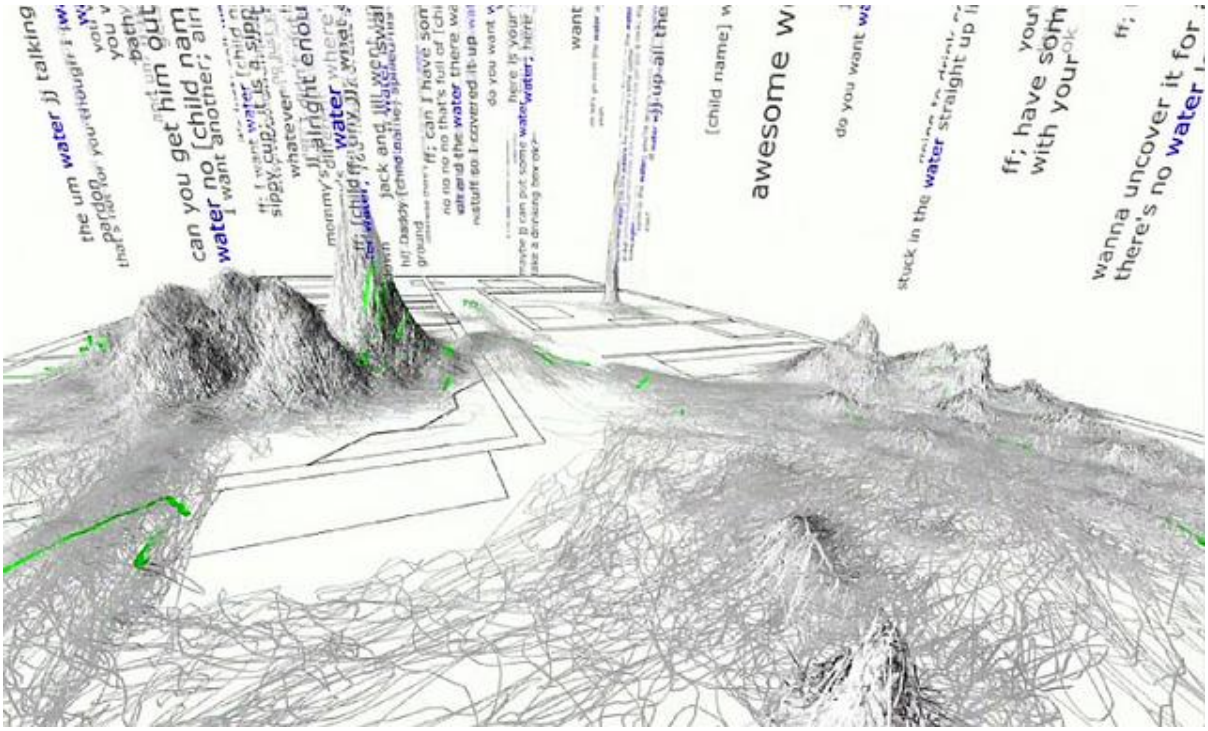

Automation in Incident Handling

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

Sometimes information about an incident, particularly about a wide-spread incident, is received in bulk – containing not just data about your networks but from all networks. This can be the case when a site under a DDoS attack shares its logs without time to sort and separate them for individual ISPs, looks for contacts, etc. Having one-to-many distribution channels at hand, such as mailing lists, they can efficiently publish information for everyone to analyse.

On the other hand, sometimes you have plenty of information collected from your own sources which you wish to share with others, distributing it on a need-to-know basis. An example can be logs from IPS systems, early warning systems, etc. While you observe attacks from all around the world, you may have a few interested parties who want to receive and handle reports about their networks. In such cases you need to sort the information out.

Can you think of other situations where automation and scripting may help you?

This exercise will let you practice your skills in the fast and automated or semi-automated analysing of logs and guide you through some tools than can be useful in these tasks.

You can find a lot of lightweight useful tools in the standard Linux shell. Some of the most commonly used are:

- cat - concatenate files and print on the standard output
- head - output the first part of files
- tail - output the last part of files
- grep, egrep - print lines matching a pattern
- sort - sort lines of text files
- cut - remove sections from each line of files
- awk - pattern scanning and processing language
- netcat - reads and writes data across network connections

Their documentation is available by typing: man command_name at the command prompt.

For more advanced processing you can use powerful programming languages like python and perl with lots of ready text-manipulation routines.

The text file 24022007.txt contains netflow logs from a DDoS attack. Although this is a UDP flood to various ports and the source hosts are likely spoofed, you may decide to verify whether this traffic was observed at origin and you happen to have good contacts with CERT teams in Poland and Turkey.

The log file format is as follows (columns separated with whitespaces):

	Column	Description
	1	Date
	2	Time
	3	Duration
	4	Protocol
	5	Source IP address:port
	6	"->"
	7	Destination IP address:port
	8	Number of packets transmitted
	9	Number of bytes transmitted
	10	Number of aggregated flows

Use the tools to dig some useful information out of this bulk data.

2 Ecercise Task

2.1 Task 1 Locating unique interesting hosts

Generate a list of unique attacking IP addresses. How many distinct source hosts were taking part in the attack? (Assume that attacking packets = UDP packets.)

Hint: sort offers an option to remove repeated lines from output. You can count lines, characters, etc, in a text file with word count .

2.2 Task 2 Geolocation

Team Cymru (http://www.team-cymru.com/) offers an IP to ASN mapping service. Use this service to find attacking IP addresses assigned to Poland and Turkey.

A detailed description of the service is available at http://www.team-cymru.org/Services/ip-to-asn.html and additional instructions can be obtained with a command:

$ whois -h whois.cymru.com help

Make sure you read the instructions and policies published on the webpage.

Hints: Use bulk query over whois protocol. You will need to enable the display of the country codes in the output.

2.3 Task 3 Looking further

While the attack consists of UDP packets to (apparently) random high ports, there are some other flows that stand out. Can you find them?

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