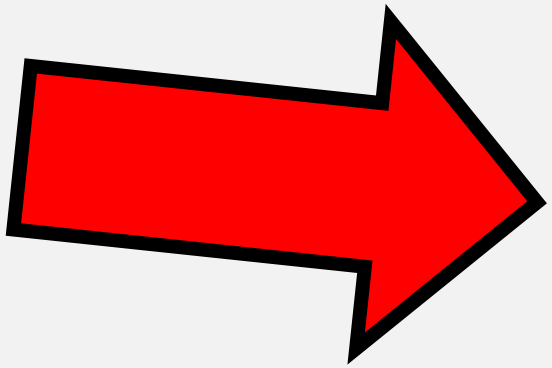
RECUPERER LE MOT DE PASSE facebook DE SA COPINE



check1.pcapng [Wireshark 1.99.3 (v1.99.3-0-g4f2c827 from master)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

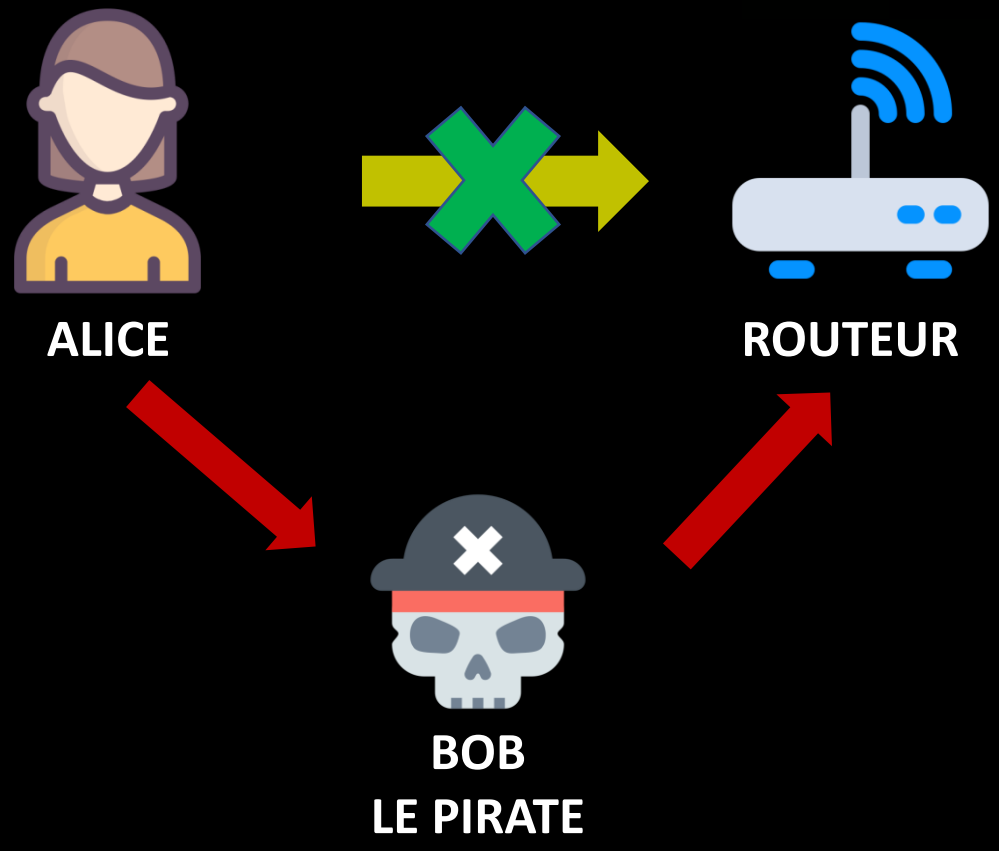
No.	Time	Source	Destination	Protocol	Length	Info
6	3.285368	54.230.130.212	10.0.2.15	TCP	60	80→49618 [SYN, ACK] Seq=0 Ack=1 Win=6
7	3.285420	10.0.2.15	54.230.130.212	TCP	54	49618→80 [ACK] Seq=1 Ack=1 Win=64240
8	3.285737	10.0.2.15	54.230.130.212	HTTP	148	GET /static/02aa/prefs.json HTTP/1.1
9	3.285852	54.230.130.212	10.0.2.15	TCP	60	80→49618 [ACK] Seq=1 Ack=95 Win=65535
10	3.311613	54.230.130.212	10.0.2.15	HTTP	729	HTTP/1.1 200 OK (application/javascr
11	3.504371	10.0.2.15	54.230.130.212	HTTP	140	GET /static/02aa/functions.js?cb=1705
12	3.504543	54.230.130.212	10.0.2.15	TCP	60	80→49618 [ACK] Seq=676 Ack=181 Win=65
13	3.531112	54.230.130.212	10.0.2.15	TCP	1474	[TCP segment of a reassembled PDU]
14	3.531116	54.230.130.212	10.0.2.15	TCP	94	[TCP segment of a reassembled PDU]
15	3.531160	10.0.2.15	54.230.130.212	TCP	54	49618→80 [ACK] Seq=181 Ack=2136 Win=6
16	3.531918	54.230.130.212	10.0.2.15	HTTP	1205	HTTP/1.1 200 OK (application/javascr

```
0050  6e 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   n HTTP/1 .1..Host
0060  3a 20 64 2e 79 6f 75 67  6f 74 75 6e 66 72 69 65   : d.youg otunfrie
0070  6e 64 65 64 2e 63 6f 6d  0d 0a 43 6f 6e 6e 65 63   nded.com ..Connec
0080  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0090  0d 0a 0d 0a                                       ....
```

File: "C:\Users\... Packets: 147 · Displayed: 147 (10... Profile: Default

L'ATTAQUE DU MILLIEU

METHODE



OSI MODELE	COUCHE	ATTTAQUE MITM
	APPLICATION	BGP, DHCP SPOOFING, DNS SPOOFING
	PRESENTATION	SSL/TLS
	TRANSPORT	IP SPOOFING
	RESEAU	
	LIAISON	ARP SPOOFING
GSM NETWORK	GSM	Fausse station (FBS)
	UTMS	

Spoofing = Usurpation identité

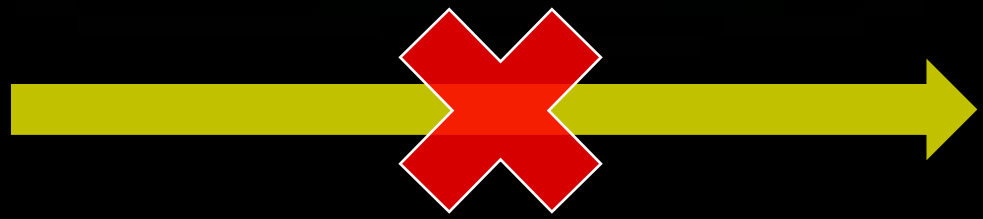
BGP = Protocol échange de route externe

ARP SPOOFING

ALICE

IP : 10.0.0.1

Mac : AA:AA:AA:AA:AA:AA



ROUTEUR

IP : 10.0.0.3

Mac : BB:BB:BB:BB:BB:BB

BOB

IP : 10.0.0.2

Mac : EE:EE:EE:EE:EE:EE

ANALYSE

Applications Emplacements Wireshark dim. 21 oct. 23:26:14 100 %

*wlan0

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

http Expression...

No.	Time	Source	Destination	Protocol	Length	Info
13	16.786499832	192.168.1.74	192.168.1.53	HTTP	446	GET / HTTP/1.1
16	16.786825161	192.168.1.53	192.168.1.74	HTTP	1514	HTTP/1.0 200 OK
22	16.790116005	192.168.1.53	192.168.1.74	HTTP	1514	Continuation
23	16.790118501	192.168.1.53	192.168.1.74	HTTP	1514	Continuation
390	17.273794847	192.168.1.53	192.168.1.74	HTTP	1514	Continuation
600	17.353434392	192.168.1.53	192.168.1.74	HTTP	1514	Continuation
604	17.355436448	192.168.1.53	192.168.1.74	HTTP	1514	Continuation
605	17.355438120	192.168.1.53	192.168.1.74	HTTP	1514	Continuation
739	26.199399095	192.168.1.74	192.168.1.53	HTTP	1035	POST /ajax/bz HTTP/1.1 (application/x-www-form-urlencoded)
754	28.150374148	192.168.1.74	192.168.1.53	HTTP	407	POST /cookie/consent/?dpr=2 HTTP/1.1 (application/x-www-form-urlencoded)
763	28.154032765	192.168.1.74	192.168.1.53	HTTP	536	POST /ajax/bz HTTP/1.1 (application/x-www-form-urlencoded)
791	43.094614179	192.168.1.74	192.168.1.53	HTTP	234	POST /ajax/bz HTTP/1.1 (application/x-www-form-urlencoded)
808	49.137170320	192.168.1.74	192.168.1.53	HTTP	598	POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1 (application/x-www-form-urlen…

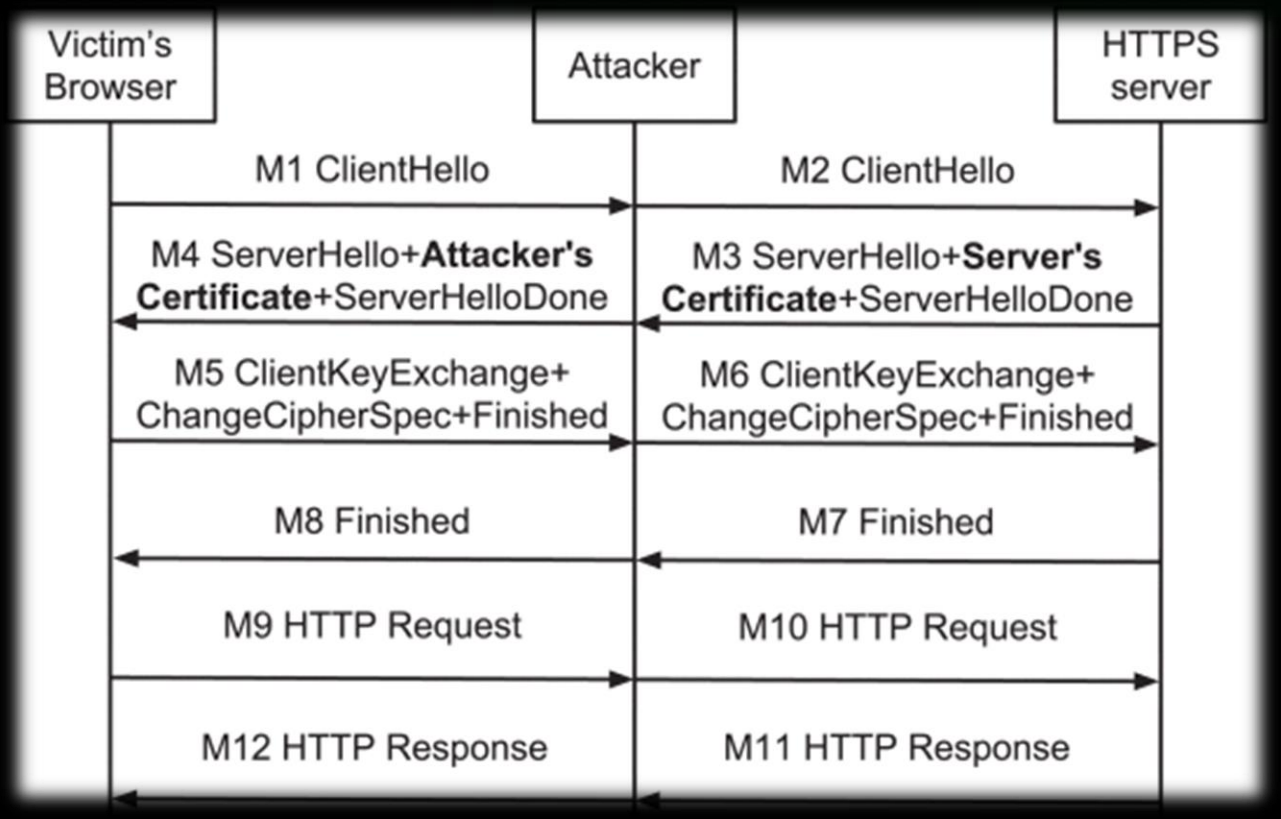
```
▸ Frame 16: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▸ Ethernet II, Src: IntelCor_b0:d4:11 (34:e1:2d:b0:d4:11), Dst: Apple_67:52:4c (c4:61:8b:67:52:4c)
▸ Internet Protocol Version 4, Src: 192.168.1.53, Dst: 192.168.1.74
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 59409, Seq: 18, Ack: 381, Len: 1448
▸ [2 Reassembled TCP Segments (1465 bytes): #15(17), #16(1448)]
▸ Hypertext Transfer Protocol
0000  c4 61 8b 67 52 4c 34 e1  2d b0 d4 11 08 00 45 00   ·a·gRL4· -·····E·
0010  05 dc ba bb 40 00 40 06  f6 90 c0 a8 01 35 c0 a8   ····@·@· ·····5··
0020  01 4a 00 50 e8 11 9d 0f  93 f0 1e d7 b1 81 80 10   ·J·P···· ········
```

Frame (1514 bytes) | Reassembled TCP (1465 bytes)

Hypertext Transfer Protocol: Protocol

```
▸ Form item: "profile_selector_ids" = ""
▸ Form item: "return_session" = ""
▸ Form item: "skip_api_login" = ""
▸ Form item: "signed_next" = ""
▸ Form item: "trynum" = "1"
▸ Form item: "timezone" = "-135"
▸ Form item: "lgndim" = "eyJ3IjozMjAsImgiOjU2OCwiYXciOjMyMCwiYWgiOjU2OCwiYyI6MzJ9"
▸ Form item: "lgnrnd" = "141019_R-Sv"
▸ Form item: "lgnjs" = "1540157139"
▸ Form item: "email" = "no_s1gnal@youtube.com"
▸ Form item: "pass" = "abonnezvous!"
▸ Form item: "prefill_contact_point" = ""
0000  34 e1 2d b0 d4 11 c4 61  8b 67 52 4c 08 00 45 00   4·-····a ·gRL··E·
0010  02 48 00 00 40 00 40 06  b4 e0 c0 a8 01 4a c0 a8   ·H··@·@· ·····J··
0020  01 35 e8 1d 00 50 70 fb  a7 9b ca e5 89 67 80 18   ·5···Pp· ·····g··
0030  04 05 3b fc 00 00 01 01  08 0a 41 59 d3 a0 da e0   ··;····· ··AY····
0040  42 bb 6c 73 64 3d 41 56  72 6b 58 46 4a 73 26 64   B·lsd=AV rkXFJs&d
0050  69 73 70 6c 61 79 3d 26  65 6e 61 62 6c 65 5f 70   isplay=& enable_p
0060  72 6f 66 69 6c 65 5f 73  65 6c 65 63 74 6f 72 3d   rofile_s elector=
0070  26 69 73 70 72 69 76 61  74 65 3d 26 6c 65 67 61   &ispriva te=&lega
0080  63 79 5f 72 65 74 75 72  6e 3d 30 26 70 72 6f 66   cy_retur n=0&prof
```

STRIPING SSL/TLS



HTTPS : version sécurisée du langage informatique HTTP se servant d'une couche de SSL/TLS

SSL/TLS : Protocole de sécurité servant à :

- Chiffrer les données
- Authentifier les serveurs
- Assuré l'intégrité des paquets

CONCLUSION

M’EFIEZ VOUS DES APPARANCES