SecLab

Praktikum IT-Sicherheit

- Versuchshandbuch -

Aufgaben | **VPN**

In diesem Versuch lernen Sie eine sichere VPN Verbindung zu einem Server aufzubauen. Dabei werden zuerst ältere Verfahren eingesetzt und mittels eines Angriffs die Verwundbarkeit dieser Verfahren gezeigt. Anschließend wird anhand eines selbst erstellten Zertifikats eine L2TP-IPSec-VPN Verbindung eingerichtet.

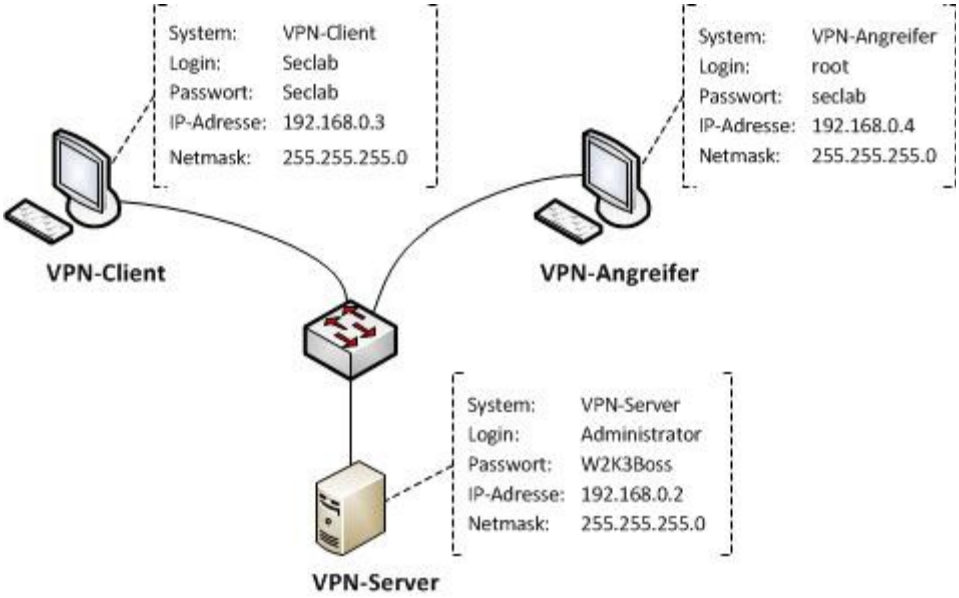
B.Sc. AI, WI
M.Sc. AI
M.Sc. EB

IT-Sicherheit

Einleitung

In diesem Versuch lernen Sie, eine sichere VPN-Verbindung zu einem Server aufzubauen. In Aufgabe 1 wird zunächst eine VPN-Verbindung unter Verwendung von älteren Verfahren für die Verschlüsselung und Authentifizierung erstellt. In Aufgabe 2 wird die Verwundbarkeit dieser Verfahren mittels eines Wörterbuchangriffes gezeigt. Abschliessend wird mittels eines selbst erstellten Client-Zertifikats eine L2TP-IPSec-VPN Verbindung eingerichtet, die Schutz vor den zuvor kennengelernten Problemen bietet.

Netzwerkplan



Aufgabe 1: Einrichtung einer VPN-Verbindung mittels PPTP

a) Melden Sie sich am VPN-Client an und errichten Sie über die Netzwerkumgebung (Desktop → Netzwerkverbindungen → Neue Verbindung) eine neue VPN-Verbindung mit dem VPN-Server. Als Firmennamen wählen Sie „Seclab VPN". Als Server geben Sie die IP-Adresse des VPN-Servers an.

b) Testen Sie die VPN-Verbindung. Verwenden Sie den Benutzernamen „Administrator" und das Passwort „W2K3Boss" für die Anmeldung.

c) Sehen Sie sich die Details der VPN-Verbindung an (Rechte Maustaste auf die Verbindung → Status). Welche Technologien werden zur Authentifizierung und Verschlüsselung eingesetzt?

.....

.....

.....

.....

.....

d) Wo befinden sich die Schwachstellen dieser Techniken?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

e) Trenne Sie nun die VPN-Verbindung.

Aufgabe 2: Angriff auf die PPTP-Verbindung

a) Offnen Sie auf dem Angreifer-PC die Konsole generieren Sie im Ordner „Desktop" die Hashwerte zu der dort befindlichen Passwortliste (german.txt). Verwenden Sie folgendes Kommando:

```
genkeys -r german.txt -f german.dat -n german.idx
```

Hinweis: Dies kann etwas dauern und verursacht zur Laufzeit mehrere Dateien auf dem Desktop, die anschliessend selbstständig gelöscht werden.

b) Führe Sie nun unter Verwendung der Passworthashes einen passiven Angriff auf die VPN-Verbindung durch. Verwenden Sie dazu folgendes Kommando:

```
asleap -i eth0 -f german.dat -n german.idx –v
```

Hinweis: Lassen Sie nach Eingabe des Kommandos die Konsole geöffnet und verändern Sie nun nichts mehr am VPN-Angreifer.

c) Starten Sie nun die VPN-Verbindung (wie in Aufgabe 1b) erneut und sehen Sie sich anschliessend die Konsole auf dem VPN-Angreifer an. Was fällt Ihnen auf?

.....

.....

d) Beschreiben Sie den durchgeführten Angriff mit einigen Worten. Welchen Zweck erfüllt die Hashwertliste?

.....

.....

.....

.....

.....

.....

.....

.....

e) Trenne Sie nun die VPN-Verbindung.

Aufgabe 3: Sichere Verbindung mittels L2TP und IPSec

a) Was ist L2TP?

.....

.....

.....

.....

b) Was ist IPSec?

.....

.....

.....

.....

.....

c) Ändern Sie die in Aufgabe 1 erstellte VPN-Verbindung so ab, dass die Technologien L2TP und IPSec verwendet werden. Gehen Sie wie folgt vor:

- Öffnen Sie die Eigenschaften der VPN-Verbindung
- Wechseln Sie zur Registerkarte Sicherheit und wählen dort die erweiterten Sicherheitsoptionen
- Wählen Sie zur Authentifizierung ausschliesslich das MS-CHAP V2 Protokoll und bestätigen Sie mit OK.
- Wechseln Sie nun in die Registerkarte Netzwerk und wählen Sie als VPN-Protokoll L2TP-IPSec-VPN aus und bestätigen Sie mit OK.

d) Versuchen Sie die Verbindung zu aktivieren. Was fällt Ihnen auf? Welches Problem liegt vor?

.....

.....

.....

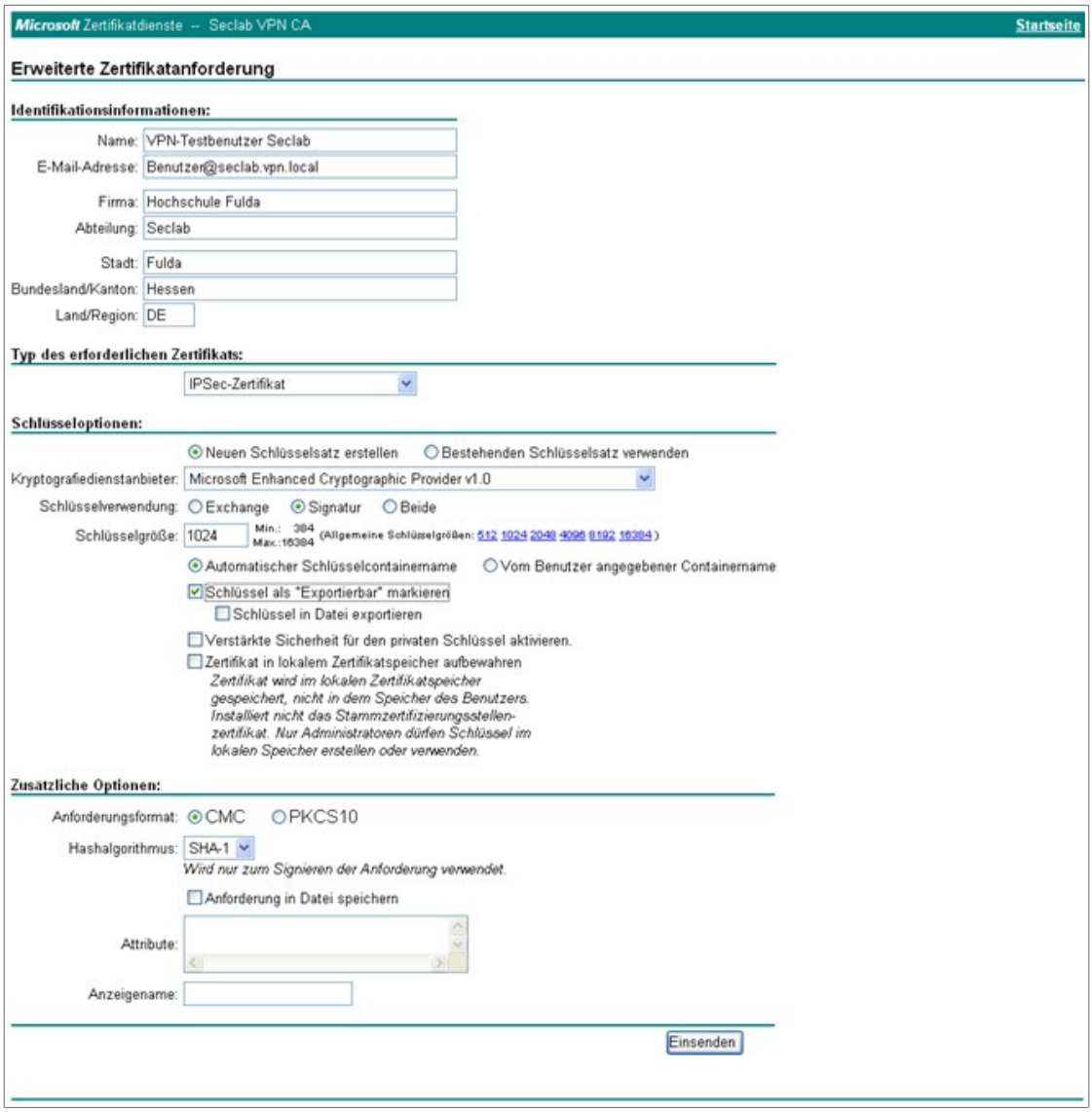
.....

.....

Aufgabe 4: Erzeugen des benötigten Zertifikats

a) Um die in Aufgabe 3 erstellten VPN-Verbindung verwenden zu können, wird ein Zertifikat benötigt. Dieses kann über den Webdienst des VPN-Servers beantragt werden. Gehen Sie wie folgt vor:

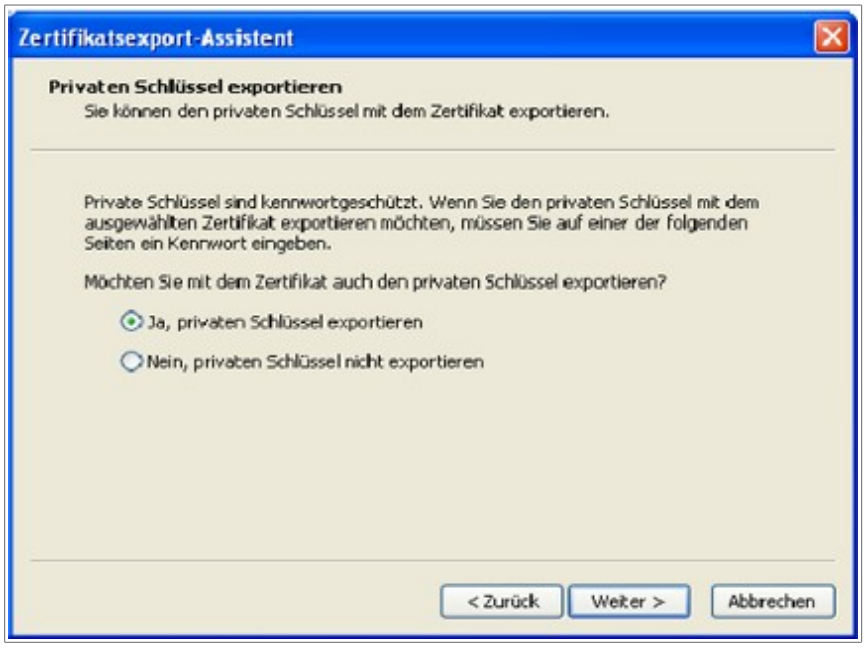
- Öffnen Sie auf dem VPN-Client einen Webbrowser und laden Sie die Webseite unter http://seclab-vpn/certsrv/
- Fordern sie über die „erweiterte Zertifikatsanforderung“ ein neues Zertifikat (ohne Base24-Codierung) an. Verwenden Sie die folgenden Angaben:

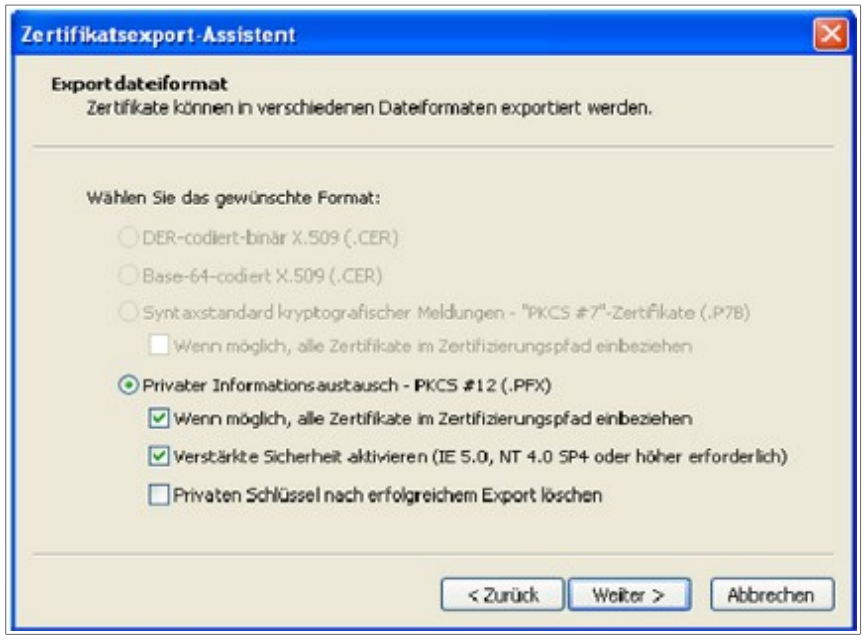


- Klicken Sie auf Einsenden und Installieren Sie das Zertifikat anschliessend. Bestätigen Sie dabei alle Sicherheitsoptionen mit „Ja“. Das Zertifikat befindet sich nun im Zertifikatspeicher des Webbrowsers.

b) Installieren Sie das Zertifikat nun in den lokalen Zertifikatspeicher des Betriebssystems. Gehen Sie wie folgt vor:

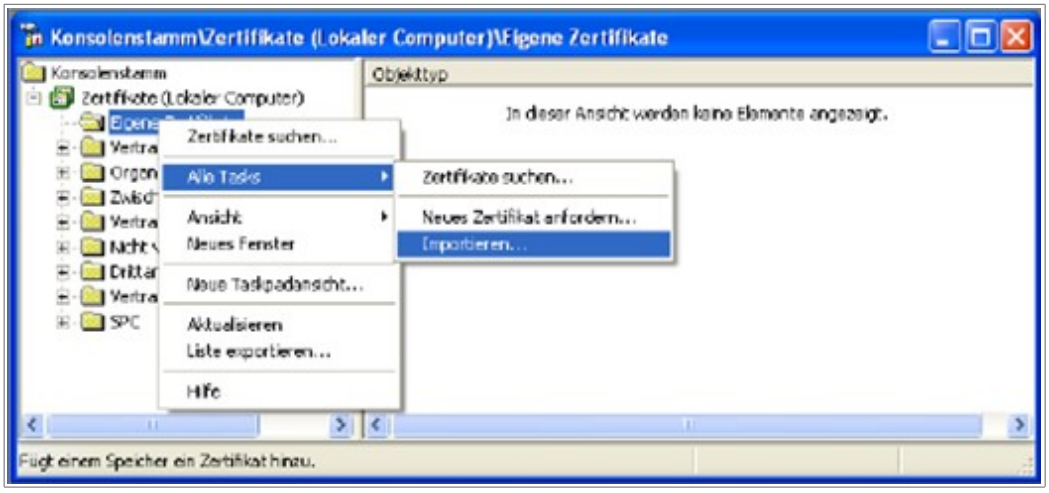
- Navigieren Sie dazu zum Zertifikatstamm des Browsers (Internetexplorer → Extras → Internetoptionen → Inhalte → Zertifikate) und exportieren Sie das zuvor erstellte Zertifikat. Wählen Sie im Export-Assistenten die folgenden Einstellungen:





- Vergeben Sie ein beliebiges Passwort, um die unbefugte Verwendung des Zertifikates zu verhindern und speichern Sie das Zertifikat auf dem Desktop ab.

- Starten Sie die Zertifikatskonsole vom Desktop aus und importieren Sie das Zertifikat.



- Kopieren Sie zum Schluss das Root Zertifikat (Verwendungszweck: <Alle>) von „Eigene Zertifikate/Zertifikate“ nach „Vertrauenswürdige Stammzertifikate/Zertifikate“

c) Die Zertifikate müssen nun auch auf dem Server nach „Eigene Zertifikate“ importiert werden, damit sich der VPN-Client mit diesem authentifizieren kann. Das Zertifikat müsste bei einem produktiven Einsatz natürlich im Firmennetz verteilt werden, wo Zugriff zu dem Server besteht, um es dann für die VPN Verbindung von extern nutzen zu können.

Kopieren Sie das Zertifikat auf den Server und importieren Sie es dort (Verwenden Sie den Freigabe-Ordner auf dem Desktop des VPN-Client)

d) Starten Sie die VPN-Verbindung (wie in Aufgabe 1b) und sehen Sie sich die Verbindungseigenschaften auf dem Client erneut an. Was hat sich verändert? Ist die Verbindung nun sicher (Begründung)?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....