12η Εργαστηριακή Άσκηση στα Δίκτυα Υπολογιστών

Ονοματεπώνυμο	Γεώργιος Στεφανάκης
Αρ. Μητρώου	el18436
Ομάδα	4
Λειτουργικό Σύστημα	Manjaro Linux x86_64
Διεύθυνση IP	147.102.131.167
Διεύθυνση MAC	b4:69:21:5e:da:03
Ημερομηνία	2023-01-16

1. Πιστοποίηση αυθεντικότητας στο πρωτόκολλο HTTP

1.1. 401 Authorization Required
1.2. WWW-Authenticate
1.3. Υπάρχει και το πεδίο Authorization
1.4. Authorization: Basic ZWR1LWR5OnBhc3N3b3Jk
1.5. edu-dy:password
1.6. Είναι πολύ εύκολο να πρακαμφθεί από οποιονδήποτε.

2. Υπηρεσία SSH – Secure SHell

2.1. TCP
2.2. Ports: 63232 (client), 22 (server)
2.3. Port 22
2.4. ssh
2.5. Έκδοση πρωτοκόλλου: SSH-2.0, Έκδοση λογισμικού: OpenSSH_6.6.1_hpn13v11, Σχόλια: FreeBSD-20140420
2.6. Έκδοση πρωτοκόλλου του εξυπηρετητή: ”SSH-2.0”, έκδοση λογισμικού: ”OpenSSH 8.1”
2.7. Το πλήθος τους είναι 10. Οι 2 πρώτοι είναι, οι curve25519-sha256, curve25519-sha256@libssh.org.
2.8. Το πλήθος τους είναι 13. Ο πρώτος είναι, ο ecdsa-sha2-nistp256-cert-v01@openssh.com.
2.9. Το πλήθος τους είναι 6. Οι 2 πρώτοι είναι, οι chacha20-poly1305@openssh.com, aes128-ctr.
2.10. Το πλήθος τους είναι 10. Οι 2 πρώτοι είναι, οι umac-64-etm@openssh.com, umac-128-etm@openssh.com.
2.11. Το πλήθος τους είναι 3. Οι 2 πρώτοι είναι, οι none, zlib@openssh.com.
2.12. Είναι ο ecdh-sha2-nistp256, και τον εμφανίζει το Wireshark σε παρένθεση δίπλα στο πεδίο Key Exchange, “Key Exchange (method:ecdh-sha2-nistp256)”.
2.13. Είναι ο ”aes128-ctr”.
2.14. Είναι ο ”umac-64@openssh.com”.
2.15. Είναι ο ”none”.
2.16. Ναι, σε παρένθεση δίπλα στο πεδίο SSH Version 2, “SSH Version 2 (encryption:aes128-ctr mac:umac-64@openssh.com compression:none)”
2.17. Τους ‘Elliptic Curve ...’, ‘New Keys’ και ‘Encrypted packet’
2.18. Όχι, είναι κρυπτογραφημένα.
2.19. Το SSH προσφέρει πολύ μεγαλύτερη ασφάλεια σε σχέση με άλλα πρωτόκολλα όπως π.χ. Telnet, καθώς χρησιμοποιεί RSA key pairs για την διαπίστευση του πελάτη, τεχνική που θεωρείται πολύ πιο ασφαλής. Λόγω του public key, μπορεί να επιβεβαιώσει την αυθεντικότητα των δύο πλευρών, ενώ παρέχει κρυπτογράφηση με πολλούς διαφορετικούς αλγορίθμους, πράγμα που το καθιστά πολύ ευέλικτο και ασφαλές.

3. Υπηρεσία HTTPS

3.1. host 147.102.40.19

3.2. tcp.seq == 0 and tcp.ack == 0
3.3. Στις θύρες 80 και 443
3.4. 80 → http, 443 → https
3.5. Στην http έγιναν 7 συνδέσεις, ενώ για την https έγιναν 6 συνδέσεις.
3.6. Είναι οι, 55643, 55644, 55647, 55648, 55649, 55650.
3.7. Είναι τα Content Type: 1 byte, Version: 2 bytes, Length: 2 bytes
3.8. Change Cipher Spec – 20, Alert – 21, Handshake – 22, Application – 23
3.9. TLS1.0
3.10. Client Hello, Server Hello, Certificate, Server Key Exchange, Server Hello Done, Encrypted Handshake Message, New Session Ticket
3.11. Έστειλε 6 μυνήματα Client Hello, κάθε ένα αντιστοιχεί σε μια σύνδεση TCP.
3.12. TLS1.2
3.13. ?
3.14.