Überblick

- **Montag**
  Setup, Intro & String Obfuscation
- **Dienstag**
  Anti-Analyse & Shellcode
- **Mittwoch**
  Algorithmusidentifikation
- **Donnerstag**
  API Hashing

Überblick Montag

- Hallo Welt
- Ghidra Setup
- Windows API
- Aufgabe 1
- Reverse Engineering: Ziele & Stile
- Aufgabe 2

Demo: Hallo Welt.

Ghidra Setup

- JDK
- Ghidra
- ghida.kbxml
- ReactOS DLLs (Options → Edit Paths)

Ghidra Intro

- Variablen (umbennen)
- Datentypen (ändern)
- An Dekompiler gewöhnen
- Empfohlene Benutzereinstellungen
  Key Bindings
  Highlight mit linker Maustaste

Aufgabe 1

https://mal.re/tmp/classes/hsbund-ws2026/aufgabe1.md

Arten von Malware

- Wiper
- Backdoor
- Remote Access Tool (RAT)
- Bot
- Rootkit / Bootkit
- Banker
- Stealer
- Ransomware
- Mineware

Welche Infromationen kann Reverse Engineering liefern

- Ist das Malware?
- Indicators of Compromise (IoCs)
- Signaturen
- Capabilities
- Klassifikation
- Kontextualisierung

Aufgabe 2

https://mal.re/tmp/classes/hsbund-ws2026/aufgabe2.md

Erinnerung: Options → Edit Paths

Demo: Structs