Security in Organizations (SIO)

Assignment 4 - 2021-2022

Goal:

- Discover online vulnerabilities and learn how to responsibly disclose them.

Instructions:

- This assignment must be completed by a team of two students.
- The assignment must be written with the Times New Roman font, in size 12pt, with normal spacing. The subtitles are in bold, and the margins must be all of size 2.5cm.
- The original numbering of the questions must be indicated for each answer.
- State your answers in a succinct and clear manner.

Deadline:

- Submit the assignment in a PDF document through Brightspace before **2021/11/11 23:59.**

If and only if you do not have a Brightspace access, you can submit your assignment by email to Anna Guinet (see SIO website) in a PDF document.

Introduction:

Shodan [1] is a search engine that interrogates devices connected to the Internet and retrieves banners with detailed information on these devices. Although the technique known as banner grabbing is not recent, Shodan makes it possible to perform this on a previously unseen scale. With this search engine, and with the application of certain filters, one is able to find devices that are unprotected and accessible through web interfaces such as routers, switches, and SCADA systems. Not all device owners are aware of the vulnerabilities caused by banner grabbing, which in its most basic form means that anyone can access a device that the owner thought was secure. Resetting, shutting down, changing settings, setting a password and locking out the owner are some of the possibilities if one has administrator access. Although not all devices are this accessible and are protected with login credentials, these credentials often start out as default settings which can be found in the manuals of these devices. This can be as simple as “admin/admin” or “admin/1234”, and although this is legal protection in that this requires either breaking through a security feature or assuming a false identity, actual security is negligible [2].

Rules:

In this assignment, you have to identify systems with inadequate security. Inadequacy here means that either there is no password protection, or the access can be obtained using a default password. During this assignment, there are a number of rules concerning the obtaining of access:

- Only devices within the Netherlands are allowed.

- For a default password, properly reference the documentation in which you found the default password.
- Do not perform any action to compromise the availability, the service or the integrity of the device.
- Only perform the minimal requirement to estimate of the impact of the device that is being compromised. For security cameras, if a stream is opened, immediately close the connection; if the possibility of opening a stream exists (e.g. 'click here to view'), do not open the stream.

Part 1:

A. Find two different devices in the Netherlands that have inadequate security. They must be of different types, different manufacturers, and different owners.
B. Explain how you found each device.
C. Present each device, and what do they control.
D. For each device, provide a screenshot (properly readable and nicely cropped) of the banner as depicted in Figure 1.
E. Explain what information is needed to obtain access.
F. Perform an assessment on each device that details the impact on the CIA triad.
G. Describe how each device can be used by malicious people.

At most one router/switch device may be submitted, because they are by far the easiest devices to find. The explanation and assessment should be at most two pages per device.

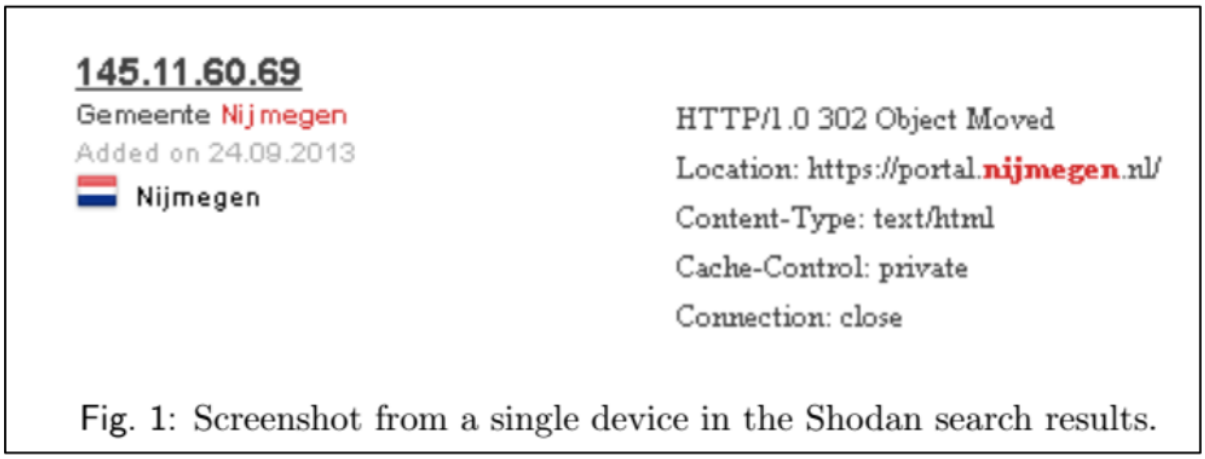

Fig. 1: Screenshot from a single device in the Shodan search results.

Part 2:

A. Based on the NCSC Responsible Disclosure Guideline [3], formulate in the form of bullet point, the most important rules a discloser (which, in this assignment, is you) must abide by.
B. For each device that you have found, identify their owners, and through responsible disclosure properly inform them of the vulnerability you have uncovered.
Afterwards, write down how you identified and found the owner of the device, and include your communications towards the owner, and their response, in your submission.
C. For each bullet that you have formulated on rules of disclosure, specify how you met this rule.

Important:

To prevent any owner from being contacted by numerous students, a channel in the category for the assignment 3 has been set in Discord. Please, go to Assignment 3 > #devices.

In this channel, you will report your student number and the one of your partner, clear information to identify each device, and the two organizations you have contacted in light of responsible disclosure. Thus, if you find a vulnerability and want to contact the owner, please refer to the thread first. If the device is already listed, you will have to find another vulnerability. This follows two principles:

1. First come, first serve.
2. Because this is a forum, the post history is available, thus do not "steal" a vulnerable device.

CALCULATION OF THE GRADE	
Part	Max. points
1. Vulnerable devices	4
2. Responsible Disclosure	5
SUM	**9**
Grade = (1 + sum_of_points) rounded to the nearest 0,5 point.	

#	**References**
[1]	https://www.shodan.io/
[2]	See "Wetboek van strafrecht Artikel 138ab" for details on how to obtain access to a computer one does not own, and the penalties that are applicable.
[3]	https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline