



Falko Dressler Tobias Limmer

Netzwerksicherheit WS 2007/08

IPSEC

4.12.2007

In dieser Übung wird in unserem Übungsnetz IPSEC am praktischen Beispiel behandelt. Wir bauen zwischen zwei Linux-Rechnern einen gesicherten Kanal auf!

Folgende Linux-Kommandos werden für diese Übung benötigt:

1. **tcpdump**: Damit können über ein Netzwerk übertragene Daten an einer Netzwerkschnittstelle abgefragt und angezeigt werden. Folgende Syntax soll verwendet werden:

```
tcpdump -n -i eth1 host <IP vom Partnersystem>
```

2. Ein Terminal-Texteditor Ihrer Wahl (`vi`, `joe`, `emacs`, ...)
3. **dd** und **xxd** zum Kopieren und Aufbereiten von Schlüsselmaterial vom Zufallsgerät:

```
dd if=/dev/random count=16 bs=1 | xxd -ps                   (128 Bit für AH)
dd if=/dev/random count=24 bs=1 | xxd -ps                   (192 Bit für ESP)
```

4. **setkey** um IPSEC Parameter zu setzen:

```
setkey -F                   (Flush SAD)
setkey -FP                  (Flush Policies)
setkey -D                   (Dump SAD)
setkey -DP                  (Dump Policy)
setkey -f <Dateiname>      (Datei mit Befehlen einlesen)
```

5. **ping**, um mit Hilfe von ICMP die Erreichbarkeit des Partnersystems zu testen.

Übungsablauf:

1. Partnergruppe suchen
2. Schlüsselmaterial erzeugen (insgesamt vier Schlüssel pro Verbindung: $A \rightarrow B$, $B \rightarrow A$ jeweils für AH und ESP)
3. Konfigurationsdatei für **setkey** erzeugen:
 - Security Associations (SA) für AH:

```
add 192.168.10.A 192.168.10.B ah <SPI> -A hmac-md5 <Schlüssel>;
add 192.168.10.B 192.168.10.A ah <SPI> -A hmac-md5 <Schlüssel>;
```
 - Security Policies (SP) für AH:

```
spdadd 192.168.10.A 192.168.10.B any -P out ipsec ah/transport//require;  
spdadd 192.168.10.B 192.168.10.A any -P in ipsec ah/transport//require;
```

- Haben Sie die richtige Schlüssellänge angegeben?
4. Konfiguration mit Hilfe von `setkey` laden - *Vorsicht*: eine bestehende Konfiguration wird standardmäßig übernommen! Also nicht vergessen, diese immer vorher zu löschen!
 5. Übertragene Daten mit `tcpdump` überprüfen. Zeigen Sie das Ergebnis einem Betreuer!
 6. SAs für ESP in Konfigurationsdatei hinzufügen:
 - SAs für ESP:

```
add 192.168.10.A 192.168.10.B esp <SPI> -E 3des-cbc <Schlüssel>;  
add 192.168.10.B 192.168.10.A esp <SPI> -E 3des-cbc <Schlüssel>;
```
 - SPs für ESP (String an beide Policy-Zeilen für AH anfügen)

```
esp/transport//require;
```
 - Haben Sie die richtige Schlüssellänge angegeben?
 7. Konfiguration mit `setkey` ins System übernehmen
 8. Erneut Datenverkehr mit `tcpdump` überprüfen und einen Betreuer rufen.
 9. Suchen sie sich einen dritten Partner und bauen Sie mit diesem auch eine IPSEC-Verbindung auf.