Schule: Handelslehranstalt Hameln Dienstag, 14. Mai 2024

Klasse: FOI22a

Fach: 12.4 IT-Projekt planen, durchführen, dokumentieren und evaluieren

Lehrkraft: Herr Daniel Stern

Von: Abdulkarim Bashir Termanini, Lucas Haase, Oguzhan Kirkaya, Jeronymo Mrozek

**Auswirkung, Durchführung und Prävention von DoS-Angriffen**

**Gliederung**:

1. Einleitung
2. Webseite
3. Begriffsdefinitionen
4. Das DoS-Tool
5. Reflexion
6. Quellenangaben

## 1. Einleitung

Cyberangriffe stellen eine bedeutende Bedrohung in unserer zunehmend digital vernetzten Welt dar. Insbesondere Denial-of-Service (DoS)-Angriffe, welche Systemressourcen überlasten und Dienste zum Erliegen bringen, verursachen erhebliche Schäden.   
Das Projekt zielt darauf ab, das Verständnis für die Mechanismen hinter DoS-Angriffen zu vertiefen und grundlegende Abläufe im Internet zu verstehen.

## 2.Webseite

HTML stellt mit Doctype, Meta-Tags und Verknüpfungen zu CSS- und JavaScript-Dateien das Grundgerüst jeder Webseite dar. CSS gewährleistet visuelle Änderungen mit Variablen und Media Queries und ein dynamisches Design, um die Seite in Abschnitte wie „Leistungen“, „Über uns“ oder „Kontakt“ aufteilen zu können. JavaScript ermöglicht Interaktionen wie das Ein- und Ausblenden von Elementen je nach Scroll-Position.

## 3. Begriffsdefinitionen

TCP (Transmission Control Protocol) sorgt für eine zuverlässige Datenübertragung mittels Fehlererkennung und -korrektur, während UDP (User Datagram Protocol) schnelle Übertragungen ohne Zustellungsgarantie ermöglicht. ICMP (Internet Control Message Protocol) wird genutzt, um Netzwerkfehler zu erkennen und Diagnosen durchzuführen. HTTP/S sichern die Übertragung von Webinhalten. Das OSI-Modell beschreibt Netzwerkprotokolle in sieben Schichten die Pakete durchlaufen. Lastenverteilung optimiert die Verteilung des Datenverkehrs. Firewalls schützen vor schädlichem Verkehr, und das BGP (Border Gateway Protocol) regelt den Datenaustausch zur Vermeidung von Netzwerküberlastungen.

## 4. Das DoS-Tool

Das Tool ermöglicht die Durchführung von Angriffen, wie Ping of Death. Nutzer können dabei die Ziel-IP oder URL eingeben und den Angriffstyp, die Geschwindigkeit sowie die Anfragen pro Sekunde festlegen. Das Tool erzeugt dabei einen hohen Datenverkehr, um Server oder Netzwerke zu überlasten.

## 5. Reflexion

Das erreichte Endergebnis ist zufriedenstellend und kann ergänzt werden. Die Etappen der Projektarbeit wurden in Gruppen abgearbeitet. Die Arbeitsweise war strukturiert und zielorientiert, durch die Zusammenarbeit online. Die Aufgabenteilung benötigt eine flexible Anpassung an veränderte Anforderungen und Gegebenheiten.

## 6. Quellenangaben

<https://www.canva.com/>

<https://www.jetbrains.com/de-de/>

<https://about.gitea.com/>

<https://www.nginx.com/>

<https://www.docker.com/>

<https://www.cloudflare.com/>

<https://www.akamai.com/de>

<https://github.com/alexzhirkevich/custom-qr-generator>