99_Readme_Testsystem.md

Readme

Die beigelegten Verzeichnisse beinhalten das Git Repository der schriftlichen Ausarbeitung sowie ein vorkonfiguriertes Testsystem in Form von Open-Virtualizaion-Format (OMV) Appliances.

- ./thesis : schriftliche Ausarbeitung
- ./i40-system : Testsystem

Installation

Zum Import der Appliances wird die Software Oracle VM VirtualBox benötigt. Dort können die virtuellen Maschinen inkl. der Einstellungen für die verwendeten Host-Systemressourcen und Netzwerkadapter importiert werden.

Beim Import ist es wichtig, darauf zu achten, dass keine neuen MAC-Adressen für die Netzwerkadapter bereitgestellt werden. Dadurch würden den Netzwerkadaptern im Betriebssystem neue Namen zugeordnet werden. Dies würde das Routing im Netzwerk beeinträchtigen und eine korrekte Funktionsweise des Systems verhindern.

Start

Der Benutzer sowie das Passwort für alle virtuellen Maschinen lautet:

- Benutzername: i40
- Passwort: industrie40

Nach dem Start der virtuellen Maschinen steht folgende Netzwerkkonfiguration bereit.

- VM i40:
  - enp0s8: 10.0.0.254
  - Docker Bridge: 172.17.0.1
- VM mgmt:
  - enp0s3: 10.0.2.15 (Host-NAT)
  - enp0s8: 10.0.0.1

    - enp0s9: 10.0.10.1
- VM comp:
    - enp0s8: 10.0.0.0/24 (DHCP)

Die Dienste des Industrie 4.0 Systems, CoAP Monitoringsystems und CoAP Clients sowie die für das Netzwerk benötigten Dienste DHCP und DNS werden automatisch gestartet und sind unter folgenden Adressen erreichbar.

- DHCP/DNS/Gateway:
    - 10.0.0.1
- Industrie 4.0 System:
    - Docker Containernetzwerk
    - Webinterface 10.0.0.254:8080
- CoAP Monitoringsystem:
    - CoAP Server: 10.0.10.1:5683
    - Monitoringsystem Webinterface: 10.0.10.1:9999

Darstellung der Bedrohungsfaktoren

Die Darstellung der Bedrohungsfaktoren findet auf der Ubuntu 18.04 LTS Client VM i40 statt. Dort befinden sich das bestehende, aktualisierte OPC UA Industrie 4.0 Testsystem sowie der CoAP Manipulationsclient im Home Verzeichnis des Benutzers i40.

Zur Analyse der Netzwerkkommunikation wurde das Netzwerkanalysetool Wireshark auf dem System vorinstalliert. Um die Sicherheitskonfiguration des Industrie 4.0 Testsystems zu analysieren muss die Netzwerkschnittstelle der Docker Bridge abgehört werden. Die Analyse der Netzwerkkommunikation während des Man-in-the-Middle Angriffs findet auf der Netzwerkschnittstelle enp0s8 statt.