Ονοματεπώνυμο: ΔΗΜΗΤΡΙΟΣ ΓΕΩΡΓΟΥΣΗΣ	ΑΜ: 03119005	Ομάδα: 4
Όνομα PC/ΛΣ: dimitris-Laptop / WINDOWS 11 HOME	Ημερομηνία: 10/01/2023	
Διεύθυνση IPv4: 147.102.131.22	Διεύθυνση MAC: 00-FF-D3-16-94-03	

Εργαστηριακή Άσκηση 12

Ασφάλεια

1. Πιστοποίηση αυθεντικότητας στο πρωτόκολλο HTTP

1.1: Status Code: 401, Response Phrase: Authorization Required

1.2: WWW-Authenticate (όνομα επικεφαλίδας) και υποδεικνύει τη μέθοδο Basic

1.3: Authorization

1.4: Authorization: Basic ZWR1LWR5OnBhc3N3b3Jk (η συμβολοσειρά μετά το "Basic" είναι τα διαπιστευτήρια)

1.5: Η συμβολοσειρά "ZWR1LWR5OnBhc3N3b3Jk" έδωσε αποτέλεσμα "edu-dy:password"

1.6: Το HTTP απλώς κωδικοποιήθηκαν, οπότε δεν παρέχει εμπιστευτικότητα

2. Υπηρεσία SSH – Secure SHell

2.1: TCP

2.2: υπολογιστής μου → edu-dy.cn.ntua.gr: 64778 → 22
edu-dy.cn.ntua.gr → υπολογιστής μου: 22 → 64778

2.3: Η θύρα 22 αντιστοιχεί στο SSH

2.4: ssh

2.5: Protocol: SSH-2.0-OpenSSH_6.6.1_hpn13v11 FreeBSD-20140420

Πρωτόκολλο: SSH-2.0, Λογισμικό: OpenSSH_6.6.1_hpn13v11, Σχόλια: FreeBSD-20140420

2.6: Protocol: SSH-2.0-PuTTY_Release_0.78

Πρωτόκολλο: SSH-2.0, Λογισμικό: PuTTY_Release_0.78

2.7: Πλήθος 19 , Πρώτοι 2: sntrup761x25519-sha512@openssh.com και curve448-sha512 (kex)

2.8: Πλήθος: 9, Πρώτοι 2: ssh-ed448 και ssh-ed25519 (server-host key)

2.9: aes256-ctr και aes256-cbc (encryption)

2.10: hmac-sha2-256 και hmac-sha1 (mac)

2.11: none, zlib

2.12: curve25519-sha256@libssh.org. Το Wireshark τον εμφανίζει μέσα σε παρενθέσεις στο πεδίο Key Exchange

2.13: aes256-ctr (encryption)

2.14: hmac-sha2-256 (mac)

2.15: none (compression)

2.16: Ναι, στην επικεφαλίδα SSH Version 2 μέσα σε παρενθέσεις

2.17: Elliptic Curve Diffie-Hellman Key Exchange Init
Elliptic Curve Diffie-Hellman Key Exchange Reply
New Keys

2.18: Μπορούμε να δούμε τα πακέτα που στείλαμε/λάβαμε αλλά δεν βλέπουμε το περιεχόμενό τους, γιατί είναι κρυπτογραφημένο

2.19: Όπως αναφέρει και στην εκφώνηση το SSH είναι ένα ασφαλές πρωτόκολλο που επιτρέπει την ανταλλαγή δεδομένων σε σχέση με το telnet (που έχουμε δει σε άλλη άσκηση). Πετυχαίνει κρυπτογράφηση των δεδομένων, παρέχει πιστοποίηση αυθεντικότητας και εμπιστευτικότητα, ακεραιότητα στα μεταφερόμενα δεδομένα

3. Υπηρεσία HTTPS

3.1: Φίλτρο σύλληψης: host bbb2.cn.ntua.gr

3.2: Φίλτρο απεικόνισης:
tcp.flags.syn==1 or (tcp.seq==1 and tcp.ack==1 and tcp.len==0 and tcp.analysis.initial_rtt)

3.3: Στις θύρες 80 και 443

3.4: HTTP: 80, HTTPS: 443

3.5: Βλέπω 6 HTTP συνδέσεις και 1 HTTPS σύνδεση

3.6: Για την TCP του HTTPS η θύρα πηγής είναι η 1115

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: Version: TLS 1.0 (0x0301) και Version: TLS 1.2 (0x0303)

3.10: Client Hello (1)
Server Hello (2)
Certificate (11)
Server Key Exchange (12)
Server Hello Done (14)
Client Key Exchange (16)
Encrypted Handshake Message
New Session Ticket (4)

3.11: Έστειλε 1 μήνυμα. Κάθε μήνυμα αντιστοιχεί σε μία σύνδεση TCP. Στην περίπτωσή μου έγινε 1 σύνδεση

3.12: Η εγγραφή TLS δηλώνει Version: TLS 1.0 (0x0301) ενώ το μήνυμα που μεταφέρει δηλώνει Version: TLS 1.2 (0x0303). Δεν ταυτίζονται

3.13: Δεν υπάρχει το "supported_versions" extensions

3.14: Δηλώνονται τα h2, http/1.1

3.15: Είναι 32 bytes. Πρώτα 4 bytes: b5 4e 52 e1. Παριστάνουν την ημερομηνία και ώρα που στάλθηκε το μήνυμα (αν και όχι πάντα από ό,τι διάβασα, δεν ξέρω αν παριστάνουν όντως αυτό στην περίπτωσή μου)

3.16: #(Cipher Suites) = 15
Πρώτες 2: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b), TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

3.17: Version: TLS 1.2 (0x0303)

3.18: 32 bytes. Πρώτα 4 bytes: Random: 17 e9 a8 c8. Έβαλα και τους δύο αριθμούς σε timestamp to human readable form converter και δεν νομίζω στην περίπτωσή μου να χρησιμοποιήθηκαν όντως ημερομηνίες. Ο τρόπος που παράγονται είναι απλά τυχαίοι αριθμοί

3.19: Όχι (Compression Method: null (0))

3.20:	Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
	Key Exchange	Diffie – Hellman
	Authentication	RSA
	Encryption	AES 128 GCM
	Hash Function	SHA 256

3.21: Length: 4276

3.22: Μεταφέρονται 3 πιστοποιητικά με μήκη 1576, 1306, 1380

3.23: Χρειάστηκαν 4

3.24: Εντοπίστηκαν τα μηνύματα αυτά. Τα κλειδιά έχουν μήκος 32 bytes

	Πελάτης	Εξυπηρετητής
5 πρώτα γράμματα	4cd2d	73065

3.25: Είναι 6 bytes και το αντίστοιχο TLS μήνυμα έχει μήκος 93 bytes, αλλά μεταφέρει και άλλα records

3.26: Είναι 45 bytes μαζί με την επικεφαλίδα του, το περιεχόμενό του είναι 40 bytes

3.27: Ναι

3.28: Του πρωτοκόλλου HTTP 2

3.29: Δεν παρατηρήθηκαν

3.30: Not Answered

3.31: Στο HTTP βρίσκουμε την φράση που αναζητούμε, ενώ στο HTTPS δεν βρίσκουμε τη φράση σε κάποιο πακέτο

3.32: Οι 3 αυτές ιδιότητες συναντώνται στο HTTPS έναντι του HTTP. Το HTTPS είναι πιο ασφαλές