howest
hogeschool

Lab 10: Audit report

Network and System

Pentesting 2021-2022

Table of content

Introduction

The company OfficeHustler called us to perform a pentest on their network. This is because security is very important nowadays and they wanted to make sure that they aren't vulnerable to malware.

Below you will find a summary of the things I found. There will also be some recommendations on how to improve the network.

I started this pentest by researching the company online (chapter 1). Then I started scanning (chapter 3) and gathering information. And to end I tried accessing the machines and abusing certain protocols until I could eventually access the domain controller and become domain enterprise admin. (chapter 4 – 10).

1 OSINT results

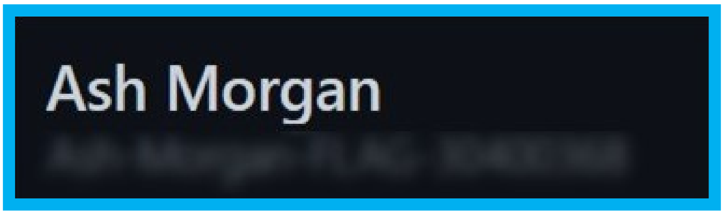
In this chapter you will read the OSINT results. OSINT is also known as Open-Source Intelligence. It is the information we can find without having access to the network. For example: we can take a look at the website to find out who CEO is.

1.1 GitHub

The first thing I decided to do was looking at the website of OfficeHustler. I quickly noticed that this is a company that creates code, so I thought they must have a GitHub page. On that GitHub page there is a lot of information. Most of this information should not be public. There are also things that aren't related with the company. These shouldn't be visible (see bullets below, for example link to twitch).

Below you find a summary of the findings. In the next chapter I will discuss what is allowed on GitHub and what isn't.

- I found confidential data in the bio of Ash Morgan

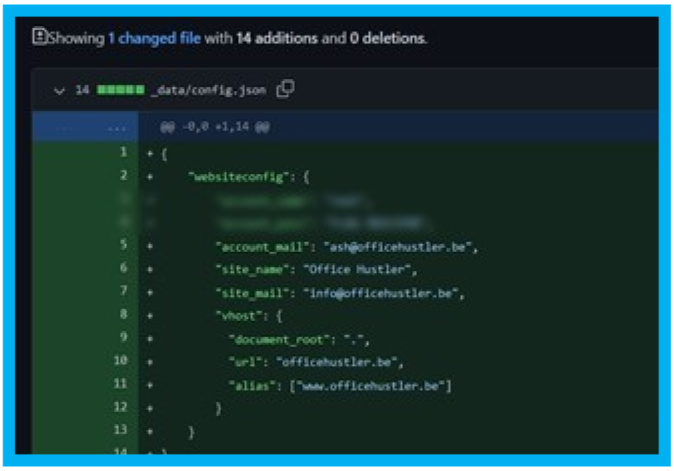


Ash Morgan

[redacted]

FIGURE 1: CONFIDENTIAL DATA IN BIO

- Then I looked at the commits of the main branch. In the past there was a mistake and some of the credentials were pushed. The problem is that you can't delete those commits. In the next chapter I will discuss a solution.



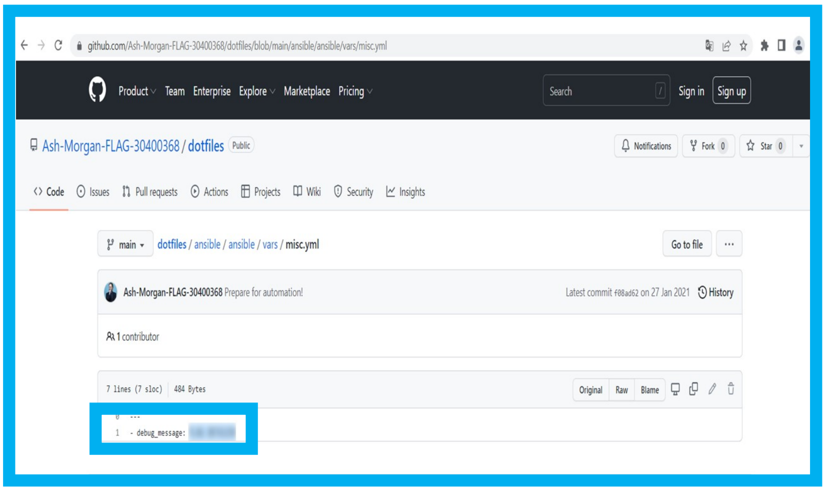
Showing 1 changed file with 14 additions and 0 deletions.

14 _data/config.json

```
@@ -0,0 +1,14 @@
+ {
+     "websiteconfig": {
[redacted]
+         "account_mail": "ash@officehustler.be",
+         "site_name": "Office Hustler",
+         "site_mail": "info@officehustler.be",
+         "vhost": {
+           "document_root": ".",
+           "url": "officehustler.be",
+           "alias": ["www.officehustler.be"]
+         }
+     }
```

FIGURE 2: CONFIDENTIAL DATA IN COMMIT

- Then I found an reposotory (repo) from Ash with a lot of confidential data. To start: SSH keys should never be in an online reposotory. You should keep the private key private. Furthermore you shouldn't have a file with the vault password from ansible in this reposotory. This way we could decrypt a file with that password. To end: I found confidential data in the mysql folder. This also should not visible for me.



github.com/Ash-Morgan-FLAG-30400368/dotfiles/blob/main/ansible/ansible/vars/misc.yml

Ash-Morgan-FLAG-30400368 / dotfiles Public

dotfiles / ansible / ansible / vars / misc.yml

Ash-Morgan-FLAG-30400368 Prepare for automation! Latest commit f08ad62 on 27 Jan 2021 History

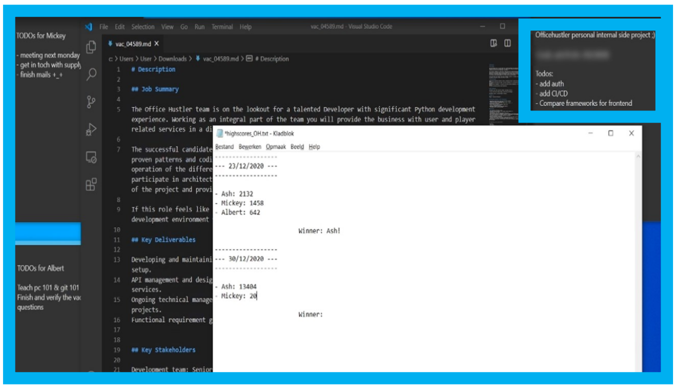
1 contributor

7 lines (7 sloc) | 484 Bytes

```
---
- debug_message: [redacted]
```

FIGURE 3: DECRYPT FILE WITH VAULT PASSWORD

- After I looked in Ash his files I saw in his bio a link to twitch. I decided to look at some videos. In one video you see that he performed an alt tab. In the end We also see confidential data in the background.



TODOs for Mickey

- meeting next monday
- get in toch with suppl
- finish mails +_+

TODOs for Albert

Teach pc 101 & git 101
Finish and verify the va
questions

File Edit Selection View Go Run Terminal Help
vac_04589.md - Visual Studio Code
vac_04589.md
c: > Users > User > Downloads > vac_04589.md > # Description

```
# Description

## Job Summary

The Office Hustler team is on the lookout for a talented Developer with significant Python development
experience. Working as an integral part of the team you will provide the business with user and player
related services in a di

The successful candidate
proven patterns and codi
operation of the differe
participate in architect
of the project and provi

If this role feels like
development environment

## Key Deliverables

Developing and maintaini
setup.
API management and desig
services.
Ongoing technical manage
projects.
Functional requirement g


## Key Stakeholders

Development team: Senior
```

Officehustler personal internal side project ;)

[redacted]

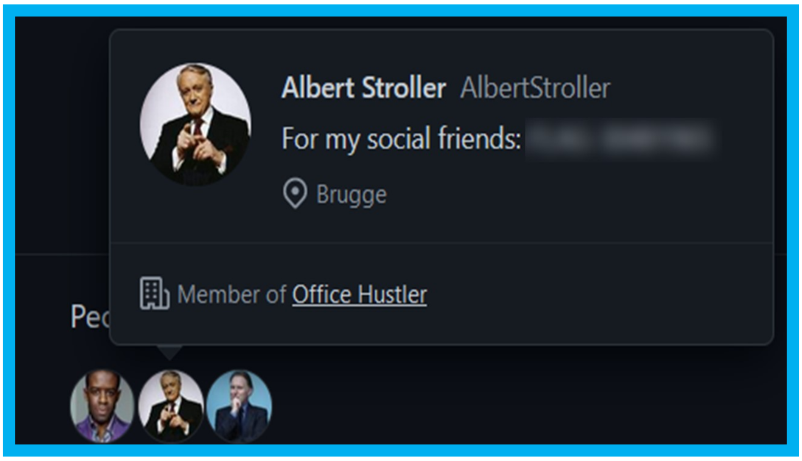
Todos:
- add auth
- add CI/CD
- Compare frameworks for frontend

*highscores_OH.txt - Kladblok
Bestand Bewerken Opmaak Beeld Help

```
-----------------
--- 23/12/2020 ---
-----------------

- Ash: 2132
- Mickey: 1458
- Albert: 642

                    Winner: Ash!

-----------------
--- 30/12/2020 ---
-----------------

- Ash: 13404
- Mickey: 20

                    Winner:
```

FIGURE 4: CONFIDENTIAL DATA TWITCH

- After I looked in Ash his GitHub profile I decided to check if there are more employees that have worked on this project, or have committed and pushed things to their repository. I found two other employees: Mickey Bricks and Albert Stroller. In Mickey's bio I discovered he is the CEO of the company. There's nothing wrong with his profile. Albert's profile, in contrary, has more has some sensitive data in his bio, which shouldn't be there.



Albert Stroller AlbertStroller

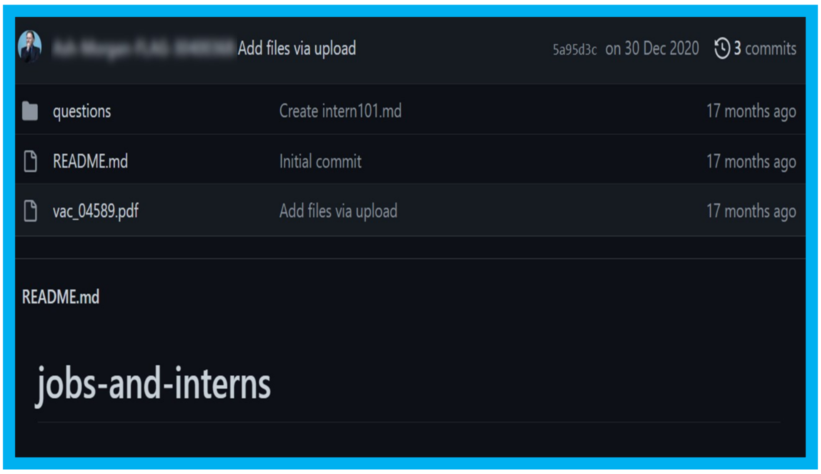
For my social friends: [redacted]

Brugge

Member of Office Hustler

FIGURE 5: ALBERT STROLLER CONFIDENTIAL DATA

- Then I took a look in the related repo's. I found out that they were searching for new employees because the pdf with the competences was in this repo.



[redacted] Add files via upload 5a95d3c on 30 Dec 2020 3 commits

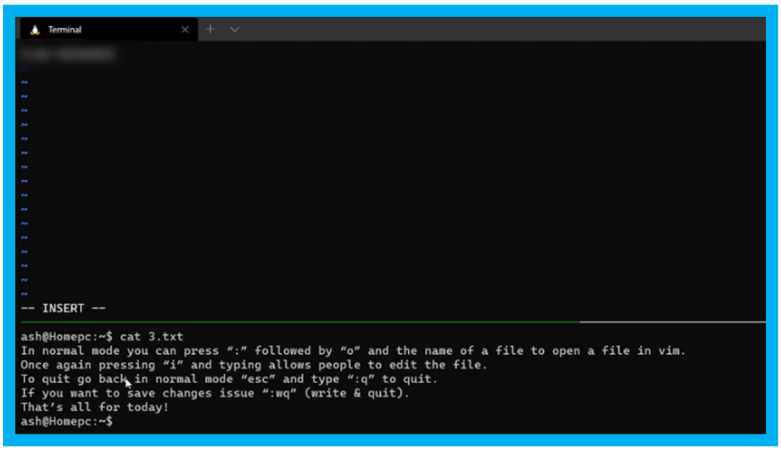
questions	Create intern101.md	17 months ago
README.md	Initial commit	17 months ago
vac_04589.pdf	Add files via upload	17 months ago

README.md

jobs-and-interns

Figure 6: job offer document

- After some research in this repo I found out that there is a link to a YouTube video. In which we see Mickey making a video on how to quit vim. Again, there is confidential data in this video.

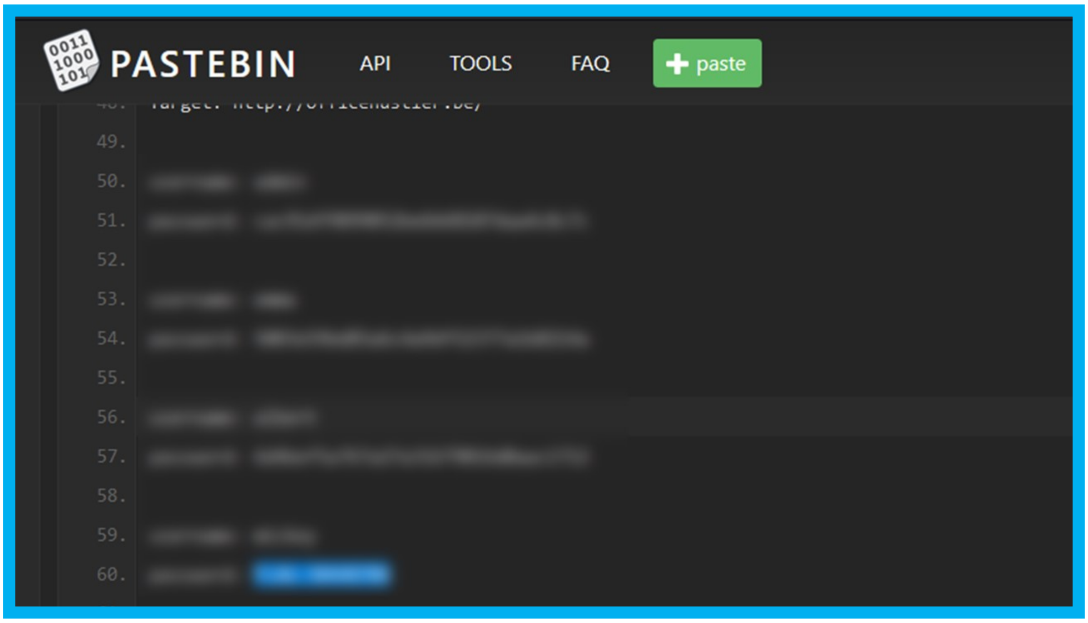


```
[redacted]
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --
```

```
ash@Homepc:~$ cat 3.txt
In normal mode you can press ":" followed by "o" and the name of a file to open a file in vim.
Once again pressing "i" and typing allows people to edit the file.
To quit go back in normal mode "esc" and type ":q" to quit.
If you want to save changes issue ":wq" (write & quit).
That's all for today!
ash@Homepc:~$
```

Figure 7: confidential data on YouTube

- On the YouTube video you can click on the owner's channel. Under the page "about" you can see if they linked other social media. There I found a link to Mickey his Facebook. On his Facebook I found once more a lot of sensitive data. But the most important thing was that somebody left a comment with the message that he hacked OfficeHustler and left a link with proof. There I found a lot of data that shouldn't be online.

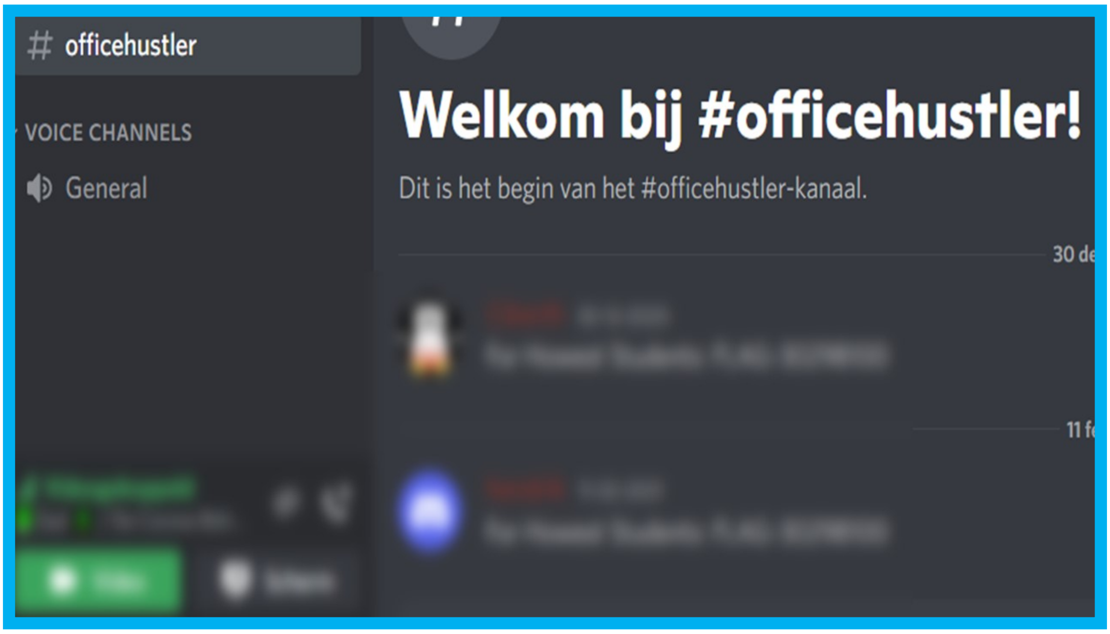


```
Target: http://officehustler.be/
```

[redacted]

FIGURE 8: OFFICEHUSTLER HACK

- Then I went back to take a look at the last repo. In this repo I found promotion material. On one of the posters there was a visible access code. I recommend not putting this online. But on another file I saw a file with at the bottom "Join us on Discord!". I clicked on this hyperlink and suddenly I joined the discord server from OfficeHustler.



Welkom bij #officehustler!

Dit is het begin van het #officehustler-kanaal.

FIGURE 9: DISCORD

1.2 Robots.txt file

What is important to know is that every website has a robot.txt file. This is a file with instructions for search engines crawlers. It defines which areas of a website crawlers are allowed to search. What's interesting here is that in the robots.txt file from the website https://www.officehustler.be/ there is something that's called "oh-db-management/". But this is disallowed. You can access it by putting it after the URL. That we can access the database so easily is not good.

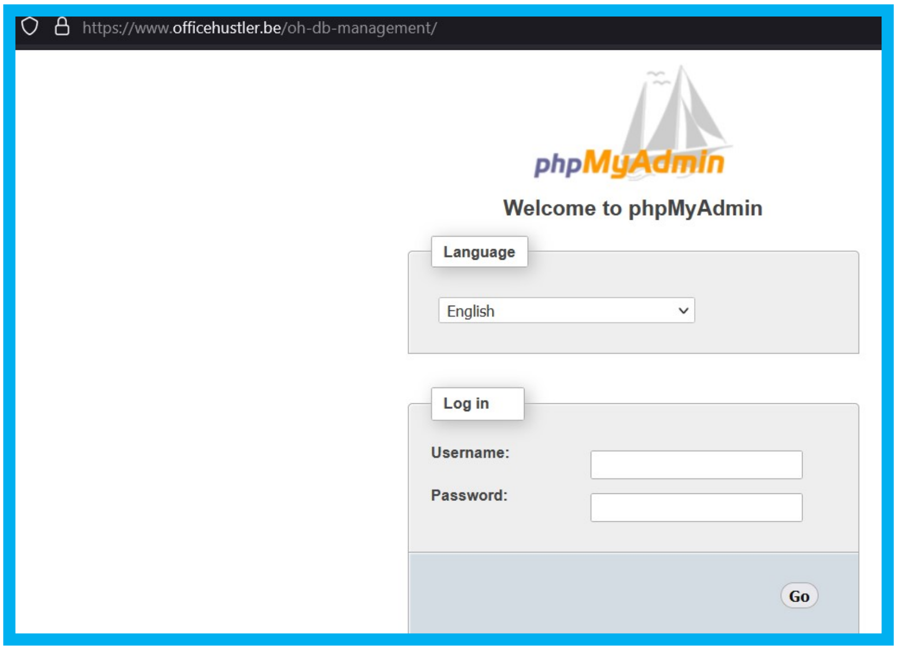

https://www.officehustler.be/oh-db-management/

FIGURE 10: ROBOTS.TXT

1.3 DNS records

I also found a lot of information in the DNS-records. Via the nslookup command I found out that there was a mail server on the network and I was able to check the SPF records. But the most interesting thing was that the DNS dumpster showed me a second website. I could find the promo code in the source code.

2 Possible solutions for OSINT

In this chapter I will discuss some possible solutions for the problems and findings discussed in the previous chapter.

2.1 GitHub solutions

Because I found a lot of sensitive data via the GitHub of the company I will start there. At first I would recommend to change all biographies of the employees from OfficeHustler who also have a GitHub account. This means deleting all personal information in their bio. Things like twitch or maybe confidential data aren't recommended to write down in a bio from a professional website. Anybody could see this and maybe abuse it.

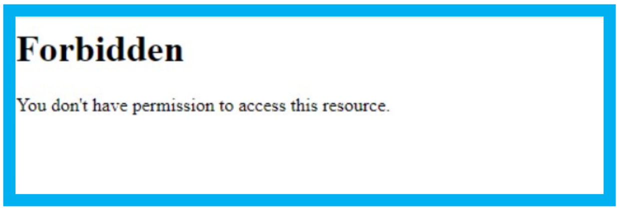
Then you should look at which files are online. Keep in mind that every commit that has been pushed to GitHub stays online. Therefore you should think about which repositories are necessary and which aren't. Also if you commit accidently a password, a private key or some other authentication method you should immediately change the password or generate a new private key. This brings us to the repo called "dot files" from Ash Morgan. This repo is filled with things that shouldn't be on GitHub. I would recommend deleting that repo and then if necessary make it again. Because GitHub ensures that nothing is truly lost. Only if you delete that repo everything is gone. First of all the directory ".ssh" shouldn't be online because there are private and public keys in there. And it is very important to keep the private keys private. So this should definitely be deleted (and not just delete the content but delete the repo and if necessary make the repo again and push the right things to it). Also it is not always smart to put all the SQL commands that you perform on your database online. People can look at it and see how your database is designed. And last of all, just like you need to keep your private key private, you should also keep your passwords private. It isn’t smart to put your vault password from ansible online. Nowadays there are extensions that can decrypt ansible files with the right password. If you put that password online everybody can decrypt that file.

What is also dangerous, is putting a file with the necessary competencies for new employees online. I understand that this is easy for the hiring procedure but people with bad intentions know perfectly which infrastructure you have or what kind of software is running by reading that file. And also you shouldn’t have files with YouTube links in it. And surely not when this is linked to a personal account. That brings us to social media. I recommend that when you get a comment on a post on Facebook which tells you that you have been hacked that you delete that comment. Because everybody that finds your Facebook account can see that comment.

to end with the GitHub findings I would also recommend that if you put promotional files online that you delete the hyperlink in it, surely when it links to your own discord server with private data in it. I also would not recommend discord for professional purposes.

2.2 Possible solution for Robots.txt file

This is something more complex to fix. That is because every website has this file. What I would do is change the permissions on server level. This means that if somebody goes to the website they get an error 403 forbidden notification.



Forbidden

You don't have permission to access this resource.

FIGURE 11: ERROR 403

What is also possible: is to make some folders above the file and put these on disallowed. In such way the websites that you are trying to hide can't be accessible. Keep in mind that there is nothing wrong with this robots.txt file if you have strong passwords on these websites that you are trying to hide.

3 Scanning

The previous chapters are findings and recommendations for OSINT which means I didn’t have access to the network. From now everything that is described is done on the network.

I will discuss everything that has to do with scanning in this chapter. Every host that is online will be shortly discussed in this chapter. In further chapters we go deeper on the hosts and the vulnerabilities that they possibly contain.

Note: all the scanning is done with the tool Nmap. Detecting scanning is difficult for firewalls, and monitoring software does often ignore it. It is very difficult to stop the scanning process.

3.1 General network information

The first thing that I checked is what network I was in. I am in the 10.11.0.0/23 network. I also checked what the domain name was and how much nameservers there are online.

3.2 Scanning

The first scan I did was to look how much live IP-addresses there are. There were 9 hosts up in scope. Below I shortly discuss them.

3.2.1 10.11.0.13

This is the first address in scope that is online. Nmap doesn’t give us a hostname. But we got the MAC-address and this indicates that this machine is an apple device. This host will be in the next chapter.

3.2.2 10.11.0.19

The second address in scope is 10.11.0.19. The scan gives us the hostname dc.officehustler.be. And the MAC-address indicates that this is a virtual machine. This host will be further discussed in another chapter.

3.2.3 10.11.0.20

This host gave us the hostname portable.officehustler.be and via the MAC-address I knew that machine is from MSI. This host will be further discussed in another chapter.

3.2.4 10.11.0.24

The hostname of this machine is router.officehustler.be. The MAC-address indicates that this is the router (routerbord.com). To verify this I browsed to the IP-address and discovered it runs pfSense software. This is one of the machines in which I didn't find anything wrong. This machine will therefore not be further discussed.

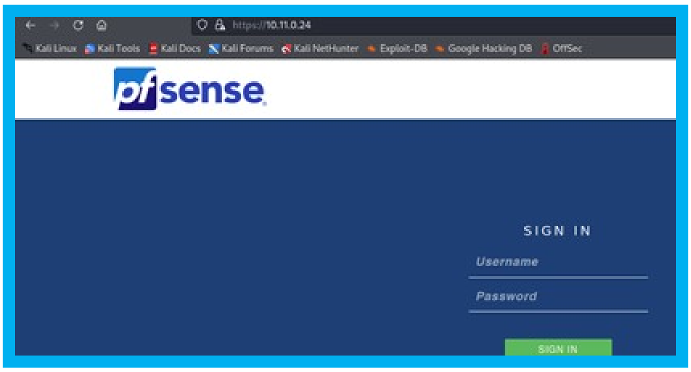


FIGURE 12: ROUTER

3.2.5 10.11.0.28

This machine gave us the hostname dns2.officehustler.be. And the MAC-address indicates that this is a virtual machine. This host will be further discussed in another chapter.

3.2.6 10.11.0.30

The hostname of this machine is client.officehustler.be. And the MAC-address indicates that this is a machine from HP. This host will be further discussed in another chapter.

3.2.7 10.11.0.37

Here I found something interesting. I don't have a hostname but the MAC-address indicates that this is a mobile device. This host will be further discussed in another chapter.

3.2.8 10.11.0.52

Here I also don't have a hostname but the MAC-address indicates that this is an NAS. This is one of the machines that I didn't find anything wrong. This machine will then also not be further discussed.

3.2.9 10.11.0.53

The last host has a hostname www.officehustler.be and the MAC-address indicates that this is a raspberry pi. This host will be further discussed in another chapter.

4 10.11.0.13

In this chapter I will discuss my findings about the 10.11.0.13 machine. And I discuss what could be done better.

4.1 Open ports

After I did some more scanning I found out that there are a lot of open ports. I will summarize them below and discuss if they are better closed or not.

- Port 22 (TCP)

  This port is for SSH, if you need to connect over SSH you should keep it open. Otherwise I recommend to close it.

- Port 25, 587 (TCP)

  This is for mail purposing. These ports can be open.

- Port 88 (TCP)

  This is for Kerberos. This port can be open.

- Port 548 (TCP)

  This is for the AFP service from Apple. I would disable anonymous user for AFP control. I would also set an authentication.

- Port 3031 (TCP)

  This is for the service eppc. If you don't use it you should close this port.

- Port 3283 (TCP)

  This is for the service net-assistant, classroom. If you don’t use it you should close this port.

- Port 5900 (TCP)

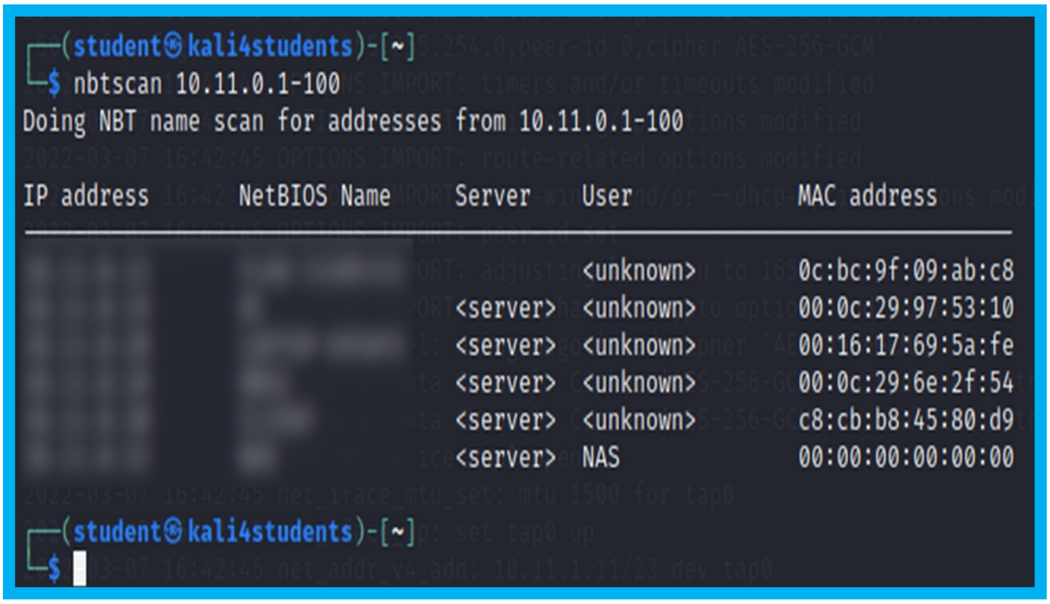
  This is for the service Apple Remote Desktop. If you don’t use it you should close this port.

- Port 49152 (TCP)

  This if for the Xscan service. If you don’t use it you should close this port.

4.2 NetBIOS

You should also disable NetBIOS. This prevents that we can find the hostname or the NetBIOS name.



```
┌──(student㉿kali4students)-[~]
└─$ nbtscan 10.11.0.1-100
Doing NBT name scan for addresses from 10.11.0.1-100

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
[redacted]                                  <unknown>        0c:bc:9f:09:ab:c8
                                  <server>  <unknown>        00:0c:29:97:53:10
                                  <server>  <unknown>        00:16:17:69:5a:fe
                                  <server>  <unknown>        00:0c:29:6e:2f:54
                                  <server>  <unknown>        c8:cb:b8:45:80:d9
                                  <server>  NAS              00:00:00:00:00:00

┌──(student㉿kali4students)-[~]
└─$ 
```

Figure 13: NetBIOS Mac device

5 10.11.0.19

In this chapter I will discuss my findings about the 10.11.0.19 machine. And I discuss what could be done better.

5.1 Open ports

After I did some more scanning I found out that there are a lot of open ports. I will summarize them below and discuss if they are better closed or not.

- Port 25, 465, 587, 2525 (TCP)

  This is for mail purposing. These ports can be open.

- Port 80, 81 (TCP)

  These are ports from Microsoft IIS. These can be open.

- Port 88 (TCP)

  This is for Kerberos. This port can be open.

- Port 135 (TCP)

  This is for the MSRPC service. This port should be closed.

- Port 139 (TCP)

  This is for the NetBIOS service. This port should be closed.

- Port 389, 3268 (TCP)

  This is for the LDAP services. These can be open.

- Port 443, 444 (TCP)

  These are ports from Microsoft IIS. These can be open.

- Port 445 (TCP)

  This is for the Microsoft-ds services. This port should be closed.

  Note: file and printer sharing will not work if you close the port.

- Port 464 (TCP)

  This is for the Microsoft kpasswd services. This can be open

- Port 596, 6001 (TCP)

  This is for Microsoft Windows RPC over HTTP 1.0. These ports should be closed.

- Port 636 (TCP)

  This is for Microsoft Windows Active Directory LDAP. This port can be open.

- Port 808 (TCP)

  This is for the service Ccproxy-http. This port can be open.

- Port 1801 (TCP)

  This is for the Msmq service. This port should be closed.

- Port 2103, 2105, 2107, 6580, 6839 (TCP)

These ports are for msrpc. These ports should be blocked.

- Port 3269 (TCP)

  This is also for SSL/LDAP service. This port can be open.

- Port 53 (UDP)

  This is for the DNS. This must be open.

6 10.11.0.20

This was actually the most vulnerable machine. This was the entry to eventually getting access to the domain controller and becoming enterprise administrator. I will discuss again the open ports and then the vulnerability that I have exploited to gain access to the machine and got remote code execution.

6.1 Open ports

After I did some more scanning I found out that there are a lot of open ports. I will summarize them below and discuss if they are better closed or not.

- Port 135 (TCP)

  This is for the MSRPC service. This port should be closed.

- Port 139 (TCP)

  This is for the NetBIOS service. This port should be closed.

- Port 445 (TCP)

  This is for the Microsoft-ds services. This port should be closed.

  Note: file and printer sharing will not work if you close the port.

7 10.11.0.28

This is the second DNS server in the network. This was actually the second part of getting to the domain controller. Again I will discuss open ports, discuss some enumeration things and tell you how I got access to this machine.

7.1 Open ports

After I did some more scanning I found out that there are a lot of open ports. I will summarize them below and discuss if they are better closed or not.

- Port 53 (TCP)

  This is for the DNS. This port must be open.

- Port 135, 49152, 49153, 49154, 49158, 49175 (TCP)

  This is for the MSRPC service. These ports should be closed.

- Port 139 (TCP)

  This is for the NetBIOS service. This port should be closed.

- Port 445 (TCP)

  This is for the Microsoft-ds services. This port should be closed.

  Note: file and printer sharing will not work if you close the port.

- Port 554

  This is for the RTSP protocol. This port can be open.

- Port 5800, 5900 (TCP)

  This is for openvnc service. These ports can be open.

8 10.11.0.30

This machine is in this environment the only machine with anti-virus enabled. I also know that if I could pawn this machine I got access to the domain controller and thus the domain. First I discuss the ports and then I will discuss how I got access

8.1 Open ports

After I did some more scanning I found out that there are a lot of open ports. I will summarize them below and discuss if they are better closed or not.

- Port 135 (TCP)

  This is for the MSRPC service. This port should be closed.

- Port 139 (TCP)

  This is for the NetBIOS service. This port should be closed.

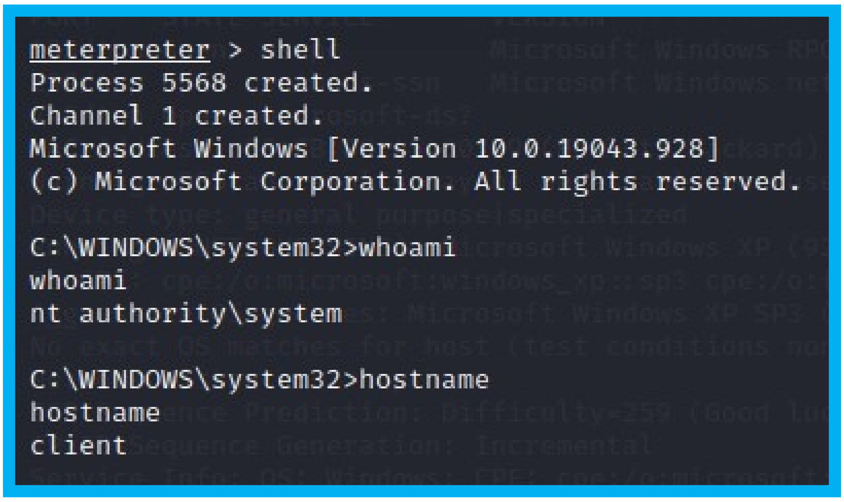
- Port 445 (TCP)

  This is for the Microsoft-ds services. This port should be closed.

  Note: file and printer sharing will not work if you close the port.

8.2 Gain access

By now I already know that SMB is enabled so I figured out how to abuse it. With some simple scanning tools I figured out that a user called Albert has an local administrator account on the 10.11.0.30 machine. And since that I have his hash I could gain access to that machine and execute remote code. This is very important because when I dump the hashes of that machine I see that Mickey has a local administrator account on that machine. Mickey is also a domain enterprise administrator. Because I have now his hashes I could do the same things and gain access to the domain controller.



```
meterpreter > shell
Process 5568 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
nt authority\system

C:\WINDOWS\system32>hostname
hostname
client
```

FIGURE 14: AUTHENTICATE ON .30 MACHINE

9 10.11.0.37

This is the only mobile phone in the environment. You can see that on the MAC-address. In this chapter I will discuss the open port and how I abused that port to gain access to the phone and could see whatever I wanted.

9.1 Open port

In this case there is only one port open.

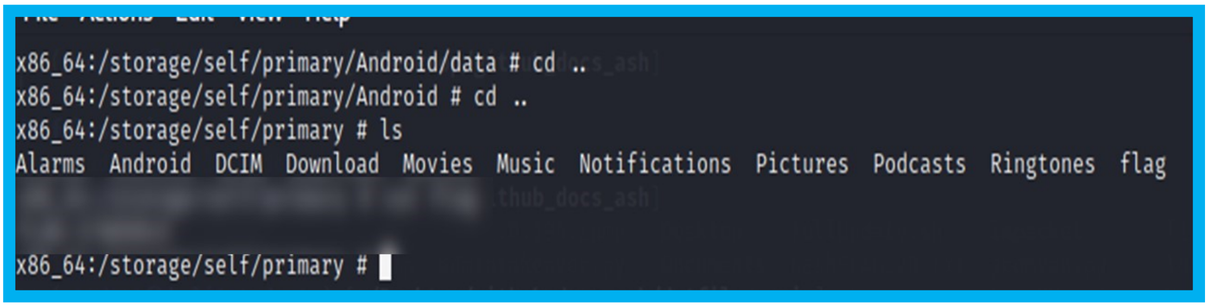
- Port 5555 (TCP)

  This indicates that the Android Debug Bridge Daemon (ADBD) is listening over the network. And if it is listening that means that you can connect with it or start an interactive shell. This port should always be closed.

9.2 Gain access

Because I knew that this port is open (because the scanning told me that) I knew that I could connect with it. There are tools that support that and the first thing I did was searching the hostname of the device. This is “android-b0371fb1f3b25cdf”.

After that I connected with the phone and got access to everything. I could read messages, see pictures, see downloaded files, and so on.



```
x86_64:/storage/self/primary/Android/data # cd ..
x86_64:/storage/self/primary/Android # cd ..
x86_64:/storage/self/primary # ls
Alarms  Android  DCIM  Download  Movies  Music  Notifications  Pictures  Podcasts  Ringtones  flag
[redacted]

x86_64:/storage/self/primary #
```

FIGURE 15: ACCESS THE FILESYSTEM OF THE PHONE

10 10.11.0.53

This is the raspberry pi of the network. There are a lot of websites on it, a database, and a lot of other things. I will discuss the open ports on it, discuss some services and I will talk about pivoting.

10.1 Open ports

After I did some more scanning I found out that there are a lot of open ports. I will summarize them below and discuss if they are better closed or not.

- Port 22, 2210, 2211, 2214, 2222

  This is a SSH port. If you don't need it you should close these.

- Port 23

  This is the port for telnet. This port should definitely closed. This is because telnet doesn't encrypt traffic. That means that your passwords are being send in clear text. I actually found credentials and was able to authenticate on this machine.

- Port 80

  Since there are websites on this machine this port should be open.

- Port 111

  This is for RPCbind service. This port should be closed.

- Port 443

  Since there are websites on this machine this port should be open.

- Port 3128

  Here runs a Proxmos server.

- Port 3306

  Here runs the SQL server.

- Port 8443

  Here runs another website.

11 Website officehustler.be

In this chapter I will discuss some findings about the website https://www.officehustler.be/. This is because I found some very interesting things that could lead to dangerous situations.

11.1 Joomla

The website is built with Joomla version 3.6.3. After some scanning and using some tools I found out that there are a lot of vulnerabilities for this software. Attachment 2 will have more information about the vulnerabilities and what is wrong. For now I would recommend to update the website to the latest stable version.

Conclusion

Almost every machine is vulnerable in this network. There are a few major things that must be happen.

1. Enable on every machine the windows defender of another firewall.
2. Make sure every machine is using the latest stable version. Keep updating the machines.
3. Check every machine and close the unnecessary ports.
4. Make sure every user has a strong password and make sure that these passwords are not used for everything. A strong password contains at least 12 characters, numbers, lower and uppercase characters and a special character.
5. Make sure the credentials are not stored in the html files or other files that are public visible.

It is also recommended to look into the information that is visible online and determine if these things need to be public (see chapter 1 OSINT). And as last look at the machines that have direct access to another network and determine of this is necessary. If that's the case you should think about vlanning to make sure that pivoting isn't possible.

Attachments

Attachment 1: List of figures

Attachment 2: Joomla website

Attachment 1: list of figures

Attachment 2: Joomla website

In the ZIP-file you can find a file called www.officehustler.be_report_2022-3-17_at_10.57.54.html. If you open that you can see all the possible vulnerabilities and things that could be improved.