ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ Ακ. έτος 2023-2024 9ο εξάμηνο, Φοιτητής: Αναστασιάδης Βασίλειος ΑΜ:03119954

Εργαστηριακή Άσκηση 12 Ασφάλεια

1. Πιστοποίηση αυθεντικότητας στο πρωτόκολλο HTTP

1. HTTP/1.1 401 Authorization Required (text/html)
2. WWW-Authenticate: Basic realm="Edu-DY TEST"\r\n
3. Authorization
4. DXNlciBuYW1lOnBhc3N3b3Jk\r\n
5. user name:password
6. Συμπερασματικά, το βασικό HTTP authentication δεν παρέχει καμία εμπιστευτικότητα από μόνο του, καθώς τα διαπιστευτήρια κωδικοποιούνται μόνο σε Base64 και δεν κρυπτογραφούνται.

2. Υπηρεσία SSH – Secure SHell

1. TCP
2. Source Port: 58082

   Destination Port: 22

3. 22
4. Ssh
5. Client: Protocol (SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6)
6. Server: Protocol (SSH-2.0-OpenSSH_6.6.1_hpn13v11 FreeBSD-20140420)
7. kex_algorithms length: 305

   Το πλήθος είναι 8

   curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256

8. Το πλήθος είναι

   ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com

9. chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr
10. umac-64-etm@openssh.com,umac-128-etm@openssh.com
11. none,zlib@openssh.com
12. Diffie-Hellman Key Exchange δεν το παρατηρώ κάπου ξεχωριστά στο Wireshark.
13. Host key type: ssh-ed25519
14. chacha20-poly1305@openssh.com

15. -
16. -
17. Message Code: Diffie-Hellman Key Exchange Init (30)

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

    Message Code: New Keys (21)

18. Όχι
19. Όχι, γιατί τα πακέτα είναι κρυπτογραφημένα
20. Το SSH είναι ασφαλέστερο από το telnet και το http basic auth, καθώς χρησιμοποιεί κρυπτογράφηση και δημόσια κλειδιά για την πιστοποίηση.

3. Υπηρεσία HTTPS

1. host 147.102.222.246
2. tcp.flags.syn==1 and tcp.flags.ack == 0
3. Στις θύρες 80 και 443
4. HTTP: 80, HTTPS:443
5. 7 συνδέσεις στην περίπτωση HTTP και 6 σύνδεση στην περίπτωση HTTPS
6. 57536,57546,57550,57552,57562,57568
7. Content Type 1 byte ,Version 2 bytes, Length 2 bytes
8. Handshake (22), Application Data (23), Change Cipher Spec (20), Alert (21), Heartbeat (24)
9. Client Hello
   Server Hello
   Encrypted Handshake Message
   Certificate
   Server Key Exchange
   Server Hello Done
   Client Key Exchange
   New Session Ticket
10. 1 μόνο Client Hello, όσες και οι συνδέσεις TCP για HTTPS
11. Version: TLS 1.0 (0x0301)
12. TLSv1.2
13. 32 bytes b08a παριστάνουν αυτό: GMT Unix Time: Nov 9, 2063 21:23:38.000000000 EET
14. Cipher Suites (17 suites)
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
    Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
15. Extension: supported_versions (len=5)
    Type: supported_versions (43)
    Length: 5
    Supported Versions length: 4
    Supported Version: TLS 1.3 (0x0304)
    Supported Version: TLS 1.2 (0x0303)

16. ALPN Next Protocol: http/1.1
17. Version: TLS 1.2 (0x0303)
18. 32 bytes afb1
19. Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
20. αλγόριθμοι ανταλλαγής κλειδιών: ecdhe rsa
    Αλγόριθμοι πιστοποίησης ταυτότητας: rsa
    Αλγόριθμοι κρυπτογράφησης: aes
    συνάρτηση κατακερματισμού: sha
21. Compression Method: null (0)
22. Length: 6205
23. 4
    Certificate Length: 1930
    Certificate Length: 1769
    Certificate Length: 1413
    Certificate Length: 1078
24. 5
25. Pubkey Length: Pubkey :65 0416c
    Pubkey Length: Pubkey :65 04340
26. μήκος εγγραφής TLS 6 bytes Μήκος μηνύματος Length: 1
27. Length: 40
28. Nai
29. Οχι
30. Και απο της δυο πλευρές
31. -
32. Δεν φαίνεται κάτι στο HTTPS(σε αντίθεση με το HTTP) γιατί είναι όλα κρυπτογραφημένα
33. Το https είναι πολύ πιο ασφαλές από το απλό http, καθώς πιστοποιεί την αυθεντικότητα μέσω των certificates, εξασφαλίζει την εμπιστευτικότητα μέσω κρυπτογράφησης και την ακεραιότητα.