ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

12^{Ο} ΕΡΓΑΣΤΗΡΙΟ

Σεραφείμ Τζελέπης AM:el18849,

Huawei MateBook 14, Windows 10,

Mac Address: 5C-3A-45-DC-95-1D,

Ομάδα : 4

1)

1.1: 401.

1.2: Το επιπλέον πεδίο είναι το Authorization

1.3: Authorization: Basic ZWR1LWR5OnBhc3N3b3Jk

1.4: edu-dy:password

1.5: Η ασφάλεια του βασικού μηχανισμού πιστοποίησης αυθεντικότητας είναι ελλιπής διότι δεν εξασφαλίζεται η εμπιστευτικότητα καθώς με ένα απλό base64 decoding μπορεί κάποιος να υποκλέψει τον κωδικό του χρήστη.

2)

2.1: Το πρωτόκολλο TCP.

2.2: Source Port: 62156, Destination Port: 22.

2.3: Η θύρα 22.

2.4: Το φίλτρο που χρησιμοποιήθηκε είναι το ‘ssh’.

2.5:

- Έκδοση πρωτόκολλου: SSH-2.0
- Έκδοση λογισμικού:OpenSSH_6.6.1_hpn13v11

- Σχόλιο: FreeBSD-20140420’

2.6:

- Έκδοση πρωτόκολλου: SSH-2.0
- Έκδοση λογισμικού: PuTTy_Release_0.76

2.7: Το πλήθος των kex αλγόριθμων είναι 13, οι δύο πρώτοι είναι οι curve448-sha512, curve25519-sha256.

2.8: Το πλήθος των server host key αλγόριθμων είναι 9, οι δύο πρώτοι είναι οι ssh-ed448, ssh-ed25519.

2.9: Το πλήθος των encryption αλγόριθμων είναι 14, οι δύο πρώτοι είναι οι aes256-ctr, aes256-cbc.

2.10: Το πλήθος των mac αλγόριθμων είναι 8, οι δύο πρώτοι είναι οι hmac-sha2-256, hmac-sha1.

2.11: Το πλήθος των compression αλγόριθμων είναι 3, οι δύο πρώτοι είναι οι none, zlib.

2.12: Key exchange method: curve25519-sha256@libssh.org

2.13: aes256-ctr.

2.14: hmac-sha2-256.

2.15: none.

2.16: Ναι στην παρένθεση δίπλα από το SSH version.

2.17: ‘Elliptic Curve Diffie-Hellman Key Exchange Init’, ‘Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys’, ‘New Keys, Encrypted Packet’, ‘Encrypted Packet’.

2.18: Όχι καθώς είναι κρυπτογραφημένα.

2.19: Το SSH εξασφαλίζει με την χρήση public-private keys την αυθεντικότητα και την εμπιστευτικότητα της υπηρεσίας. Επίσης με την κρυπτογράφηση των μηνυμάτων που χρησιμοποιεί εξασφαλίζεται η ακεραιότητα των δεδομένων κάτι το οποίο είδαμε ότι δεν ισχύει στην περίπτωση του βασικού μηχανισμού πιστοποίησης αυθεντικότητας

3)

3.1: ‘host bbb2.cn.ntua.gr’.

3.2: ‘tcp.connection.syn’.

3.3: Στις θύρες 80 και 443, για http και https αντίστοιχα.

3.4: Όπως προαναφέρθηκε η θύρα 80 είναι για το πρωτόκολλο εφαρμογής http ενώ η θύρα 443 είναι για το πρωτόκολλο εφαρμογής https.

3.5: Έγιναν 3 συνδέσεις για http ενώ 1 για https.

3.6: Source Port: 55573.

3.7:

- Content Type: 1 Byte
- Version: 2 Bytes
- Length: 2 Bytes

3.8:

- Handshake-22
- Change Cipher Spec-20
- Application Data-23

3.9:

- Client Hello
- Server Hello
- Certificate
- Server Key Exchange
- Server Hello Done
- Client Key Exchange
- New Session Ticket
-
- Encrypted Handshake Message

3.10: Έστειλε ένα Client Hello όπως μια είναι η tcp σύνδεση για το https.

3.11: TLS 1.2 (0x0303).

3.12: 32 Bytes. Τα πρώτα 4 είναι 9e 83 0b 3a και στο αρχικό TLS 1.2 τα πρώτα 4 Bytes έπρεπε να είναι η ημερομηνία και η ώρα του πελάτη.

3.13: Το πλήθος τους είναι 16 και οι δεκαεξαδικές τιμές των πρώτων δύο είναι:

- Reserved (GREASE): 0x7a7a
- TLS_AES_128_GCM_SHA256: 0x1301

3.14: Η έκδοση που θα χρησιμοποιηθεί είναι η TLS 1.2 και η σουίτα κωδικών κρυπτογράφησης είναι η TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 με δεκαεξαδική τιμή 0xc02f.

3.15: 32 Bytes. Τα πρώτα 4 είναι 6f 39 b0 5b.

3.16: Όχι, η τιμή του πεδίου είναι NULL.

3.17:

- Key exchange/agreement: EDCHE
- Authentication: RSA
- Block/stream ciphers: AES_128_GCM
- Message authentication: SHA256

3.18: 4278 Bytes.

3.19: Μεταφέρονται τρία πιστοποιητικά, τα ονόματα τους δεν αναγράφονται.

3.20: 4 πλαίσια.

3.21: Το κλειδί που αποστέλλει ο πελάτης έχει μήκος 32 Bytes τα πρώτα 4 είναι τα 3c 32 4d a3, ενώ το κλειδί που αποστέλλει ο εξυπηρετητής έχει επίσης μήκος 32 Bytes και τα πρώτα 4 Bytes είναι τα 63 11 87 f3.

3.22: 6 Bytes.

3.23: 45 Bytes.

3.24: Ναι.

3.25: Όχι.

3.26: Δεν υπάρχουν.

3.27: Η αναζήτηση βρίσκει αποτελέσματα μόνο για http πρωτόκολλο.

3.28: Το πρωτόκολλο HTTPS παρέχει εμπιστευτικότητα με την κρυπτογράφηση των δεδομένων , πιστοποίηση της αυθεντικότητας με την χρήση των certificates καθώς και ακεραιότητα των δεδομένων με τη χρήση των hash functions. Κανένα από τα παραπάνω δεν συναντώνται στο HTTP.