Afbeelding met logo

Automatisch gegenereerde beschrijving

Afbeelding met Website

Automatisch gegenereerde beschrijving

Kenzo Staelens

Jonathan van Caloen

Jonas Van den Berghe

Michaël Vasseur

Professionele Bachelor Elektronica-ICT

2022-2023

Mentor: Tom Cordemans

Taalmentor: Sabine Martens

Afbeelding met logo

Automatisch gegenereerde beschrijving

Afbeelding met Website

Automatisch gegenereerde beschrijving

Kenzo Staelens

Jonathan van Caloen

Jonas Van den Berghe

Michaël Vasseur

Professionele Bachelor Elektronica-ICT

2022-2023

Mentor: Tom Cordemans

Taalmentor: Sabine Martens

Malicious Internet traffic interception

K. Staelens, J. van Caloen, J. Van den Berghe, M. Vasseur

This project investigates a way to intercept malicious internet traffic and how a solution can be provided, with an aim for ease of use. By using a webserver as a gateway and a firewall built on software developed in python. Emphasis is placed on the third and fourth network layers.

The first chapter regarding malware is given to understand how malware works. Types of attacks and what effect they have are discussed here. Understanding how it works is a baseline to prevent malicious software from infecting a system and helps develop a solution. Subsequently the existing solutions are described and compared. The next chapter discusses the criteria for efficient malware interception and blocking.

From all the known data, a firewall will be developed that will efficiently analyse the network traffic and throw up the necessary actions. The coming chapters cover the technical side of the solution, aiming to provide a look at the firewall coded in python with a user-friendly interface. Responding to the end user's demand for ease of use.

In the final chapter the evaluation of the project is described. The pros and cons of combining this solution with artificial intelligence for a possible sequel are also stated.

Keywords: Firewall, infrastructure, packet analyser, webserver, malware, artificial intelligence, user-friendly interface

Inhoudsopgave

[codefragmentenlijst 3](#_Toc130396549)

[tabellenlijst 4](#_Toc130396550)

[figurentenlijst 5](#_Toc130396551)

[afkortingenlijst 6](#_Toc130396552)

[begrippenlijst 7](#_Toc130396553)

[Inleiding 8](#_Toc130396554)

[1 Firewalls 8](#_Toc130396555)

[1.1 Wat is een firewall 9](#_Toc130396556)

[1.1.1 Doel 9](#_Toc130396557)

[1.1.2 Werking 9](#_Toc130396558)

[1.2 Types firewall 9](#_Toc130396559)

[1.2.1 Stateless en Stateful 9](#_Toc130396560)

[1.2.2 Stateless Firewalls 10](#_Toc130396561)

[1.2.3 Stateful firewalls 10](#_Toc130396562)

[1.2.7 Hybride firewalls 12](#_Toc130396563)

[2 malware 13](#_Toc130396564)

[2.1 types 13](#_Toc130396565)

[2.2 tekenen van infectie 13](#_Toc130396566)

[2.3 gebruik 13](#_Toc130396567)

[2.4 Type aanvallen 13](#_Toc130396568)

[3 mogelijke oplossingen 14](#_Toc130396569)

[3.1 criteria voor malware detectie 14](#_Toc130396570)

[3.2 mogelijke oplossingen 14](#_Toc130396571)

[3.2.1 python 14](#_Toc130396572)

[3.2.2 c# 14](#_Toc130396573)

[3.3 vergelijking 14](#_Toc130396574)

[4 uiteindelijke oplossing 15](#_Toc130396575)

[4.1 laag drie: Netwerk 15](#_Toc130396576)

[4.2 laag vier: Transport 15](#_Toc130396577)

[4.3 user interface 15](#_Toc130396578)

[5 evaluatie 16](#_Toc130396579)

[Conclusie 17](#_Toc130396580)

[handleiding 18](#_Toc130396581)

[Literatuurlijst 19](#_Toc130396582)

[Bijlagen 20](#_Toc130396583)

[bijlage 1: kopieën van datasheets 21](#_Toc130396584)

[bijlage 2: vergaderverslagen 22](#_Toc130396585)

[bijlage 3: logboek rapporteren 23](#_Toc130396586)

# codefragmentenlijst

# tabellenlijst

# figurentenlijst

# afkortingenlijst

DoS Denial of Service

OSI-model Open Systems Interconnection model

SaaS Software as a Service

FWaaS Firewall as a Service

# begrippenlijst

# Inleiding

Voor dit project wordt er eerst een theoretisch onderzoek gedaan als voorstudie voor het ontwikkelen van een softwarefirewall. De software wordt ontwikkeld in Python. Het project is bedoeld om een beter inzicht te verkrijgen in de werking van malware.   
  
Malware is een samentrekking van de Engelse woorden ‘malicious’ en ‘software’, en wordt vertaald als kwaadaardige software. Het vormt een dagelijkse dreiging voor het internetverkeer en kent vele vormen. Vanuit de vraag naar bescherming wordt er gezocht naar een mogelijke oplossing vanuit het inzicht dat in de voorstudie wordt verkregen. Dergelijke oplossingen bestaan reeds en worden door verschillende softwarebedrijven op de markt gebracht. Het is dan ook niet de kern van dit project om een betere oplossing te bekomen, maar om een ruimer inzicht in een deelaspect van computerbeveiliging te krijgen.   
  
In het eerste hoofdstuk wordt onderzocht wat malware is. In deze studie wordt besproken welke types er bestaan en wat voor effecten deze hebben bij het geïnfecteerde toestel. Vervolgens worden de bestaande oplossingen besproken. Dit hoofdstuk behandeld firewalls en antivirussoftware.   
  
Uit al deze voorgaande kennis wordt in de volgende hoofdstukken een mogelijke oplossing voorgesteld. Deze behandelden de softwarefirewall die ontwikkeld wordt in Python. Het filteren en analyseren van netwerkpakketten moet plaatsvinden op OSI-netwerklaag drie en vier. Netwerkpakketten uit bepaalde landen kunnen een verhoogd risico vormen, deze moeten door de ingebouwde lokalisering worden geblokkeerd. De software moet draaien op een centrale server die samen fungeert met de firewallsoftware. Hierdoor kan deze ook fungeren als een man-in-the-middle. Dit is nodig om HTTPS-pakketten te decrypteren. De firewall moet ook vroegtijdig een DOS-aanval kunnen detecteren en stoppen. Er moet interactie tussen de firewall en de eindgebruiker zijn, zodat deze steeds op de hoogte wordt gesteld van mogelijke aanvallen. De gebruiksvriendelijke interface moet de optie voor een eenvoudig beheer bieden. Ten slotte volgt een voorstel tot een mogelijk vervolg, waar artificiële intelligentie een rol zou kunnen spelen bij de behandeling van netwerkpakketten.   
  
De belangrijkste onderzoeksmethode is literatuurstudie van online bronnen. Het geeft inzicht in de werking van malware en hoe er zich tegen te beschermen. Ook geven de vele testen die worden uitgevoerd op de firewall bij de ontwikkeling vele inzichten.

# 1 Firewalls

## 1.1 Doel

Apparaten verbonden met het internet worden voortdurend aangevallen door andere apparaten. Het doel van de aanvallen wordt in het hoofdstuk malware besproken. Ze kunnen voor onder andere data breaches en downtime zorgen. Bij een data breach worden gevoelige gegevens van klanten of van services gestolen. Deze kunnen dan voor veel geld verkocht worden. Downtime wil zeggen dat een service of machine buiten gebruik zijn. De financiële schade hiervan kan zeer snel hoog oplopen. Zo is de gemiddelde kost voor downtime 5600$ per minuut. [1] Een firewall is de eerste lijn van bescherming voor het blokkeren van dit gevaarlijk en schadelijk netwerkverkeer. Op deze manier worden de dieperliggende netwerkapparaten ook vrijgehouden voor andere taken, waaronder complexere bedreigingen ontdekken. [2] Niet alle malware kan namelijk door de firewall gedetecteerd worden.

## 1.2 Werking

Een firewall kijkt naar de eigenschappen van de netwerkpakketten. Eenvoudige firewalls kijken enkel naar de bron en bestemming van zowel IP-adressen als poorten. Waar complexere firewalls ook kijken naar de patronen van ontvangen en verstuurde pakketten en naar de data die in die pakketten zit. Enkel het netwerkverkeer wordt hier gecontroleerd. Wanneer malware via een ander medium het toestel bereikt en geen verdachte handelingen stelt tijdens de overdracht, worden deze niet gedetecteerd. De manier waarop de detectie gebeurt hangt af van het type firewall.

## 1.3 Types firewall

### 1.3.1 Stateless en Stateful

De klassieke firewalls zijn stateless, dit betekent dat ze enkel kijken naar individuele pakketten. Binnen een pakket kijken ze enkel naar de informatie die in de headers van het pakket te vinden is. De bron- en bestemmingsadressen en poorten zijn belangrijke elementen om te beslissen welke pakketten al dan niet veilig zijn. De andere parameters moeten manueel ingesteld worden door gebruik te maken van regels. Als een pakket niet aan deze regels voldoet wordt het geblokkeerd.

De firewalls die momenteel in productieomgevingen worden gebruikt zijn daarentegen stateful firewalls. Dit houdt in dat het pakket bijgehouden wordt om later te kijken naar patronen in het netwerkverkeer. De mogelijkheid bestaat dus om naar een volledige sessie te kijken. Zo kan een firewall beslissingen nemen op eerder ontvangen verdacht verkeer en die pakketten vroegtijdig tegenhouden zonder nieuwe regels nodig te hebben. [3] [4] Deze functionaliteit loopt parallel met de basisfuncties van een stateless firewall.

### 1.3.2 Stateless Firewalls

#### Packet Filtering Firewall

Dit is een minimale vorm van firewall aangezien de firewall enkel een lijst van regels bevat. Als een pakket binnenkomt bij een packet filtering firewall kijkt die in de geconfigureerde regels en de regels die matchen met de beschrijving van het pakket worden dan gebruikt om een beslissing te nemen. Vaak heeft de beslissing van blokkeren voorrang op het toelaten van een pakket. Als toch een pakket moet doorgelaten worden krijgt de desbetreffende regel een lager ingestelde prioriteit, een lagere waarde voor prioriteit wil zeggen dat een regel meer doorslag heeft op de finale beslissing of een pakket wordt geaccepteerd of niet. [5] Het filteren van pakketten kan op twee manieren. De eerste is whitelisting, deze blokkeert al het netwerkverkeer behalve dat wat in de regels staat. De tweede is blacklisting, hier gebeurt net het omgekeerde. Al het verkeer wordt doorgelaten behalve wat in de regels staat. Het is altijd veiliger om whitelisting toe te passen.

#### Proxy firewall

Een proxy firewall werkt als een standaard proxy met geïntegreerde firewall. Zo’n firewall kan dan ook naar data in de pakketten kijken op lagen vijf tot zeven van het OSI-model. Dit kan omdat de proxy zelf ook een certificaat bevat en daarmee een koppeling maakt met de client die een request stuurt en de server dat request ontvangt. Zo kan de proxy de pakketten decrypteren en naar de data in lagen vijf tot zeven kijken. Het grote voordeel van deze firewall is dat een externe netwerkconnectie geen direct contact kan hebben met het netwerk.

### 1.3.3 Stateful firewalls

#### Next-Generation Firewall

Een next-generation firewall (NGFW) gaat veel verder dan enkel pakketten filteren. Om als next-generation beschouwt te worden, moet de firewall aan een aantal voorwaarden voldoen:

* een slim-aanpassende toegangscontrole gebaseerd op stateful inspectie;
* een geïntegreerd intrusion prevention systeem (IPS);
* mogelijkheid tot upgraden naar nieuwere databronnen;
* URL-filtering gebaseerd op reputatie en geolocatie;
* het controleren en blokkeren van gevaarlijke applicaties;
* detectie over het hele netwerk.

Deze functies zorgen ervoor dat de firewall veel sneller en preciezer kan reageren op mogelijke bedreigingen. Ook zorgt dit ervoor dat een veel kleinere kans bestaat dat de bedreigingen in het lokale netwerk hun functie kan uitvoeren.

De implementatie en verdere functies hangen sterk af van product tot product. Verder worden nog twee types next-generation firewalls aangehaald. [5]

##### Threat-focused Next Generation Firewall

Dit soort firewall houdt zich vooral bezig met bedreigingen detecteren en blokkeren. Dit doet het nog voordat de bedreiging het interne netwerk binnen kan komen. Voordat deze firewall een beslissing neemt worden nog veel meer uitgebreidere testen uitgevoerd dan bij andere firewalls. Om dit te bereiken maakt die onder andere gebruik van een sandbox-omgeving. Dit komt neer op een gemonitorde container die geïsoleerd is van de rest van het systeem. Als die geïnfecteerd wordt door een virus kunnen gepaste maatregelen genomen worden. Hierna wordt de container automatisch verwijderd. Na de procedure in de sandbox wordt een beslissing genomen of het bestand veilig is of niet.

##### Unified threat management (UTM) firewall

Een UTM doet nog meer dan een next-generation firewall en voert ook de taken uit van een traditioneel antivirusprogramma. Waaronder bescherming van individuele apparaten, zoals bescherming tegen dataverlies. De functies kunnen zeer sterk afhangen van de omgeving waarin de UTM-firewall wordt gebruikt. Toch zijn ze makkelijker in gebruik te nemen dan een NGFW. Dit maakt ze interessanter voor kleine tot middelgrote bedrijven.

### 1.3.4 Hardware Firewalls

Hardware firewalls zijn firewalls die op basis van vooraf ingebouwde hardware regels veel sneller kan verweren dan wanneer het op basis van softwareregels moet verwerken. Dit geeft vele voordelen. De eigen hardware en software maakt ze veel veiliger tegen malware dat gebruik maakt van fouten in het onderliggende besturingssysteem. Aangezien ze niet door een besturingssysteem worden verwerkt kunnen andere processen moeilijk inpikken op de beslissingen. Vaak loopt dit zelf over een apart ingebouwde chip en zal de snelheid van de routing niet gehinderd worden door de rekentijd van het checken van pakketten.

Doordat de firewall gecentraliseerd is, is het aanpassen van de configuratie voor de netwerkbeheerder veel gemakkelijker. Dit garandeert dat elk apparaat achter de firewall dezelfde beveiliging krijgt. Ook zorgt dit ervoor dat eindgebruikers en malafide software deze configuraties veel moeilijker kan bereiken.

Aangezien de firewall ingebouwd is in de hardware is het wel moeilijker om de fysieke mogelijkheden te upgraden. Daardoor is vaak een volledig nieuwe firewall nodig. Ze hebben hierdoor ook een veel hogere aankoopprijs. De unieke hardware maakt het ook moeilijker om te onderhouden, vaak is dus een specifieke expertise nodig. Als toch updates moeten uitgevoerd worden zal dit gebeuren door het gebruikte besturingssysteem te updaten.

### 1.3.5 Software Firewalls

Software firewalls kunnen gedraaid worden op niet gespecialiseerde hardware. Dit kan als één of meerdere processen op het besturingssysteem. Vaak worden deze gebruikt als client based firewalls. Hierbij is wel te vermelden dat zo’n firewall wel met root privileges draait. Wanneer malware dus toegang krijgt tot de firewall dan het ook volledige controle over het netwerkverkeer. Vaak hebben dit type firewall veel standaard ingestelde regels.

Nog een mogelijkheid voor het gebruik van een software based firewall is als service op het toegangspunt tot een netwerk. Voordat dit toegangspunt pakketten kan toelaten moeten deze eerst langs de software passeren. Zo kan dit type toch aan de rand van een netwerk staan.

Dit soort firewall is vaak veel kost effectiever dan een hardware firewall omdat de middelen veel makkelijker geschaald kunnen worden. Als de firewall niet genoeg geheugen heeft, kan er simpelweg meer geheugen aan het proces toegewezen worden. Ook is de aankoopprijs veel lager aangezien dit vaak enkel over een softwarelicensie gaat. Het installeren kan volledig van op afstand gebeuren en updates makkelijker te installeren.

### 1.3.6 Cloud Firewalls

Meer en meer delen van organisaties worden naar de cloud verplaatst. Ook de firewall heeft een variant dat in de cloud werkt. Wanneer een organisatie services in de cloud heeft kan dit dus een goede optie zijn. Dit kan als off-site virtuele machines of als een SaaS-model. Een firewall-as-a-Service (FWaaS) aanschaffen heeft een aantal unieke voordelen. Zo heeft deze een veel groter, praktisch onbeperkt, bandbreedtelimiet. Verder kan een FWaaS snel schalen om meer of minder verkeer te kunnen verwerken. Hierdoor kan de startkost zeer klein zijn.

### 1.3.7 Hybride firewalls

Hybride firewalls zijn een combinatie van meerdere firewalls. Zo kan voor verschillende scenario’s op het netwerk een ander type verwerking gebeuren afhankelijk van hoe veilig de verbinding moet zijn. Zo kan in een minder gevoelige regio van het netwerk een minder intensieve firewall gebruikt worden. Hybride firewalls kunnen zo het netwerk veiliger en sneller maken en toch goedkoper zijn.

# 2 malware

## 2.1 types

### 2.1.1 VIRUS

Een computervirus infecteert bestanden door zich van een besmet bestand naar een gezond bestand over te plaatsen. Op deze manier kunnen virussen zich ongecontroleerd verspreiden en zo een heel systeem infecteren.

### 2.1.2 TROJANS

Trojans hebben hun naam gekregen doordat ze zich net als het paard van Troje voordoen als iets dat ze eigenlijk niet zijn. De gebruiker downloadt het bestand en gaat ervanuit dat dit onschuldige software is. Zonder het te weten haalt hij zelf de malware binnen op het systeem en kan hij het zelf de nodige rechten geven om zo extra malware te downloaden.

### 2.1.3 SPYWARE

Spyware is, net zoals de naam zegt, ontworpen om zoveel mogelijk informatie van het systeem te halen. Het kan ook gebruikt worden om specifieke info te zoeken. Zo heb je bijvoorbeeld keyloggers. Ze registreren elke druk op het toetsenbord om op deze manier gebruikersnamen en wachtwoorden te stelen.

### 2.1.4 WORMS

Worms wormen zich als het ware een weg door het netwerk dat verschillende systemen met elkaar verbindt. Doordat ze verspreiden van systeem naar systeem hebben ze geen geïnfecteerde file nodig zoals virussen.

### 2.1.5 RANSOMWARE

Wanneer een systeem overgenomen is door ransomware is het onbruikbaar. Alle bestanden en programma’s worden geblokkeerd. Dit is voor een particulier ongemakkelijk maar voor een bedrijf is dat een ramp. Daarom wordt dit soort malware vaak gebruikt door criminelen om losgeld te vragen voor het deblokkeren van de systemen. Wanneer dit niet gebeurd dreigen ze ermee om alle bestanden te verwijderen.

### 2.1.6 ADWARE

Adware is een vrij onschuldige soort malware. Het verzwakt de beveiliging van het systeem om je constant advertenties te tonen. Dit kan gevaarlijk zijn omdat de zwakke beveiliging een gemakkelijke weg naar binnen kan zijn voor andere malware.

### 2.1.7 SCAREWARE

Scareware is genaamd naar de manier waarop de gebruikers bijna verplicht worden om het te installeren. Zo is er bijvoorbeeld een pop-up die zegt dat er iets mis is met de computer en dat je door deze software het probleem kan oplossen. Zo wordt de gebruiker om de tuin geleidt en kan de malware geïnstalleerd worden.

### 2.1.8 ROOTKITS

Een rootkit valt zeer moeilijk te detecteren. Het geeft de criminelen administratierechten op het geïnfecteerde systeem. Op deze manier kunnen ze de volledige controle over het systeem overnemen.

### 2.1.9 BROWSER HIJACKERS

Browser hijackers zijn relatief ongevaarlijk. Ze nemen je browser over en sturen je naar andere pagina’s en tonen je net als adware zeer veel advertenties.

### 2.1.10 CRYPTOMINERS

### 2.1.11 LOGIC BOMBS

## 2.2 tekenen van infectie

De tekenen die een gebruiker ervaart wanneer zijn systeem geïnfecteerd is hangen af van de soort malware. Iets wat bij bijna altijd voorkomt is het vertragen van het systeem. Dit komt doordat de malware veel middelen van het systeem vraagt om te kunnen doen waarvoor het ontworpen is.

## 2.3 gebruik

BOTNETS

Cryptominer

## 2.4 Type aanvallen

Een systeem kan op verschillende manieren met malware aangevallen en geinfecteerd worden.

# 3 mogelijke oplossingen

## 3.1 criteria voor malware detectie

## 3.2 mogelijke oplossingen

### 3.2.1 python

### 3.2.2 c#

## 3.3 vergelijking

# 4 uiteindelijke oplossing

## 4.1 laag drie: Netwerk

## 4.2 laag vier: Transport

## 4.3 user interface

# 5 evaluatie

# Conclusie

# handleiding

# Literatuurlijst

|  |  |
| --- | --- |
| [1] | L. M. Pelzer, „The True Cost of Cybersecurity Incidents,” paloalto networks, 06 2021. [Online]. Available: https://www.paloaltonetworks.com/blog/2021/06/the-cost-of-cybersecurity-incidents-the-problem/. [Geopend 20 03 2023]. |
| [2] | Check Point, „Key Ingredients of a Strong Firewall,” Check Point, 2023. [Online]. Available: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/key-ingredients-of-a-strong-firewall/. [Geopend 20 03 2023]. |
| [3] | Check Point, „The Different Types of Firewalls,” Check Point, 2023. [Online]. Available: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/the-different-types-of-firewalls/. [Geopend 20 03 2023]. |
| [4] | Fortinet, „Stateful & Stateless Firewall Differences,” Fortinet, 2023. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/stateful-vs-stateless-firewall. [Geopend 21 03 2023]. |
| [5] | Cisco, “What is a next-generation firewall?,” Cisco, 2023. [Online]. Available: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html. [Accessed 22 03 2023]. |
| [6] | Fortinet, „How does a firewall work?,” Fortinet, 2023. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/how-does-a-firewall-work. [Geopend 20 03 2023]. |
| [7] | Fortinet, „Hybrid Firewall Advantages and Disadvantages,” Fortinet, 2023. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/hybrid-firewall-advantages-disadvantages. [Geopend 20 03 2023]. |
| [8] | Cisco, „What is a firewall?,” Cisco, 2023. [Online]. Available: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html. [Geopend 20 03 2023]. |
| [9] | Sangfor Technologies, „What is Software Firewall? Difference between Hardware Firewall and Software Firewall,” Sangfor, 2023. [Online]. Available: https://www.sangfor.com/blog/cybersecurity/what-software-firewall-difference-between-hardware-firewall-and-software. [Geopend 21 03 2023]. |

# Bijlagen

# bijlage 1: kopieën van datasheets

# bijlage 2: vergaderverslagen

# bijlage 3: LOGBOEK rapporteren

|  |  |  |
| --- | --- | --- |
| Jonas Van den Berghe | N.v.t. | Schrijven inleiding, abstract, toevoegen titels, maken van inhoudsopgave. |
| Vasseur Michaël | Kaft, Abstract, 8 | Kaft voorzien van figuur met titel en subtitel. Abstract en inleiding herschreven. |
| Kenzo Staelens | 1 | Inhoudsopgave genereren en paginanummers toevoegen. |
| Jonathan van Caloen | N.v.t, Kaft, 9-12 | Aanpassen van titels en subtitels van de hoofdstukken.  Herwerken structuur kaft, herwerken structuur document, H1 firewalls geschreven, bronnenlijst aangemaakt |
| Jonas Van den Berghe | 9-12 | Aanpassen H1 firewalls |
| Kenzo Staelens | 9-12 | Aanpassen H1 firewalls |
| Vasseur Michaël | 9-12 | Aanpassen H1 firewalls |
| Jonas Van den Berghe | 9-12 | Verbeteren H1 firewalls |
| Vasseur Michaël | 9-12 | Verbeteren H1 firewalls |
| Jonas Van den Berghe | 13 | Schrijven H2 malware |