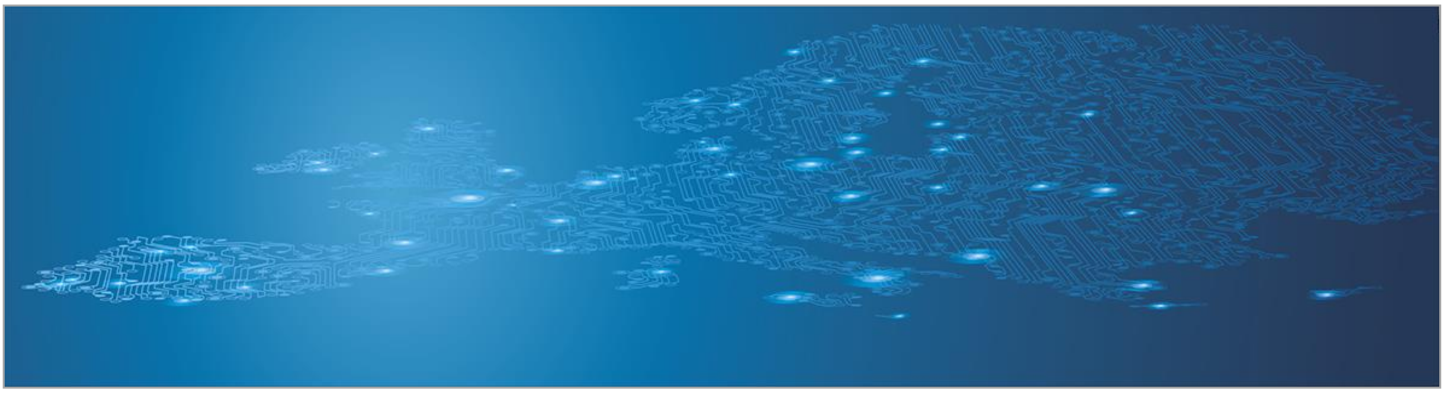

Large Scale Incident Handling

Handbook, Document for teachers

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

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Table of Contents

1 Introduction

Goal

The main objective of the exercise is to teach incident handlers the key information and actions required for the successful resolution of large-scale incidents.

Target audience

Technical CERT staff.

Course Duration

Roughly 5 hours

Frequency

The exercise should be carried out when the team is first setup or whenever new team members arrive or a new type of threat appears. (In the last case you should expand the exercise to accommodate this threat.)

Structure of this document

	Task	Duration
	Introduction to the exercise	15 min
	PART 1 LARGE SCALE PHISHING ATTACK	
	Task 1: Source of information	10 min
	Task 2: Initial investigation	10 min
	Task 3: Takedown	10 min
	Task 4: Warning & mitigation	10 min
	PART 2 LARGE BOTNET SPREADING THROUGH A NEW VULNERABILITY	
	Task 1: Source of information	10 min
	Task 2: Initial investigation	10 min
	Task3: Takedown	10 min
	Task 4: Warning & mitigation	10 min
	PART 3 INTERNAL WORM OUTBREAK	
	Task 1: Internal worm outbreak	10 min
	Task 2: Type of attack	10 min
	Task 3: Malware capture & analysis	10 min
	Task 4: Worm/botnet controller identification	10 min

	PART 4 LARGE SCALE DDoS ATTACK AGAINST AN ENTIRE COUNTRY	
	Task 1: Case study: hypothetical cyber attack against country X	60 min
	Task 2: Another perspective: your country is under cyber-attack	30 min
	Task 3: Analysis of a particular DDoS method	30 min
	Task 4: Lessons learned	15 min
	Summary of the exercise	15 min

2 General Description

The purpose of the exercise is to introduce incident handlers to the complexity of handling large-scale incidents. After completion of this exercise, the students should be able to:

- Understand the nature and the consequences of a common large-scale incident;
- Determine the key information required for the successful resolution of such incidents; and
- Coordinate the exchange of information with various authorities.

This exercise does not require Internet access. It is recommended that you, the trainer, carefully read through the handbook to understand what is required from you. The exercise is split into four different parts, concerning different types of large-scale incidents. The exercises listed here are intended as examples, so you are welcome to create additional examples of your own. Similarly, any solutions presented are not intended to be complete – you and the students are encouraged to present solutions of your own. The form of the exercise is a moderated discussion, led by the trainer.

3 EXERCISE COURSE

The course of this exercise is as follows:

3.1 Introduction to the exercise

At the beginning, introduce the students to the exercise, outlining its main parts and how the exercise will be carried out. This exercise consists of four main parts:

- PART 1: Large scale phishing attack;
- PART 2: Large botnet spreading through a new vulnerability;
- PART 3: Internal worm outbreak; and
- PART 4: Large scale DDoS attack against an entire country.

3.2 Keys to the exercise

3.2.1 PART 1 LARGE SCALE PHISHING ATTACK

This exercise is meant to be carried out with the help of a trainer. As the trainer, your role is to present a step-by-step description of a potential phishing attack. At the beginning, you are expected to give a short overview of what phishing is.

The form of the exercise is somewhat similar to role-playing. You are expected to give a short introduction to the particular incident, asking the students what they should do next to move forward with the incident handling process. Once the students 'solve' a certain phase, they should be introduced to the next phase of the incident handling process and the problems encountered there. If students have problems answering certain questions, you should provide leading questions that help them solve the problem. To help you, some example answers are also provided. Remember that other variants are possible – feel free to lead the investigation in the manner you see fit.

3.2.1.1 Task 1 Source of information

Step 1 is the reporting of the incident. Ask the students, how they could become aware of the attack. Various possible ways are listed below. Did the students cover these variants? Did they suggest other ones? What should be the result of this step?

Variant 1.1

The CERT team starts receiving reports about a phishing campaign from its constituency. These reports contain full phishing e-mail with headers and body including URL to phishing site.

Variant 1.2

The CERT team find a phishing attempt by themselves – for example through spam traps or some of the team members received phishing e-mails in their mailboxes. The e-mails have URLs embedded in them, which point to a phishing site.

Variant 1.3

A phishing URL was reported by a bank, whose customers are being targeted.

Results (for all three variants are the same):

The CERT team has obtained a URL or URLs pointing to phishing site(s).

3.2.1.2 Task 2 Initial investigation

Next step is to find out a) if this is not a false alert, b) where the phishing sites are located, and c) how the attack is carried out. The answers may overlap, so all are included in one step. Questions that can help students find out what is going on:

1. Are the phishing sites still active or alive? How to check this? (Answer: the simplest way is to get there by the most popular browsers: IE, Firefox, Opera, and Chrome. It is recommended that these sites be checked with wget. Remember to be careful; the sites could be malicious, so using a specially prepared machine for this action would be advisable.)

2.1 Leading questions: Are they active in all popular browsers or just in a particular one? What about wget? Maybe the phishing site requires a specific ‘user agent’ field set or another (for example ‘referer’)?

3. Where are the phishing sites (logically and physically) located? How to find out?

3.1 Leading questions: What is the domain and IP address of the www server? To whom does the IP and domain name belong? Who is the host-master? Who is the ISP? (Answer: look at the URL. Is there an IP address or domain name? Use tools like dig, host, etc. Next – when you get an IP – use the whois database and traceroute tool. Look at the main page of this domain: after ‘http://’ and before the next slash ‘/’.)

4. How is the attack being carried out? What technique is used to serve the phishing site? How to check this?

4.1 Leading questions: Is the fast-flux technique used? Does every IP returned from the dns query lead to a response? Are there other sites on this server (IP)? What about the main page from the phishing URL? (Answer: the results of dig or host could be helpful in determining fast-flux. In the context of other sites: go to the main page of the phishing URL, for example: if the phishing URL is www.somesite.com/some/directories/thebank/login.html, go to the www.somesite.com URL and analyse it.)

Result:

There could be numerous answers to the above questions. A couple of them are listed below. Did the students cover these or suggest something new?

Variant 2.1

The URL is www.somesite.com/some/directories/thebank/login.html. On the www.somesite.com there is a web page that is typical of some small business. There is a strong possibility that the administrator or webmaster of this site does not know about this situation. In most cases this server was compromised by a miscreant. There are three sub-variants of this scenario:

Variant 2.1a

The compromised server is in your network (for example you are the CERT team of a large ISP or hosting centre). The owner of the site – potentially one of the victims – is your customer.

Variant 2.1b

The compromised server belongs to some large ISP in your country. The victims are not your customers.

Variant 2.1c

The compromised server is located in another country.

Variant 2.2

The domain name resolves to many and various IPs. There is a strong possibility of fast-flux. The IPs belong to different ISPs, perhaps in a different country. There is no 'main page' on the 'server'.

Digression: Why are there so many IPs and why do some of them do not respond? Why do the miscreants use fast-flux?

(Answer: these IPs are probably zombies from some botnet. They are probably desktop-computers infected by special malware. Some of them are simply switched off.)

3.2.1.3 Task 3 Take down

The next step is to organize the takedown of this site as soon as possible. It is recommended that an attempt be made to try to track down the miscreants and victims of the phishing. Questions for the students:

1. How to take down the phishing site in variants 2.1.a to c? What is the fastest way to communicate with the administrator of the site? From which source can you get contact information? (Answer: in variant 2.1a there is no problem – you should contact your administrator. In 2.1b you should search 'contact with admin' on the main page or about page. You could also check the whois database. The fastest way for contacting is by telephone. Many times it is better to send details via e-mail and call to inform that there was a phishing and details were sent via e-mail. Maybe there is an abuse-team or CERT team operating at the ISP? In variant 2.1c you must take language and time differences into account. In this case it is recommended that another CERT team from that country be involved – you could look one up on the FIRST site, www.first.org.)

2. Is the deletion of the phishing site by the administrator of a compromised site enough?

- Leading question: What about the vulnerability that was exploited to compromise the server and upload the phishing site? (Answer: in variant 2.1a you must, together with your administrators, find and patch this vulnerability. In variants b and c you must explain this possibility – with hints – to the server administrator, perhaps offering help.)

3. Where could you search for information about the break-in to the server and the vulnerability?

- Leading question: If there could be a vulnerability in the www server or in the PHP scripts or in the database, etc, where can you find information about suspicious requests, form entries, errors, etc? (Answer: inadequate server logs, etc.)

4. How to track down the miscreants? Where can you find some information about them? Where are the drop sites of the miscreants? (Answer: you must analyse the source code of the phishing site, as there may be information about where stolen data is sent. Other scripts on the compromised server, as well as server and e-mail logs could be helpful.)

5. Where to find information about victims?

6. What to do with this information?

7. Are these steps enough? What about cases, when we were unable to take the site down?

8. Should law enforcement become involved?

9. How to take down the phishing site in variant 2.2?

3.2.1.4 Task 4 Warning & Mitigation

It is strongly recommended that potential victims be warned.

1. Does the bank know about the phishing? (Answer: phishing should be reported to the bank)

2. Should you write an alert on your webpage? Who should first know about this: the bank or the people reading your site?

3. How to alert people who have visited phishing site(s)?

- Leading questions: Most popular browsers can warn people – how do you get them to do this? In which external services can you report phishing URL(s)? (Answer: phishing sites should be reported to Google Safe Browsing (used by Firefox, www.google.com/safebrowsing/report_badware/), Netcraft (http://toolbar.netcraft.com/report_url), PhishTank (www.phishtank.com), Microsoft PhishingFilter (https://phishingfilter.microsoft.com/faq.aspx). Where else? Students could propose their own.)

3.2.2 PART 2 LARGE BOTNET SPREADING THROUGH A NEW VULNERABILITY

Once the first exercise has been completed, the students should be presented with another scenario. Again, the trainer should serve as a mentor of the exercise but this time allow students more flexibility. Scenario outline and leading questions are proposed below. The trainer should be prepared to explain concepts such as honeypots, sandboxes, BGP and DNS blackholing.

The second exercise involves a botnet that spreads through a new vulnerability in a Windows service, available on port 42/TCP.

3.2.2.1 Task 1 Source of information

The CERT team starts to receive reports about a series of new hacking incidents from its constituency. The first question that can be asked is how the team can get more information about what is going on:

- What (open) discussion lists could supply some supporting information?
- What public websites could provide extensive information?
- What kind of detection systems could the team operate to get more information by itself?

3.2.2.2 Task 2 Initial investigation

Once the students identify some sources, point out useful ones they have missed. After this, you should provide some supporting information, such as:

- observed controllers.

Once the controller is identified:

- How can the team identify which sources in their constituency are infected? (hint: netflow)
- In what way could the team obtain a malware sample to verify or discover new controllers? If the students miss this, introduce the idea of honeypots and sandboxes.

3.2.2.3 Task 3 Takedown

This task concerns the takedown of the controller.

- How could the controller be taken down? What happens if it is in your constituency, or in another ISP in your country, or abroad in the USA, or in China?
- What research could be carried out to determine the botnet owner?
- How could law enforcement become involved?

It turns out that the controller is fast flux.

- How could that have been determined?
- What implication does it have for containment and takedown?

3.2.2.4 Task 4 Warning & Mitigation

A list of infected IPs related to the constituency is obtained. In the case of a national CERT:

- How could the identified IPs be assigned to specific ISPs?
- How could contact addresses for CERT or abuse teams of these ISPs be obtained?

Once these infected hosts are assigned and the administrators or abuse teams notified:

- How the threat could be contained, especially if taking it down turns out to be impossible? Explain BGP and DNS blackholing to the students.

3.2.3 PART 3 Internal worm outbreak

This part of the exercise deals with a different case than the two previous parts. 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, you should:

- present the students with a hypothetical scenario of a worm entering a corporate network;
- present a diagram of a hypothetical organization’s network;

- give general information about the initial situation; and
- guide the students in a step-by-step manner by providing leading questions to make them understand what is happening and how to resolve the situation.

What follows is an example scenario for the exercise. Note that this is a hypothetical scenario, loosely based on facts.

3.2.3.1 Introduction to the scenario

The incident that we are going to analyse happens in a hypothetical company called 'Innovative Software'. Figure 1 depicts the diagram of the network.

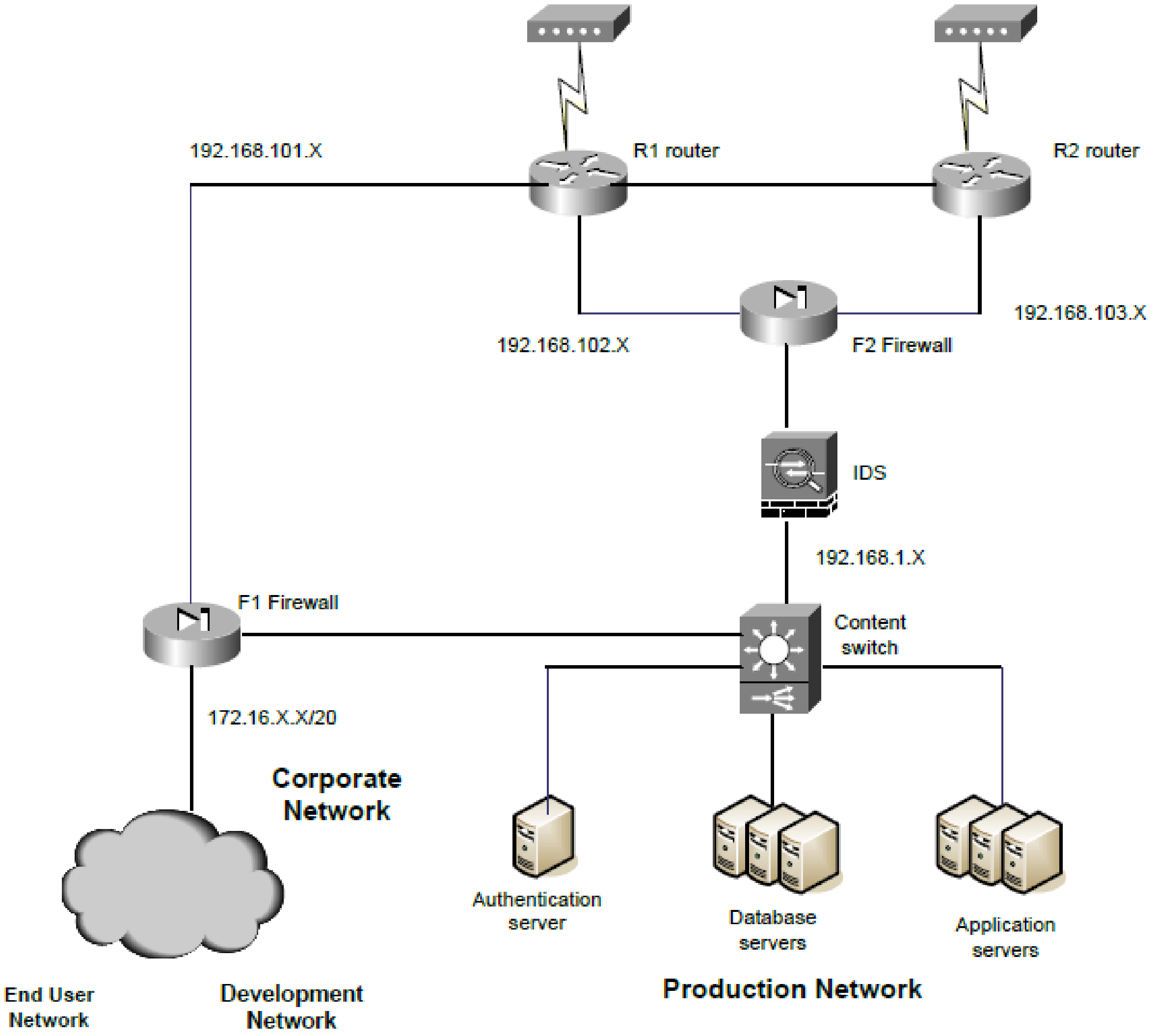

Figure 1: Network map

Conduct a general introduction and explain the above network diagram.

Innovative Software has two redundant Internet connections from two independent ISPs. When the network is operating normally, only the connection through router R1 is used. Router R2 is used only in case of problems with the first connection. There are two main networks in the company: Production Network and Corporate Network.

Production Network is supposed to be available externally - for clients using Innovative Software services. Aside from application and database servers there are also authentication servers that allow authentication with advanced credentials using TACACS+ and RADIUS protocols. Corporate Network is divided into two sub-networks - End User Network and Development Network. The distinction is that users from the End User Network cannot reach the Production Network through firewall F1. Development Network is used by the R&D department. The access control lists on both routers and firewalls are configured in a deny-base setup. This means that only necessary traffic is allowed. The access for customers is strictly a web interface so only HTTP traffic is allowed to Production Network through F2 firewall.

We will not analyse the access list thoroughly - entry by entry, as this is not important for the exercise. Moreover, when dealing with the attack performed on a large scale, security specialists often do not know the details of network configuration immediately and have no time to become familiar with it. Therefore being able to estimate possible security flaws based only on general knowledge of the network structure is very important.

Innovative Software has experienced performance problems recently. Investigation of logs on machines in the Production Network revealed that the problem came from sluggish MS-SQL servers that play a critical role in the entire service. Administrators checked to see if there were any recent updates or configuration changes. Nothing appeared to be suspicious so they tried the desperate step of rebooting. At first it looked as if that solved the problems so the administrators sequentially rebooted all of the servers. Unfortunately, it only took minutes for the servers to slow down again to an unacceptable rate of processed requests. Administrators suspected that the network configuration was causing delays. However, running a few pings, traceroutes and DNS lookups at various points on the network did not reveal any problems.

At this point administrators brought up the possibility of compromise. Security engineers from the local CERT team were contacted.

3.2.3.2 Task 1 Possible source of the attack

At this step, ask the students to speculate on the possible source of the attack. Encourage them to ask questions, provide them with answers and guide them through, asking leading questions if necessary.

The Innovative Software network seems to be secured enough. The external firewalls appear to be configured properly, and they do filter traffic to MS-SQL ports.

Task: Estimate where the attack could come from?

Solution: The only users that can reach the Production Network are the developers working in the R&D department. Do they use MS-SQL servers in the Development Network? (Yes) Do they have any access to the Internet beside the two firewalled connections? (No) Can R&D employers take their laptops home and bring them back infected with viruses? (Yes)

3.2.3.3 Task 2 Type of attack

As it becomes clearer that users from the Development Network could be the source of compromise, further investigation is needed to see if this really is the case.

Task: If a virus came from the development network, as we suspect, then how can you find out more information about the attack, especially the kind of threat you face? Why does the IDS not signal anything?

Answer: The first thing that could be done is to check the logs on all the network nodes that could ‘see’ anything interesting. Logs of neither firewall F1 nor router R1 contain any useful information. Interesting entries, however, can be found on firewall F2 – a huge amount of denied outbound UDP connections to port 1434 to hosts that appear to be random. This is a clear indication that some type of exploit had compromised the SQL servers. Does the IDS have updated signatures?

It is very important at this point to stop the worm from spreading in the network. We know that firewall F2 stops the traffic, but the original source of attack can still be active and the worm is probably propagating through firewall F1. The following deny statements could be added to the firewall F1 outbound interface (from the 192.168.101 network):

deny tcp any eq 1434 any any log

deny tcp any eq 1434 any any log

That way you stop the network from propagating the worm and the host that caused infection can be localized through firewall logs.

Next, we should investigate the vulnerability and, especially, try to find out from the controller if the compromised systems are part of a botnet.

3.2.3.4 Task 3 Malware capture & analysis

Task: Investigate the hosts to which the exploit is trying to connect and try to gain some information from the data that the exploit sends.

Solution: We may want to separate the exploited server from the production network. To catch the traffic that the exploit sends, it is necessary to set up an environment for the worm to propagate. Such an environment could be a honeypot or sandbox system.

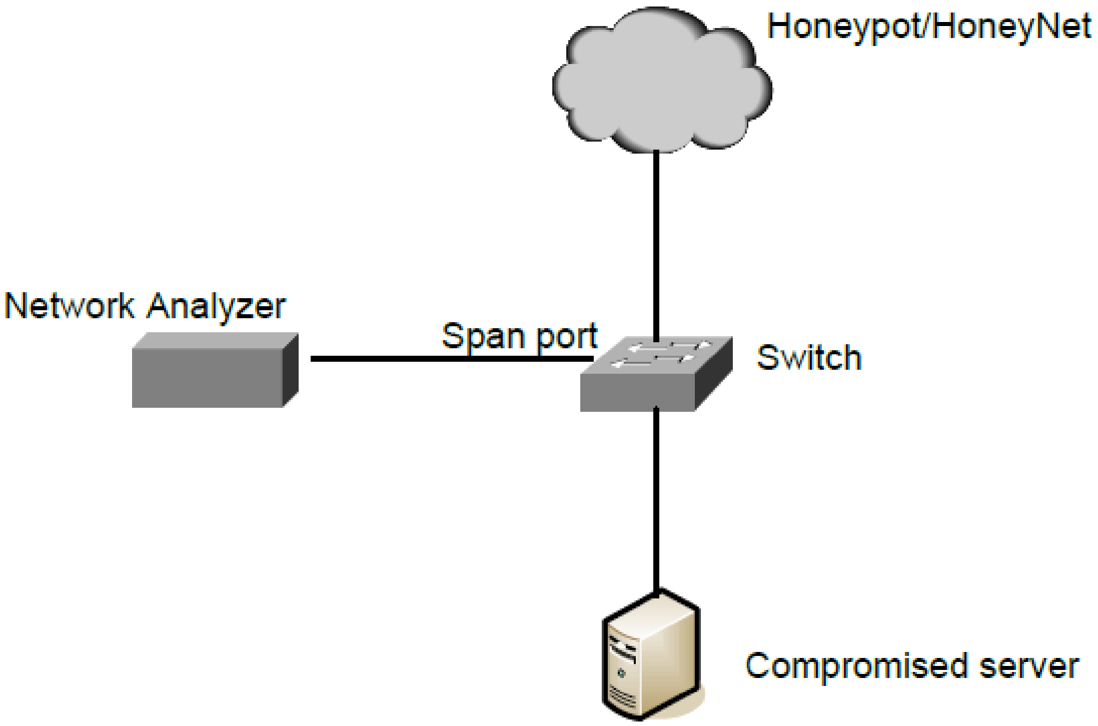

Figure 2: Network map

The network analyser is connected to the switch SPAN port. (Traffic from all other ports is forwarded to the SPAN port.) Due to the network analyser on the SPAN port, all the communications from and to the compromised SQL server can be observed.

You would need a honeypot that emulates the vulnerability used by the worm to obtain a copy and to understand the infection process. What honeypots do the students know about? What is the difference between a honeypot and a sandbox?

If the students are not familiar with the concept of honeypots and sandboxes, you should introduce these to them.

3.2.3.5 Task 4 Worm/botnet controller identification

Task: To find out with whom the malware communicates and to try to identify other nodes on the malware network.

Solution: First of all, you should investigate the range of the IP addresses that are attacked. Do they belong to any particular sub-network or does it look like they are chosen at random? All requests to the DNS server should also be reported. The technique that could be used to catch the URL requests and forward them to a specific IP address is called DNS blackholing. (In this solution the DNS server replies with a preconfigured IP address on specified URLs instead of resolving it.) There is a chance that the worm is actually a botnet and has the address of its controller as a URL rather than an IP address. First of all, IP addresses to which the worm tries to connect often should be considered suspicious. We know that the vulnerable service works on port 1434, so connections to other ports may imply communication with the controller. If no suspicious IP addresses can be found this way, the payload of connections can be analysed. Communication with the controller is different than packets containing exploit payload. So, theoretically, it should be possible to differentiate attack vectors from any other communication. As you have the list of IP addresses, you should check who they belong to. Usually the data you get from whois points to an ISP. In such a case, your role is to notify the ISP of the incident.

We are considering the case of the Innovative Software company network, so the last phase is to secure the network. First of all patches from the vendor should be applied (Microsoft in this case). The second problem is that the network is not secured properly. It should not be possible for the users to connect their laptops (potentially compromised) to the network and have unrestricted access to the production network. There are remedies for this, but they are another large topic which is beyond the scope of this exercise.

3.2.4 PART 4 LARGE SCALE DDoS ATTACKS AGAINST AN ENTIRE COUNTRY

This part of the exercise is devoted particularly to developing skills and ideas on handling DDoS attacks. The exercise should start with a short reminder of examples of cyber attacks against Estonia in 2007, Georgia in 2008, and many recent global politically-motivated DDoS attacks. Before the exercise, students can get familiar with, eg, the report [1] prepared by Georgian CERT-GE about the cyber attack against Georgian network infrastructure in 2008, its effects and the actions used to mitigate it.

During the exercise, students will learn how to:

- develop a defence strategy for the large-scale attacks (particularly DDoS attacks);
- prepare for cyber warfare in the future (procedures, tools, contact lists); and
- recognize and overcome various types of difficulties.

3.2.4.1 Task 1 Case study: hypothetical cyber-attack against country X

Present a hypothetical large-scale cyber-attack that happens to some country X, described below. The attack progress (conflict, attack synopsis) could be presented on a whiteboard as a timeline of the main events. Additionally, give each student a copy of a detailed description of the attack.

This case study describes a hypothetical cyber-attack against country X: Country X is a medium size country with a quite advanced network infrastructure designed to allow consumers, businesses and government to use high bandwidth wire and mobile Internet connectivity. Country X has a substantial (10%) ethnic minority from country Y. Country X has two CERT teams: one ISP CERT and the GOV CERT. In the CERT of the ISP (which is the largest Internet provider in country X) there are some people of nationality Y. The national CERT, the GOV CERT, is a newly established team (three months ago). Country X has no cyber security policy yet. For a couple of years, country X and country Y have been candidates for the Famous International Organization (FIO). One day, country X becomes a member of FIO, while country Y does not. Just after this momentous event, the authorities of country X start to increase discrimination against the minority from country Y. The names of streets (in districts where most of minority Y lives) are replaced with the names in the official language of country X. Shops and schools of country Y are forced to close. Moreover, speaking the language of country Y in offices, shops, and in the streets is forbidden. Subtitles in language Y are eliminated from all TV programs. These government actions are an immediate reason for the start of the conflict. Within a few days, there are a lot of protests by people of nationality Y against these decisions (protest marches, etc.). Almost simultaneously, the conflict in cyberspace begins. Cyber conflict (Phase I) During the first week, there are the following incidents: - The government of country X receives millions of e-mails of protest from all over world, so government mail servers go down. - There are a few cases of defacement attacks targeted again websites of the majority government. - There are some DDoS attacks against government web servers, so they go off-line. - Offensive texts in the language of country X are put on some popular country X websites. - Some content on news portals of country X is replaced with new content in the language of country Y. Cyber conflict (Phase II) The following week, after some relatively simple incidents, cyber attacks increase. There are many sophisticated and well coordinated attacks. Many of them use large international botnets (a few thousand compromised machines) controlled by five virtual domain name servers (from abroad). DDoS attacks are launched against the critical national information infrastructure of country X: - Many government sites are overwhelmed by a series of DDoS attacks. - The computer systems of the largest TV station are attacked and remain unavailable. - The five biggest banks become unreachable and most banking transactions are paralysed. - The police network infrastructure is under constant attack. - Information services, news portals and press agencies are under heavy DDoS attacks. - On-line shops stop offering electronic services. - Besides the attacks of botnets, detailed instructions (in many languages) on how to launch attacks and the tools to carry out these attacks, together with 'a list of objectives', circulate on the Internet and are readily available, so even persons not familiar with hacker techniques take part in attacks. - The ISP is overwhelmed, so Internet access is limited. Cyber conflict (Phase III) After two weeks, the attacks continue. There is the beginning of complete information chaos and on-line communication is limited. Most of the important websites and networks (government, information services, police, banks, etc) remain unavailable. GOV CERT comes under heavy DDoS attack.

After sketching the attack synopsis, split the students into three groups. The task of each group is to develop the defence strategy for country X. The appropriate actions should be proposed for each phase separately.

In particular, the students should prepare and state their opinion about:

- Is it possible to mitigate (if yes – how?) the particular attacks described in the synopsis?
- What kind of measurements would you use for particular attacks?
- What kind of response actions could be taken?
- What kind of difficulties would you expect to face (regarding attacks, specific procedures)?

The students should consider the consequences of situations described (eg, disabled on-line news sources), explaining the reasons for the actions proposed, and the potential difficulties (lack of tools, no possibility of control, etc). Students have up to 45 minutes for completing this task.

When all groups are ready, the representative of each group presents its strategy to the whole exercise group.

The whole presentation should end up with your conclusion about the ideas proposed and a moderated discussion. You should indicate the points missed in the proposed strategies, note the mistakes, and evaluate whether the ideas presented are feasible and appropriate, referring to the cyber law of the country represented by the participants. During the discussion, you can ask the group to address more aspects (both operational and technical).

1. What priorities would you assign to the proposed actions in mitigation?

2. Who do you think should be a coordinator of mitigating actions in country X?

3. What kind of support can be offered or are you able to offer (as a representative of a CERT team), to country X? How would you organize the support?

4. What kind of problems, which are different or more serious than those that took place in Estonia or Georgia, can you image? How would you handle them?

5. What difficulties can occur during the recovery process?

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

Ask participants to imagine that a similar attack occurs in their own country or happens to their constituency. What would be their actions? Ask them to develop the basic defence procedure for their CERT team, considering issues that include the following:

1. Who and how would you notify about the problems or actions?

2. What should you do when there is a lack of necessary information about the situation inside the country or abroad?

3. How and what type of information about the situation would you report to the media?

4. How would you organize effective communication? How would you propagate the necessary information quickly?

5. On the other hand, what are your ideas for dealing with information (notifications) overload and communications overload?

3.2.4.3 Task 3 Analysis of a particular DDoS method

Ask participants to consider some specific DDoS attacks.

1. How would they analyse the attack method used and determine the source of the attacks?

2. What would be their actions to defend against these attacks?

3. What type of control would work best against distributed coordinated attacks?

3.2.4.4 Task 4 Lessons learned

At the end, discuss with participants ‘the lessons learned’ regarding the following aspects:

 What should a national and international response to large scale attacks be?

 How can we be better prepared to defend ourselves future large-scale attacks?

Consider issues related to prevention, preparedness and sustainability (eg, checking the national infrastructures for DDoS weaknesses; for CERT: taking actions by scanning all networks for which it is responsible, etc). List the most important aspects, such as government support (national strategy), crisis management plan, early warning systems, national coordination, involvement of international CERTs, communication plans, arrangements for close cooperation and cooperation between strategic partners, and regular exercises[1].

4 Summary of the exercise

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

5 EVALUATION METRICS

It is suggested that at the end of the exercise, students take a test quiz that is available on the Virtual Image. The results of this quiz could be part of the evaluation process.

Furthermore, in evaluating the results of this exercise, you should take into consideration the following aspects:

PART 1

- How many variants of each step and solutions did the students enumerate by themselves?
- Did the students propose something different than what is outlined in the handbook?

PART 2

- Were students able to repeat the steps from Part 1?
- Did they understand the concept of fast-flux networks introduced in Part 1?

PART 3

- How many variants of each step and the solutions did the students enumerate by themselves?

PART 4

- Did the students consider the need for a national coordinator in responding to the attacks?
- Did they consider the involvement and specific roles of various entities (ISP, FIRST, TF-CERT, LEA, NATO) including the notification of systems administrators, filing cases against unknown attackers with the police, etc?
- Were the proposed measurements for specific attacks appropriate (statistics, botnet infiltration, command tracking, flow data, news monitoring, keywords triggers, eg, ‘gov’ in commands)? Did they consider the problem that some things can be invisible from inside the country?

[1] *EU Workshop on Learning from large scale attacks on the Internet - Policy Implications. Brussels, January 2008. Presentations and a workshop report available at :http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/index_en.html*

- Did they propose appropriate or feasible defence actions (filtering traffic, localization and shutting down virtual DNSs, localization of compromised machines, research, investigations, collaboration)? Did they consider implementing BCP38[2]?

References

1. Russian Invasion of Georgia. Russian Cyberwar on Georgia. Report of the Government of Georgia. Available at: http://georgiaupdate.gov.ge/doc/10006744/CYBERWAR-%20fd_2_new.pdf (October, 2008)

2. EU Workshop on Learning from large scale attacks on the Internet - Policy Implications. Brussels, January 2008. Presentations and a workshop report available at :http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/index_en.htm

3. BCP38, Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Available at http://www.faqs.org/rfcs/bcp/bcp38.html.

Additional materials:

The official document of the Estonian Ministry of Defence about Estonian Cyber Security Strategy (prepared in the context of the cyber attack on Estonia) is available at http://www.mod.gov.ee/?op=body&id=518.

[2] *BCP38, Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Available at http://www.faqs.org/rfcs/bcp/bcp38.html.*

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