Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*

Shodan

Sandi Gec, Anže Jenšterle, Modic, David

18.11.2020

Outline

- Shodan overview
- Search results and data representation
- Benefits for the course INFOSEC
- The biggest data exposures uncovered through Shodan
- How to make a *Shodan.io* account
- Practical exercises
- Scientific overview
- Additional information
- Homework IV.

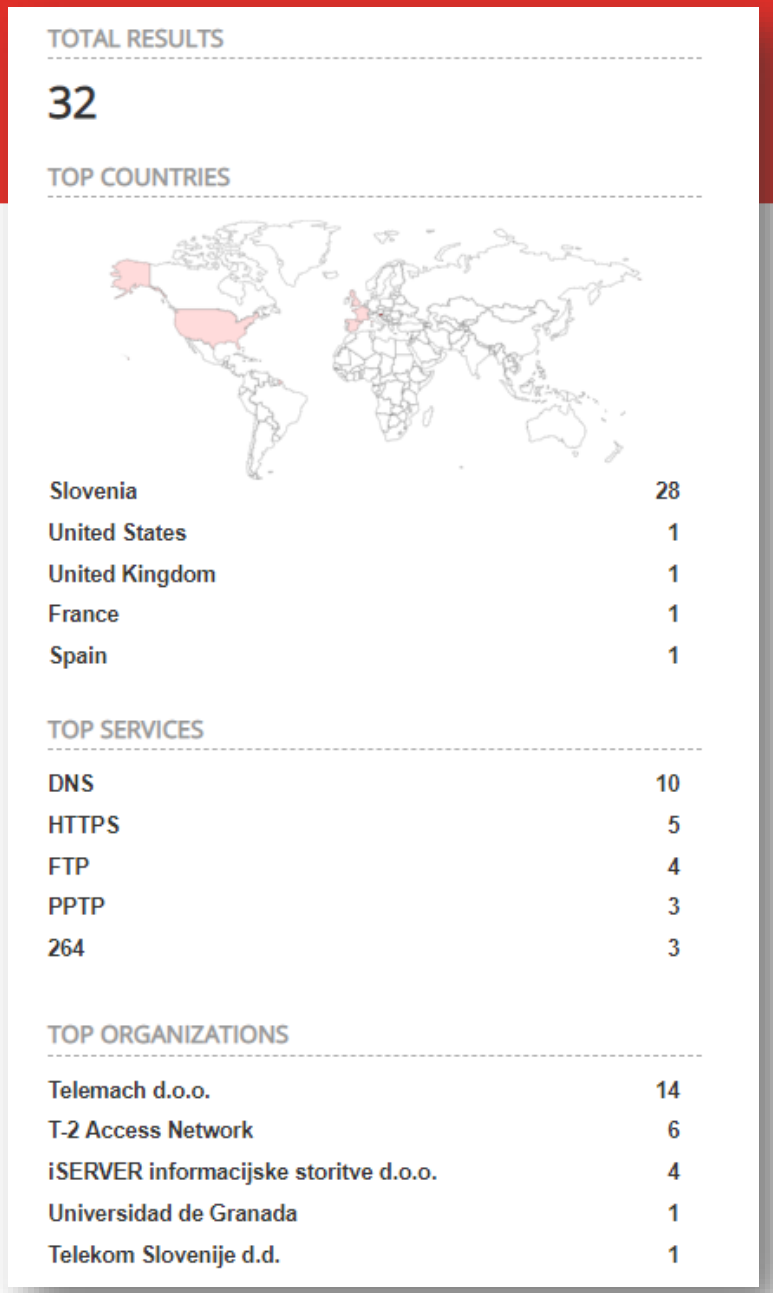
david.modic@fri.uni-lj.si

Shodan overview

- Shodan is a search engine for hackers and it has been even called "**the world's most dangerous search engine**".
- It was developed by John Matherly in **2009**, and unlike other search engines, it looks for specific information that can be invaluable to hackers.
- Shodan is pretty much like Google, but instead of showing you fancy images and rich content / informative websites, it will show you things that are more related to the interest of IT security researchers like **SSH**, **FTP**, **SNMP**, **Telnet**, **RTSP**, **IMAP** and **HTTP server** banners and public information.

Shodan overview

- Example of a search string: „Ljubljana“ →
- Shodan users are not only able to reach **servers, webcams and routers**.
- It can be used to scan almost anything that is connected to the internet (e.g. traffic lights systems, home heating systems, water park control panels, water plants, nuclear power plants, and much more).



david.modic@fri.uni-lj.si

Search results and data representation

- The main search result unit is the **banner**:
  - **data**: the main response from the service itself
  - **ip_str:** IP address of the device
  - **port:** port number of the service
  - **org:** the organization that owns this IP space
  - **location.country_code:** the country where the device is located

193.2.11.79

dedibuntu.zrc-sazu.si
ARNES
Added on 2019-03-31 06:01:27 GMT
Slovenia, Preserje

```
HTTP/1.1 200 OK
Date: Sun, 31 Mar 2019 06:01:27 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Tue, 27 Nov 2018 11:40:24 GMT
ETag: "223-57ba3ea4eb2d9"
Accept-Ranges: bytes
Content-Length: 547
Vary: Accept-Encoding
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<title>Welcome ...
```

- Additional gathered data is the **device metadata** that may contain information such as: geographic location, hostname, opera SSH props., SSL props., etc.

- Banners information from **IPv6*** accessible devices.

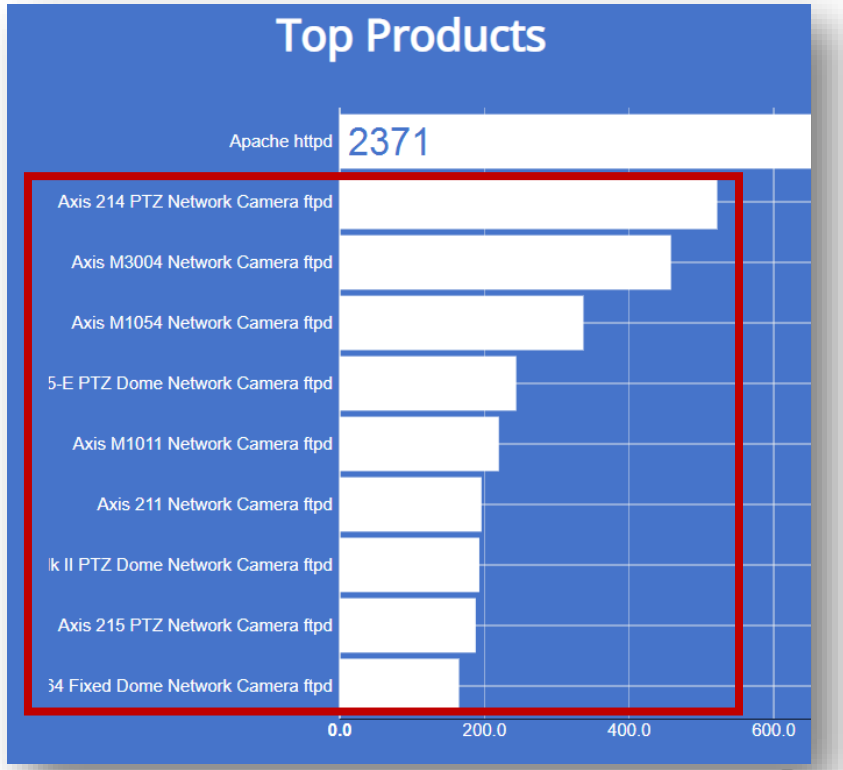
- <u>How is the data actually gathered?</u>
  - With Shodan crawlers (24/7) that update the DB in real-time.

*from october 2015

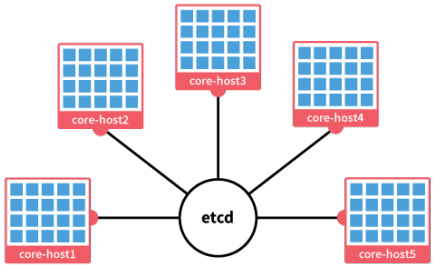
david.modic@fri.uni-lj.si

Benefits for the course INFOSEC

- Shodan is one of the top reconnaissance and intel gathering tool.
- Usefull as a tool for OSINT:
  - performing penetration tests,
  - Searching for devices (e.g. routers, webcams, etc.), services.
  - Find specific targets with filters (e.g. city, country, geo, os, port, ...)
- Example: Search result for active cameras of the company Axis.

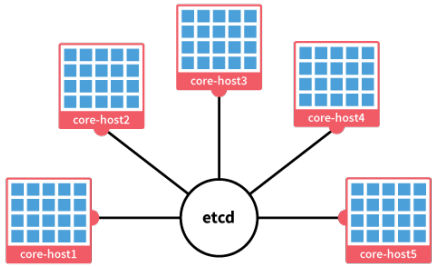


The biggest data exposures uncovered through Shodan



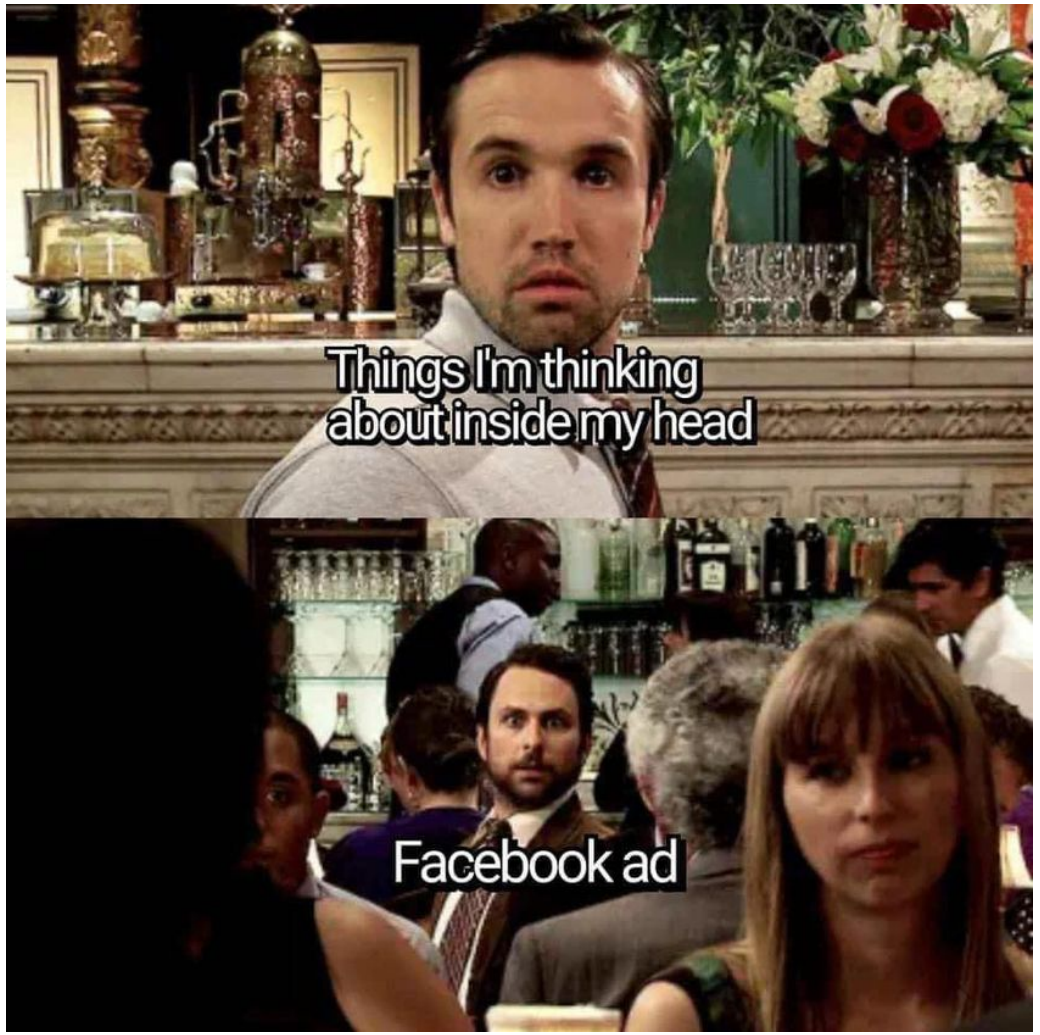
- Database of 560 Million Previously Compromised Credentials
  - During a regular security audit of Shodan, researchers at the **Kromtech Security Center** came across **313** large databases with **more than 1 gigabyte** and in some cases several terabytes of data. One of those databases was a MongoDB instance with default configuration enabled. The result? discovered more than **560 million** email addresses and passwords.
- 13 Million Users' Account Credentials Potentially Exposed
  - Chris Vickery queried Shodan for vulnerable MongoDB instances listening on port 27101 for incoming connections. He then took this information and posted it into MongoVue (a GUI interface tool). In so doing, he came across a security issue on the web servers for **MacKeeper**, software developed by **Kromtech** ; DB access without authentication.

The biggest data exposures uncovered through Shodan



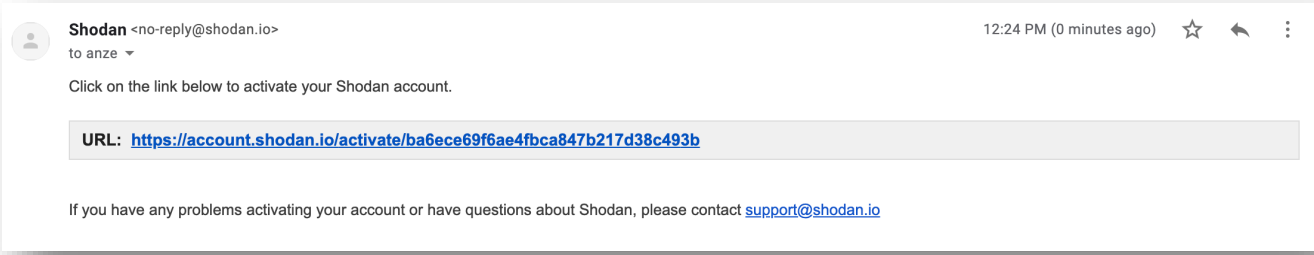
- 750 MB from Thousands of etcd Servers Disclosed
  - Researcher Giovanni Collazo conducted a simple search of Shodan by querying "**etcd**," a type of database which stores passwords, configuration settings and other sensitive information across a cluster of machines. The search yielded **2284 etcd** servers open to the web (+disabled authentication).
- Tens of Thousands of Computers Infected by DoublePulsar
  - In April 2017, the Shadow Brokers group published a dump of **internal NSA documents** containing exploits, hacking tools, and attack code. Among the leaked resources was backdoor vulnerability **DoublePulsar**. The infection was spread on **50 000 machines**.
- 5.12 PETABYTES of Data Uncovered
  - An analysis conducted by Shodan uncovered nearly **4500** servers with the **Hadoop Distributed File System (HDFS), (Common Vulnerabilities and Exposures (CVE): CVE-2016-6811)**. That's far fewer than the 47,820 MongoDB servers detected online. But while the MongoDB instances exposed 25 terabytes of data, the HDFS servers compromised **5120 terabytes**. That's 5.12 petabytes of information. (publish data: 4.11.2017, update date: 5.10.2018)

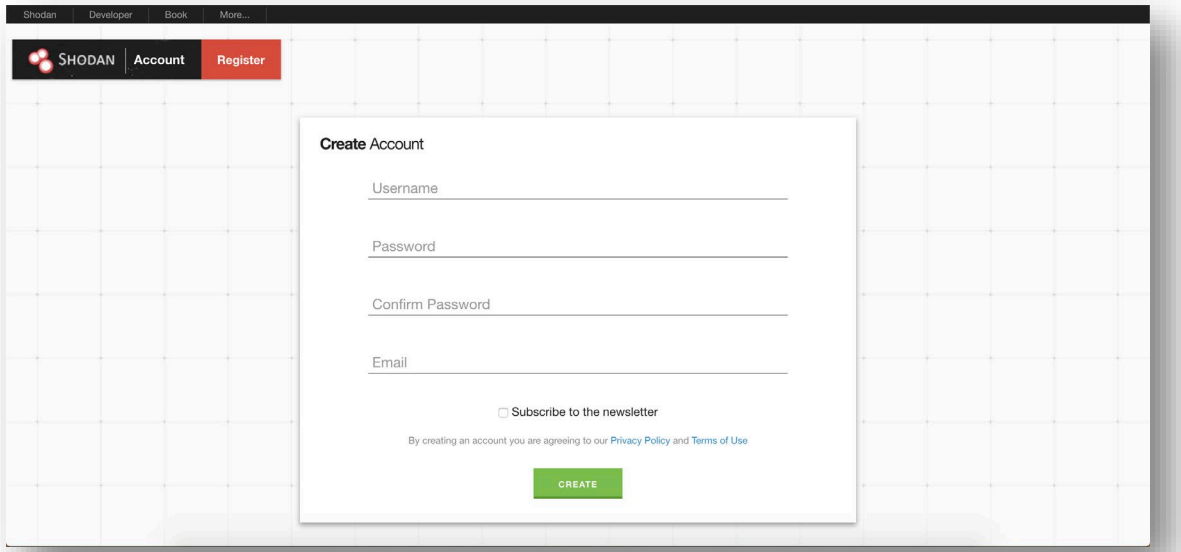
Practicals



How to make a Shodan.io account

- https://account.shodan.io/register
- Enter the details (no personal id data, except email)
  - Use your *student.uni-lj.si* email for academic status
- Confirm your email
- Write to academic@shodan.io for an academic account





Shodan Cheat Sheet

- More at: https://thor-sec.com/cheatsheet/shodan/shodan_cheat_sheet/
- **port:** Look for an open port (i.e. port:22).
- **net:** IP/CIDR (i.e. net:"193.2.1.0/24" for arnes).
- **Hostname:** „hostname“ (i.e. jagababa.crq.systems).
- **os:** operating system (i.e. os:"Windows").
- **city:** town (i.e. city:"Ljubljana").
- **country:** i.e. country:si.
- **geo:** gps coordinates (i.e. geo:42.9693,-74.1224)
- **org:** organisation (i.e. org:"University of Ljubljana").
- **before/after:** date range.
- **has_screenshot:true** Only hits with a screenshot.
- **title:** Look for specific string in title of a page (i.e. title:“David Modic“ or title:"+tm01+")

More at: https://thor-sec.com/cheatsheet/shodan/shodan_cheat_sheet/

Exercises

1. Find me a webcam in Slovenia, with a screenshot.
   -
2.
   -
3.
   -

- **port:** open port (i.e. port:22).
- **net:** IP/CIDR (i.e. net:"193.2.1.0/24").
- **Hostname:** „hostname“
- **os:** i.e. os:"Windows"
- **city:** town (i.e. city:"Ljubljana").
- **country:** i.e. country:si.
- **geo:** (i.e. geo:42.9693,-74.1224)
- **org:** i.e. org:"University of Ljubljana".
- **before/after:** date range.
- **has_screenshot:true**
- **title:** i.e. title:“David Modic“

More at: https://thor-sec.com/cheatsheet/shodan/shodan_cheat_sheet/

Exercises

1. Find me a webcam in Slovenia, with a screenshot.
   - webcamxp country:si OR webcam country:si
2. Find me devices in Slovenia, that have "default password" on a web page.
   -
3.
   -

- **port:** open port (i.e. port:22).
- **net:** IP/CIDR (i.e. net:"193.2.1.0/24").
- **Hostname:** „hostname"
- **os:** i.e. os:"Windows"
- **city:** town (i.e. city:"Ljubljana").
- **country:** i.e. country:si.
- **geo:** (i.e. geo:42.9693,-74.1224)
- **org:** i.e. org:"University of Ljubljana".
- **before/after:** date range.
- **has_screenshot:true**
- **title:** i.e. title:"David Modic"

More at: https://thor-sec.com/cheatsheet/shodan/shodan_cheat_sheet/

Exercises

1. Find me a webcam in Slovenia, with a screenshot.
   - webcamxp country:si OR webcam country:si
2. Find me devices in Slovenia, that have "default password" on a web page.
   - "default password" country:si
3. Find me a machine with remote desktop on in Slovenia.
   -

- **port:** open port (i.e. port:22).
- **net:** IP/CIDR (i.e. net:"193.2.1.0/24").
- **Hostname:** „hostname"
- **os:** i.e. os:"Windows"
- **city:** town (i.e. city:"Ljubljana").
- **country:** i.e. country:si.
- **geo:** (i.e. geo:42.9693,-74.1224)
- **org:** i.e. org:"University of Ljubljana".
- **before/after:** date range.
- **has_screenshot:true**
- **title:** i.e. title:"David Modic"

More at: https://thor-sec.com/cheatsheet/shodan/shodan_cheat_sheet/

Exercises

1. Find me a webcam in Slovenia, with a screenshot.
   - webcamxp country:si OR webcam country:si
2. Find me devices in Slovenia, that have "default password" on a web page.
   - "default password" country:si
3. Find me a machine with remote desktop on in Slovenia.
   - RDP country:si OR VNC country:si

- **port:** open port (i.e. port:22).
- **net:** IP/CIDR (i.e. net:"193.2.1.0/24").
- **Hostname:** „hostname"
- **os:** i.e. os:"Windows"
- **city:** town (i.e. city:"Ljubljana").
- **country:** i.e. country:si.
- **geo:** (i.e. geo:42.9693,-74.1224)
- **org:** i.e. org:"University of Ljubljana".
- **before/after:** date range.
- **has_screenshot:true**
- **title:** i.e. title:"David Modic"

More at: https://thor-sec.com/cheatsheet/shodan/shodan_cheat_sheet/

Exercises II.

4. Find me a traffic light in the world, where I can turn on the red light remotely.
   -
5.
   -
6.
   -

- **port:** open port (i.e. port:22).
- **net:** IP/CIDR (i.e. net:"193.2.1.0/24").
- **Hostname:** „hostname“
- **os:** i.e. os:"Windows"
- **city:** town (i.e. city:"Ljubljana").
- **country:** i.e. country:si.
- **geo:** (i.e. geo:42.9693,-74.1224)
- **org:** i.e. org:"University of Ljubljana".
- **before/after:** date range.
- **has_screenshot:true**
- **title:** i.e. title:“David Modic“

More at: https://thor-sec.com/cheatsheet/shodan/shodan_cheat_sheet/

Exercises II.

4. Find me a traffic light in the world, where I can turn on the red light remotely.
   - mikrotik streetlight
5. Find me non-protected file servers in Slovenia.
   -
6.
   -

- **port:** open port (i.e. port:22).
- **net:** IP/CIDR (i.e. net:"193.2.1.0/24").
- **Hostname:** „hostname“
- **os:** i.e. os:"Windows"
- **city:** town (i.e. city:"Ljubljana").
- **country:** i.e. country:si.
- **geo:** (i.e. geo:42.9693,-74.1224)
- **org:** i.e. org:"University of Ljubljana".
- **before/after:** date range.
- **has_screenshot:true**
- **title:** i.e. title:“David Modic“

More at: https://thor-sec.com/cheatsheet/shodan/shodan_cheat_sheet/

Exercises II.

4. Find me a traffic light in the world, where I can turn on the red light remotely.
   - mikrotik streetlight
5. Find me non-protected file servers in Slovenia.
   - "Authentication: disabled" port:445 country:si
6. Find me unprotected machine in Slovenia with remote desktop (no authentication).
   -

- **port:** open port (i.e. port:22).
- **net:** IP/CIDR (i.e. net:"193.2.1.0/24").
- **Hostname:** „hostname“
- **os:** i.e. os:"Windows"
- **city:** town (i.e. city:"Ljubljana").
- **country:** i.e. country:si.
- **geo:** (i.e. geo:42.9693,-74.1224)
- **org:** i.e. org:"University of Ljubljana".
- **before/after:** date range.
- **has_screenshot:true**
- **title:** i.e. title:“David Modic“

More at: https://thor-sec.com/cheatsheet/shodan/shodan_cheat_sheet/

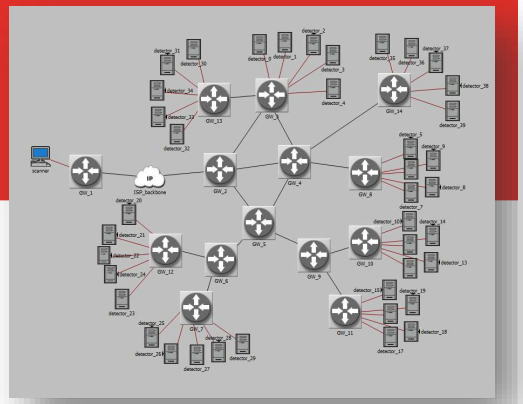
Exercises II.

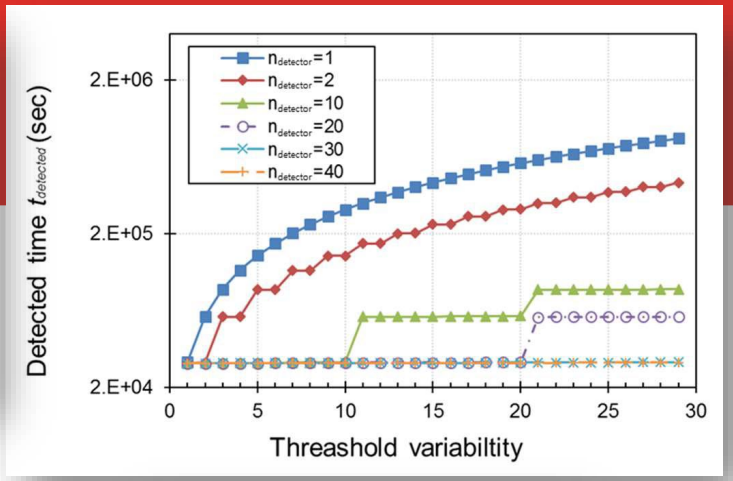
4. Find me a traffic light in the world, where I can turn on the red light remotely.
   - mikrotik streetlight
5. Find me non-protected file servers in Slovenia.
   - "Authentication: disabled" port:445 country:si
6. Find me unprotected machine in Slovenia with remote desktop (no authentication).
   - "authentication disabled" "RFB 003.008" country:si

- **port:** open port (i.e. port:22).
- **net:** IP/CIDR (i.e. net:"193.2.1.0/24").
- **Hostname:** „hostname“
- **os:** i.e. os:"Windows"
- **city:** town (i.e. city:"Ljubljana").
- **country:** i.e. country:si.
- **geo:** (i.e. geo:42.9693,-74.1224)
- **org:** i.e. org:"University of Ljubljana".
- **before/after:** date range.
- **has_screenshot:true**
- **title:** i.e. title:“David Modic“

Miscellania

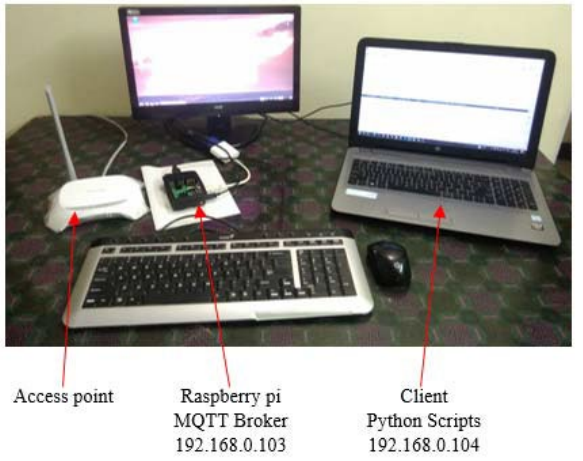
Scientific overview





- S. Lee, S. Shin and B. Roh, "**Abnormal Behavior-Based Detection of Shodan and Censys-Like Scanning**," 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, 2017, pp. 1048-1052.
- T. Phan, D. M. Krum and M. Bolas, "**ShodanVR: Immersive visualization of text records from the Shodan database**," 2016 Workshop on Immersive Analytics (IA), Greenville, SC, 2016, pp. 31-31.
- V. J. Ercolani, M. W. Patton and H. Chen, "**Shodan visualized**," 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, 2016, pp. 193-195.*
- M. S. Harsha, B. M. Bhavani and K. R. Kundhavai, "**Analysis of vulnerabilities in MQTT security using Shodan API and implementation of its countermeasures via authentication and ACLs**," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, 2018, pp. 2244-2250.
- H. Al-Alami, A. Hadi and H. Al-Bahadili, "**Vulnerability scanning of IoT devices in Jordan using Shodan**," 2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS), Amman, 2017, pp. 1-6.

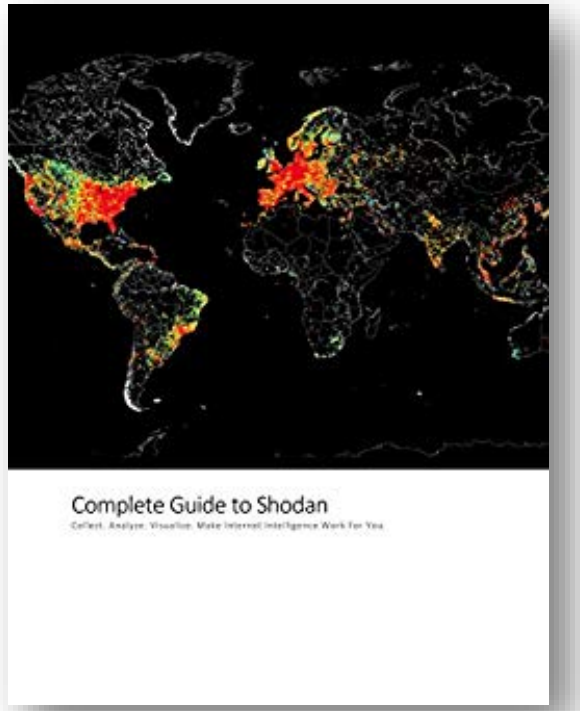
Modularity of Network



*Supervisory Control and Data Acquisition (SCADA)

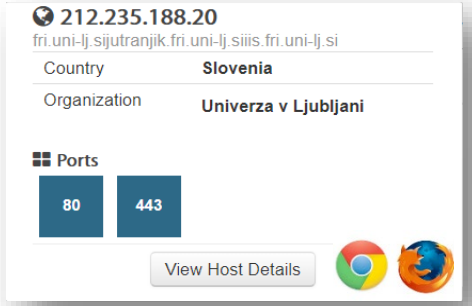
Additional information

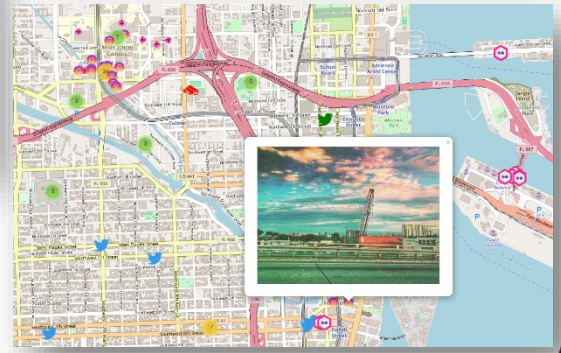
- Books and papers:
  - Matherly, John. "Complete Guide to Shodan." Shodan, LLC (2016-02-25) (2015).
  - Genge, B., and Enăchescu, C. (2016) ShoVAT: Shodan based vulnerability assessment tool for Internet facing services. Security Comm. Networks, 9: 2696– 2714.
  - Prakhar Prasad: Mastering Modern Web Penetration Testing (Paperback), October 28, 2016.



- Web based content:
  - Official Web page: https://www.shodan.io/
  - Shodan basic tutorial: https://danielmiessler.com/study/shodan/
  - REST API documentation: https://developer.shodan.io/api

- Tools:
  - Shodan Chrome or Firefox plugin
  - Shodan Ship Tracker: https://shiptracker.shodan.io/
  - Keep track of internet exposed devices: https://monitor.shodan.io/
  - Ƙamerka 2.0 aka FIST (Flickr, Instagram, Shodan, Twitter): https://github.com/woj-ciech/kamerka
  - LeakLooker: Find open databases with Shodan: https://github.com/woj-ciech/LeakLooker





david.modic@fri.uni-lj.si

Homework IV.

Prerequisite: Visit Shodan Web page and create an **academic** account (use your FRI student/employee e-mail).

1. Search for organization „University of Ljubljana“ limited to geographical location of Slovenia. List all information that you can gather from the results. Use filters (LINK).
   - Example search: **city:“Ljubljana“ os:“Windows“**

2. **(1) S**earch for servers vulnerable to Heartbleed that are running on AWS. Heartbleed (Common Vulnerabilities and Exposures (CVE): **CVE-2014-0160. (2)** Find a vulnerability that intrigues you from the Shodan API JSON result (from year 2018 till today) or simply search it on CVE Web page. Use at least one additional filter to narrow your result.
   Example search: **vuln:"CVE-2014-0160" country:it**

3. Find interesting results at non-urban location in Slovenia or abroad (e.g. IoT devices on public roads). List them based on the IoT device type (e.g. camera, X sensor,..) if you are able to categorize them. For the task help yourself with Shodan map engine: https://maps.shodan.io and a short walkthrough.

If you find any vulnerability or entity exposed **report the finding to me. No active measures!**

Send it to me by 23.11.2020 @ 12:00 through učilnica.

david.modic@fri.uni-lj.si