

Überblick Dientag

- RE Stile
- Aufgabe 2
- String Obfuscation
- Shellcode vs. PE Format
- Anti-Reversing
- Struct (evtl.)

Reverse Engineering Stile

- Tiefensuche vs. Breitensuche
- Dynamisch vs. Statisch
- Deduktiv vs. Induktiv
- Top-Down vs. Bottom-Up

Aufgabe 2 (cont)

<https://mal.re/tmp/classes/hsbund-2025/aufgabe2-lesbar.md>

String Obfuscation Beispiel

```
void * __cdecl FUN_00401430(char *param_1)
{
    void *pvVar1;
    size_t sVar2;
    uint uVar3;

    uVar3 = 0;
    pvVar1 = calloc(1, 0x1b);
    while( true ) {
        sVar2 = strlen(param_1);
        if (sVar2 <= uVar3) break;
        *(byte *) ((int)pvVar1 + uVar3) = param_1[uVar3] ^ 3;
        uVar3 = uVar3 + 1;
    }
    *(undefined *) ((int)pvVar1 + uVar3) = 0;
    return pvVar1;
}
```

Aufgabe 3

<https://mal.re/tmp/classes/hsbund-2025/aufgabe3.md>

Anti-Reversing

- String Obfuscation
- Stack Strings
- Packing
- Kontrollfluss Obfuscation
- Auflösung von API Funktionen zur Laufzeit
- ...

Shellcode vs. PE-Format

- Shellcode
- PE-Format
- Demo: Netwalker

Aufgabe 4 (Teil 1)

<https://mal.re/tmp/classes/hsbund-2025/aufgabe4.md>