Security in Organizations: Assignment 4

Group number 27

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

Part 1

A. We found 2 devices, D1: 77.60.200.41 and D2: 13.73.150.124.

B. D1: We used the following query in shodan.io: *test test port:"80" country:nl*, which searches for generic test credentials over HTTP.

D2: We used the following query in shodan.io: *kibana content-length:217 country:NL*, which searches for Kibana dashboards accessible without authentication.

Both queries were found on:
https://www.osintme.com/index.php/2021/01/16/ultimate-osint-with-shodan-100-great-shodan-queries/ and modified to include the country.

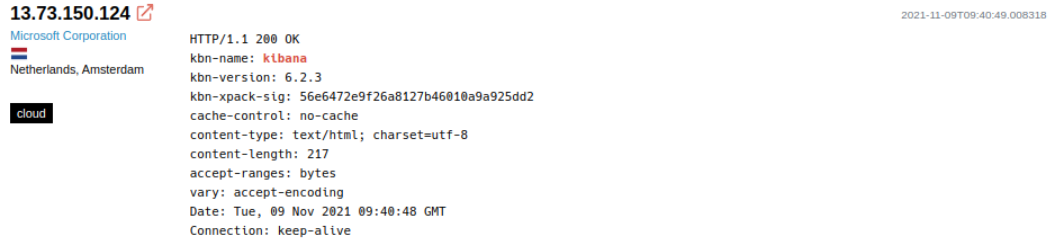
C. D1: This device is a camera system from a "De Plantenhal" in Oud-Beijerland, it displays the cameras from the building and gives access to older recordings and the log files of the system.

D2: This device is an Azure server hosting an Elasticsearch database and a Kibana frontend, which can explore and visualize the data in the database. A quick look at the data presented in Kibana reveals that the database is used for something related to booking hotels, because the data contains booking information or search queries for hotels.

D. D1:


```
HTTP/1.0 200 OK
Server: GeoHttpServer
Date: Tue, 09 Nov 2021 09:52:22 GMT
Content-type: text/html
Content-length: 5648
Authentication: test
Last-Modified: Tue, 09 Nov 2021 10:52:22 GMT
```

D2:



E. D1: The first thing that is needed is the brand of the device, which is geovision in this case. Geovision has a few default passwords based on the model of the device, most common is admin/admin. This information can be found in the manual (*Default IP Addresses and Login Settings of GeoVision Products* 2017).

D2: None, there is no authentication configured to access any of the data.

F. D1:
- Confidentiality: There is no confidentiality at all, as someone can use the default login credentials to get access to security cameras, to which they should not have Access.
- Integrity: Integrity is safe, since the attacker can not change anything with the default credentials, the credentials can only be used to access information, not to change it.
- Availability: The password of the admin account can be changed by an attacker, which would make it impossible for the user to get back into the system until an administrator has given access to the system.

D2:
- Confidentiality: There is no confidentiality because there is no authentication required to gain access to the data. Anyone who has the url can see the booking queries.
- Integrity: The integrity of the database is safe, because it seems that Kibana is configured in such a way that it is not possible to modify or delete the data inside the database. It is also not possible to change the configuration of Kibana inside the Kibana explorer. The database itself is not reachable outside Kibana.
- Availability: It is possible to delete the dashboards in Kibana, which does not delete any data in the database but it could be used by the owners of the systems to analyse the data.

G. D1: The cameras can be used to look into the store, this information can then be used to do criminal acts like breaking-and-entering and seeing when someone is close to parts of the store that the criminal wants to do criminal acts in.

D2: The data contains information about hotel bookings, which can be actual bookings or search queries. Each query also contains the client IP address, so an attacker can use this information to track someone and see where and when they will go.

Part 2

A.
- To notify the vulnerable party as soon as possible.
- To only abuse the vulnerability as much as is needed to confirm it without doing harm to the system.
- To make sure that only authorized people learn about the vulnerability, so it is not abused by someone that should not have access to it.
- To never destroy, break, harm or do any damage to the system.

B. D1: We first tried to find the owner using whois, but it only returned the ISP. We also looked up the location of the IP but it returned multiple provinces. We then used the camera feed to figure out which store we were looking at, because there was no other indication, we used the exterior camera to identify the street and the interior camera that was pointed at the door to determine which store it was, as there was a poster there with the name and logo on it.

D2: We could not find the real owner of this device. We tried to find the device using whois and we looked up the location of the IP address, but it only shows contact information of Microsoft who hosts the system, so we think it is running on a Microsoft Azure server. We could also not identify the owner in Kibana itself. So instead we contacted Microsoft.

We notified them by email, which can be found in the appendices. Unfortunately, we did not receive any reply to our emails before the deadline of the assignment. We decided to call the owner of D1 if we still haven't received a reply tomorrow.

C.
- We notified them as soon as we could, after finding the contact information.
- D1: We had to use the camera feed to figure out which store we were looking at, because there was no other way to identify the owner. After we identified the owner we closed the stream immediately.

  D2: We only checked that the device indeed did not have any security and a quick look at what kind of data it contained to make sure it was some sample database.
- We sent a mail to the owner of D1 with only the information that we found a security flaw in one of their stores and are waiting for a reply so we can inform someone that has permission to know about these kinds of things. The email we sent to Microsoft for D2 only contains the IP address without disclosing the details of the vulnerability so they can help us to get in contact with the real owners.
- We did not change passwords or anything of the sort, so we abided by this rule.

References

Default IP Addresses and Login Settings of GeoVision Products (2017).
URL: *http://pd.geovision.tw/technotice/IP*$_{D}evice/Default_{I}P_{P}W_{o}f_{G}V_{P}roducts.pdf$

Appendix A - Email sent to De Plantenhal (D1)

Digitale kwestbaarheid gevonden in een van uw panden

Laan, L.S. van der (Lucas)

Tue 09/11/2021 16:48

To: info@deplantenhal.nl <info@deplantenhal.nl>;

Cc: Tamminga, E.J. (Elwin) <elwin.tamminga@ru.nl>;

1 attachment

A4_Disclosure_letter.pdf;

Geachte heer/mevrouw,

Voor een van onze opdrachten moesten wij kwetsbare systemen vinden online, zie de bijlage voor meer informatie.
Een van de systemen die wij hebben gevonden zit in het pand van Oud-Beijerland aan de Langeweg 35, 3261 LJ Oud-Beijerland.

Voor informatie waar het over gaat, reageer op deze mail zodat wij de systeembeheerder kunnen inlichten.

Met vriendelijke groeten,
Lucas en Elwin

Appendix B - Email sent to Microsoft (D2)

Server of Azure customer may contain vulnerability

Tamminga, E.J. (Elwin)

Wed 10/11/2021 18:36

To: abuse@microsoft.com <abuse@microsoft.com>;

Cc: Laan, L.S. van der (Lucas) <lucas.vanderlaan@ru.nl>;

1 attachment

A4_Disclosure_letter.pdf;

Dear Microsoft,

We are cyber security students and for one of our assignments we had to find online vulnerable devices.

We found that one of your Azure customers may run a vulnerable server. The IP of this server is 13.73.150.124. We do not know how to contact the owner, but maybe you can forward this mail to the owners? They can contact us for more information.

Kind regards,
Elwin and Lucas