Intrusion Detection System (IDS)

Ein Intrusion Detection System (IDS) ist ein wesentlicher Bestandteil der Netzwerksicherheit. Es überwacht den Netzwerkverkehr auf verdächtige Aktivitäten, sowohl in Echtzeit als auch durch die Analyse von Protokolldaten, und warnt Administratoren bei Verdacht auf unbefugte Zugriffe oder Angriffe.

1. Snort-Installation und -Konfiguration

Erklärung: Snort ist ein Open-Source-IDS, das als Paket-Analyse-Tool funktioniert und in der Lage ist, sowohl alarmierende als auch präventive Maßnahmen zu ergreifen.

Installation

Snort installieren:

- **sudo apt update**

sudo apt install snort

- Netzwerk-Interface konfigurieren: Bei der Installation werden Sie aufgefordert, die Netzwerkschnittstelle anzugeben, die Snort überwachen soll (z.B. eth0 oder wlan0).

- Überprüfen Sie die Installation:

snort -V

Grundkonfiguration

Konfigurationsdatei anpassen: Die Hauptkonfigurationsdatei befindet sich normalerweise unter /etc/snort/snort.conf. Sie sollten diese Datei überprüfen und anpassen, um den Pfad zu den Regeln, Logdateien und der Netzwerkumgebung festzulegen.

Regeln festlegen: Snort verwendet Regeln, um verdächtigen Verkehr zu identifizieren. Diese befinden sich in /etc/snort/rules. Sie können Regeln gemäß Ihrer Anforderungen hinzufügen oder anpassen.

Snort im IDS-Modus betreiben: Um Snort im IDS-Modus zu starten, verwenden Sie:

sudo snort -A console -c /etc/snort/snort.conf -i [Ihre Netzwerk-Schnittstelle]

Snort als Dienst einrichten (optional): Sie können Snort als Dienst einrichten, um es im Hintergrund laufen zu lassen.

Verwendung von Netzwerksicherheits-Scanning-Tools

Erklärung: Netzwerksicherheits-Scanning-Tools wie nmap helfen dabei, Schwachstellen durch Scannen des Netzwerkverkehrs und Erkennen offener Ports zu identifizieren.

nmap-Installation und -Verwendung

Installation

nmap installieren:

sudo apt update

sudo apt install nmap

Grundlegende Verwendung

Scannen eines Hosts auf offene Ports: Um einen einzelnen Host auf offene Ports zu scannen, verwenden Sie:

- **nmap [IP-Adresse]**
- Scannen eines Subnetzes: Um ein ganzes Subnetz zu scannen (z.B. 192.168.1.0/24):
- **nmap -sS 192.168.1.0/24**

Hierbei wird ein syn-Scan verwendet, um Ports scannend zu identifizieren.

- Erweiterte Optionen:

Nutzung von -A für detaillierte Informationen über Dienste:

- **nmap -sS -A [IP-Adresse]**
- Verwendung von -O, um das Betriebssystem zu identifizieren:

nmap -O [IP-Adresse]