

## Задание категории «СЕТЬ» с захватом пакетов

Twitter authentication

15 Баллы

Packet capture analysis

Автор

g0uZ, 30 Август 2010

Валидации

57093 Challengeurs

Примечание

★★★★★ 3173 голоса

Мне нравится

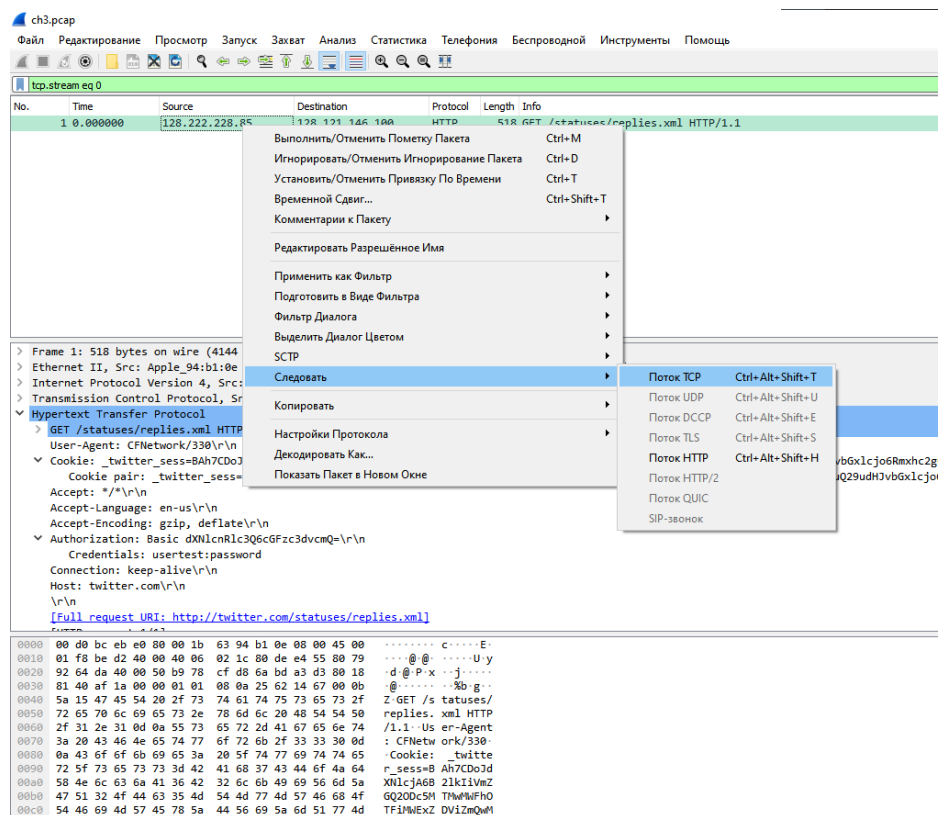
Не нравится

Заявление

A twitter authentication session has been captured, you have to retrieve the password.

Начать вызов

- 1)Скачали пакет ch3.pcap
- 2)Загружаем в wireshark



- 3) копируем сегмент авторизации

```
GET /statuses/replies.xml HTTP/1.1
User-Agent: CFNetwork/330
Cookie:
_twitter_sess=BAh7CD0jdXNlcjA6B2lkIiVmZGQ2ODc5MTMwMWFhOTFiMWE5ZDVz
ea12e7bc090d05202cd7e3f972c2b4414a97f657
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Authorization: Basic dXNlcmlrc3Q6cGFzc3dvcmQ=
Connection: keep-alive
Host: twitter.com
```

- 4) переводим в Base64 и получаем флаг **password** или открываем вкладку

```

> Frame 1: 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits)
> Ethernet II, Src: Apple_94:b1:0e (00:1b:63:94:b1:0e), Dst: Cisco_eb:e0:80 (00:d0:bc:eb:e0:80)
> Internet Protocol Version 4, Src: 128.222.228.85, Dst: 128.121.146.100
> Transmission Control Protocol, Src Port: 55872, Dst Port: 80, Seq: 1, Ack: 1, Len: 452
√ Hypertext Transfer Protocol
  > GET /statuses/replies.xml HTTP/1.1\r\n
    User-Agent: CFNetwork/330\r\n
  √ Cookie: _twitter_sess=BAh7CDoJdXNlcjA6B2lkIiVmZGQ2ODc5MTMwMWFhOTFiMWEzZDVhZmQwMGEz%250AOWNkMyIKZmxh
    Cookie pair: _twitter_sess=BAh7CDoJdXNlcjA6B2lkIiVmZGQ2ODc5MTMwMWFhOTFiMWEzZDVhZmQwMGEz%250AOWNk
    Accept: */*\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
  √ Authorization: Basic dXNlcjRlc3Q6cGFzc3dvcmQ=\r\n
    Credentials: usertest:password
    Connection: keep-alive\r\n
    Host: twitter.com\r\n
    \r\n
    [Full request URI: http://twitter.com/statuses/replies.xml]
0040  5a 15 47 45 54 20 2f 73 74 61 74 75 73 65 73 2f  Z GET /s tatuses/
0050  72 65 70 6c 69 65 73 2e 78 6d 6c 20 48 54 54 50  replies. xml HTTP
0060  2f 31 2e 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74  /1.1. Us er-Agent
0070  3a 20 43 46 4e 65 74 77 6f 72 6b 2f 33 33 30 0d  : CFNetw ork/330
0080  0a 43 6f 6f 6b 69 65 3a 20 5f 74 77 69 74 74 65  Cookie: _twitte
0090  73 5f 73 6f 73 73 3d 43 41 68 73 43 44 6f 45 64  - sess=BAh7CDoJd

```