|  |  |  |
| --- | --- | --- |
|  |  | Logo_HSMW_blau_CMYK |
| **DOKUMENTATION**  **Programmierung I** |  |  |
|  |  |  |
| Herr Philipp Dellwo  Frau Melissa Futtig | * < |  |
| **Dokumentation Cisco Logdatei Analyse Programm** |  |  |
| Mittweida, 2025 |  |  |

|  |  |  |
| --- | --- | --- |
| Fakultät: Fakultät Angewandte Computer- und Biowissenschaften |  |  |
|  |
| **DOKUMENTATION**  **Programmierung I** |
|  |  |  |
| **Dokumentation Cisco Logdatei Analyse Programm** |  |  |
| Autoren: **Herr Philipp Dellwo**  **Frau Melissa Futtig** |  |  |
| Studiengang: **Bachelor of Science IT-Forensik/ Cybercrime** |  |  |
| Seminargruppe: **CC24w1-B** |  |  |
| Prüfer: **Herr Prof. Dirk Pawlaszczyk** |  |  |
| Einreichung: **Mittweida, 30.08.2025** |  |  |

Inhaltsverzeichnis

[1. Einleitung 4](#_Toc206147117)

[1.1 Zweck des Dokuments/ Aufgabenstellung 4](#_Toc206147118)

[1.2 Umfang des Programms 4](#_Toc206147119)

[1.3 Zielgruppe 5](#_Toc206147120)

[2. Grundlagen und Analyse 6](#_Toc206147121)

[2.1 SysLog-Protokoll 6](#_Toc206147122)

[2.2 Aufbau von Cisco Router-Logdateien 6](#_Toc206147123)

[3. Programmentwurf 7](#_Toc206147124)

[3.1 Diagramm/ Architektur des Programms 7](#_Toc206147125)

[3.2 Log-Einträge/ Filterkriterien 7](#_Toc206147126)

[3.3 Ausgabeformatierung 7](#_Toc206147127)

[4. Implementierung und Einrichtung 8](#_Toc206147128)

[4.1 Entwicklungsumgebung und Code-Struktur 8](#_Toc206147129)

[4.2 Installation, Kompilierung und Ausführung 8](#_Toc206147130)

[4.3 Bedienung 8](#_Toc206147131)

[5. Fazit 9](#_Toc206147132)

[5.1 Zusammenfassung 9](#_Toc206147133)

[5.2 Limitationen 9](#_Toc206147134)

# Einleitung

### Zweck des Dokuments/ Aufgabenstellung

Die Belegarbeit wird im Rahmen des Moduls „Programmierung I“ des Studiengang Bachelor of Science IT-Forensik/ Cybercrime erstellt.

Das Ziel ist die Erstellung, die erfolgreiche Implementierung und der Dokumentation eines Kommandozeilenprogramms, geschrieben in der Programmiersprache „C“. Dieses soll die Analyse von Cisco SysLog Router-Dateien ermöglichen.

Die Aufgabenstellung besteht darin, ein effizientes Tool zu entwickeln, das bestimmte Informationen, wie IP-Adressen, Zeitstempel und Ereignisbeschreibungen aus den Logdateien in eine separate Datei extrahiert und dem Nutzer Filteroptionen bietet, um eine zielgerichtete Auswertung zu erhalten.

### Umfang des Programms

In diesem Dokument wird sich mit einem Kommandozeilenprogramm befasst, das in der Sprache „C“ implementiert wurde und ohne grafische Benutzeroberfläche (GUI) auskommen soll.

Es ist darauf ausgelegt, Cisco SysLog Router-Dateien einzulesen und deren Inhalt zu parsen.

Das Programm enthält eine breite Palette an Filtermöglichkeiten, die es dem Nutzer ermöglicht, die Log-Einträge nach verschiedenen Kriterien zu durchsuchen und einzugrenzen.

Folgende Suchfunktionen sind implementiert:

* IP-Adresssuche (ipSuche(), ipFilterSucheEinfach())
* Zeitbereichsuche (zeitraum())
* Inhaltliche Suche (eigenerSuchbegriff())
* Benutzersuche (userSuche(), eigeneUserSuche())
* Severity Level Suche (severityLevel())
* Facility Suche (facilitySuche(), eigeneFacilitySuche())
* Mnemotics (mnemonicSuche(), eigeneMnemonicSuche())

### Zielgruppe

Zielgruppe dieses Projektes sind Personen, besonders jene mit einem praktischen Verständnis für die Programmierung von Analyse Tools und den effizienten Umgang mit großen Mengen an Logdaten. Weiterführend richtet sich das Programm an mögliche Netzwerkadministratoren und IT-Forensiker, die im Rahmen ihrer Tätigkeit Cisco Router SysLog-Dateien auswerten.

Im Zuge der Aufgabenstellung aus 1.1 richtet sich das Kommandozeilenprogramm an den Dozenten des Moduls Programmierung I und die Studierende des Studiengangs IT-Forensik/ Cybercrime der Hochschule Mittweida.

# Grundlagen und Analyse

### SysLog-Protokoll

Das Syslog-Protokoll steht für „System Logging Protocol“ und ist ein Standardprotokoll, das verwendet wird, um Systemprotokoll- oder Ereignismeldungen eines Netzwerkgerätes zu generieren. Meist ist das Protokoll auf diesen aktiviert.

### Aufbau von Cisco Router-Logdateien

Cisco SysLog-Dateien sind Protokolldateien, die in diesem Fall von Cisco Netzwerkgeräten, wie bspw. eines Routers oder Switches, automatisch erstellt werden. Diese enthalten, meist zeitlich geordnete Systemmeldungen, Ereignisse, Warnungen und Fehler, welche im Gesamten bestimmte Aktionen von Prozessen eines Computersystems mitschreiben.

Mit der Betrachtung einer beispielhaften Logging Nachricht aus einem Router Syslog, lässt sich folgendes Format aus Abbildung 1 betrachten:



Abbildung 1 Format Router SysLog-Datei

Eine Cisco IOS Syslog Nachricht teilt sich in grob fünf Bereiche auf: Zeitstempel, Facility, Severity Level, Mnemonic und der allgemeinen Beschreibung.

Der Zeitstempel, oft wie folgend aussehend, „\*Feb 14 09:40:10.326:“, gibt das Datum und die genaue Uhrzeit des jeweiligen Ereignisses an. Dabei kann es sein, dass die Nachricht anstatt mit eines „\*“, mit einer Nummer in Vergleichsoperatoren „<187>:“ beginnt. Das Beispiel hier bedeutet, dass am 14. Februar um 9:40 Uhr und 10.326 Sekunden ein Ereignis stattgefunden hat.

Das Facility, gibt die Subsystem- oder Prozessbezeichnung an, aus dem die Nachricht stammt. Es ist eine Art der internen Absendererkennung. In diesem Sinne zeigt „%LINEPROTO“ das momentane Line Protocol Subsystem an. Das Konzept der Facilities stammt ursprünglich aus UNIX-Systemen. Cisco hingegen verwendet eigene Bezeichnungen wie LINEPROTO, LINK, KERNEL usw., die auf die jeweiligen internen Module bzw. Prozesse verweisen.

# Programmentwurf

### Ein Bild, das Entwurf, Zeichnung, Diagramm, Lineart enthält. KI-generierte Inhalte können fehlerhaft sein.Diagramm/ Architektur des Programms

Abbildung 2 FlowChart Programmübersicht

Das in der Abbildung 2 dargestellte Diagramm stellt eine grobe Programmübersicht dar.

### Log-Einträge/ Filterkriterien

### Ausgabeformatierung

# Implementierung und Einrichtung

### Entwicklungsumgebung und Code-Struktur

### Installation, Kompilierung und Ausführung

#### 4.2.1 Schritte zur Einrichtung

### Bedienung

# Fazit

### Zusammenfassung

### Limitationen