Bezpieczeństwo w sieci. Lab 02

Marcin Fabrykowski

1 Odczytywanie niebezpiecznych danych użytkownika

W tym ćwiczeniu uruchamiamy sniffer i wchodzimy na stronę z formularzem logowania o której wiemy że nie szyfruje danych.
Efektem podłuchu jest możliwość odczytania takigo pakietu:

```
No.     Time        Source                Destination           Protocol Length Info
      8 9.041630    10.0.2.15             85.234.150.53         HTTP     720    POST /index.ph

Frame 8: 720 bytes on wire (5760 bits), 720 bytes captured (5760 bits)
    Arrival Time: Jun  1, 2012 01:54:28.113836000 CEST
    Epoch Time: 1338508468.113836000 seconds
    [Time delta from previous captured frame: 0.001571000 seconds]
    [Time delta from previous displayed frame: 0.001571000 seconds]
    [Time since reference or first frame: 9.041630000 seconds]
    Frame Number: 8
    Frame Length: 720 bytes (5760 bits)
    Capture Length: 720 bytes (5760 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Dst: 52:55:0a:00:02:02 (52:55:0a:00:0
    Destination: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
        Address: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the
    Source: RealtekU_12:34:56 (52:54:00:12:34:56)
        Address: RealtekU_12:34:56 (52:54:00:12:34:56)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 85.234.150.53 (85.234.150.53)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capab
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x0
    Total Length: 706
    Identification: 0x0012 (18)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
```

```
    Header checksum: 0x3ff6 [correct]
        [Good: True]
        [Bad: False]
    Source: 10.0.2.15 (10.0.2.15)
    Destination: 85.234.150.53 (85.234.150.53)
Transmission Control Protocol, Src Port: 50072 (50072), Dst Port: http (80), Seq: 1, Ack: 1, L
    Source port: 50072 (50072)
    Destination port: http (80)
    [Stream index: 2]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 667    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgement: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
    Window size value: 14600
    [Calculated window size: 14600]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x9fcc [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
    [SEQ/ACK analysis]
        [Bytes in flight: 666]
Hypertext Transfer Protocol
    POST /index.php3 HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): POST /index.php3 HTTP/1.1\r\n]
            [Message: POST /index.php3 HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: POST
        Request URI: /index.php3
        Request Version: HTTP/1.1
    Host: www.haxite.org\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:11.0) Gecko/20100101 Firefox/11.0\r
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://haxite.org/\r\n
    Cookie: __utma=229948165.756951228.1338508449.1338508449.1338508449.1; __utmb=229948165; _
```

```
    Content-Type: application/x-www-form-urlencoded\r\n
    Content-Length: 79\r\n
        [Content length: 79]
    \r\n
    [Full request URI: http://www.haxite.org/index.php3]
Line-based text data: application/x-www-form-urlencoded
    logujsie=ok&site=loginpage&go_fwd=%2F&user=moj_login&haslo=tajne&submit=+loguj+

0000  52 55 0a 00 02 02 52 54 00 12 34 56 08 00 45 00   RU....RT..4V..E.
0010  02 c2 00 12 40 00 40 06 3f f6 0a 00 02 0f 55 ea   ....@.@.?.....U.
0020  96 35 c3 98 00 50 cd 18 a1 3f 26 c4 ce 02 50 18   .5...P...?&...P.
0030  39 08 9f cc 00 00 50 4f 53 54 20 2f 69 6e 64 65   9.....POST /inde
0040  78 2e 70 68 70 33 20 48 54 54 50 2f 31 2e 31 0d   x.php3 HTTP/1.1.
0050  0a 48 6f 73 74 3a 20 77 77 77 2e 68 61 78 69 74   .Host: www.haxit
0060  65 2e 6f 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e   e.org..User-Agen
0070  74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28   t: Mozilla/5.0 (
0080  58 31 31 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e   X11; Ubuntu; Lin
0090  75 78 20 78 38 36 5f 36 34 3b 20 72 76 3a 31 31   ux x86_64; rv:11
00a0  2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31   .0) Gecko/201001
00b0  30 31 20 46 69 72 65 66 6f 78 2f 31 31 2e 30 0d   01 Firefox/11.0.
00c0  0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74   .Accept: text/ht
00d0  6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78   ml,application/x
00e0  68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61   html+xml,applica
00f0  74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a   tion/xml;q=0.9,*
0100  2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74   /*;q=0.8..Accept
0110  2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73   -Language: en-us
0120  2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70   ,en;q=0.5..Accep
0130  74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70   t-Encoding: gzip
0140  2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e 65   , deflate..Conne
0150  63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76   ction: keep-aliv
0160  65 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70   e..Referer: http
0170  3a 2f 2f 68 61 78 69 74 65 2e 6f 72 67 2f 0d 0a   ://haxite.org/..
0180  43 6f 6f 6b 69 65 3a 20 5f 5f 75 74 6d 61 3d 32   Cookie: __utma=2
0190  32 39 39 34 38 31 36 35 2e 37 35 36 39 35 31 32   29948165.7569512
01a0  32 38 2e 31 33 33 38 35 30 38 34 34 39 2e 31 33   28.1338508449.13
01b0  33 38 35 30 38 34 34 39 2e 31 33 33 38 35 30 38   38508449.1338508
01c0  34 34 39 2e 31 3b 20 5f 5f 75 74 6d 62 3d 32 32   449.1; __utmb=22
01d0  39 39 34 38 31 36 35 3b 20 5f 5f 75 74 6d 63 3d   9948165; __utmc=
01e0  32 32 39 39 34 38 31 36 35 3b 20 5f 5f 75 74 6d   229948165; __utm
01f0  7a 3d 32 32 39 39 34 38 31 36 35 2e 31 33 33 38   z=229948165.1338
0200  35 30 38 34 34 39 2e 31 2e 31 2e 75 74 6d 63 63   508449.1.1.utmcc
0210  6e 3d 28 64 69 72 65 63 74 29 7c 75 74 6d 63 73   n=(direct)|utmcs
0220  72 3d 28 64 69 72 65 63 74 29 7c 75 74 6d 63 6d   r=(direct)|utmcm
0230  64 3d 28 6e 6f 6e 65 29 0d 0a 43 6f 6e 74 65 6e   d=(none)..Conten
0240  74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74   t-Type: applicat
0250  69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75   ion/x-www-form-u
0260  72 6c 65 6e 63 6f 64 65 64 0d 0a 43 6f 6e 74 65   rlencoded..Conte
0270  6e 74 2d 4c 65 6e 67 74 68 3a 20 37 39 0d 0a 0d   nt-Length: 79...
0280  0a 6c 6f 67 75 6a 73 69 65 3d 6f 6b 26 73 69 74   .logujsie=ok&sit
```

```
0290  65 3d 6c 6f 67 69 6e 70 61 67 65 26 67 6f 5f 66   e=loginpage&go_f
02a0  77 64 3d 25 32 46 26 75 73 65 72 3d 6d 6f 6a 5f   wd=%2F&user=moj_
02b0  6c 6f 67 69 6e 26 68 61 73 6c 6f 3d 74 61 6a 6e   login&haslo=tajn
02c0  65 26 73 75 62 6d 69 74 3d 2b 6c 6f 67 75 6a 2b   e&submit=+loguj+
```

Jak można zauważyć, w powyższym pakiecie przysyłane sa jawnie dane logowania: "moj_login" oraz "tajne"

2 Wireshark

Chciałbym wspomnieć na wstępie, iż uważam że wstawianie screenshotów z wiresharka mija się z celem.

2.1 Analiza ramek

We wstępie teoretycznym jest błąd, gdyż protokół ARP rozsyła request po macu FF:FF:FF:FF:FF, gdyż jeszcze nie zna maca odbiorcy. Pozostałe zaobserwowane rzeczy zgadzają się z wstępem teoretycznym.

2.2 Analiza liczby pakietow

Łącząc się ze swoją prostą strona, zaobserowałem wymianę kilku pakietów:

1. 3-way-handshake
2. 2 pakiety requesta i 2 ACK

natomiast, łącząc się z stroną onetu zaobserwowałem

1. 3-way-handshake
2. ok 20 pakietów segmentowych dla jednej dużej treści strony (+20 tyle samo ACK)

Chciałbym dodać, że wykorzystywaną przeglądarką był links. Przypuszczam również, że oczekiwanym wynikiem była porcja danych którą otrzymałem, a następnie kolejne połączenia dla takich elementów jak obrazki, skrypty JS, oraz CSS.

2.3 Traceroute

Wykonanie polecenia traceroute nie dało żadnych przydatnych danych, prawdopodobnie z powodu filtrów na bramie w sieci.
Jednak zauważamy w snifferze, że traceroute wysyła dane do badanego hosta, z rosnącymi ttlami. Począwszy od 1. Oczekuje on odpowiedzi od poszczególnych hostów po drodze ze "pakiet umarł" i na tej podstawie próbować będzie badać hosty pośredniczące w komunikacji.

3 3-way-handshake

Połączenie inicjowane jest przez klienta. Następuje wymiana pakietów SYN→SYN,ACK→ACK, po czym połączenie jest nawiązane.
Następnie odbywa się wymiana danych.
Zakonczenie połączenia inicjuje klient. Wymiana pakietów: FIN,ACK→ACK.
Następnie od servera: FIN,ACK→ACK

4 POP3

Zauważyłem, że dane do logowania były przesyłane w formie jawnej, co niesie za sobą możliwość bezproblemowego dostępu do skrzynki pocztowej osobom postronnym.

5 FTP

Tutaj podobnie jak w POP3, dane do logowania, oraz wykonywane operacje były przesyłane w sposób jawny. Niestety nie udało mi się pobrać żadnego pliku, dlatego całe moje połączenie odbyło się na porcie 21 i nie zostałem przekierowany na ftp-data (port 20), co zgodnie z moją wiedzą, powinno stać się w przybadku przesyłu danych.