ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Δρ. Μαριάς Ιωάννης
Επικ. Καθηγητής

Προπτυχιακό Πρόγραμμα Σπουδών
Χειμερινό εξάμηνο 2022-2023

Ασφάλεια Δικτύων
Εργαστηριακή Άσκηση OpenSSL

Βήματα εργασίας:

1) Αίτηση συμμετοχής στο project netsec.aueb.gr στο ~okeanos και στη συνέχεια η δημιουργία της Ιδεατής Μηχανής (VM). Μέχρι 9/12/2022 *
Οδηγίες στο eclass:
Έγγραφα/ LABS 2023 / Δημιουργία Ιδεατής Μηχανής_v2.pdf
Παράδοση στο eclass (Εργασίες) την IP (v4) (σε μορφή κειμένου)
Π.χ.: 123.45.67.89

2) Κυρίως εργασία. Μέχρι 23/12/2022
Παράδοση στο eclass (σε μορφή .pdf) σύντομο report.

3) Κατόπιν ειδοποίησης από τον διδάσκοντα, τερματισμός του VM.

ΣΗΜΑΝΤΙΚΟ:
Η εργασία είναι ατομική

Διαβάζετε τα FAQ στο eclass (Ιστολόγιο >> FAQ εργασίας OpenSSL)

Απορίες υποβάλετε στο eclass (είναι δημόσιες, μη συμπεριλάβετε credentials):
Συζητήσεις/ 3. OpenSSL

Ώρες γραφείου για απορίες κατόπιν επικοινωνίας

Τις ημέρες 21 & 22 Δεκεμβρίου στις 18:00 (περίπου) θα γίνεται μια φορά την ημέρα έλεγχος συνδεσιμότητας, στον οποίο θα ελέγχεται κατά πόσο λειτουργεί η σύνδεση του teacher με ssh καθώς είναι σημαντικό να λειτουργεί για να βαθμολογηθεί το μεγαλύτερο μέρος της εργασίας.
Τα αποτελέσματα θα δημοσιεύονται στο eclass:
Έγγραφα/ LABS 2023/ Προκαταρκτικά αποτελέσματα ελέγχου συνδεσιμότητας

* Συνιστώμενη ημερομηνία, προκειμένου να έχετε χρόνο για την υλοποίηση της εργασίας. Θα γίνουν δεκτές εκπρόθεσμες υποβολές της IP, καθώς και τροποποιήσεις αν προκύψουν.

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Ακολουθείστε πιστά τις οδηγίες δημιουργίας της Ιδεατής Μηχανής.
Αποτέλεσμα της διαδικασίας είναι να έχετε δημιουργήσει ένα VM με OS CentOS 7.
Η σύνδεση στο server γίνεται μόνο με SSH με τη χρήση οποιουδήποτε client (πχ PuTTY).
Για τη σύνδεση με SSH απαιτείται η χρήση AUEB VPN, οδηγίες εδώ.
Ρυθμίστε την πιστοποίηση να γίνεται μόνο με SSH keys.

Ζητούμενα εργασίας:

A. Δημιουργία χρήστη "teacher". Ο χρήστης teacher θα πρέπει να συνδέεται με ssh key.
Public key του χρήστη teacher στο eclass:
Έγγραφα/LABS 2023/Teacher's public key
(Σημείωση: για να ελέγξτε τη συνδεσιμότητα μπορείτε να προσθέσετε στο αρχείο με τα public keys (authorized_keys) πέρα από το public key του teacher σε νέα γραμμή και το δικό σας.)

B. Να δοθούν στον χρήστη «teacher» δικαιώματα read παντού στο /home και στο /root (στους φακέλους, τους υποφακέλους και τα αρχεία)
και να μην έχει κανένα δικαίωμα write στο /home (στον φάκελο, τους υποφακέλους και τα αρχεία)

C. Εγκατάσταση και παραμετροποίηση όλων των απαραίτητων services για να λειτουργεί ο server ως web-server με Apache.

D. Προσθήκη των απαραίτητων inbound rules στο service FirewallD του CentOS , ώστε http και https να είναι προσπελάσιμα από παντού. Περιορισμός της πρόσβασης με ssh μόνο μέσω AUEB VPN (αν η public ip σας στο vpn είναι άλλη από την 195.251.255.77 προσθέστε και τις 2) .
(screenshot με όλα τα rules στο report)
(Σημείωση: αν «κλειδωθείτε» έξω από το VM σας, μπορείτε να συνδεθείτε μέσω κονσόλας από το διαχειριστικό της υπηρεσίας ~okeanos και να κάνετε login με τα credentials σας)

E. Χρησιμοποιώντας το OpenSSL δημιουργήστε Certificate Authority (CA), CSR και ένα SSL certificate.
Στο Organizational Unit Name (OU) ορίστε τον ΑΜ σας (πχ: 3180000 και όχι p3180000).

F. Παραμετροποιήστε τον Apache προκειμένου να σερβίρει το πιστοποιητικό σας σε https και να ανακατευθύνει τα http σε https.
Βεβαιωθείτε ότι το όλο το SSL certificate chain εμφανίζεται σωστά.

G. Δημιουργήστε ένα απλό website με μόνο ένα πεδίο κειμένου με name="username" και ένα κουμπί υποβολής (submit).
Θα πρέπει αν γίνει υποβολή του ΑΜ σας (πχ: 3180000) να εμφανίζει ένα μήνυμα επιτυχίας, ενώ σε οποιαδήποτε άλλη περίπτωση μήνυμα αποτυχίας (να περιέχονται οι λέξεις «success» και «fail» αντίστοιχα)
Μπορείτε να χρησιμοποιήσετε οποιαδήποτε τεχνολογία.
Χρησιμοποιήστε ως DocumentRoot: /var/www/html

H. Δημιουργήστε ένα αρχείο txt με όνομα τον ΑΜ σας πχ: 3180000.txt

Αντιγράψτε το bash history σας μέσα στο txt (ιδανικά καθαρίστε το από περιττές εντολές). Αποθηκεύστε το txt στο home directory σας πχ: /root/3190000.txt

I. Υποβάλετε σύντομο report όπου θα συμπεριλάβετε:
   1. όλες τις αλλαγές στο configuration του Apache
   2. screenshot στο οποίο θα κάνετε list τα rules του (D)
   3. Μία παράγραφο για το πώς υλοποιήσατε και με ποιες εντολές το (E)
   4. Μία παράγραφο στην οποία θα περιγράφετε πως υλοποιήσατε το (G).

   Στο report να μην συμπεριλάβετε πρόσθετες πληροφορίες.