Ονοματεπώνυμο: Χρήστος Τσούφης			**Ομάδα:** 2
Όνομα PC/ΛΣ: DESKTOP-EUMLCMA/Windows 10		**Ημερομηνία:**	07/01/2021
Διεύθυνση IP: 192.168.1.3	**Διεύθυνση MAC:**	34-F6-4B-07-39-B5	

Εργαστηριακή Άσκηση 12
Ασφάλεια

1

1.1 Ο αριθμητικός κωδικός κατάστασης (status code) είναι: 401

Η φράση που επιστρέφει ο εξυπηρετητής ως απόκριση στο αρχικό μήνυμα HTTP τύπου GET του πλοηγού ιστού είναι: Authorization Required

1.2 Συγκρίνοντας το δεύτερο με το πρώτο μήνυμα HTTP GET, το επιπλέον πεδίο που περιλαμβάνει η επικεφαλίδα HTTP είναι: Authorization

1.3 Το περιεχόμενο του παραπάνω πεδίου όπως αυτό εμφανίζεται στο παράθυρο με τα περιεχόμενα του επιλεγμένου πλαισίου σε μορφή ASCII είναι:

Basic ZWRILWR 50nBnc3N3b3JK

1.4 Το αποτέλεσμα της αποκωδικοποίησης είναι: edu-dy : password

1.5 Το συμπέρασμα που προκύπτει για την ασφάλεια του βασικού μηχανισμού πιστοποίησης αυθεντικότητας που παρέχει το HTTP είναι το εξής:

Δεν προσφέρει confidentiality καθώς τα δεδομένα μόνο κωδικοποιούνται, δεν κρυπτογραφούνται.

2

2.1 Το SSH χρησιμοποιεί το πρωτόκολλο μεταφοράς: TCP

2.2 Οι θύρες του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την επικοινωνία μεταξύ του υπολογιστή και του edu-dy.cn.ntua.gr είναι:

Src: 1315/3320 (?) Dst: 22

2.3 Από τις παραπάνω θύρες, αυτή που αντιστοιχεί στο πρωτόκολλο εφαρμογής SSH είναι: Port 22

2.4 Η σύνταξη του φίλτρου είναι: ssh

2.5 Ο εξυπηρετητής χρησιμοποιεί την έκδοση του πρωτοκόλλου SSH 2.0 και την έκδοση λογισμικού OpenSSH_S.8p2_hpn13x11 FreeBSD. Περιλαμβάνονται σχόλια στο αναγνωριστικό αυτό: 20110503.

2.6 Ο πελάτης χρησιμοποιεί την έκδοση του πρωτοκόλλου SSH 2.0 και την έκδοση λογισμικού Putty_Release_060. Δεν περιλαμβάνονται σχόλια στο αναγνωριστικό αυτό.

2.7 Το πλήθος τους είναι: 4

Οι πρώτοι δύο είναι: Diffie-hellman group-exchange-aes256

2.8 Το πλήθος τους είναι: 2

Ο πρώτος είναι: ssh-_54

2.9 Οι δύο πρώτοι είναι: aes256-ctr & aes256-cbc

2.10 Οι δύο πρώτοι είναι: hmac-shal & hmac-shal-96

2.11 Οι δύο πρώτοι είναι: none, zlib

2.12 Ο αλγόριθμος ανταλλαγής κλειδιών που θα ακολουθήσουν τα δύο μέρη εμφανίζεται στο Wireshark στο: Diffie-hellman-group-exchangr-shal

2.13 Αυτός που τελικά θα χρησιμοποιηθεί είναι: aes256-cbc

2.14 Αυτός που τελικά θα χρησιμοποιηθεί είναι:

2.15 Αυτός που τελικά θα χρησιμοποιηθεί είναι:

2.16 Το Wireshark εμφανίζει τους επιλεχθέντες αλγορίθμους κρυπτογράφησης πιστοποίησης αυθεντικότητας μηνυμάτων και συμπίεσης στο σημείο:

2.17 Καταγράφηκαν οι εξής τύποι μηνυμάτων SSH:

2.18 Τα πακέτα όπου μεταφέρεται η πληροφορία για την προτροπή login & password στην περίπτωση του SSH δεν εντοπίζονται διότι μεταδίδονται μεταξύ των 2 υπολογιστών κρυπτογραφημένα.

2.19 Η ασφάλεια της υπηρεσίας SSH όσον αφορά την πιστοποίηση της αυθεντικότητας, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων σε σύγκριση με άλλα πρωτόκολλα ανταλλαγής δεδομένων είναι :

Το ssh καθιστά ασφαλή τη σύνδεση αφού χρησιμοποιεί κρυπτογράφηση άρα και διασφαλίζει την ακεραιότητα των δεδομένων που πρέπει να μεταδοθούν καθώς και την εμπιστευτικότητα. Τέλος, η κρυπτογράφηση δημόσιου κλειδιού πιστοποιεί την αυθεντικότητα των δύο πλευρών.

3

3.1 Η σύνταξη του φίλτρου σύλληψης είναι: host my.ntua.gr

3.2 Η σύνταξη του φίλτρου απεικόνισης είναι: tcp.flags.syn == 1 and tcp.flags.ack == 0

3.3 Οι συνδέσεις του εξυπηρετητή my.ntua.gr γίνονται στις πασίγνωστες θύρες: 80 & 443

3.4 Στο πρωτόκολλο εφαρμογής HTTP αντιστοιχεί η θύρα: 80

Στο πρωτόκολλο εφαρμογής HTTPS αντιστοιχεί η θύρα: 443

3.5 Ανοίχθηκαν 6 συνδέσεις μεταξύ του υπολογιστή και του εξυπηρετητή ιστού my.ntua.gr στην περίπτωση του HTTP και 6 συνδέσεις στην περίπτωση HTTPS.

3.6 Για τις συνδέσεις TCP της περίπτωσης HTTPS οι θύρες πηγής είναι:

3.7 Τα πεδία αυτά είναι: Content Type: 1 byte, Version: 2 bytes, Length: 2 bytes

3.8 Οι τιμές για όλες τις εγγραφές TLS που έχουν καταγραφεί είναι:

20 – Change Gipher Spec

21 – Alert

22 – Handshake

23 – Application Data

3.9 Οι διαφορετικοί τύποι μηνυμάτων χειραψίας που παρατηρήθηκαν είναι:

3.10 Ο πελάτης έστειλα μηνύματα Client Hello και η σχέση τους με τις συνδέσεις TCP που καταγράφηκαν είναι:

3.11 Η μέγιστη έκδοση TLS που υποστηρίζεται από τον πελάτη είναι: TLS 1.2 (Handshake)

3.12 Το μήκος του τυχαίου αριθμού που περιέχει, είναι: 32 & 28

Τα πρώτα 4 byte είναι: 09 cc 32 f4 (?) και παριστάνουν την ημερομηνία.

3.13 Το πλήθος τους είναι: 15

Οι δεκαεξαδικές τιμές των δύο πρώτων είναι: 0xc02b, 0xc02f

3.14 Η έκδοση TLS που χρησιμοποιήθηκε είναι: TLS 1.2

Το όνομα και η δεκαεξαδική τιμή της σουίτας κωδικών κρυπτογράφησης που επιλέχθηκε είναι: 0x1030

3.15 Το μήκος του τυχαίου αριθμού που περιέχει, είναι: 32 & 28

Τα πρώτα 4 byte είναι: 37 a6 d5 90

3.16 Δεν χρησιμοποιείται κάποια μέθοδος συμπίεσης από τον εξυπηρετητή και τον πελάτη.

3.17 Οι αλγόριθμοι ανταλλαγής κλειδιών ECDH, πιστοποίησης ταυτότητας RSA, κρυπτογράφησης AES 256 και η συνάρτηση κατακερματισμού SHA 784 που επιλέχτηκαν είναι:

3.18 Το μήκος της σύμφωνα με το πεδίο length της επικεφαλίδας είναι: 5207 bytes

3.19 Μεταφέρονται 4 πιστοποιητικά. Τα ονόματά τους είναι:

My.ntua.gr

TERENA SLL CA

MTN-USER First-Hardware

Add Trust External CA Root

3.20 Χρειάστηκαν 4 πλαίσια Ethernet.

3.21 Το μήκος του δημόσιου κλειδιού που αποστέλλει ο πελάτης 65 είναι και του εξυπηρετητή είναι 65:

Τα 5 πρώτα γράμματα αμφότερων των κλειδιών είναι:

04 76 19 b6 b9

04 76 0A 4f 60

3.22 Το μήκος της εγγραφής TLS είναι: 8 bytes

3.23 Το μήκος της εγγραφής TLS είναι: 40 bytes

3.24 Παρατηρήθηκαν εγγραφές TLS με την υπόδειξη από την πλευρά του εξυπηρετητή.

3.25 Παρατηρήθηκαν εγγραφές TLS του πρωτοκόλλου Alert από την πλευρά

3.26 Υπάρχουν διότι

3.27 Στην περίπτωση του πρωτοκόλλου HTTP σε σύγκριση με αυτή του HTTPS παρατηρείται ότι στο HTTP εντοπίζονται τα πακέτα αμέσως ενώ στο HTTPS όχι καθώς τα δεδομένα είναι κρυπτογραφημένα.

3.28 Η ασφάλεια του πρωτοκόλλου HTTPS σε σύγκριση με το απλό HTTP, όσον αφορά την πιστοποίηση της αυθεντικότητας, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων αναλύεται παρακάτω. Το HTTPS παρέχει αυθεντικότητα για τα δεδομένα που επισκέπτεται καθώς και εμπιστευτικότητα και ακεραιότητα δεδομένων. Αυτό επιτυγχάνεται με την αμφίδρομη κωδικοποίηση των δεδομένων και του αλγορίθμου κατακερματισμού και ανταλλαγή κλειδιών που χρησιμοποιούνται σε αντίθεση με το απλό HTTP.