopia and the Utopia CERT is asked for assistance in taking them down. If possible, the appropriate ISPs should be asked to retain any evidence of malicious activities such as connection logs from the machines. However, this can be problematic where home-user machines are parts of a botnet. Additional actions might include re-examining the domain from time to time as new IPs may pop up on the list of zombies hosting the website in question.

1.3.9 Task 9 [MBL# 89603] Malware Block List Alert

A malicious file is hosted somewhere under the .ut domain. The report does not indicate if the host itself is also located in Utopia, so the first step would be to resolve the domain name. There are a few scenarios to try with such incidents. If the website where the malware was injected (3q.ut in this case) seems legitimate itself, you should try contacting the company which owns it and inform them of the problems. Many companies will do enough to fix the problem just for the sake of saving their reputation. Another path to try would be the hosting company, as in many cases the website's owners outsource website administration and will need to contact the administrators anyway. If the feeling is that the malware is hosted intentionally (or at least knowingly), the best thing to do is to contact the ISP straightaway, possibly bringing the police into the loop.

1.4 Discussion

When the time is due, ask one person from each team to state clearly:

- their view of the situation;
- how would they proceed, whom would they contact;
- what type of incident they are dealing with (using the proposed classification scheme); and
- what priority would they assign to the incident and why.

At this time, do not comment the results. Write them all down on a whiteboard for everyone to see.

When you have collected all the answers, discuss each case, focusing on those which received various grades of priority or different classification from different groups. Sometimes the very

same report is ranked as very important by one group and given a very low priority by others. This is okay as long as the groups can provide justifications for their rankings. Be open to arguments and describe cases from your own experience where applicable.

1.5 Summary of the exercise

Some points to use for wrap-up and conclusions in the summary:

- None of the existing classification schemes are perfect. Creating a classification scheme specifically for a given team can make the choices more obvious initially, but it will have to be updated from time to time. On the other hand, using one classification scheme over a longer period of time and sharing it with other teams would allow for the comparison of statistics.
- When an incident type is ambiguous, it is not the name of the class that matters. More important is how you describe this class in your statistics. And the most important thing is consistency, so make sure that all incident handlers classify similar incidents in the same way. Regular meetings and *ad hoc* discussions should help resolve any discrepancies.
- Priority is not a function of just one variable – the incident type. Some groups might have classified a report in the same way, but give them different priorities based on additional knowledge or assumptions such as 'it is a widespread worm'. In real life, it is vital to know these factors and collect any necessary information to avoid confusion.

1.6 EVALUATION METRICS

As stated above, there are no single 'correct' answers in this exercise. Some cases can be more disputable than others. Following the key provided above and the suggested answers below, make sure that the students have not missed some important spots that may not be obvious in the first place and have correctly identified the nature of the problem. It is also vital that, when justifying the priorities applied to the reports, students take into account not just the type of incident but also its scope and relevance to the constituency.

The table below contains suggested classification and prioritization for the exercise:

Task	Classification	Priority	Comments
1	None	N/A	This is not an incident
2	DDoS	1	If the attack is not ongoing, the priority may be lowered.
3	Spam	3	
4	Login attempts	2	
5	Scanning	2	Worm, if worm activity is high or other evidence is available.
6	Fraud	3	
7	Worm	2	
8	Masquerade	1	Active phishing and malware distribution sites should be treated with higher than usual priority.
9	Malicious Code	1	See above. It may be suggested that the classification scheme should be expanded to include drive-by-download infections and other malware distribution mechanisms.