Εργαστηριακή Άσκηση 12

Θοδωρής Φρίξος Παπαρρηγόπουλος
el18040
Ομάδα 4η.
Ipv6: 2a02:587:4f0e:2b65:34b0:9e4a:d912:2f8a
MAC: 40-1C-83-38-F7-20
Λειτουργικό: Windows
DESKTOP-1403ER3

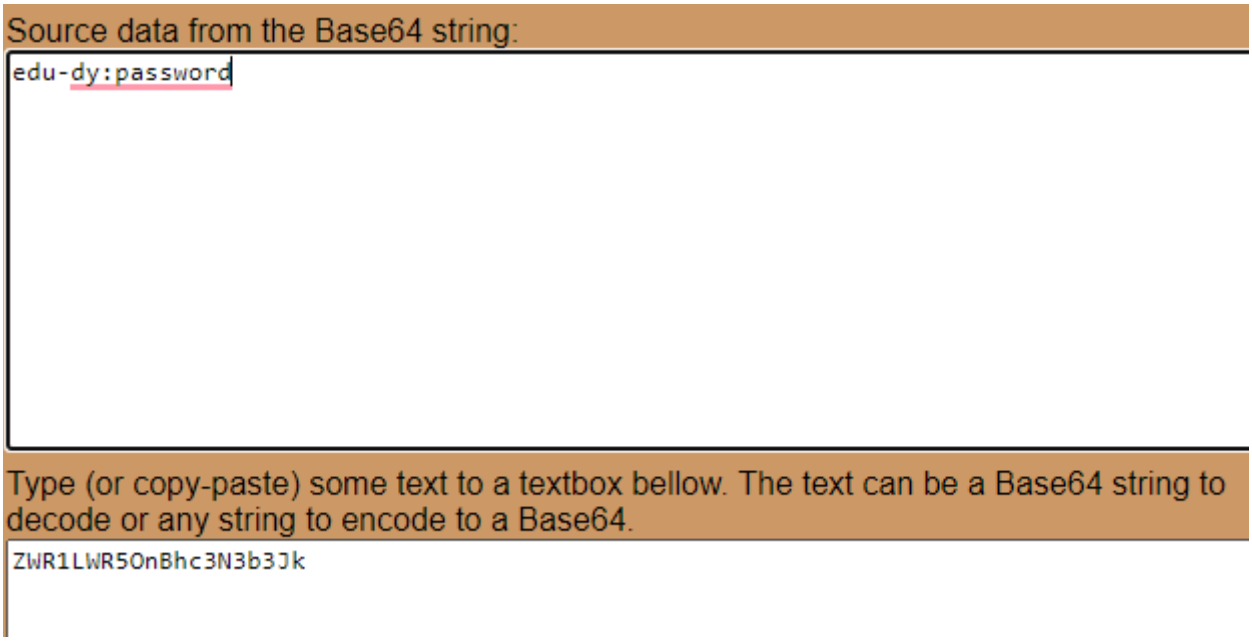
Άσκηση 1

1.1) Έχει status code το 401 και φράση Authorization Required

1.2) Υπάρχουν 2 νέα πεδία, το Connection και το Authorization

1.3) Authorization: Basic ZWR1LWR5OnBhc3N3b3Jk

1.4)



1.5) Ο μηχανισμός ανταλλαγής των credentials που χρησιμοποιείται στο HTTP Base64 είναι πολύ αδύναμος καθώς έχει έλλειψη εμπιστευτικότητας (confidentiality). Οποιοσδήποτε ενδιάμεσος κόμβος μπορεί να μάθει τα στοιχεία ταυτοποίησης του χρήστη

Άσκηση 2

2.1) TCP
2.2)
Source: 62830
Destination: 22
2.3) 22
2.4) ssh
2.5)
Πρωτόκολλο Εξυπηρετητή: SSH-2.0
Έκδοση Λογισμικού: OpenSSH_6.6.1_hpn13v11 FreeBSD-20140420
Σχόλιο: (κενό)
2.6)
Πρωτόκολλο Εξυπηρετητή: SSH-2.0
Έκδοση Λογισμικού: PuTTY_Release_0.76
Σχόλιο: (κενό)
2.7) Το πλήθος τους είναι 10. Οι 2 πρώτοι είναι, οι curve25519-sha256, curve25519-sha256@libssh.org
2.8) Το πλήθος τους είναι 13. Ο πρώτος είναι, ο ecdsa-sha2-nistp256-cert-v01@openssh.com
2.9) Το πλήθος τους είναι 6. Οι 2 πρώτοι είναι, οι chacha20-poly1305@openssh.com, aes128-ctr
2.10) Το πλήθος τους είναι 10. Οι 2 πρώτοι είναι, οι umac-64-etm@openssh.com, umac-128-etm@openssh.com
2.11) Το πλήθος τους είναι 3. Οι 2 πρώτοι είναι, οι none, zlib@openssh.com
2.12) Είναι ο ecdh-sha2-nistp256, και τον εμφανίζει το Wireshark σε παρένθεση δίπλα στο πεδίο Key Exchange. (Key Exchange (method:ecdh-sha2-nistp256))
2.13) Είναι ο ”aes128-ctr”. Βρέθηκε ομοίως με 2.12
2.14) Είναι ο ”umac-64@openssh.com”
2.15) Είναι ο ”none”
2.16) Ναι, σε παρένθεση δίπλα στο πεδίο SSH Version 2. (SSH Version 2 (encryption:aes128-ctr mac:umac-64@openssh.com compression:none))
2.17) Τους εξής, “Elliptic Curve Diffie-Hellman Key Exchange Init”, “Elliptic Curve Diffie-Hellman Key Exchange Reply”, “New Keys”, “Encrypted Packet”
2.18) Όχι, είναι κρυπτογραφημένα
2.19)
Authentication: Με την χρήση public-private keys.
Access control: Με την χρήση public-private keys.
Confidentiality: Με την κρυπτογράφηση των μυνημάτων.
Integrity: Με την συμπίεση compress και Mac.
Privacy: Με την δημιουργία κοινού μυστικού κλειδιού

Άσκηση 3

3.1) host bbb2.cn.ntua.gr
3.2) tcp.flags.syn == 1
3.3)
http: 80
https: 443
3.4)
http: 80
https: 443
3.5) 6 http & 1 https
3.6) 52197
3.7)
Content Type: 1 byte
Version: 2 byte
Length: 2 byte
3.8)
Change Cipher Spec – 20
Handshake – 22
Application Data - 23
3.9)
Client Hello (1)
Server Hello (2)
Certificate
Server Key Exchange
Client Key Exchange
Change Cipher Spec
Encrypted Handshake Message
Server Hello Done
New Session Ticket
3.10) Έστειλε 1 μύνημα Client Hello, αντιστοιχεί σε μια σύνδεση TCP
3.11) TLS 1.2
3.12) 32 bytes [39 78 a1 b4 …] που κανονικα αναπαριστούν τη χρονική στιγμή της αποστολής του πακέτου, πλέον δεν γίνεται (η χρονική στιγμή είναι τυχαία)
3.13) 16 suites & [0x7a7a, 0x1301 …]
3.14)
TLS 1.2
TLS ECDHE RSA WITH AES 256 GCM SHA384 (0xc02f)
3.15) 32 bytes [db 8d d8 d8 …]
3.16) Όχι
3.17)
Αλγόριθμος ανταλλαγής κλειδιών: ECDHE
Πιστοποίησης ταυτότητας: RS

Κρυπτογράφησης: AES_256_GCM
Συνάρτηση κατακερματισμού: SHA384
3.18) 552 bytes
3.19) Μεταφέρονται 4 πιστοποιητικά
GEANT OV RSA CA 4
USERTrust RSA Certification Authority
AAA Certificate Services
AAA Certificate Services
3.20) 5 πλαίσια ethernet
3.21)
Πελάτης:
- Μήκος: 32
- 4df37...
Εξυπηρετητής:
- Μήκος: 32
- 0dcd9...
3.22) 6 bytes
3.23) 45 bytes
3.24) Ναι
3.25) Όχι
3.26) Ακολουθέι τερματισμός της σύνδεσης στην συγκεκριμένη θύρα
3.27) Η αναζήτηση βρίσκει αποτέλεσμα μόνο για το πρωτόκολλο http και όχι για το https
3.28)
Στο πρωτόκολλο HTTPS έχουμε,
Πιστοποίηση της αυθεντικότητας: Με χρήση των certificates.
Εμπιστευτικότητα: Με την κρυπτογράφηση των δεδομένων.
Ακεραιότητα των δεδομένων: Με χρήση των hash functions.

Αντιθέτως, στο HTTP δεν έχουμε τίποτα απο τα παραπάνω.