SOC Documentatie

1. Network setup

De labomgeving bestaat uit een gesegmenteerd netwerk waarin zowel aanval- als detectiecomponenten aanwezig zijn. Het doel van deze opstelling is om gecontroleerde aanvallen op een doelwit uit te voeren en vervolgens via het SOC te kunnen detecteren, analyseren en rapporteren.

De opstelling bestaat uit volgende virtuele machines:

Kali VM (attacker)

OPNsense Firewall VM

Wazuh-server VM (SOC/SIEM)

Target VM (slachtoffersysteem met DVWA en SSH)

Het netwerkverkeer verloopt als volgt:

Kali VM → OPNsense Firewall VM → Target VM

|

└→ Wazuh-server VM (logverwerking en detectie)

Deze architectuur bootst een klein bedrijfsnetwerk na: een interne target host achter een firewall en een aparte SOC-omgeving die loggegevens centraliseert en analyseert.

2. Netwerkconfiguratie

OPNsense Firewall

De firewall vormt de scheiding tussen de aanvaller en het interne labnetwerk.

Outside interface: NAT DHCP (verbinding met de host / internet)

Inside interface: 192.168.56.1

Functies:

routering van verkeer tussen attacker en target

firewall logging

potentiële bron voor SOC-detecties

Wazuh Server

De Wazuh server fungeert als SOC-platform en ontvangt loggegevens van de verschillende systemen.

IP-adres: 192.168.56.10

Functies:

verzameling en correlatie van logs

detectie van brute force en webaanvallen

genereren van alerts

eventueel automatisering (notificaties)

Target VM

Het doelwit van de aanvallen.

IP-adres: 192.168.56.20

Geïnstalleerde diensten:

DVWA (Damn Vulnerable Web Application)

SSH-server

Doel:

gecontroleerd aanvallen

detectie van malafide activiteiten door SOC valideren

3. Voorbereide aanvallen

In dit project worden zowel handmatige als geautomatiseerde aanvallen uitgevoerd. Deze aanvallen dienen niet om systemen te compromitteren, maar om te testen of het SOC deze activiteiten correct kan registreren en alarmeren.

3.1 Manuele aanval – SQL Injection

Er wordt een handmatige aanval uitgevoerd tegen de DVWA webapplicatie.

type aanval: SQL injection

doel: misbruik maken van inputvelden in DVWA

doelstelling:

kwaadaardige parameters invoeren

zien of de webserver foutmeldingen/logs genereert

nagaan of Wazuh deze activiteit detecteert

verwachte logging:

webserver access/error logs

Wazuh webattack regels (bijvoorbeeld injection patterns)

3.2 Geautomatiseerde aanval – Hydra SSH bruteforce

Hydra wordt gebruikt als adversary simulation tool voor brute-force aanvallen.

doelwit: SSH-dienst op 192.168.56.20

type aanval: geautomatiseerde wachtwoordpogingen

reden van keuze:

duidelijk detecteerbaar patroon

veel mislukte authenticaties

realistische aanvalssituatie

verwachte logging:

meerdere mislukte SSH inlogpogingen

Wazuh authentication-failure alerts

eventueel firewall rate-limit logs

3.3 Geautomatiseerde aanval – Burp Suite

Burp Suite wordt ingezet als tweede adversary tool gericht op de DVWA webapplicatie.

gebruik van:

spidering

parameter fuzzing

basic active scanning

doel:

webapplicatieverkeer genereren

verdachte requests veroorzaken

testen van Wazuh web-aanval detectie

verwachte logging:

grote hoeveelheid HTTP-requests

detectie van verdacht gedrag

mogelijke triggers voor SQLi, XSS of directory probing regels

4. SOC-detectie en monitoring

De Wazuh server verzamelt logs van:

target machine (SSH, webserver)

OPNsense firewall

systeemlogs