

Linux_Essentials_Ρύθμιση_ssh

Απομακρυσμένη σύνδεση SSH

Το **SSH** (Secure Shell) είναι ένα κρυπτογραφικό πρωτόκολλο δικτύου που επιτρέπει την ασφαλή λειτουργία υπηρεσιών δικτύου. Χρησιμοποιείται κυρίως για την ασφαλή απομακρυσμένη σύνδεση σε έναν άλλο H/Y-Server και εκτέλεση εντολών σε αυτών.

Τα παρακάτω βασίζονται σε διανομές Debian/Ubuntu

Για να εκμεταλλευτούμε το SSH στο Linux, θα πρέπει να εγκαταστήσουμε το εργαλείο openssh στον **τοπικό** μας H/Y (αν δεν υπάρχει):

```
sudo apt install openssh-client
```

και αντίστοιχα να εγκαταστήσουμε το παρακάτω πακέτο στον **απομακρυσμένο server**:

```
sudo apt install openssh-server
```

Στη συνέχεια θα πρέπει να **ξεκινήσουμε** την υπηρεσία ssh στον **server**:

```
sudo systemctl enable ssh
```

Και να **ελέγξουμε** ότι όντως "τρέχει":

```
sudo systemctl status ssh
```

Είμαστε έτοιμοι να **συνδεθούμε** στον απομακρυσμένο server (πχ στην IP 192.168.1.61):

```
ssh root@192.168.1.61
```

όπου ο `root` είναι ο χρήστης στον οποίο συνδεόμαστε και το `192.168.1.61` είναι η IP του server.

Για την επαλήθευση πληκτρολογούμε τον κωδικό του χρήστη `root`

Μια πρώτη ενέργεια που μπορούμε να κάνουμε, είναι να **ενημερώσουμε το σύστημα και τα πακέτα**:

```
apt update  
apt dist-upgrade
```

Ο παραπάνω τρόπος επαλήθευσης με κωδικό, όμως, δεν είναι ιδιαίτερα ασφαλής. Έτσι, δημιουργούμε **κλειδιά κρυπτογράφησης** (ένα δημόσιο και ένα ιδιωτικό), μέσω του **αλγορίθμου Ed25519**. Στον τοπικό μας H/Y γράφουμε:

```
ssh-keygen -t ed25519
```

Δημιουργούνται τα κλειδιά:

```
id_ed25519 ιδιωτικό κλειδί  
id_ed25519.pub δημόσιο κλειδί
```

Πατάμε `enter` για να αποθηκευτούν στον **προεπιλεγμένο κατάλογο** (`/home/user/.ssh`)

Αν θέλουμε ορίζουμε και κωδικό πρόσβασης (**passphrase**) για επιπλέον ασφάλεια.

Το δημόσιο κλειδί πρέπει να μεταφερθεί στον server, ενώ το **ιδιωτικό παραμένει στον τοπικό Η/Υ** και δεν το δίνουμε πουθενά!!

Στη συνέχεια, μεταφέρουμε το **δημόσιο κλειδί** στον server:

```
ssh-copy-id -i ~/.ssh/id_ed25519.pub root@192.168.1.61
```

Τα 2 αυτά κλειδιά μπορούν να χρησιμοποιηθούν και σε άλλες υπηρεσίες/server για ταυτοποίηση (github/gitlab, κτλ).

Τέλος, για να **συνδεόμαστε μόνο με κλειδιά ssh**, απενεργοποιούμε την επαλήθευση μέσω κωδικού στον server.

Ανοίγουμε το παρακάτω αρχείο στο **server**:

```
nano /etc/ssh/sshd_config
```

βρίσκουμε το πεδίο `PasswordAuthentication` και αλλάζουμε την τιμή από `yes` σε `no` :
Αφαιρούμε το `#` για να ενεργοποιηθεί η γραμμή:

```
PasswordAuthentication no
```

Αποθηκεύουμε το αρχείο.

Εκτελούμε επανεκκίνηση της υπηρεσίας ssh για να εφαρμοστούν οι ρυθμίσεις:

```
systemctl restart ssh
```

Τώρα η **επαλήθευση** πραγματοποιείται **μόνο μέσω των κλειδιών** και μόνο αν κάποιος έχει στην κατοχή του το ιδιωτικό μας κλειδί μπορεί να έχει πρόσβαση στο απομακρυσμένο μηχανήμά μας.

Χρήση του Secure copy (scp)

Αντιγραφή από το τοπικό Η/Υ στον server:

Για να αντιγράψουμε κάτι από το **τοπικό Η/Υ στον server** χρησιμοποιούμε το scp:

Παράδειγμα:

Εκτελούμε από το τερματικό του τοπικού Η/Υ

```
scp -r /home/user/dir/ root@192.168.1.61:/root
```

Στο παραπάνω αντιγράφουμε τον κατάλογο `dir` με όλα τα περιεχόμενα του, που βρίσκεται στο `home` του χρήστη `user` του τοπικού Η/Υ, προς το `home` του χρήστη `root` μέσα στον server.

Αντιγραφή από τον server στον τοπικό Η/Υ:

Εκτελούμε από το τερματικό του τοπικού Η/Υ

```
scp root@172.159.200.143:/απομακρυσμενη/διαδρομή/αρχείο.txt ~/
```

Εγκατάσταση και χρήση `ufw` (uncomplicated firewall)

Το `ufw` είναι το πιο απλό εργαλείο διαχείρισης firewall για πολλές διανομές.

Το εγκαθιστούμε στον **server**:

```
apt install ufw
```

Στη συνέχεια ορίζουμε να απαγορεύονται όλες οι εισερχόμενες συνδέσεις και να επιτρέπονται όλες οι εξερχόμενες:

```
ufw default deny incoming
```

```
ufw default allow outgoing
```

Προτού ενεργοποιήσουμε το `ufw` **επιτρέπουμε την είσοδο με ssh για να μην κλειδωθούμε απ' έξω**:

```
sudo ufw allow ssh
```

Τέλος, το ενεργοποιούμε:

```
sudo ufw enable
```

Για να ελέγξουμε την κατάστασή του:

```
sudo ufw status verbose
```

Το αρχείο διέπεται από την άδεια:

Creative Commons Αναφορά Δημιουργού - Μη Εμπορική Χρήση - Παρόμοια Διανομή 4.0
Διεθνές (CC BY-NC-SA 4.0)

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.el>

Ελληνική Ένωση Φίλων ΕΛ/ΛΑΚ (GreekLUG)

<https://www.greeklug.gr/>