ETH zürich

Discussion exercise sheet 10

Marc-Philippe Bartholomä
Student Assistant for Network Security 2020
19 November 2020, At home

Introduction

- Take pen and paper and write down the manufacturer and model of:
  - All routers in your home network
  - The internet modem (if separate)
  - A networked surveillance camera (if any)
  - A smart doorbell (if any)

- Zoom poll (with results)

Students know their router: manufacturer: 2, no, it's managed by the ISP: 1, no: 4

Students know their internet modem: manufacturer: 1, no separate modem: 4, no: 2

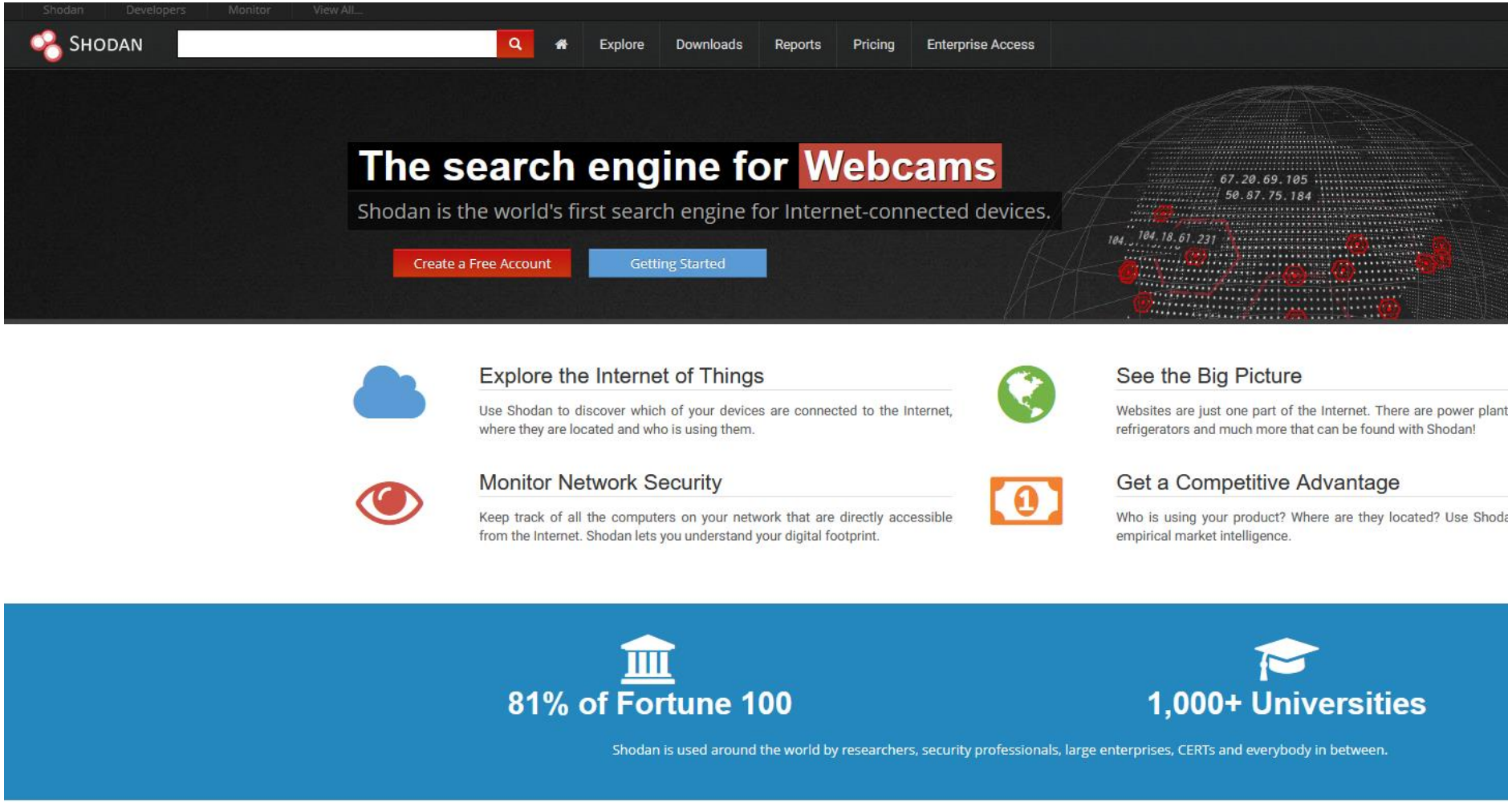
No student owns either of the smart devices

Only one student out of seven indicated that he updated the router manually within the last year.

(The other components of this question were inconclusive)

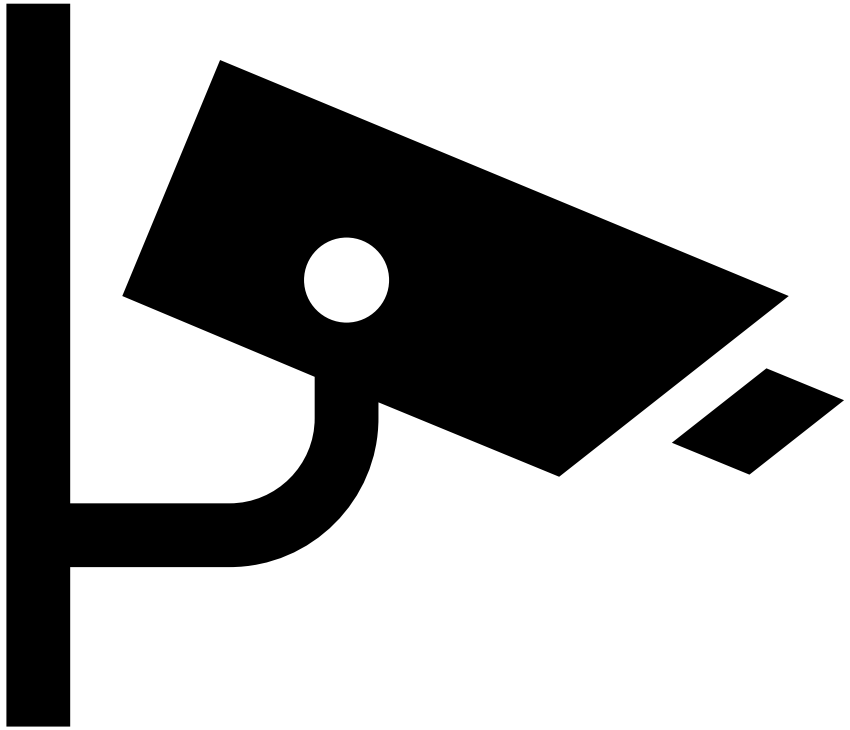
Question 1 – Shodan

- Question: Negative Aspects

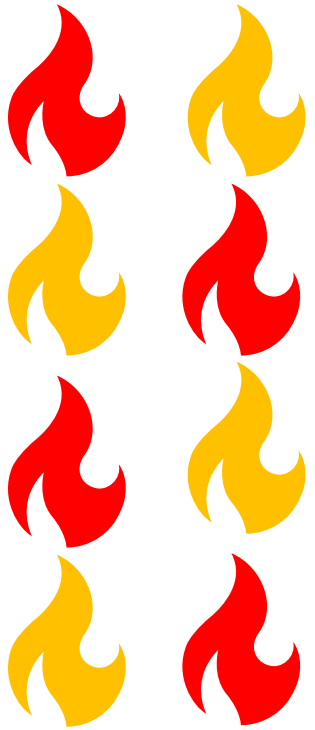


Question 1 – IoT Cameras

- Question: Camera behind NAT / Firewall



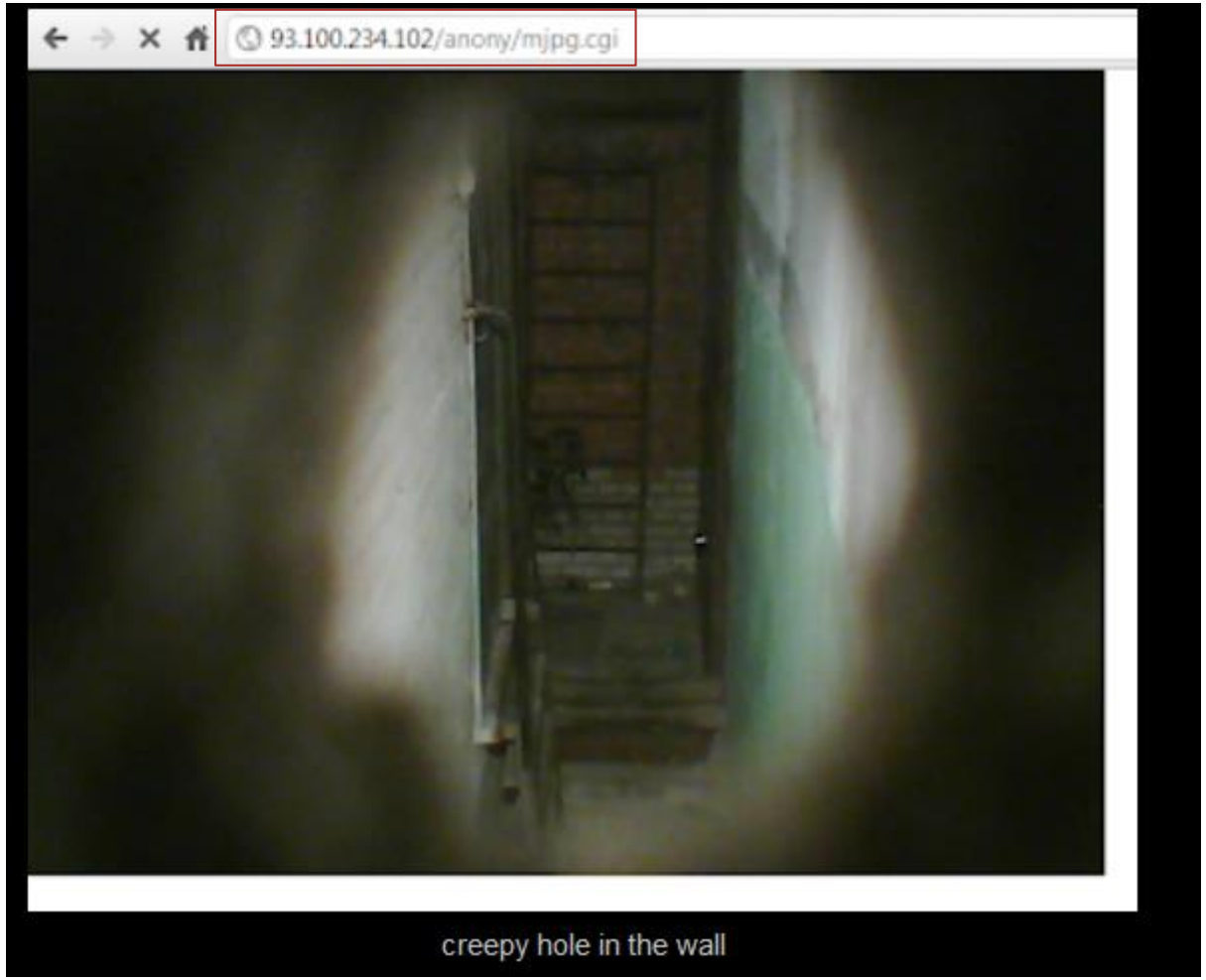
Port forwarding?
Generally, reduction of attack surface



Question 1 – IoT Cameras

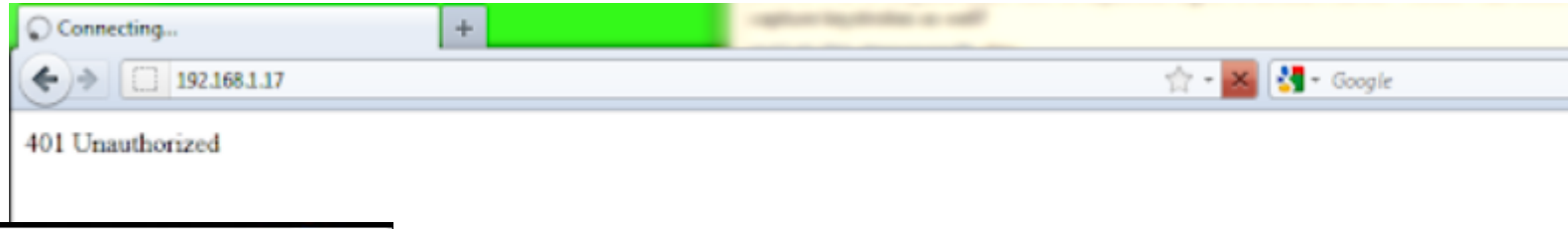
- Question: Vulnerability in Trendnet TV-IP-110W

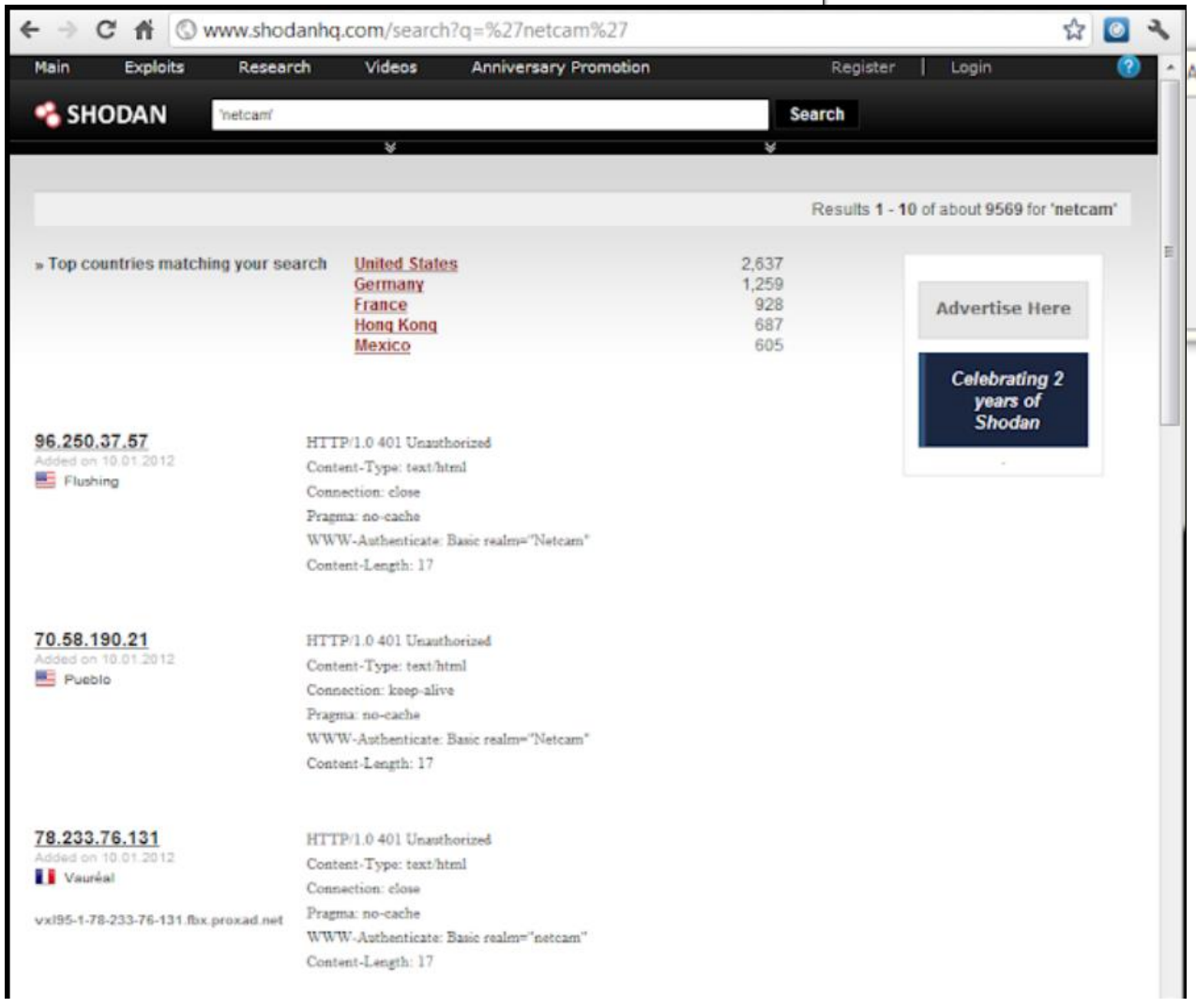
Stream available without Authentication

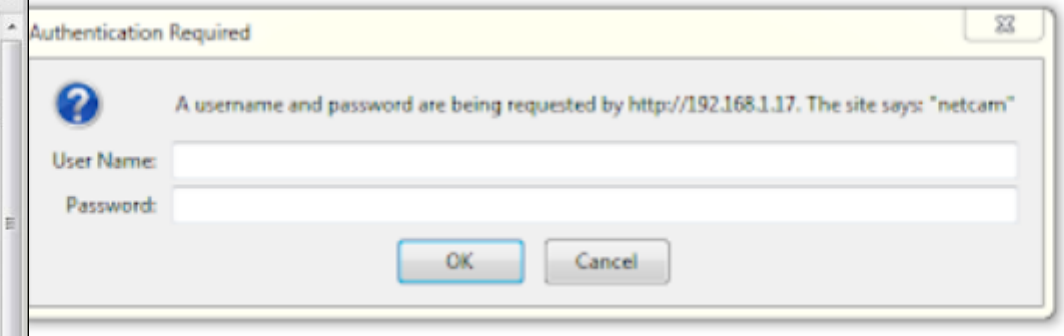


Question 1 – IoT Cameras

- Question: Shodan Abuse







Question 1 – IoT Cameras

- Question: Fixing strategy

- Released update and invited customers to update. Is this enough?

- Zoom poll:
- If there is a vulnerability in a device that you own, what would you want the manufacturer to do?

Update automatically: 1, Notify and allow cancellation: 4, Prompt and wait for user decision: 4

- Assuming the device provides all options regarding updates, which one should be the default?

Update automatically: 4, Notify and allow cancellation: 3, Prompt and wait for user decision: 3

- In case of a severe security vulnerability, like the one in Trendnet Cameras, should the manufacturer disregard the update setting?

Yes: 4, Only if manual wasn’t the default setting: 2, No: 4

Question 1 – IoT Security Standards

Pros

Cons

Question 1 – Vendor Reaction

- "We are scrambling to discover how the code was introduced and at this point it seems like a coding oversight" said Zak Wood, Trendnet’s director of marketing.

Bonus Material IoT

- https://www.troyhunt.com/iot-unravelled-part-3-security/

Supply Chain Attack

Question 2 – Supply Chain Attack

Question: Capabilities & Detection?

- Connected to the Baseboard Management Controller
  - BMC can reinstall OS or restart machine
  - Implant can modify BMC firmware
  - Basically full access
- Runs below OS
  - Direct connection to memory
  - Direct connection to network card

https://www.servethehome.com/explaining-the-baseboard-management-controller-or-bmc-in-servers/

Question 2 – Supply Chain Attack

- Question: Historical Evidence

(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away… In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are ***intercepted***. Next, they are ***redirected to a secret location*** where Tailored Access Operations/Access Operations (AO – S326) employees, with the support of the Remote Operations Center (S321), enable the ***installation of beacon implants*** directly into our targets' electronic devices. These devices are then re-packaged and ***placed back into transit*** to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Question 2 – Low level security

Question: In your devices?

- Zoom poll: Is your laptop equipped with hardware with similar capabilities as the board management unit?
- Yes, it has Intel Management Engine: 2
- I don’t know, but probably yes: 5
- I don’t know, but probably no: 1

- Depending on the CPU vendor, you likely have either Intel ME or AMD Secure Technology

Your Questions