Basic knowledge assignment

**Gemaakt door:** Tim Chermin

**Versie:** 1.2

**Datum:** 06/03/2020

Table of Contents

[Version 3](#_Toc34983287)

[Introduction 4](#_Toc34983288)

[Demo en Test Omgeving 4](#_Toc34983289)

[Test en Analyse resultaat (Screenshots and explanation of all working solutions, like): 4](#_Toc34983290)

[Overall Conclusion 4](#_Toc34983291)

[Reflection 5](#_Toc34983292)

[My company 6](#_Toc34983293)

[Security incident management 7](#_Toc34983294)

[Bibliography 12](#_Toc34983295)

[Notes for later 13](#_Toc34983296)

# Version

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Autor** | **Date** | **Changes** | **Time spend** |
| 1.0 | Tim Chermin | 13/02/2020 | * Basic setup | 10 min |
| 1.1 | Tim Chermin | 06/03/2020 | * Firewall setup | 6 hours |
| 1.2 | Tim Chermin | 12/03/2020 | * Security incident management | 5 hours |
| 1.3 | Tim Chermin | 13/03/2020 | * Continuation of the firewall setup | 6 hours |

# Introduction

Before this semester I already had some experience since I did the CSA-course before CSB. I didn’t know much about the defensive side of things though. I really liked style 1 when I did the CSA course, so I decided I will be doing the same for CSB.

In this document, I have documented everything I learned this semester and how I learned it.

My main goal was to learn the basics of the defending site of cyber security. I will try to use as much of the knowledge I gained when following the CSA course in this course.

**A lot of the document is still a work in progress.**

# Demo and teste environment

Build (Implementation details and essential configurations for each basic knowledge theme):

* Threat Analysis
* IP-address plan and network drawing reflecting your own demo network
* Firewall settings and rules necessary
* Secure Network Connections needed
* Secure Remote Access and Management (VPN settings)
* Intrusion Detection rules
* IT monitoring configuration
* User and management accounts for role based access (System security)

# Test and Analyse result (Screenshots and explanation of all working solutions, like):

* Basic functioning of internal and public functionality/services (securely)
* Inbound and outbound firewall filtering (examples of both access and blocking of communication).
* VPN access and secure remote management of DMZ and LAN servers
* IDS functioning: show/prove for detections of intrusions, attempts, scans, attacks, abuse, malware that you wanted to detect.
* How should Incident Management (concepts) be set up if this was a real company
* Monitoring: Show that good and bad statuses of your IT environment can be monitored in a SOC-like environment
* What are the results of your IT Risk Analysis (qualitative)
* Is user management (System Defence) correctly implemented?

# Overall Conclusion

* Conclusions on the accomplished level of security for the company, and an advice for remaining improvements of the security for the company.

# Reflection

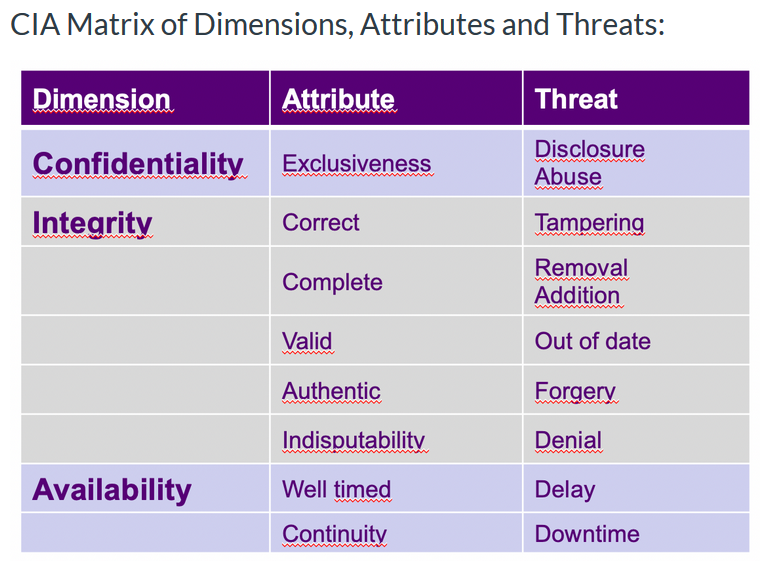
* Critical reflection on the results of your own learning process thus far.
* How was your Pro-active attitude (being present, taking initiative) towards the basic knowledge and the project activities
* How did you communicate with teachers, fellow students, experts (presenting, advising, inquiring and eventual reporting)

# My company

I use the company found on canvas.

“The example design is based on company X, a small company with about 10 employees that hosts web-sites for their customers. They provide so-called virtual hosting in the Company X DMZ to serve the Internet (WAN). They also run their own company X web site in the same environment. DNS-service is also provided here. Internally (LAN), they host internal services like a Windows domain controller for managing user accounts, corresponding security policies and eventually hosting an internal DNS service. Both networks DMZ and LAN contain an IDS-sensor that detects specific intrusions and hacking attempts. The LAN (users and internal servers use the same network) also contains a monitoring server.” (explanation basic knowledge assignment, n.d.)

|  |  |  |
| --- | --- | --- |
| **Dimension** | **Attribute** | **Threat** |
| **Confidentiality** |  |  |
| **Integrity** |  |  |
|  |  |  |
| **Availability** |  |  |



# Security incident management

Attackers try to breach the network by targeting unsecured ports, penetrating network security, or abusing network access.

1. **Alert reception:**

A security alert should come from the monitoring systems, or from a service desk. (reference security incident management, n.d.) From here the company can further analyse the alert and take action if the incident is a security incident.

**Best practices:**

Track connections to your network from the outside to detect intrusions, compromises, malicious software, and even users abusing network access.

Log network flow to record access to and from the internet.

Apply Network Behaviour Anomaly Detection and Network Behaviour Analysis.

So in my company the monitoring systems and operators in an Security Operations Centre (SOC) should detect an issue. When the attack happens, they will then start with the second phase.

2**. Alert Triage and prioritization.**

Triage is the first step to take, after first detection or reception of a security alert. In triage you gather information to be able to determine if the alert is a real incident or a false positive and what the severity and impact of the incident is. From that you determine the priority.  
There are 3 steps in the triage:

1. categorise the incident. How severe is it and what are the potential impacts?  
2. Prioritise. Does this require an urgent escalation, or can it be easily resolved?  
3. Assignment. Who is responsible managing and resolving the incident, and by when?

Traffic from compromised servers may leave distinctly visible patterns, which can be analysed for information or used to mitigate an attack. Identifying this type of traffic can help with the response of the company before data is lost or damaged.

3. **Respond:**

The response can have different types of communication which can all be important.

**The technical response:** This can include analysing the incident, advising on or planning a resolution, co-ordinating actions internally and externally, containing any on-going malicious activity, repairing or recovering any affected systems. With advice from your technology/service provider or accredited IT security consultant may be required.

**Management response:** focuses on activities such as notifying staff and affected customers of a breach and advising of steps taken to resolve the situation, approving courses of action and other communications.

**Legal response:** If the incident involves fraud or cyber crime you should report the incident to the police.

4. **Close the incident and review:**after the incident a review has to be done to see if any further actions have to be taken to minimize the risk of the incident occurring again.

**Attack 1: Network breach and database access.**

1. **categorise the incident. How severe is it and what are the potential impacts?**With the monitoring of the network through pre-setup applications, the SOC team will know that the network has been breached that the attackers have access to the database. Meaning it is very severe and the potential impacts are huge. Once they have access to the network and database, they could delete valuable data.

2. **Prioritise. Does this require an urgent escalation, or can it be easily resolved?**  
This problem would require an quick response since it can deal a lot of damage to the whole company and all of its users.

3. **Assignment. Who is responsible managing and resolving the incident, and by when?**This incident should be solved as fast as possible. The SOC team will inform, the people who maintain the database, the people who maintain the network and the lead of the applications/company. If any user data has been stolen, the company should also inform the police about the incident.

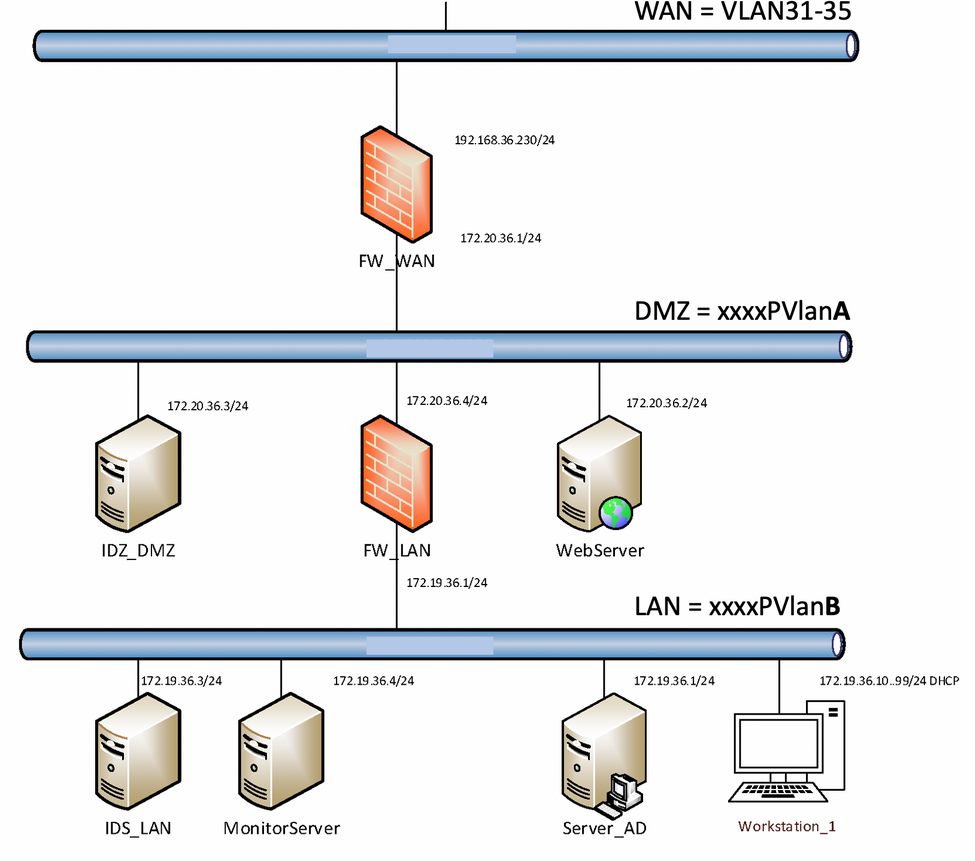
**Attack 2: Port scan detected.**

1. **categorise the incident. How severe is it and what are the potential impacts?**The problem is not severe at all since the scanning of ports itself isn’t something with a huge impact.

2. **Prioritise. Does this require an urgent escalation, or can it be easily resolved?**   
This is not an urgent problem at all since it is not really a in the short run. But it would be wise to keep the most important ports in check.

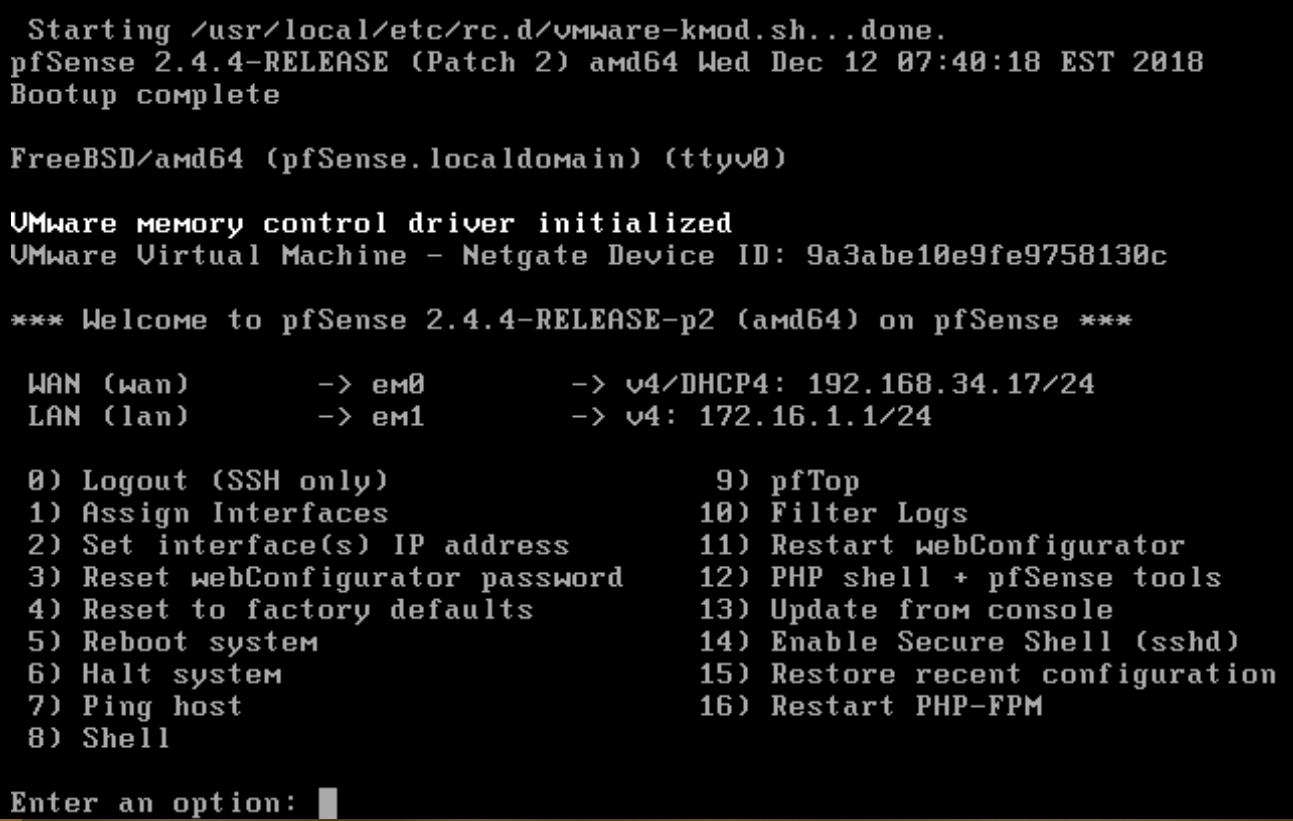
3. **Assignment. Who is responsible managing and resolving the incident, and by when?**

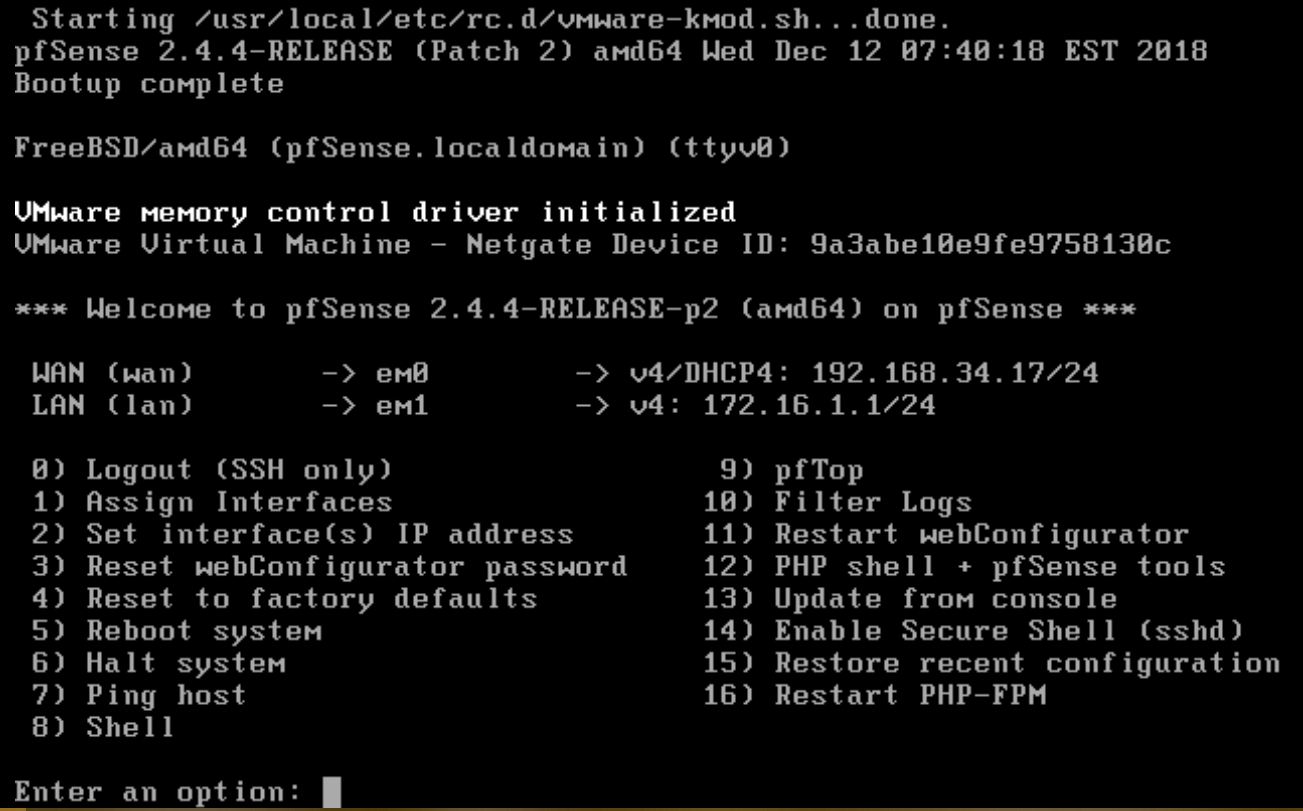
This incident can mostly just be neglected by the company.

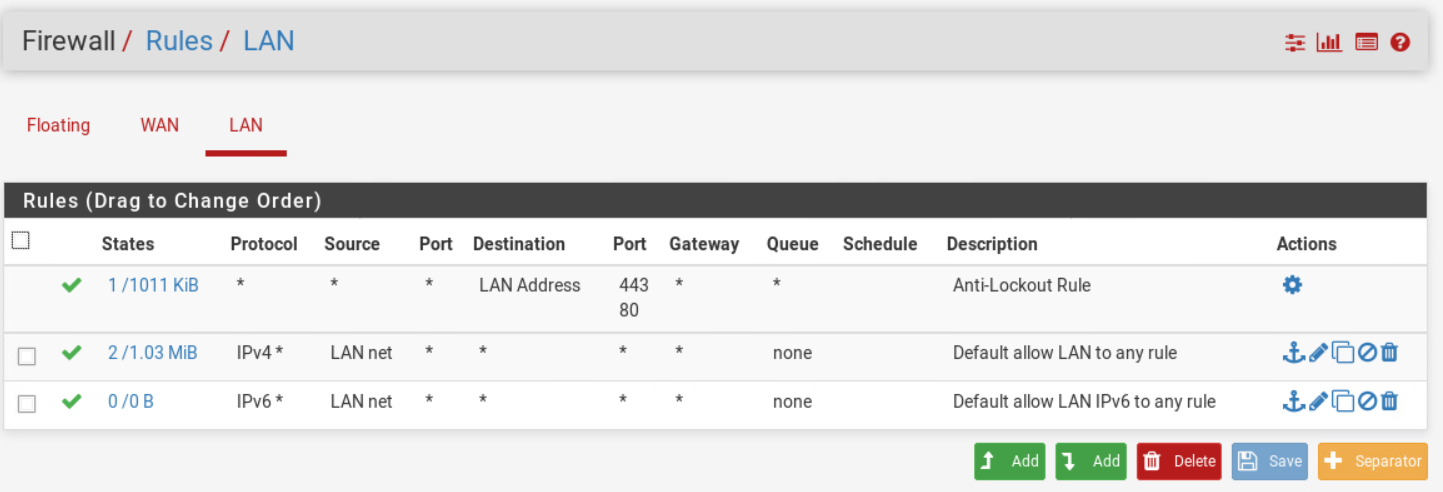


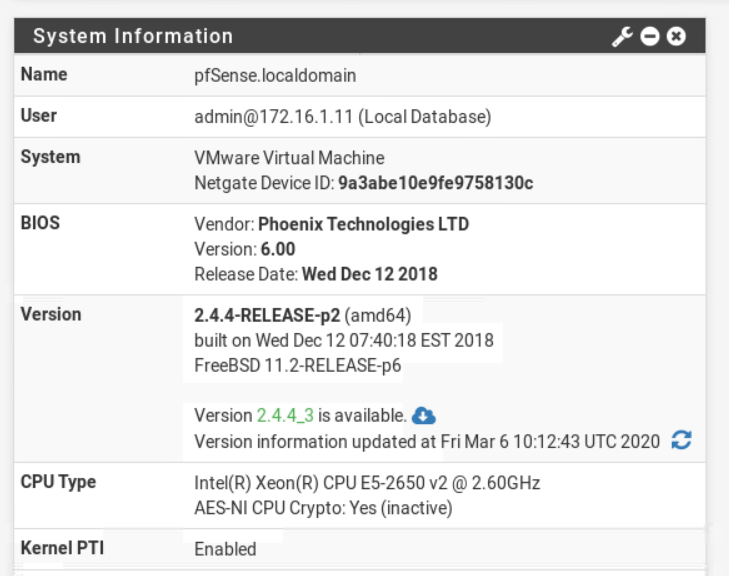
Firewall:

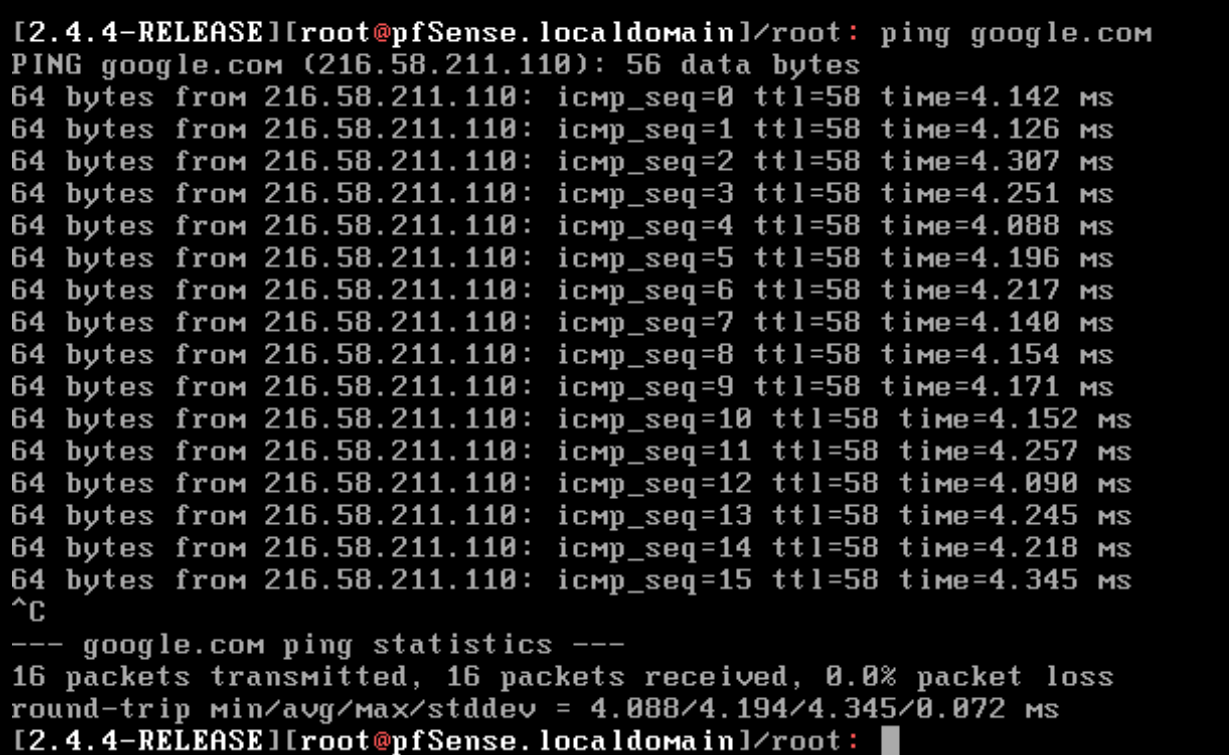
Opzet pfSense:

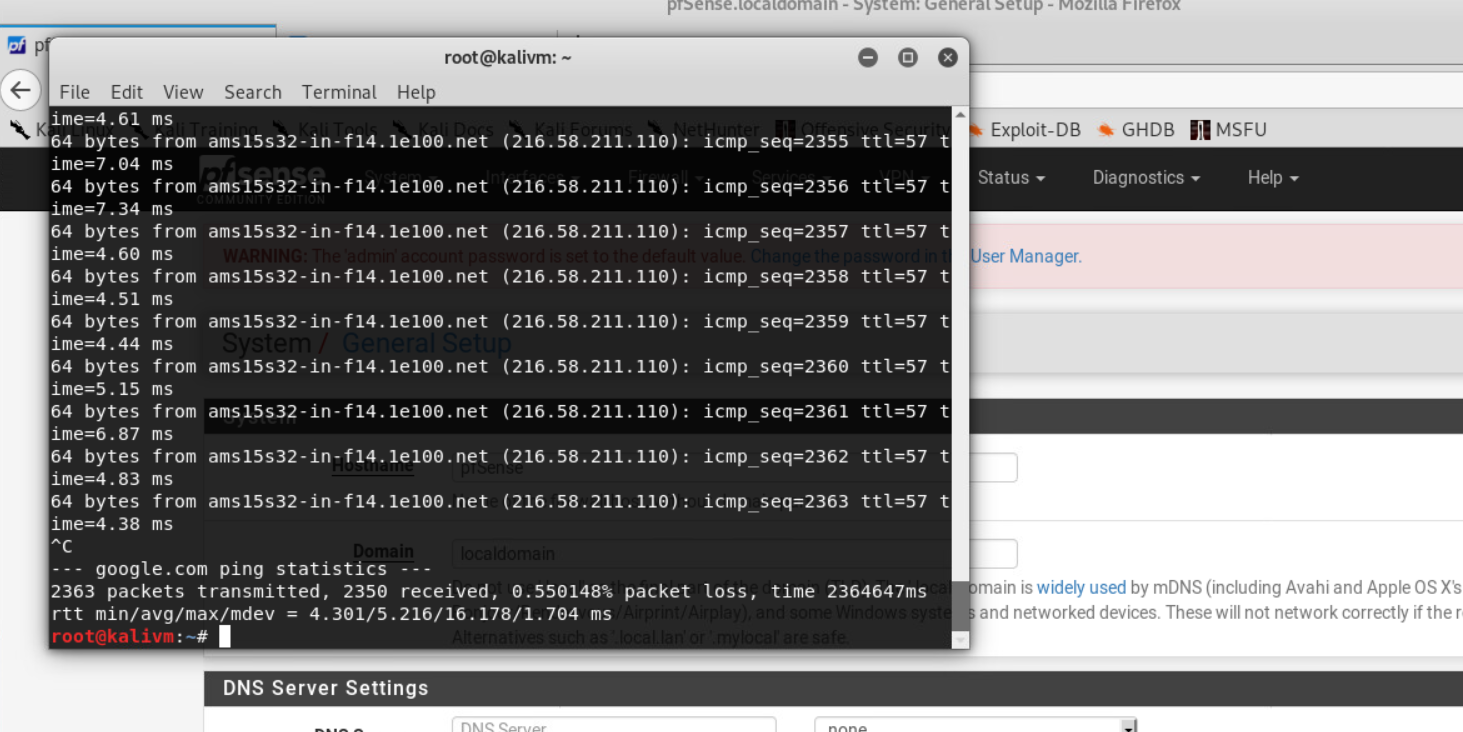












# Bibliography

*explanation basic knowledge assignment*. (n.d.). Retrieved from fhict.instructure: https://fhict.instructure.com/courses/9462/pages/explanation-basic-knowledge-assignment?module\_item\_id=466732

*reference security incident management*. (n.d.). Retrieved from fhict.instructure: https://fhict.instructure.com/courses/9462/pages/reference-security-incident-management?module\_item\_id=466743

# Notes for later

**Network separation:**

Why?

* Security omdat als er 1 gehacked zou worden dan is de rest nog niet gehacked.
* Performance als alles op 1 netwerk zit dan wordt t trager omdat alles broadcast.

Waar plaats je firewalls

1. between a local network and external networks

2. on gateways to important subnets within the LAN

3. End-points user-device/server

Een groter netwerk met meer firewalls betekend niet gelijk dat het veiliger is, als de firewalls niet sterk zijn of niet goed opgezet dan kan het weinig nut hebben.

DMZ: zit een webserver in die met de buitenkant praat.

**Internal examples:** Data center, extranet, remote access, lab, desktop, wireless.

**External:** DMZ, server data center, remote access, test or staging, internet.

**Firewall rules/policies:** DMZ only accessible from the outside, not connected to internal network.

2 kinds of firewalls: **Stateless:** firewall filter, also known as an access.

**Stateful:** firewalls can watch traffic streams from end to end. Firewall might know what the intensions of the user is.

**Next-generation firewall:** NGFWs typically feature advance functions including: application awareness, integrated intrusion prevention systems, identity awareness – user group control.

**Secure connections met crypto:**

Modern crypto: Password hasing, secure connections and transactions/commnications, encrtyped wifi, disk encryption, digitale signatures, digital money, cars.

Symmetrical encryption sender and receiver use the same key

Asymmetrical encryption: every user has a keypair consisting of a

public key

1. used for encryption.

2. check signatures

A private key:

1. used for decryption

2. place signature (signen)

**Never design your own crypto**