Titel: Sicherheit neu gedacht – Eine intelligente, erweiterbare Firewall

Folie 1: Einführung

AI Shield: Intelligente Firewall mit Anomalieerkennung und Dashboard
Slogan: Ein Schritt in die Zukunft der Netzwerksicherheit
Kernidee:
Eine Kombination aus Firewall, maschinellem Lernen und Benutzerfreundlichkeit
Geeignet für Anfänger und gleichzeitig leistungsfähig für Profis

Folie 2: Problemstellung

Warum brauchen wir eine intelligente Firewall?

1. Herausforderungen traditioneller Firewalls:
Statische Regeln sind unflexibel gegenüber neuen Bedrohungen
Hohe Komplexität in der Konfiguration

2. Moderne Anforderungen:
Dynamische Netzwerke erfordern Anpassungsfähigkeit
Anomalieerkennung ist essenziell zur Identifikation unbekannter Angriffe

3. Unsere Lösung:
Eine KI-gestützte Firewall mit intuitivem Dashboard

Folie 3: Projektübersicht

Hauptfunktionen:

1. Firewall:
Blockieren unerlaubter IPs, Ports und Protokolle
Logging verdächtiger Aktivitäten

2. KI-Anomalieerkennung:

Isolation Forest zur Erkennung ungewöhnlicher Muster im Netzwerkverkehr

3. Dashboard:
Echtzeit-Visualisierung und einfache Verwaltung

4. Skalierbarkeit:
Modularer Aufbau für zukünftige Erweiterungen

Folie 4: Architektur und Funktionen

Technische Umsetzung:
Netzwerküberwachung mit Paketfilterung durch Scapy
KI-Anomalieerkennung mit Isolation Forest
Dashboard auf Basis von Flask
Log-Management zur detaillierten Protokollierung blockierter Pakete
Benutzerfreundlichkeit durch übersichtlichen Code und klare Dokumentation

Folie 5: Besondere Merkmale

Warum ist diese Lösung besonders?

1. Lernorientiert:
Einsteigerfreundlich mit Schritt-für-Schritt-Anleitungen

2. Interaktiv:
Das Dashboard bildet eine Brücke zwischen Theorie und Praxis

3. Erweiterbar:
Einfach anpassbar für zusätzliche Algorithmen oder Schnittstellen

4. Innovativ:
Verbindung von klassischer Firewall und moderner KI

Folie 6: Implementierungsschritte

1. Vorbereitung der Entwicklungsumgebung

2. Paketfilterung mit Regeln für unerlaubte IPs und Ports

3. Training und Anwendung der KI-Anomalieerkennung

4. Entwicklung des Dashboards zur Visualisierung und Verwaltung

5. Parallele Ausführung durch Multithreading

Folie 7: Vorteile

Technisch:
Die KI erkennt unbekannte Bedrohungen in Echtzeit
Die intuitive Weboberfläche erleichtert die Bedienung
Lernvorteile:
Perfekt für Anfänger, um Netzwerksicherheit und KI zu verstehen
Praktischer Nutzen für erfahrene Anwender

Folie 8: Ergebnisse statt Live-Demo

Da keine Live-Demo möglich ist, hier eine Zusammenfassung der Funktionalität:

Der Code blockiert erfolgreich unerlaubte Pakete und protokolliert sie

Die KI erkennt Anomalien im Netzwerkverkehr basierend auf trainierten Mustern

Das Dashboard bietet eine klare Visualisierung der Netzwerkaktivitäten

Der modulare Aufbau ermöglicht einfache Anpassungen und Erweiterungen

Folie 9: Erweiterungsmöglichkeiten

Wie kann das Projekt weiterentwickelt werden?
Erweiterte Anomalieerkennung durch Deep-Learning-Algorithmen
Automatisiertes Blockieren von Angreifern in Echtzeit
Integration in größere Netzwerke
Optimierung der Benutzeroberfläche des Dashboards

Folie 10: Fazit und Call-to-Action

Warum ist das Projekt relevant?
Die Lösung bietet innovative Ansätze für Netzwerksicherheit
Sie ist flexibel und kann zukünftigen Herausforderungen angepasst werden
Call-to-Action:
Anfänger können die Lösung ausprobieren und Netzwerksicherheit lernen
Profis können den Code als Grundlage für weiterführende Projekte nutzen

Folie 11: Fragen und Diskussion

Vielen Dank für eure Aufmerksamkeit
Diskussionsthemen:
Verbesserungsvorschläge
Erfahrungen mit ähnlichen Projekten
Kontakt:
E-Mail: timothylanger472@gmail.com

Title: Rethinking Security – An Intelligent, Scalable Firewall

Slide 1: Introduction

AI Shield: Intelligent Firewall with Anomaly Detection and Dashboard
Slogan: A Step into the Future of Network Security
Core Idea:

A combination of a firewall, machine learning, and user-friendliness

Suitable for beginners and powerful for professionals

Slide 2: Problem Statement

Why do we need an intelligent firewall?

1. Challenges of Traditional Firewalls:

Static rules are inflexible against new threats

High complexity in configuration

2. Modern Requirements:

Dynamic networks demand adaptability

Anomaly detection is essential to identify unknown attacks

3. Our Solution:

An AI-powered firewall with an intuitive dashboard

Slide 3: Project Overview

Key Features:

1. Firewall:

Blocking unauthorized IPs, ports, and protocols

Logging suspicious activities

2. AI-Anomaly Detection:

Isolation Forest to detect unusual patterns in network traffic

3. Dashboard:

Real-time visualization and easy management

4. Scalability:

Modular design for future extensions

Slide 4: Architecture and Features

Technical Implementation:

Network monitoring with packet filtering via Scapy

AI anomaly detection using Isolation Forest

Dashboard built with Flask

Log management for detailed records of blocked packets

User-friendliness through clean code and clear documentation

Slide 5: Unique Features

Why is this solution special?

1. Learning-Oriented:

Beginner-friendly with step-by-step guides

2. Interactive:

The dashboard bridges the gap between theory and practice

3. Expandable:

Easily adaptable for additional algorithms or interfaces

4. Innovative:

Combines traditional firewalls with modern AI

Slide 6: Implementation Steps

1. Set up the development environment

2. Packet filtering with rules for unauthorized IPs and ports

3. Train and apply the AI anomaly detection

4. Develop the dashboard for visualization and management

5. Enable parallel execution using multithreading

Slide 7: Benefits

Technical:

AI detects unknown threats in real-time

Intuitive web interface simplifies usage

Learning Advantages:

Ideal for beginners to understand network security and AI

Practical utility for experienced users

Slide 8: Results Instead of Live Demo

Since a live demo isn’t possible, here’s a summary of the functionality:

The code successfully blocks unauthorized packets and logs them

The AI detects anomalies in network traffic based on trained patterns

The dashboard provides clear visualization of network activities

The modular structure allows easy adjustments and extensions

Slide 9: Future Development

How can this project evolve?

Enhanced anomaly detection with deep learning algorithms

Automated attacker blocking in real-time

Integration into larger networks

Optimized dashboard user interface

Slide 10: Conclusion and Call-to-Action

Why is this project relevant?

It offers innovative approaches to network security

Flexible and adaptable to future challenges

Call-to-Action:

Beginners can use the solution to learn about network security

Professionals can build on the code for advanced projects

Slide 11: Questions and Discussion

Thank you for your attention!

Topics for Discussion:

Suggestions for improvements

Experiences with similar projects

Contact:

Email: timothylanger472@gmail.com