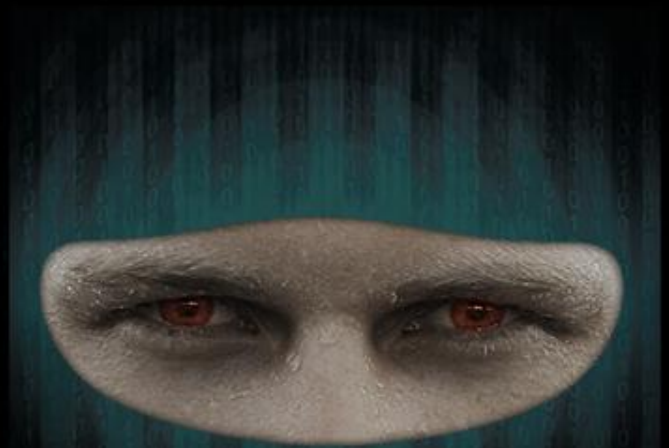


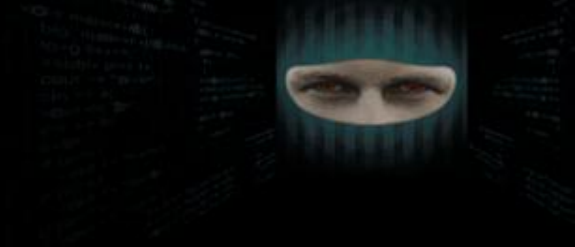
SHADOWSERVER REPORTS AUTOMATED TOOL

Viktor Janevski

Supervisor: Sebastian Lopienski
Dept.: IT-DI-CSO

Thursday, 18 August 2016

CERN openlab

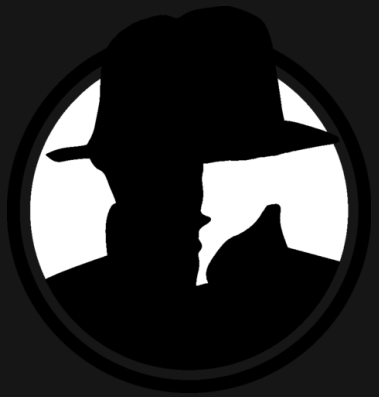


#1
WHAT?

#2
WHY?

#3
HOW?

What is Shadowserver?



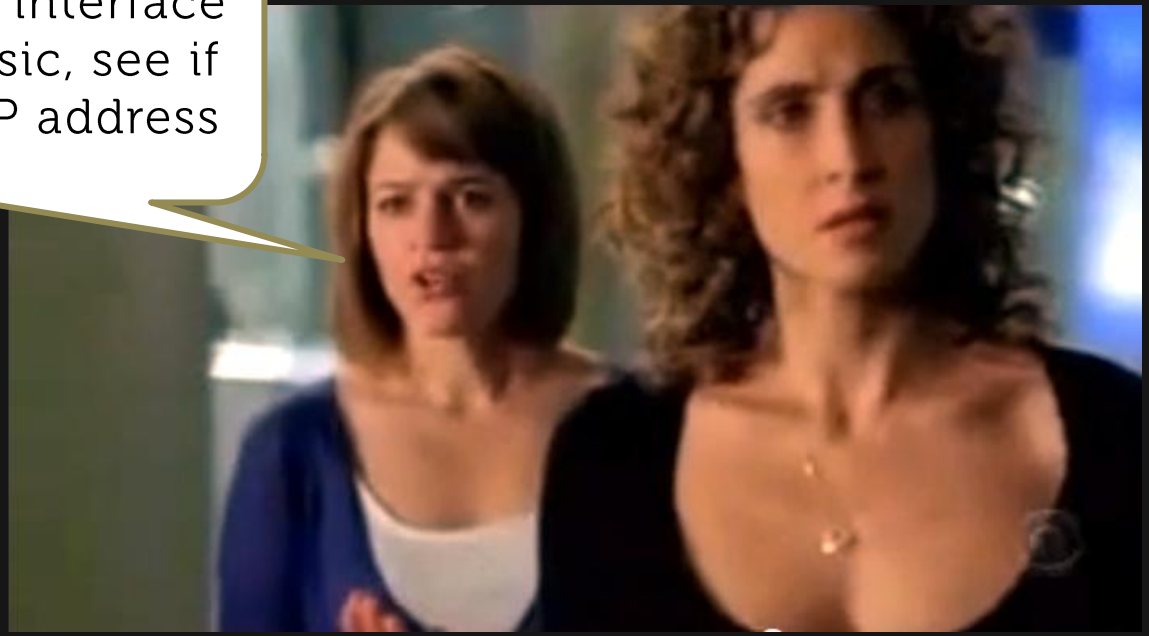
- external non-profit organization
- free scanning of networks
- looks for security issues and vulnerabilities
- sends periodical reports to the subscribers, on-demand

Sample report

	A	B	C	E	F	G	H	I	J	K	L	M	N	O
1	timestamp	ip	port	tag	handshake	asn	geo	region	city	cipher_su	ssl_poodle	cert_length	subject_common_name	issuer_common_name
2	2016-07-26 02:19:00	128.142.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	MEYRIN	TLS_ECDH	Y	2048	tile-in-one.cern.ch	CERN Grid Certification Authority
3	2016-07-26 02:28:24	128.142.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	MEYRIN	TLS_ECDH	Y	2048	mcplots4cms.cern.ch	mcplots4cms.cern.ch
4	2016-07-26 03:02:36	188.184.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	MEYRIN	TLS_ECDH	Y	2048	fts3devel04.cern.ch	fts3devel04.cern.ch
5	2016-07-26 03:36:32	128.142.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	MEYRIN	TLS_ECDH	Y	2048	indico-jacow.cern.ch	Symantec Class 3 Secure Server CA - G
6	2016-07-26 08:40:18	128.142.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	MEYRIN	TLS_ECDH	Y	2048	fts3devel05.cern.ch	fts3devel05.cern.ch
7	2016-07-26 09:34:51	188.185.xxx.yyy	443	ssl-poodle	TLSv1.2	61339	CH	GENEVE	MEYRIN	TLS_ECDH	Y	4096	aipanda093.cern.ch	CERN Grid Certification Authority
8	2016-07-26 09:52:16	137.138.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	PETIT-LAN	TLS_RSA_\	Y	2048	ams.cern.ch	CERN Trusted Certification Authority
9	2016-07-26 10:52:02	128.142.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	MEYRIN	TLS_ECDH	Y	2048	3f43f5c20d23	3f43f5c20d23
10	2016-07-26 10:56:16	137.138.xxx.yyy	443	ssl-poodle	TLSv1.0	513	CH	GENEVE	MEYRIN	TLS_RSA_\	Y	1024	wwweth.cern.ch	wwweth.cern.ch
11	2016-07-26 11:18:46	137.138.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	MEYRIN	TLS_RSA_\	Y	1024	pcuwxdata9.cern.ch	CERN Trusted Certification Authority
12	2016-07-26 11:54:37	128.142.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	MEYRIN	TLS_ECDH	Y	2048	fts3devel01.cern.ch	fts3devel01.cern.ch
13	2016-07-26 12:21:29	188.184.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	MEYRIN	TLS_ECDH	Y	2048	fts3devel02.cern.ch	fts3devel02.cern.ch
14	2016-07-26 12:39:57	188.184.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	MEYRIN	TLS_ECDH	Y	2048	fts3devel03.cern.ch	fts3devel03.cern.ch
15	2016-07-26 13:25:00	128.142.xxx.yyy	443	ssl-poodle	TLSv1.2	513	CH	GENEVE	MEYRIN	TLS_ECDH	Y	2048	vrcs.cern.ch	CERN Grid Certification Authority

How do they do it?

I'll create a GUI interface using Visual Basic, see if I can track an IP address



What do we want?

- automated tool
- fetch the e-mails and extract all needed data
- handle repeated reports for the same machine
- deal with known false positives and whitelist them
- filter out non-CERN hosts
- notify devices owners

Why not manually?

Login to the e-mail account

Open each mail

Download the attachment

Extract contents

Go through each line of the report

Look up each device in LanDB

Compare IP addresses to history

React on the previously unseen issues

Tedious

Repetitive

Time-consuming

which leads to

IMPORTANT THINGS BEING MISSED

What are the results?

1. detailed report about the execution of the tool and its results

2. whitelisting per device and per security issue type – limited amount of time or forever

3. managing the whitelist information – adding, updating, removing

Sample output report (summary)

```
==============
SUMMARY REPORT:
==============

Total number of issues: 21
Number of issues that are new or not recently reported: 0
Number of issues that have recently been processed: 19
Number of whitelisted devices found: 1
Number of devices not registered in LanDB: 1
```

Sample output report (manual handles)

```
================================
REPORTS TO BE HANDLED MANUALLY:
================================

ntp: 192.16.xxx.yyy - device NAME1
    Previous report(s) older than 7 day(s) (last received on 2016-07-20 11:28:44)
    To notify the device owner, please run:
        cert ssdb device-notify --device NAME1 --template vulnerable-generic --escalation 1 --batch --batch -D DATE=2016/07/27 --
        text "Vulnerability of type ntp was detected on port 123, reported to CERN by an external source.
Please find more details about this type of vulnerability at: https://www.shadowserver.org/wiki/pmwiki.php/Services/NTP-Version
"

ssl_poodle: 188.185.xxx.yyy - device NAME2
    No previous reports.
    To notify the device owner, please run:
        cert ssdb device-notify --device NAME2 --template vulnerable-generic --escalation 1 --batch --batch -D DATE=2016/07/27 --
        text "Vulnerability of type ssl_poodle was detected on port 443, reported to CERN by an external source.
Please find more details about this type of vulnerability at: https://www.shadowserver.org/wiki/pmwiki.php/Services/Ssl-Scan
"
```

Sample output report (unknown devices)

```
================
UNKNOWN DEVICES:
================

netbios: 192.91.xxx.yyy - device unknown
    Device not registered in LanDB => ignoring
```

Sample output report (recent issues)

```
==========================================
ISSUES RECENTLY REPORTED BY SHADOWSERVER:
==========================================

ntp: 192.65.xxx.yyy - device name NAME1
    Device whitelisted for report ntp (until 2016-08-01 11:28:12) => ignoring
    Device last report for ntp was 4 day(s) ago (on 2016-07-25 11:28:12)

ntp: 192.65.xxx.yyy - device name NAME2
    Device whitelisted for report ntp (until 2016-08-01 11:28:10) => ignoring
    Device last report for ntp was 4 day(s) ago (on 2016-07-25 11:28:10)
```

Sample output report (whitelisted)

```
====================
WHITELISTED DEVICES:
====================

ssl_poodle: 137.138.xxx.yyy - device name NAME1
    Device whitelisted for report type ssl_poodle (until 9999-12-31 23:59:59) => ignoring
    Device whitelisted for report type all (until 9999-12-31 23:59:59) => ignoring
```

How to use the whitelist?

1. Inserting a new device

```
$ ShadowserverReports.py whitelist insert -t TYPE/all -d DAYS/forever ip_address
```

2. Modifying the next notification time

```
$ ShadowserverReports.py whitelist modify_time -t TYPE/all -d DAYS/forever ip_address
```

3. Removing a device

```
$ ShadowserverReports.py whitelist remove -t TYPE/all ip_address
```

How to use the whitelist?

4. Listing certain devices

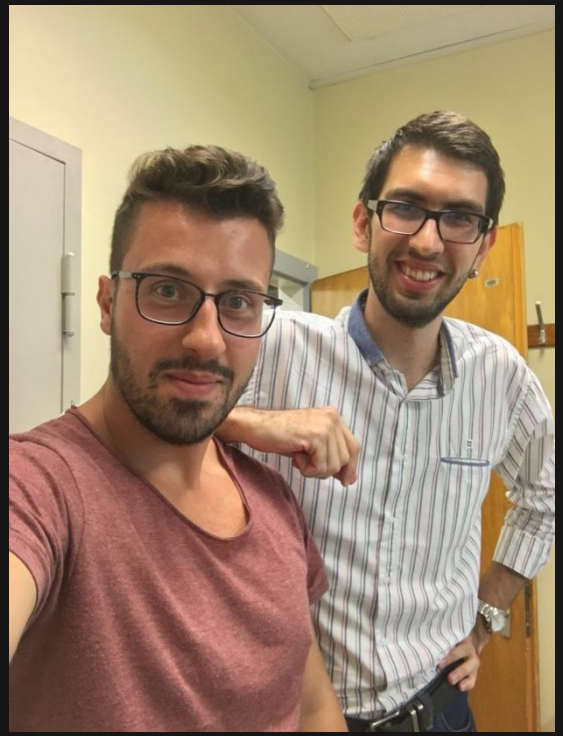
```
$ ShadowserverReports.py whitelist print -t TYPE/all -i
ip_address
```

5. Listing all devices

```
$ ShadowserverReports.py whitelist print
```

Acknowledgments

Thanks to the coolest officemate



Acknowledgments

- Thank you to Openlab for giving me this wonderful opportunity
- Thank you to Stefan Lueders and the Computer Security Office for accepting me and treating me as an equal part of their team
- Thank you to Sebastian Lopienski for providing support and constructive criticism
- Thank you to Vincent Brillaut and Liviu Valsan for their enormous patience with my endless questions
- Thank you to my parents for their endless encouragement
- Thank you to all the Summer students for being wonderful friends

Thank you for your attention

Viktor Janevski
E-mail: vikjan94@gmail.com
LinkedIn: https://www.linkedin.com/in/viktor-janevski-96ab02114