Triage and Basic Incident Handling

Toolset, Document for students

September 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Copyright Notice

Table of Contents

1 What Will You Learn

This exercise will give you some practice in triage – the initial incident handling phase, covering:

- 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).

After finishing the exercise you 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.

2 Exercise Task

You are an incident response investigator working for Utopia CERT. This team is part of a research and academic network in Utopia – a decent ISP serving universities and high schools. As the oldest and most recognized IRT in Utopia, your team is quite often approached about all security incidents happening in your country. You maintain good relationships with other providers and have secure and effective ways of sharing information with them.

You start your work at 8 am with 9 reports in your mailbox. Read through them and try to understand what really happened and what are the reporters' expectations. How are you going to handle them? Whom will you contact and what information will you share? For each report, assign ONE type from your classification scheme and give a priority of high, medium or low, determining the order in which you would handle the incidents. Make sure you are ready to explain your decisions and keep in mind that you are the decision-maker here – there is no single correct answer.

Unless instructed otherwise by the trainer, launch the Icedove mail client from the Virtual Image. You will find the incident reports in the Inbox.

The reports are taken from real life. They were anonymized according to the following rules:

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

The classification scheme used in Utopia CERT[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)	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	

	DDoS Sabotage	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).
Information Security	Unauthorised access to information Unauthorised modification of 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.
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.

Complete the table below to assign an appropriate classification and priority to each of the reports. The priority should be a number between 1 and 3:

1 – top priority

2 – normal priority

3 – low priority

	Report Subject	Classification	Priority	Suggested Actions
1	(from: UKSUtopia Inspections)			
2	Abuse: 10.187.137.4			
3	[SpamCop (http://www.company.ut/) id:3091085703] 3-4 June -Workshops for Managers			
4	[CERTPT #56817] Unauthorized access attempt registered			
5	Incident 10.187.21.203			
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 …			
7	Incident 10.187.108.39			
8	Bank Phish Site [211889] - Please Reply …			
9	[MBL# 89603] Malware Block List Alert			

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu