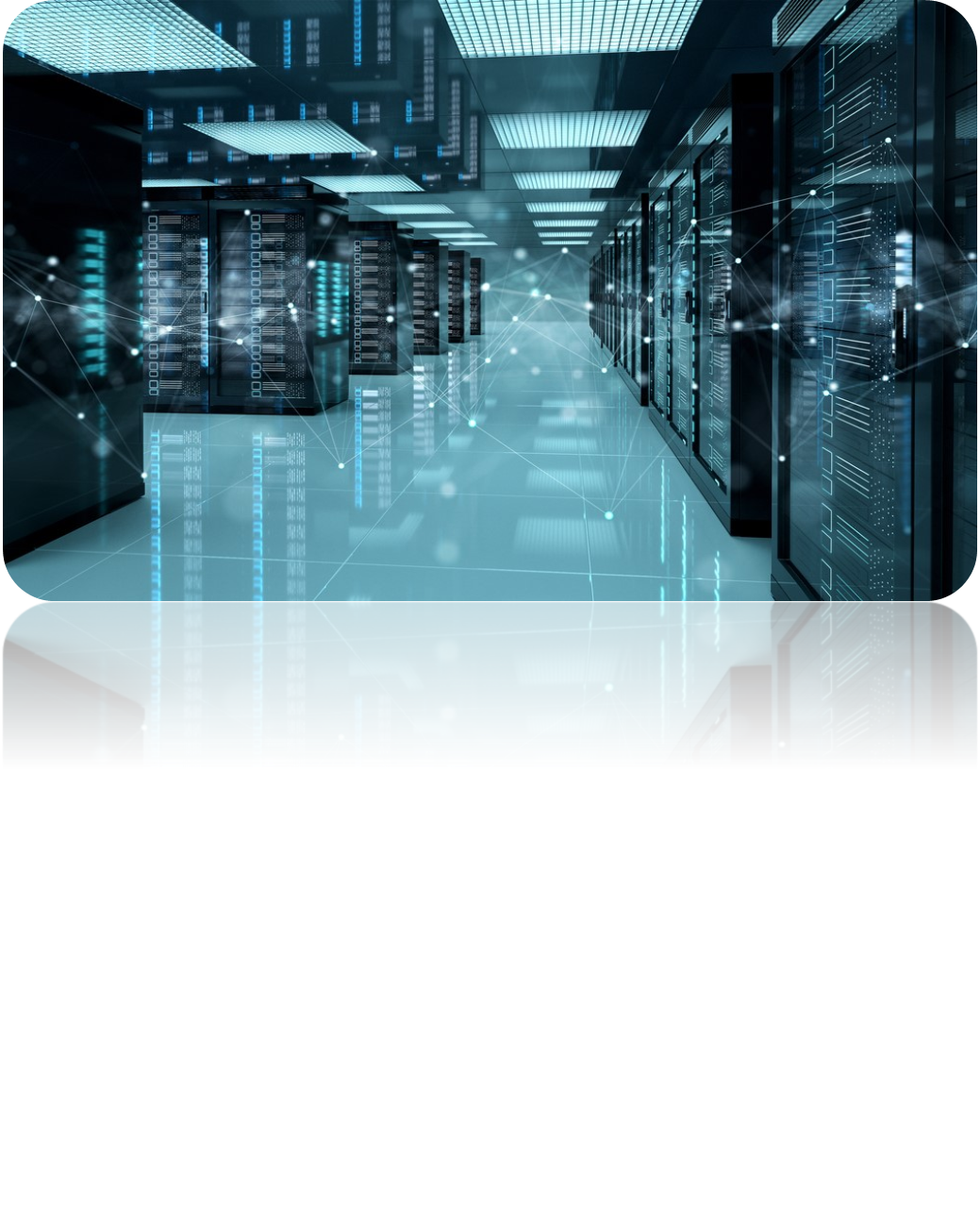
Infrastructure pen-testing Document



|  |
| --- |
| Authors: Yoan-Asen Popov, Mihai Glodici, Joep Vinken  Student Number: 4472152, 4538528, 4475003  Class & group: I02, group 8  Assignment: Case study 2 infrastructure |

# Table of contents

[Table of contents 2](#_Toc106469791)

[Summary of results 3](#_Toc106469792)

[Attack Narrative 3](#_Toc106469793)

[Nmap 3](#_Toc106469794)

[Hydra 4](#_Toc106469795)

[SQLInjection 5](#_Toc106469796)

[Conclusion 6](#_Toc106469797)

# Summary of results

The reconnaissance of Fontys8 network resulted in weak passwords on the network. After creating a custom wordlist using social engineering on some of the employees, a successful brute-force attack was conducted.

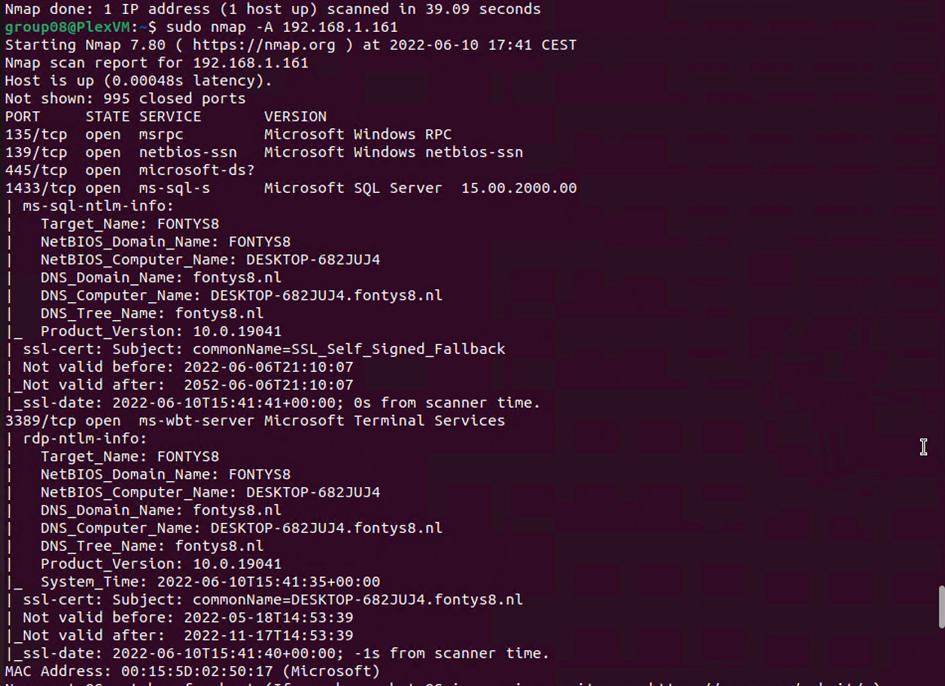
Scanning the network resulted in discovering insecure ports. And thus, creating an opportunity of easier attacks.

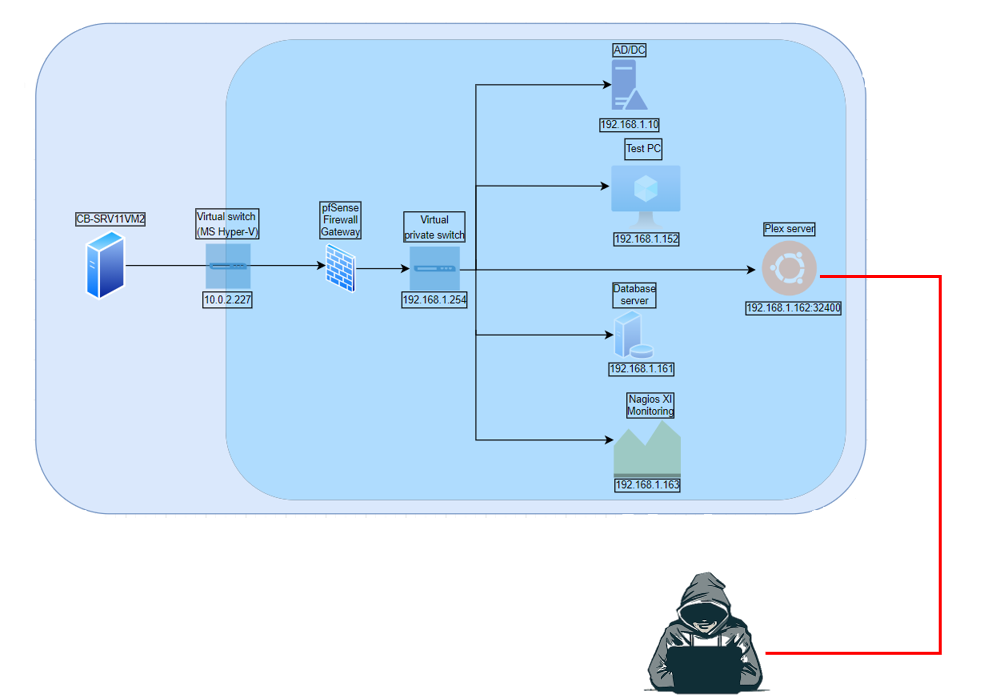
Resulting these tests, we could say that the general security of this server is fairly good, but employees should be aware of social engineering and what information they can and can't share with somebody. Without the list of possible passwords, it would be a lot harder to get into the server if you are not allowed to.

# Attack Narrative

## Nmap

For the port-scanning, we used Nmap to see what ports are opened and what purpose they serve. The first step we took is installing Nmap on one of our virtual machines. This was successfully done and this is where the fun starts. We used the sudo nmap –O 'IP 'command to see all the open ports on the specified IP address. We could also see the versions and the service of these ports which made it easy to see if the port should be open or not. This resulted in a minimal number of unsecure ports that are opened, although they should be opened. There was for example an HTTP port opened which it should be, but there wasn't an extra layer of protection added to the port. This could make it easier for a hacker to access our server without our knowledge or consent. All the other ports that are opened are secured and should stay open to keep our systems up and running.

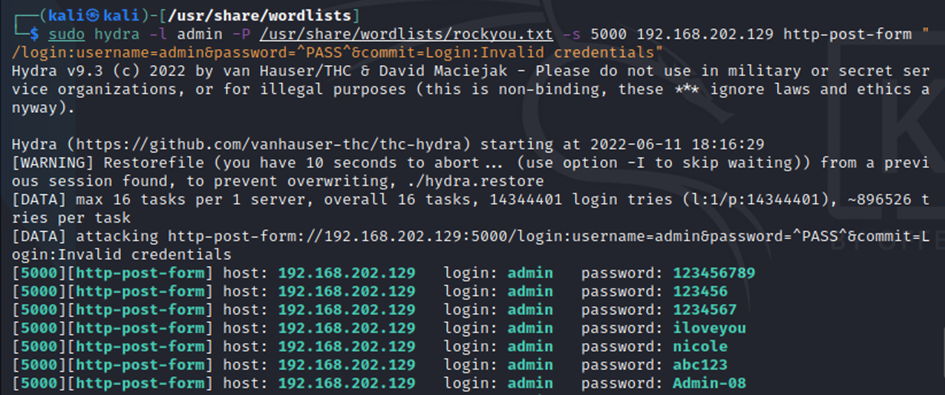




## Hydra

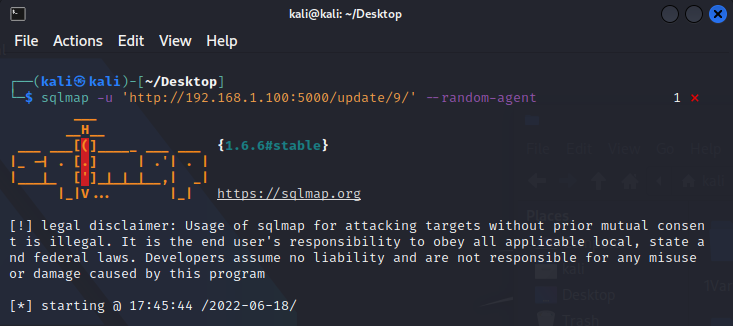
Before starting the brute-force attack, a careful investigation was made via social engineering techniques that made it possible to develop a word-list dictionary for it. The attack was conducted on the computer that hosted a website. The dictionary file was used with the username ‘admin’ against the login page of the site. This attack uncovered the password ‘Admin-08’ for the username ‘admin’.

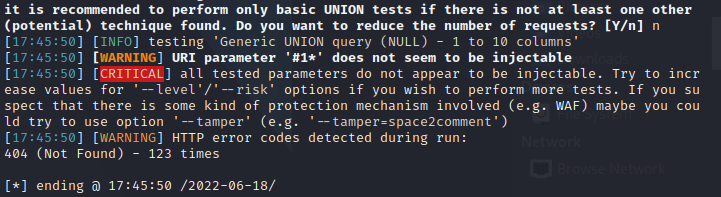
The interface gave us direct access to the whole data of every employee and the ability to change and delete it.

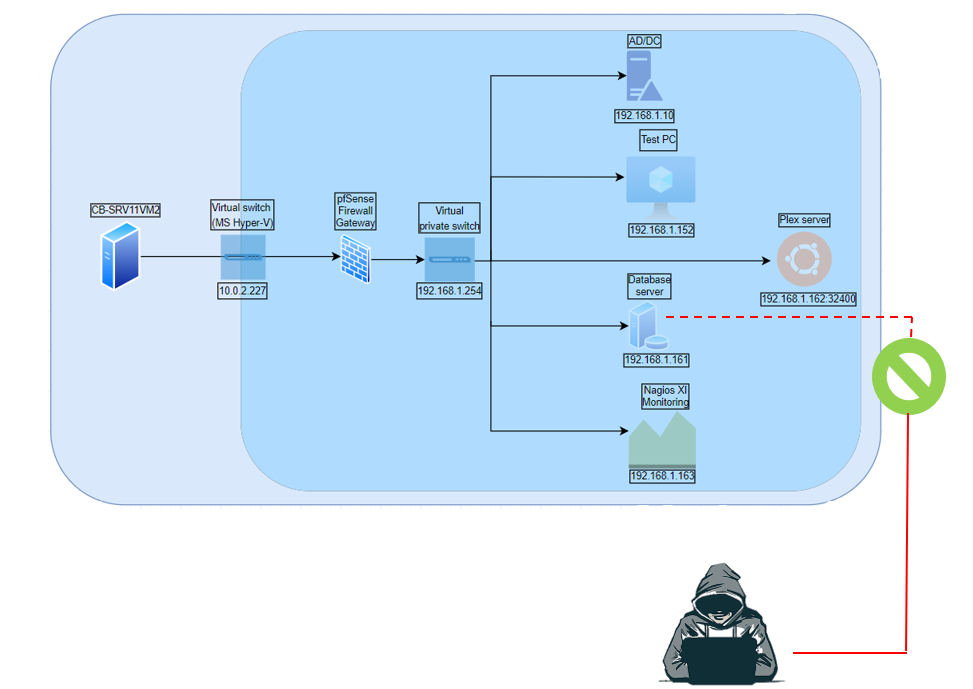


## SQLInjection

After successful authorization we tried an SQLInjection with ‘SQLMap’. The attempt to download the used tables were unsuccessful.







# Conclusion

Recommendations

Due to the impact to the overall organization as uncovers by this penetration test, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner.

Group 8 Security recommends the following:

1. Change protocols. The protocol for the webserver is not using https, thus it is more vulnerable.
2. Establish a password policy. The use of weak passwords and reuse of them can be the reason of malicious activities.
3. Conduct regular vulnerability assessments. As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on regular basis. Doing this, it will show if security policies need updates.