***Visualisatie opdracht:***

***Netwerkmonitoring en Beveiliging met SNMP en Syslog***

**Inleiding**

Dit project is een theoretische denkoefening waarin ik visueel en stapsgewijs heb geleerd wat nodig is om een netwerkmonitoringssysteem op te zetten. Door gebruik te maken van protocollen zoals SNMP en tools zoals Syslog, kunnen netwerk- en systeembeheerders real-time inzicht krijgen in netwerkprestaties, beveiligingsproblemen detecteren en waarschuwingen genereren.

Hoewel dit project niet praktisch is uitgevoerd, heb ik door middel van een visuele aanpak een duidelijk stappenplan uitgewerkt, inclusief benodigde technologieën en configuraties.

**Doelstellingen**

1. Begrijpen hoe SNMP werkt voor het monitoren van netwerkapparatuur zoals routers en switches.
2. Leren hoe een Syslog-server wordt geconfigureerd om loggegevens van netwerkapparatuur te ontvangen en te analyseren.
3. Theoretisch een real-time dashboard ontwerpen met tools zoals Grafana.
4. Begrijpen hoe proactieve meldingen kunnen worden ingesteld bij beveiligingsincidenten.

**Benodigdheden**

**Hardware**

* Netwerkapparatuur:
  + Routers en switches die SNMP en Syslog ondersteunen.
* Servers:
  + Virtuele of fysieke servers om monitoringtools te hosten.
* Firewalls:
  + Optioneel voor extra beveiligingslagen.

**Software**

* **Linux-distributie**:
  + Bijvoorbeeld Ubuntu Server 22.04.
* **Monitoringtools**:
  + Zabbix of Nagios voor SNMP-integratie.
* **Logbeheer**:
  + Graylog of Rsyslog om Syslog-berichten te beheren.
* **Dashboardtools**:
  + Grafana voor visuele weergave van statistieken.
* **Scriptingtools**:
  + Python of Bash voor automatisering.

**Stappenplan**

**1. Netwerkconfiguratie**

**Wat moet gebeuren:**

1. Configureer **SNMP** op netwerkapparatuur om real-time statistieken zoals CPU-gebruik, RAM-gebruik en netwerkverkeer te verzamelen.
2. Stel **Syslog** in om loggegevens van netwerkapparatuur te verzenden naar een centrale Syslog-server.

snmp-server community public RO

snmp-server enable traps

logging host 192.168.1.10

logging trap debugging

* public: SNMP-community string voor read-only toegang.
* 192.168.1.10: Het IP-adres van de Syslog-server

**2. Serverconfiguratie**

**Wat moet gebeuren:**

1. Installeer een Syslog-server zoals **Rsyslog** op een Linux-server.
2. Configureer SNMP-tools zoals Net-SNMP om SNMP-gegevens te verzamelen.

**Voorbeeldinstallatie van Rsyslog op Ubuntu:**

sudo apt update

sudo apt install rsyslog

sudo systemctl start rsyslog

sudo systemctl enable rsyslog

**Configuratiebestand aanpassen (/etc/rsyslog.conf):**

module(load="imudp") # UDP-module laden

input(type="imudp" port="514") # UDP-poort 514 activeren

module(load="imtcp") # TCP-module laden

input(type="imtcp" port="514") # TCP-poort 514 activeren

**Herstart Rsyslog na wijzigingen:**

sudo systemctl restart rsyslog

**3.Dashboard Setup**

**Wat moet gebeuren:**

1. Installeer Grafana en koppel dit aan monitoringtools zoals Zabbix en Rsyslog.
2. Ontwerp panels om belangrijke statistieken zoals netwerkverkeer en CPU-gebruik visueel weer te geven.

**Installatie van Grafana op Ubuntu:**

**Wat moet gebeuren:**

1. Installeer Grafana en koppel dit aan monitoringtools zoals Zabbix en Rsyslog.
2. Ontwerp panels om belangrijke statistieken zoals netwerkverkeer en CPU-gebruik visueel weer te geven.

**Installatie van Grafana op Ubuntu:**

sudo apt install -y software-properties-common

wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -

sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"

sudo apt update

sudo apt install grafana

sudo systemctl start grafana-server

sudo systemctl enable grafana-server

**Panels ontwerpen in Grafana:**

1. Open de webinterface (http://<IP-server>:3000).
2. Voeg een datasource toe (bijv. Zabbix of Prometheus).
3. Maak een nieuw dashboard en voeg panels toe zoals:
   * CPU-gebruik
   * RAM-gebruik
   * Netwerkverkeer (inbound/outbound)

**4. Beveiliging en Waarschuwingen**

**Wat moet gebeuren:**

1. Analyseer loggegevens met Graylog of Rsyslog om verdachte activiteiten te identificeren.
2. Stel waarschuwingen in voor kritieke gebeurtenissen zoals port scanning.

**Simulatie van een port scan met Nmap:**

nmap -sS 192.168.1.100

**Waarschuwingen instellen in Graylog:**

1. Maak een stream met specifieke filterregels (bijv. meldingen met “critical”).
2. Koppel een alarm aan deze stream, zoals een e-mailnotificatie.

**Testen**

**Simulatie van netwerkprestaties:**

* Gebruik tools zoals **iperf** om verhoogd netwerkverkeer te simuleren:

iperf -s (op server)

iperf -c <IP-server> -t 60 (op client)

**Simulatie van beveiligingsincidenten:**

* Voer een port scan uit met **Nmap** en controleer of meldingen worden gegenereerd.

**Validatie van het dashboard:**

* Controleer of Grafana het juiste netwerkverkeer en CPU-gebruik weergeeft.

**Resultaat**

Dit project heeft geleid tot een theoretisch werkend model voor netwerkmonitoring. Hoewel het niet praktisch is uitgevoerd, biedt het:

* Een duidelijk overzicht van benodigde technologieën en configuraties.
* Inzicht in de integratie van tools zoals SNMP, Syslog en Grafana.
* Een solide basis om dit in de toekomst praktisch te implementeren.