SSL/TLS туннелирование соединений защищённой доставки почты

Практическая часть

Цель работы

Изучение принципов безопасного обмена информации с использованием протокола SSL/TLS и ОС Linux.

Схема лабораторной работы

На данном рисунке показана схема, которую вы должны будете исследовать в процессе выполнения лабораторной работы.

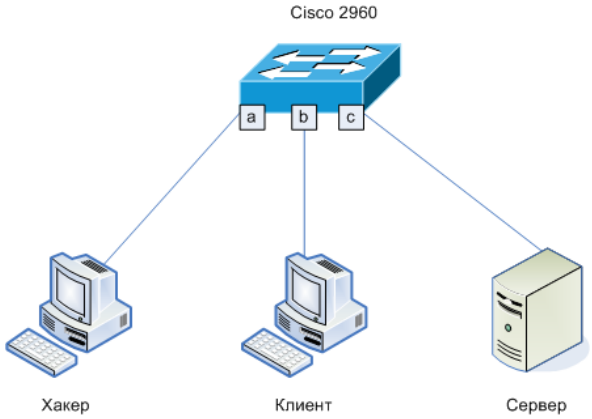

Рисунок. Топология SSL-туннелирования клиент-сервер

Порядок выполнения работы

1). Постройте топологию сети, представленную на рисунке.

2). Настройте «зеркалирование» (Port Mirroring) на коммутаторе следующим образом: порт «a» – приемник, порт «b» – источник. Таким образом, хакер сможет «прослушивать» весь трафик клиента.

3). В качестве POP3-сервера используйте *dovecot.*
Dovecot является производительным и гибким POP/IMAP-сервером, поддерживает SSL/TLS. Для этого выполните базовые настройки конфигурационных файлов */etc/dovecot/dovecot.conf, 10-auth.conf, 10-mail.conf, 10-master.conf, 10-ssl.conf.*

4). Запустите сервер ***Dovecot.***

5). Запустите почтовый клиент *KMail* и настройте на работу с почтовым сервером:
Для этого войдите в меню и добавьте новую учетную запись ***POP3*** , т.е. в качестве сервера укажите адрес машины с сервером ***Dovecot.*** Логин и пароль укажите от любой учетной записи, кроме ***root.***

6). Перехватите незашифрованный пароль.
Для этого получите почту пользователя на машине клиента. Параллельно с этим процессом запустите утилиту *tcpdump* на компьютере хакера и обнаружьте пароль на почтовый ящик в перехваченных пакетах.

7). Настройте SSL туннелирование для защищённой доставки почты. Для этого на сервере запустите утилиту ***stunnel*** на *995* порту.

8). Включите использование SSL/TLS на клиенте.

9). Перехватите зашифрованный пароль. Для этого получите защищенную почту пользователя на машине клиента.

10). Сделайте выводы.

Требования к оформлению лабораторной работы

Отчет студента по проделанной работе оформляется в электронном и печатном виде и должен содержать:

1) титульный лист по принятой форме с название работы, ФИО студента,

2) цель работы, топологию сети с обозначением всех сконфигурированных портов и интерфейсов,

3) последовательность пошагового выполнения всех действий в соответствии с заданием **В**, а именно:

- листинги команд с комментариями,
- скриншоты выполнения команд,

4) анализ и выводы по работе,

5) ответы на контрольные вопросы.

Контрольные вопросы

1. Какое основное назначение протоколов SSL и TLS?
2. В чем отличие протоколов SSL и TLS?
3. Где можно применить SSL/TLS протоколы?
4. Назовите основные свойства SSL -канала.
5. Какие типы аутентификации поддерживает протокол SSL?
6. Какие протоколы записи SSL можно выделить и в чём их отличие?
7. Какие атаки можно проводить на SSL и в чём заключается основная идея атак?

Литература, источники

1. James Boney, Cisco IOS in a Nutshell, O`Reilly, 2010
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2010
3. ru.wikipedia.org/wiki