stunnel

instrukcja do zajęć laboratoryjnych

Michał Trojnara 2005
uaktualnienie Waldemar Grabski (waldemar.grabski@pw.edu.pl) 2016

1 CEL ĆWICZENIA

Celem ćwiczenia jest zdobycie umiejętności zestawiania połączeń szyfrowanych przy użyciu protokołu SSL. Liczba wykorzystywanych opcji specyficznych dla programu stunnel została ograniczona do minimum. Po odbyciu ćwiczenia student powinien być w stanie prawidłowo skonfigurować szyfrowanie w dowolnej aplikacji wykorzystującej protokół SSL.

2 ZAKRES ĆWICZENIA

W ramach ćwiczenia studenci będą konfigurowali klienty i serwery SSL. Studenci nabędą praktycznej umiejętności użycia certyfikatów X.509 i list CRL do kontroli dostępu.

3 WYMAGANIA WSTĘPNE

W trakcie ćwiczenia wykorzystywana będzie umiejętność generowania certyfikatów oraz list CRL. Studenci mogą użyć dowolnego oprogramowania Centrum Certyfikacji, które pozwala wygenerować certyfikat X.509 i zapisać go w pliku o formacie PEM.

W ramach przygotowania do ćwiczenia należy zapoznać się ze standardową dokumentacją programu stunnel: http://stunnel.mirt.net/static/stunnel.pl.html

4 PRZEBIEG ĆWICZENIA

Ćwiczenie wykonywane będzie w zespołach po dwa komputery w zespole. Na jednym z komputerów konfigurowane będzie oprogramowanie klienta, a na drugim oprogramowanie serwera.

Po realizacji kolejnych etapów należy zaprezentować prowadzącemu uzyskane rezultaty (w momentach zaznaczonych w instrukcji). Będzie to podstawą oceny z laboratorium.

Przydatne opcje pliku konfiguracyjnego

```
debug = 7
chroot=~/stunnel
foreground=yes
output=stunnel.log
pid=stunnel.pid

[tunel1]
client=
accept=
connect=
cert=
key=
CAfile=
CRLfile=
Verify=2
```

Proszę zwrócić uwagę, że parametry wpisujemy w części globalnej (np. debug) oraz w sekcjach dla konkretnych tuneli (patrz sekcja [tunel1]).

4.1 Konfiguracja podstawowa

Na komputerze pełniącym rolę serwera należy skonfigurować program stunnel w trybie serwera SSL nasłuchującego na porcie 1995 i łączącego się do maszyny elka.pw.edu.pl na port 80. Ponieważ serwer SSL wymaga certyfikatu należy go wygenerować (jako nazwę podmiotu proszę użyć nazwy komputera na którym będzie uruchomiony serwer stunnel) i wskazać w pliku stunnel.conf.

Na komputerze pełniącym rolę klienta należy skonfigurować program stunnel w trybie klienta SSL nasłuchującego na porcie 1080 i łączącego się do komputera pełniącego rolę serwera na port 1995.

Proszę narysować na kartce schemat połączenia oznaczając na nim:

- Komputery na których uruchomiony jest: klient (przeglądarka internetowa), klient stunnel, serwer stunnel, maszyna docelowa (serwer www elka.pw.edu.pl),
- Uruchomione procesy: przeglądarka internetowa, stunnel (klient i serwer) i połączenia przez nie nawiązywane z zaznaczeniem numerów portów i adresów IP (na których te procesy nasłuchują i z kim się łączą).

1 Prezentacja realizacji etapu:

- Przedstawić narysowany schemat połączeń

Przetestować połączenie na komputerze klienta, używając przeglądarki internetowej podając jako adres:

```
localhost:1080
```

Po uzyskaniu działającego połączenia należy obejrzeć informacje znajdujące się w logu programu stunnel.

2 Prezentacja realizacji etapu:

- Zaprezentować zestawione połączenie, pokazać pliki konfiguracyjne serwera i klienta

Przydatne opcje pliku stunnel.conf

cert, key, accept, connect, client, debug, output

4.2 Konfiguracja uwierzytelnienia serwera

Na komputerze pełniącym rolę klienta należy włączyć weryfikację certyfikatu serwera (opcja verify=2). Należy sprawdzić, że połączenie przestało działać i obejrzeć komunikat o błędzie w logu programu stunnel. Następnie należy dodać na komputerze pełniącym rolę klienta certyfikat Centrum Certyfikacji użytego do wygenerowania certyfikatu serwera, po czym sprawdzić, że połączenie ponownie działa.

3 Prezentacja realizacji etapu:

- Pokazać komunikat o błędzie w pliku logu, który pojawił się po włączeniu weryfikacji
- Zaprezentować zestawione połączenie z uwierzytelnianiem serwera (pokazać plik konfiguracyjny klienta)

Przydatne opcje pliku stunnel.conf

verify, CAfile

4.3 Konfiguracja uwierzytelnienia klienta

Należy wygenerować certyfikat i zainstalować go na komputerze pełniącym rolę klienta.

Następnie na komputerze pełniącym rolę serwera należy wykonać operacje, które w poprzednim punkcie wykonywane były na komputerze pełniącym rolę klienta.

Przydatne opcje pliku stunnel.conf

cert, key, verify, CAfile

4.4 Odwołanie certyfikatu

Przy użyciu oprogramowania Centrum Certyfikacji należy wygenerować listę˛ CRL odwołującą wygenerowany w poprzednim punkcie certyfikat klienta. Następnie listę˛ CRL należy zainstalować na komputerze pełniącym role˛ serwera. Należy sprawdzić, że serwer odrzuca połączenie od klienta oraz obejrzeć komunikat o błędzie w logu programu stunnel.

4 Prezentacja realizacji etapu:

- Zaprezentować odrzucanie połączenia przez serwer

Przydatne opcje pliku stunnel.conf

CRLfile