|  |
| --- |
| **SURFids Data Visualisatie** |
| HoneyPot data visualisatie met Kibana |
|  |
| SURFids bestaat uit een aantal HoneyPots die data verzamelen. SURFids biedt onvoldoende mogelijkheden om deze data te visualiseren en correleren. Met ElasticSearch, Logstash en Kibana kunnen deze mogelijkheden gemakkelijk en efficiënt worden toegevoegd. |
|  |
| **Gijs Rijnders, Hin Liu, Dominik De Smit, Mathijs Cox, Lennart van Oosterhoud, Robin Wolters** |
| **16-1-2015** |
|  |

Inhoudsopgave

[Inleiding 3](#_Toc409163726)

[Voorwaarden 3](#_Toc409163727)

[ELK (Elasticsearch, Logstash, Kibana) Stack 4](#_Toc409163728)

[Java 7 4](#_Toc409163729)

[Installatie 4](#_Toc409163730)

[Elasticsearch 4](#_Toc409163731)

[Installatie 4](#_Toc409163732)

[Configuratie 4](#_Toc409163733)

[Kibana 5](#_Toc409163734)

[Installatie 5](#_Toc409163735)

[Configuratie 5](#_Toc409163736)

[Nginx 6](#_Toc409163737)

[Installatie 6](#_Toc409163738)

[Configuratie 6](#_Toc409163739)

[Logstash 6](#_Toc409163740)

[Installatie 6](#_Toc409163741)

[Configuratie 7](#_Toc409163742)

[Logstash Forwarder 8](#_Toc409163743)

[Installatie 8](#_Toc409163744)

[Configuratie 9](#_Toc409163745)

[GEO Ip 9](#_Toc409163746)

[Installatie 9](#_Toc409163747)

[Wereldkaart toevoegen in Kibana 10](#_Toc409163748)

[Toevoegen van honeypots aan ELK 13](#_Toc409163749)

[Installatiehandleiding 13](#_Toc409163750)

[Stap 1: Forwarden van gewenste logbestanden naar logstash 13](#_Toc409163751)

[Stap 2: Grok-filter schrijven om de data te vertalen voor logstash 13](#_Toc409163752)

[Bibliografie 14](#_Toc409163753)

# Inleiding

Het doel van dit document is om de ELK stack op te zetten binnen de SURFids omgeving en om logs van verschillende honeypots te verzamelen en te visualiseren. Door middel van correlatie kunnen bijvoorbeeld trends worden ontdekt.

We hebben 4 basis componenten nodig:

* Logstash is de module die alle inkomende logs verwerkt en opslaat;
* Elasticsearch is de module die logs indexeert en realtime zoekopdrachten mogelijk maakt;
* Kibana is de web interface om de logs te visualiseren;
* Logstash Forwarder is de module die de logs doorstuurt naar logstash. Logstash forwarder moet worden geïnstalleerd op servers waar logs worden gegenereerd.

Na het opzetten van de ELK stack in combinatie met SURFids is er een werkend dashboard voor de weergave van aanvallen en bedreigingen.

### Voorwaarden

Om succesvol de ELK stack op te zetten is root toegang op een Ubuntu 14.04 machine nodig. De systeemvereisten voor de machine hangen af van het volume van de logs die verzameld moeten worden. In deze handleiding wordt uitgegaan van een machine met 4GB RAM en 2 processoren.

Er wordt uitgegaan dat de lezer een basiskennis van Linux bevat en kennis heeft van SURFids.

# ELK (Elasticsearch, Logstash, Kibana) Stack

## Java 7

### Installatie

Elasticsearch en Logstash vereisen Java 7. Java 7 wordt aanbevolen door ElasticSearch. Voer het volgende commando uit om de JRE (Java Runtime Environment) en JDK (Java Development Kit) te installeren.

sudo apt-get install openjdk-7-jre openjdk-7-jdk

Als Java 7 is geïnstalleerd kunnen we verder gaan.

## Elasticsearch

### Installatie

Let op: Logstash 1.4.2 beveelt Elasticsearch 1.3.5 aan.

Importeer de Elasticsearch publieke GPG sleutel in apt:  
wget -O - http://packages.elasticsearch.org/GPG-KEY-elasticsearch | sudo apt-key add -

Maak een source-list aan voor Elasticsearch:  
echo 'deb http://packages.elasticsearch.org/elasticsearch/1.3/debian stable main' | sudo tee /etc/apt/sources.list.d/elasticsearch.list

Update de package database:  
sudo apt-get update

Installeer Elasticsearch:

sudo apt-get -y install elasticsearch

### Configuratie

Nu Elasticsearch is geïnstalleerd kan de configuratie aangepast worden:  
sudo vi /etc/elasticsearch/elasticsearch.yml

We willen toegang van buitenaf blokkeren omdat er anders verbindingen via poort 9200 mogelijk zijn. Er kan data uit Elasticsearch worden lezen en de server kan afgesloten worden. Zoek de regel die “network.host” bevat en haal het commentaarkarakter weg. De regel ziet er nu als volgt uit:  
network.host: localhost

Sla het bestand op en herstart de Elasticsearch service op de server:

sudo service elasticsearch restart

Voer het volgende commando uit om Elasticsearch te starten wanneer de machine opstart:

cd /etc/init.d;sudo update-rc.d elasticsearch defaults 95 10

## Kibana

### Installatie

Let op: Logstash 1.4.2 beveelt Kibana 3.1.2 aan.

Download Kibana met het volgende commando. Kibana zal worden opgeslagen in de home directory van de ingelogde gebruiker:  
cd ~; wget https://download.elasticsearch.org/kibana/kibana/kibana-3.1.2.tar.gz

Pak het Kibana archief uit:  
tar xvf kibana-3.1.2.tar.gz

### Configuratie

Open nu het Kibana configuratie bestand:  
sudo vi ~/kibana-3.1.2/config.js

Zoek de regel die begint met “elasticsearch” en vervang het poortnummer (9200) met 80:  
elasticsearch: "http://"+window.location.hostname+":80",

Dit is nodig omdat we Kibana op port 80 willen benaderen.

We gaan Nginx gebruiken om onze Kibana web interface te hosten. Hiervoor moeten we een directory aanmaken en de bestanden verplaatsen:  
sudo mkdir -p /var/www/kibana3

Kopieer nu de Kibana files in de zojuist aangemaakte directory:   
sudo cp -R ~/kibana-3.1.2/\* /var/www/kibana3/

Voordat we de Kibana web interface kunnen gebruiken moeten we Nginx installeren. Daar gaan we nu mee verder.

## Nginx

### Installatie

Installeer Nginx:  
sudo apt-get install nginx

We moeten nu instellen dat alle verzoeken die op poort 80 binnen komen worden doorgestuurd naar poort 9200 waarop Elasticsearch luistert. Kibana heeft hiervoor een eigen Nginx configuratiebestand dat we gaan downloaden. Het bestand zal in de home directory worden opgeslagen:.  
cd ~; wget https://gist.githubusercontent.com/thisismitch/2205786838a6a5d61f55/raw/f91e06198a7c455925f6e3099e3ea7c186d0b263/nginx.conf

### Configuratie

Open nu het configuratiebestand om een aantal aanpassingen te maken:  
vi nginx.conf

Zoek en verander de waardes van “server\_name” naar de FQDN (of localhost als er geen domein naam gebruikt wordt) en “root” naar de plaats waar Kibana is geïnstalleerd:  
server\_name FQDN; root /var/www/kibana3;

Sla het bestand op en sluit de tekstverwerker. Kopieer het bestand vervolgens naar het default Nginx server block:  
sudo cp nginx.conf /etc/nginx/sites-available/default

We gaan nu apache2-utils installeren. Dit maakt het mogelijk om htpasswd te gebruiken. We gaan htpasswd gebruiken om een gebruikersnaam en wachtwoord te genereren:  
sudo apt-get install apache2-utils

Genereer een gebruikersnaam- en wachtwoordcombinatie die Kibana kan gebruiken om dashboards op te slaan, te wijzigen of te delen. Vervang ‘user’ door een eigen username.   
sudo htpasswd -c /etc/nginx/conf.d/kibana.myhost.org.htpasswd user

Voer een wachtwoord in. Het htpasswd-bestand is nu aangemaakt.

Herstart Nginx om de wijzigingen door te voeren:  
sudo service nginx restart

Kibana kan nu benaderd worden via de FQDN of het IP adres van de Logstash Server. Wanneer je daar naartoe gaat zie je de startpagina van Kibana met een aantal standaard dashboards. Er zijn nog geen logs beschikbaar omdat we deze nog niet geconfigureerd hebben.

## Logstash

### Installatie

De Logstash package is beschikbaar op dezelfde repository als Elasticsearch. Hiervan hebben we de publieke sleutel al. Maak een source-list voor Logstash:  
echo 'deb http://packages.elasticsearch.org/logstash/1.4/debian stable main' | sudo tee /etc/apt/sources.list.d/logstash.list

Update de package database:  
sudo apt-get update

Installeer Logstash:  
sudo apt-get install logstash=1.4.2-1-2c0f5a1

### Configuratie

#### SSL Certificaten Genereren

Omdat we voor het versturen van logs Logstash Forwarder gaan gebruiken moet er een SSL certificaat en keypair worden gemaakt. Het certificaat wordt gebruikt door Logstash Forwarder om de identiteit van de Logstash Server te verifiëren. Maak de directories waar het certificaat en de keys opgeslagen gaan worden:  
sudo mkdir -p /etc/pki/tls/certs sudo mkdir /etc/pki/tls/private

Genereer nu het SSL certificaat en private sleutel in de boven gecreëerde locatie (/etc/pki/tls/...), met het volgende commando:  
cd /etc/pki/tls; sudo openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout private/logstash-forwarder.key -out certs/logstash-forwarder.crt

Het *logstash-forwarder.crt* bestand wordt gekopieerd naar alle servers die logs gaan versturen naar Logstash. Hierop komen we later terug.

#### Logstash Configureren

De configuratiebestanden van Logstash zijn in JSON-formaat en zijn opgeslagen in /etc/logstash/conf.d. De configuratie is in drie delen op te splitsen: input, filters, en output.

Maak een bestand genaamd: “01-lumberjack-input.conf” om vervolgens de ‘lumberjack’ input plugin te configureren. Dit is het protocol dat Logstash Forwarder gebruikt.  
sudo vi /etc/logstash/conf.d/01-lumberjack-input.conf

Zet de volgende configuratie in het aangemaakte bestand:  
input {

lumberjack {

port => 5000

type => "logs"

ssl\_certificate => "/etc/pki/tls/certs/logstash-forwarder.crt"

ssl\_key => "/etc/pki/tls/private/logstash-forwarder.key" } }

Deze configuratie specificeert een lumberjack input die luistert op tcp poort 5000, het gegenereerde SSL certificaat en de bijbehorende private sleutel gebruikt.

Als laatste moet er een configuratiebestand worden gemaakt dat ervoor zorgt dat de logs doorgestuurd worden naar Elasticsearch door middel van het Lumberjack protocol.

sudo vi /etc/logstash/conf.d/30-lumberjack-output.conf

Zet de volgende configuratie in het aangemaakte bestand:

output {

elasticsearch {

host => localhost

}

stdout {

codec => rubydebug

}

}

Andere configuraties toevoegen gaat op dezelfde manier in hetzelfde soort bestanden. Waar op gelet moet worden is dat de bestanden tussen het input en output configuratie bestand moeten komen, dus een cijfer tussen de 01 en 30 moeten krijgen.

Herstart Logstash om de wijzigingen door te voeren:  
sudo service logstash restart

Nu dat de Logstash server geconfigureerd is kunnen we naar de configuratie van de Logstash Forwarders gaan kijken.

## Logstash Forwarder

Let op: Volg deze stappen voor elke server waar honeypot logs op komen te staan.

### Installatie

#### SSL Certificaat Kopiëren

Verstuur vanaf de Logstash server het SSL certificaat naar de server waarop de logstash forwarder is geïnstalleerd (vervang ‘user’ en ‘server\_private\_IP’ door eigen gegevens):  
scp /etc/pki/tls/certs/logstash-forwarder.crt  
user@server\_private\_IP:/tmp

#### Logstash Forwarder Package Instaleren

Op de server waar logstash forwarder wordt geïnstalleerd moet een source list aangemaakt worden. Doe dit op de volgende manier:  
echo 'deb http://packages.elasticsearch.org/logstashforwarder/debian stable main' | sudo tee /etc/apt/sources.list.d/logstashforwarder.list

Nu kunnen we de Logstash Forwarder package gaan installeren op de volgende manier:  
sudo apt-get update sudo apt-get install logstash-forwarder

Let op: Als er een 32-bit versie van Ubuntu wordt gebruikt moet het volgende commando in plaats van het bovenstaande worden uitgevoerd:  
wget https://assets.digitalocean.com/articles/logstash/logstash-forwarder\_0.3.1\_i386.deb sudo dpkg -i logstash-forwarder\_0.3.1\_i386.deb

Vervolgens willen we het Logstash Forwarder init script installeren zodat Logstash Forwarder tijdens het opstarten zal worden uitgevoerd:  
cd /etc/init.d/; sudo wget https://raw.github.com/elasticsearch/logstash-forwarder/master/logstash-forwarder.init -O logstash-forwarder; sudo chmod +x logstash-forwarder; sudo update-rc.d logstash-forwarder defaults

Kopieer nu het SSL certificaat naar de juiste locatie (/etc/pki/tls/certs):  
sudo mkdir -p /etc/pki/tls/certs; sudo cp /tmp/logstash-forwarder.crt /etc/pki/tls/certs/

### Configuratie

Nu gaan we de Logstash Forwarder configuratie file aanpassen. Dit bestand is in JSON formaat:  
sudo vi /etc/logstash-forwarder

Voeg nu de volgende regels toe aan het bestand en vervang ‘logstash\_server\_private\_IP’ door het IP van de Logstash server:

{

"network": {

"servers": [ "logstash\_server\_private\_IP:5000" ],

"timeout": 15,

"ssl ca": "/etc/pki/tls/certs/logstash-forwarder.crt"

},

"files": [

{

"paths": [

"/var/artillery/logs/alerts.log "

],

"fields": { "type": "Artillery" }

}

]

}

Sla op en exit. Hiermee word de verbinding tussen Logstash Forwarder en de Logstash server op poort 5000 vastgelegd. Onder ‘paths’ moeten de locaties van de honeypot logs worden beschreven. En de type beschrijft welke honeypot het betreft.

Herstart Logstash Forwarder om de wijzigingen door te voeren:  
sudo service logstash-forwarder restart

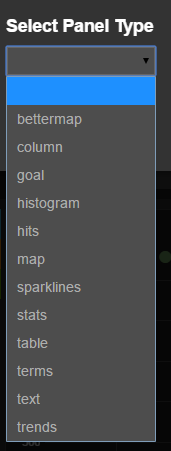
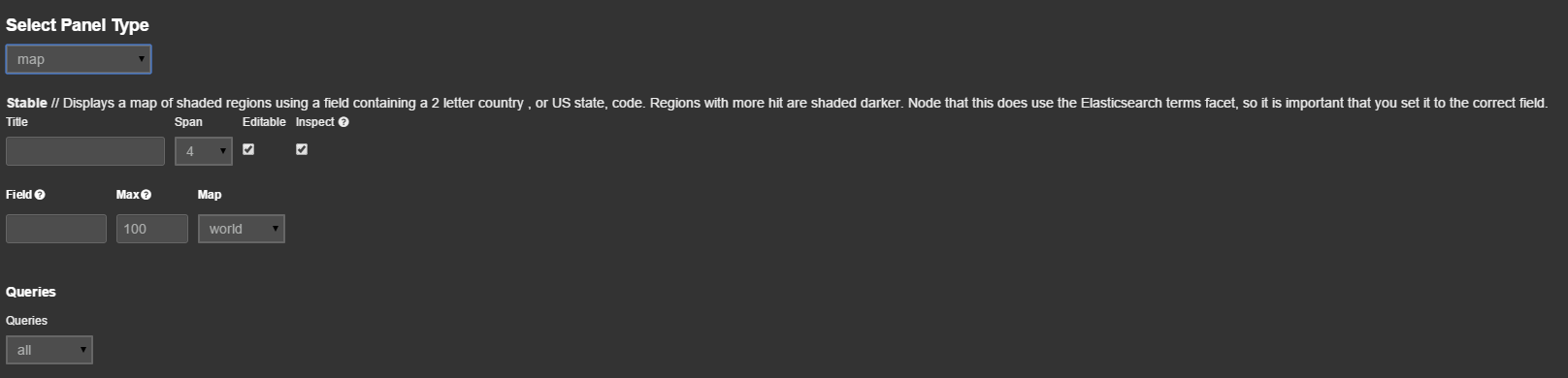
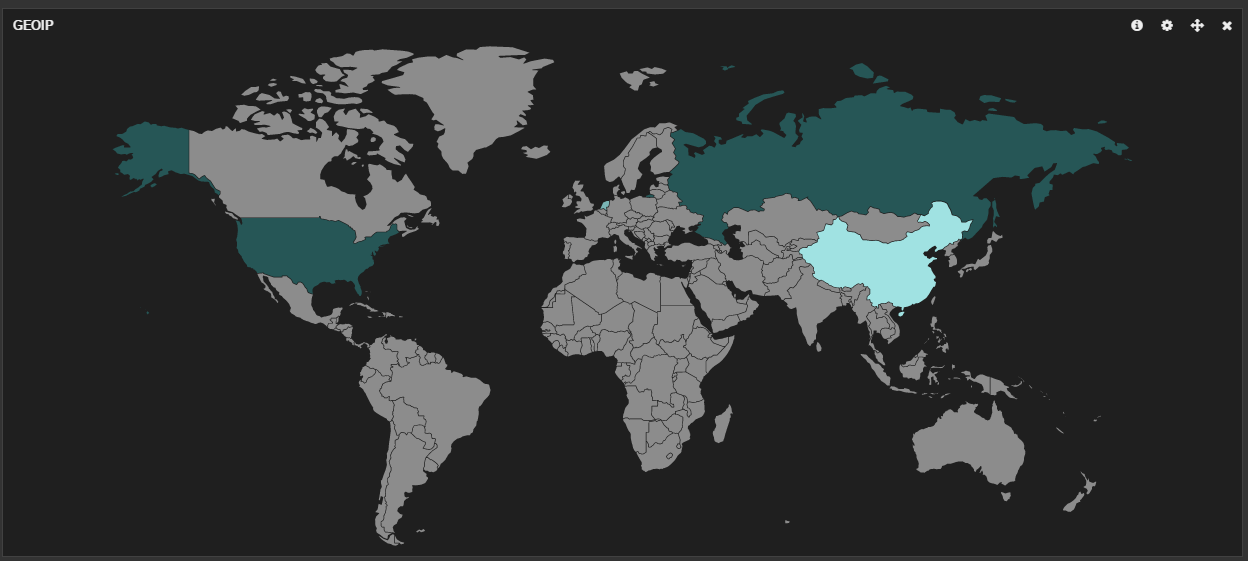
Herhaal dit proces voor elke server waar honeypot logs op komen.

## GEO Ip

### Installatie

1. Voer het commando “sudo nano /etc/logstash/conf.d/%bestandsnaam%” uit. Kies als %bestandsnaam% een duidelijke naam met een uniek ID ervoor. Bijvoorbeeld: 05-geoip.conf.
2. Plaats de onderstaande tekst in het bestand (src\_ip is het veldnaam van de gefilterde IP address).  
   
3. Voer het commando “sudo service logstash restart” uit om de Logstash service te herstarten.

### Wereldkaart toevoegen in Kibana

1. Open het dashboard van Kibana.
2. Klik op de “configure” knop rechtsboven in het dashboard.  
   
3. Klik op “Rows”.  
   
4. Vul een “Title” en een “Height” in beschrijvend voor de GEO-ip widget in het dashboard.  
   
5. Klik op “Create Row” en daarna op “Save” om de widget op te slaan.  
   
6. Klik onderaan de pagina op de knop “Add panel to empty row” om de widget toe te voegen aan het dashboard.  
   
7. Klik op “Map” in de panel type list.  
   
8. Vul alle velden in. Het veld field dient de 2-letter landcode te bevatten. In het geval van de GEO-ip plugin is dit “geoip.country\_code2”.
9. Klik op “Save”.  
   
10. Het resultaat ziet er als volgt uit:  
    
11. Klik rechtsboven op de “save” icon om het dashboard op te slaan.  
      
    

# Toevoegen van honeypots aan ELK

## Installatiehandleiding

Dit stappenplan kan gebruikt worden om de log van een honeypot te exporteren naar de ELK stack (Elasticsearch, Logstash & Kibana).

Let op: De honeypot dient geïnstalleerd te zijn voordat aan deze handleiding wordt begonnen.

### Stap 1: Forwarden van gewenste logbestanden naar logstash

Eerst moet de locatie van de honeypot logs worden bepaald. Wanneer de locatie(s) ofwel het pad naar de honeypot bekend is dient dit te worden toegevoegd aan het configuratiebestand van de logstash forwarder. De locatie van deze configfile is: /etc/logstash-forwarder

Hierin dient de locatie van de log te worden gespecificeerd, met een field die aangeeft van welke honeypot de log komt.

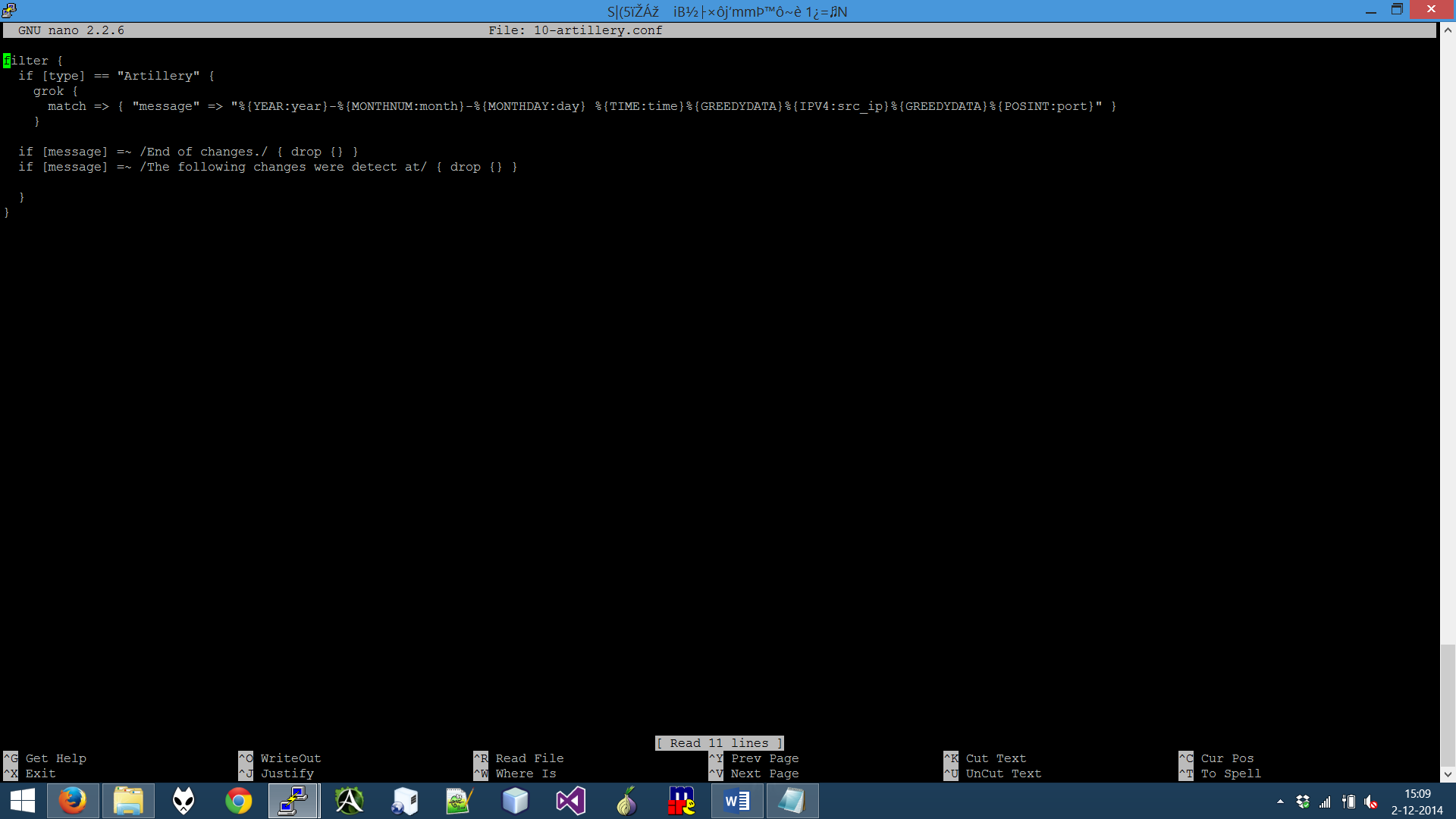
### Stap 2: Grok-filter schrijven om de data te vertalen voor logstash

Vervolgens moet er een grok-filter gemaakt worden. Dit filter geeft aan welke datavelden er aangemaakt worden voor de betreffende log. De syntax van grok-filter is als volgt:

Figuur 1 Voorbeeld logstash-forwarder config

%{TIMESTAMP\_ISO8601:time} %{GREEDYDATA},%{IPV4:src\_ip},%{GREEDYDATA}

De filter is opgebouwd uit de losse filters %{SYNTAX:SEMANTIC}. De syntax geeft het type data aan. Binnen Logstash zijn er vooraf gedefinieerde syntaxis. De semantic geeft de naam aan die wordt gebruikt binnen logstash en wordt weergegeven op het Kibana dashboard. Tussen de losse filters kunnen seperators worden aangegeven. Deze seperators worden niet opgenomen in de data in logstash. Een seperator kan worden aangegeven door een filtercomponent toe te voegen dat geen semantic heeft.

De grok-filter wordt toegevoegd op de locatie: /etc/logstash/conf.d/$FILENAME. De $FILENAME heeft als syntax $ID-$NAME.conf waar $ID een uniek cijfer tussen de 1 en 30 is en $NAME de naam van de honeypot gebruikt dient te worden. Als laatste moet Logstash herstart worden via het commando “sudo service logstash restart”.

Figuur 2 Voorbeeld grok-filter Artillery honeypot

# Bibliografie

(2015, Januari 16). Opgehaald van logstash - open source log management: http://logstash.net/docs/1.4.2/filters/grok

(2015, Januari 16). Opgehaald van logstash/patterns at v1.4.2 · elasticsearch/logstash · GitHub: https://github.com/elasticsearch/logstash/tree/v1.4.2/patterns

Heinlein, R. A. (2015, Januari 16). Opgehaald van Grok Debugger: http://grokdebug.herokuapp.com