Δίκτυα υπολογιστών

Εργαστηριακή άσκηση 12 (Ασφάλεια)

Τσάκωνας Παναγιώτης (03119610) Ομάδα: 2

Ακαδημαϊκό Έτος: 2022-2023

Άσκηση 1: Πιστοποίηση αυθεντικότητας στο πρωτόκολλο HTTP

1.1) Ο αριθμητικός κωδικός κατάστασης είναι 401 και η φράση που επιστρέφει ο εξυπηρετητής ως απόκριση στο αρχικό αίτημα HTTP τύπου GET του πλοηγού ιστού είναι: Authorization Required.

1.2) Το όνομα της σχετικής επικεφαλίδας HTTP και η μέθοδος που υποδεικνύει είναι: Basic realm="Edu-DY TEST".

1.3) Το όνομα της σχετικής επικεφαλίδας HTTP είναι: `Authorization.`

1.4) Τα διαπιστευτήρια που εμφανίζονται σε μορφή ASCII είναι: Basic ZWR1LWR5OnRzcCEjQCUyMDAxNQ==.

1.5) Το αποτέλεσμα είναι: edu-dy:password.

1.6) Συμπεραίνω ότι η ασφάλεια του μηχανισμού πιστοποίησης είναι αρκετά αδύναμη.

Άσκηση 2: Υπηρεσία SSH – Secure Shell

2.1) Το πρωτόκολλο μεταφοράς που χρησιμοποιεί το SSH είναι TCP.

2.2) 56037 και 22.

2.3) Η θύρα 22 αντιστοιχεί στο πρωτόκολλο της εφαρμογής SSH.

2.4) Το φίλτρο που χρησιμοποίησα είναι: `ssh.`

2.5) Ο εξυπηρετητής χρησιμοποιεί την ακόλουθη έκδοση πρωτοκόλλου SSH: SSH-2.0-OpenSSH_6.6.1_hpn13v11 FreeBSD-20140420 και δεν περιλαμβάνονται σχόλια.

2.6) Ο εξυπηρετητής χρησιμοποιεί την ακόλουθη έκδοση πρωτοκόλλου SSH: SSH-2.0-OpenSSH_9.0

2.7) 11 αλγόριθμοι και οι 2 πρώτοι είναι οι: sntrup761x25519-sha512@openssh.com και curve25519-sha256.

2.8) 8 αλγόριθμοι και οι 2 πρώτοι είναι οι: curve25519-sha256@libssh.org και ecdh-sha2-nistp256

2.9) aes128-ctr και aes192-ctr

2.10) hmac-md5-etm@openssh.com και hmac-sha1-etm@openssh.com

2.11) none και zlib@openssh.com

2.12) Είναι ο curve25519-sha256@libssh.org και το Wireshark τον εμφανίζει σε παρένθεση δίπλα στην αντίστοιχη επικεφαλίδα.

2.13) chacha20-poly1305@openssh.com

2.14) umac-64-etm@openssh.com

2.15) None

2.16) Ναι, τους εμφανίζει σε παρένθεση δίπλα από τις σχετικές επικεφαλίδες.

2.17) Elliptic Curve Diffie-Hellman Key Exchange Init, Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys και New Keys.

2.18) Όχι, διότι είναι κρυπτογραφημένα.

2.19) Είναι αρκετά ασφαλές πρωτόκολλο όσον αφορά την πιστοποίηση της αυθεντικότητας, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων που μεταφέρονται σε σύγκριση με άλλα πρωτόκολλα ανταλλαγής δεδομένων που έχουμε δει έως τώρα.

Άσκηση 3: Υπηρεσία HTTPS

3.1) Το φίλτρο που χρησιμοποίησα είναι το: `host bbb2.cn.ntua.gr`
3.2) Η σύνταξη του φίλτρου απεικόνισης είναι: `tcp.flags.syn == 1 && tcp.flags.ack == 0`
3.3) Στις θύρες 443 και 80.
3.4) Η 80 αντιστοιχεί στην HTTP και η 443 στην HTTPS.
3.5) 6 στην περίπτωση του HTTP και 1 στην περίπτωση του HTTPS
3.6) Η θύρα 56602 είναι θύρα πηγής.
3.7) Τα πεδία είναι τα: Content Type (1 byte), Version (2 bytes) και Length (2 bytes)
3.8) Τα διαφορετικά πεδία που εμφανίζονται στην καταγραφή είναι τα: Handshake (22), Application Data (23) και Change Cipher Spec (20).
3.9) Η έκδοση πρωτοκόλλου Στρώματος Εγγραφών TLS που δηλώνεται και η αριθμητική της τιμή είναι: TLS 1.2 (0x0303).
3.10) Οι διαφορετικοί τύποι μηνυμάτων χειραψίας που παρατηρώ είναι: Client Hello (1), Server Hello (2), Certificate (11), Server Key Exchange (12), Server Hello Done (14), Client Key Exchange (16) και New Session Ticket (4).
3.11) Έστειλε ένα Client Hello, όπως και ένα TCP handshake για HTTPS
3.12) Η έκδοση πρωτοκόλλου Στρώματος Εγγραφών TLS που δηλώνεται και η αριθμητική της τιμή είναι: TLS 1.0 (0x0303) και παρατηρούμε ότι δεν είναι η ίδια τιμή με το ερώτημα 3.9.
3.13) Δηλώνονται 3 εκδόσεις και αυτές είναι: Reserved (GREASE): 0xfafa, TLS 1.3: 0x0304 και TLS 1.2: 0x0303.
3.14) Δηλώνονται 2 εκδόσεις: h2 και http/1.1
3.15) Το μήκος του τυχαίου αριθμού που περιέχει το μήνυμα Client Hello είναι 32 bytes. Τα πρώτα 4 bytes είναι: ee 63 c9 66.
3.16) Το πλήθος τους είναι 16 και οι 2 πρώτες είναι: Reserved (GREASE): 0x9a9a και TLS_AES_128_GCM_SHA256: 0x1301
3.17) Θα χρησιμοποιηθεί TLS 1.2
3.18) Το μήκος του είναι 32 bytes όσα και στην ερώτηση 3.14 και τα 4 πρώτα bytes είναι: 65 4e f0 ae
3.19) Όχι δεν χρησιμοποιείται.
3.20) Το όνομα και η δεκαεξαδική τιμή της σουίτας κωδίκων που τελικά επιλέχθηκε είναι: Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f). Οι αλγόρθμοι ανταλλαγής κλειδιών, πιστοποίησης ταυτότητας, κρυπτογράφησης και η συνάρτηση κατακερματισμού είναι οι ακόλουθοι: KEX: ECDH, Authentication: RSA, BSC: AES128 και Hash: SHA256
3.21) Το μήκος του είναι 4276 bytes.
3.22) Μεταφέρθηκε 3 πιστοποιητικά με μήκος 1574, 1306, 1380 bytes αντίστοιχα.
3.23) Χρειάστηκαν 4 πακέτα Ethernet.
3.24) Το μήκος του κλειδιού είναι 32 bytes και στις δύο περιπτώσεις. Για τον πελάτη τα 5 πρώτα είναι: 3f 6a 75 d3 89 και για τον εξυπηρετητή είναι: e7 13 da 45 54
3.25) Μήκος μηνύματος 1 byte και μήκος εγγραφής 6 bytes
3.26) 40 bytes

3.27) Όχι, δεν παρατήρησα.
3.28) HTTP
3.29) Όχι δεν παρατηρήθηκαν.
3.30) –
3.31) Στο HTTPS τα δεδομένα είναι κρυπτογραφημένα οπότε δεν μπορούμε να βρούμε το πακέτο που περιλαμβάνει αυτή τη φράση.
3.32) Το HTTPS είναι πιο ασφαλές, διότι όλα τα δεδομένα κρυπτογραφούνται για να σταλθούν. Έτσι, παρέχεται ασφάλεια από κακόβουλους χρήστες που ίσως βρίσκονται στο δίκτυο καθώς δεν μπορούν να δουν τα δεδομένα που στέλνουμε και λαμβάνουμε.