Reading configuration file '/etc/wpa\_supplicant-2.10/wpa\_supplicant/wpa\_supplicantm.conf'

ctrl\_interface='/var/run/wpa\_supplicant'

update\_config=1

Line: 4 - start of a new network block

ssid - hexdump\_ascii(len=16):

41 69 72 74 65 6c 5f 63 68 65 6e 5f 39 33 36 39 Airtel\_chen\_9369

key\_mgmt: 0x1

eap methods - hexdump(len=16): 00 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00

identity - hexdump\_ascii(len=5):

73 74 65 76 65 steve

password - hexdump\_ascii(len=7):

74 65 73 74 69 6e 67 testing

phase2 - hexdump\_ascii(len=13):

61 75 74 68 3d 4d 53 43 48 41 50 56 32 auth=MSCHAPV2

Priority group 0

id=0 ssid='Airtel\_chen\_9369'

Authentication server 127.0.0.1:1812

RADIUS local address: 127.0.0.1:55128

ENGINE: Loading builtin engines

ENGINE: Loading builtin engines

EAPOL: SUPP\_PAE entering state DISCONNECTED

EAPOL: KEY\_RX entering state NO\_KEY\_RECEIVE

EAPOL: SUPP\_BE entering state INITIALIZE

EAP: EAP entering state DISABLED

EAPOL: External notification - portValid=0

EAPOL: External notification - portEnabled=1

EAPOL: SUPP\_PAE entering state CONNECTING

EAPOL: SUPP\_BE entering state IDLE

EAP: EAP entering state INITIALIZE

EAP: EAP entering state IDLE

Sending fake EAP-Request-Identity

EAPOL: Received EAP-Packet frame

EAPOL: SUPP\_PAE entering state RESTART

EAP: EAP entering state INITIALIZE

EAP: EAP entering state IDLE

EAPOL: SUPP\_PAE entering state AUTHENTICATING

EAPOL: SUPP\_BE entering state REQUEST

EAPOL: getSuppRsp

EAP: EAP entering state RECEIVED

EAP: Received EAP-Request id=95 method=1 vendor=0 vendorMethod=0

EAP: EAP entering state IDENTITY

CTRL-EVENT-EAP-STARTED EAP authentication started

EAP: Status notification: started (param=)

EAP: EAP-Request Identity data - hexdump\_ascii(len=0):

EAP: using real identity - hexdump\_ascii(len=5):

73 74 65 76 65 steve

EAP: EAP entering state SEND\_RESPONSE

EAP: EAP entering state IDLE

EAPOL: SUPP\_BE entering state RESPONSE

EAPOL: txSuppRsp

WPA: eapol\_test\_eapol\_send(type=0 len=10)

TX EAP -> RADIUS - hexdump(len=10): 02 5f 00 0a 01 73 74 65 76 65

Encapsulating EAP message into a RADIUS packet

Learned identity from EAP-Response-Identity - hexdump(len=5): 73 74 65 76 65

Sending RADIUS message to authentication server

RADIUS message: code=1 (Access-Request) identifier=0 length=127

Attribute 1 (User-Name) length=7

Value: 'steve'

Attribute 4 (NAS-IP-Address) length=6

Value: 127.0.0.1

Attribute 31 (Calling-Station-Id) length=19

Value: '02-00-00-00-00-01'

Attribute 12 (Framed-MTU) length=6

Value: 1400

Attribute 61 (NAS-Port-Type) length=6

Value: 19

Attribute 6 (Service-Type) length=6

Value: 2

Attribute 77 (Connect-Info) length=24

Value: 'CONNECT 11Mbps 802.11b'

Attribute 30 (Called-Station-Id) length=3

Value: '\x00'

Attribute 79 (EAP-Message) length=12

Value: 025f000a017374657665

Attribute 80 (Message-Authenticator) length=18

Value: d32e5ce5653918e8dc9de814b1576451

Next RADIUS client retransmit in 3 seconds

EAPOL: SUPP\_BE entering state RECEIVE

Received 80 bytes from RADIUS server

Received RADIUS message

RADIUS message: code=11 (Access-Challenge) identifier=0 length=80

Attribute 79 (EAP-Message) length=24

Value: 0160001604108ca8c780e913ead1400d2518daf113f5

Attribute 80 (Message-Authenticator) length=18

Value: 804101ce4e123744d9de16b01d477152

Attribute 24 (State) length=18

Value: 7583638c75e3670a9a7e5f1775f4795f

STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.00 sec

RADIUS packet matching with station

decapsulated EAP packet (code=1 id=96 len=22) from RADIUS server: EAP-Request-MD5 (4)

EAPOL: Received EAP-Packet frame

EAPOL: SUPP\_BE entering state REQUEST

EAPOL: getSuppRsp

EAP: EAP entering state RECEIVED

EAP: Received EAP-Request id=96 method=4 vendor=0 vendorMethod=0

EAP: EAP entering state GET\_METHOD

EAP: configuration does not allow: vendor 0 method 4

EAP: vendor 0 method 4 not allowed

CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=4 -> NAK

EAP: Status notification: refuse proposed method (param=MD5)

EAP: Building EAP-Nak (requested type 4 vendor=0 method=0 not allowed)

EAP: allowed methods - hexdump(len=1): 19

EAP: EAP entering state SEND\_RESPONSE

EAP: EAP entering state IDLE

EAPOL: SUPP\_BE entering state RESPONSE

EAPOL: txSuppRsp

WPA: eapol\_test\_eapol\_send(type=0 len=6)

TX EAP -> RADIUS - hexdump(len=6): 02 60 00 06 03 19

Encapsulating EAP message into a RADIUS packet

Copied RADIUS State Attribute

Sending RADIUS message to authentication server

RADIUS message: code=1 (Access-Request) identifier=1 length=141

Attribute 1 (User-Name) length=7

Value: 'steve'

Attribute 4 (NAS-IP-Address) length=6

Value: 127.0.0.1

Attribute 31 (Calling-Station-Id) length=19

Value: '02-00-00-00-00-01'

Attribute 12 (Framed-MTU) length=6

Value: 1400

Attribute 61 (NAS-Port-Type) length=6

Value: 19

Attribute 6 (Service-Type) length=6

Value: 2

Attribute 77 (Connect-Info) length=24

Value: 'CONNECT 11Mbps 802.11b'

Attribute 30 (Called-Station-Id) length=3

Value: '\x00'

Attribute 79 (EAP-Message) length=8

Value: 026000060319

Attribute 24 (State) length=18

Value: 7583638c75e3670a9a7e5f1775f4795f

Attribute 80 (Message-Authenticator) length=18

Value: a078d3657ae6ddbc3441219020848de3

Next RADIUS client retransmit in 3 seconds

EAPOL: SUPP\_BE entering state RECEIVE

Received 64 bytes from RADIUS server

Received RADIUS message

RADIUS message: code=11 (Access-Challenge) identifier=1 length=64

Attribute 79 (EAP-Message) length=8

Value: 016100061920

Attribute 80 (Message-Authenticator) length=18

Value: 078ce49aa5fa4ea1ed28f1d76bf26340

Attribute 24 (State) length=18

Value: 7583638c74e27a0a9a7e5f1775f4795f

STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.00 sec

RADIUS packet matching with station

decapsulated EAP packet (code=1 id=97 len=6) from RADIUS server: EAP-Request-PEAP (25)

EAPOL: Received EAP-Packet frame

EAPOL: SUPP\_BE entering state REQUEST

EAPOL: getSuppRsp

EAP: EAP entering state RECEIVED

EAP: Received EAP-Request id=97 method=25 vendor=0 vendorMethod=0

EAP: EAP entering state GET\_METHOD

CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25

EAP: Status notification: accept proposed method (param=PEAP)

EAP: Initialize selected EAP method: vendor 0 method 25 (PEAP)

TLS: Phase2 EAP types - hexdump(len=8): 00 00 00 00 1a 00 00 00

TLS: using phase1 config options

CTRL-EVENT-EAP-METHOD EAP vendor 0 method 25 (PEAP) selected

EAP: EAP entering state METHOD

SSL: Received packet(len=6) - Flags 0x20

EAP-PEAP: Start (server ver=0, own ver=1)

EAP-PEAP: Using PEAP version 0

SSL: (where=0x10 ret=0x1)

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:before SSL initialization

OpenSSL: TX ver=0x301 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 16 03 01 00 b3

OpenSSL: TX ver=0x303 content\_type=22 (handshake/client hello)

OpenSSL: Message - hexdump(len=179): 01 00 00 af 03 03 df 5d 1a a7 ba a5 f8 70 59 3f 23 ca e2 63 c3 5c 44 62 e6 3b 01 ac a4 e9 a9 9c 79 aa a3 68 9d ae 00 00 38 c0 2c c0 30 00 9f cc a9 cc a8 cc aa c0 2b c0 2f 00 9e c0 24 c0 28 00 6b c0 23 c0 27 00 67 c0 0a c0 14 00 39 c0 09 c0 13 00 33 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 ff 01 00 00 4e 00 0b 00 04 03 00 01 02 00 0a 00 0c 00 0a 00 1d 00 17 00 1e 00 19 00 18 00 16 00 00 00 17 00 00 00 0d 00 2a 00 28 04 03 05 03 06 03 08 07 08 08 08 09 08 0a 08 0b 08 04 08 05 08 06 04 01 05 01 06 01 03 03 03 01 03 02 04 02 05 02 06 02

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS write client hello

SSL: (where=0x1002 ret=0xffffffff)

SSL: SSL\_connect:error in SSLv3/TLS write client hello

SSL: SSL\_connect - want more data

SSL: 184 bytes pending from ssl\_out

SSL: Using TLS version TLSv1.2

SSL: 184 bytes left to be sent out (of total 184 bytes)

EAP: method process -> ignore=FALSE methodState=MAY\_CONT decision=FAIL eapRespData=0x7fffd0772d40

EAP: EAP entering state SEND\_RESPONSE

EAP: EAP entering state IDLE

EAPOL: SUPP\_BE entering state RESPONSE

EAPOL: txSuppRsp

WPA: eapol\_test\_eapol\_send(type=0 len=194)

TX EAP -> RADIUS - hexdump(len=194): 02 61 00 c2 19 80 00 00 00 b8 16 03 01 00 b3 01 00 00 af 03 03 df 5d 1a a7 ba a5 f8 70 59 3f 23 ca e2 63 c3 5c 44 62 e6 3b 01 ac a4 e9 a9 9c 79 aa a3 68 9d ae 00 00 38 c0 2c c0 30 00 9f cc a9 cc a8 cc aa c0 2b c0 2f 00 9e c0 24 c0 28 00 6b c0 23 c0 27 00 67 c0 0a c0 14 00 39 c0 09 c0 13 00 33 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 ff 01 00 00 4e 00 0b 00 04 03 00 01 02 00 0a 00 0c 00 0a 00 1d 00 17 00 1e 00 19 00 18 00 16 00 00 00 17 00 00 00 0d 00 2a 00 28 04 03 05 03 06 03 08 07 08 08 08 09 08 0a 08 0b 08 04 08 05 08 06 04 01 05 01 06 01 03 03 03 01 03 02 04 02 05 02 06 02

Encapsulating EAP message into a RADIUS packet

Copied RADIUS State Attribute

Sending RADIUS message to authentication server

RADIUS message: code=1 (Access-Request) identifier=2 length=329

Attribute 1 (User-Name) length=7

Value: 'steve'

Attribute 4 (NAS-IP-Address) length=6

Value: 127.0.0.1

Attribute 31 (Calling-Station-Id) length=19

Value: '02-00-00-00-00-01'

Attribute 12 (Framed-MTU) length=6

Value: 1400

Attribute 61 (NAS-Port-Type) length=6

Value: 19

Attribute 6 (Service-Type) length=6

Value: 2

Attribute 77 (Connect-Info) length=24

Value: 'CONNECT 11Mbps 802.11b'

Attribute 30 (Called-Station-Id) length=3

Value: '\x00'

Attribute 79 (EAP-Message) length=196

Value: 026100c21980000000b816030100b3010000af0303df5d1aa7baa5f870593f23cae263c35c4462e63b01aca4e9a99c79aaa3689dae000038c02cc030009fcca9cca8ccaac02bc02f009ec024c028006bc023c0270067c00ac0140039c009c0130033009d009c003d003c0035002f00ff0100004e000b000403000102000a000c000a001d0017001e001900180016000000170000000d002a0028040305030603080708080809080a080b080408050806040105010601030303010302040205020602

Attribute 24 (State) length=18

Value: 7583638c74e27a0a9a7e5f1775f4795f

Attribute 80 (Message-Authenticator) length=18

Value: 66c7be38518c091ff09e2c6b57ba7bfd

Next RADIUS client retransmit in 3 seconds

EAPOL: SUPP\_BE entering state RECEIVE

Received 1068 bytes from RADIUS server

Received RADIUS message

RADIUS message: code=11 (Access-Challenge) identifier=2 length=1068

Attribute 79 (EAP-Message) length=255

Value: 

Attribute 79 (EAP-Message) length=255

Value: 

Attribute 79 (EAP-Message) length=255

Value: 

Attribute 79 (EAP-Message) length=247

Value: 15a854ce64ce3e3265bfd968f8dc489f74a7e8a8b0b153c7c5f58be13d4254560f42e6177a1a878388f68caca244f077b4d3e8b99ce199167777ac82aee725e362d6ea52fc0011d34dd4739fcd71d71a32f8d8dafa70326d76d6cec3098ddd019406d4bc73bef17484e4a90cc2ae2976e9cf68ab94160303012c0c00012803001d20cf59e402b69be5b4f93a53b123684f30383e6a2410e0a8b9eaf65a9a3d4c3708080401006b2686834e191067f0024c471ada8158a9c3b509cabb46028021ace011494c530b9c68fc60451899650310afc89de655b5ea0a2440983d53fa076a93da3ffacbf2df09054864a9b85ee280b652f666

Attribute 80 (Message-Authenticator) length=18

Value: 454dfd626f218fbfade2c32e74292b57

Attribute 24 (State) length=18

Value: 7583638c77e17a0a9a7e5f1775f4795f

STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.00 sec

RADIUS packet matching with station

decapsulated EAP packet (code=1 id=98 len=1004) from RADIUS server: EAP-Request-PEAP (25)

EAPOL: Received EAP-Packet frame

EAPOL: SUPP\_BE entering state REQUEST

EAPOL: getSuppRsp

EAP: EAP entering state RECEIVED

EAP: Received EAP-Request id=98 method=25 vendor=0 vendorMethod=0

EAP: EAP entering state METHOD

SSL: Received packet(len=1004) - Flags 0xc0

SSL: TLS Message Length: 1180

SSL: Need 186 bytes more input data

SSL: Building ACK (type=25 id=98 ver=0)

EAP: method process -> ignore=FALSE methodState=MAY\_CONT decision=FAIL eapRespData=0x7fffd0760140

EAP: EAP entering state SEND\_RESPONSE

EAP: EAP entering state IDLE

EAPOL: SUPP\_BE entering state RESPONSE

EAPOL: txSuppRsp

WPA: eapol\_test\_eapol\_send(type=0 len=6)

TX EAP -> RADIUS - hexdump(len=6): 02 62 00 06 19 00

Encapsulating EAP message into a RADIUS packet

Copied RADIUS State Attribute

Sending RADIUS message to authentication server

RADIUS message: code=1 (Access-Request) identifier=3 length=141

Attribute 1 (User-Name) length=7

Value: 'steve'

Attribute 4 (NAS-IP-Address) length=6

Value: 127.0.0.1

Attribute 31 (Calling-Station-Id) length=19

Value: '02-00-00-00-00-01'

Attribute 12 (Framed-MTU) length=6

Value: 1400

Attribute 61 (NAS-Port-Type) length=6

Value: 19

Attribute 6 (Service-Type) length=6

Value: 2

Attribute 77 (Connect-Info) length=24

Value: 'CONNECT 11Mbps 802.11b'

Attribute 30 (Called-Station-Id) length=3

Value: '\x00'

Attribute 79 (EAP-Message) length=8

Value: 026200061900

Attribute 24 (State) length=18

Value: 7583638c77e17a0a9a7e5f1775f4795f

Attribute 80 (Message-Authenticator) length=18

Value: 4f5c742e8af03232d24b66f761d1baef

Next RADIUS client retransmit in 3 seconds

EAPOL: SUPP\_BE entering state RECEIVE

Received 250 bytes from RADIUS server

Received RADIUS message

RADIUS message: code=11 (Access-Challenge) identifier=3 length=250

Attribute 79 (EAP-Message) length=194

Value: 016300c01900dd647852057b501078f3e1bc07e6137da655f81d645903da499eaaba4314134f913f748becb346df23ee66ccf792b55d487134f72aae146b58a0c7300283ab43e3d50e88f440b9cbd70a42e4ee454c4c5afb4311f997e6dc141607fc82ed331108d87f4437da71f2d85ee9b4ab1b8cb3f094f6377ccdba988296b7b4a28c87e1c7b98cce75fcfdc919d3fb9797c545ce86388ea16e3e3cedd57bdc668adc82f7dea022565e046f366955e227366b9dc9c216030300040e000000

Attribute 80 (Message-Authenticator) length=18

Value: 2488d9f831f0c98a5780a4a5d8070b65

Attribute 24 (State) length=18

Value: 7583638c76e07a0a9a7e5f1775f4795f

STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.00 sec

RADIUS packet matching with station

decapsulated EAP packet (code=1 id=99 len=192) from RADIUS server: EAP-Request-PEAP (25)

EAPOL: Received EAP-Packet frame

EAPOL: SUPP\_BE entering state REQUEST

EAPOL: getSuppRsp

EAP: EAP entering state RECEIVED

EAP: Received EAP-Request id=99 method=25 vendor=0 vendorMethod=0

EAP: EAP entering state METHOD

SSL: Received packet(len=192) - Flags 0x00

OpenSSL: RX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 16 03 03 00 3d

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS write client hello

OpenSSL: RX ver=0x303 content\_type=22 (handshake/server hello)

OpenSSL: Message - hexdump(len=61): 02 00 00 39 03 03 b4 27 e2 39 3b 9b 31 db ec 85 df 5f 03 13 f6 55 58 e0 26 dd 2f 1f 05 fa 39 70 14 80 b9 6f c4 d5 00 c0 30 00 00 11 ff 01 00 01 00 00 0b 00 04 03 00 01 02 00 17 00 00

OpenSSL: Server selected cipher suite 0xc030

OpenSSL: RX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 16 03 03 03 1b

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS read server hello

OpenSSL: RX ver=0x303 content\_type=22 (handshake/certificate)

OpenSSL: Message - hexdump(len=795): 0b 00 03 17 00 03 14 00 03 11 30 82 03 0d 30 82 01 f5 a0 03 02 01 02 02 14 3c c4 06 9a 6c 1b 8d ce d5 9b 65 69 86 0a d0 bd 00 05 1f 09 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 1b 31 19 30 17 06 03 55 04 03 0c 10 44 45 53 4b 54 4f 50 2d 42 47 52 56 44 4c 31 2e 30 1e 17 0d 32 34 30 33 31 34 30 37 31 35 30 30 5a 17 0d 33 34 30 33 31 32 30 37 31 35 30 30 5a 30 1b 31 19 30 17 06 03 55 04 03 0c 10 44 45 53 4b 54 4f 50 2d 42 47 52 56 44 4c 31 2e 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 b9 45 b6 df 13 27 d0 f6 5f d7 1b b4 dc 50 0b 55 83 09 ec c3 d8 b8 67 f9 59 25 07 a8 df c0 db 6c e9 f4 ec 5e b0 48 23 9c df 8f cc 8f 64 5a e7 11 94 11 76 73 68 5f 47 e0 3d 9c d0 a7 5b 7e 51 2f 45 62 3e 76 e2 c0 28 95 42 80 b4 5d 25 3f 27 b7 5a e2 46 10 47 ab 2d a9 99 25 5e db 84 a0 e6 a5 83 eb d0 3a c6 28 18 0a 1e 1c 8d b3 9d 72 a1 04 e6 a9 db 23 50 be 87 da 73 67 9d a8 03 e0 0f 60 bd a9 9a 7b 30 3b 66 6a ef b0 ca ef da c3 dc 47 dc f8 92 a3 c4 eb f2 33 5d eb 3d 91 80 49 94 2a 7b 30 d1 f1 4f cc 16 f4 14 ee a1 1c 7c 90 70 ab c2 50 c6 16 18 07 ac 05 5b 47 4d 66 15 cc e5 7b 50 62 11 56 b4 31 05 05 b6 df 7e be b2 7e f4 72 97 6e a1 9b aa 5a ea c1 3f 99 19 1a 7f 39 04 b5 74 84 e2 ff 9c b3 de a5 75 be 76 43 54 7a cf cc 85 89 11 7f 4f 37 83 8a 85 b9 74 5c 4f dc e8 0b 02 03 01 00 01 a3 49 30 47 30 09 06 03 55 1d 13 04 02 30 00 30 1b 06 03 55 1d 11 04 14 30 12 82 10 44 45 53 4b 54 4f 50 2d 42 47 52 56 44 4c 31 2e 30 1d 06 03 55 1d 0e 04 16 04 14 0c 1e 23 76 a7 00 38 35 5b 64 e9 a7 24 35 b0 bf 50 b7 ac d4 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 03 82 01 01 00 11 0a eb a3 5d a8 93 d1 74 b2 ae 02 3f e9 f7 76 49 ec 35 26 74 41 22 ff 2d 62 c3 20 e0 83 6c a5 3b e4 40 29 ae 40 77 04 dc 0f f9 dd db 25 95 5f 77 a9 6a ee f3 34 f5 8d 9b 00 92 99 d8 89 3b 8e 3a f4 74 46 9a 44 b8 7e 9e f8 68 55 c6 de 89 73 02 5f 12 e6 a6 c2 28 47 ed 07 0b 66 89 b6 54 07 55 f2 e3 fe 66 13 41 88 ef 4c bc b5 ba 06 ff 99 dc 6b 8b 53 a0 91 d6 01 50 f2 f3 25 83 b1 41 cb 1b a7 a7 4b c3 85 cc 35 af f0 6e 15 a8 54 ce 64 ce 3e 32 65 bf d9 68 f8 dc 48 9f 74 a7 e8 a8 b0 b1 53 c7 c5 f5 8b e1 3d 42 54 56 0f 42 e6 17 7a 1a 87 83 88 f6 8c ac a2 44 f0 77 b4 d3 e8 b9 9c e1 99 16 77 77 ac 82 ae e7 25 e3 62 d6 ea 52 fc 00 11 d3 4d d4 73 9f cd 71 d7 1a 32 f8 d8 da fa 70 32 6d 76 d6 ce c3 09 8d dd 01 94 06 d4 bc 73 be f1 74 84 e4 a9 0c c2 ae 29 76 e9 cf 68 ab 94

OpenSSL: Peer certificate - depth 0

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

3c:c4:06:9a:6c:1b:8d:ce:d5:9b:65:69:86:0a:d0:bd:00:05:1f:09

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=DESKTOP-BGRVDL1.

Validity

Not Before: Mar 14 07:15:00 2024 GMT

Not After : Mar 12 07:15:00 2034 GMT

Subject: CN=DESKTOP-BGRVDL1.

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:b9:45:b6:df:13:27:d0:f6:5f:d7:1b:b4:dc:50:

0b:55:83:09:ec:c3:d8:b8:67:f9:59:25:07:a8:df:

c0:db:6c:e9:f4:ec:5e:b0:48:23:9c:df:8f:cc:8f:

64:5a:e7:11:94:11:76:73:68:5f:47:e0:3d:9c:d0:

a7:5b:7e:51:2f:45:62:3e:76:e2:c0:28:95:42:80:

b4:5d:25:3f:27:b7:5a:e2:46:10:47:ab:2d:a9:99:

25:5e:db:84:a0:e6:a5:83:eb:d0:3a:c6:28:18:0a:

1e:1c:8d:b3:9d:72:a1:04:e6:a9:db:23:50:be:87:

da:73:67:9d:a8:03:e0:0f:60:bd:a9:9a:7b:30:3b:

66:6a:ef:b0:ca:ef:da:c3:dc:47:dc:f8:92:a3:c4:

eb:f2:33:5d:eb:3d:91:80:49:94:2a:7b:30:d1:f1:

4f:cc:16:f4:14:ee:a1:1c:7c:90:70:ab:c2:50:c6:

16:18:07:ac:05:5b:47:4d:66:15:cc:e5:7b:50:62:

11:56:b4:31:05:05:b6:df:7e:be:b2:7e:f4:72:97:

6e:a1:9b:aa:5a:ea:c1:3f:99:19:1a:7f:39:04:b5:

74:84:e2:ff:9c:b3:de:a5:75:be:76:43:54:7a:cf:

cc:85:89:11:7f:4f:37:83:8a:85:b9:74:5c:4f:dc:

e8:0b

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Subject Alternative Name:

DNS:DESKTOP-BGRVDL1.

X509v3 Subject Key Identifier:

0C:1E:23:76:A7:00:38:35:5B:64:E9:A7:24:35:B0:BF:50:B7:AC:D4

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

11:0a:eb:a3:5d:a8:93:d1:74:b2:ae:02:3f:e9:f7:76:49:ec:

35:26:74:41:22:ff:2d:62:c3:20:e0:83:6c:a5:3b:e4:40:29:

ae:40:77:04:dc:0f:f9:dd:db:25:95:5f:77:a9:6a:ee:f3:34:

f5:8d:9b:00:92:99:d8:89:3b:8e:3a:f4:74:46:9a:44:b8:7e:

9e:f8:68:55:c6:de:89:73:02:5f:12:e6:a6:c2:28:47:ed:07:

0b:66:89:b6:54:07:55:f2:e3:fe:66:13:41:88:ef:4c:bc:b5:

ba:06:ff:99:dc:6b:8b:53:a0:91:d6:01:50:f2:f3:25:83:b1:

41:cb:1b:a7:a7:4b:c3:85:cc:35:af:f0:6e:15:a8:54:ce:64:

ce:3e:32:65:bf:d9:68:f8:dc:48:9f:74:a7:e8:a8:b0:b1:53:

c7:c5:f5:8b:e1:3d:42:54:56:0f:42:e6:17:7a:1a:87:83:88:

f6:8c:ac:a2:44:f0:77:b4:d3:e8:b9:9c:e1:99:16:77:77:ac:

82:ae:e7:25:e3:62:d6:ea:52:fc:00:11:d3:4d:d4:73:9f:cd:

71:d7:1a:32:f8:d8:da:fa:70:32:6d:76:d6:ce:c3:09:8d:dd:

01:94:06:d4:bc:73:be:f1:74:84:e4:a9:0c:c2:ae:29:76:e9:

cf:68:ab:94

CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/CN=DESKTOP-BGRVDL1.' hash=265539896eabc13e0df10479b2d728ae7e359c790f5d8918b0860e4fca98f44e

CTRL-EVENT-EAP-PEER-ALT depth=0 DNS:DESKTOP-BGRVDL1.

TLS: tls\_verify\_cb - preverify\_ok=1 err=18 (self-signed certificate) ca\_cert\_verify=0 depth=0 buf='/CN=DESKTOP-BGRVDL1.'

EAP: Status notification: remote certificate verification (param=success)

OpenSSL: Peer certificate - depth 0

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

3c:c4:06:9a:6c:1b:8d:ce:d5:9b:65:69:86:0a:d0:bd:00:05:1f:09

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=DESKTOP-BGRVDL1.

Validity

Not Before: Mar 14 07:15:00 2024 GMT

Not After : Mar 12 07:15:00 2034 GMT

Subject: CN=DESKTOP-BGRVDL1.

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:b9:45:b6:df:13:27:d0:f6:5f:d7:1b:b4:dc:50:

0b:55:83:09:ec:c3:d8:b8:67:f9:59:25:07:a8:df:

c0:db:6c:e9:f4:ec:5e:b0:48:23:9c:df:8f:cc:8f:

64:5a:e7:11:94:11:76:73:68:5f:47:e0:3d:9c:d0:

a7:5b:7e:51:2f:45:62:3e:76:e2:c0:28:95:42:80:

b4:5d:25:3f:27:b7:5a:e2:46:10:47:ab:2d:a9:99:

25:5e:db:84:a0:e6:a5:83:eb:d0:3a:c6:28:18:0a:

1e:1c:8d:b3:9d:72:a1:04:e6:a9:db:23:50:be:87:

da:73:67:9d:a8:03:e0:0f:60:bd:a9:9a:7b:30:3b:

66:6a:ef:b0:ca:ef:da:c3:dc:47:dc:f8:92:a3:c4:

eb:f2:33:5d:eb:3d:91:80:49:94:2a:7b:30:d1:f1:

4f:cc:16:f4:14:ee:a1:1c:7c:90:70:ab:c2:50:c6:

16:18:07:ac:05:5b:47:4d:66:15:cc:e5:7b:50:62:

11:56:b4:31:05:05:b6:df:7e:be:b2:7e:f4:72:97:

6e:a1:9b:aa:5a:ea:c1:3f:99:19:1a:7f:39:04:b5:

74:84:e2:ff:9c:b3:de:a5:75:be:76:43:54:7a:cf:

cc:85:89:11:7f:4f:37:83:8a:85:b9:74:5c:4f:dc:

e8:0b

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Subject Alternative Name:

DNS:DESKTOP-BGRVDL1.

X509v3 Subject Key Identifier:

0C:1E:23:76:A7:00:38:35:5B:64:E9:A7:24:35:B0:BF:50:B7:AC:D4

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

11:0a:eb:a3:5d:a8:93:d1:74:b2:ae:02:3f:e9:f7:76:49:ec:

35:26:74:41:22:ff:2d:62:c3:20:e0:83:6c:a5:3b:e4:40:29:

ae:40:77:04:dc:0f:f9:dd:db:25:95:5f:77:a9:6a:ee:f3:34:

f5:8d:9b:00:92:99:d8:89:3b:8e:3a:f4:74:46:9a:44:b8:7e:

9e:f8:68:55:c6:de:89:73:02:5f:12:e6:a6:c2:28:47:ed:07:

0b:66:89:b6:54:07:55:f2:e3:fe:66:13:41:88:ef:4c:bc:b5:

ba:06:ff:99:dc:6b:8b:53:a0:91:d6:01:50:f2:f3:25:83:b1:

41:cb:1b:a7:a7:4b:c3:85:cc:35:af:f0:6e:15:a8:54:ce:64:

ce:3e:32:65:bf:d9:68:f8:dc:48:9f:74:a7:e8:a8:b0:b1:53:

c7:c5:f5:8b:e1:3d:42:54:56:0f:42:e6:17:7a:1a:87:83:88:

f6:8c:ac:a2:44:f0:77:b4:d3:e8:b9:9c:e1:99:16:77:77:ac:

82:ae:e7:25:e3:62:d6:ea:52:fc:00:11:d3:4d:d4:73:9f:cd:

71:d7:1a:32:f8:d8:da:fa:70:32:6d:76:d6:ce:c3:09:8d:dd:

01:94:06:d4:bc:73:be:f1:74:84:e4:a9:0c:c2:ae:29:76:e9:

cf:68:ab:94

CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/CN=DESKTOP-BGRVDL1.' hash=265539896eabc13e0df10479b2d728ae7e359c790f5d8918b0860e4fca98f44e

CTRL-EVENT-EAP-PEER-ALT depth=0 DNS:DESKTOP-BGRVDL1.

TLS: tls\_verify\_cb - preverify\_ok=1 err=18 (self-signed certificate) ca\_cert\_verify=0 depth=0 buf='/CN=DESKTOP-BGRVDL1.'

EAP: Status notification: remote certificate verification (param=success)

OpenSSL: RX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 16 03 03 01 2c

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS read server certificate

OpenSSL: RX ver=0x303 content\_type=22 (handshake/server key exchange)

OpenSSL: Message - hexdump(len=300): 0c 00 01 28 03 00 1d 20 cf 59 e4 02 b6 9b e5 b4 f9 3a 53 b1 23 68 4f 30 38 3e 6a 24 10 e0 a8 b9 ea f6 5a 9a 3d 4c 37 08 08 04 01 00 6b 26 86 83 4e 19 10 67 f0 02 4c 47 1a da 81 58 a9 c3 b5 09 ca bb 46 02 80 21 ac e0 11 49 4c 53 0b 9c 68 fc 60 45 18 99 65 03 10 af c8 9d e6 55 b5 ea 0a 24 40 98 3d 53 fa 07 6a 93 da 3f fa cb f2 df 09 05 48 64 a9 b8 5e e2 80 b6 52 f6 66 dd 64 78 52 05 7b 50 10 78 f3 e1 bc 07 e6 13 7d a6 55 f8 1d 64 59 03 da 49 9e aa ba 43 14 13 4f 91 3f 74 8b ec b3 46 df 23 ee 66 cc f7 92 b5 5d 48 71 34 f7 2a ae 14 6b 58 a0 c7 30 02 83 ab 43 e3 d5 0e 88 f4 40 b9 cb d7 0a 42 e4 ee 45 4c 4c 5a fb 43 11 f9 97 e6 dc 14 16 07 fc 82 ed 33 11 08 d8 7f 44 37 da 71 f2 d8 5e e9 b4 ab 1b 8c b3 f0 94 f6 37 7c cd ba 98 82 96 b7 b4 a2 8c 87 e1 c7 b9 8c ce 75 fc fd c9 19 d3 fb 97 97 c5 45 ce 86 38 8e a1 6e 3e 3c ed d5 7b dc 66 8a dc 82 f7 de a0 22 56 5e 04 6f 36 69 55 e2 27 36 6b 9d c9 c2

OpenSSL: RX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 16 03 03 00 04

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS read server key exchange

OpenSSL: RX ver=0x303 content\_type=22 (handshake/server hello done)

OpenSSL: Message - hexdump(len=4): 0e 00 00 00

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS read server done

OpenSSL: TX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 16 03 03 00 25

OpenSSL: TX ver=0x303 content\_type=22 (handshake/client key exchange)

OpenSSL: Message - hexdump(len=37): 10 00 00 21 20 da a8 26 30 64 d8 70 65 6d 5e 71 60 a5 fd 74 25 81 03 1c fa c3 6d 17 bc 28 1e a4 e2 fb 02 63 18

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS write client key exchange

OpenSSL: TX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 14 03 03 00 01

OpenSSL: TX ver=0x303 content\_type=20 (change cipher spec/)

OpenSSL: Message - hexdump(len=1): 01

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS write change cipher spec

OpenSSL: TX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 16 03 03 00 28

OpenSSL: TX ver=0x303 content\_type=22 (handshake/finished)

OpenSSL: Message - hexdump(len=16): 14 00 00 0c cc ac 96 23 d0 6b 88 68 ea 1e 5f be

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS write finished

SSL: (where=0x1002 ret=0xffffffff)

SSL: SSL\_connect:error in SSLv3/TLS write finished

SSL: SSL\_connect - want more data

SSL: 93 bytes pending from ssl\_out

SSL: Using TLS version TLSv1.2

SSL: 93 bytes left to be sent out (of total 93 bytes)

EAP: method process -> ignore=FALSE methodState=MAY\_CONT decision=FAIL eapRespData=0x7fffd0773520

EAP: EAP entering state SEND\_RESPONSE

EAP: EAP entering state IDLE

EAPOL: SUPP\_BE entering state RESPONSE

EAPOL: txSuppRsp

WPA: eapol\_test\_eapol\_send(type=0 len=103)

TX EAP -> RADIUS - hexdump(len=103): 02 63 00 67 19 80 00 00 00 5d 16 03 03 00 25 10 00 00 21 20 da a8 26 30 64 d8 70 65 6d 5e 71 60 a5 fd 74 25 81 03 1c fa c3 6d 17 bc 28 1e a4 e2 fb 02 63 18 14 03 03 00 01 01 16 03 03 00 28 58 12 51 4b d4 bd 7f 59 c8 ae 1f 3f 0c 18 91 fe 1e 43 fa 88 cf 24 07 5c 34 28 7e 0b 67 23 37 e0 67 dd 0d 45 e1 5d 2b 9a

Encapsulating EAP message into a RADIUS packet

Copied RADIUS State Attribute

Sending RADIUS message to authentication server

RADIUS message: code=1 (Access-Request) identifier=4 length=238

Attribute 1 (User-Name) length=7

Value: 'steve'

Attribute 4 (NAS-IP-Address) length=6

Value: 127.0.0.1

Attribute 31 (Calling-Station-Id) length=19

Value: '02-00-00-00-00-01'

Attribute 12 (Framed-MTU) length=6

Value: 1400

Attribute 61 (NAS-Port-Type) length=6

Value: 19

Attribute 6 (Service-Type) length=6

Value: 2

Attribute 77 (Connect-Info) length=24

Value: 'CONNECT 11Mbps 802.11b'

Attribute 30 (Called-Station-Id) length=3

Value: '\x00'

Attribute 79 (EAP-Message) length=105

Value: 0263006719800000005d16030300251000002120daa8263064d870656d5e7160a5fd742581031cfac36d17bc281ea4e2fb02631814030300010116030300285812514bd4bd7f59c8ae1f3f0c1891fe1e43fa88cf24075c34287e0b672337e067dd0d45e15d2b9a

Attribute 24 (State) length=18

Value: 7583638c76e07a0a9a7e5f1775f4795f

Attribute 80 (Message-Authenticator) length=18

Value: e5eb7568afc69d15347d75f213567da7

Next RADIUS client retransmit in 3 seconds

EAPOL: SUPP\_BE entering state RECEIVE

Received 115 bytes from RADIUS server

Received RADIUS message

RADIUS message: code=11 (Access-Challenge) identifier=4 length=115

Attribute 79 (EAP-Message) length=59

Value: 0164003919001403030001011603030028e9c23bbdecc1421960ffb4cb8aa449b618d98c3122d61e4bde8e576a938f1d0bc76851a9f5cbf14b

Attribute 80 (Message-Authenticator) length=18

Value: e65a49d8cfb3048d859027ddab1682d8

Attribute 24 (State) length=18

Value: 7583638c71e77a0a9a7e5f1775f4795f

STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.00 sec

RADIUS packet matching with station

decapsulated EAP packet (code=1 id=100 len=57) from RADIUS server: EAP-Request-PEAP (25)

EAPOL: Received EAP-Packet frame

EAPOL: SUPP\_BE entering state REQUEST

EAPOL: getSuppRsp

EAP: EAP entering state RECEIVED

EAP: Received EAP-Request id=100 method=25 vendor=0 vendorMethod=0

EAP: EAP entering state METHOD

SSL: Received packet(len=57) - Flags 0x00

OpenSSL: RX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 14 03 03 00 01

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS write finished

OpenSSL: RX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 16 03 03 00 28

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS read change cipher spec

OpenSSL: RX ver=0x303 content\_type=22 (handshake/finished)

OpenSSL: Message - hexdump(len=16): 14 00 00 0c 3f 40 81 32 30 21 9b 6d 3f 90 b0 02

SSL: (where=0x1001 ret=0x1)

SSL: SSL\_connect:SSLv3/TLS read finished

SSL: (where=0x20 ret=0x1)

SSL: (where=0x1002 ret=0x1)

SSL: 0 bytes pending from ssl\_out

OpenSSL: Handshake finished - resumed=0

SSL: No Application Data included

SSL: Using TLS version TLSv1.2

SSL: No data to be sent out

EAP-PEAP: TLS done, proceed to Phase 2

EAP-PEAP: using label 'client EAP encryption' in key derivation

EAP-PEAP: Derived key - hexdump(len=64): 35 3e 33 66 0e 02 c5 31 34 63 bd 55 76 d4 ea 6b 60 f9 0d 1e 77 15 45 f0 83 2a 47 b8 1e 8e 19 f5 70 4b 1b 4d 6d f2 e0 18 ba e2 ff 46 a8 06 9f a6 01 d2 95 e2 a4 a3 74 4e 7d 91 61 d9 42 5e a5 b3

EAP-PEAP: Derived EMSK - hexdump(len=64): d6 09 de d3 72 59 27 44 de c2 1d cc 6e f3 17 d2 cc 1f db 3a cb 78 73 93 78 45 9c af d4 d1 b0 bb bd 68 7d ba fd 2d e7 14 02 16 fa 0f 61 82 90 60 88 db 5b b3 cd 94 cf 4a bf 69 b0 6f 3f e9 3f bb

EAP-PEAP: Derived Session-Id - hexdump(len=65): 19 df 5d 1a a7 ba a5 f8 70 59 3f 23 ca e2 63 c3 5c 44 62 e6 3b 01 ac a4 e9 a9 9c 79 aa a3 68 9d ae b4 27 e2 39 3b 9b 31 db ec 85 df 5f 03 13 f6 55 58 e0 26 dd 2f 1f 05 fa 39 70 14 80 b9 6f c4 d5

SSL: Building ACK (type=25 id=100 ver=0)

EAP: method process -> ignore=FALSE methodState=MAY\_CONT decision=FAIL eapRespData=0x7fffd079be10

EAP: EAP entering state SEND\_RESPONSE

EAP: EAP entering state IDLE

EAPOL: SUPP\_BE entering state RESPONSE

EAPOL: txSuppRsp

WPA: eapol\_test\_eapol\_send(type=0 len=6)

TX EAP -> RADIUS - hexdump(len=6): 02 64 00 06 19 00

Encapsulating EAP message into a RADIUS packet

Copied RADIUS State Attribute

Sending RADIUS message to authentication server

RADIUS message: code=1 (Access-Request) identifier=5 length=141

Attribute 1 (User-Name) length=7

Value: 'steve'

Attribute 4 (NAS-IP-Address) length=6

Value: 127.0.0.1

Attribute 31 (Calling-Station-Id) length=19

Value: '02-00-00-00-00-01'

Attribute 12 (Framed-MTU) length=6

Value: 1400

Attribute 61 (NAS-Port-Type) length=6

Value: 19

Attribute 6 (Service-Type) length=6

Value: 2

Attribute 77 (Connect-Info) length=24

Value: 'CONNECT 11Mbps 802.11b'

Attribute 30 (Called-Station-Id) length=3

Value: '\x00'

Attribute 79 (EAP-Message) length=8

Value: 026400061900

Attribute 24 (State) length=18

Value: 7583638c71e77a0a9a7e5f1775f4795f

Attribute 80 (Message-Authenticator) length=18

Value: e532a0623cafcc90d576e3384d8030c0

Next RADIUS client retransmit in 3 seconds

EAPOL: SUPP\_BE entering state RECEIVE

Received 98 bytes from RADIUS server

Received RADIUS message

RADIUS message: code=11 (Access-Challenge) identifier=5 length=98

Attribute 79 (EAP-Message) length=42

Value: 016500281900170303001de9c23bbdecc1421a4feb5d4d8316ee1896a10ba29b6e80507d8aab0630

Attribute 80 (Message-Authenticator) length=18

Value: 9f7ee780ae3b1c9941ccbb17d1bc9627

Attribute 24 (State) length=18

Value: 7583638c70e67a0a9a7e5f1775f4795f

STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.00 sec

RADIUS packet matching with station

decapsulated EAP packet (code=1 id=101 len=40) from RADIUS server: EAP-Request-PEAP (25)

EAPOL: Received EAP-Packet frame

EAPOL: SUPP\_BE entering state REQUEST

EAPOL: getSuppRsp

EAP: EAP entering state RECEIVED

EAP: Received EAP-Request id=101 method=25 vendor=0 vendorMethod=0

EAP: EAP entering state METHOD

SSL: Received packet(len=40) - Flags 0x00

EAP-PEAP: received 34 bytes encrypted data for Phase 2

OpenSSL: RX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 17 03 03 00 1d

EAP-PEAP: Decrypted Phase 2 EAP - hexdump(len=5): 01 65 00 05 01

EAP-PEAP: received Phase 2: code=1 identifier=101 length=5

EAP-PEAP: Phase 2 Request: type=1

EAP: using real identity - hexdump\_ascii(len=5):

73 74 65 76 65 steve

EAP-PEAP: Encrypting Phase 2 data - hexdump(len=10): 02 65 00 0a 01 73 74 65 76 65

OpenSSL: TX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 17 03 03 00 1e

SSL: 35 bytes left to be sent out (of total 35 bytes)

EAP: method process -> ignore=FALSE methodState=MAY\_CONT decision=FAIL eapRespData=0x7fffd0774c80

EAP: EAP entering state SEND\_RESPONSE

EAP: EAP entering state IDLE

EAPOL: SUPP\_BE entering state RESPONSE

EAPOL: txSuppRsp

WPA: eapol\_test\_eapol\_send(type=0 len=41)

TX EAP -> RADIUS - hexdump(len=41): 02 65 00 29 19 00 17 03 03 00 1e 58 12 51 4b d4 bd 7f 5a 0c 72 15 f9 fd f4 8d 41 60 ba 59 90 8d c3 3c 9f 8a c8 50 35 38 10

Encapsulating EAP message into a RADIUS packet

Copied RADIUS State Attribute

Sending RADIUS message to authentication server

RADIUS message: code=1 (Access-Request) identifier=6 length=176

Attribute 1 (User-Name) length=7

Value: 'steve'

Attribute 4 (NAS-IP-Address) length=6

Value: 127.0.0.1

Attribute 31 (Calling-Station-Id) length=19

Value: '02-00-00-00-00-01'

Attribute 12 (Framed-MTU) length=6

Value: 1400

Attribute 61 (NAS-Port-Type) length=6

Value: 19

Attribute 6 (Service-Type) length=6

Value: 2

Attribute 77 (Connect-Info) length=24

Value: 'CONNECT 11Mbps 802.11b'

Attribute 30 (Called-Station-Id) length=3

Value: '\x00'

Attribute 79 (EAP-Message) length=43

Value: 026500291900170303001e5812514bd4bd7f5a0c7215f9fdf48d4160ba59908dc33c9f8ac850353810

Attribute 24 (State) length=18

Value: 7583638c70e67a0a9a7e5f1775f4795f

Attribute 80 (Message-Authenticator) length=18

Value: 55982d87004f68af6b0df3ba21f5ae26

Next RADIUS client retransmit in 3 seconds

EAPOL: SUPP\_BE entering state RECEIVE

Received 132 bytes from RADIUS server

Received RADIUS message

RADIUS message: code=11 (Access-Challenge) identifier=6 length=132

Attribute 79 (EAP-Message) length=76

Value: 0166004a1900170303003fe9c23bbdecc1421befc4b49aa20373f1b4f7094a1249bd3e6b4ac0f6156fc0e916ef2f1ab2374cd86831a654a2ea81c22f654174efc2add2aaadc7309291f5

Attribute 80 (Message-Authenticator) length=18

Value: 8acd0a4aec043e1ae92bc2b26ff1a787

Attribute 24 (State) length=18

Value: 7583638c73e57a0a9a7e5f1775f4795f

STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.00 sec

RADIUS packet matching with station

decapsulated EAP packet (code=1 id=102 len=74) from RADIUS server: EAP-Request-PEAP (25)

EAPOL: Received EAP-Packet frame

EAPOL: SUPP\_BE entering state REQUEST

EAPOL: getSuppRsp

EAP: EAP entering state RECEIVED

EAP: Received EAP-Request id=102 method=25 vendor=0 vendorMethod=0

EAP: EAP entering state METHOD

SSL: Received packet(len=74) - Flags 0x00

EAP-PEAP: received 68 bytes encrypted data for Phase 2

OpenSSL: RX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 17 03 03 00 3f

EAP-PEAP: Decrypted Phase 2 EAP - hexdump(len=39): 1a 01 66 00 26 10 21 c9 03 80 d7 d5 a8 cd 79 db ae 60 21 64 25 c4 66 72 65 65 72 61 64 69 75 73 2d 33 2e 30 2e 32 36

EAP-PEAP: received Phase 2: code=1 identifier=102 length=43

EAP-PEAP: Phase 2 Request: type=26

EAP-PEAP: Selected Phase 2 EAP vendor 0 method 26

EAP-MSCHAPV2: RX identifier 102 mschapv2\_id 102

EAP-MSCHAPV2: Received challenge

EAP-MSCHAPV2: Authentication Servername - hexdump\_ascii(len=17):

66 72 65 65 72 61 64 69 75 73 2d 33 2e 30 2e 32 freeradius-3.0.2

36 6

EAP-MSCHAPV2: Generating Challenge Response

Get randomness: len=16 entropy=0

random from os\_get\_random - hexdump(len=16): e1 ad 99 32 c8 39 ae dd 43 81 55 01 c1 0d 03 91

random\_mix\_pool - hexdump(len=20): 0d b9 b1 bf 70 7c bd fa 8b 8c 0a 46 d8 96 87 a4 8e 89 0d 7d

random from internal pool - hexdump(len=16): 52 c7 66 0a bf 85 ed d3 d8 c1 5b 8c 5d 36 f0 8e

mixed random - hexdump(len=16): b3 6a ff 38 77 bc 43 0e 9b 40 0e 8d 9c 3b f3 1f

MSCHAPV2: Identity - hexdump\_ascii(len=5):

73 74 65 76 65 steve

MSCHAPV2: Username - hexdump\_ascii(len=5):

73 74 65 76 65 steve

MSCHAPV2: auth\_challenge - hexdump(len=16): 21 c9 03 80 d7 d5 a8 cd 79 db ae 60 21 64 25 c4

MSCHAPV2: peer\_challenge - hexdump(len=16): b3 6a ff 38 77 bc 43 0e 9b 40 0e 8d 9c 3b f3 1f

MSCHAPV2: username - hexdump\_ascii(len=5):

73 74 65 76 65 steve

MSCHAPV2: password - hexdump\_ascii(len=7):

74 65 73 74 69 6e 67 testing

MSCHAPV2: NT Response - hexdump(len=24): 42 9a c7 32 bf e6 6e 86 ea fc 0e 2a ad 25 b2 95 57 3a 78 b0 39 8d 7d 3d

MSCHAPV2: Auth Response - hexdump(len=20): cd 0e bd 18 0b c6 ba 9c 5f b2 c7 e7 96 0d 6a 5d 2f 4a cf c6

MSCHAPV2: Master Key - hexdump(len=16): c7 7e 99 2a ea 0a 20 3c 84 39 6f 21 78 d8 74 6e

EAP-MSCHAPV2: TX identifier 102 mschapv2\_id 102 (response)

EAP-PEAP: Encrypting Phase 2 data - hexdump(len=64): 02 66 00 40 1a 02 66 00 3b 31 b3 6a ff 38 77 bc 43 0e 9b 40 0e 8d 9c 3b f3 1f 00 00 00 00 00 00 00 00 42 9a c7 32 bf e6 6e 86 ea fc 0e 2a ad 25 b2 95 57 3a 78 b0 39 8d 7d 3d 00 73 74 65 76 65

OpenSSL: TX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 17 03 03 00 54

SSL: 89 bytes left to be sent out (of total 89 bytes)

EAP: method process -> ignore=FALSE methodState=MAY\_CONT decision=FAIL eapRespData=0x7fffd07712c0

EAP: EAP entering state SEND\_RESPONSE

EAP: EAP entering state IDLE

EAPOL: SUPP\_BE entering state RESPONSE

EAPOL: txSuppRsp

WPA: eapol\_test\_eapol\_send(type=0 len=95)

TX EAP -> RADIUS - hexdump(len=95): 02 66 00 5f 19 00 17 03 03 00 54 58 12 51 4b d4 bd 7f 5b 50 19 0e f5 8e 88 93 fd 99 10 bc 92 b0 33 6b 12 bd 4d a8 5c dd 05 7c e9 f2 ee f1 04 da 3f f8 66 ca f9 98 ed eb c2 1a 2f 99 e1 6e 79 56 99 45 c6 e2 d9 ba d3 48 6d 5b 0c cf 58 f0 17 70 c3 41 2d 97 48 e0 46 f2 5d e8 ae 9c c9 fa fb

Encapsulating EAP message into a RADIUS packet

Copied RADIUS State Attribute

Sending RADIUS message to authentication server

RADIUS message: code=1 (Access-Request) identifier=7 length=230

Attribute 1 (User-Name) length=7

Value: 'steve'

Attribute 4 (NAS-IP-Address) length=6

Value: 127.0.0.1

Attribute 31 (Calling-Station-Id) length=19

Value: '02-00-00-00-00-01'

Attribute 12 (Framed-MTU) length=6

Value: 1400

Attribute 61 (NAS-Port-Type) length=6

Value: 19

Attribute 6 (Service-Type) length=6

Value: 2

Attribute 77 (Connect-Info) length=24

Value: 'CONNECT 11Mbps 802.11b'

Attribute 30 (Called-Station-Id) length=3

Value: '\x00'

Attribute 79 (EAP-Message) length=97

Value: 0266005f190017030300545812514bd4bd7f5b50190ef58e8893fd9910bc92b0336b12bd4da85cdd057ce9f2eef104da3ff866caf998edebc21a2f99e16e79569945c6e2d9bad3486d5b0ccf58f01770c3412d9748e046f25de8ae9cc9fafb

Attribute 24 (State) length=18

Value: 7583638c73e57a0a9a7e5f1775f4795f

Attribute 80 (Message-Authenticator) length=18

Value: 133bd5f9725e26db0a678b3f04b938f4

Next RADIUS client retransmit in 3 seconds

EAPOL: SUPP\_BE entering state RECEIVE

Received 140 bytes from RADIUS server

Received RADIUS message

RADIUS message: code=11 (Access-Challenge) identifier=7 length=140

Attribute 79 (EAP-Message) length=84

Value: 0167005219001703030047e9c23bbdecc1421cd322b72be12bc0689d1f7431da7902545f66f01ce4f8108d2eb45f781d3eccb8b780cb4134f087f1c125a48c6b57704b7548f16a7ee21c98c36203a4886086

Attribute 80 (Message-Authenticator) length=18

Value: 6e208df6201d058187c3ab472fe9dd32

Attribute 24 (State) length=18

Value: 7583638c72e47a0a9a7e5f1775f4795f

STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.00 sec

RADIUS packet matching with station

decapsulated EAP packet (code=1 id=103 len=82) from RADIUS server: EAP-Request-PEAP (25)

EAPOL: Received EAP-Packet frame

EAPOL: SUPP\_BE entering state REQUEST

EAPOL: getSuppRsp

EAP: EAP entering state RECEIVED

EAP: Received EAP-Request id=103 method=25 vendor=0 vendorMethod=0

EAP: EAP entering state METHOD

SSL: Received packet(len=82) - Flags 0x00

EAP-PEAP: received 76 bytes encrypted data for Phase 2

OpenSSL: RX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 17 03 03 00 47

EAP-PEAP: Decrypted Phase 2 EAP - hexdump(len=47): 1a 03 66 00 2e 53 3d 43 44 30 45 42 44 31 38 30 42 43 36 42 41 39 43 35 46 42 32 43 37 45 37 39 36 30 44 36 41 35 44 32 46 34 41 43 46 43 36

EAP-PEAP: received Phase 2: code=1 identifier=103 length=51

EAP-PEAP: Phase 2 Request: type=26

EAP-MSCHAPV2: RX identifier 103 mschapv2\_id 102

EAP-MSCHAPV2: Received success

EAP-MSCHAPV2: Success message - hexdump\_ascii(len=0):

EAP-MSCHAPV2: Authentication succeeded

EAP-PEAP: Encrypting Phase 2 data - hexdump(len=6): 02 67 00 06 1a 03

OpenSSL: TX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 17 03 03 00 1a

SSL: 31 bytes left to be sent out (of total 31 bytes)

EAP: method process -> ignore=FALSE methodState=MAY\_CONT decision=FAIL eapRespData=0x7fffd07a9f00

EAP: Session-Id - hexdump(len=65): 19 df 5d 1a a7 ba a5 f8 70 59 3f 23 ca e2 63 c3 5c 44 62 e6 3b 01 ac a4 e9 a9 9c 79 aa a3 68 9d ae b4 27 e2 39 3b 9b 31 db ec 85 df 5f 03 13 f6 55 58 e0 26 dd 2f 1f 05 fa 39 70 14 80 b9 6f c4 d5

EAP: EAP entering state SEND\_RESPONSE

EAP: EAP entering state IDLE

EAPOL: SUPP\_BE entering state RESPONSE

EAPOL: txSuppRsp

WPA: eapol\_test\_eapol\_send(type=0 len=37)

TX EAP -> RADIUS - hexdump(len=37): 02 67 00 25 19 00 17 03 03 00 1a 58 12 51 4b d4 bd 7f 5c f3 91 3e e8 ca 5b 68 3d 38 aa f8 6a bf 52 78 5d 92 8b

Encapsulating EAP message into a RADIUS packet

Copied RADIUS State Attribute

Sending RADIUS message to authentication server

RADIUS message: code=1 (Access-Request) identifier=8 length=172

Attribute 1 (User-Name) length=7

Value: 'steve'

Attribute 4 (NAS-IP-Address) length=6

Value: 127.0.0.1

Attribute 31 (Calling-Station-Id) length=19

Value: '02-00-00-00-00-01'

Attribute 12 (Framed-MTU) length=6

Value: 1400

Attribute 61 (NAS-Port-Type) length=6

Value: 19

Attribute 6 (Service-Type) length=6

Value: 2

Attribute 77 (Connect-Info) length=24

Value: 'CONNECT 11Mbps 802.11b'

Attribute 30 (Called-Station-Id) length=3

Value: '\x00'

Attribute 79 (EAP-Message) length=39

Value: 026700251900170303001a5812514bd4bd7f5cf3913ee8ca5b683d38aaf86abf52785d928b

Attribute 24 (State) length=18

Value: 7583638c72e47a0a9a7e5f1775f4795f

Attribute 80 (Message-Authenticator) length=18

Value: 7af5fdc71eefb704bb217c55626f2376

Next RADIUS client retransmit in 3 seconds

EAPOL: SUPP\_BE entering state RECEIVE

Received 104 bytes from RADIUS server

Received RADIUS message

RADIUS message: code=11 (Access-Challenge) identifier=8 length=104

Attribute 79 (EAP-Message) length=48

Value: 0168002e19001703030023e9c23bbdecc1421dd1a14a87a248a3d522a6fde235b9dc834d513ef8dfa4755c0a460f

Attribute 80 (Message-Authenticator) length=18

Value: 39fc805ef939af12b3cd80e603252527

Attribute 24 (State) length=18

Value: 7583638c7deb7a0a9a7e5f1775f4795f

STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.00 sec

RADIUS packet matching with station

decapsulated EAP packet (code=1 id=104 len=46) from RADIUS server: EAP-Request-PEAP (25)

EAPOL: Received EAP-Packet frame

EAPOL: SUPP\_BE entering state REQUEST

EAPOL: getSuppRsp

EAP: EAP entering state RECEIVED

EAP: Received EAP-Request id=104 method=25 vendor=0 vendorMethod=0

EAP: EAP entering state METHOD

SSL: Received packet(len=46) - Flags 0x00

EAP-PEAP: received 40 bytes encrypted data for Phase 2

OpenSSL: RX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 17 03 03 00 23

EAP-PEAP: Decrypted Phase 2 EAP - hexdump(len=11): 01 68 00 0b 21 80 03 00 02 00 01

EAP-PEAP: received Phase 2: code=1 identifier=104 length=11

EAP-PEAP: Phase 2 Request: type=33

EAP-TLV: Received TLVs - hexdump(len=6): 80 03 00 02 00 01

EAP-TLV: Result TLV - hexdump(len=2): 00 01

EAP-TLV: TLV Result - Success - EAP-TLV/Phase2 Completed

EAP-PEAP: Encrypting Phase 2 data - hexdump(len=11): 02 68 00 0b 21 80 03 00 02 00 01

OpenSSL: TX ver=0x303 content\_type=256 (TLS header info/)

OpenSSL: Message - hexdump(len=5): 17 03 03 00 23

SSL: 40 bytes left to be sent out (of total 40 bytes)

EAP: method process -> ignore=FALSE methodState=DONE decision=UNCOND\_SUCC eapRespData=0x7fffd0771030

EAP: Session-Id - hexdump(len=65): 19 df 5d 1a a7 ba a5 f8 70 59 3f 23 ca e2 63 c3 5c 44 62 e6 3b 01 ac a4 e9 a9 9c 79 aa a3 68 9d ae b4 27 e2 39 3b 9b 31 db ec 85 df 5f 03 13 f6 55 58 e0 26 dd 2f 1f 05 fa 39 70 14 80 b9 6f c4 d5

EAP: EAP entering state SEND\_RESPONSE

EAP: EAP entering state IDLE

EAPOL: SUPP\_BE entering state RESPONSE

EAPOL: txSuppRsp

WPA: eapol\_test\_eapol\_send(type=0 len=46)

TX EAP -> RADIUS - hexdump(len=46): 02 68 00 2e 19 00 17 03 03 00 23 58 12 51 4b d4 bd 7f 5d a9 b8 82 68 c8 2a cc 57 85 8a ec 50 7d fe 36 09 6f fe e7 0d dd 6c 32 86 0c e8 c7

Encapsulating EAP message into a RADIUS packet

Copied RADIUS State Attribute

Sending RADIUS message to authentication server

RADIUS message: code=1 (Access-Request) identifier=9 length=181

Attribute 1 (User-Name) length=7

Value: 'steve'

Attribute 4 (NAS-IP-Address) length=6

Value: 127.0.0.1

Attribute 31 (Calling-Station-Id) length=19

Value: '02-00-00-00-00-01'

Attribute 12 (Framed-MTU) length=6

Value: 1400

Attribute 61 (NAS-Port-Type) length=6

Value: 19

Attribute 6 (Service-Type) length=6

Value: 2

Attribute 77 (Connect-Info) length=24

Value: 'CONNECT 11Mbps 802.11b'

Attribute 30 (Called-Station-Id) length=3

Value: '\x00'

Attribute 79 (EAP-Message) length=48

Value: 0268002e190017030300235812514bd4bd7f5da9b88268c82acc57858aec507dfe36096ffee70ddd6c32860ce8c7

Attribute 24 (State) length=18

Value: 7583638c7deb7a0a9a7e5f1775f4795f

Attribute 80 (Message-Authenticator) length=18

Value: b1b8ba6e75ba55edc3bed649b9d6a7e5

Next RADIUS client retransmit in 3 seconds

EAPOL: SUPP\_BE entering state RECEIVE

Received 173 bytes from RADIUS server

Received RADIUS message

RADIUS message: code=2 (Access-Accept) identifier=9 length=173

Attribute 26 (Vendor-Specific) length=58

Value: 0000013711349214d41c6f1148f0ba2395c361397bf6c52f779006cbd58e30aae792da1253792fc4ca84bb945a1f34832da960a0dbd06a71

Attribute 26 (Vendor-Specific) length=58

Value: 0000013710349fcd3648bd41d15882bc7aedcebf50e0fad71850b8d3f13e66cca31cf07caa2a01940f7cc5328f347c9e380d8740e0c42dbf

Attribute 79 (EAP-Message) length=6

Value: 03680004

Attribute 80 (Message-Authenticator) length=18

Value: ae77b4bcfc22ba35d07d07e7ff4c9794

Attribute 1 (User-Name) length=7

Value: 'steve'

Attribute 12 (Framed-MTU) length=6

Value: 994

STA 02:00:00:00:00:01: Received RADIUS packet matched with a pending request, round trip time 0.00 sec

RADIUS packet matching with station

MS-MPPE-Send-Key (sign) - hexdump(len=32): 70 4b 1b 4d 6d f2 e0 18 ba e2 ff 46 a8 06 9f a6 01 d2 95 e2 a4 a3 74 4e 7d 91 61 d9 42 5e a5 b3

MS-MPPE-Recv-Key (crypt) - hexdump(len=32): 35 3e 33 66 0e 02 c5 31 34 63 bd 55 76 d4 ea 6b 60 f9 0d 1e 77 15 45 f0 83 2a 47 b8 1e 8e 19 f5

decapsulated EAP packet (code=3 id=104 len=4) from RADIUS server: EAP Success

EAPOL: Received EAP-Packet frame

EAPOL: SUPP\_BE entering state REQUEST

EAPOL: getSuppRsp

EAP: EAP entering state RECEIVED

EAP: Received EAP-Success

EAP: Status notification: completion (param=success)

EAP: EAP entering state SUCCESS

CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully

EAPOL: IEEE 802.1X for plaintext connection; no EAPOL-Key frames required

WPA: EAPOL processing complete

Cancelling authentication timeout

State: DISCONNECTED -> COMPLETED

EAPOL: SUPP\_PAE entering state AUTHENTICATED

EAPOL: SUPP\_BE entering state RECEIVE

EAPOL: SUPP\_BE entering state SUCCESS

EAPOL: SUPP\_BE entering state IDLE

eapol\_sm\_cb: result=1

EAPOL: Successfully fetched key (len=32)

PMK from EAPOL - hexdump(len=32): 35 3e 33 66 0e 02 c5 31 34 63 bd 55 76 d4 ea 6b 60 f9 0d 1e 77 15 45 f0 83 2a 47 b8 1e 8e 19 f5

No EAP-Key-Name received from server

Writing configuration file '/etc/wpa\_supplicant-2.10/wpa\_supplicant/wpa\_supplicantm.conf.tmp'

Configuration file '/etc/wpa\_supplicant-2.10/wpa\_supplicant/wpa\_supplicantm.conf' written successfully

WPA: Clear old PMK and PTK

EAP: deinitialize previously used EAP method (25, PEAP) at EAP deinit

ENGINE: engine deinit

MPPE keys OK: 1 mismatch: 0

SUCCESS