Πανεπιστήμιο Αθηνών	Εαρινό 2014
ΥΣ13 Ασφάλεια Υπολογιστικών Συστημάτων	ΚΙΑΓΙΑΣ
Due: `6.6.2013`	Project #2

Επίθεσεις Man-in-the-middle εναντίον του TLS

Ο στόχος του δεύτερου project είναι να παίξετε το ρόλο ενός man-in-the-middle attacker εναντίον του πρωτοκόλλου TLS (RFC 5246[1]).

Ένα ηλεκτρονικό κατάστημα με όνομα webshop.com τρέχει στη διεύθυνση https://sbox.di.uoa.gr. Ενας αριθμός από έξι clients προσπαθούν να συνδεθούν με το webshop χρησιμοποιώντας το TLS. Το webshop έχει ένα πιστοποιητικό το οποίο υπογράφεται από την certification authority `Compsec CA`. Όλοι οι clients έχουν πρόσβαση στο self-signed certificate της `Compsec CA`.

Με κάθε ssh σύνδεση σας στο `sbox.di.uoa.gr`, οι έξι clients θα προσπαθήσουν με τη σειρά να συνδεθούν στο webshop. Θα δείτε το εξής μήνυμα:

```
timestamp: XXXXXXXXXX
forwarding webshop client requests to port YYYYY
```

Οι clients λόγω κάποιου misconfiguration θα προσπαθήσουν να συνδεθούν στην πόρτα YYYYY αντί της κανονικής (443) στην οποία ακούει το webshop. Αυτό δίνει σε εσάς την δυνατότητα να κάνετε ένα man-in-the-middle attack. Οι clients θα συνδεθούν με την σειρά και είναι οι εξής:

1. Mr. Blonde.
2. Mr. Blue.
3. Mr. Brown.
4. Mr. Orange.
5. Mr. Pink.
6. Mr. White.

Όταν ένας από τους clients συνδέεται με το webshop τότε προσπαθεί να αγοράσει κάποιο αντικείμενο συμπληρώνοντας τη φορμα του webshop με την πιστωτική του κάρτα. Ο στόχος σας είναι να βρείτε τις πιστωτικές κάρτες των clients κάνοντας διάφορες δοκιμές. Όλοι οι clients -- εκτός από έναν -- υλοποιούν το πρωτόκολλο TLS με κάποια αδυναμία ή λάθος που επιτρέπει να γίνει μια man-in-the-middle επίθεση. Οι αδυναμίες που υπάρχουν έχουν να κάνουν με το πως ελέγχουν τα πιστοποιητικά οι clients αλλά και το αν δεχονται ανωνυμη ανταλλαγή κλειδιών.

Για να διευκολυνθείτε στην υλοποίηση της επίθεσης θα χρησιμοποιήσετε το εργαλείο που έχει αναπτυχθεί[2] για το project που λέγεται `twistedeve` και είναι διαθέσιμο στο sbox. Η διεύθυνση του εργαλείου είναι `https://github.com/d-mo/TwistedEve` αν θέλετε να δείτε την υλοποίηση του.

Επίσης έχετε στην κατοχή σας ένα valid certificate από την `Compsec CA` το οποίο είναι στο όνομα `mysite.com`. Το certificate και το μυστικό κλειδί (αντίστοιχα τα αρχεία `mysite.com.crt` και

[1] T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2. http://tools.ietf.org/html/rfc5246.

[2] Δημήτρης Μωραΐτης, Επιθέσεις Ενδιαμέσου στο πρωτόκολλο TLS, http://crypto.di.uoa.gr/CRYPTO.SEC/Theses.html

`mysite.com.key`) βρίσκονται μέσα στον κατάλογο `/var/project2/` στο `sbox.di.uoa.gr`. Επίσης εκεί θα βρείτε και κάποια φίλτρα για την twistedeve (δείτε το documentation).

Οδηγίες παράδοσης του project. Πρέπει να δουλέψετε μόνοι σε αυτό το project. Πρέπει να γράψετε την αναφορά σας ηλεκτρονικά και να την παραδώσετε ηλεκτρονικά στη διεύθυνση :

`csec.di@gmail.com`

σε μορφή doc, ps η pdf αρχείου. Το e-mail πρέπει να έχει subject "project 2." Θα πρέπει να συμπεριλάβετε στην αναφορά κώδικα που τυχόν γράψατε και να εξηγήσετε όλο το συλλογιστικό σας για το πως κάνατε την επίθεση. Αν βρείτε κάποιες πιστωτικές κάρτες θα πρέπει να τις συμπεριλάβετε στην αναφορά σας μαζί με το timestamp XXXXXXXXXX.

Καθυστερημένες Υποβολές Project. Μπορείτε να χρησιμοποίησετε μέχρι 10 μέρες για να καθύστερησετε την παράδωση ενος project (συνολικά για όλο το εξάμηνο). Η ημερομηνία υποβολής κρίνεται η ημερομηνία που παραδίνεται το e-mail σας στον server.

Εξώφυλλο Project. Το εξώφυλλο του project σας πρέπει να περιέχει το όνομα σας, το ΑΜ σας, καθώς και τα στοιχεία "Project #2", "ΥΣ13 ΕΑΡΙΝΟ 2014" καθώς και μια ένδειξη για το πόσες μέρες καθυστέρησης χρησιμοποιήθηκαν (`0` αν καμμία).