MKC-NBS: Úkol č.4

EAP, RADIUS

Filip Paul

19.04.2022

EAP

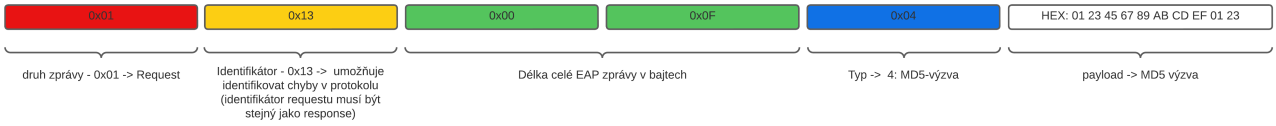
Zadání:

Klient se vůči serveru autentizuje pomocí protokolu EAP. Jeho dokazovacím faktorem je klíč K, což je v kódu ASCII řetězec ”Secret”. Znáte následující EAP zprávu:
01:13:00:0F:04:01:23:45:67:89:AB:CD:EF:01:23.
Určete, kdo je odesílatelem zprávy, jaký typ autentizace je použit a vysvětlete význam jednotlivých bajtů zprávy. Dále odvoďte bajtovou podobu EAP zprávy, která bude odezvou na zadanou EAP zprávu a význam bajtů této odezvy vysvětlete. K překladu ASCII znaků klíče na bajty použijte ASCII tabulku z adresy:
https://cs.wikipedia.org/wiki/ASCII
K výpočtu heše použijte kalkulátor na adrese:
http://www.fileformat.info/tool/hash.htm

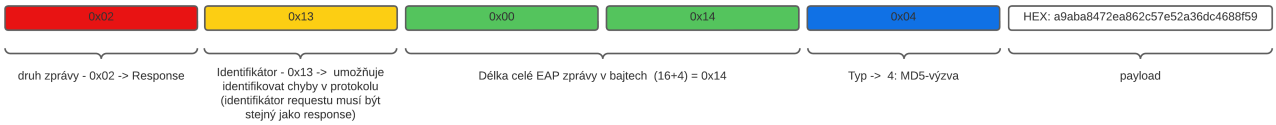
Vypracování:

Autentizátor odesílá EAP-MD5 požadavek, kde ve svém payload odesílá "náhodné" číslo, které slouží k následné autentizaci

01:13:00:0F:04:01:23:45:67:89:AB:CD:EF:01:23



Očekávaná odezva od žadatele:



Výpočet odpovědi:

payload = H(I+1 || Secret || MD5 výzva)

payload = H(I+1 || Secret || MD5 výzva)Secret
(HEX) = 53 65 63 72 65 74
I+1 = 0x14
MD5 výzva = 01 23 45 67 89 AB CD EF 01 23

payload = H(14 53 65 63 72 65 74 01 23 45 67 89 AB CD EF 01 23)
payload = a9aba8472ea862c57e52a36dc4688f59 (16B)

RADIUS

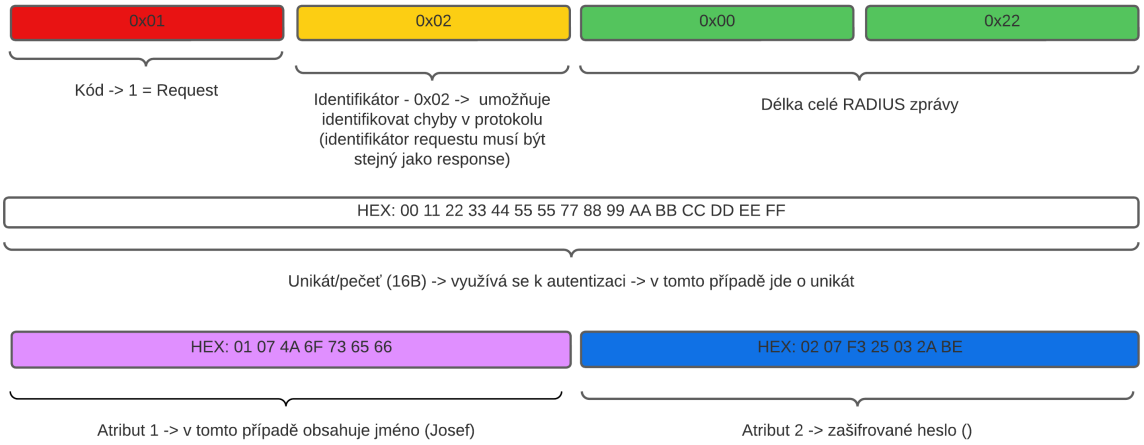
Zadání:

Serveru byla z brány doručena následující zpráva protokolu RADIUS:
01:02:00:22:00:11:22:33:44:55:55:77:88:99:AA:BB:CC:DD:EE:FF:01:07:4A:6F:73:65:66: 02:07:F3:25:03:2A:BE.
Víme přitom, že k zabezpečení provozu mezi branou a serverem je používán klíč K = Secret. U dané zprávy uveďte její typ a vysvětlete význam jednotlivých bajtů. Pokud se v ní vyskytuje přihlašovací jméno, tak je uveďte v textové podobě podle ASCII tabulky. Pokud se v ní bude nacházet zašifrované heslo, tak je dešifrujte a převeďte do textové podoby. Dále uveďte jaká bude odpověď serveru a význam jednotlivých bajtů této odpovědi vysvětlete. Předpokládejte přitom, že kontroly na straně serveru měly pozitivní výsledek.
K výpočtu hešů a ke konverzi bajtů na text použijte stejné odkazy jako v předchozím příkladu

Vypracování:

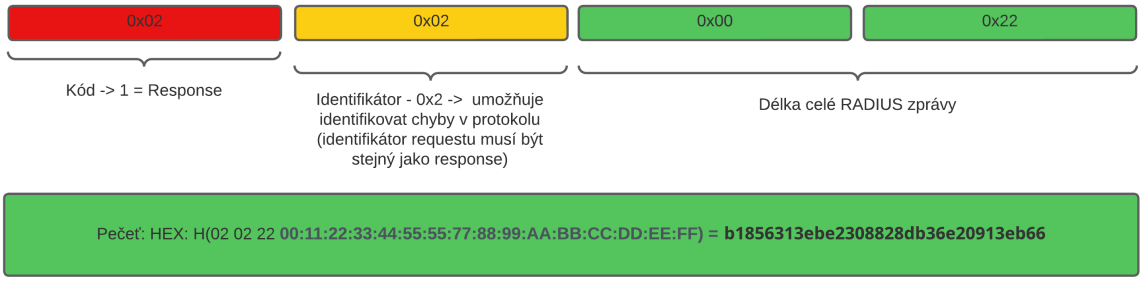
Žádost serveru o přístup:

01:02:00:22:00:11:22:33:44:55:55:77:88:99:AA:BB:CC:DD:EE:FF:01:07:4A:6F:73:65:66:02:07:F3:25:03:2A:BE



Šifrování hesla:
C = P XOR S
S = MD5(K||X) = (Secret || Unikát)
S = MD5 (53 65 63 72 65 74 ||00 11 22 33 44 55 55 77 88 99 AA BB CC DD EE FF)
S = b8444f7fce89bf1753f465043fdddb4f
P = C XOR S
P = F3 25 03 2A BE XOR **b8444f7**fce89bf1753f465043fdddb4f
P -> ASCII KaLU; HEX: 4b614c55

Odpověď ze serveru:



Pečeť: HEX: H(02 02 22 **00:11:22:33:44:55:55:77:88:99:AA:BB:CC:DD:EE:FF) = b1856313ebe2308828db36e20913eb66**