Large Scale 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

The purpose of this exercise is to introduce you to the way large-scale incidents can be handled. You will face different scenarios, presented by the trainer. For each scenario, follow carefully what the trainer has to say. The trainer will explain a certain initial situation and you will be asked to suggest ways of moving forward. To help you, the trainer will pose leading questions. Answering the questions will move you to the next phase of the scenario, until you arrive at the final solution.

2 Exercise Task

2.1 PART 1 LARGE-SCALE PHISHING ATTACK

This exercise is meant to be carried out with the help of the trainer. At the beginning, you will be given a short overview of what phishing is. The trainer will then present a scenario to you. The scenario will be resolved through a series of steps (tasks).

2.1.1 Task 1 Source of information

What are your possible sources for obtaining information about phishing incidents?

2.1.2 Task 2 Initial investigation

What would be your first steps in tackling a reported phishing incident?

2.1.3 Task 3 Take down

How would you organize the takedown of the phishing site? What are the possible obstacles?

2.1.4 Task 4 Warning & Mitigation

How would you organize the takedown of the phishing site? What are the possible obstacles?

2.2 PART 2 LARGE BOTNET SPREADING THROUGH A NEW VULNERABILITY

You have gained some experience on how to handle large-scale phishing attacks. Now you are faced with a large botnet which is blasting through your network using some new vulnerability you have never heard of. The trainer will introduce some more details to you. As in the previous example, you should resolve the incident through the tasks listed below. The trainer will be there to help you, answering your questions so that you may proceed to the next task. Try to enumerate as many possible variants as you can think of.

2.2.1 Task 1 Source of information

What are your possible sources for obtaining information about new botnets and vulnerabilities? What services could you use to monitor networks and acquire information about network events?

2.2.2 Task 2 Initial investigation

What would be your first steps in tackling such a situation?

2.2.3 Task 3 Take down

How would you organize the takedown of a controller? What are the possible obstacles?

2.2.4 Task 4 Warning & Mitigation

How would you go about warning victims? What steps could be taken, other than organizing a takedown, to mitigate the problem?

2.3 PART 3 INTERNAL WORM OUTBREAK

9.5 This scenario deals with a different case than the two previous scenarios. Those involved handling incidents external to a CERT. But what if an attack is happening in a network of a corporate CERT?

In this scenario, the trainer will:

- present you with a hypothetical scenario of a worm entering a corporate network;
- present a diagram (below) of a hypothetical organization's network;
- give general information about the initial situation; and
- guide you in a step-by-step manner, by providing leading questions to help you understand what is happening and how to resolve the situation.

The network topology looks like the following:

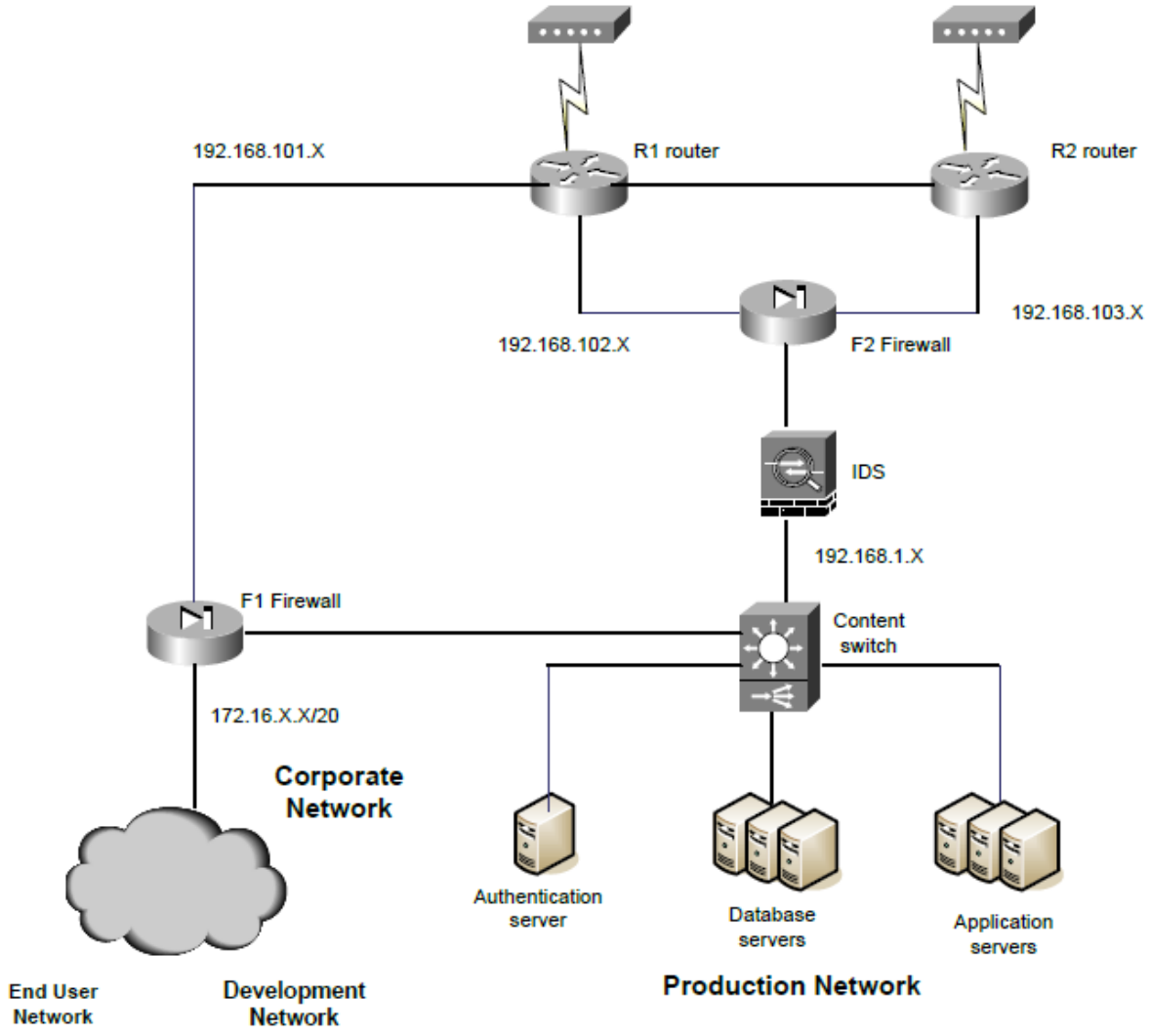

Figure 1: Network map

Perform the following tasks, enumerating all the possible variants of the problem you can think of. How would you resolve the situation? Again, the trainer will provide you with leading questions.

2.3.1 Task 1 Possible source of attack

Where could the attack have come from?

2.3.2 Task 2 Type of attack

How does the worm spread?

2.3.3 Task 3 Malware capture and analysis

How could you capture and analyze the worm?

2.3.4 Task 4 Worm controller identification

How could you determine if this worm has a controller and adds infected hosts to a botnet?

2.4 PART 4 LARGE SCALE DDoS ATTACKS AGAINST THE ENTIRE COUNTRY

This part of the exercise is devoted particularly to developing your skills and ideas on handling large-scale country-wide DDoS attacks. You will learn how to prepare the attack defence strategy, undertake appropriate actions and overcome various types of difficulties at different levels, both technical and organizational.

2.4.1 Task 1 Case study: hypothetical cyber attack against country X

You will receive a case study which describes some hypothetical cyber attack against country X. Your task is to prepare the defence strategy for this cyber attack. Think about the consequences of the situations described and the potential difficulties a CERT could face. Explain the motivation for the actions you propose. You have 45 minutes to complete this task. Be prepared to present your ideas to the whole group. Use the following form to prepare your strategy.

Your ideas for Phase I

……
……
……
……
……
……
……
……

Your ideas for Phase II

……
……
……
……
……
……
……
……
……
……

Your ideas for Phase III

……
……
……
……
……
……
……

Present and discuss your ideas with the others.

2.4.2 Task 2 Another perspective: your country is under cyber attack

Imagine a similar attack occurs against your country or happens to your constituency. What would be your actions? Develop a basic defence procedure for your CSIRT team.

Defence procedure (*You are your CERT)*

……
……
……
……
……
……
……
……
……

2.4.3 Task 3 Analysis of a particular DDoS method

You will receive a description of some DDoS attack. Your task will be to give ideas about the types of analytical methods and actions which can be used to defend against it.

2.4.4 Task 4 Lesson learnt

Think about how to be better prepared to defend future large-scale attacks? Consider issues connected to prevention, preparedness and sustainability.

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