OS OBJECTIF SÉCURITÉ
Architecte de la sécurité informatique

Proxy transparent pour l'interception et la modification de trafic TCP

Bertrand Mesot

bertrand.mesot@objectif-securite.ch

Exemples

Exemple

Ticket: 7-13

Sandwich	1x 4.50	4.50
TOTAL :	**SFr.**	**4.50**
EURO	EUR	3.78

Compte personnel: 4.50

Numéro de TVA: 123456

TVA%	MONTANT
8.00	0.33

Federer Roger Compte personnel 44447
Solde: 94.70

MERCI DE VOTRE VISITE!

****

Ticket: 7-14

Sandwich	-1x 4.50	-4.50
TOTAL :	**SFr.**	**-4.50**
EURO	EUR	-3.78

Compte personnel: -4.50

Numéro de TVA: 123456

TVA%	MONTANT
8.00	-0.33

Federer Roger Compte personnel 44447
Solde: 2.20

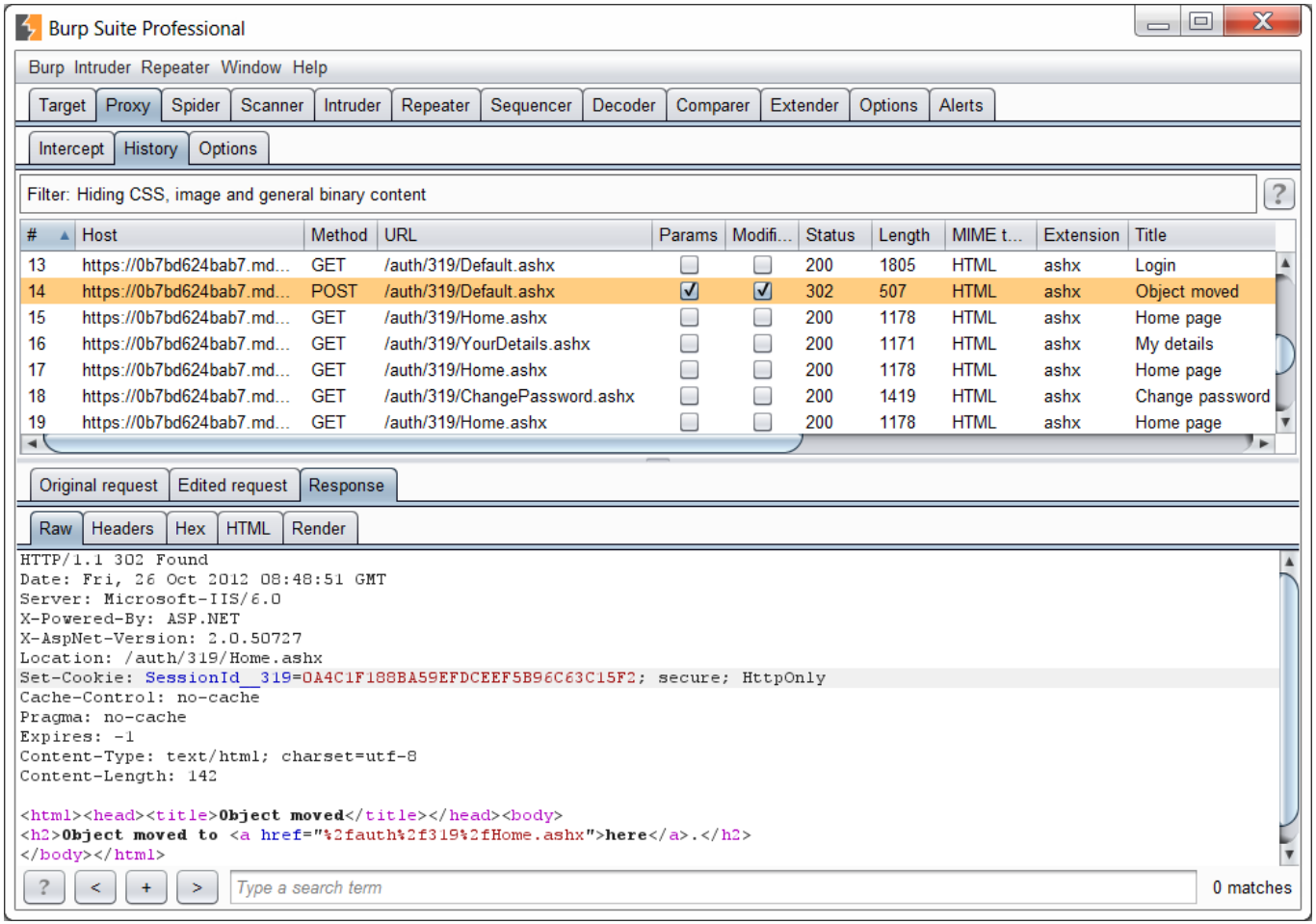
MERCI DE VOTRE VISITE!

****

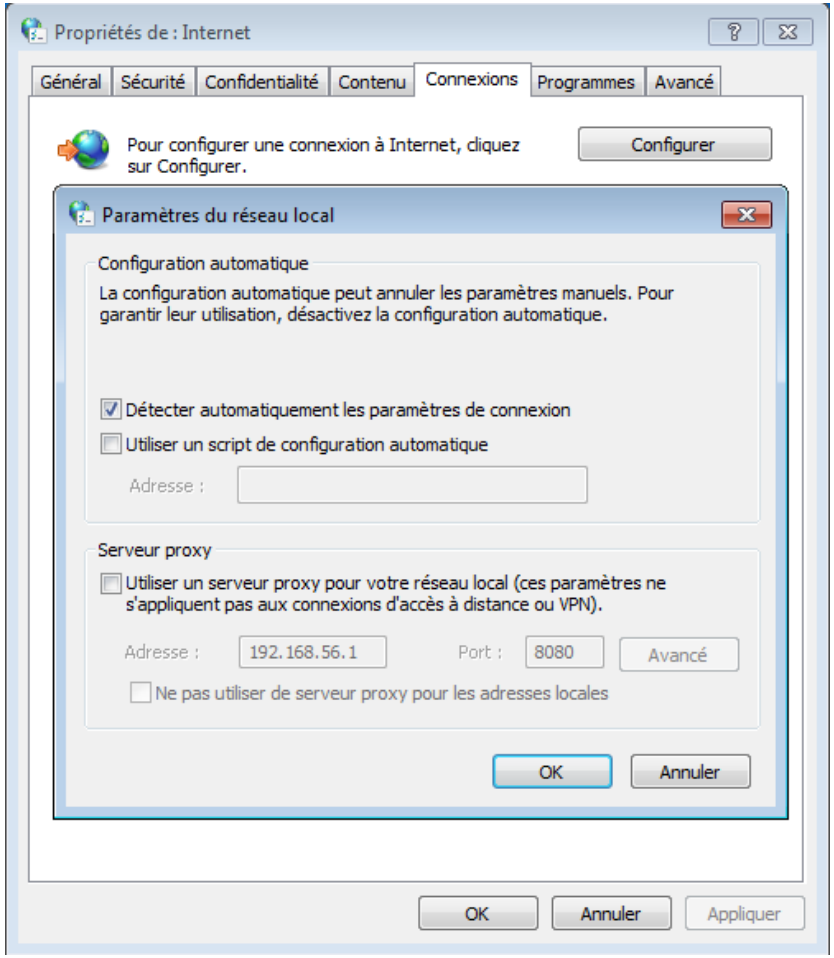
Fonctionnement

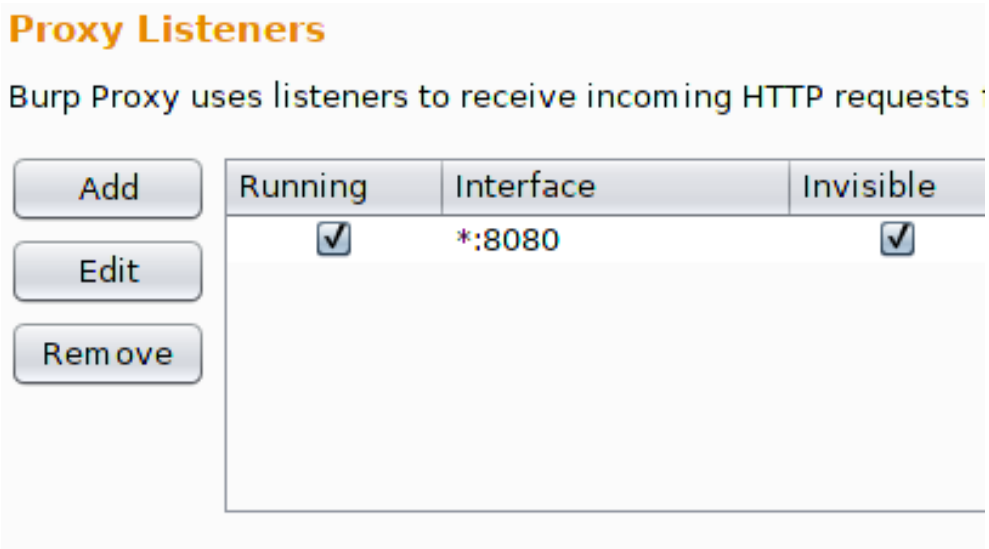
- Interception du trafic
  - Redirection explicite (configuration, routage)
  - Détournement (ARP spoofing, bridging)
- Modification des données interceptées
  - Déchiffrement SSL / TLS
  - Décompression (zip), désérialisation (objects Java)
- Envoi des données à la bonne destination

Proxy HTTP(s)


Burp Suite Professional
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept History Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Modifi... Status Length MIME t... Extension Title
13 https://0b7bd624bab7.md... GET /auth/319/Default.ashx 200 1805 HTML ashx Login
14 https://0b7bd624bab7.md... POST /auth/319/Default.ashx 302 507 HTML ashx Object moved
15 https://0b7bd624bab7.md... GET /auth/319/Home.ashx 200 1178 HTML ashx Home page
16 https://0b7bd624bab7.md... GET /auth/319/YourDetails.ashx 200 1171 HTML ashx My details
17 https://0b7bd624bab7.md... GET /auth/319/Home.ashx 200 1178 HTML ashx Home page
18 https://0b7bd624bab7.md... GET /auth/319/ChangePassword.ashx 200 1419 HTML ashx Change password
19 https://0b7bd624bab7.md... GET /auth/319/Home.ashx 200 1178 HTML ashx Home page
Original request Edited request Response
Raw Headers Hex HTML Render
HTTP/1.1 302 Found
Date: Fri, 26 Oct 2012 08:48:51 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Location: /auth/319/Home.ashx
Set-Cookie: SessionId__319=0A4C1F188BA59EFDCEEF5B96C63C15F2; secure; HttpOnly
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Content-Type: text/html; charset=utf-8
Content-Length: 142
<html><head><title>Object moved</title></head><body>
<h2>Object moved to here.</h2>
</body></html>
? < + >
Type a search term
0 matches

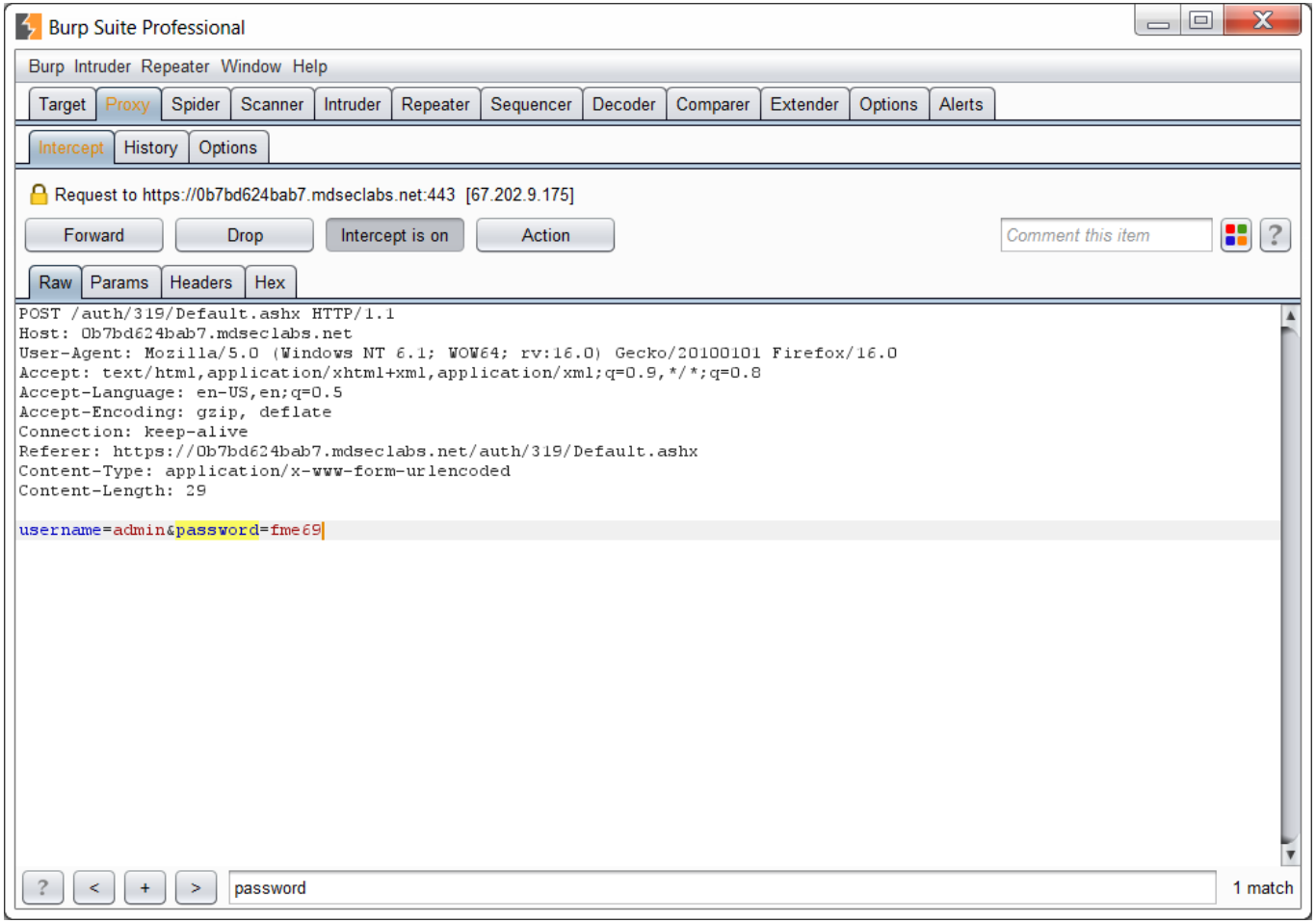
HTTP(s): Interception






```
iptables
   -t nat
   -A PREROUTING
   -s 192.168.56.2
   -p tcp -m tcp --dport 80
   -j REDIRECT --to-port 8080
```

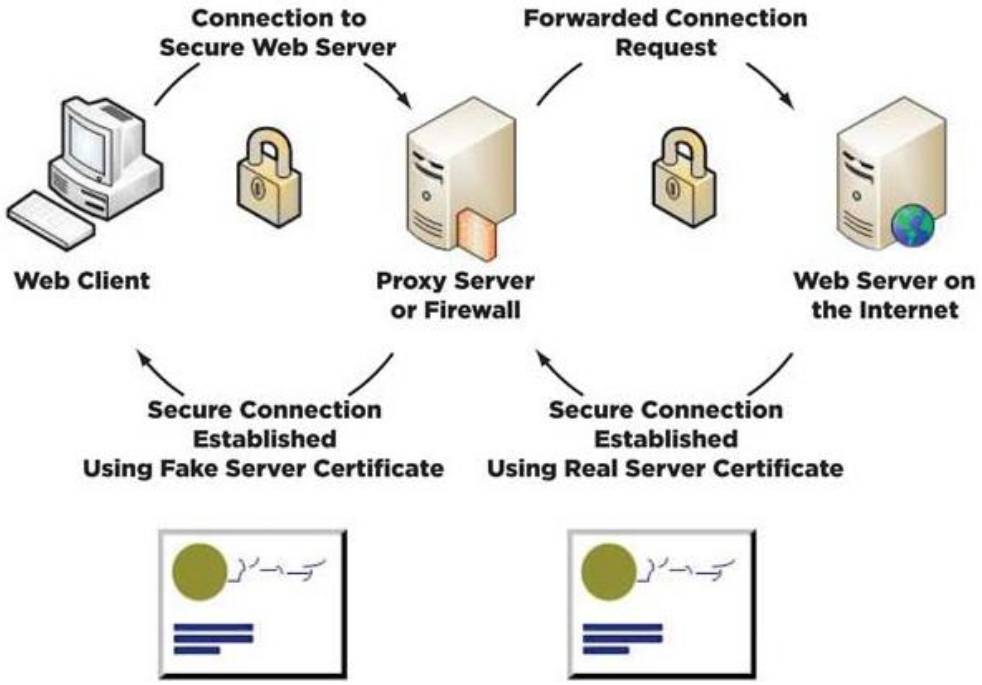
HTTP(s): Modification



HTTP(s): Déchiffrement

```
Frame 4: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits) on interface 0
Ethernet II, Src: WistronI_be:c1:a8 (3c:97:0e:be:c1:a8), Dst: IntelCor_22:9e:09 (00:1b:21:22:9e:09)
Internet Protocol Version 4, Src: 192.168.5.103 (192.168.5.103), Dst: 80.74.147.72 (80.74.147.72)
Transmission Control Protocol, Src Port: 51636 (51636), Dst Port: https (443), Seq: 1, Ack: 1, Len: 191
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 186
  Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 182
    Version: TLS 1.2 (0x0303)
    Random
    Session ID Length: 0
    Cipher Suites Length: 46
    Cipher Suites (23 suites)
    Compression Methods Length: 1
    Compression Methods (1 method)
    Extensions Length: 95
    Extension: server_name
```

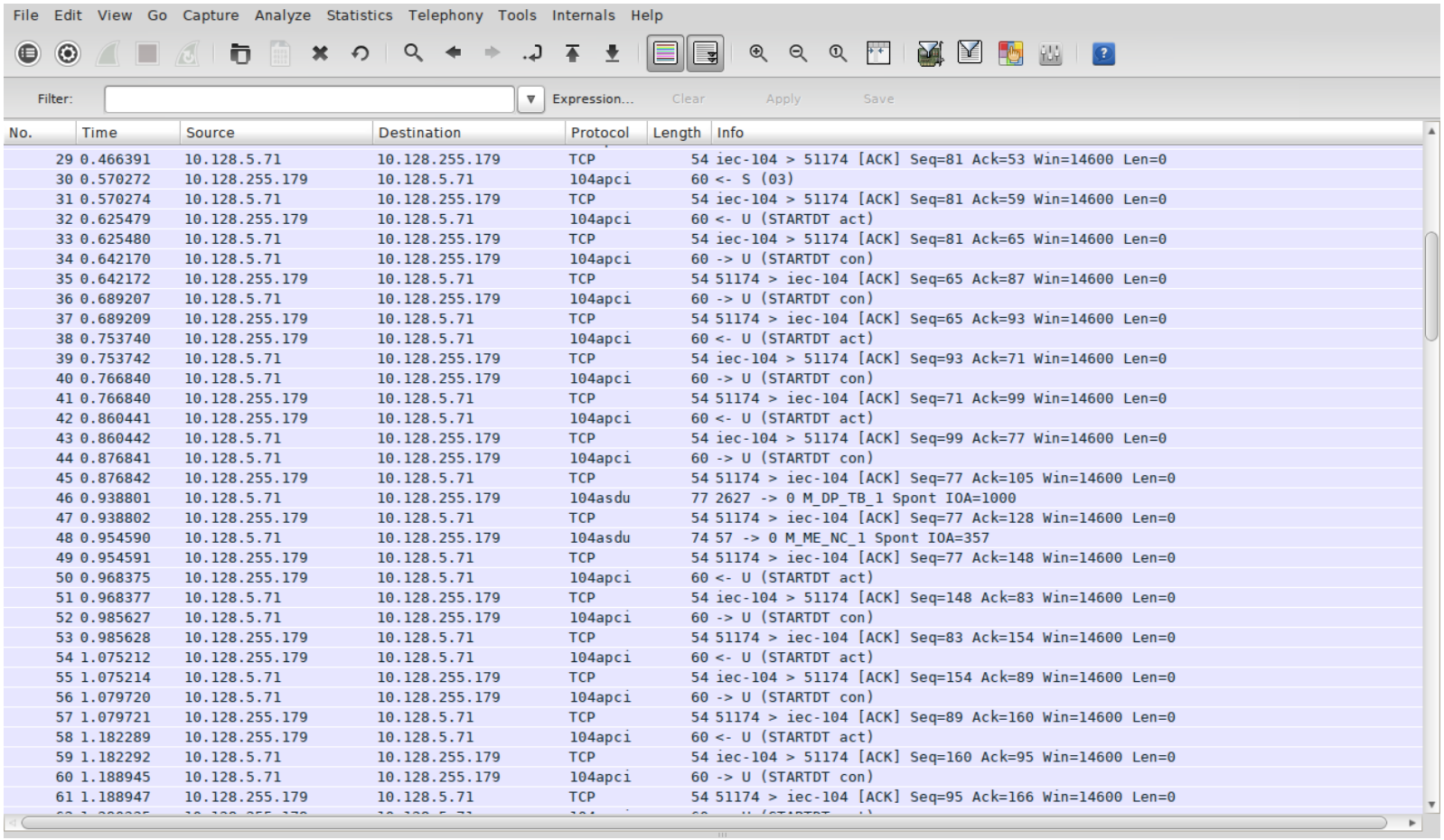
```
0000  00 1b 21 22 9e 09 3c 97  0e be c1 a8 08 00 45 00   ..!"..<. ......E.
0010  00 f3 fa 35 40 00 40 06  96 2d c0 a8 05 67 50 4a   ...5@.@. .-...gPJ
0020  93 48 c9 b4 01 bb 07 4f  82 4f 22 83 48 e7 80 18   .H.....O .O".H...
0030  00 e5 aa 87 00 00 01 01  08 0a 00 47 78 84 e4 98   ........ ...Gx...
0040  b7 bc 16 03 01 00 ba 01  00 00 b6 03 03 b1 02 a9   ........ ........
0050  1d e2 2b 50 5b 09 49 35  98 81 f0 b3 2e a2 e9 5b   ..+P[.I5 .......[
0060  8b 12 86 1f b5 b9 4e 1a  7a 67 33 66 a9 00 00 2e   ......N. zg3f....
0070  c0 2b c0 2f c0 0a c0 09  c0 13 c0 14 c0 12 c0 07   .+./.... ........
0080  c0 11 00 33 00 32 00 45  00 39 00 38 00 88 00 16   ...3.2.E .9.8....
0090  00 2f 00 41 00 35 00 84  00 0a 00 05 00 04 01 00   ./.A.5.. ........
00a0  00 5f 00 00 00 1d 00 1b  00 00 18 77 77 77 2e 6f   ._...... ...www.o
00b0  62 6a 65 63 74 69 66 2d  73 65 63 75 72 69 74 65   bjectif- securite
00c0  2e 63 68 ff 01 00 01 00  00 0a 00 08 00 06 00 17   .ch..... ........
00d0  00 18 00 19 00 0b 00 02  01 00 00 23 00 00 33 74   ........ ...#..3t
00e0  00 00 00 05 00 05 01 00  00 00 00 00 0d 00 12 00   ........ ........
00f0  10 04 01 05 01 02 01 04  03 05 03 02 03 04 02 02   ........ ........
0100  02                                                .
```



HTTP(s): Transmission

```
GET /wiki/Hypertext_Transfer_Protocol HTTP/1.1
Host: en.wikipedia.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:27.0)
Gecko/20100101 Firefox/27.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

TCP: Interception



No.	Time	Source	Destination	Protocol	Length	Info
29	0.466391	10.128.5.71	10.128.255.179	TCP	54	iec-104 > 51174 [ACK] Seq=81 Ack=53 Win=14600 Len=0
30	0.570272	10.128.255.179	10.128.5.71	104apci	60	<- S (03)
31	0.570274	10.128.5.71	10.128.255.179	TCP	54	iec-104 > 51174 [ACK] Seq=81 Ack=59 Win=14600 Len=0
32	0.625479	10.128.255.179	10.128.5.71	104apci	60	<- U (STARTDT act)
33	0.625480	10.128.5.71	10.128.255.179	TCP	54	iec-104 > 51174 [ACK] Seq=81 Ack=65 Win=14600 Len=0
34	0.642170	10.128.5.71	10.128.255.179	104apci	60	-> U (STARTDT con)
35	0.642172	10.128.255.179	10.128.5.71	TCP	54	51174 > iec-104 [ACK] Seq=65 Ack=87 Win=14600 Len=0
36	0.689207	10.128.5.71	10.128.255.179	104apci	60	-> U (STARTDT con)
37	0.689209	10.128.255.179	10.128.5.71	TCP	54	51174 > iec-104 [ACK] Seq=65 Ack=93 Win=14600 Len=0
38	0.753740	10.128.255.179	10.128.5.71	104apci	60	<- U (STARTDT act)
39	0.753742	10.128.5.71	10.128.255.179	TCP	54	iec-104 > 51174 [ACK] Seq=93 Ack=71 Win=14600 Len=0
40	0.766840	10.128.5.71	10.128.255.179	104apci	60	-> U (STARTDT con)
41	0.766840	10.128.255.179	10.128.5.71	TCP	54	51174 > iec-104 [ACK] Seq=71 Ack=99 Win=14600 Len=0
42	0.860441	10.128.255.179	10.128.5.71	104apci	60	<- U (STARTDT act)
43	0.860442	10.128.5.71	10.128.255.179	TCP	54	iec-104 > 51174 [ACK] Seq=99 Ack=77 Win=14600 Len=0
44	0.876841	10.128.5.71	10.128.255.179	104apci	60	-> U (STARTDT con)
45	0.876842	10.128.255.179	10.128.5.71	TCP	54	51174 > iec-104 [ACK] Seq=77 Ack=105 Win=14600 Len=0
46	0.938801	10.128.5.71	10.128.255.179	104asdu	77	2627 -> 0 M_DP_TB_1 Spont IOA=1000
47	0.938802	10.128.255.179	10.128.5.71	TCP	54	51174 > iec-104 [ACK] Seq=77 Ack=128 Win=14600 Len=0
48	0.954590	10.128.5.71	10.128.255.179	104asdu	74	57 -> 0 M_ME_NC_1 Spont IOA=357
49	0.954591	10.128.255.179	10.128.5.71	TCP	54	51174 > iec-104 [ACK] Seq=77 Ack=148 Win=14600 Len=0
50	0.968375	10.128.255.179	10.128.5.71	104apci	60	<- U (STARTDT act)
51	0.968377	10.128.5.71	10.128.255.179	TCP	54	iec-104 > 51174 [ACK] Seq=148 Ack=83 Win=14600 Len=0
52	0.985627	10.128.5.71	10.128.255.179	104apci	60	-> U (STARTDT con)
53	0.985628	10.128.255.179	10.128.5.71	TCP	54	51174 > iec-104 [ACK] Seq=83 Ack=154 Win=14600 Len=0
54	1.075212	10.128.255.179	10.128.5.71	104apci	60	<- U (STARTDT act)
55	1.075214	10.128.5.71	10.128.255.179	TCP	54	iec-104 > 51174 [ACK] Seq=154 Ack=89 Win=14600 Len=0
56	1.079720	10.128.5.71	10.128.255.179	104apci	60	-> U (STARTDT con)
57	1.079721	10.128.255.179	10.128.5.71	TCP	54	51174 > iec-104 [ACK] Seq=89 Ack=160 Win=14600 Len=0
58	1.182289	10.128.255.179	10.128.5.71	104apci	60	<- U (STARTDT act)
59	1.182292	10.128.5.71	10.128.255.179	TCP	54	iec-104 > 51174 [ACK] Seq=160 Ack=95 Win=14600 Len=0
60	1.188945	10.128.5.71	10.128.255.179	104apci	60	-> U (STARTDT con)
61	1.188947	10.128.255.179	10.128.5.71	TCP	54	51174 > iec-104 [ACK] Seq=95 Ack=166 Win=14600 Len=0

TCP: Modification

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 3c 7c bd 40 00 40 06  a4 04 0a 80 05 47 0a 80   .<|.@.@. .....G..
0020  ff b3 09 64 c7 e6 32 83  d5 5a 6b 93 f6 c8 50 18   ...d..2. .Zk...P.
0030  39 08 00 00 00 00 68 12  08 00 02 00 0d 01 03 00   9.....h. ........
0040  39 00 65 01 00 66 66 9e  42 00                     9.e..ff. B.
```

```
IEC 60870-5-104-Apci
   START
   ApduLen: 18
   .... ..00 = Type: I (0x00)
   Tx: 4
   Rx: 1
IEC 60870-5-104-Asdu
   TypeId: M_ME_NC_1 (13)
   .000 0001 = NumIx: 1
   ..00 0011 = CauseTx: Spont (3)
   .0.. .... = Negative: False
   0... .... = Test: False
   OA: 0
   Addr: 57
   IOA: 357
```

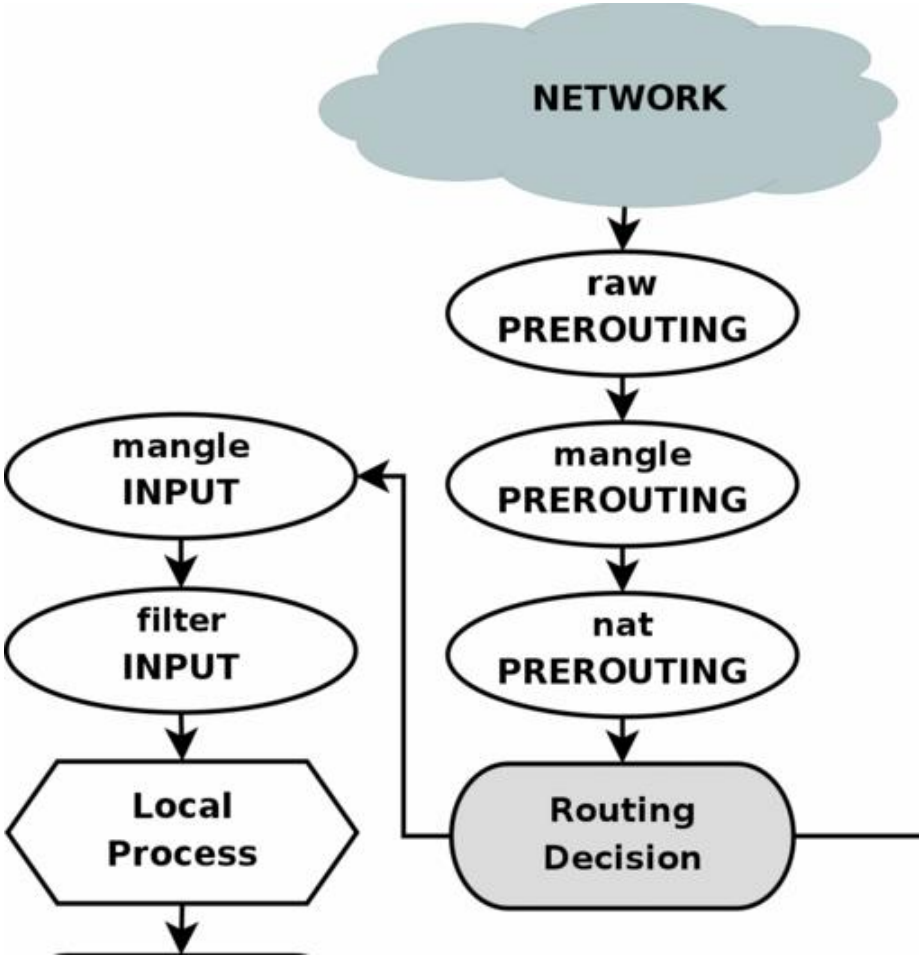
TCP: Transmission

- En général
  - La destination ne figure pas dans les données
  - Deux alternatives: proxy SOCKS ou redirection
- Information à disposition

```
Internet Protocol Version 4, Src: 10.128.5.71 (10.128.5.71), Dst: 10.128.255.179 (10.128.255.179)
Transmission Control Protocol, Src Port: iec-104 (2404), Dst Port: 51174 (51174), Seq: 128, Ack: 77, Len: 20
```

- Redirection classique
  - Approche la moins invasive
  - L’adresse et le port de destination sont perdus

TProxy: trafic externe

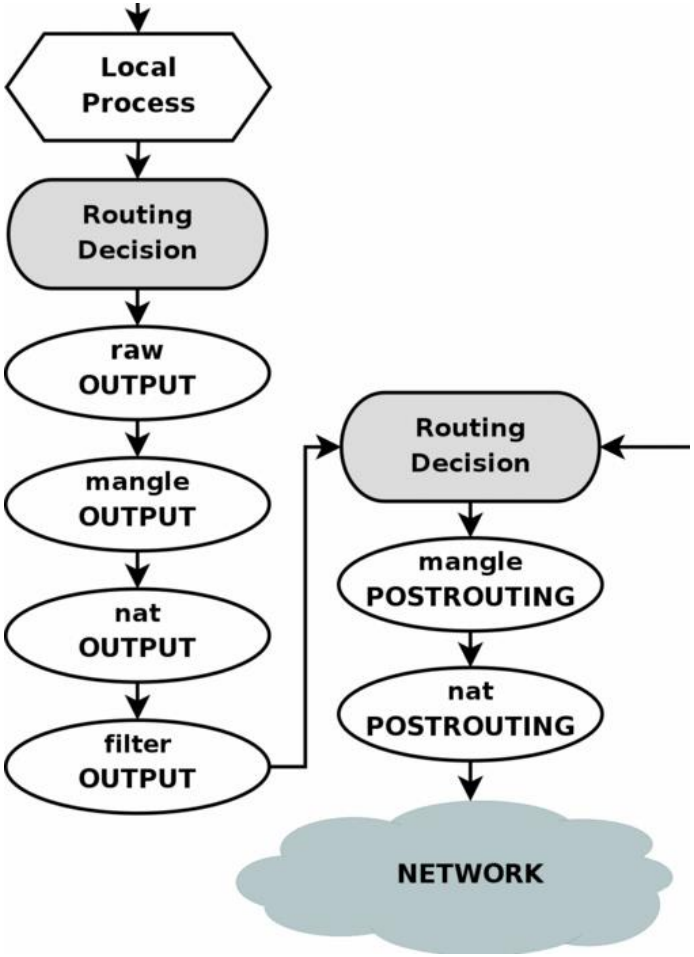



```
iptables
  -t mangle
  -A PREROUTING
  -p tcp --dport 80
  -j TPROXY
  --tproxy-mark 0x1/0x1
  --on-port 9080
```

```
ip rule add
   fwmark 1 lookup 100
```

```
ip route add local
   default dev lo table 100
```

TProxy: trafic interne




```
iptables
  -t mangle
  -A OUTPUT
  -p tcp --dport 80
  -m tos ! --tos 0x20
  -j MARK --set-mark 1

iptables
  -t mangle
  -A PREROUTING
  -p tcp -d 127.0.0.1
  -m tos --tos 0x20
  -j ACCEPT
```

Différence: Redirect & TProxy

- Client se connecte à en.wikipedia.org

  IP 91.198.174.192 et port 80

- Avec REDIRECT –to-port 9080, le proxy voit:

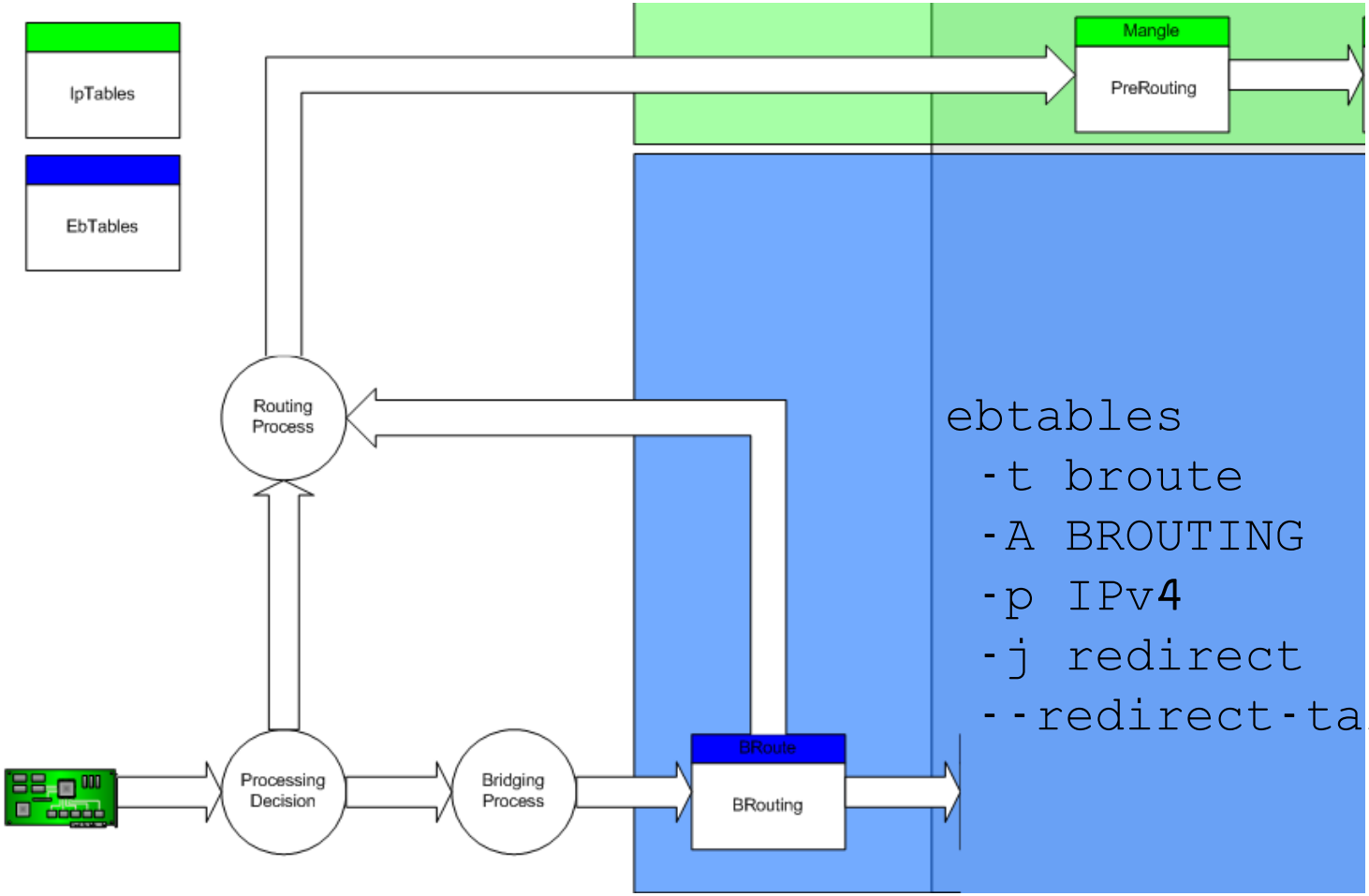
  IP 127.0.0.1 et port 9080

- Avec TPROXY –on-port 9080, le proxy voit:

  IP 91.198.174.192 et port 80

- TPROXY conserve la destination originale

Bridging → Routing




```
ebtables
  -t broute
  -A BROUTING
  -p IPv4
  -j redirect
  --redirect-target DROP
```

Notre approche

- Interception transparente du trafic
  - Option IP_TRANSPARENT sur un socket Linux
- Capacité de traiter un trafic soutenu
  - Connexions traitées en *//* par plusieurs processus
- Activation dynamique de SSL/TLS (STARTTLS)
  - Détection automatique des SSL/TLS client_hello
- Capacité de traiter n'importe quel protocole
  - Dissecteurs Wireshark pour segmenter et interpréter les données

Implémentation

- Principalement implémenté en Scala
  - Bibliothèque standard
  - Processus distribués implémentés avec Akka
- Gestion des trames TCP et dissection en C
  - Avec l'aide des dissecteurs Wireshark
- SSL/TLS via le SSLEngine du JDK Java
  - Implémentation standard des protocoles
  - Suffisamment versatile