

Εργαστηριακή Άσκηση 12

Ασφάλεια

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΚΟΥΣΤΕΝΗΣ ΧΡΙΣΤΟΣ (03120227)

ΟΜΑΔΑ: 3

ΟΝΟΜΑ PC/ΛΣ: LAPTOP-TK5Q3T95 / WINDOWS 11

ΗΜΕΡΟΜΗΝΙΑ: 9/1/2024

ΔΙΕΥΘΥΝΣΗ IP: 192.168.1.14 / 147.102.131.22

ΔΙΕΥΘΥΝΣΗ MAC: B4-B5-B6-79-4B-09

1. Πιστοποίηση αυθεντικότητας στο πρωτόκολλο HTTP

Με τη βοήθεια του Wireshark, καταγράψτε την κίνηση ενώ κάνετε χρήση της υπηρεσίας HTTP του υπολογιστή edu-dy.cn.ntua.gr (147.102.40.15). Εφαρμόστε φίλτρο σύλληψης host 147.102.40.15 για να παρατηρείτε μόνο την κίνηση που σχετίζεται με αυτόν. Ξεκινήστε μία καταγραφή κίνησης και επισκεφτείτε τη σελίδα <http://edu-dy.cn.ntua.gr/auth/>. Η πρόσβαση σε αυτή τη σελίδα απαιτεί την επαλήθευση της ταυτότητάς σας. Δώστε edu-dy στο πεδίο του ονόματος χρήστη (user name) και password στο πεδίο του μυστικού κωδικού (password). Σταματήστε την καταγραφή.

1.1 Να καταγραφεί ο αριθμητικός κωδικός κατάστασης (status code) και η φράση που επιστρέφει ο εξυπηρετητής ως απόκριση στο αρχικό αίτημα HTTP τύπου GET του πλοηγού ιστού.

Response Phrase: Authorization Required

Status Code: 401

1.2 Στην απόκριση ο εξυπηρετητής υποδεικνύει τη μέθοδο (scheme) πιστοποίησης αυθεντικότητας που πρέπει να χρησιμοποιήσει ο πλοηγός ώστε να επιτραπεί η πρόσβαση. Ποιο είναι το όνομα της σχετικής επικεφαλίδας HTTP και ποια μέθοδο υποδεικνύει; [Υποδ. Δείτε κατάλογο των διαθέσιμων μεθόδων στην ιστοθέση <https://www.iana.org/assignments/http-authschemes/httpauthschemes.xhtml>.]

WWW-Authenticate: Basic realm="Edu-DY TEST"

1.3 Ο πλοηγός ιστού συμμορφούμενος με την υπόδειξη στέλνει δεύτερο αίτημα HTTP τύπου GET στον εξυπηρετητή όπου περιλαμβάνει τα διαπιστευτήριά του. Ποιο είναι το όνομα της σχετικής επικεφαλίδας HTTP;

Authorization

1.4 Το περιεχόμενο της επικεφαλίδας περιλαμβάνει τη μέθοδο πιστοποίησης αυθεντικότητας που βρήκατε στην ερώτηση 1.2 καθώς και τα σχετικά διαπιστευτήρια. Καταγράψτε τα όπως αυτά εμφανίζονται στο παράθυρο με τα περιεχόμενα του επιλεγμένου πλαισίου σε μορφή ASCII. Τα στοιχεία πιστοποίησης αυθεντικότητας που καταχωρήσατε στον πλοηγό δεν κρυπτογραφήθηκαν για να αποσταλούν στον εξυπηρετητή, απλώς κωδικοποιήθηκαν σύμφωνα με μια πολύ γνωστή μέθοδο, τη Base64.

Basic ZWR1LWR5OnBhc3N3b3Jk

1.5 Επισκεφτείτε την ιστοσελίδα <https://www.base64encode.org/>, επιλέξτε το Decode στην κορυφή της σελίδας και εισάγετε στο παράθυρο που θα εμφανισθεί τα διαπιστευτήρια που καταγράψατε στο ερώτημα 1.4. Αποκωδικοποιήστε το περιεχόμενό τους κάνοντας κλικ στο κουμπί “DECODE” και καταγράψτε το αποτέλεσμα. [Σημείωση: Το Wireshark αυτομάτως εκτελεί την αποκωδικοποίηση αυτή. Μπορείτε να δείτε το αποτέλεσμα κάνοντας διπλό κλικ στο πεδίο “Authorization: Basic” της επικεφαλίδας HTTP.]

BASE64
Decode and Encode Encode

Language: Eng

Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or **decode** your data.

Decode from Base64 format
Simply enter your data then push the decode button.

ZWR1LWR5OnBhc3N3b3Jk\r\n

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

Source character set: ASCII

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

edu-dy:password

Decoding result: edu-dy:password

1.6 Τι συμπεραίνετε για την ασφάλεια του βασικού μηχανισμού πιστοποίησης αυθεντικότητας που παρέχει το HTTP; [Υπόδ.: https://en.wikipedia.org/wiki/Basic_access_authentication.]

Το HTTP Basic authentication (BA) είναι η απλούστερη τεχνική για την επιβολή ελέγχων πρόσβασης σε πόρους ιστού, επειδή δεν απαιτεί cookies, αναγνωριστικά περιόδου σύνδεσης ή σελίδες σύνδεσης. Αντίθετα, ο βασικός έλεγχος ταυτότητας HTTP χρησιμοποιεί τυπικά πεδία στην κεφαλίδα HTTP. Ωστόσο ο μηχανισμός αυτός δεν παρέχει προστασία εμπιστευτικότητας για τα διαβιβαζόμενα διαπιστευτήρια. Απλώς κωδικοποιούνται με Base64 κατά τη μεταφορά και δεν κρυπτογραφούνται ή κατακερματίζονται με οποιονδήποτε τρόπο. Επομένως, ο βασικός έλεγχος ταυτότητας χρησιμοποιείται συνήθως σε συνδυασμό με το HTTPS για την παροχή εμπιστευτικότητας.

2. Υπηρεσία SSH – Secure Shell

Για αυτό το μέρος της άσκησης θα πρέπει να είστε συνδεδεμένοι στο εσωτερικό δίκτυο του ΕΜΠ. Καταγράψτε με τη βοήθεια του Wireshark την κίνηση ενώ κάνετε χρήση της υπηρεσίας SSH του υπολογιστή edu-dy.cn.ntua.gr. Όπως πριν, εφαρμόστε φίλτρο σύλληψης host 147.102.40.15 για να παρατηρείτε μόνο την κίνηση που σχετίζεται με αυτόν και ξεκινήστε την καταγραφή. Στο πεδίο Host Name του παραθύρου που ανοίγει όταν εκτελέσετε το PuTTY, πληκτρολογήστε edu-dy.cn.ntua.gr, στη συνέχεια κάνετε κλικ στο πρωτόκολλο SSH και τέλος στο κουμπί Open. Αν ενδεχομένως ανοίξει κάποιο παράθυρο διαλόγου, επιλέξτε Yes για να προχωρήσετε. Στην προτροπή login: πληκτρολογήστε abcd ως όνομα χρήστη ακολουθούμενο από , ενώ στην προτροπή Password: πληκτρολογήστε efgh ως κωδικό ακολουθούμενο από . Σε συστήματα Linux/Unix σε παράθυρο γραμμής εντολών γράψτε ssh abcd@147.102.40.15 και συνεχίστε δίνοντας τον κωδικό. Σημειώνεται ότι ο χρήστης abcd δεν υπάρχει στον συγκεκριμένο εξυπηρετητή και η αναγνώριση του χρήστη θα αποτύχει. Πληκτρολογήστε +c για να κλείσει το παράθυρο και σταματήσετε την καταγραφή κίνησης.

2.1 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το SSH (TCP ή UDP);
TCP

2.2 Καταγράψτε τις θύρες του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την επικοινωνία μεταξύ του υπολογιστή σας και του edu-dy.cn.ntua.gr.

Port : 61813(από το άκρο του υπολογιστή μας)

Port : 22 (στο άκρο του εξυπηρετητή)

2.3 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής SSH; [Προσδιορίστε τη ζητούμενη θύρα συμβουλευόμενοι τον κατάλογο πασίγνωστων θυρών στην ιστοσελίδα http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.]

Port 22

2.4 Εφαρμόστε φίλτρο ώστε να παραμείνουν μόνο τα μηνύματα SSH. Ποια είναι η σύνταξη του φίλτρου που χρησιμοποιήσατε;

Display filter : ssh

2.5 Αναλύοντας το αναγνωριστικό που στέλνει ο πελάτης στον εξυπηρετητή, ποια έκδοση του πρωτοκόλλου SSH και ποια έκδοση λογισμικού χρησιμοποιεί ο πελάτης; Περιλαμβάνονται σχόλια στο αναγνωριστικό αυτό; Αν ναι, να καταγραφούν.

Πρωτόκολλο : SSH-2.0

Λογισμικό : PuTTY_Release_0.80

Δεν υπάρχουν σχόλια.

2.6 Εντοπίσετε τα μηνύματα SSH τύπου Protocol. Αναλύοντας το αναγνωριστικό που στέλνει ο εξυπηρετητής στον πελάτη, ποια έκδοση του πρωτοκόλλου SSH και ποια έκδοση λογισμικού χρησιμοποιεί ο εξυπηρετητής; Περιλαμβάνονται σχόλια στο αναγνωριστικό αυτό; Αν ναι, να καταγραφούν.

Πρωτόκολλο : SSH-2.0

Λογισμικό : OpenSSH_6.6.1_hpn13v11

Σχόλια : FreeBSD-20140420

2.7 Εντοπίσετε το μήνυμα SSH τύπου Key Exchange Init που έστειλε ο πελάτης και αναπτύξτε την επικεφαλίδα για τους αλγόριθμους. Ποιο είναι το μήκος της συμβολοσειράς `kex-algorithms` που περιέχει τη λίστα των υποστηριζόμενων αλγορίθμων ανταλλαγής κλειδιών; Καταγράψτε το πλήθος τους και τους πρώτους δύο. [Υπόδειξη: Κάντε δεξί κλικ στο σχετικό πεδίο στο παράθυρο με τις λεπτομέρειες και επιλέξτε Show Packet Bytes... προκειμένου να δείτε το πλήρες περιεχόμενό του `kex-algorithms`.]

`kex_algorithms length: 499`

Είναι 20 και οι πρώτοι δύο είναι οι

`sntrup761x25519-sha512@openssh.com, curve448-sha512`

2.8 Από τη λίστα των αλγορίθμων παραγωγής κλειδιών (server host key) που μπορεί να δεχθεί ο πελάτης καταγράψτε το πλήθος τους και τους πρώτους δύο εξ αυτών.

`server_host_key_algorithms length: 123`

Είναι 8 και οι πρώτοι δύο είναι : `ssh-ed448, ssh-ed25519`

2.9 Από τις λίστες αλγορίθμων κρυπτογράφησης (encryption) που υποστηρίζει ο πελάτης καταγράψτε τους δύο πρώτους για την κατεύθυνση πελάτης -> εξυπηρετητής.

`aes256-ctr, aes256-cbc`

2.10 Από τις λίστες αλγορίθμων πιστοποίησης αυθεντικότητας μηνυμάτων (mac) που υποστηρίζει ο πελάτης καταγράψτε τους δύο πρώτους για την κατεύθυνση πελάτης -> εξυπηρετητής.

`hmac-sha2-256, hmac-sha2-512`

2.11 Από τις λίστες αλγορίθμων συμπίεσης (compression) που υποστηρίζει ο πελάτης καταγράψτε τους δύο πρώτους για την κατεύθυνση πελάτης -> εξυπηρετητής.

`none, zlib`

2.12 Εντοπίσετε το μήνυμα SSH τύπου Key Exchange Init που έστειλε ο εξυπηρετητής και προσδιορίστε τον αλγόριθμο ανταλλαγής κλειδιών που θα ακολουθήσουν τα δύο μέρη. Τον εμφανίζει κάπου το Wireshark; [Υπόδειξη: Όπως προαναφέρθηκε, είναι εν γένει ο πρώτος της λίστας του πελάτη που υπάρχει και στη λίστα του εξυπηρετητή. Λεπτομέρειες για την ακριβή διαδικασία επιλογής μπορείτε να βρείτε στην παρ. 7.1 Algorithm Negotiation του RFC 4253.]

Key Exchange (method:curve25519-sha256@libssh.org)

2.13 Από τη λίστα των αλγορίθμων παραγωγής κλειδιών (server host key) για τους οποίους διαθέτει κλειδιά ο εξυπηρετητής, βρείτε αυτόν που τελικά θα χρησιμοποιηθεί.

Ο ssh-ed25519 είναι ο πρώτος αλγόριθμος παραγωγής κλειδιών του πελάτη που υποστηρίζεται από τον Server.

2.14 Από τις λίστες με τους αλγόριθμους κρυπτογράφησης που υποστηρίζει ο εξυπηρετητής, βρείτε αυτόν που τελικά θα χρησιμοποιηθεί στην κατεύθυνση πελάτη -> εξυπηρετητής.

encryption : aes256-ctr

2.15 Από τις λίστες με τους αλγόριθμους πιστοποίησης αυθεντικότητας μηνυμάτων που υποστηρίζει ο εξυπηρετητής, βρείτε αυτόν που τελικά θα χρησιμοποιηθεί στην κατεύθυνση πελάτη <- εξυπηρετητής.

mac : hmac-sha2-256

2.16 Από τις λίστες με τους αλγόριθμους συμπίεσης που υποστηρίζει ο εξυπηρετητής, βρείτε αυτόν που τελικά θα χρησιμοποιηθεί στην κατεύθυνση πελάτη -> εξυπηρετητής.

compression : none

2.17 Μετά την ολοκλήρωση της διαπραγμάτευσης αλγορίθμων και ανταλλαγής κλειδιών, ακολουθεί η φάση παραγωγής του κοινού μυστικού που θα χρησιμοποιηθεί για την κρυπτογράφηση της μετάδοσης δεδομένων. Ποιους άλλους σχετικούς με τη φάση αυτή τύπους μηνυμάτων SSH καταγράψατε; [Υπόδειξη: σε ένα μήνυμα μπορεί να περιέχονται περισσότεροι του ενός τύποι.]

Message Code: Elliptic Curve Diffie-Hellman Key Exchange Init (30)

Message Code: Elliptic Curve Diffie-Hellman Key Exchange Reply (31)

Message Code: New Keys (21)

2.18 Εμφανίζει σε κάποιο σημείο το Wireshark τους επιλεγθέντες αλγόριθμους παραγωγής κλειδιών, κρυπτογράφησης, πιστοποίησης αυθεντικότητας μηνυμάτων και συμπίεσης;

Για τις προαναφερθέντες περιπτώσεις εμφανίζονται στα σημεία που υποδεικνύονται στην παρακάτω εικόνα με εξαίρεση την πρώτη περίπτωση.

9	0.000000	62	147.102.131.22	147.102.40.15	SSHv2	Client: Key Exchange Init
14	0.021640	534	147.102.40.15	147.102.131.22	SSHv2	Server: Key Exchange Init
15	0.002309	102	147.102.131.22	147.102.40.15	SSHv2	Client: Elliptic Curve Diffie-Hellman
19	0.000060	262	147.102.40.15	147.102.131.22	SSHv2	Server: Elliptic Curve Diffie-Hellman
21	17.5926...	134	147.102.131.22	147.102.40.15	SSHv2	Client: New Keys
22	0.012242	118	147.102.40.15	147.102.131.22	SSHv2	Server:
24	8.132391	134	147.102.131.22	147.102.40.15	SSHv2	Client:
25	0.029993	134	147.102.40.15	147.102.131.22	SSHv2	Server:
26	0.000180	166	147.102.131.22	147.102.40.15	SSHv2	Client:
27	0.014617	166	147.102.40.15	147.102.131.22	SSHv2	Server:
29	11.8430...	326	147.102.131.22	147.102.40.15	SSHv2	Client:
30	0.036596	134	147.102.40.15	147.102.131.22	SSHv2	Server:
31	0.001656	166	147.102.131.22	147.102.40.15	SSHv2	Client:
32	0.030187	166	147.102.40.15	147.102.131.22	SSHv2	Server:
34	18.7565...	134	147.102.131.22	147.102.40.15	SSHv2	Client:


```

[Frame: 12, payload: 536-1071 (536 bytes)]
[Frame: 14, payload: 1072-1551 (480 bytes)]
[Segment count: 3]
[Reassembled TCP length: 1552]
[Reassembled TCP Data [truncated]: 0000060c0614e97a350ddf6abec4399361bcf502ca48000000d463757276653]
SSH Protocol
  SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
    Packet Length: 1548
    Padding Length: 6
    Key Exchange (method:curve25519-sha256@libssh.org)
      Message Code: Key Exchange Init (20)
      Algorithms
        Cookie: e97a350ddf6abec4399361bcf502ca48
        kex algorithms length: 212
  
```

2.19 Μπορείτε να εντοπίσετε τα πακέτα όπου μεταφέρεται η πληροφορία για την προτροπή login και password στην περίπτωση του SSH; Να δικαιολογήσετε την απάντησή σας.

Παρατηρώ πως δε γίνεται αντιληπτό ποια πακέτα αφορούν το login και το password στην περίπτωση του SSH και ο λόγος είναι πως τα πακέτα αυτά είναι κρυπτογραφημένα.

2.20 Σχολιάστε την ασφάλεια της υπηρεσίας SSH όσον αφορά την πιστοποίηση της αυθεντικότητας, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων συγκρίνοντας με άλλα πρωτόκολλα ανταλλαγής δεδομένων.

Αναφορικά με την ασφάλεια του SSH:

- Πιστοποίηση αυθεντικότητας: Έχουμε authentication μέσω public-private keys, από τις ασφαλέστερες δηλαδή μεθόδους.
- Εμπιστευτικότητα: Λόγω της κρυπτογράφησης, το περιεχόμενο γίνεται κατανοητό μόνο από τον εξυπηρετητή και τον πελάτη.
- Ακεραιότητα δεδομένων: Παρέχονται hashing αλγόριθμοι για data-integrity (MAC). Κρίνεται, επομένως, ως μια ασφαλής επιλογή.

3. Υπηρεσία HTTPS

Σε αυτή την άσκηση θα καταγραφούν τα μηνύματα που παράγονται κατά τη χρήση της υπηρεσίας HTTPS του υπολογιστή `www.noc.ntua.gr`. Επανεκκινήστε τον πλοηγό ιστού που χρησιμοποιείτε αφού προηγουμένως αδειάσετε την προσωρινή μνήμη (cache) του, π.χ πιέζοντας ταυτόχρονα τα πλήκτρα Ctrl-Shift-Delete και επιλέγοντας το διάστημα διαγραφής. Κατόπιν ξεκινήστε μια νέα καταγραφή εφαρμόζοντας φίλτρο σύλληψης ώστε να παρατηρείτε μόνο την κίνηση που σχετίζεται με τον `www.noc.ntua.gr`. Πρώτα, επισκεφθείτε με τον πλοηγό ιστού την ιστοσελίδα `http://www.noc.ntua.gr`. Μόλις φορτωθεί η σελίδα, επισκεφθείτε την πάλι, χρησιμοποιώντας αυτή τη φορά το πρωτόκολλο HTTPS. Για το σκοπό αυτό, πληκτρολογήστε τη διεύθυνση `https://www.noc.ntua.gr`. Όταν φορτωθεί πλήρως η σελίδα περιμένετε λίγο, κλείστε τον πλοηγό ιστού και σταματήστε την καταγραφή. Να σημειωθεί ότι το Wireshark εμφανίζει τα πακέτα που μεταφέρουν τα μηνύματα του HTTPS ως TLS (Transport Layer Security).

3.1 Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε;

Capture filter : `host www.noc.ntua.gr`

3.2 Εφαρμόστε κατάλληλο φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα πρώτα τεμάχια TCP των τριμερών χειραψιών που διεξήχθησαν με τον εξυπηρετητή `www.noc.ntua.gr`. Ποια είναι η σύνταξή του;

Display filter :

`tcp.len==0 and ((tcp.seq==0 and tcp.ack==0) or (tcp.seq==0 and tcp.ack==1) or (tcp.seq==1 and tcp.ack==1))`

3.3 Σε ποιες (πασίγνωστες) θύρες του εξυπηρετητή `www.noc.ntua.gr` γίνονται οι συνδέσεις;

Port : 80

Port : 443

3.4 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής HTTP και ποια στο HTTPS;

[Προσδιορίστε τις ζητούμενες θύρες συμβουλευόμενοι και την ιστοσελίδα

`http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.`]

Port : 80 => HTTP

Port : 443 => HTTPS

3.5 Βρείτε πόσες συνδέσεις ανοίχθηκαν μεταξύ του υπολογιστή σας και του εξυπηρετητή ιστού `bbb2.cn.ntua.gr` στην περίπτωση HTTP και πόσες στην περίπτωση HTTPS.

Ανοίχτηκαν συνολικά 12 συνδέσεις:

- 6 για HTTP
- 6 για HTTPS

3.6 Για τις συνδέσεις TCP της περίπτωσης HTTPS καταγράψτε τις θύρες πηγής.

Οι θύρες πηγής από την πλευρά μας ήταν οι εξής : 51360, 51361, 51362, 51363, 51364, 51365 και από την πλευρά του εξυπηρετητή η θύρα 443.

Σε αυτό το σημείο πρέπει να αναφερθεί ότι το πρωτόκολλο TLS αποτελείται στην πραγματικότητα από δύο στρώματα. Στο κατώτερο επίπεδο και πάνω από κάποιο αξιόπιστο πρωτόκολλο μεταφοράς (π.χ. το TCP), είναι το Στρώμα Εγγραφών (Record Layer) TLS. Το στρώμα αυτό χρησιμοποιείται για την ενθυλάκωση κάποιου πρωτοκόλλου TLS ανώτερου επιπέδου, όπως είναι, το Πρωτόκολλο Χειραψίας (Handshake Protocol), το πρωτόκολλο συναγερμών (Alert Protocol), το πρωτόκολλο μετάβασης σε κρυπτογράφηση (ChangeCipherSpec) και το πρωτόκολλο εφαρμογής (Application). Πρέπει επίσης να τονιστεί ότι κάθε πλαίσιο Ethernet μπορεί να περιλαμβάνει μία ή περισσότερες εγγραφές TLS. Επιπλέον, στην περίπτωση που μια εγγραφή TLS δεν χωράει σε ένα πλαίσιο Ethernet, τότε θα χρειαστούν πολλαπλά πλαίσια για να τη μεταφέρουν. Εφαρμόστε το φίλτρο απεικόνισης `tls.record` ώστε να παραμείνουν μόνο πλαίσια τα οποία περιλαμβάνουν εγγραφές TLS. Υπενθυμίζεται ότι οι εγγραφές αυτές δημιουργήθηκαν από τη χρήση του πρωτοκόλλου HTTPS με τον `www.noc.ntua.gr`.

3.7 Αναπτύσσοντας τις επικεφαλίδες Στρώματος Εγγραφών TLS κάθε πλαισίου θα παρατηρήσετε ότι τα τρία πρώτα πεδία είναι κοινά. Ποια είναι αυτά και ποιο το μήκος τους;

- **Content Type (1 Byte)**
- **Version (2 Bytes)**
- **Length (2 Bytes)**

3.8 Ένα από τα πεδία είναι ο τύπος περιεχομένου (content type). Να καταγραφούν τα ονόματα των διαφορετικών τύπων εγγραφών TLS που εμφανίζονται στην καταγραφή και οι αριθμητικές τους τιμές, π.χ. (20) για το πρωτόκολλο μετάβασης σε κρυπτογράφηση (Change Cipher Spec Protocol). [Υπόδειξη: Υπενθυμίζεται ότι ορισμένα πλαίσια μπορεί να περιλαμβάνουν περισσότερες από μία εγγραφές TLS.]

Content Type: Handshake (22)

Content Type: Change Cipher Spec (20)

Content Type: Application Data (23)

3.9 Για εγγραφές TLS που αφορούν το πρωτόκολλο χειραψίας (handshake protocol) καταγράψτε τους διαφορετικούς τύπους μηνυμάτων χειραψίας που παρατηρήσατε και τις αριθμητικές τους τιμές, π.χ. Client Hello (1).

Handshake Type: Client Hello (1)

Handshake Type: Server Hello (2)

Handshake Type: New Session Ticket (4)

Handshake Type: Certificate (11)

Handshake Type: Server Key Exchange (12)

Handshake Type: Server Hello Done (14)

Handshake Type: Client Key Exchange (16)

3.10 Πόσα μηνύματα Client Hello έστειλε ο πελάτης και ποια η σχέση τους με τις συνδέσεις TCP που καταγράψατε προηγουμένως;

6 μηνύματα Client Hello

tls.record && tls.handshake.type == 1						
No.	Time	Length	Source	Destination	Protocol	Info
1171	0.000408	829	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)
1235	0.000394	829	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)
1244	0.000117	765	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)
1245	0.000377	765	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)
1246	0.000277	797	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)
1247	0.000289	765	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)

3.11 Εντοπίστε την εγγραφή TLS με το πρώτο μήνυμα Client Hello που στέλνει ο πελάτης κατά τη χειραψία του πρωτοκόλλου TLS. Ποια έκδοση του πρωτοκόλλου TLS δηλώνεται στην εγγραφή TLS και ποια η αριθμητική της τιμή;

Version: TLS 1.0 (0x0301)

3.12 Ποια είναι η έκδοση πρωτοκόλλου TLS που δηλώνεται στο μήνυμα Client Hello και ποια η αριθμητική τιμή της; Είναι ταυτόσημες με αυτές στην εγγραφή TLS;

Version: TLS 1.2 (0x0303)

Όχι, δεν είναι.

3.13 Ποιο είναι το μήκος σε byte του τυχαίου αριθμού (Random) που περιέχει το μήνυμα Client Hello; Καταγράψτε τα πρώτα 4 byte. Τι παριστάνουν;

Το μήκος του τυχαίου αριθμού είναι 32 bytes, με τα πρώτα 4 εξ αυτών να είναι τα 61 51 87 86. Τα bytes αυτά δηλώνουν το

GMT Unix Time: Dec 28, 2025 21:39:50.000000000 GTB Standard Time

3.14 Στην επικεφαλίδα για τις σουίτες κωδίκων (cipher suites) δηλώνονται αυτές που υποστηρίζει ο πελάτης. Να καταγραφεί το πλήθος τους και οι δεκαεξαδικές τιμές των δύο πρώτων από αυτές.

Cipher Suites : 16

#1 Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

#2 Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

3.15 Εάν ο πλοηγός σας είναι συμβατός με την έκδοση TLS1.3 του πρωτοκόλλου, τότε στην επικεφαλίδα επέκτασης supported_versions δηλώνει όλες τις υποστηριζόμενες εκδόσεις TLS. Εάν ναι, πόσες και ποιες δηλώνονται; Ποια είναι η αριθμητική τιμή για την έκδοση TLS1.3;

Δηλώνονται 2 εκδόσεις :

- Supported Version: TLS 1.2 (0x0303)
- Supported Version: TLS 1.3 (0x0304)

```

  ▶ Extension: signed_certificate_timestamp (len=0)
  ▼ Extension: supported_versions (len=7) TLS 1.3, TLS 1.2
    Type: supported_versions (43)
    Length: 7
    Supported Versions length: 6
    Supported Version: Reserved (GREASE) (0x5a5a)
    Supported Version: TLS 1.3 (0x0304)
    Supported Version: TLS 1.2 (0x0303)
  ▶ Extension: extended_master_secret (len=0)
  ▶ Extension: status_request (len=5)
  ▶ Extension: psk_key_exchange_modes (len=2)
  ▶ Extension: application_layer_protocol_negotiation (len=14)

```

3.16 Εάν ο πλοηγός σας είναι συμβατός με HTTP/2, τότε δηλώνει τις υποστηριζόμενες εκδόσεις στην επικεφαλίδα επέκτασης `application_layer_protocol_negotiation` σε εγγραφές τύπου ALPN Next Protocol. Εάν ναι, ποια πρωτόκολλα δηλώνονται;

Δηλώνονται 2 πρωτόκολλα :

- ALPN Next Protocol: h2
- ALPN Next Protocol: http/1.1

3.17 Εντοπίστε το μήνυμα Server Hello με το οποίο απαντά ο εξυπηρετητής στη χειραψία που ξεκίνησε με το προηγούμενο Client Hello. Εξετάζοντας την επικεφαλίδα της εγγραφής TLS, καταγράψτε την έκδοση TLS που θα χρησιμοποιηθεί.

TLS1.2

3.18 Ποιο είναι το μήκος σε byte του τυχαίου αριθμού που περιέχει το μήνυμα Server Hello; Καταγράψτε τα πρώτα 4 byte. Συγκρίνοντας με την ερώτηση 3.13, τι συμπεραίνετε για το πώς παράγονται; Το μήκος του τυχαίου αριθμού είναι 32 bytes, με τα πρώτα 4 εξ αυτών να είναι τα 5a d8 14 7e. Τα bytes αυτά δηλώνουν το

GMT Unix Time: Apr 19, 2018 07:01:02.000000000 GTB Daylight Time

Διαφέρουν αφού τα GMT Unix Time είναι διαφορετικά.

3.19 Ποιο είναι το όνομα και η δεκαεξαδική τιμή της σουίτας κωδίκων που τελικά επιλέχθηκε;

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

3.20 Ποιοι είναι οι αλγόριθμοι ανταλλαγής κλειδιών, πιστοποίησης ταυτότητας, κρυπτογράφησης και η συνάρτηση κατακερματισμού; [Υπόδ.: Για τον τρόπο ονομασίας (Naming scheme) των σουιτών και τα ονόματα των υποστηριζόμενων αλγορίθμων στις εκδόσεις TLS 1.0–1.2 συμβουλευθείτε την ιστοσελίδα https://en.wikipedia.org/wiki/Cipher_suite].

TLS

defines the protocol that this cipher suite is for; it will usually be TLS.

ECDHE

indicates the key exchange algorithm being used.

RSA

Μηχανισμός ελέγχου ταυτότητας κατά τη διάρκεια της χειραψίας.

AES

Κρυπτογράφηση συνεδρίας.

128

Μέγεθος κλειδιού κρυπτογράφησης περιόδου λειτουργίας (bits) για κρυπτογράφηση.

GCM

Τύπος κρυπτογράφησης (εξάρτηση μπλοκ κρυπτογράφησης και πρόσθετες επιλογές).

SHA

(SHA2)hash function. Για μια έξοδο 256 bits και άνω. Μηχανισμός υπογραφής. Υποδεικνύει τον αλγόριθμο ελέγχου ταυτότητας μηνύματος που χρησιμοποιείται για τον έλεγχο ταυτότητας ενός μηνύματος.

256

Μέγεθος εξόδου (bits).

3.21 Χρησιμοποιείται κάποια μέθοδος συμπίεσης από τον εξυπηρετητή και τον πελάτη;

Όχι,

Compression Method: null (0)

3.22 Εντοπίστε το μήνυμα Certificate που μεταφέρει τα πιστοποιητικά του εξυπηρετητή. Ποιο είναι το μήκος του σύμφωνα με το πεδίο length της επικεφαλίδας στρώματος εγγραφών TLS;

Length: 6209

3.23 Πόσα πιστοποιητικά μεταφέρονται και τι μήκος έχει το καθένα από αυτά;

Μεταφέρονται 4 πιστοποιητικά με μήκη :

Certificate Length: 1930

Certificate Length: 1769

Certificate Length: 1413

Certificate Length: 1078

3.24 Πόσα πλαίσια Ethernet χρειάστηκαν ώστε να μεταφερθεί η παραπάνω εγγραφή TLS; [Υπόδειξη: Δείτε πεδίο [Reassembled TCP Segments] στο παράθυρο με τις λεπτομέρειες.]

[6 Reassembled TCP Segments (6214 bytes): #1172(1285), #1173(1355), #1175(1355), #1176(31), #1178(1355), #1179(833)]. Άρα χρειάστηκαν 6 Ethernet frames.

3.25 Εντοπίστε τα μηνύματα για την ανταλλαγή κλειδιών Diffie–Hellman (ServerKeyExchange, ClientKeyExchange). Ποιο είναι το μήκος του δημόσιου κλειδιού που αποστέλλει ο πελάτης και ποιο του εξυπηρετητή; Καταγράψτε τα 5 πρώτα γράμματα αμφοτέρων των κλειδιών.

Client Pubkey Length: 65 bytes (5 πρώτα γράμματα = «04203»)

1171	0.000408	829	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)
1181	0.000817	180	147.102.131.22	147.102.222.246	TLSv1.2	Client Key Exchange, Change Cipher Spec, En
1183	0.000421	820	147.102.131.22	147.102.222.246	TLSv1.2	Application Data
1232	0.001158	749	147.102.131.22	147.102.222.246	TLSv1.2	Application Data
1235	0.000394	829	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)
1244	0.000117	765	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)
1245	0.000377	765	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)
1246	0.000277	797	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)
1247	0.000289	765	147.102.131.22	147.102.222.246	TLSv1.2	Client Hello (SNI=www.noc.ntua.gr)
1249	0.010330	754	147.102.131.22	147.102.222.246	TLSv1.2	Application Data
1251	0.000351	105	147.102.131.22	147.102.222.246	TLSv1.2	Change Cipher Spec, Encrypted Handshake Mes
1252	0.000280	760	147.102.131.22	147.102.222.246	TLSv1.2	Application Data
1255	0.000245	105	147.102.131.22	147.102.222.246	TLSv1.2	Change Cipher Spec, Encrypted Handshake Mes
1256	0.000210	105	147.102.131.22	147.102.222.246	TLSv1.2	Change Cipher Spec, Encrypted Handshake Mes
1257	0.000195	752	147.102.131.22	147.102.222.246	TLSv1.2	Application Data
1258	0.000137	751	147.102.131.22	147.102.222.246	TLSv1.2	Application Data
1261	0.000262	105	147.102.131.22	147.102.222.246	TLSv1.2	Change Cipher Spec, Encrypted Handshake Mes
1262	0.000196	105	147.102.131.22	147.102.222.246	TLSv1.2	Change Cipher Spec, Encrypted Handshake Mes
1263	0.000663	750	147.102.131.22	147.102.222.246	TLSv1.2	Application Data

▶ Frame 1181: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \De	0000	00 ff 24
▶ Ethernet II, Src: 00:ff:23:cc:18:cd, Dst: 00:ff:24:cc:18:cd	0010	00 a6 36
▶ Internet Protocol Version 4, Src: 147.102.131.22, Dst: 147.102.222.246	0020	de f6 c8
▶ Transmission Control Protocol, Src Port: 51360, Dst Port: 443, Seq: 776, Ack: 6632, Len: 1	0030	04 02 0c
▼ Transport Layer Security	0040	04 20 35
▼ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange	0050	24 77 40
Content Type: Handshake (22)	0060	5a 02 2a
Version: TLS 1.2 (0x0303)	0070	76 bb 1f
Length: 70	0080	cc 14 03
▼ Handshake Protocol: Client Key Exchange	0090	00 00 00
Handshake Type: Client Key Exchange (16)	00a0	32 05 d1
Length: 66	00b0	17 f9 a2
▼ EC Diffie-Hellman Client Params		
Pubkey Length: 65		
Pubkey: 042035a72caeb505e0e8a660c9e81ca82477400b8b4316ae5e0932340432610f5a022a		
▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec		
Content Type: Change Cipher Spec (20)		
Version: TLS 1.2 (0x0303)		
Length: 1		
Change Cipher Spec Message		

Server Pubkey Length: 65 bytes (5 πρώτα γράμματα = «044c5»)

3.26 Ποιο είναι το μήκος της εγγραφής TLS τύπου ChangeCipherSpec που μεταφέρει στον εξυπηρετητή την υπόδειξη ότι η επικοινωνία από εδώ και πέρα θα είναι κρυπτογραφημένη και ποιο το μήκος του αντίστοιχου μηνύματος;

Record length : 6 bytes

Length of message : 1 byte

3.27 Ποιο είναι το μήκος σε byte του μηνύματος EncryptedHandshakeMessage που περιέχει από την πλευρά του πελάτη το αποτέλεσμα της συνάρτησης κατακερματισμού επί των προηγούμενων μηνυμάτων της χειραφσίας;

Length : 40 bytes

3.28 Παρατηρήσατε εγγραφή TLS με την υπόδειξη (ChangeCipherSpec) και μήνυμα με το αποτέλεσμα της συνάρτησης κατακερματισμού (EncryptedHandshakeMessage) από την πλευρά του εξυπηρετητή;

Ναι.

3.29 Εντοπίστε μια εγγραφή TLS για πρωτόκολλο εφαρμογής. Ποιου πρωτοκόλλου δεδομένα μεταφέρονται σύμφωνα με τις ενδείξεις του Wireshark;

TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

3.30 Παρατηρήσατε εγγραφές TLS του πρωτοκόλλου Alert (Encrypted Alert); Από ποια πλευρά στάλθηκαν;

Όχι, δε παρατηρήσαμε.

3.31 Εάν ναι, γιατί νομίζετε ότι υπάρχουν;[Υπόδειξη: Απενεργοποιήστε το ισχύον φίλτρο απεικόνισης και δείτε τι ακολουθεί στην αντίστοιχη σύνδεση TCP.]

Ο λόγος που θα υπήρχαν, θα ήταν προκειμένου ο πελάτης να ειδοποιήσει τον εξυπηρετητή για την απόλυση της TCP σύνδεσης.

3.32 Επιλέξτε από την ιστοσελίδα μια φράση με λατινικούς χαρακτήρες (π.χ. “webmail”). Προσπαθήστε να βρείτε το πακέτο που μεταφέρει αυτή την πληροφορία. Τι παρατηρείτε στην περίπτωση του πρωτοκόλλου HTTP σε σύγκριση με αυτή του HTTPS;

Στη περίπτωση του HTTP βρίσκουμε πακέτο που έχει ως περιεχόμενο το περιεχόμενο της ιστοσελίδας που ζητήσαμε σε μορφή html, όπως βλέπουμε παρακάτω. Αντίθετα, στα πακέτα HTTPS δε μπορούμε να βρούμε κάποιο πακέτο αναζητώντας τη φράση webmail και αυτό διότι η πληροφορία μεταφέρεται κρυπτογραφημένη στο https σε αντίθεση με το http.

3.33 Σχολιάστε την ασφάλεια του πρωτοκόλλου HTTPS σε σχέση με το HTTP, όσον αφορά την πιστοποίηση της αυθεντικότητας, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Συγκρίνοντας το HTTP με το HTTPS, μπορούμε να πούμε πως:

- Πιστοποίηση αυθεντικότητας: Στο HTTPS, όταν ένας client εκκινεί έναν “διάλογο” επικοινωνίας με έναν εξυπηρετητή, ο εξυπηρετητής επαληθεύει τη γνησιότητα του αντιστοιχίζοντας το private key του με το public key στο SSL certificate (το οποίο είναι signed από μία έμπιστη αρχή) της σελίδας που επισκεπτόμαστε. Στο HTTP δεν υπάρχει κάποια αντίστοιχη διαδικασία που να εξασφαλίζει την πιστότητα του εξυπηρετητή.
- Εμπιστευτικότητα: Στο HTTP τα δεδομένα στέλνονται ως plaintext, επομένως είναι άμεσα αναγνώσιμα από κάποιον που θα καταφέρει να υποκλέψει κάποια πακέτα. Αντιθέτως, το περιεχόμενο στο HTTPS είναι κρυπτογραφημένο, με αποτέλεσμα ακόμα και αν κάποιος υποκλέψει πακέτα να διαβάσει κάτι που δε βγάζει νόημα και από το οποίο δε μπορεί να εξαγει κάτι χρήσιμο.
- Ακεραιότητα: Στο HTTPS είναι αδύνατον να μεταβληθούν τα δεδομένα χωρίς αυτό να γίνει αντιληπτό από τους συμμετέχοντες στη σύνδεση. Αντιθέτως, το HTTP είναι επιρρεπές σε επιθέσεις τύπου Man-In-The-Middle, οι οποίες θα μπορούσαν να αλλοιώσουν το περιεχόμενο των πακέτων.