Technische README für suricata_config.sh

Übersicht

Das Bash-Skript suricata_config.sh installiert und konfiguriert die Netzwerküberwachungssoftware **Suricata** auf einem Linux-System für das Netzwerkinterface enp0s8. Suricata ist ein leistungsstarkes Tool zur Erkennung von Eindringversuchen, zur Überwachung von Netzwerkverkehr und zur Durchführung von Netzwerkforensik. Dieses Skript automatisiert die Installation, Konfiguration und Aktivierung des Suricata-Dienstes sowie den Download und die Einbindung der Regeln.

Skript-Funktionen

Das Skript führt folgende Schritte aus:

1. **Systemaktualisierung**: Aktualisiert die Systempakete, um sicherzustellen, dass alle installierten Pakete auf dem neuesten Stand sind.
2. **Installation von Suricata**: Installiert die neueste Version von Suricata über das Paketverwaltungstool apt.
3. **Konfiguration von Suricata**: Konfiguriert Suricata so, dass es das Netzwerkinterface enp0s8 überwacht.
4. **Herunterladen von Suricata-Regeln**: Lädt die neuesten Bedrohungsregeln von **Emerging Threats** herunter.
5. **Einbindung der Regeln**: Fügt die heruntergeladenen Regeln in die Konfigurationsdatei von Suricata ein.
6. **Start und Aktivierung des Dienstes**: Startet den Suricata-Dienst und stellt sicher, dass er beim Systemstart automatisch ausgeführt wird.
7. **Statusüberprüfung**: Zeigt den Status des Suricata-Dienstes an.
8. **Protokollüberwachung**: Gibt den Befehl zur Überwachung der Suricata-Logs aus.

Voraussetzungen

- **Betriebssystem**: Das Skript wurde für Debian-basierte Systeme (wie Ubuntu) entwickelt.
- **Netzwerkinterface**: Es wird standardmäßig das Interface enp0s8 verwendet. Du kannst dies jedoch im Skript anpassen, falls dein System ein anderes Interface verwendet.
- **Root-Rechte**: Du benötigst Root- oder Sudo-Rechte, um das Skript auszuführen, da es Systemänderungen vornimmt (z.B. Installation von Paketen, Änderungen an Konfigurationsdateien).

Verwendung

1. Skriptvorbereitung

1. Kopiere das Skript in eine Datei mit dem Namen suricata_config.sh.
2. Stelle sicher, dass das Skript ausführbar ist :
   chmod +x suricata_config.sh

2. Ausführung des Skripts

Führe das Skript mit folgenden Schritten aus:
sudo ./suricata_config.sh

Das Skript wird die Schritte in der folgenden Reihenfolge durchführen:

1. **Systemaktualisierung**: Führt apt-get update und apt-get upgrade aus, um sicherzustellen, dass dein System auf dem neuesten Stand ist.
2. **Suricata-Installation**: Installiert das Suricata-Paket.
3. **Suricata-Konfiguration**: Konfiguriert Suricata so, dass es den Netzwerkverkehr auf enp0s8 überwacht.
4. **Regeln-Download**: Lädt die **Emerging Threats**-Regeln für Suricata herunter.
5. **Regeln in Konfiguration einbinden**: Bindet die heruntergeladenen Regeln in die suricata.yaml-Konfigurationsdatei ein.
6. **Dienststart**: Startet den Suricata-Dienst und aktiviert ihn für den automatischen Start.
7. **Dienststatus**: Zeigt den aktuellen Status von Suricata an.
8. **Log-Anzeige**: Gibt den Befehl aus, um die Suricata-Protokolle in Echtzeit zu überwachen.

Beispielausgabe des Skripts

Updating the system...

Installing Suricata...

Configuring Suricata...

Downloading Suricata rules...

Adding rule files to the configuration...

Starting Suricata...

Checking the status of Suricata...

suricata.service - LSB: Suricata Intrusion Detection Service

Loaded: loaded (/etc/init.d/suricata; generated)

Active: active (running)

You can monitor Suricata logs using:

tail -f /var/log/suricata/suricata.log

Suricata installation and configuration completed.

Protokollüberwachung

Nachdem das Skript die Installation abgeschlossen hat, kannst du die Suricata-Protokolle überwachen, um sicherzustellen, dass alles ordnungsgemäß funktioniert:

tail -f /var/log/suricata/suricata.log

Anpassungen

Falls du ein anderes Netzwerkinterface als enp0s8 verwenden möchtest, kannst du die folgende Zeile im Skript anpassen:

sudo sed -i 's/^\(interface:\)./\1 enp0s8/' /etc/suricata/suricata.yaml*

Ersetze enp0s8 durch das gewünschte Interface (z.B. eth0 oder wlan0).

Lizenz

Dieses Skript steht unter der MIT-Lizenz.

Die MIT-Lizenz ist eine sehr einfache und populäre Open-Source-Lizenz, die Entwicklern erlaubt, den Code frei zu verwenden, zu modifizieren und weiterzugeben. Dabei gelten folgende Bedingungen:

1. **Erlaubnisse**: Der Code darf kostenlos verwendet, kopiert, verändert und weitervertrieben werden, auch in kommerziellen Projekten.
2. **Pflicht**: In jeder Kopie oder jedem abgeleiteten Werk muss der ursprüngliche Copyright-Hinweis sowie die Lizenz erhalten bleiben.
3. **Haftungsausschluss**: Der ursprüngliche Autor übernimmt keine Haftung für Schäden, die durch die Verwendung des Codes entstehen.