Использование SystemTap для расшифровки локального HTTPS-трафика

В состав выпуска системы динамической трассировки SystemTap 3.3 добавлен скрипт capture_ssl_master_secrets.stp с примером захвата сессионных ключей SSL/TLS от приложений, использующих gnutls (libgnutls.so) или openssl (libssl.so), которые могут использоваться для организации расшифровки перехваченного трафика.

Пример использования в Debian 9:

Включаем SystemTap:

```
sudo stap-prep
```

Устанавливаем отладочные версии библиотек:

```
sudo apt-get install libgnutls30-dbgsym libssl1.0.2-dbgsym libssl1.1-dbgsym libssl-dev
```

Запускаем перехват ключей, генерируемых при вызове обработчиков tls1_generate_master_secret и generate_normal_master в libssl.so и libgnutls.so:

```
./capture_ssl_master_secrets.stp | tee keylog.txt &
```

Включаем запись дампа трафика в формате pcap:

```
sudo tcpdump -s0 -w traffic.pcap -U port 443 &
```

Формируем тестовые запросы к защищённым сайтам:

```
curl https://www.ssllabs.com/curl_secret
wget https://www.ssllabs.com/wget_secret
echo "GET /sclient_secret HTTP/1.1\nHost: www.ssllabs.com\n\n" | openssl s_client -connect www.ssllabs.com:443 -servername www.ssllabs.com
```

Смотрим, какие ключи удалось захватить:

```
cat keylog.txt

# 1509378583063892 process("/usr/lib/x86_64-linux-gnu/libssl.so.1.0.2").function("tls1_generate_master_secret@./ssl/t1_enc.c:1134").return curl (24745)
CLIENT_RANDOM 92...69000
# 1509378587558501 process("/usr/lib/x86_64-linux-gnu/libgnutls.so.30.13.1").function("generate_normal_master@./lib/kx.c:131").return wget (24755)
CLIENT_RANDOM 59f...28a 560...67c8
# 1509378592611222 process("/usr/lib/x86_64-linux-gnu/libssl.so.1.1").function("tls1_generate_master_secret@../ssl/t1_enc.c:463").return openssl (24757)
CLIENT_RANDOM aa2...fc93 741...127a
```

Расшифровываем дамп трафика, используя захваченные ключи:

```
$ tshark -o ssl.keylog_file:keylog.txt -d tcp.port==443,ssl -x -r traffic.pcap -V | grep -A1 'Decrypted SSL data' |grep "GET "

0000  47 45 54 20 2f 63 75 72 6c 5f 73 65 63 72 65 74   GET /curl_secret
0000  47 45 54 20 2f 77 67 65 74 5f 73 65 63 72 65 74   GET /wget_secret
0000  47 45 54 20 2f 73 63 6c 69 65 6e 74 5f 73 65 63   GET /sclient_sec
```