Ονοματεπώνυμο: Ναυσικά Αμπατζή		Ομάδα: 2
Όνομα PC/ΛΣ: Dell XPS 15-7590 Windows		Ημερομηνία: 7 /1 /2021
Διεύθυνση IP: 192.168.1.12	Διεύθυνση MAC:24-41-8C-65-26-BF	

Μέρος 1

1.1 Status code = 401 και επιστρέφεται το μήνυμα Authentication Required.
1.2 Στο δεύτερο μήνυμα GET υπάρχει το επιπλέον πεδίο Authorization.
1.3 Authorization: Basic ZWR1LWR5OnBhc3Nb3Jk
1.4 edu-dy:pass
1.5 Ο τρόπος αυτός πιστοποίησης είναι μη ασφαλής, καθώς τα δεδομένα εισόδου απλά κωδικοποιούνται με έναν αρκετά απλό τρόπο, ενώ δεν υπάρχει καθόλου κρυπτογράφιση ή κάποιο hash function για την καλύτερη προστασία τους.

Μέρος 2

2.1 Το SSH χρησιμοποιεί πρωτόκολλο μεταφοράς TCP.

2.2 Χρησιμοποιούνται οι θύρες 22 και 51011.

2.3 Για το πρωτόκολλο εφαρμογής SSH, χρησιμοποιείται η θύρα 22.

2.4 Φίλτρο: ssh

2.5 Έκδοση πρωτοκόλλου: SSH 2.0

Έκδοση λογισμικού : OpenSSH5.8

Σχόλια : `FreeBSD-20110503`

2.6 Έκδοση πρωτοκόλλου: SSH 2.0

Έκδοση λογισμικού : PUTTY-Release 0.74

Σχόλια : Δεν υπάρχουν.

2.7 Υπάρχουν 10 αλγόριθμοι kex και οι πρώτοι δύο είναι οι ecdh-sha2-nistp256 και ecdh-sha2-nistp384.

2.8 Υπάρχουν 6 αλγόριθμοι και ο πρώτος είναι ο ssh-ed25519.

2.9 aes256-ctr και aes256-cbc

2.10 hmac-sha2-256,hmac-sha1

2.11 none και zlib

2.12 Ο αλγόριθμος είναι ο ecdh-sha2-nistp256 και εμφανίζεται στις λεπτομέρειες στο πεδίο hex algorithms string.

2.13 `aes256-ctr`

2.14 hmac-sha1

2.15 none

2.16 Οι παραπάνω επιλεχθέντες αλγόριθμοι εμφανίζονται στην αρχή, στις λεπτομέρειες του SSH Protocol σε μία παρένθεση :

```
SSH Version 2 (encryption:aes256-ctr mac:hmac-sha1 compression:none)
```

2.17 Άλλοι τύποι μηνυμάτων SSH που καταγράφτηκαν: Elliptic Curve Diffie-Hellman Key Exchange Init, Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet

2.18 Τα πακέτα για την προτροπή login και password δεν υπάρχουν στην περίπτωση του SSH, καθώς έχει γίνει κρυπτογράφηση των δεδομένων, ώστε να προστατεύονται.

2.19 Όσον αφορά την ακεραιότητα δεδομένων παρατηρούμε (ερώτημα 2.18) ότι τα δεδομένα που εισάγει ο χρήστης δεν είναι ορατά κάπου, καθώς υπάρχει κρυπτογράφηση. Επομένως το SSH πρωτόκολλο είναι ασφαλές όσον αφορά την ακεραιότητα δεδομένων. Για την πιστοποίηση αυθεντικότητας χρησιμοποιούνται αλγόριθμοι, ενώ η γνησιότητα των μηνυμάτων πιστοποιείται με την σύνοψη που παράγεται από τα περιεχόμενα του μηνύματος. Καταλήγουμε στο συμπέρασμα ότι το πρωτόκολλο είναι αρκετά ασφαλές, λόγω της κρυπτοφραφίας που χρησιμοποιείται σε σχέση με το Telnet.

Μέρος 3

3.1 Με tracert my.ntua.gr στο cmd βρέθηκε η IPV4 της ιστοσελίδας κι έτσι το φίλτρο σύλληψης που χρησιμοποιήθηκε είναι το host 147.102.222.242.

3.2 tcp.flags.syn == 1 && ip.addr==147.102.222.242

3.3 Οι συνδέσεις γίνονται στις θύρες 80 και 443.

3.4 Το πρωτόκολλο HTTP αντιστοιχεί στη θύρα 80 και το HTTPS στη θύρα 443.

3.5 Για να βρούμε τις συνδέσεις στο HTTP εφαρμόζουμε το φίλτρο απεικόνισης : tcp.flags.syn == 1 && ip.addr==147.102.222.242 && tcp.port == 80 και βρίσκουμε 5 συνδέσεις.

Για να βρούμε τις συνδέσεις στο HTTPS εφαρμόζουμε το φίλτρο απεικόνισης : tcp.flags.syn == 1 && ip.addr==147.102.222.242 && tcp.port == 443 και βρίσκουμε 6 συνδέσεις.

3.6 Θύρες πηγής : 443, 57342, 57343, 57346, 57346, 57347, 57349.

3.7 Τα τρία πρώτα κοινά πεδία είναι τα Content type (1 byte), Version(2 bytes) και Length(2 bytes).

3.8

- Client Hello - 22
- Server Hello – 22
- Certificate – 22
- Server Key Exchange – 22
- Server Hello Done – 22
- Change Cipher Spec – 22
- Encrypted Handshake Message – 22
- New Session Ticket

- Application Data – 23
- Encrypted Alert – 21

3.9

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

3.10 Ο πελάτης έστειλε 2 μηνύματα Client Hello, και οι TCP συνδέσεις είναι δύο από αυτές που καταγράφτηκαν στο ερώτημα 3.6 (θύρες πηγής 57342 και 57343).

3.11 Μέγιστη έκδοση : TLS 1.2

3.12 Ο τυχαίος αριθμός έχει μήκος 32bytes και τα 4 πρώτα από αυτά είναι τα εξής: 852a

3.13 Υποστηρίζονται 16 cipher suites και οι δύο πρώτες έχουν τιμές 0x1301 και 0x1302.

3.14 Θα χρησιμοποιηθεί η έκδοση TLS 1.2 και τελικά επιλέχθηκε η σουίτα κωδικών 0xc030.

3.15 Ο τυχαίος αριθμός που περιέχει έχει μήκος 32 bytes και τα 4 πρώτα είναι τα eb2e.

3.16 Από τον πελάτη χρησιμοποιείται 1 μέθοδος συμπίεσης, ενώ από τον εξυπηρετητή όχι.

3.17 Αλγόριθμος ανταλλαγής κλειδιών: RSA

Αλγόριθμοι πιστοποίησης ταυτότητας: RSA, ECDSA

Αλγόριθμος κρυπτογράφησης: AES

Συνάρτηση κατακερματισμού: SHA

3.18 Το μήκος της εγγραφής που μεταφέρει το πιστοποιητικό Certificate του εξυπηρετητή είναι σύμφωνα με το πεδίο Length 6304 bytes.

3.19 Μεταφέρονται 4 πιστοποιητικά με ονόματα: my.ntua.gr, GEANT,USERTrust,AAA

3.20 Για να μεταφερθεί η παραπάνω εγγραφή χρειάστηκαν 4 πλαίσια Ethernet.

3.21 Το μήκος του δημόσιου κλειδιού που στέλνει ο πελάτης είναι 65 bytes και τα πρώτα 5 γράμματα είναι τα εξής: 0417c

Το μήκος του δημόσιου κλειδιού που στέλνει ο εξυπηρετητής είναι 65 bytes και τα πρώτα 5 γράμματα είναι τα εξής: 04f36

3.22 6 bytes

3.23 45 bytes

3.24 Ναι υπάρχουν τέτοιες εγγραφές.

3.25 Ναι παρατηρήθηκαν Encrypted Alert εγγραφές και στάλθηκαν και από τις δύο μεριές.

3.26 Οι εγγραφές αυτές σηματοδοτούν την απόλυση της TCP σύνδεσης, καθώς υπάρχουν ακριβώς πριν την ανακοίνωση της απόλυσης σύνδεσης για κάθε πλευρά.

3.27 Παρατηρώ ότι στο πρωτόκολλο HTTP δεν υπάρχει καμία ασφάλεια, σε σχέση με το HTTPS, αφού τα δεδομένα δεν προστατεύονται με κάποιον τρόπο.

3.28 Το πρωτόκολλο HTTPS κρυπτογραφεί τα μηνύματα HTTP πριν τη μετάδοση και τα αποκρυπτογραφεί κατά την λήψη. Ο πελάτης και εξυπηρετητής ακολουθούν μία διαδικασία χειραψίας χρησιμοποιώντας διάφορες παραμέτρους σχετικά με την ασφάλεια της σύνδεσης. Το συμπέρασμα είναι ότι το HTTPS είναι ένα αρκετά ασφαλές πρωτόκολλο, σε αντίθεση με το HTTP.