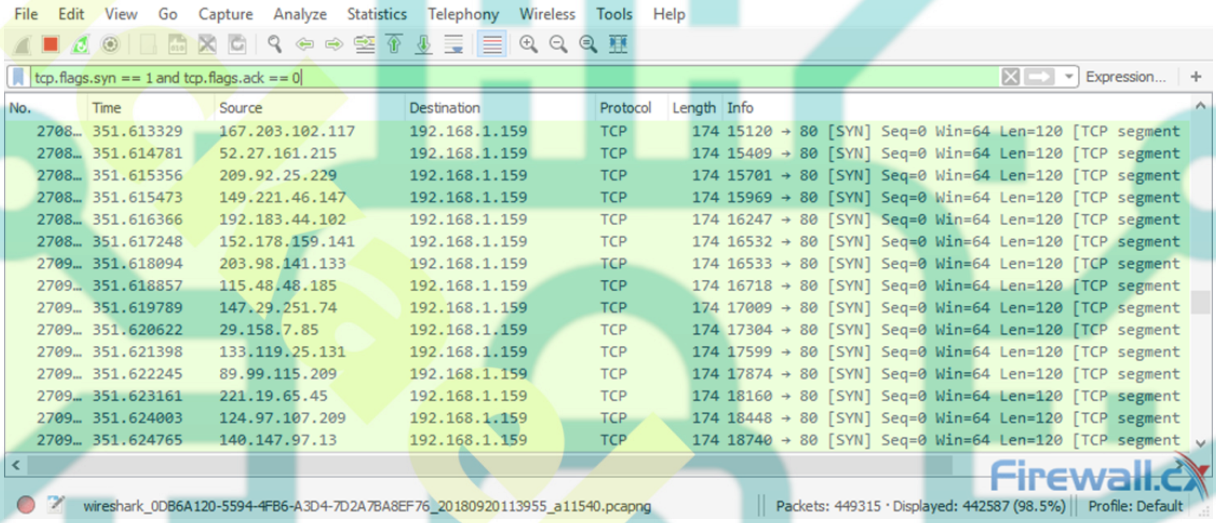
TP – Reconnaitre les attaques

Capture 1



- De quel type est cette attaque ?

Capture 2

```
Line-based text data: text/html (29 lines)
    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">\r\n
    <html xmlns="http://www.w3.org/1999/xhtml">\r\n
    <head>\r\n
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>\r\n
    <title>401 - Non autoris�: acc�s refus� en raison d'informations d'identification non valides.</title>\r\n
    <style type="text/css">\r\n
    <!--\r\n
    body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}\r\n
    fieldset{padding:0 15px 10px 15px;} \r\n
    h1{font-size:2.4em;margin:0;color:#FFF;}\r\n
    h2{font-size:1.7em;margin:0;color:#CC0000;} \r\n
    h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} \r\n
    #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;\r\n
    background-color:#555555;}\r\n
    #content{margin:0 0 0 2%;position:relative;}\r\n
    .content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}\r\n
    -->\r\n
    </style>\r\n
    </head>\r\n
    <body>\r\n
```

- Que représente le contenu de cette trame ?

Capture 3

```
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
  Request Method: GET
  Request URI: /
  Request Version: HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, */*\r\n
Accept-Language: fr-FR\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\r\n
Accept-Encoding: gzip, deflate\r\n
If-Modified-Since: Sun, 03 Apr 2022 10:47:06 GMT\r\n
If-None-Match: "15ab47294847d81:0"\r\n
Host: 192.168.2.1\r\n
Connection: Keep-Alive\r\n
Authorization: Basic cGllcnJlOlBhJCR3b3Jk\r\n
  Credentials: pierre:Pa$$word
```

- Quel est le navigateur utilisé ?
- Quelle est l'authentification utilisée ?
- Trouve-t'on des informations sensibles ?

Capture 4

Capture avant spoofing

```
Ethernet II, Src: PcsCompu_b1:a1:6c (08:00:27:b1:a1:6c), Dst: PcsCompu_67:68:fe (08:00:27:67:68:fe)
  Destination: PcsCompu_67:68:fe (08:00:27:67:68:fe)
  Source: PcsCompu_b1:a1:6c (08:00:27:b1:a1:6c)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.2.3, Dst: 192.168.2.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 539
  Identification: 0x0035 (53)
  Flags: 0x40, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x7353 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.2.3
  Destination Address: 192.168.2.1
Transmission Control Protocol, Src Port: 49157, Dst Port: 80, Seq: 1, Ack: 1, Len: 499
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x
  Accept-Language: fr-FR\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727;
```

Capture après spoofing

```
Ethernet II, Src: PcsCompu_96:18:98 (08:00:27:96:18:98), Dst: PcsCompu_67:68:fe (08:00:27:67:68:fe)
> Destination: PcsCompu_67:68:fe (08:00:27:67:68:fe)
> Source: PcsCompu_96:18:98 (08:00:27:96:18:98)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.2.3, Dst: 192.168.2.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 539
  Identification: 0x0040 (64)
> Flags: 0x40, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x7348 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.2.3
  Destination Address: 192.168.2.1
Transmission Control Protocol, Src Port: 49158, Dst Port: 80, Seq: 1, Ack: 1, Len: 499
Hypertext Transfer Protocol
> GET / HTTP/1.1\r\n
  Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap,
  Accept-Language: fr-FR\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
  Accept-Encoding: gzip, deflate\r\n
  If-Modified-Since: Sun, 03 Apr 2022 10:47:06 GMT\r\n
  If-None-Match: "15ab47294847d81:0"\r\n
```

- Repérer les différences dans la couche Ethernet
- Repérer les différences dans la couche IP
- Repérer les différences dans la couche http

Capture 5

```
Transmission Control Protocol, Src Port: 21, Dst Port: 49159, Seq: 28, Ack: 1, Len: 14
  Source Port: 21
  Destination Port: 49159
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 14]
  Sequence Number: 28    (relative sequence number)
```

- Quels ports sont utilisés lors de la connexion ?
- De quelle application s'agit-il ?

Capture 6

```
File Transfer Protocol (FTP)
  331 Password required\r\n
      Response code: User name okay, need password (331)
      Response arg: Password required
  [Current working directory: ]
```

- Que demande l'applicatif ?

Capture 7

```
Ethernet II, Src: PcsCompu_b1:a1:6c (08:00:27:b1:a1:6c), Dst: PcsCompu_67:68:fe (08:00:27:67:68:fe)
  > Destination: PcsCompu_67:68:fe (08:00:27:67:68:fe)
  > Source: PcsCompu_b1:a1:6c (08:00:27:b1:a1:6c)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.2.3, Dst: 192.168.2.1
> Transmission Control Protocol, Src Port: 49160, Dst Port: 21, Seq: 14, Ack: 65, Len: 15
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  08 00 27 67 68 fe 08 00  27 b1 a1 6c 08 00 45 00   ··'gh··· '··l··E·
0010  00 37 00 51 40 00 80 06  75 1b c0 a8 02 03 c0 a8   ·7·Q@··· u·······
0020  02 01 c0 08 00 15 79 8d  78 a2 e2 02 13 a8 50 18   ·····y· x·····P·
0030  40 19 1b 57 00 00 50 41  53 53 20 50 61 24 24 77   @··W··PA SS Pa$$w
0040  6f 72 64 0d 0a                                    ord··
```

- Quel est le mot de passe saisi ?

Capture 8

```
Ethernet II, Src: PcsCompu_b1:a1:6c (08:00:27:b1:a1:6c), Dst: PcsCompu_67:68:fe (08:00:27:67:68:fe)
  > Destination: PcsCompu_67:68:fe (08:00:27:67:68:fe)
  > Source: PcsCompu_b1:a1:6c (08:00:27:b1:a1:6c)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.2.3, Dst: 192.168.2.1
> Transmission Control Protocol, Src Port: 49160, Dst Port: 21, Seq: 1, Ack: 42, Len: 13
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  08 00 27 67 68 fe 08 00  27 b1 a1 6c 08 00 45 00   ··'gh··· '··l··E·
0010  00 35 00 50 40 00 80 06  75 1e c0 a8 02 03 c0 a8   ·5·P@··· u·······
0020  02 01 c0 08 00 15 79 8d  78 95 e2 02 13 91 50 18   ·····y· x·····P·
0030  40 1e 3c 7d 00 00 55 53  45 52 20 70 69 65 72 72   @·<}··US ER pierr
0040  65 0d 0a                                          e··
```

- Quel est le nom de l'utilisateur ?

Capture 9

```
> Destination: PcsCompu_67:68:fe (08:00:27:67:68:fe)
> Source: PcsCompu_b1:a1:6c (08:00:27:b1:a1:6c)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.2.3, Dst: 192.168.2.1
> Transmission Control Protocol, Src Port: 49167, Dst Port: 21, Seq: 65, Ack: 177, Len: 22
v File Transfer Protocol (FTP)
  v RETR /Secret/mdp.txt\r\n
      Request command: RETR
      Request arg: /Secret/mdp.txt
  [Current working directory: ]
```

```
0000  08 00 27 67 68 fe 08 00  27 b1 a1 6c 08 00 45 00   ··'gh··· '··l··E·
0010  00 3e 00 92 40 00 80 06  74 d3 c0 a8 02 03 c0 a8   ·>··@··· t·······
0020  02 01 c0 0f 00 15 fe 55  83 9c be c5 9c a1 50 18   ·······U ·····P·
0030  3f fd 22 03 00 00 52 45  54 52 20 2f 53 65 63 72   ?·"···RE TR /Secr
0040  65 74 2f 6d 64 70 2e 74  78 74 0d 0a               et/mdp.t xt··
```

- Dans quel répertoire se situe-t-on ?

Capture 10

```
FTP Data (22 bytes data)
[Setup frame: 32]
[Setup method: PASV]
[Command: SIZE /Secret/mdp.txt]
Command frame: 36
[Current working directory: ]
v Line-based text data (3 lines)
    password\r\n
    azerty\r\n
    toto
```

```
0000  08 00 27 b1 a1 6c 08 00  27 67 68 fe 08 00 45 00   ··'··l·· 'gh···E·
0010  00 3e 10 db 40 00 80 06  00 00 c0 a8 02 01 c0 a8   ·>··@··· ········
0020  02 03 c5 66 c0 10 b1 7f  f7 b7 a0 a0 d7 25 50 18   ···f···· ·····%P·
0030  08 05 85 85 00 00 70 61  73 73 77 6f 72 64 0d 0a   ·····pa ssword··
0040  61 7a 65 72 74 79 0d 0a  74 6f 74 6f              azerty·· toto
```

- Quel est le nom du fichier
- Quel est son contenu

Capture 11

144	58.817616	60	192.168.2.3	192.168.2.1	SMTP	C: mail f
148	59.393688	60	192.168.2.3	192.168.2.1	SMTP	C: mail fro
150	59.665645	60	192.168.2.3	192.168.2.1	SMTP	C: mail from
156	63.881620	60	192.168.2.3	192.168.2.1	SMTP	C: mail from:
158	65.665684	60	192.168.2.3	192.168.2.1	SMTP	C: mail from:
160	68.153606	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: s
164	68.641619	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: ser
166	69.217723	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: serv
170	69.953676	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: servic
174	70.393631	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: servicec
176	70.817663	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: servicecl
180	71.305765	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: serviceclie
184	71.713647	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: serviceclient
186	72.577710	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: serviceclient@
190	73.609671	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: serviceclient@go
194	74.073726	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: serviceclient@goog
199	74.593679	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: serviceclient@google
201	74.937671	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: serviceclient@google.
205	75.577661	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: serviceclient@google.co
207	75.825667	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: serviceclient@google.com
209	76.961599	60	192.168.2.3	192.168.2.1	SMTP	C: mail from: serviceclient@google.com

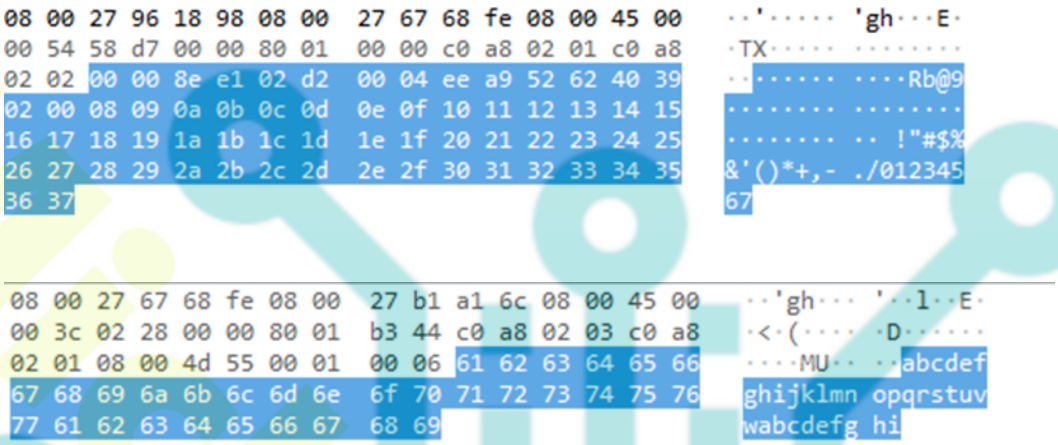
- Quel est le protocole utilisé ?
- D'où provient le message ?
- Avec quel applicatif a été créé le message ?

Capture 12

```
Domain Name System (response)
    Transaction ID: 0xfc52
  > Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    > smtp.test.lan: type A, class IN
  ⌄ Answers
    > smtp.test.lan: type A, class IN, addr 192.168.2.1
```

- De quel protocole s'agit-il ?
- Quelle est la demande du client ?
- Quelle est la réponse du serveur ?

Capture 13


08 00 27 96 18 98 08 00 27 67 68 fe 08 00 45 00 ··'····· 'gh···E·
00 54 58 d7 00 00 80 01 00 00 c0 a8 02 01 c0 a8 ·TX····· ········
02 02 00 00 8e e1 02 d2 00 04 ee a9 52 62 40 39 ······· ····Rb@9
02 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 ········ ········
16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ········ ·· !"#$%
26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345
36 37 67

08 00 27 67 68 fe 08 00 27 b1 a1 6c 08 00 45 00 ··'gh··· '··l··E·
00 3c 02 28 00 00 80 01 b3 44 c0 a8 02 03 c0 a8 ·<·(····· ·D·····
02 01 08 00 4d 55 00 01 00 06 61 62 63 64 65 66 ····MU·· ··abcdef
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
77 61 62 63 64 65 66 67 68 69 wabcdefg hi