$12^ο$ Εργαστήριο στα Δίκτυα Υπολογιστών
Ασφάλεια

Όνοματεπώνυμο: **Αλέξανδρος Κυριακάκης (03112163)**
Ομάδα: **2**
Όνομα PC/ΛΣ: **MacBook Pro - Alexandros, macOS Big Sur**
Ημερομηνία: **8/1/2021**
Διεύθυνση IP: **192.168.1.3**
Διεύθυνση MAC: **a4:83:e7:97:af:31**

1 Πιστοποίηση αυθεντικότητας στο πρωτόκολλο HTTP

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 edu-dy:password

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.

2 Υπηρεσία SSH – Secure SHell

2.1 Το TCP.

2.2

- Source (My Mac): 49798
- Destination (Server): 22

2.3 Η Θύρα 22.

2.4 Χρησιμοποίησα το "ssh".

2.5

- Η έκδοση πρωτοκόλλου του εξυπηρετητή είναι: "SSH-2.0"
- Η έκδοση του λογισμικού: "OpenSSH_5.8p2_hpn13v11"
- Το σχόλιο: "FreeBSD-20110503"

2.6

- Η έκδοση πρωτοκόλλου του εξυπηρετητή είναι: "SSH-2.0"
- Η έκδοση του λογισμικού: "OpenSSH_8.1"
- Το σχόλιο: ""

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.

3 Υπηρεσία HTTPS

3.1 Είναι "host my.ntua.gr".

3.2 Είναι "tcp.flags.syn == 1".

3.3 Για την http έγινε στην θύρα 80, ενώ για την https στην 443.

3.4 Βλέπε 3.3.

3.5 Στην http έγιναν 7 συνδέσεις, ενώ για την https έγιναν 6 συνδέσεις.

3.6 Είναι οι, 55643, 55644, 55647, 55648, 55649, 55650.

3.7 Είναι τα,

- Content Type: 1 byte
- Version: 2 bytes
- Length: 2 bytes

3.8 Είναι τα,

- Change Cipher Spec – 20
- Alert - 21
- Handshake - 22
- Application - 23

3.9 Είναι τα,

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

3.10 Έστειλε 6 μυνήματα Client Hello, κάθε ένα αντιστοιχεί σε μια σύνδεση TCP.

3.11 Η TLS 1.2 .

3.12 Είναι 32 bytes, ενώ τα πρώτα 4 (a0 9a 51 e8) που κανονικα αναπαριστούν τη χρονική στιγμή της αποστολής του πακέτου, πλέον δεν γίνεται (η χρονική στιγμή είναι τυχαία).

3.13 Είναι 18 suites σε πλήθος και οι δεκαεξαδικές τιμές των 2 πρώτων είναι 0x1301 και 0x1303

3.14 Η έκδοση που θα χρησιμοποιηθεί είναι η TLS 1.2 ενώ η σουίτα κωδικών κρυπτογράφησης είναι η Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030).

3.15 Είναι 32 bytes, ενώ τα πρώτα 4 bytes του τυχαίου μέρους είναι τα (f3 be ff 4f).

3.16 Όχι.

3.17 Είναι,

- Αλγόριθμος ανταλλαγής κλειδιών: ECDHE
- Πιστοποίησης ταυτότητας: RSA
- Κρυπτογράφησης: AES_256_GCM
- Συνάρτηση κατακερματισμού: SHA384

3.18 Είναι 6304 bytes.

3.19 Μεταφέρονται 4 πιστοποιητικά. Τα,

- GEANT OV RSA CA 4
- USERTrust RSA Certification Authority
- AAA Certificate Services
- AAA Certificate Services

3.20 Χρειάστηκαν 5 πλαίσια ethernet.

3.21 Είναι,

- Πελάτης,
  - Μήκος κλειδιού: 65 bytes
  - 5 πρώτα γράμματα: ”045ba”
- Εξυπηρετητής,
  - Μήκος κλειδιού: 65 bytes.
  - 5 πρώτα γράμματα: ”0479a”

3.22 Είναι 6 bytes.

3.23 Είναι 45 bytes.

3.24 Ναι.

3.25 Ναι παρατήρησα και πο τις 2 πλευρές.

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.