Vorbereitung

Bereits vor dem 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
- 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, ein UBUNTU-Image wird Ihnen bereitgestellt, sind die Ergebnisse von anderen Praktikumsgruppen 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. Deswegen ist es unabdingbar, dass Sie selbst Ihre Ergebnisse zwischenspeichern und so archivieren, dass Sie von solchen „Katastrophen“ unbeeinträchtigt weiterarbeiten können!

Aufgabe 2a: Zugang zum UBUNTU-Image

Auf dem Projektrechner soll jede Gruppe ein UBUNTU-Image innerhalb der Docker-Umgebung 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.

Starten Sie das UBUNTU-Image und benutzen Sie den SSH-Clienten, um mit dem Passwort zunächst initialen Zugriff zu erlangen. Dann Erzeugen Sie mit dem SSH-Clienten ein eigenes SSH-Schlüsselpaar und übertragen den öffentlichen Schlüssel auf den Server. Danach überprüfen Sie, ob Sie Zugriff ohne Passwort erhalten können. Gelingt dies, setzen Sie das Passwort auf einen nur Ihrer Gruppe bekannten Wert und verwenden weiterhin nur Ihre Schlüsselpaare.

Aufgabe 2b: Aufsetzen von Apache

Auf dem Projektrechner soll für jede Gruppe ein Apache-Server gestartet werden. Von den Arbeitsplatzsystemen aus ist der Zugriff auf den Apache z.B. mit Firefox oder Safari zu überprüfen. Dafür reicht das Anlegen einer simplen index.html-Datei im Wurzelverzeichnis des Dokumentenbereichs für einen initialen Test zunächst aus.

Wenn das nicht klappt, prüfen Sie bitte unbedingt, ob die TCP-Verbindung nicht durch „irgendwas“ in der lokalen Netzinfrastruktur geblockt wird, d.h. das die Pakete tatsächlich auf beim Server ankommen!

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

Auf dem Projektrechner ist openssl verfügbar. Legen Sie eine entsprechende Konfiguration für eine PKI so an, dass Sie im weiteren die folgenden SSL-Artifakte generieren können:

- ein SSL-Server-Zertifikat für den Apache-Server:
  /C=DE; /O=haw-hamburg; /OU=informatik; \
  /CN=<teamname>.informatik.haw-hamburg.de

- unterhalb einer SSL-CA für die Organisationseinheit mit Namen:
  /C=DE; /O=haw-hamburg; /OU=informatik; /CN=CA

- diese wiederum unterhalb einer Wurzel-SSL-CA (self-signed CA certificate) für die HAW mit Namen:
  /C=DE; /O=haw-hamburg; /CN=CA

- beide CAs mit je einer für vier Wochen gültigen und passenden CRL

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 ggf., den ganzen Vorgang zu skripten, damit Sie ihn ohne Probleme wiederholen können.

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. 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, das den Browser startet, 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. 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 der ausstellenden Zertifizierungsstelle (SSL-Server-CA) zukünftig ohne weitere Rückfrage an den Benutzer vertraut wird. Die CRLs, die Sie erzeugt haben, müssen dabei auch aufzufinden sein. Und natürlich muss die immer aktuell sein … abgelaufene CRLs können das Browserverhalten auf unvorhersehbare Art und Weise beeinflussen! Denken Sie an den Warnhinweis von Aufgabe 2d!

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

Aufgabe 2e: Mitschnitt der Web-Zugriffe

Zeichnen Sie mit tcpdump zwei Minuten Netzwerkverkehr auf. Bauen Sie während der Aufzeichnung mindestens eine ungesicherte (HTTP) und eine gesicherte (HTTPS) Web-Verbindung zu ihrem Image auf und rufen Sie index.html-Seite ab. Übertragen Sie nach Abschluss der Aufzeichnung die libpcap-Datei zur weiteren Analyse auf Ihren Arbeitsplatz.

Identifizieren Sie Ihre Verbindung innerhalb der aufgezeichneten Daten und überprüfen Sie die Payload, d.h. die Nutzdaten der übertragenen Pakete, für das Anwendungsprotokoll. Recherchieren Sie ggf. im Internet, warum die beiden Verbindungen so unterschiedlich aussehen, sofern Sie sich dies nicht herleiten können.