12ο Εργαστήριο Δίκτυα Υπολογιστών
Ονοματεπώνυμο: Βλαχάκης Νικόλαος (el18441) Ομάδα: 4
΄Ονομα PC/ΛΣ: DESKTOP-91TTTR6, Windows
Ημερομηνία: 11/1/2022
Διεύθυνση IP: 192.168.1.7
Διεύθυνση MAC: 9C-B6-D0-E8-2C-EB

Άσκηση 1)

1.1) Status code 401 και Authorization Required.

1.2) Σε σχέση με το προηγούμενο request υπάρχουν επίσης 1 νέο πεδίο, το Authorization.

1.3) Authorization: Basic ZWR1LWR5OnBhc3N3b3Jk\r\n

1.4) edu-dy:password

1.5) Ο μηχανισμός ανταλλαγής των μηνυμάτων που χρησιμοποιείται στο HTTP Base64 στερείται ασφάλειας καθώς ένας κακόβουλος χρήστης μπορεί να δεί οποιαδήποτε πληροφορία.

Άσκηση 2)

2.1) χρησιμοποιεί TCP.

2.2) Source: 55653, Destination: 22

2.3) Η θύρα 22.

2.4) ssh

2.5)
έκδοση του πρωτοκόλλου SSH : SSHv2
έκδοση λογισμικού : Protocol (SSH-2.0-OpenSSH_6.6.1_hpn13v11
σχόλια : FreeBSD-20140420

2.6)
έκδοση του πρωτοκόλλου SSH : SSHv2
έκδοση λογισμικού : Protocol (SSH-2.0-PuTTY_Release_0.76)
σχόλια: ‘’

2.7) Το πλήθος τους είναι 14 και οι πρώτοι δύο είναι :
`curve448-sha512,curve25519-sha256`

2.8) Το πλήθος τους είναι 9 και οι δύο πρώτοι είναι :
`ssh-ed25519,ssh-ed448`

2.9) Οι δύο πρώτοι είναι aes256-ctr,aes256-cbc.

2.10) Οι δύο πρώτοι είναι hmac-sha2-256,hmac-sha1.

2.11) Οι δύο πρώτοι είναι none,zlib

2.12) Είναι ο αλγόριθμος που βρίσκεται δίπλα στο Key Exchange , δηλαδή (method:curve25519-sha256@libssh.org)

2.13) Είναι aes256-ctr.

2.14) Είναι hmac-sha2-256

2.15) Είναι none

2.16) Ναι τους εμφανίζει στην παένθεση δίπλα στο SSH version2

2.17) ”Elliptic Curve Diffie-Hellman Key Exchange Init”, ”Elliptic Curve Diffie-Hellman Key Exchange Reply”, ”New Keys”, ”Encrypted Packet”.

2.18) Όχι γιατί είναι κρυπτογραφημένα.

2.19)
- Authentication,Access control: Με την χρήση public-private keys.
- Confidentiality: Με κρυπτογράφηση των μυνημάτων.
- Integrity: Με συμπίεση compress και Mac.
- Privacy: Με δημιουργία κοινού μυστικού κλειδιού.

Άσκηση 3)

3.1) host bbb2.cn.ntua.gr

3.2) tcp.flags.syn == 1 and tcp.flags.ack == 0

3.3) Για http η 80 και για https η 443.

3.4) απάντηση 3.3

3.5) Στην περίπτωση HTTP → 3 συνδέσεις και στην περίπτωση HTTPS → 1 σύνδεση.

3.6) Η μοναδική θύρα πηγής είναι η 62335.

3.7) Είναι τα : Content Type: 1 byte, Version: 2 bytes, Length: 2 bytes

3.8) Είναι τα : Handshake - 22 , Application - 23 .

3.9) Είναι τα : Client Hello(1), Server Hello(2), Certificate(11), Client Key Exchange(16)

3.10) Έστειλε ένα μήνυμα Client Hello και αυτό αντιστοιχεί σε μία tcp σύνδεση.

3.11) Η TLS 1.0

3.12) Είναι 32 bytes και τα 4 πρώτα είναι (f4 ce 61 be) και αναπαριστούν την χρονική στιγμή παράδοσης του πακέτου.

3.13) Υποστηρίζει 16 suites και οι δύο πρώτες είναι :
0x5a5a και 0x1301

3.14) Θα χρησιμοποιηθεί η έκδοση TLS 1.2, με όνομα
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
και δεκαεξαδική τιμή (0xc02f)

3.15) Είναι 32 Bytes και τα πρώτα 4 είναι (9a c7 a7 d6)

3.16) Όχι δεν χρησιμοποιείται.

3.17) Αλγόριθμος ανταλλαγής κλειδιών → ECDHE, Πιστοποίησης ταυτότητας → RSA Κρυπτογράφησης → AES 256 GCM, Συνάρτηση κατακερματισμού → SHA384

3.18) Είναι 4283 Bytes.

3.19) Μεταφέρονται 3 certificates τα οποία είναι : bbb2.cn.ntua.gr, R3, ISRG Root X1

3.20) Χρειάστηκαν 4 πλαίσια ethernet.

3.21) Το μήκος του public key που αποστέλλει ο σερβερ είναι 32 Bytes και τα 5 πρώτα γράμματα είναι 3e6d1. Στην άλλη περίπτωση ομοίως είναι 32 Bytes και τα 5 πρώτα γράμματα είναι 742ef.

3.22) Το μήκος είναι 6 Bytes.

3.23) Το μήκος είναι 45 Bytes.

3.24) Ναι παρατήρησα.

3.25) Όχι δεν παρατήρησα.

3.26) Υπάρχει λήξη σύνδεσης.

3.27) Παρατηρώ ότι η αναζήτηση βρίσκει αποτέλεσμα μόνο στην περίπτωση HTTP protocol.

3.28) Στο HTTPS protocol έχουμε πιστοποίηση της αυθεντικότητας μέσω των certificates, εμπιστευτικότητα μέσω της κρυπτογράφησης δεδομένων και ακεραιότητα των δεδομένων μέσω των hash functions. Στην περίπτωση του HTTP protocol δεν έχουμε τίποτα από αυτά.