Vorbereitung

Für ein erfolgreiches Praktikum sollten Sie sich anhand der im Internet verfügbaren Informationen über folgende Anwendungen informieren:

- SSH-Clients für Ihr Endgerät
  - für Windows: PUTTY bzw. WINSCP
- WIRESHARK für Ihr Endgerät
- OPENVPN für Ihr Endgerät (Client), um Zugang zu den laufenden Prozessen auf dem Docker-Host mit privaten IP-Adressen zu bekommen
- TCPDUMP für Linux (Kommandozeile)
- OPENSSL für Linux (Kommandozeile)
  - Erzeugung von Wurzel-CA-, CA- und Server-Zertifikaten im Rahmen einer PKI
- APACHE
  - Konfiguration von SSL-Servern mit entsprechenden Zertifikaten

Sicherlich müssen Sie auch Zugriffsrechte unter LINUX/UBUNTU anpassen und Netzwerkdienste im Betriebssystem verankern, wobei erfahrungsgemäß bei vielen praktische Erfahrung fehlt. Also bitte ggf. auch dazu etwas lesen.

Warnhinweis!

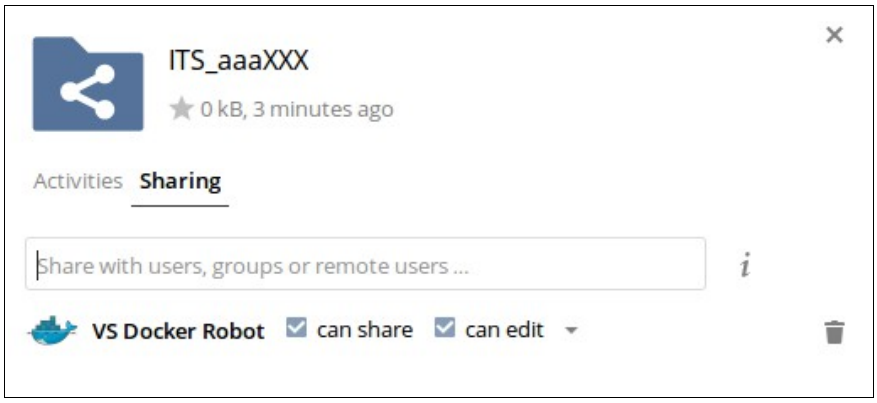
Da die Aufgaben auf einem zentralen Rechner innerhalb virtueller Maschinen gelöst werden sollen, werden Ihnen bestimmte Images von Anfang an bereitgestellt. Ihre virtuellen Maschinen befinden sich zwar auf der gleichen Hardware, sind aber weitestgehend von den anderer Studentinnen bzw. Studenten unabhängig.

Allerdings gibt es auch keine zentrale IT-Abteilung, die Ihnen die lästigen Aufgaben wie Backup und Maintenance abnimmt. Tatsächlich kann es vorkommen, dass die Maschine von heute auf morgen nicht verfügbar ist. Hierbei könnte es auch zu Datenverlusten kommen. Deswegen ist es unabdingbar, dass Sie selbst Ihre Ergebnisse zwischenspeichern und so archivieren, dass Sie von solchen „Katastrophen“ unbeeinträchtigt weiterarbeiten können!

Das Docker-System auf der IP-Adresse 141.22.34.20 arbeitet mit dem OWNCLOUD-Dienst zusammen. Deswegen ist es auch nötig, dass Sie innerhalb Ihres OWNCLOUD-Zugangs einen neuen Ordner auf der obersten Ebene anlegen. Der Name muss mit „ITS_“ beginnen und von ihrer Benutzerkennung (drei Buchstaben klein, drei Ziffern) beendet werden, also z.B. „ITS_abc123“. Dieser Ordner muss dann mit einem bestimmten Benutzer, genannt „VS Docker Robot“, geteilt werden.

Wichtig: Die Freigabe muss für den Benutzer, nicht aus Versehen für die Gruppe „vs_docker“, die es auch gibt, erteilt werden.

Wie es danach aussieht, wenn Sie auf „Geteilt“ des richtigen Ordners klicken, zeigt der folgende Screenshot für den Beispielnutzer „aaaXXX“:



Der Zugang zu der Übersicht Ihrer Images und Builds ist über die folgende URL möglich:

https://141.22.34.20

Diese Oberfläche erlaubt die Verwaltung Ihrer Container (Es muss leider das Zertifikat akzeptiert werden, so wie es ist, falls es zu einer Fehlermeldung führt). Dort loggen Sie sich mit Ihrer HAW-Kennung ein. Sie finden vorbereitete Images und die in der OWNCLOUD abgelegten Docker-Verzeichnisse werden Ihnen dort angezeigt als baubare Container. Da mittels Synchronisation gearbeitet wird, kann es zu leichten Verzögerungen kommen zwischen dem Ablegen einer neuen Datei in der OWNCLOUD und der Aktualisierung auf dem Docker-System.

Um einen Container zu bauen, drücken Sie in der Oberfläche bei dem gewünschten „Buildable“ auf „build“. Hierbei wird automatisch ein Container erstellt und gestartet, sofern der Build erfolgreich war. Dieser Container trägt automatisch den Namen „<user>_<container>“ und ist unter diesem Namen auch im Netzwerk der Container erreichbar. Außerdem bekommt er eine IP-Adresse, welche in der Oberfläche angezeigt wird. Die Container sind nicht direkt von außen zu erreichen, da die privaten IPs nur im Kontext des Docker-Systems bekannt sind und funktionieren.

Ihre gestarteten Container werden in der Oberfläche angezeigt und Sie können diese verwalten, wie z.B. stoppen, neu starten oder löschen.

Es existiert ein VPN-Zugang, um von Arbeitsplatzsystemen oder Laptops auf die Container zugreifen zu können. Hierbei gibt es „hinter“ dem VPN-Gateway keine Einschränkungen der erreichbaren Ports bzw. IP-Adressen. Die Konfiguration für den VPN-Zugriff ist Benutzer-Spezifisch und wird Ihnen von der Docker-Oberfläche generiert („Openvpn-Access to the docker network: config“). Über den Link kann die Konfiguration heruntergeladen und direkt genutzt werden. Um eine Verbindung zu öffnen, speichern Sie die CONFIG-Datei als „<user>.ovpn“ und starten:

```
openvpn –config <user>.ovpn
```

Aufgabe 2a: Zugang zum UBUNTU-Image

Auf dem Docker-System soll jede Gruppe ein UBUNTU-Image zur Ausführung bringen. Der Zugriff auf das gestartete Image erfolgt über SSH, durch die Verwendung individueller Public-Keys soll ein authentisierter und vertraulicher Zugriff möglich sein. Hierzu muss mit einem lokalen Client ein solcher individueller Public-Key zunächst erzeugt und in Ihrer OWNCLOUD „neben“ dem Docker-File des entsprechenden Containers als Datei mit dem Namen „authorized_keys“ abgelegt werden.

Beim Build Ihres Images wird diese Datei an die richtige Stelle kopiert und steht damit für die spätere Authentisierung Ihrer Zugriffe zu Verfügung.

Starten Sie den Build-Prozess ihres UBUNTU-Image und benutzen Sie den SSH-Clienten Ihres Arbeitsplatzsystems, um Zugriff zu erlangen. Damit eine Verbindung von Ihrem Arbeitsplatzsystem zu dem fertig gebauten Image per SSH möglich ist, bedarf es einer natürlich funktionierenden und gerouteten TCP/IP-Verbindungsmöglichkeit über das VPN.

Aufgabe 2b: Aufsetzen von Apache

Auf dem Image soll jede Gruppe dann einen Apache-Server starten. Von den Arbeitsplatzsystemen aus ist der Zugriff auf den Apache z.B. mit Firefox oder Safari über das VPN zu überprüfen. Dafür reicht das Anlegen einer simplen index.html-Datei im Wurzelverzeichnis des Dokumentenbereichs zunächst aus.

Der Dateitransfer zu Ihrem UBUNTU-Image erfolgt über den SSH-Clienten. Datensicherungen und Kopien von Ergebnissen können mit SSH von dem Image auf Ihr Arbeitsplatzsystem gemacht werden.

Aufgabe 2c: Erzeugung von CA- und Server-Zertifikaten

Auf dem Image oder auf Ihrem Arbeitsplatzrechner können Sie dies mit OPENSSL machen. Legen Sie entsprechende Konfigurationen für eine PKI so an, dass Sie im weiteren die folgenden SSL-Artifakte generieren können:

- eine oberste Wurzel-SSL-CA (sogenanntes „self-signed CA certificate“) für die HAW mit Namen:
  /C=DE; /O=haw-hamburg; /CN=CA
- darunter eine weitere SSL-CA für die Organisationseinheit mit dem Namen der Gruppe anstelle von „<teamname>“:
  /C=DE; /O=haw-hamburg; /OU=informatik; /CN=CA-<teamname>
- darunter ein SSL-Server-Zertifikat für den Apache-Server:
  /C=DE; /O=haw-hamburg; /OU=informatik; \
  /CN=<teamname>.informatik.haw-hamburg.de
- für beide CAs gültige und passende CRLs mit einer Gültigkeit von je vier Wochen

Bedenken Sie, dass Sie diese Artifakte für spätere Übungen weiter benötigen und Sie z.B. die Passphrases für die erzeugten Schlüssel noch öfter brauchen werden! Es empfiehlt sich, den ganzen Vorgang zu skripten, damit Sie ihn ohne Probleme wiederholen können. Erfahrungsgemäß werden des öfteren Korrekturen oder Erweiterungen nötig!

Wenn Sie Skripte und Konfigurationsdateien aus dem Internet kopieren, machen Sie sich unbedingt die Mühe, **alle** Einträge zu überprüfen und ggf. zu säubern. Es ist also nicht richtig, wenn irgendwo plötzlich ein Zertifikat für Norwegen (oder ein anderes schönes Land) ausgestellt wird, etc.

Warnhinweis!

Da die Aufgaben auf einem zentralen Rechner innerhalb virtueller Maschinen gelöst werden, die Sie über ein VPN erreichen, gibt es keine vernünftige Namensauflösung innerhalb des DNS der HAW.

Diese wird aber beim Browser u.a. dazu verwendet, die Plausibilität des SSL-Server-Zertifikats zu prüfen. D.h. es kann durchaus sein, dass Sie lokal dem Betriebssystem auf Ihrem Arbeitsplatzsystem beibringen müssen, dass eine bestimmte IP-Adresse einen bestimmten Hostnamen hat – und umgedreht.

Aufgabe 2d: Einrichten des SSL-Server-Zertifikats

Richten Sie den Apache-Server auf ihrem Image so ein, dass ein Zugriff über HTTPS (443/tcp, Zertifikate aus Aufgabe 2c) auf „Ihre“ Home-Page (siehe Aufgabe 2b) möglich wird, für diese reicht nach wie vor die bereits erzeugte einfache index.html-Datei aus. Der Zugriff auf dieselbe Home-Page soll auch per HTTP (80/tcp) möglich sein, d.h. es gibt zwei Zugriffswege zur gleichen Datei!

Überprüfen Sie mit einem SSL-fähigen Browser, dass das konfigurierte SSL-Server-Zertifikat bei einer HTTPS-Verbindung verwendet wird und stellen Sie den Browser so ein, dass den ausstellenden Zertifizierungsstellen zukünftig ohne weitere Rückfrage an den Benutzer vertraut wird. Die CRLs, die Sie erzeugt haben, müssen dabei auch aufzufinden sein. Und natürlich müssen diese immer aktuell und vor allem gültig sein … abgelaufene CRLs können das Browserverhalten auf unvorhersehbare Art und Weise beeinflussen! Denken Sie auch an den Warnhinweis von Aufgabe 2d!

Überprüfen Sie mit dem gleichen SSL-fähigen Browser, dass beim Zugriff auf Ihre Seite über HTTP kein SSL verwendet wird.

Aufgabe 2e: Mitschnitt der Web-Zugriffe

Zeichnen Sie mit TCPDUMP ca. zwei Minuten Netzwerkverkehr zwischen Ihrem Arbeitsplatzsystem / Browser und Ihrem Web-Server auf dem Docker-System auf. Bauen Sie während der Aufzeichnung mindestens eine ungesicherte (HTTP) und eine gesicherte (HTTPS) Web-Verbindung zu ihrem Image auf.

Übertragen Sie nach Abschluss der Aufzeichnung die erzeugten LIBPCAP-Dateien zur weiteren Analyse mit WIRESHARK auf Ihren Arbeitsplatz.

Identifizieren Sie die beiden Verbindungen innerhalb der aufgezeichneten Daten und überprüfen Sie die Nutzdaten (engl.: Payload) der übertragenen Pakete auf das Anwendungsprotokoll.

Recherchieren Sie ggf. im Internet, warum die beiden Verbindungen so unterschiedlich aussehen, sofern Sie sich dies nicht herleiten können.