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 usisng 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 analyze 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 9](#_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 9](#_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

# 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 software bedrijven 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 geolokalisering 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 Wat is een firewall

### 1.1.1 Doel

Apparaten verbonden met het internet worden voortdurend aangevallen. Deze aanvallen kunnen voor onder andere data breaches en downtime zorgen. De financiële schade hiervan kan zeer hoog oplopen. Bijvoorbeeld de gemiddelde kost voor downtime is 5600$ per minuut. [1] Een firewall is de eerste lijn van bescherming voor het blokkeren van dit gevaarlijk netwerkverkeer. Dit houdt de dieper liggende netwerkapparaten ook vrij voor andere taken, waaronder complexere bedreigingen te ontdekken. [2]

### 1.1.2 Werking

Een firewall kijkt naar de eigenschappen van de netwerkpakketten. Simpele firewalls gebruiken de bron- en bestemmingsip-adressen en bron- en bestemmingspoorten. Complexere firewalls kijken ook naar de patronen van ontvangde en verstuurde pakketten en naar de data die in die pakketten zit.

## 1.2 Types firewall

### 1.2.1 Stateless en Stateful

De klassieke firewalls zijn stateless, dit betekent dat ze enkel kijken naar individuele pakketten. Verder kijken stateless firewalls enkel naar de informatie die in de headers van de packet te vinden is. Zoals onder andere de bron- en bestemmingsip-adressen en bron- en bestemmingspoorten.

De modernere firewalls zijn stateful wat in houd dat er naar een volledige sessie wordt gekeken. Een sessie is bijvoorbeeld een volledige TCP-transactie. De firewall kan dan onderzoeken of elk onderdeel van de TCP-transactie correct gebeurt. Stel dat er een bevestiging van het TCP-SYN-pakket wordt ontvangen zonder dat er een TCP-SYN-pakket was verstuurd, dan kan een stateful firewall dit blokkeren. [3] [4]

### 1.2.2 Stateless Firewalls

#### Packet Filtering

Dit is een zeer simpele vorm van firewall. De firewall bevat enkel een lijst regels. Voor elk pakket wordt deze lijst overlopen. Wanneer een pakket met één van de regels matcht wordt de pakket behandeld volgens die regel.

#### Proxy firewall

Proxy firewalls werken als een tussenstop voor al het netwerkverkeer, en fungeren dus als een Man-in-the-Middlemachine. De proxy firewall werkt voornamelijk in de zevende laag van het OSI-model. Hier analyseert het verkeer van bijvoorbeeld HTTP en FTP verkeer. Dit is mogelijk omdat clients requests sturen naar de proxy en de firewall deze dan analyseert om ze dan verder te sturen. Ook kan de proxy als caching server etc. dienen.

### 1.2.3 Stateful firewalls

#### Next Generation Firewall

Een next-generationfirewall gaat veel verder dan enkel pakketten filteren. Om als next-generation beschouwt te worden, moet de firewall aan volgende voorwaarden voldoen:

* 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 kan reageren op mogelijke bedreigingen. Ook zorgt dit ervoor dat er een veel kleinere kans is 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 NGFW aangehaald, maar elk bedrijf heeft hier hun eigen versie van met verschillende mogelijkheden. [5]

#### Threat-focused NGFW

Deze soort firewalls houdt zich, zoals de naam al vertelt, vooral bezig met bedreigingen detecteren en blokkeren. Dit probeert het te doen nog voor dat de bedreiging het interne netwerk binnen komt. Om dit te bereiken gebruikt het onder andere een sandbox-omgeving. Hier worden gedownloade bestanden en applicaties in uitgevoerd om te detecteren wat voor effect ze hebben. Als een bestand niet door alle checks geraakt, wordt dit gemeld aan de netwerkbeheerder.

#### Unified threat management (UTM) firewall

Een UTM doet nog meer dan een next-generationfirewall en voert ook de taken uit van een traditionele antivirus. Waaronder bescherming van individuele apparaten, bijvoorbeeld bescherming tegen dataverlies. Ook bevat een UTM-firewall vaak bescherming tegen spam-emails en gelijkaardige bedreigingen. 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.

#### 1.2.4 Hardware Firewalls

Hardwarefirewalls zijn firewalls dat op hun eigen hardware, specifiek ontwikkeld voor hun doel werken. Dit geeft vele voordelen. De eigen hardware en software maakt ze veel veiliger tegen malware dat gebruik maakt van fouten in het onderliggende besturingsysteem. Tevens doordat ze gescheiden zijn kunnen ze aan de netwerkgrenzen geplaatst worden waardoor ze veel efficiënter het verkeer dat over de grens komt kunnen controleren. Ook gebruiken ze niet de middelen dat gebruikt zouden kunnen worden door andere processen. Zoals bandbreedte van de netwerkinterfaces, of processortijd. Dit zorgt er voor dat de performantie voor andere processen niet variëert met het volume van netwerkverkeer.

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.

Maar hun eigen hardware maakt het veel moeilijker om de fysieke mogelijkheden te upgraden. Om dit te bereiken 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, en vaak is er specifieke expertise nodig. Updates moeten vaak gebeuren door het besturingsysteem te updaten, wat voor lange downtime kan zorgen.

#### 1.2.5 Software Firewalls

Softwarefirewalls zijn een proces dat draait op al bestaande hardware. Dit kan als een gewoon programma op het besturingsysteem. Deze beschermen dus meestal enkel het apparaat waarop de firewall draait. Dit betekent ook dat eindgebruikers en malafide software makkelijk toegang hebben tot de firewall. De hoeveelheid bescherming kan voor dit type makkelijk aangepast worden per apparaat.

Een tweede type is zeer gelijkaardig aan een hardwarefirewall, maar hier draait de firewall in een gevirtualiseerde omgeving in plaats van om eigen hardware. Dit zorgt er voor dat de firewall grotendeels dezelfde functionaliteit kan hebben als een hardwarefirewall. Doch met enkele beperkingen waaronder vaak het delen van systeemmiddelen.

Dit soort firewall is vaak veel kost effectiever dan een hardwarefirewall 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 ook volledig van op afstand gebeuren. Ook zijn updates makkelijker te installeren en zijn deze frequenter.

#### 1.2.6 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 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.

### 1.2.7 Hybride firewalls

Hybride firewalls verwerken meerdere types firewall in een netwerk. Zo kan bijvoorbeeld een cloudfirewall gebruikt worden voor de cloudservices en connectie met het internet te beveiligen. Een next-gen firewall voor het interne netwerk te beveiligen op malware en als tweede lijn van bescherming van de buitenwereld.

Hybride firewalls kunnen het netwerk veiliger en sneller maken, en terwijl goedkoper zijn. Ook kunnen nieuwe types firewall makkelijk getest en toegevoegd worden op het al bestaande netwerk zonder downtime.

# 2 malware

## 2.1 types

## 2.2 tekenen van infectie

## 2.3 gebruik

## 2.4 Type aanvallen

# 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 |