ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΑΘΗΜΑ: «ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ (8ο ΕΞΑΜΗΝΟ)»

ΚΑΘΗΓΗΤΕΣ: ΚΟΤΖΑΝΙΚΟΛΑΟΥ ΠΑΝΑΓΙΩΤΗΣ

ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ:

ΔΗΜΗΤΡΕΛΛΟΣ ΠΑΝΑΓΙΩΤΗΣ, Π17026

ΚΑΡΑΜΠΟΪΚΗΣ ΝΙΚΟΛΑΟΣ, Π17040

ΡΟΥΝΤΟΥ ΑΝΝΑ-ΦΑΝΗ, Π17113

4η Άσκηση - Ασφάλεια στο SSL/TLS

ΠΕΡΙΕΧΟΜΕΝΑ

1. Να αναλύσετε δύο επιθέσεις στο πρωτόκολλο SSL/TLS.

1.1 Heartbleed attack (CVE-2014-0160).

Το Heartbleed είναι ένα σφάλμα λογισμικού που προκαλεί κενό ασφάλειας (security bug) στην ανοιχτού κώδικα βιβλιοθήκη κρυπτογραφίας OpenSSL, που χρησιμοποιείται ευρέως στο πρωτόκολλο ασφάλειας επιπέδου μεταφοράς του Διαδικτύου TLS (Transport Layer Security). Πρόκειται για ένα τρωτό σημείο, που οφείλεται σε απουσία ελέγχου ορίων, στην επέκταση heartbeat του πρωτοκόλλου TLS.

a. Τρόπος λειτουργίας της επίθεσης.

Η επέκταση RFC 6520 (Heartbeat) ελέγχει τις ασφαλείς τηλεπικοινωνιακές ζεύξεις βάσει πρωτοκόλλων TLS/DTLS επιτρέποντας στον υπολογιστή στη μία άκρη της σύνδεσης να αποστείλει ένα «Αίτημα Heartbeat», που περιέχει το φορτίο, τυπικά μία συμβολοσειρά, μαζί με το μήκος της, εκφρασμένου ως ενός ακεραίου 16 ψηφίων. Ο άλλος υπολογιστής, πρέπει να αποστείλει πίσω στον αποστολέα το ίδιο ακριβώς μήνυμα.

Οι επηρεαζόμενες εκδόσεις του OpenSSL δεσμεύουν μία προσωρινή περιοχή στη μνήμη για το επιστρεφόμενο μήνυμα βάσει του πεδίου που ορίζει το μήκος στο μήνυμα αίτησης, χωρίς να ελέγχουν το πραγματικό μέγεθος του μηνύματος. Εξαιτίας αυτής της αποτυχίας ελέγχου ορίων, το επιστρεφόμενο μήνυμα περιέχει το αρχικό μήνυμα, που δυνητικά ακολουθείται από οτιδήποτε άλλο παρείσφρησε στη δεσμευμένη περιοχή μνήμης.

Μπορεί κάποιος να εκμεταλλευτεί το Heartbleed στέλνοντας ένα κλεψίτυπο αίτημα Heartbeat. Προϋπόθεση να έχει μικρό όγκο με πεδίο μήκους με μεγάλη δηλωμένη ψευδή τιμή. Έτσι, ο στόχος (συνήθως εξυπηρετητής) αποστέλει αίτημα απάντησης, επιτρέποντας στον επιτιθέμενο να διαβάσει ως και 64 kilobytes μνήμης από τον υπολογιστή - θύμα, που πιθανόν να περιέχουν χρήσιμες πρόσφατες πληροφορίες σύνδεσης μέσω OpenSSL.

b. Οπτική του επιτιθέμενου.

Ο επιτιθέμενος για να πραγματοποιήσει μια τέτοια επίθεση θα χρειάζεται να γνωρίζει αν το θύμα είναι ευάλωτο σε αυτήν την ευπάθεια.

Πιο συγκεκριμένα θα πρέπει να γνωρίζει την θύρα του θύματος που είναι ο ευάλωτος webserver καθώς και την IP του. Κοιτάει δηλαδή αν το πρωτόκολλο sll για την θύρα αυτή φαίνεται να είναι version 1.0.1 ή κάποια beta version 1.0.2. Αυτήν την πληροφορία μπορεί να την συλλέξει με διάφορα εργαλεία scanning (π.χ nmap) εφόσον η πληροφορία είναι εμφανής.

Έχοντας κάνει το κατάλληλο enumeration ο επιτιθέμενος μπορεί να πραγματοποιήσει την επίθεση τρέχοντας ένα verified python script , heartbleed.py(https://github.com/ctfs/write-ups-2014/blob/master/plaid-ctf-2014/heartbleed/heartbleed.py), γραμμένο με τέτοιον τρόπο ώστε να ξεγελάει το πρωτόκολλο και να παίρνει πίσω τα ίσως ευαίσθητα και άλλοτε σημαντικά στοιχεία του συστήματος.

c. Αν και πόσο είναι πρακτικά εφικτή η επίθεση.

Η ευπάθεια αυτή είχε ανακαλυφθεί και επιδιορθωθεί το 2014. Στην σύγχρονη εποχή εν έτη 2021 η επιτυχία αυτής της επίθεση είναι σχετικά σπάνια καθώς τα συστήματα έχουν αναβαθμισμένες εκδώσεις του openssl με αποτέλεσμα αυτή η ευπάθεια στο heartbeat module να μην είναι πλέον υπαρκτή. Παρόλα αυτά ακόμα υπάρχουν συστήματα που δεν έχουν αναβαθμιστεί.

d. Τι μέτρα πρόληψης, σε επίπεδο υλοποίησης, διαμόρφωσης και λογισμικού, υπάρχουν σήμερα για αυτή την επίθεση.

Οι ευπαθείς εκδόσεις είναι από την 1.0.1 μέχρι και τις beta 1.0.2. Ύστερες εκδόσεις (1.0.1g και μετά) και προηγούμενες εκδόσεις (1.0.0 και παλαιότερες) δεν είναι τρωτές σε αυτό το κενό ασφάλειας.

Έτσι λοιπόν το καλύτερο μέτρο πρόληψης για αυτήν την επίθεση είναι η αναβάθμιση του OpenSSL σε κάποια πιο καινούργια και ασφαλή έκδοση.

1.2 BEAST attack.

Το BEAST σημαίνει Browser Exploit Against SSL / TLS. Είναι μια επίθεση εναντίον τρωτών σημείων του δικτύου στο πρωτόκολλο TLS 1.0 και παλαιότερα. Σύμφωνα με έρευνα που έγινε για την έκθεση ευπάθειας εφαρμογών ιστού του 2020 Acunetix, το 30,7% των σαρωμένων διακομιστών ιστού εξακολουθούν να έχουν ενεργοποιημένο το TLS 1.0, πράγμα που σημαίνει ότι είναι ευαίσθητα στην επίθεση BEAST.

a. Τρόπος λειτουργίας της επίθεσης.

Η επίθεση με την οποία χρησιμοποιούμαι μια αλυσίδα cipher block με σκοπό την προσάρτηση μιας επιλεγμένης επίθεση κειμένου plaintext με προβλέψιμα διανύσματα αρχικοποίησης (IV) έναντι ssl/tls (ή αλλιώς BEAST) λειτουργεί με τον εξής τρόπο:

Αρχικά ο επιτιθέμενος αξιοποιεί μία κρυπτογραφική επίθεση που λέγεται plaintext μαντεύοντας ουσιαστικά το περιεχόμενο του κρυπτογραφημένου κειμένου. Στην συνέχεια για να μπορέσει να ελέγξει το κατά πόσο είναι σωστή η μαντεψιά του χρειάζεται ένα μαντείο , το οποίο ουσιαστικά είναι ένα θεωρητικό κουτί το οποίο απαντά σε κάθε query με μία πραγματικά τυχαία απόκριση η οποία επιλέγεται από το domain εξόδου. Το κρυπτογραφικό πρωτόκολλο tls όμως , χρησιμοποιεί μηχανισμούς άμυνας για να αντιμετωπίσει την χρήση Plaintext. Χρησιμοποιεί IVs το οποίο έχει ως αποτέλεσμα να γίνεται κρυπτογράφηση πριν την αποστολή του μηνύματος ώστε το ίδιο κείμενο να είναι διαφορετικό αν σταλεί δυο φορές. Επίσης γίνεται χρήση αλυσίδα block cipher (CBC) το οποίο σε μεγάλα κείμενα χρησιμοποιεί ως IV το προηγούμενο κρυπτογραφημένο block για το κρυπτογραφημένο Plaintext που ακολουθεί. Οι δύο αυτές μέθοδοι αντιμετώπισης της επίθεσης δεν είναι τέλειοι αφού ο επιτιθέμενος μπορεί να μαντέψει το IV το οποίο θα χρησιμοποιηθεί για την κρυπτογράφηση του Plaintext που ελέγχει ο επιτιθέμενος , το οποίο μάλιστα έχει χρησιμοποιηθεί για να μαντέψει το μήνυμα που έχει σταλθεί. Παρατηρήθηκε λοιπόν ότι στις εκδόσεις tls 1.0 και ssl 3.0 σε κάθε session χρησιμοποιούν πολλαπλά πακέτα σε σειρά στα οποία γίνεται χρήση του IV το οποίο είναι το κρυπτογραφημένο μπλοκ κειμένου που χρησιμοποιήθηκε στο αμέσως προηγούμενο πακέτο με αποτέλεσμα το κάθε session να είναι ένα μεγάλο μήνυμα. Αυτό έχει ως αποτέλεσμα ο επιτιθέμενος να μπορεί να δει αν το κρυπτογραφημένο κείμενο ταιριάζει χρησιμοποιώντας το session cookie ΄,το οποίο αρχικά είναι προβλέψιμο και στην συνέχεια δείχνει στον επιτιθέμενο ποιο IV χρησιμοποιείται. Άρα, βάσει των παραπάνω ο επιτιθέμενος ο οποίος κάνει sniff στο δίκτυο μπορεί να μαθαίνει ποια IV χρησιμοποιούνται. Παρουσιάζεται όμως ξανά ένα πρόβλημα. Είναι δύσκολο για τον επιτιθέμενο να μαντέψει και τα 16 byte ενός cookie. Για να λυθεί λοιπόν αυτό το πρόβλημα ο επιτιθέμενος μπορεί να ελέγξει τα όρια του μπλοκ κρυπτογράφησης απομονώνοντας κάθε φορά ένα μόνο byte , και ουσιαστικά αφού βρει το πρώτο προχωράει στο επόμενο αλλάζοντας τα όρια τα οποία έχει θέση. Συγκεκριμένα εάν το cookie είναι κωδικοποιημένο σε Base64 χρειάζονται 32 γύροι για κάθε Byte.

b. Οπτική του επιτιθέμενου.

1. Παθητικό δίκτυο υποκλοπής: Ο επιτιθέμενος πρέπει να "πιάνει" κρυπτογραφημένα HTTPS request ώστε να γνωρίζει το κρυπτογραφημένο κείμενο του της κρυφής τιμής του IV για οποιοδήποτε block κρυπτογράφησης.

2. Προνομιακό σχήμα επιλεγμένου ορίου: Ο επιτιθέμενος μπορεί να ελέγξει σε ποιο σημείο του cookie στέλνεται το κείμενο προσθέτοντας παραμέτρους στο URL η με το να ρυθμίζει τις επικεφαλίδες, κάτι που του δίνει την δυνατότητα να δημιουργεί block τα οποία περιέχουν με 1 γνωστό και 15 άγνωστα bytes.

3. Chosen blockwise plaintext injection privilege: Ο επιτιθέμενος μαντεύει τα plaintext που σχετίζονται με τα block κρυπτογραφημένου κειμένου τα οποία γνωρίζει μέσα από το παθητικό δίκτυο υποκλοπής.

Αναλυτικότερα, κάνει έγχυση plaintext block της επιλογής του τα οποία κρυπτογραφούνται. Έτσι του δίνεται η δυνατότητα να χρησιμοποιεί το περιηγητή του χρήστη ως ένα encryption oracle.

c. Αν και πόσο είναι πρακτικά εφικτή η επίθεση.

Η συγκεκριμένη επίθεση είναι δύσκολο να πραγματοποιηθεί καθώς οι περιηγητές χρησιμοποιούν την πολιτική κοινής πηγής (SOP) . Ο επιτιθέμενος πρέπει να έχει την δυνατότητα να παρακολουθήσει το δίκτυο του χρήστη, χρησιμοποιώντας κάποια επίθεση όπως Phising ή Mitm, ώστε να μπορέσει να καταγράψει το κρυπτογραφημένο cookie του χρήστη. Τέλος ο επιτιθέμενος αφού χρησιμοποιήσει κάποια τεχνική Sop bypass θα προσπαθήσει να μαντέψει το session cookie μέσα από τα συνεχόμενα request ώστε να δει αν το κρυπτογραφημένο κείμενο ταιριάζει με το κρυπτογραφημένο cookie session που καταγράφηκε.

d. Τι μέτρα πρόληψης, σε επίπεδο υλοποίησης, διαμόρφωσης και λογισμικού, υπάρχουν σήμερα για αυτή την επίθεση.

1. Ενημέρωση των Browser και διάφορων ευάλωτων τεχνολογιών όπως η Java με τα τελευταία patch.

2. Χρήση TLS 1.2.

3. Μετεγκαταση προστατευμένων υπηρεσιών TLS χωρίς προβλήματα συμβατότητας, όπως ορισμένα VPN, στο TLS 1.2.

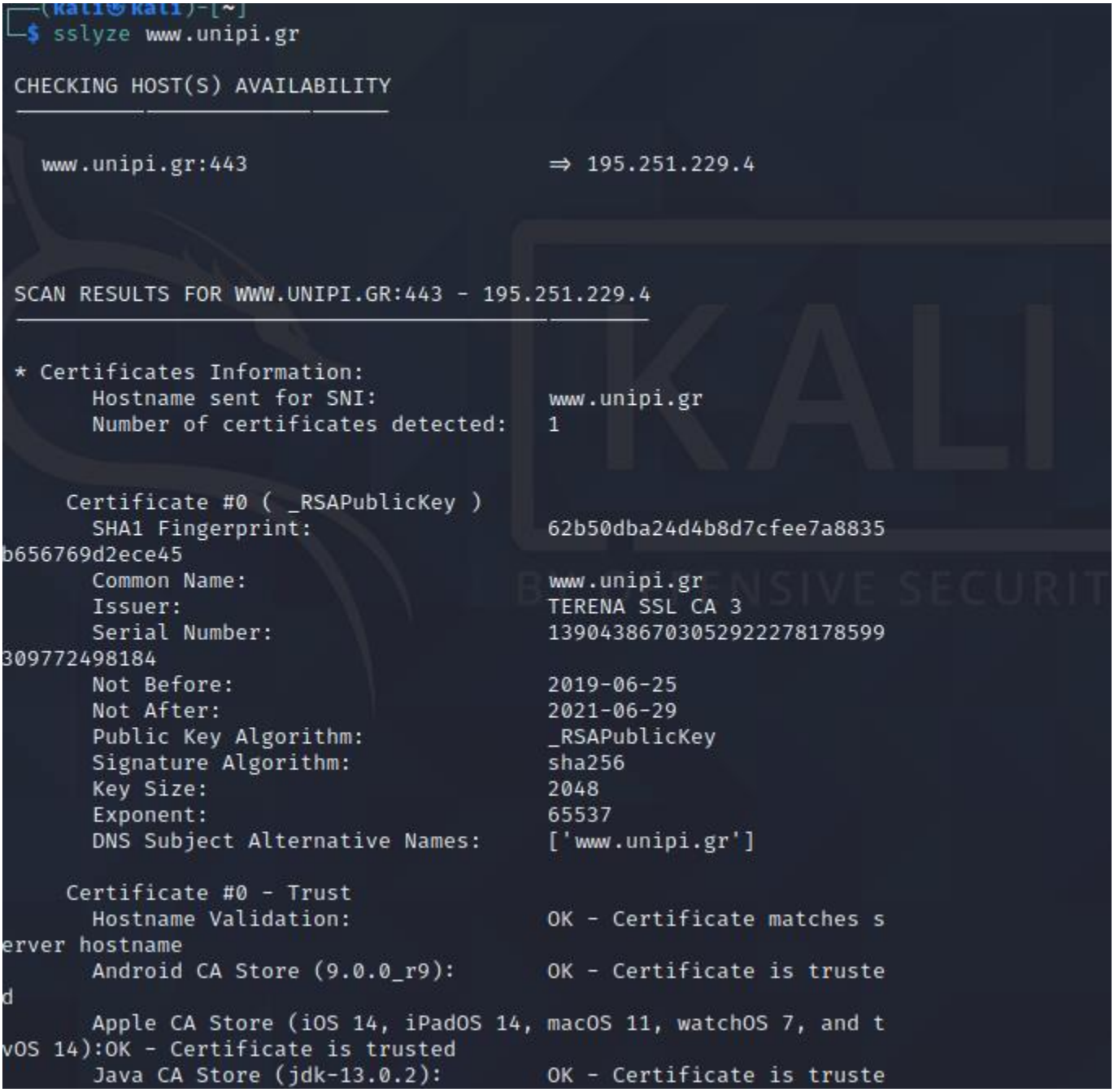
4. Απενεργοποίηση αιτημάτων πολλαπλής προσέλευσης στη μεριά του διακομιστή στις περιπτώσεις που δεν χρειάζεται.

5. Απενεργοποίηση υποστήριξης σε όσους δεν χρησιμοποιούν TLS 1.2.

2. Χρησιμοποιείστε γνωστά εργαλεία ανίχνευσης ώστε να επαληθεύεστε την ασφαλή λειτουργία του ssl σε web server (ενδεικτικά, sslscan, sslyze κτλ).

Τρέχουμε την εντολή:

sslyze www.unipi.gr



Βλέπουμε ότι εμφανίζονται οι πληροφορίες για την ιστοσελίδα. Μας δείχνει το Fingerprint, το όνομα και λοιπές πληροφορίες και στην συνέχεια εμφανίζεται αν τα πιστοποιητικά είναι έγκυρα αν ισχύουν κάποια πρωτόκολλα.

Ύστερα για τα πρωτόκολλα του TLS προσπαθεί να συνδεθεί με τα Cipher Suites και ο Server ανταποκρίνεται σε κάποια από αυτά δίνοντας μας κάποιες πληροφορίες σχετικά με τους αλγορίθμους που χρησιμοποιούνται και με τις ιδιότητες των Cipher Suites που εντοπίζουν στην ιστοσελίδα, πχ. αν είναι ασφαλής από επιθέσεις τύπου OpenSSL CCS Injection.

```
d
      Mozilla CA Store (2021-01-24):     OK - Certificate is truste
d
      Windows CA Store (2021-01-24):     OK - Certificate is truste
d
      Symantec 2018 Deprecation:         OK - Not a Symantec-issued
 certificate
      Received Chain:                    www.unipi.gr ⟶ TERENA SS
L CA 3
      Verified Chain:                    www.unipi.gr ⟶ TERENA SS
L CA 3 ⟶ DigiCert Assured ID Root CA
      Received Chain Contains Anchor:    OK - Anchor certificate no
t sent
      Received Chain Order:              OK - Order is valid
      Verified Chain contains SHA1:      OK - No SHA1-signed certif
icate in the verified certificate chain

    Certificate #0 - Extensions
      OCSP Must-Staple:                  NOT SUPPORTED - Extension
not found
      Certificate Transparency:          OK - 3 SCTs included

    Certificate #0 - OCSP Stapling
                                         NOT SUPPORTED - Server did
 not send back an OCSP response

 * TLS 1.0 Cipher Suites:
    Attempted to connect using 80 cipher suites.

    The server accepted the following 13 cipher suites:
       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                256

       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                128

       TLS_RSA_WITH_AES_256_CBC_SHA                     256

       TLS_RSA_WITH_AES_128_CBC_SHA                     128

       TLS_RSA_WITH_3DES_EDE_CBC_SHA                    168

       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA               256
ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA               128
ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA              168
ECDH: prime256v1 (256 bits)
       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA            256
DH (2048 bits)
       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA            128
DH (2048 bits)
       TLS_DHE_RSA_WITH_AES_256_CBC_SHA                 256
```

```
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA                    256
DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA                    128
DH (2048 bits)
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA                   168
DH (2048 bits)

     The group of cipher suites supported by the server has the foll
owing properties:
       Forward Secrecy                    OK - Supported
       Legacy RC4 Algorithm               OK - Not Supported


 * Downgrade Attacks:
       TLS_FALLBACK_SCSV:                 OK - Supported

 * OpenSSL CCS Injection:
                                          OK - Not vulnerable to Ope
nSSL CCS injection

 * ROBOT Attack:
                                          OK - Not vulnerable.

 * TLS 1.2 Cipher Suites:
     Attempted to connect using 156 cipher suites.

     The server accepted the following 25 cipher suites:
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                   256

        TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                   128

        TLS_RSA_WITH_AES_256_GCM_SHA384                     256

        TLS_RSA_WITH_AES_256_CBC_SHA256                     256

        TLS_RSA_WITH_AES_256_CBC_SHA                        256

        TLS_RSA_WITH_AES_128_GCM_SHA256                     128

        TLS_RSA_WITH_AES_128_CBC_SHA256                     128

        TLS_RSA_WITH_AES_128_CBC_SHA                        128

        TLS_RSA_WITH_3DES_EDE_CBC_SHA                       168

        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384               256
ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384               256
ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                  256
ECDH: prime256v1 (256 bits)
```

```
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA                    256
DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA                    128
DH (2048 bits)
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA                   168
DH (2048 bits)

     The group of cipher suites supported by the server has the foll
owing properties:
       Forward Secrecy                    OK - Supported
       Legacy RC4 Algorithm               OK - Not Supported


 * Downgrade Attacks:
       TLS_FALLBACK_SCSV:                 OK - Supported

 * OpenSSL CCS Injection:
                                          OK - Not vulnerable to Ope
nSSL CCS injection

 * ROBOT Attack:
                                          OK - Not vulnerable.

 * TLS 1.2 Cipher Suites:
     Attempted to connect using 156 cipher suites.

     The server accepted the following 25 cipher suites:
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                   256

        TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                   128

        TLS_RSA_WITH_AES_256_GCM_SHA384                     256

        TLS_RSA_WITH_AES_256_CBC_SHA256                     256

        TLS_RSA_WITH_AES_256_CBC_SHA                        256

        TLS_RSA_WITH_AES_128_GCM_SHA256                     128

        TLS_RSA_WITH_AES_128_CBC_SHA256                     128

        TLS_RSA_WITH_AES_128_CBC_SHA                        128

        TLS_RSA_WITH_3DES_EDE_CBC_SHA                       168

        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384               256
ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384               256
ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                  256
ECDH: prime256v1 (256 bits)
```

Έπειτα μας εμφανίζεται τα υποστηριζόμενα curves τα οποία χρησιμοποιεί ο server για το πρωτόκολλο TLS 1.1.

```
DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA                256
DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA                128
DH (2048 bits)
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA               168
DH (2048 bits)

     The group of cipher suites supported by the server has the foll
owing properties:
       Forward Secrecy                    OK - Supported
       Legacy RC4 Algorithm               OK - Not Supported


 * Elliptic Curve Key Exchange:
       Supported curves:                  prime256v1, secp384r1, sec
p521r1, secp256k1
       Rejected curves:                   sect409k1, secp160k1, sect
163r2, sect409r1, secp160r1, sect193r1, sect571k1, secp160r2, sect19
3r2, sect571r1, secp192k1, X25519, sect233k1, secp224k1, X448, sect2
33r1, secp224r1, sect239k1, sect283k1, sect163k1, sect283r1, prime19
2v1, sect163r1

 * TLS 1.3 Cipher Suites:
     Attempted to connect using 5 cipher suites; the server rejected
 all cipher suites.

 * OpenSSL Heartbleed:
                                        OK - Not vulnerable to Hea
rtbleed

 * SSL 2.0 Cipher Suites:
     Attempted to connect using 7 cipher suites; the server rejected
 all cipher suites.

 * Session Renegotiation:
       Client Renegotiation DoS Attack:   OK - Not vulnerable
       Secure Renegotiation:              OK - Supported

 * SSL 3.0 Cipher Suites:
     Attempted to connect using 80 cipher suites; the server rejecte
d all cipher suites.

 * Deflate Compression:
                                        OK - Compression disabled

 * TLS 1.2 Session Resumption Support:
      With Session IDs: OK - Supported (5 successful resumptions out
 of 5 attempts).
      With TLS Tickets: OK - Supported.
```

```
ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256            128
ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256            128
ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA               128
ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA              168
ECDH: prime256v1 (256 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA            256
DH (2048 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA            128
DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_GCM_SHA384              256
DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA256              256
DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA                 256
DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256              128
DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA256              128
DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA                 128
DH (2048 bits)
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA                168
DH (2048 bits)

     The group of cipher suites supported by the server has the foll
owing properties:
       Forward Secrecy                    OK - Supported
       Legacy RC4 Algorithm               OK - Not Supported


 * TLS 1.1 Cipher Suites:
     Attempted to connect using 80 cipher suites.

     The server accepted the following 13 cipher suites:
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                256

        TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                128

        TLS_RSA_WITH_AES_256_CBC_SHA                     256

        TLS_RSA_WITH_AES_128_CBC_SHA                     128

        TLS_RSA_WITH_3DES_EDE_CBC_SHA                    168

        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA               256
ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA               128
```