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 CoAP Monitoringsystems, 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
- CoAP Monitoringsystem:
    - CoAP Server: 10.0.10.1:5683
    - Monitoringsystem Webinterface: 10.0.10.1:9999

Start und Konfiguration des Industrie 4.0 Testsystems

Das aktualisierte Testsystem ist im Verzeichnis "home/i40/i40-testbed" des Ubuntu 18.04 LTS Clients installiert. Es kann mit Hilfe der im Verzeichnis `scripts` beigelegten Scripte gesteuert werden.

- ./scripts/startDockers.sh: Container starten
- ./scripts/stopContainers.sh: Container stoppen
- ./scripts/changeSecurityMode.sh: Sicherheitskonfiguration ändern

Vor der Änderung der Sicherheitskonfiguration der OPC UA Kommunikation, müssen die Container beendet werden.

```
./scripts/stopContainers.sh
```

Mit dem Script `changeSecurityMode.sh` kann die Sicherheitskonfiguration des schedulers und des control Dockers angepasst werden.

```
./scripts/changeSecurityMode.sh [true/false]
```

Die Container werden vom Script nach Änderung der Konfiguration automatisch neu gebaut. Anschließend müssen diese neu gestartet werden.

```
./scripts/startDockers.sh
```

Nach dem Start besitzt das System die folgende Netzwerkkonfiguration

- Industrie 4.0 System:
    - Docker-Netzwerk 172.18.0.0/16
    - Webinterface 10.0.0.254:8080

Rogue DHCP Server

Der Rogue DHCP Server ist auf dem Ubuntu 18.04 LTS Client installiert und wird nicht automatisch gestartet, damit die Kommunikation im Netzwerk bei normaler Nutzung nicht gestört wird.

VM i40

Zum Angriff muss der Dienst des DHCP Servers mit Hilfe von `systemctl` gestartet werden.

```
systemctl start isc-dhcp-server
```

VM mgmt

Des Weiteren kann, um die Chancen einer Zuweisung der IP Adresse des Rogue DHCP Servers im Netzwerk zu erhöhen ein Delay auf den Netzwerkadapter des für das Netzwerk zuständigen DHCP Servers gelegt werden, um die Paketvermittlung zu manipulieren. Dies geschieht am Netzwerkadapter des DHCP Servers auf der virtuellen Maschine "mgmt". Es wird dafür im "home" Verzeichnis des Benutzers "i40" das Script `setNetworkDelay.sh` bereitgestellt.

```
./scripts/setNetworkDelay.sh
```

Alternativ kann das Delay auch manuell gesetzt werden.

```
tc qdisc add dev enp0s8 root netem delay 500ms
```

VM comp

Um nun einen Neubezug der DHCP Adresse im Netzwerk darzustellen, kann die VM "comp" dazu bewegt werden, sich eine neue IP Adresse per DHCP zuweisen zu lassen.

```
netplan apply
```

CoAP Manipulation

Zur Manipulation des CoAP Systems steht im "home" Verzeichnis des Benutzers "i40" auf der virtuellen Maschine "i40" das Verzeichnis "CoAP_Manipulation" mit einem Client bereit. Der CoAP Server des Monitoringsystems ist im Testsystem unter der IP Adresse 10.0.10.1 erreichbar. Der Client kann mit den folgenden Parametern gestartet werden:

```
node index.js [DESTINATION URL] [PAYLOAD TITLE] [INTERVAL]
```

- Destination URL: Zieladresse der Pakete. Format: `coap://host/address`
- Payload Title: Titel des CoAP Payload
- Interval: Intervall der Paketsendung in Sekunden

Beispiel:

```
node index.js coap://10.0.10.1/moldingmachine/1 Temperatursensor_#2 0.5
```

Darstellung der Bedrohungsfaktoren

Zur Analyse der Netzwerkkommunikation wurde das Netzwerkanalysetool Wireshark auf der virtuellen Maschine "i40" 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.

Die Darstellung der Manipulation der CoAP Kommunikation wird mit Hilfe des Monitoringsystems visualisiert.