**Handleiding**

Project SecMon

Opdrachtgever: Arnim Eijkhoudt, Hogeschool van Amsterdam

Project: Project SecMon

Originele Auteurs: Dave van Ast, Stanley Numan, Jasper Groot

Verbeterd door: Christiaan Druif

Datum: 30 juni 2014

Versie: 0.3

Status: Final

# Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Omschrijving | Auteur |
| 0.1 | 28-06-2013 | Final versie | Dave van Ast, Stanley Numan en Jasper Groot |
| 0.2 | 27-06-2014 | Concept van vernieuwde versie | Christiaan Druif |
| 0.3 | 30-06-2014 | Final versie | Christiaan Druif |

Table of Contents

[Versiebeheer 2](#_Toc391552648)

[1. Inleiding 4](#_Toc391552649)

[2. Overzicht applicatie 5](#_Toc391552650)

[3. Beschrijving modules 6](#_Toc391552651)

[4. Configuratie van de applicatie 7](#_Toc391552652)

[4.1. Mappenstructuur van de applicatie 7](#_Toc391552653)

[4.2. Algemene applicatieconfiguratie 7](#_Toc391552654)

[4.3. Configuratie definities 8](#_Toc391552655)

[4.3.1. Aanmaken nieuwe definitie 8](#_Toc391552656)

[4.4. Configuratie rule bestanden 9](#_Toc391552657)

[4.4.1. Aanmaken van een rule 10](#_Toc391552658)

[4.5. Configuratie rule bestanden 11](#_Toc391552659)

[4.5.1. Aanmaken actiescripts 11](#_Toc391552660)

[5. Webpagina 12](#_Toc391552661)

[6. Applicatie starten, stoppen, herstarten en status opvragen. 14](#_Toc391552662)

# Inleiding

Dit document dient als handleiding voor de applicatie Security Monitor (SecMon). In dit document wordt de opbouw van de applicatie beschreven. Daarnaast worden de verschillende modules van de applicatie beschreven en wordt beschreven hoe de applicatie geconfigureerd en beheerd kan worden.

De applicatie SecMon is een product wat is voortgekomen uit het project Security Monitor, onderdeel van de minor Forensic Intelligence and Security aan de Hogeschool van Amsterdam.

Het project is voor het eerst in 2013 gemaakt door Dave van Ast, Stanley Numan, Jasper Groot, Sujen Kandasamy en Vinesh Koenjbiharie. In 2014 is het project door Christiaan Druif aangepast en verbeterd.

Het doel van het project was het opleveren van een applicatie die de VMWare omgeving van de Hogeschool van Amsterdam kan beschermen tegen cyber-aanvallen van zowel binnen uit als buitenaf. De applicatie moet in staat zijn verschillende aanvallen te herkennen en daarop volgend een actie uit te voeren. Dit moet gerealiseerd worden door middel van het parsen van de firewall log(s). Daarna is de applicatie uitgebreid waardoor het nu ook mogelijk is om andere logfiles, zoals Apache logfiles te parsen.

# Overzicht applicatie

Onderstaand een overzicht van alle onderdelen van de applicatie.

* **secmon** *(root directory)*
  + **Core** *(core componenten directory)*
    - Config.txt
    - Configuration.py
    - Daemon.py
    - FileManager.py
    - Main.py
    - Monitor.py
    - securitymonitor.py
    - Trigger.py
    - Rules.py
    - MatchManager.py
    - SearchManager.py
  + **Custom** *(gebruikers componenten directory)*
    - **Actions**
      * Email.py
    - **Rules**
      * RuleDefinitionTable.txt
      * <naam rule>.txt

De structuur van de applicatie is als volgt:

/secmon/core

/secmon/custom

/secmon/custom/rule

/secmon/custom/actions

# Beschrijving modules

In de core componenten directory ‘secmon/core/’ bevinden de volgende modules:

* Configuration.py
  + Deze module leest Config.txt, waar de configuratie in staat. Andere bestanden maken hier gebruik van. Bijvoorbeeld om de mail configuratie in te stellen.
* Daemon.py
  + Deze module zorgt ervoor dat de applicatie daadwerkelijk gestart, gestopt en herstart kan worden als een Disk And Execution MONitor. Deze module wordt door securitymonitor.py aangesproken door wijze van argumenten.
* FileManager.py
  + Deze module zorgt ervoor dat de rules worden uitgelezen door Rules.py aan te spreken en leest tevens de logfiles uit.
* Main.py
  + Deze module zorgt ervoor dat de monitor wordt aangeroepen en start daarmee in principe het monitoren van de applicatie.
* Monitor.py
  + Deze module is de kern van de applicatie en is het combinatiestuk met alle andere modules.
* Rules.py
  + Deze module zorgt ervoor dat de verschillende bestanden in de rules directory worden uitgelezen en zet deze in een dictionary. Tevens wordt de RuleDefinitionTable.txt uitgelezen en in een dictionary gezet.
* Securitymonitor.py
  + Deze module zorgt ervoor dat de applicatie als Daemon kan worden gestart door middel van argumenten. De volgende vier mogelijkheden kunnen worden gebruikt: start, stop, status of restart.
* MatchManager.py
  + Deze module zorgt ervoor dat de matches die in de rule zijn opgegeven in een aparte lijst worden gezet. De matches zijn de sleutelwoorden waarop er in de log gezocht gaat worden. Deze matchlist wordt in deze module opgebouwd en gecombineerd met de dictionary van de RuleDefinitionTable.txt
* SearchManager.py
  + Deze module ontvangt de matchlist van de MatchManager.py. Aan de hand van deze matchlist wordt er een regex opgebouwd waarmee de opgegeven logfile wordt geparsed op zoek naar matches. Tevens worden hier de counts bijgehouden en indien nodig wordt er aangegeven of er een actie uitgevoerd moet worden. Dit wordt doorgegeven aan de Trigger.py
* Trigger.py
  + De module zorgt ervoor dat er een actie wordt uitgevoerd. De actie die wordt uitgevoerd wordt uit de rule dictionary gehaald.

# Configuratie van de applicatie

## Mappenstructuur van de applicatie

Onderstaand de onderdelen van de applicatie benoemd met een korte uitleg.

**/secmon/**

Dit is de hoofdmap van de applicatie, waarin de submappen /core en /custom staan.

**/secmon/core**

Dit is de map waar alle kritieke onderdelen van de applicatie staan.

**/secmon/custom**

Dit is de map waar de actions en rules staan.

**/secmon/custom/rules**

Dit is de map waar de rules staan. Elk bestand in deze map wordt uitgelezen, niet elk bestand kan gebruikt worden. Het bestand moet wel plain-tekst zijn.

**/secmon/custom/actions**

In deze map staan de actiebestanden, standaard staat alleen de Email.py actie in deze map.

## Algemene applicatieconfiguratie

Nadat de applicatie op de server is geplaatst zijn er een aantal punten die aangepast dienen te worden aan de specifieke locatie van applicatie en de modules. De bestanden die aangepast moeten worden zijn:

* Config.txt

In de Config.txt dienen de juiste waardes en paden opgegeven te worden achter het ‘=’ teken. De standaard opmaak ziet er als volgt uit.

// directories of the Files

logDir = [pad naar de firewall log]

ruleDir = [pad naar de rulebestanden]

actionDir = [pad naar actiebestanden]

interval = 30

fromaddr = sendfrom@example.com

toaddr = sendto@example.com

username = [smtpserver username]

password = [password]

server = smtp.server.com:[poort]

sleeptimer = 0.01

Deze waardes kunnen aangepast worden naar eigen configuratie en credentials. Om deze file aan te passen is er een optionele mogelijkheid om gebruik te maken van een webGUI. zie hoofdstuk Webpagina.

## Configuratie definities

RuleDefinitionTable.txt is een configuratiebestand die optioneel is om te wijzigen. Dit bestand zal alleen worden gewijzigd in een situatie waar een nieuwe definitie aangemaakt moet worden. Dit bestand wordt gebruikt als een mapping van sleutelwoorden die te vinden zijn in logs en die gebruikt kunnen worden in de rule bestanden.

De standaard inhoud van het bestand is als volgt:

PROTOCOL = 'PROTO='

SOURCEIP = 'SRC='

SOURCEPT = 'SPT='

TARGETIP = 'DST='

TARGETPT = 'DPT='

Er kunnen op elk moment definities toegevoegd worden.

Het woord *voor* de ‘=’ teken is een definitie die gebruikt kan worden in de rule bestanden voor het definiëren van rules. Het woord/waarde wat *ná* de ‘=’ komt is een sleutelwoord die te vinden is in de firewalllog en deze moet overeenkomen met wat er daadwerkelijk in een firewalllog voorkomt. Anders werkt de mapping niet.

### Aanmaken nieuwe definitie

Dit bestand is dus alleen maar nodig als er extra informatie nodig is voor een match. Bijvoorbeeld: In een logfile van iptables willen we als er boven de 400 UDP pakketten van een bepaald IP-adres afkomstig zijn, een actie ondernemen. In de logfile van iptables wordt het protocol als PROTO=UDP aangegeven. In de rule file is PROTOCOL = UDP opgegeven bij protocol. In de RuleDefinitionsTable.txt staat PROTOCOL = ‘PROTO=’. Na combinatie wordt er gezocht op PROTO=UDP, exact zoals het in de logfile staat.

Een nieuwe definitie wordt automatisch uitgelezen en er wordt automatisch een match gevonden bij de rule. Wel moet dezelfde keyword gebruikt worden. Dus PROTOCOL in de rule, moet ook PROTOCOL in de RuleDefinitionsTable.txt zijn.

## Configuratie rule bestanden

In de directory /var/secmon/custom/rule/ kunnen rulebestanden worden aangemaakt en gewijzigd. In een rulebestand worden sleutelwoorden met waarden aangemaakt. De meeste sleutelwoorden zijn woorden die ‘gemapped’ zijn aan sleutelwoorden die logs teruggevonden kunnen worden, zoals het sleutelwoord: TARGETIP. Deze is gemapped aan het sleutelwoord ‘DST=’ binnen de firewalllog. Sleutelwoorden zoals: NAME, DESCRIPTION, COUNT en ACTION zijn geen mappings die gekoppeld zijn aan de firewalllog, maar zijn wel essentieel voor de applicatie.

Hieronder een aantal voorbeeld sleutelwoorden. De sleutelwoorden met een \* zijn verplicht.

NAME = ‘’

\*DESCRIPTION = ‘’

SOURCEIP =

SOURCEPT =

TARGETIP =

TARGETPT =

PROTOCOL =

MESSAGE =

\*COUNT [<,<=,>,>=,=]

INTERVAL = hh:mm:ss

\*ACTION = ‘’

\*MATCH =

\*LOG =

|  |  |  |
| --- | --- | --- |
| Sleutelwoord | Operator | Uitleg |
| Name | = | Hier kan binnen de ‘’ een naam opgegeven worden van de rule. |
| Description | = | Hier kan binnen de ‘’ een beschrijving opgegeven worden van de rule. |
| SOURCEIP | = | Hier kan een source IP adres opgegeven. |
| SOURCEPT | = | Hier kan een source poort opgegeven. |
| TARGETIP | = | Hier kan een target IP adres opgegeven. |
| TARGETPT | = | Hier kan een target poort opgegeven. |
| PROTOCOL | = | Hier kan een protocol, zoals: UDP of TCP opgegeven worden. |
| COUNT | [<,<=,>,>=,=] | Hier kan een packet teller opgegeven worden. |
| INTERVAL | hh:mm:ss | Hier kan een tijdbereik opgegeven worden. |
| ACTION | = | Hier kan één of meerdere action script opgegeven worden |
| LOG | = | De logfile waar de rule op doelt |
| MESSAGE | = | Een zin waar de logfile naar kan kijken, zoals een bepaalde error melding in een Apache error log |
| MATCH | = | Een lijst van sleutelwoorden, waar in de rules op gezocht wordt. Dus bijvoorbeeld SOURCEIP, TARGETIP, PROTOCOL |

### Aanmaken van een rule

Rules kunnen worden aangemaakt in plain-text formaat onder de locatie /var/secmon/custom/rules/.

Een nieuwe rule hoeft niet aan speciale eisen te voldoen, alleen dat het een plain-tekst bestand is. Zoals bovenstaand aangegeven zijn de volgende sleutelwoorden verplicht:

**DESCRIPTION**

Verplicht omdat deze in Email.py wordt gebruikt om aan te geven welke rule het betreft wat getriggerd is.

**COUNT**

Verplicht omdat de applicatie moet weten bij welke hoeveelheid matches er getriggerd moet worden

**ACTION**

Verplicht omdat de applicatie moet weten welke actie(s) ondernomen moeten worden bij een trigger.

**MATCH**

Wordt gebruikt voor de matchlist. Hierin staan vermeld op welke sleutelwoorden er in een logbestand gezocht moeten worden. Zonder deze sleutelwoord wordt er niets gematcht.

**LOG**

Geeft aan welke log gebruikt moet worden.

Onderstaand een voorbeeld van hoe een rule eruit kan zien:

NAME = 'DoS TCP flood attack'

LOG = log.txt

DESCRIPTION = 'Rule check for: (TCP flood)-TCP packets with a threshold of 400 or more that are targeted at a specific target IP.'

SOURCEIP = 145.92.6.10

TARGETIP = 192.168.2.128

PROTOCOL = TCP

COUNT > 20

ACTION = 'Email.py'

MATCH = SOURCEIP, PROTOCOL, TARGETIP

## Configuratie rule bestanden

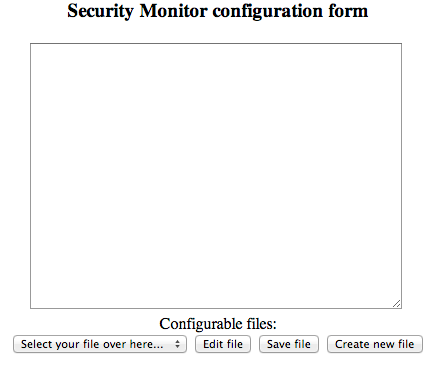
Onderstaand een beschrijving van hoe een actie script aangemaakt kan worden.

### Aanmaken actiescripts

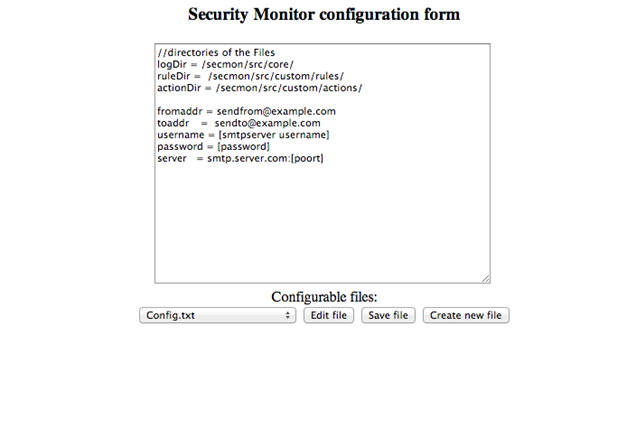
Actiescripts kunnen naar eigensmaak worden gemaakt bijvoorbeeld in Python. In Trigger.py worden argumenten meegegeven aan actiescripts die staan opgegeven in een een rulebestand. In de standaardlevering van de applicatie is een email notificatie script meegeleverd. Deze is te vinden onder /var/secmon/custom/actions. Binnen deze directory kunnen meerdere actiescripts worden aangemaakt, vergeet niet om deze op te geven in een rulebestand anders werkt de actiescript niet. Om de actiescript op te geven in een rulebestand moet er achter het sleutelwoord ACTION = en binnen de single quotes de naam + extensie van de actiescript worden opgegeven. Bijvoorbeeld: ACTION = ‘Email.py’ of ACTION = ‘Email.py, test.test’. Meerdere opgegeven actiescripts moeten worden gescheiden met een komma.

# Webpagina

Met de levering van de applicatie wordt er ook een webform meegeleverd geschreven in PHP. Via dit webform kunnen de configuratie files worden aangepast. Als de directory wijzigt, moet in het webform ook de directory/pad worden gewijzigd, dit wordt opgegeven achter de variabele **$rootDir**.



Via het dropdown menu “ select your file over here” kan de Config.txt gekozen worden. Klik edit file en het bestand word geopend in het tekstvak.



De waardes in de configuratie kunnen nu aangepast worden. Zodra dit voltooid is dient er op “Save File” geklikt te worden om de nieuwe configuratie op te slaan.

De webGui is opgebouwd in PHP en heeft ook apache in combinatie met de PHP nodig om te kunnen werken.

# Applicatie starten, stoppen, herstarten en status opvragen.

Het uitvoeren van het onderstaande vereist minimaal zonder enige toepassingen/wijzigingen dat de gebruiker in de directory zit waar het bestand ‘securitymonitor.py’ zich ook bevindt. Dit wordt gerealiseerd door de cd command, die hieronder staat opgegeven.

Het starten van de applicatie kan door middel van het onderstaande worden uitgevoerd:

* + - cd /var/secmon/core
    - securitymonitor.py start

Het stoppen van de applicatie wordt via de volgende manier uitgevoerd:

* + - cd /var/secmon/core
    - securitymonitor.py stop

Het herstarten van de applicatie wordt via de volgende manier uitgevoerd:

* + - cd /var/secmon/core
    - securitymonitor.py restart

De status opvragen van de applicatie wordt op de volgende manier uitgevoerd:

* + - cd /var/secmon/core
    - securitymonitor.py status