ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΜΑΘΗΜΑ: ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ, 2022-2023
ΔΙΔΑΣΚΟΝΤΕΣ: Γ. Στεργιόπουλος

2η Σειρά Ασκήσεων
Προθεσμία Παράδοσης: 30/12/2022

Άσκηση 1 [3 μονάδες]

Μία Αρχή Πιστοποίησης (CA) αποτελεί μια οντότητα υπεύθυνη για την έκδοση ψηφιακών πιστοποιητικών και την επαλήθευση ταυτότητας στο Διαδίκτυο. Παρόλο που οι δημόσιες CAs είναι μια δημοφιλής επιλογή για την επαλήθευση της ταυτότητας των ιστότοπων και άλλων υπηρεσιών που παρέχονται στο ευρύ κοινό, οι ιδιωτικές Cas χρησιμοποιούνται συνήθως για κλειστές ομάδες και ιδιωτικές υπηρεσίες.

Η δημιουργία μιας ιδιωτικής αρχής έκδοσης πιστοποιητικών θα σας επιτρέψει να διαμορφώσετε, να δοκιμάσετε και να εκτελέσετε προγράμματα που απαιτούν κρυπτογραφημένες συνδέσεις μεταξύ ενός πελάτη και ενός διακομιστή. Με μια ιδιωτική CA, μπορείτε να εκδίδετε πιστοποιητικά για χρήστες, διακομιστές ή μεμονωμένα προγράμματα και υπηρεσίες εντός της υποδομής σας.

Σε αυτήν την εργασία, καλείστε να δημιουργήσετε μια ιδιωτική αρχή έκδοσης πιστοποιητικών σε διακομιστή Ubuntu 20.04 και να εκπονήσετε τις ακόλουθες δευτερεύουσες εργασίες:

- Δημιουργία και υπογραφή ενός testing certificate με χρήση της δικής σας CA.
- Import το CA server's public certificate στο λειτουργικό σύστημα (operating system's certificate store) για δυνατότητα επιβεβαίωσης του chain of trust αναμεσα στην CA και σε χρήστες.
- Revoke certificates
- Distribute a Certificate Revocation List για να βεβαιωθείτε ότι μόνο εξουσιοδοτημένοι χρήστες και συστήματα μπορούν να χρησιμοποιούν υπηρεσίες της CA.

Κάθε βήμα σας πρέπει να το καταγράφετε και να το περιγράφετε με σύντομες φωτογραφίες και κείμενα, εν οίδει tutorial ή manual.

Άσκηση 2 [3 μονάδες]

Το OpenVPN είναι ένα λογισμικό υποστήριξης συνδέσεων SSL VPN που επεκτείνει την ασφάλεια δικτύου OSI επιπέδου 2 ή 3 χρησιμοποιώντας το βιομηχανικό πρότυπο πρωτόκολλο SSL / TLS. Το OpenVPN υποστηρίζει μεθόδους ελέγχου ταυτότητας πελάτη που βασίζονται σε πιστοποιητικά, έξυπνες κάρτες ή / και διαπιστευτήρια ονόματος χρήστη / κωδικού πρόσβασης και επιτρέπει την εφαρμογή πολιτικών ελέγχου πρόσβασης χρησιμοποιώντας κανόνες τείχους προστασίας που εφαρμόζονται στην εικονική διεπαφή VPN.

Σε αυτήν την εργασία, καλείστε να εγκαταστήσετε, να τεκμηριώσετε και να παρουσιάσετε βήμα προς βήμα την εγκατάσταση και τη διαμόρφωση ενός ελάτη / διακομιστή OpenVPN. Αυτό πρέπει να περιλαμβάνει τα ακόλουθα βήματα:

1. Installing OpenVPN και χρήση της δικής σας certificate authority (CA)
2. Δημιουργία των certificates και keys για τον OpenVPN server και πολλαπλούς (2) πελάτες.

3. Δημιουργία των configuration files για τον server και τους clients.
4. Περαιτέρω ρύθμιση του OpenVPN για να περιλαμβάνει επιπλέον μηχανήματα από το client subnet (μπορείτε να βάλετε ενδεικτικές, συμβολικές IP στο παράδειγμα).
5. Ενεργοποίηση και ρύθμιση του TLS-auth στο OpenVPN Security.

Κάθε βήμα σας πρέπει να το καταγράφετε και να το περιγράφετε με σύντομες φωτογραφίες και κείμενα, εν οίδει tutorial ή manual.

Άσκηση 3 [3 μονάδες]

Το IPSec είναι μια ασφαλής σουίτα πρωτοκόλλου δικτύου που αυθεντικοποιεί και κρυπτογραφεί πακέτα δεδομένων που αποστέλλονται μέσω ενός δικτύου IP. Αναπτύχθηκε από το Internet Engineering Task Force και, σε αντίθεση με το SSL το οποίο λειτουργεί σε επίπεδο εφαρμογής, το IPSec λειτουργεί σε επίπεδο δικτύου και μπορεί να χρησιμοποιηθεί εγγενώς με πολλά λειτουργικά συστήματα. Επειδή τα περισσότερα λειτουργικά συστήματα υποστηρίζουν το IPSec, μπορεί να χρησιμοποιηθεί χωρίς την ανάγκη για εγκατάσταση 3rd party εφαρμογών (σε αντίθεση με το OpenVPN).

Σε αυτό το task, καλείστε να στήσετε μια σημείο-προς-σημείο σύνδεση με IPSec χρησιμοποιώντας το Strongswan σε Ubuntu 20.04. Στο κείμενο που θα περιγράψετε, καλείστε να αναλύσετε και παρουσιάσετε τα ακόλουθα βήματα (μαζί με χρήση φωτογραφιών).

- Step 1: Enable Kernel Packet Forwarding
- Step 2: Install strongSwan in Debian and Ubuntu
- Step 3: Configure Security Gateways
- Step 4: Test IPSec connection and show printscreen results.

Κάθε βήμα σας πρέπει να το καταγράφετε και να το περιγράφετε με σύντομες φωτογραφίες και κείμενα, εν οίδει tutorial ή manual.

Άσκηση 4 [1 μονάδα]

Συγκρίνετε τις ανωτέρω τεχνολογίες και επεκτείνετε την ανάλυσή σας για το πώς αυτές συνεργάζονται/συνδυάζονται ή ανταγωνίζονται τις ακόλουθες αρχιτεκτονικές ασφάλειας που βασίζονται στην κρυπτογραφία:

- TOR network

- Zero Trust architecture

- Tunneling / Diodes communication channels