



# CERT participation in incident handling related to the Article 13a obligations

Handbook, Document for teachers

September 2014



\*\*\*\* \* enisa

European Union Agency for Network and Information Security



# 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 <u>www.enisa.europa.eu</u>.

# 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**

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.



# **Table of Contents**

1	Introduction	1
2	General Description	1
3	EXERCISE COURSE	2
3.1	Introduction to the exercise	2
3.2	Task 1: Building a technical environment for analysing network monitoring data	4
3.3	Task 2: Analysing of network monitoring data	5
3.4	Task 3: Evaluating countermeasures values	14
4	Summary of the exercise	16



# **1** Introduction

#### Goal

This exercise provides students with information about rules, procedures and best practice in handling incident related to obligation for internet service providers described in the Article 13a of the European Telecom Package.<sup>1</sup>

#### **Target audience**

Incident handlers and CERT managers responsible for incident handling procedures within an organisation

#### **Course Duration**

3 hours

#### Frequency

Once for each new CERT member

## Structure of this document

Task	Duration
Introduction to the exercise	10 min
<i>Task 1:</i> Building technical environment for analysing network monitoring data	30 min
Task 2: Analysing of network monitoring data	90 min
<i>Task 3:</i> Preparing report according to the Article 13a template report	30 min

# 2 General Description

The purpose of this exercise is to prepare participants to be ready to analyse a set of data related to a DDoS attack. The proposed type of attack is similar to those that should be reported to the Regulatory Authority according to the rules and obligations for internet service providers (ISPs) described in Article 13a of the European Telecom Package. In this particular example, the attack is against an important online service provided by ISP and used by ISP customers for e-services. The service for customers is not available due to on-going DDoS attack. Additionally due to the DDoS attack, the network service is temporarily unavailable.

<sup>&</sup>lt;sup>1</sup> Directive 2009/140/ec of the European Parliament and of the Council (dealing with electronic communications) - <u>http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF</u>



During the exercise participants will learn:

- how to analyse network traffic data related to the attack;
- what kind of information can be obtained from network traffic data;
- how to prepare the report that should be used for reporting security incidents according to Article 13a.

# **3** EXERCISE COURSE

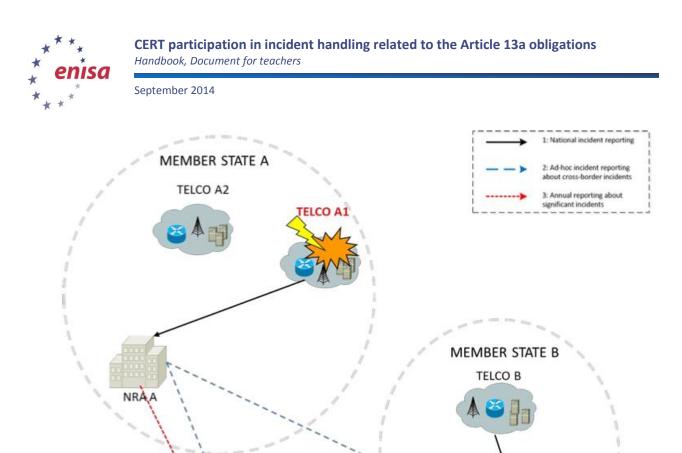
The course of this exercise is as follows. All assumptions and discussions should be moderated by the trainer.

# **3.1** Introduction to the exercise

At the beginning of the exercise you should introduce participants to the attack that occurred in the network of the ISP. Participants play the role of representatives of the ISP CERT team, which is responsible, along with other duties, for analysing network monitoring data and preparing an incident security report for the national regulatory authority.

There are three different levels of incident notifications and obligations related to them:<sup>2</sup>

- a service provider reporting to the national regulatory authority;
- a national regulatory authority reporting to other national regulatory authorities;
- a national regulatory authority reporting to ENISA.



These obligations are described in paragraph 3 of Article 13a<sup>3</sup>:

ENISA

and EC

Figure1: Reporting schemes of Article 13a<sup>2</sup>

Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.

NRA B

In practice it means that the provider (mainly this will relate to ISPs) should continuously monitor the level of the security of their telecommunication resources. Detection and especially reaction and handling to observed incidents should be based on the best practices related to incident handling activities,<sup>4</sup> which means that incident handling capability should exists in all providers.

A citation from Article 13a of the European Telecom Package: "Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). The national regulatory

<sup>&</sup>lt;sup>2</sup> 'Technical Guideline on Reporting Incidents – Article 13a Implementation' - <u>http://www.enisa.europa.eu/activities/Resilience-and-</u>

<sup>&</sup>lt;u>CIIP/Incidents%20reporting/Technical%20Guidelines%20on%20Incident%20Reporting/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting</u>

<sup>&</sup>lt;sup>3</sup> http://ec.europa.eu/information\_society/policy/ecomm/doc/library/regframeforec\_dec2009.pdf

<sup>&</sup>lt;sup>4</sup> ENISA Good Practice Guide for Incident Management: <u>http://www.enisa.europa.eu/activities/cert/support/incident-</u> <u>management</u>



authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest."

In particular cases, where the security incident could have a significant influence on the level of security in countries other than the country of the incident's origin, cooperation and effective communication between national regulatory authorities is very important. Thanks to this cooperation an appropriate warning and alerting in other countries is possible. It is worth adding that this internal country warning and alerting activities are very often based on CERT involvement in these processes.

A citation from Article 13a of the European Telecom Package: "Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph."

The purpose of such reporting is to gather relevant information about Internet network breaches. The assumption is that it will help authorities to better understand new trends and mechanisms in Internet threats as well as being an important element in raising the public's level of awareness regarding Internet security.

In this exercise a security incident related to the ISP network is discovered: the online service for customers is not available due to on-going DDoS attack. Additionally due to the DDos the network service is temporarily unavailable. There is no clear information on how long it could last, what requests might come from customers in case they have no access to their data or network.

# **3.2** Task 1: Building a technical environment for analysing network monitoring data

Participants will have to build a technical environment for analysing network monitoring data. They will need to install Wireshark software<sup>5</sup> for extracting data from Pcap files (packet capture).

Additionally as a recommended tool they would need the tcpdump application. Alternatively the technical environment can be prepared by trainer.

The Wireshark application installation guide can be found in *Wireshark User's Guide* in Chapter 2: 'Building and Installing Wireshark'.<sup>6</sup>

<sup>&</sup>lt;sup>5</sup> <u>http://www.wireshark.org</u>

<sup>&</sup>lt;sup>6</sup> <u>http://www.wireshark.org/download/docs/user-guide-a4.pdf</u>



Filter:			<ul> <li>Expres</li> </ul>	sion Clea	r Apply
No.	Time	Source	Destination	Protocol L	epath Info
	1 0.000000000		192.168.0.1	ТСР	54 13083 > http [ACK] Seq=1 Ack=1 Win=64511 Len=0
	2 0.000005000		10.157.5.204	HTTP	2102 Continuation or non-HTTP traffic[Packet size limited during capture]
		10.230.46.182	192.168.0.1	ТСР	66 46921 > http [ACK] Seg=1 Ack=1 Win=6432 Len=0 TSval=970311826 TSecr=88
	4 0.004149000		10.14.148.186	HTTP	269 Continuation or non-HTTP traffic[Packet size limited during capture]
	5 0.004761000		192.168.0.1	ICMP	70 Destination unreachable (Communication administratively filtered)
	6 0.005275000		192.168.0.1	TCP	54 13083 > http [ACK] Seg=1 Ack=1025 Win=65535 Len=0
		200.150.68.218	192,168,0,1	UDP	256 Source port: chargen Destination port: distinct
		203.218.45.124	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
	9 0.008059000		192.168.0.1	ICMP	70 Destination unreachable (Communication administratively filtered)
	0 0.009933000		192.168.0.1	тср	54 13083 > http [ACK] Seq=1 Ack=2049 Win=64511 Len=0
1	1 0.009978000	192.168.0.1	10.157.5.204	нттр	2102 Continuation or non-HTTP traffic[Packet size limited during capture]
1	2 0.010950000	99.150.164.202	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
		200.196.50.249	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
1	4 0.011883000	200.196.50.249	192.168.0.1	IPv4	1049 Fragmented IP protocol (proto=UDP 0x11, off=5920, ID=260f)
1	5 0.011993000	200.137.128.25	192.168.0.1	IPv4	297 Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=2684)
1	6 0 012111000	200 137 128 25	102 168 0 1	IIDP	1514 Source nort: chargen Destination nort: distinct
Frame	409: 1514 by	tes on wire (12112 bit	s), 96 bytes captured	(768 bits)	
Ether	net II, Src:	JuniperN_a5:0e:80 (50:	c5:8d:a5:0e:80), Dst:	SuperMic_3	5:81:68 (00:25:90:35:81:68)
Lener		Version 4, Src: 200.14	5.25.26 (200.145.25.2	6), Dst: 19	2.168.0.1 (192.168.0.1)
	net Protocol		n (10) Det Borti die	tinct (9999	))
Inter		ocol, Src Port: charge	an (19), DSC POIL: dis		
Inter User	Datagram Prot	ocol, Src Port: charge	an (19), DSt Port: dis		
Inter User		ocol, Src Port: chargo	en (19), DST FOIT: dis		
Inter User	Datagram Prot	ocol, Src Port: charg	an (19), DSC POIL. dis		
Inter User	Datagram Prot	ocol, Src Port: charg	n (19), DSC POLC. 015		
Inter User	Datagram Prot	ocol, Src Port: charg	n (19), DSC POLC. 015		
Inter User	Datagram Prot	ocol, Src Port: charg	an (19), DSC POLC. UIS		
Inter User	Datagram Prot	ocol, Src Port: charg	an (19), DSC POLC. GIS		
Inter User	Datagram Prot	ocol, Src Port: charg	n (19), DSC POLC. 015		
Inter User Data	Datagram Prot			P F	
Inter User Data	Datagram Prot (54 bytes) 00 25 90 35 81	68 50 c5 8d a5 0e 8 00 6d 11 6a 60 c8 9	0 08 00 45 00 .%.5.h	PE. m. j`	

Figure 2: Using Wireshark

The figure presents the Wireshark interface with pcap loaded into the application; information about packets can be seen in the picture.

# **3.3 Task 2: Analysing of network monitoring data**

Network monitoring data, provided to participants in this exercise, includes different types of network TCP/IP protocol data, like ICMP flows and UDP flows. Participants should make the following types of analysis.

#### Subtask 1 – determination of time and volume of the attack

Firstly, participants should create a short summary including basic information of each pcap file they have. They should check:

- the start and end time of capture;
- the size of captured packets;
- the total number of packets as well as average packet/byte rates;

This information should give a general overview of the size of data that are going to be analysed and allow the placement of PCAP files on the timeline (note that capture times of separate PCAPs can overlap).

All of this information can be easily checked using the capinfos tool that comes with Wireshark:<sup>7</sup>

<sup>&</sup>lt;sup>7</sup> http://www.wireshark.org/docs/man-pages/capinfos.html



\$ capinfos /path/to/pcap/file.pcap

	\$ capinfos ddos.pcap
File name:	
File type:	Wireshark/tcpdump/ libpcap
File encapsulation:	Ethernet
Packet size limit:	file hdr: 96 bytes
Packet size limit:	inferred: 96 bytes
Number of packets:	5809766
File size:	631017266 bytes
Data size:	
Capture duration:	484 seconds
Start time:	2012
End time:	2012
Data byte rate:	13242515.58 bytes/sec
Data bit rate:	105940124.63 bits/sec
Average packet size:	1103.76 bytes
Average packet rate:	11997.63 packets/sec
SHA1:	f97f61a03813c289d685749d7dafd3c3f1e56fbd
RIPEMD160:	e010c9cceaaac66188eceefa761044d5db254750
MD5:	00e4502241fc357415218cf4ce32bba1
Strict time order:	False
<pre>@debian1:~/ddos</pre>	s 🗌

Figure 3: Using capinfos

Figure 3 shows the output of the capinfos application, allowing the user to obtain general information about the pcap file. Information consists of file size, number of captured packets, checksums, capture times and also a few average values.

In the next step, participants should examine the captured traffic and try to determine what kind of DDoS attack was performed. Usually, during a DDoS attack, more than one DDoS technique is used; or there are separate and distinct attack sources. At this point, they should try to create a Wireshark filter <sup>8</sup> or a tcpdump Berkeley Packet Filter (BPF) filter,<sup>9</sup> which would allow filtering out each type of DDoS attack stream.

In fact there were two kinds of attacks and this should be found out by participants (see below).

- ICMP flood
- UDP flood

In the ICMP flood, all ICMP packets were type 3 (Destination Unreachable) with codes 3 (Destination Port Unreachable) and a few cases of code 1 (Destination host unreachable) and 13 (Communication administratively prohibited).

<sup>&</sup>lt;sup>8</sup> More on Wireshark filters: https://www.wireshark.org/docs/dfref/

<sup>&</sup>lt;sup>9</sup> More on tcpdump filters: http://www.cs.ucr.edu/~marios/ethereal-tcpdump.pdf



1301         0.961362000         20.           1589         0.9613680000         99           1592         0.965316000         99           1596         0.967381000         99           1608         0.974086000         20.           1609         0.97566000         19.           1617         0.979676000         19.           1622         0.981248000         99.           1628         0.985755000         99.           1640         0.995775000         20.           1645         0.995775000         99.           1647         1.0158000         99.           1657         1.01383000         99.           1687         1.022240000         20.           1683         1.022243000         99.	.150.164.202 .156.206.232 3.218.45.124 .150.164.202 2.168.0.1 .29.79.36 .150.164.202 .156.206.232	192.108.0.1 192.168.0.1 192.168.0.1 192.168.0.1 192.168.0.1	ICMP	Length Info	еаспарте (Рогт и	пеаспарте)	
1592 0.965316000 99 1596 0.967381000 99 1608 0.974086000 20 1609 0.97506600 99 1617 0.979676000 19 1622 0.981248000 99 1628 0.985755000 99 1640 0.995175000 20 1645 0.997974000 99 1667 1.010158000 99 1667 1.010158000 99 1668 1.022240000 20	.150.164.202 .156.206.232 3.218.45.124 .150.164.202 2.168.0.1 .29.79.36 .150.164.202 .156.206.232	192.168.0.1 192.168.0.1		70 Destination un	eachable (Communi	ication administ	ratively filtered)
1608 0.974086000 203 1609 0.975066000 99 1617 0.979676000 193 1622 0.981248000 99 1631 0.98725000 99 1640 0.995175000 203 1645 0.997974000 99 1667 1.010158000 99 1675 1.013883000 99 1675 1.013883000 203	3.218.45.124 .150.164.202 2.168.0.1 .29.79.36 .150.164.202 .156.206.232		ICMP	74 Destination un	eachable (Port u	nreachable)	
1609         0.975066000         99           1617         0.979676000         19           1622         0.981248000         99           1631         0.987270000         99           1640         0.995175000         90           1645         0.997974000         99           1645         0.997974000         99           1667         1.01058000         99           1675         1.01383000         99           1678         1.022240000         203	.150.164.202 2.168.0.1 .29.79.36 .150.164.202 .156.206.232	192.100.0.1	ICMP ICMP	74 Destination un 74 Destination un			
1622 0.981248000 99 1628 0.985755000 99 1631 0.987270000 99 1640 0.995175000 20 1645 0.997974000 99 1667 1.010158000 99 1675 1.013983000 99 1689 1.022240000 20	.29.79.36 .150.164.202 .156.206.232	192.168.0.1	ICMP	74 Destination un			
1628 0.985755000 99 1631 0.987270000 99 1640 0.995175000 20 1645 0.997974000 99 1667 1.010158000 99 1675 1.013983000 99 1689 1.022240000 20	.150.164.202	200.196.50.249	ICMP	590 Destination un	· · · · · · · · · · · · · · · · · · ·		anticolo filterado
1640         0.995175000         203           1645         0.997974000         99           1667         1.010158000         99           1675         1.013983000         99           1689         1.022240000         203		192.168.0.1 192.168.0.1	ICMP ICMP	70 Destination un 74 Destination un			ratively filtered)
1645         0.997974000         99           1667         1.010158000         99           1675         1.013983000         99           1689         1.022240000         203		192.168.0.1	ICMP	74 Destination un	eachable (Port u	nreachable)	
16671.0101580009916751.0139830009916891.022240000203		192.168.0.1 192.168.0.1	ICMP ICMP	74 Destination un 74 Destination un			
1689 1.022240000 203		192.168.0.1	ICMP	74 Destination un	eachable (Port u	nreachable)	
		192.168.0.1 192.168.0.1	ICMP ICMP	74 Destination un 74 Destination un			
		192.168.0.1	ICMP	70 Destination un			ratively filtered)
10 00 3c 20 b3 00 00 20 00 01 03 03 17 e4 30 00 00 f3 11 4e 71	0 74 01 5d 04 63 4 00 00 00 00 45 1 c0 a8 00 01 63	5 00 00 20 b0 51 . 3 96 a4 ca 27 0f . kets: 5809634 Displayed:	<t. ].c<br="">Nqc' Nqc' </t.>	. Q		- Dr	ofile: Default
	packet of t		ation Unro	eachable) with		estination P	
	packet of t	C 🖹 Q 🗲	iation Unre	eachable) with			
gure4: ICMP p	packet of t	C 🖹 Q 🗲	⇒ 🗘 📅 🛓 xpression Cle	eachable) with		estination P	
gure4: ICMP p Composition for the solution of	Dacket of tr	C 2 C C C C C C C C C C C C C C C C C C	ixpression Cle Protocol	eachable) with	eachable (Port u	estination P	
gure4: ICMP p i in	Coacket of ty	C Destination	⇒ 🐌 ቸ s Expression Cle Protocol	eachable) with	eachable (Port u	estination P	
gure4: ICMP p Composition of the second sec	Deacket         of         ty           Image: Ima	C 2 C C C C C C C C C C C C C C C C C C	> > ?  Systems Protocol ICMP	eachable) with  eachable) with  ar Apply Length Info  74 Destination un	e d T eachable (Port u reachable (Port u reachable (Port u reachable (Port u	estination P	
gure4: ICMP p Composition of the second sec	Dacket of ty	C P C C C C C C C C C C C C C C C C C C		eachable) with	reachable (Port u reachable (Port u reachable (Port u reachable (Port u reachable (Port u	estination P	
gure4: ICMP p image: participation of the second s	Dacket of ty	C Destination 192.168.0.1 192.168.0.1 192.168.0.1 192.168.0.1 192.168.0.1 192.168.0.1 192.168.0.1	Comparison Cle  Protocol  ICMP  ICM	eachable) with	■ ① 評 eachable (Port u reachable (Port u reachable (Port u reachable (Port u reachable (Port u reachable (Port u reachable (Port u	estination P	Port Unreachab
gure4: ICMP p implementation of the second	Deacket         of         ty           Image: Ima	C E C C C C C C C C C C C C C C C C C C	Classing Control of the second secon	eachable) with	eachable (Port u reachable (Port u	estination P	Port Unreachab
gure4: ICMP p c C C C C C C C C C C C C C C C C C C C	Cource	C E C C C C C C C C C C C C C C C C C C	Comparison Clear Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	eachable) with	reachable (Port u reachable (Port u	estination P	Port Unreachab
gure4: ICMP p ter: icmp b. Time So 2380 1.364910000 99 2398 1.377103000 20 2402 1.378311000 20 2402 1.378311000 20 2413 1.398453000 99 2433 1.398453000 99 2435 1.398425000 19 2435 1.408238400 19 2465 1.410796000 99	Coacket of ty	C 2 2 C 2 C 2 C 2 C 2 C 2 C 2 C 2 C 2 C		eachable) with	eachable (Port u reachable (Port u	estination P	Port Unreachab
gure4: ICMP p c C C C C C C C C C C C C C C C C C C C	Coacket of ty	C 2 2 C 2 C 2 C 2 C 2 C 2 C 2 C 2 C 2 C	CAPPERSION Cle Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	eachable) with	reachable (Port u reachable (Port u	estination P	Port Unreachab



🗒 🎆 🚳 😂 🚳 🗎 🛅 🔀 🗶 (	C 🚊 🔍 🔶 =	-> 🗣 🛓 🗐 曼 😑 🖪 📅 👹 🔀 💥 👔
Filter: icmp	▼ E>	Expression Clear Apply
No. Time Source	Destination	Protocol Length Info
1589 0.961686000 99.29.79.36	192.168.0.1	ICMP         70 Destination unreachable (Communication administratively filtered)
1592 0.965316000 99.150.164.202	192.168.0.1	ICMP 74 Destination unreachable (Port unreachable)
1596 0.967381000 99.156.206.232	192.168.0.1	ICMP 74 Destination unreachable (Port unreachable)
1608 0.974086000 203.218.45.124	192.168.0.1	ICMP 74 Destination unreachable (Port unreachable)
1609 0.975066000 99.150.164.202	192.168.0.1	ICMP 74 Destination unreachable (Port unreachable)
1617 0.979676000 192.168.0.1	200.196.50.249	ICMP 590 Destination unreachable (Port unreachable)
1622 0.981248000 99.29.79.36		ICMP 70 Destination unreachable (Communication administratively filtered)
1628 0.985755000 99.150.164.202	192.168.0.1	ICMP 74 Destination unreachable (Port unreachable)
1631 0.987270000 99.156.206.232	192.168.0.1	ICMP 74 Destination unreachable (Port unreachable)
1640 0.995175000 203.218.45.124	192.168.0.1	ICMP 74 Destination unreachable (Port unreachable)
1645 0.997974000 99.150.164.202	192.168.0.1	ICMP 74 Destination unreachable (Port unreachable)
1667 1.010158000 99.150.164.202	192.168.0.1	ICMP 74 Destination unreachable (Port unreachable)
1675 1.013983000 99.156.206.232	192.168.0.1	ICMP 74 Destination unreachable (Port unreachable)
1689 1.022240000 203.218.45.124	192.168.0.1	ICMP 74 Destination unreachable (Port unreachable)
1693 1.022834000 99.29.79.36	192.168.0.1	ICMP 70 Destination unreachable (Communication administratively filtered)
Frame 1622: 70 bytes on wire (560 bit	s) 70 bytes canture	red (560 hits)
		, Dst: SuperMic 35:81:68 (00:25:90:35:81:68)
<ul> <li>Internet Protocol Version 4, Src: 99.</li> </ul>		
Internet Control Message Protocol		
Type: 3 (Destination unreachable)		
Code: 13 (Communication administrati	velv filtered)	
Checksum: 0xd5c5 [correct]	,	
Internet Protocol Version 4, Src: 19	2.168.0.1 (192.168.0	.0.1). Dst: 99.29.79.36 (99.29.79.36)
▶ User Datagram Protocol, Src Port: di		

0000 00 25 90 35 81 68 50 c5 8d a5 11 c0 08 00 45 00	.%.5.hPE.	
0010 00 38 15 37 00 00 f3 01 3f a3 63 1d 4f 24 c0 a8	.8.7 ?.c.0\$	
0020 00 01 03 0d d5 c5 00 00 00 00 45 00 00 20 cf cc	E	
0030 00 00 f4 11 84 15 c0 a8 00 01 63 1d 4f 24 27 0f		
File: "/home/user/Downloads/dat Packets: 5809634 Displa	wod: 197199 Markod: 01 and time: 1:01 707	Profile: Default
File. /IIOIIIe/usei/Dowilloads/dat Fackets. 5605054 Displa	197 190 Marked. 0 Load Line. 1.01.707	- Fronte, Deraute

Figure 6: ICMP packet of type 3 (Destination Unreachable) with code 13 (Communication administratively filtered)

The UDP flood consisted of many fragmented IP packets. For all of them, the protocol field was set to UDP and for most of them either the MF flag was set or the fragment offset was greater than zero.

Help participants by explaining the filters presented below. If participants have problems with finding the solution, provide the proper Wireshark.

Filters which could be used for this analysis are the Wireshark display filter, and the tcpdump filter.

Wireshark display filter: (udp && not udp.port == 53) || ip.flags.mf == 1 || ip.frag offset > 0

This is a sample Wireshark display filter allowing us to separate DDoS UDP flood. To do this we select all packets matching a) or b) or c) rule:

- a) (udp && not.udp == 53) all udp packets with port other than 53 (we're not interested in DNS traffic which isn't part of DDoS attack)
- b) ip.flags.mf == 1 packets having IP flag MF (More Frag.) set
- c) ip.frag\_offset > 0 packets with fragment offset greater than 0.

Tcpdump filter: ip[6:2]&8191>0 or ip[6]&32!=0 or (udp and not port 53)<sup>10</sup>

The second filter is the same filter, but written in BPF tcpdump filter syntax. This time we can't refer to separate fields of IP or UDP headers. To filter packets by IP header fields values we must refer to IP

<sup>&</sup>lt;sup>10</sup> ip[6:2]&8191>0 is for checking IP fragment offset field (2 bytes length starting from 6th byte of IP hdr, counting from 0)

ip[6]&32!=0 is for checking whether MF (More fragments) flag was set



header as byte array with ip[0] being a first byte of IP header. Syntax is as follows: ip[a:n] - 'n' bytes starting from 'a' position/element/byte. & operator denotes bitwise AND operation. a) ip[6:2]&8191>0 - fragment offset greater than 0 b) ip[6]&32!=0 - flag MF is set c) udp and not port 53 - all udp packets with port other than 53

Packets to port 53 are excluded as packets sent to this port were proper DNS requests and weren't part of DDoS attack (at least in this case).

o. Time Source	Destination	Protocol	Length Info
3452 1.970980000 200.145.156.238	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
3454 1.972579000 200.145.25.26	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
3460 1.975467000 99.29.79.36	192.168.0.1	ICMP	70 Destination unreachable (Communication administratively filtered)
3461 1.977129000 99.29.79.36	192.168.0.1	ICMP	70 Destination unreachable (Communication administratively filtered)
3470 1.978669000 68.85.179.170	192.168.0.1	ICMP	70 Destination unreachable (Host unreachable)
3473 1.980085000 99.150.164.202	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
3480 1.986712000 203.218.45.124	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
3489 1.990863000 200.145.25.26	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
3493 1.992277000 203.218.45.124	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
3494 1.992330000 99.150.164.202	192.168.0.1	ICMP	74 Destination unreachable (Port unreachable)
3495 1.992963000 200.145.156.238	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
3496 1.996105000 200.143.210.11	192.168.0.1	UDP	1208 Source port: chargen Destination port: distinct
3499 1.996437000 200.196.50.249	192.168.0.1	UDP	1329 Source port: chargen Destination port: distinct
3500 1.996468000 192.168.0.1	192.168.0.1 200.196.50.249	ICMP	590 Destination unreachable (Port unreachable)
35001.996468000192.168.0.135011.997002000200.145.78.193	200.196.50.249 192.168.0.1	ICMP UDP	
<b>3500 1.996468000 192.168.0.1</b> <b>3501 1.997002000 200.145.78.193</b> <b>3505 1.997405000 192 168</b> 0 <b>1</b>	200.196.50.249 192.168.0.1 200.145.78.193	ICMP UDP TCMP	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable)
<b>3500 1.996468000 192.168.0.1</b> <b>3501 1.997002000 200.145.78.193</b> <b>3505 1.997405000 192 168</b> 0 <b>1</b>	200.196.50.249 192.168.0.1 200.145.78.193	ICMP UDP TCMP	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable)
3500         1.995468000         192.168.0.1           3501         1.997002000         200.145.78.193           3505         1.997405000         102.158         0.1           Internet         Protocol         Version         4, Src:	200.196.50.249 192.168.0.1 200.145.78.193	ICMP UDP TCMP	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable)
3500         1.996468000         192.168.0.1           3501         1.997002000         200.145.78.193           3505:         1.997002000         200.145.78.193           3506:         1.997002000         102.168.0.1           Internet Protocol Version 4, Src:         Version: 4           Header length:         20 bytes	200.196.50.249 192.168.0.1 200.145.78.103 200.145.156.238 (200.1	ICMP UDP TCMP (45.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable)
3500         1.996468000         192.168.0.1           3501         1.997002000         200.145.78.193           3505:         1.997002000         200.145.78.193           3506:         1.997002000         102.168.0.1           Internet Protocol Version 4, Src:         Version: 4           Header length:         20 bytes	200.196.50.249 192.168.0.1 200.145.78.103 200.145.156.238 (200.1	ICMP UDP TCMP (45.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable) Dest: 192.168.0.1 (192.168.0.1)
3500         1.996468000         192.168.0.1           3501         1.997002000         200.145.78.193           3505         1.907040000         102.168.0.1           Internet Protocol Version 4, Src:         Version: 4           Header length: 20 bytes         Differentiated Services Field: 0	200.196.50.249 192.168.0.1 200.145.78.103 200.145.156.238 (200.1	ICMP UDP TCMP (45.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable) Dest: 192.168.0.1 (192.168.0.1)
3500 1.996468000 192.168.0.1 3501 1.997002000 200.145.78.193 2503 1.997002000 200.145.78.193 2503 1.90702000 Version 4, Src: Version: 4 Header length: 20 bytes Differentiated Services Field: 0 Total Length: 1500 Identification: 0x652b (25899)	200.196.50.249 192.168.0.1 200.145.78.103 200.145.156.238 (200.1	ICMP UDP TCMP (45.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable) Dest: 192.168.0.1 (192.168.0.1)
3500 1.996468000 192.168.0.1 3501 1.997002000 200.145.78.193 25034 002246900 102 163 1 1 Internet Protocol Version 4, Src: Version: 4 Header length: 20 bytes Differentiated Services Field: 0 Total Length: 1500 Identification: 0x652b (25899)	200.196.50.249 192.168.0.1 200.145.78.103 200.145.156.238 (200.1	ICMP UDP TCMP (45.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable) Dest: 192.168.0.1 (192.168.0.1)
3500         1.996468000         192.168.0.1           3501         1.997002000         200.145.78.193           3501         1.997002000         200.145.78.193           3501         1.997002000         200.145.78.193           3501         1.997002000         200.145.78.193           3501         1.997002000         200.145.78.193           3501         1.997002000         200.145.78.193           3501         1.997002000         200.145.78.193           Meader         length: 20         bytes           Differentiated Services Field: 0         Total Length: 1500           Identification:         0x652b (25899)           Flags:         0x01 (More Fragments)	200.196.50.249 192.168.0.1 200.145.78.103 200.145.156.238 (200.1	ICMP UDP TCMP (45.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable) Dest: 192.168.0.1 (192.168.0.1)
3500 1.996468000 192.168.0.1 3501 1.997002000 200.145.78.193 2505 1 0020406000 100.1450 n 1 Internet Protocol Version 4, Src: Version: 4 Header length: 20 bytes Differentiated Services Field: 0 Total Length: 1500 Identification: 0x652b (25899) Flags: 0x01 (More Fragments) Fragment offset: 0	200.196.50.249 192.168.0.1 200.145.78.103 200.145.156.238 (200.1	ICMP UDP TCMP (45.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable) Dest: 192.168.0.1 (192.168.0.1)
3500 1.996468000 192,168.0.1 3501 1.997002000 200.145.78.193 Enternet Protocol Version 4, Src: Version: 4 Header length: 20 bytes Differentiated Services Field: 0 Total Length: 1500 Identification: 0x652b (25899) Flags: 0x01 (More Fragments) Fragment offset: 0 Time to live: 108 Protocol: UDP (17)	200.196.50.249 192.168.0.1 200.145.72.109 200.145.156.238 (200.1 x00 (DSCP 0x00: Default	ICMP UDP TCMP (45.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable) Dest: 192.168.0.1 (192.168.0.1)
3500 1.996468000 192,168.0.1 3501 1.997002000 200.145.78.193 Enternet Protocol Version 4, Src: Version: 4 Header length: 20 bytes Differentiated Services Field: 0 Total Length: 1500 Identification: 0x652b (25899) Flags: 0x01 (More Fragments) Fragment offset: 0 Time to live: 108 Protocol: UDP (17)	200.196.50.249 192.168.0.1 200.145.156.238 (200.1 200.145.156.238 (200.1 x00 (DSCP 0x00: Default	ICMP UDP TCMP (45.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable) Dest: 192.168.0.1 (192.168.0.1)
3500 1.996468000 192.168.0.1 3501 1.997002000 200.145.78.193 2404 1 002413400 102.154 0 1 Internet Protocol Version 4, Src: Version: 4 Header length: 20 bytes Differentiated Services Field: 0 Total Length: 1500 Identification: 0x652b (25899) Flags: 0x01 (More Fragments) Fragment offset: 0 Time to live: 108 Protocol: UDP (17) Header checksum: 0x9dbc [correct	200.196.50.249 192.168.0.1 200.145.75.0238 (200.1 200.145.156.238 (200.1 x00 (DSCP 0x00: Default	ICMP UDP TCMP (45.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 590 Destination unreachable (Port unreachable) Dest: 192.168.0.1 (192.168.0.1)
3300 1.996468000 192.168.0.1 3501 1.997002000 200.145.78.193 2505 1 002746000 100.145 78.193 2505 1 002746000 100.1450 0.1 Internet Protocol Version 4, Src: Version: 4 Header length: 20 bytes Differentiated Services Field: 0 Total Length: 1500 Identification: 0x652b (25899) Flags: 0x01 (More Fragments) Fragment offset: 0 Time to live: 108 Protocol: UDP (17) Header checksum: 0x9dbc [correct Source: 200.145.156.238 (200.145 Destination: 192.168.0.1 (192.16	200.196.50.249 192.168.0.1 200.145 75 102 200.145.156.238 (200.1 x00 (DSCP 0x00: Default x00 (DSCP 0x00: Default 1 .156.238) 3.0.1)	ICMP UDP TCAD 145.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct 500 Destination unreachable (Port unreachable) 501 Destination (192.168.0.1) Not-ECT (Not ECN-Capable Transport))
3500 1.996468000 192.168.0.1 3501 1.997002000 200.145.78.193 2005 1 0.997002000 200.145.78.193 2005 1 0.9270600 100.1450 10 Internet Protocol Version 4, Src: Version: 4 Header length: 20 bytes Differentiated Services Field: 0 Total Length: 1500 Identification: 0x652b (25899) Flags: 0x01 (More Fragments) Fragment offset: 0 Time to live: 108 Protocol: UDP (17) Header checksum: 0x9dbc [correct Source: 200.145.156.238 (200.145)	200.196.50.249 192.168.0.1 200.145.70.100 200.145.156.238 (200.1 x00 (DSCP 0x00: Default x00 (DSCP 0x00: Default 156.238) 3.0.1) 5 0e 80 08 00 45 00	ICMP UDP TCMP (45.156.238), D	590 Destination unreachable (Port unreachable) 1514 Source port: chargen Destination port: distinct CONDICIENTING Uncompared and a state of the st

Figure 7: Excluded packets to port 53 that are legitimate packets



er: udp && not udp.port ==53    ip.flags.	mf == 1    ip.frag_o 🔻 E	Expression C	ilear Apply
Time Source	Destination		l Length Info
+1472 330.2082310(98.23.121.63 +1473 350.2683520(98.215.157.124	192.100.0.1		1514 Source port, chargen Destination port, distinct
1475 350.2683520(98.213.157.124	192.168.0.1	UDP UDP	1514 Source port: chargen Destination port: distinct 1514 Source port: chargen Destination port: distinct
1477 350.2684840(202.142.218.218	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
1477 350.2689770(202.142.218.218	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
1486 350.2690180(101.140.18.78	192.168.0.1	UDP	1490 Source port: chargen Destination port: distinct
1491 350.2692870(203.68.179.85	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
1492 350.2693220(98.223.66.157	192.168.0.1	UDP	715 Source port: chargen Destination port: distinct
1493 350.2694250(203.94.64.17	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
1495 350.2696480(202.143.146.108	192.168.0.1	UDP	1123 Source port: chargen Destination port: distinct
1497 350.2697460(200.198.193.174	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
1498 350.2698030(200.208.204.102	192.168.0.1	UDP	1514 Source port: hdap Destination port: distinct
1499 350.2698160(98.223.214.14	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
1500 350.2698190(200.91.233.61	192.168.0.1	UDP	131 Source port: chargen Destination port: distinct
11501 350.2698920(202.157.179.209	192.168.0.1	UDP	1514 Source port: chargen Destination port: distinct
11502 350.2699360(203.135.192.130	192.168.0.1	UDP	1466 Source port: chargen Destination port: distinct
Version: 4 Header length: 20 bytes Differentiated Services Field: 0x0 Total Length: 1500 Identification: 0x377c (14204) Flags: 0x01 (More Fragments) 0 = Reserved bit: Not set .0 = Nort fragment: Not s = More fragments: Set Fragment offset: 0		:; ECN: 0×00:	Not-ECT (Not ECN-Capable Transport))
Fragment offset: 0 Time to live: 111			
Protocol: UDP (17)			
		.7	

Figure 8: UDP packet with More Fragments (MF) bit set

Next, participants should recognise what distinct streams the DDoS attack consisted of (either different attack methods/techniques or clear source distinction). They can analyse input/output statistics for those streams in comparison with normal server traffic. To complete this task they should:

- 1. open the PCAP file in Wireshark;
- 2. choose Statistics  $\rightarrow$  IO Graph;
- 3. use the display filters created in the previous point to create separate graphs;
- 4. adjust other options if needed (X and Y axis scale, line style, etc.)



\*\*\*\* \* enisa \*\*\*\*

September 2014

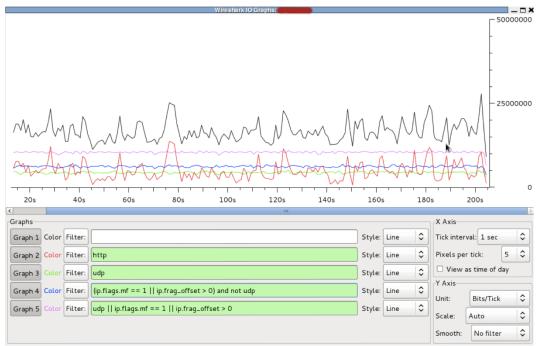


Figure 9: statistics of the initial DDoS phase.

Figure 9 presents the initial phase of the DDoS attack. Legitimate HTTP traffic is marked with a red line. We can see strong fluctuations over time of this type of traffic (which is quite normal). DDoS traffic (UDP flood) is marked with a pink line. In this case, fluctuations are much smaller and its throughput is almost constant (~10 Mbps). Also we can see that DDoS traffic doubles the average throughput of HTTP traffic.

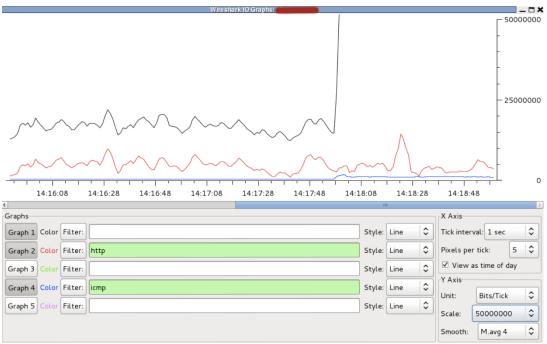


Figure 10: Slight increase of ICMP traffic (blue line) with the start of the second DDoS phase

Figure 10 presents a slight increase of value for ICMP traffic around 14:18:00. This increase is a representation of the second phase of the DDoS attack.





#### Figure 11: Second DDoS phase

Around 14:17:58, the second DDoS phase started. We can see that with the start of the second DDoS phase, the total traffic significantly increased. Total traffic throughput increased from ~22.5 Mbps to ~200 Mbps, which means that traffic increased nearly nine times in comparison with the first phase, and forty times in comparison with legitimate HTTP traffic (~5Mbps). We should also note that traffic increase was almost entirely due to UDP flood (green line).



Figure 12: Second DDoS phase in detail



Figure 12 more clearly shows us increase of UDP flood (green line) traffic with the beginning of the second DDoS phase.

The next subtask for participants is to determine the endpoints' addresses of analysed hosts. There are various ways to export such addresses – they can do this using either Wireshark or tcpdump.

#### Method 1 with Wireshark:

If participants use Wireshark application they should follow the following steps.

- 1. Open pcap with DDoS traffic in Wireshark (alternatively just apply the proper display filter to the file with all captured traffic).
- 2. Choose Statistics  $\rightarrow$  Endpoints and switch to IPv4 tab.

IPv4 Endpoints								
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
10.157.5.204	4 401	2 330 335	2 500	334 389	1 901	1 995 946		-
192.168.0.1	5 436 937	5 955 477 201	321 809	268 372 725	5 115 128	5 687 104 476		-
10.230.46.182	1 082	559 146	684	71 411	398	487 735		-
10.14.148.186	443	218 516	251	55 983	192	162 533		-
99.29.79.36	13 344	934 080	6 672	467 040	6 672	467 040		-
200.150.68.218	16 244	18 122 259	15 892	17 979 650	352	142 609		-
203.218.45.124	41 624	3 080 176	20 812	1 540 088	20 812	1 540 088		-
99.150.164.202	40 208	2 975 392	20 104	1 487 696	20 104	1 487 696		-
200.196.50.249	24 646	30 120 777	24 294	29 945 808	352	174 969		-
200.137.128.25	24 950	30 491 811	24 601	30 315 773	349	176 038		-
99.156.206.232	34 238	2 533 612	17 119	1 266 806	17 119	1 266 806		-
200.128.79.52	25 764	31 717 867	25 412	31 542 774	352	175 093		-
200.136.91.11	24 879	30 707 637	24 528	30 534 219	351	173 418		-
202.5.131.5	24 862	30 298 864	24 510	30 125 999	352	172 865		-
10.27.121.68	31	3 338	10	564	21	2 774		-
203.81.218.138	6 945	7 115 964	6 605	6 995 080	340	120 884		-
200.145.25.26	25 389	31 287 228	25 041	31 111 144	348	176 084		-
203.94.64.17	16 612	20 092 922	16 264	19 940 558	348	152 364		-
200.133.238.11	14 465	16 211 320	14 118	16 084 428	347	126 892		-
200.145.156.238	47 642	58 705 180	47 292	58 525 100	350	180 080		-
200.143.210.11	24 855	30 385 347	24 503	30 208 606	352	176 741		-

Figure 13 Sources of the DDoS attack and packets statistics

- 3. If necessary make sure the 'Limit to display filter' option is selected.
- 4. Click 'Copy' and paste the data to some file. The data is in CSV format.
- 5. Save file as ddos.csv
- 6. Get the ip addresses only from .csv file using the following command:
  - cat ddos.csv | cut -d '"' -f 2 > ddos ip.uniq

#### Method 2 with tcpdump

If participants want to use tcpdump they should follow the following steps.

- 1. Use the tcpdump command:
  - tcpdump -n -r data ddos.pcap '<filter>'

As the result they should receive:





14:13:28.944879 IP 99.29.x.x > 92.158.x.x: ICMP host 99.29.79.36 unreachable - admin prohibited filter, length 36

14:13:28.947665 IP 203.218.x.x > 92.158.x.x: ICMP 203.218.45.124 udp port 19 unreachable, length 40

14:13:28.948177 IP 99.29.x.x > 92.158.x.x: ICMP host 99.29.79.36 unreachable - admin prohibited filter, length 36

14:13:28.951068 IP 99.150.x.x > 92.158.x.x: ICMP 99.150.164.202 udp port 19 unreachable, length 40 2. Use the tcpdump command:

tcpdump -n -r ddos.pcap | perl -ne 'if (m/IP
 (\d+\.\d+\.\d+\.\d+)/){print "\$1\n";}' | sort -u >
 ddos ip.uniq

This should produce the list of unique IP addresses (ddos\_ip.uniq). Such list can be used for finding more information, e.g. autonomous systems. To get list of autonomous systems associated with these addresses, participants can use the free service available at The Shadowserver Foundation: <a href="http://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP">http://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP</a>

All information gathered during the subtasks should be used to prepare the full report (see Task 3).

#### 3.4 Task 3: Evaluating countermeasures values

After collecting all information from network monitoring data, participants should prepare a security incident report for the national regulatory authority (NRA). To better prepare this report, they should first learn more about the reporting schema template. You should present them the template and explain its fields using the following guide from the ENISA document *Technical Guide on Reporting Incidents*.<sup>11</sup> Each participant should use one of the ISP providers that they are most familiar with. The name of the ISP can be fictitious. Keeping in mind and referring to the real examples from their countries gives participants an additional chance to exchange information about practical aspects of cooperation between CERTs and ISPs in different countries. There is no need to use real names for this purpose.

Field	Description	Tip for fulfilling
Country	The country that sends the report to NRA	
Date and time	Details of the date and time when the incident took place (in national time). It can be interpreted as the time the incident was discovered.	According to analysed logs

<sup>&</sup>lt;sup>11</sup> (http://www.enisa.europa.eu/activities/Resilience-and-

<sup>&</sup>lt;u>CIIP/Incidents%20reporting/Technical%20Guidelines%20on%20Incident%20Reporting/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting) (page 20).</u>



	Time should be expressed in both CET and local time.	
Impacted services	The affected service: the service rendered unavailable to the end- user. This field includes a description of the service whose continuity and availability are affected by the impact level. It should be noted that assessing the Level of Service (LoS) Quality of Service (QoS) introduces complexity into the analysis criteria and can become subjective. The possible choice is: fixed telephony, mobile telephony, (short) message services, Internet, email.	According to participants' knowledge of online service functionality and services
Number of users affected	The total number of users affected when an incident occurs (percentage of all affected users of that service in a given country). The national report to the NRA may include the absolute number the NRA would have to translate into percentages for inclusion in the annual report to ENISA and the European Commission.	According to participants' knowledge of online service functionality and services
Duration	The duration of the incidents	According to analysed logs
Geographic spread/region	If available, the region impacted by the incident	According to the participants' choice of ISP geographical location. Add information about geographical location of attacking parties.
Impact on Emergency calls	If available emergency service impacted by the incident	For the purpose of the exercise, the real data of CERTs represented by participants
Description	Fill in any further information you can share on the impact of the incident.	According to the findings from logs analysis



Root cause	What kind of disaster or reason caused the security problem. The potential choices are: natural disaster or phenomena, human error, malicious attack, hardware or software failure, failure at third party or external party.	According to participants' knowledge of the source of incident. The description and findings can be changed during the analysis.
Other incident information	A general description of the incident. Also the description of all the incident handling actions and activities undertaken by a handler and post-incident actions. In this part of the report, there is information about other possible parties affected by an incident. Other descriptive information about an incident includes lessons learnt from an incident and further remarks. There is one more particular piece of information requested – NRA's contacted (in case of a cross –border incident). This one is especially dedicated for the NRA. From the perspective of the ISP and its CERT it is included in information about cooperation and contact with other parties.	

Some of the information is not very important in preparing the report in terms of the exercise purposes, but it is important to give participants the whole picture and mention and discuss all information.<sup>12</sup>

#### 4 Summary of the exercise

In the summary ask participants to present their findings about the incident by presenting the requested fields of the security incident report. Be sure that all participants present their work results. In particular, discuss findings if they differ among participants. Find a proper solution.

At the end of the summary, present again the main rules for incident reporting schema between ISPs, NRAs and ENISA and explain the purposes of these regulations, as well as benefits for CERTs. These benefits may include:

closer cooperation between CERTs on the operational level;

<sup>&</sup>lt;sup>12</sup> More descriptions of the report fields are available in the ENISA document 'Technical Guideline on Reporting Incidents – Article 13a Implementation' (page 21). <u>https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-for-incident-reporting-v1.0</u>



- common schema for collecting information about incidents;
- closer cooperation inside each Member States between parties involved in improving security level;
- systematic collection of security incident related data and its usage for building awareness about security threats in the Internet;



#### 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