



Πανεπιστήμιο Αιγαίου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών  
Συστημάτων

ICSD120 – Ασφάλεια Πληροφοριακών & Επικοινωνιακών Συστημάτων

ΑΣΚΗΣΗ 1:  
**ΕΓΚΑΤΑΣΤΑΣΗ ΕΞΥΠΗΡΕΤΗΤΗ ΛΣ LINUX  
ΕΝΔΥΝΑΜΩΣΗ ΕΞΥΠΗΡΕΤΗΤΗ/ΛΙΣΤΑ ΕΛΕΓΧΟΥ  
ΑΣΦΑΛΕΙΑΣ**

Διδάσκων: Γεώργιος Στεργιόπουλος

Υπεύθυνη Εργαστηρίου: Αναστασία Δούμα

**Φοιτητική ομάδα:**

**321/2019231 Φακιόλας Γεώργιος**

**321/2019127 Μανωλάκος Κωνσταντίνος**

**321/2021061 Σωματόπουλος Στυλιανός**



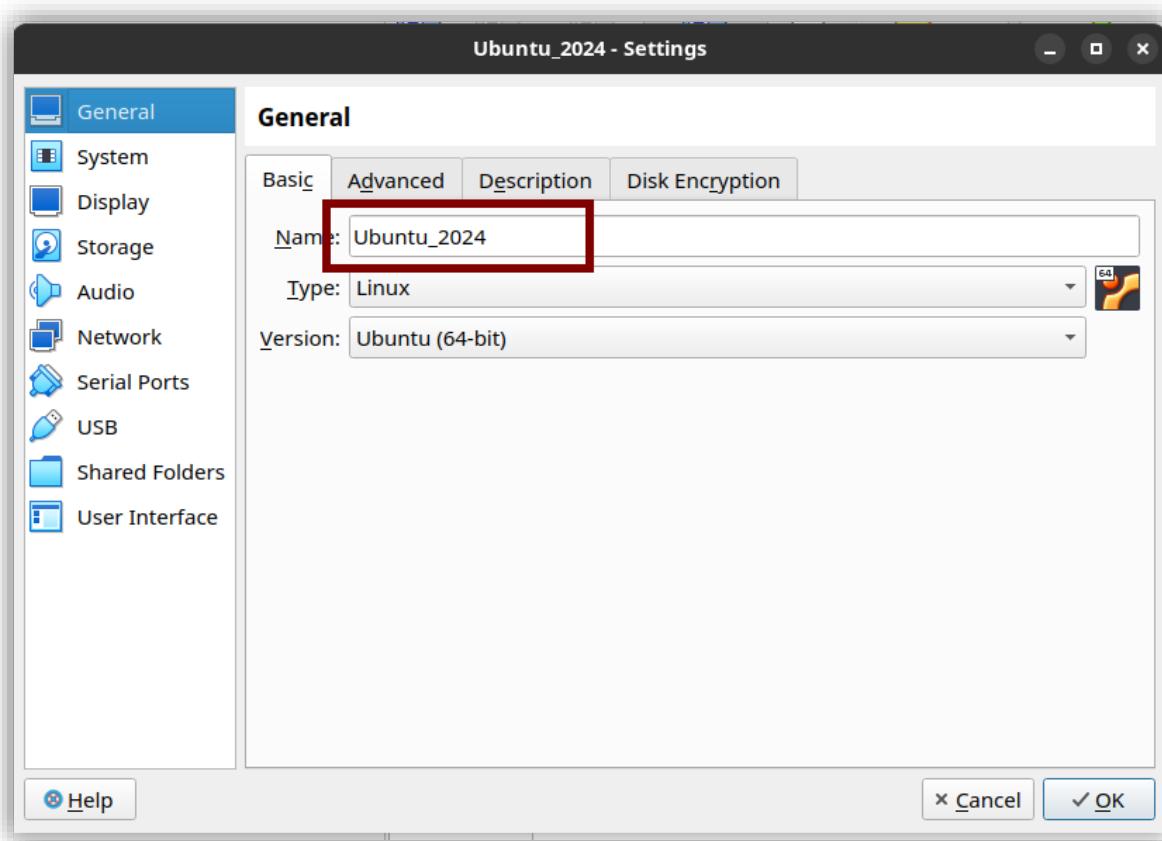
## Πίνακας Περιεχομένων

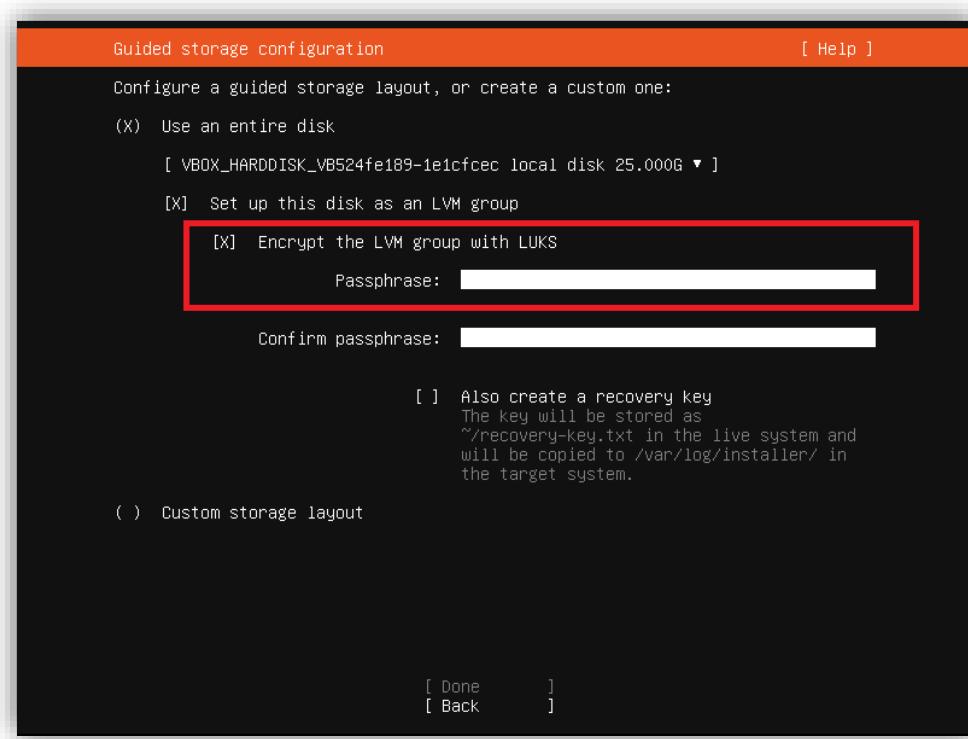
A. Αρχική εγκατάσταση και βασική παραμετροποίηση του λειτουργικού συστήματος.....	3
A1.....	3
A2.....	6
A3.....	12
A4.....	18
B. Διαμόρφωση και Διαχείριση Χρηστών Συστήματος .....	22
B1.....	22
B2.....	23
B3.....	26
B4.....	28
B5.....	29
B6.....	30
B7.....	32
B8.....	33
Γ. Καταγραφή και Παρακολούθηση Συστήματος .....	34
Γ1.....	34
Γ2.....	37
Γ3.....	39
Γ4.....	41
Δ. Εγκατάσταση υπηρεσιών στον εξυπηρετητή .....	44
Δ1.....	44
Δ2.....	50
Ε. Ενδυνάμωση του Λειτουργικού Συστήματος .....	56
ΣΤ. Αντίγραφα ασφαλείας και αποκατάσταση μετά από καταστροφή .....	59
Βιβλιογραφία .....	66



## A. Αρχική εγκατάσταση και βασική παραμετροποίηση του λειτουργικού συστήματος.

A1. Αρχικά θα πρέπει να εγκαταστήσετε μια διανομή του Linux. Μπορείτε να επιλέξετε όποια διανομή (Ubuntu, Fedora, openSUSE κλπ.) θεωρείτε ότι είναι πιο εύχρηστη για εσάς εφόσον πρώτα μελετήσετε τις απαιτήσεις της άσκησης. Εγκαταστήστε την τελευταία έκδοση που είναι διαθέσιμη για την διανομή που επιλέξατε. Ξεκινήστε με την ελάχιστη δυνατή εγκατάσταση του λειτουργικού συστήματος για να μειώσετε την επιφάνεια επίθεσης.





Εγκατάσταση όλων των ενημερώσεων και εκκαθάριση περισσευούμενου πακέτου.

Αφού μελετήσαμε διάφορες διανομές του λειτοργικού συστήματος Linux, επιλέξαμε το Ubuntu και συγκεκριμένα την έκδοση 20.04 λόγω της πληθόρας πληροφοριών που υπάρχουν στο διαδίκτυο και της ευκολίας χρήσης του. Έπειτα, από δική σας υπόδειξη επιλέξαμε την έκδοση του server την ελάχιστη δυνατή εγκατάσταση του λειτουργικού συστήματος για να μειώσουμε την επιφάνεια επίθεσης.

Στη συνέχεια αφού εγκαταστήσαμε το Virtual Box ξεκινήσαμε ένα καινούριο machine (που το ονομάσαμε skynet) το οποίο και φροντίσαμε να κρυπτογραφίσουμε για να διασφαλίσουμε ένα επιπλέον επίπεδο ασφαλείας. Έπειτα, εγκαταστήσαμε όλες τις απαραίτητες ενημερώσεις και φροντίσαμε να αφαιρέσουμε τα περιττά πακέτα. Μετά, όπως θα δείτε και σε όλα τα screenshot που έπονται, έχουμε δημιουργήσει ένα χρήστη με όνομα terminator (που δεν είναι μέρος των default χρηστών απλώς έπρεπε να δημιουργηθεί στη εκκίνηση και θα διαγραφεί στο τέλος μετά το πέρας της δημιουργίας του server). Τέλος, ως ένα έξτρα βήμα αλλάξαμε το shell από bash σε zsh για μεγαλύτερη ευκολία στη χρήση και ρυθμίσαμε το prompt ώστε να μας εμφανίζει τη κάθε ώρα όπως και μας ζητήθηκε.



```
[terminator@skynet ~]$ sudo apt update && sudo apt upgrade
2024-03-16T16:27:35.82+0200
Hit:1 http://gr.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://gr.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://gr.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
```

```
terminator@skynet ~]$ sudo apt autoremove
2024-03-16T16:29:59.84+0200
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  libevent-2.1-7 libunbound8 openvswitch-common python3-openvswitch
  python3-sortedcontainers
0 upgraded, 0 newly installed, 5 to remove and 2 not upgraded.
After this operation, 5,054 kB disk space will be freed.
Do you want to continue? [Y/n] █
```



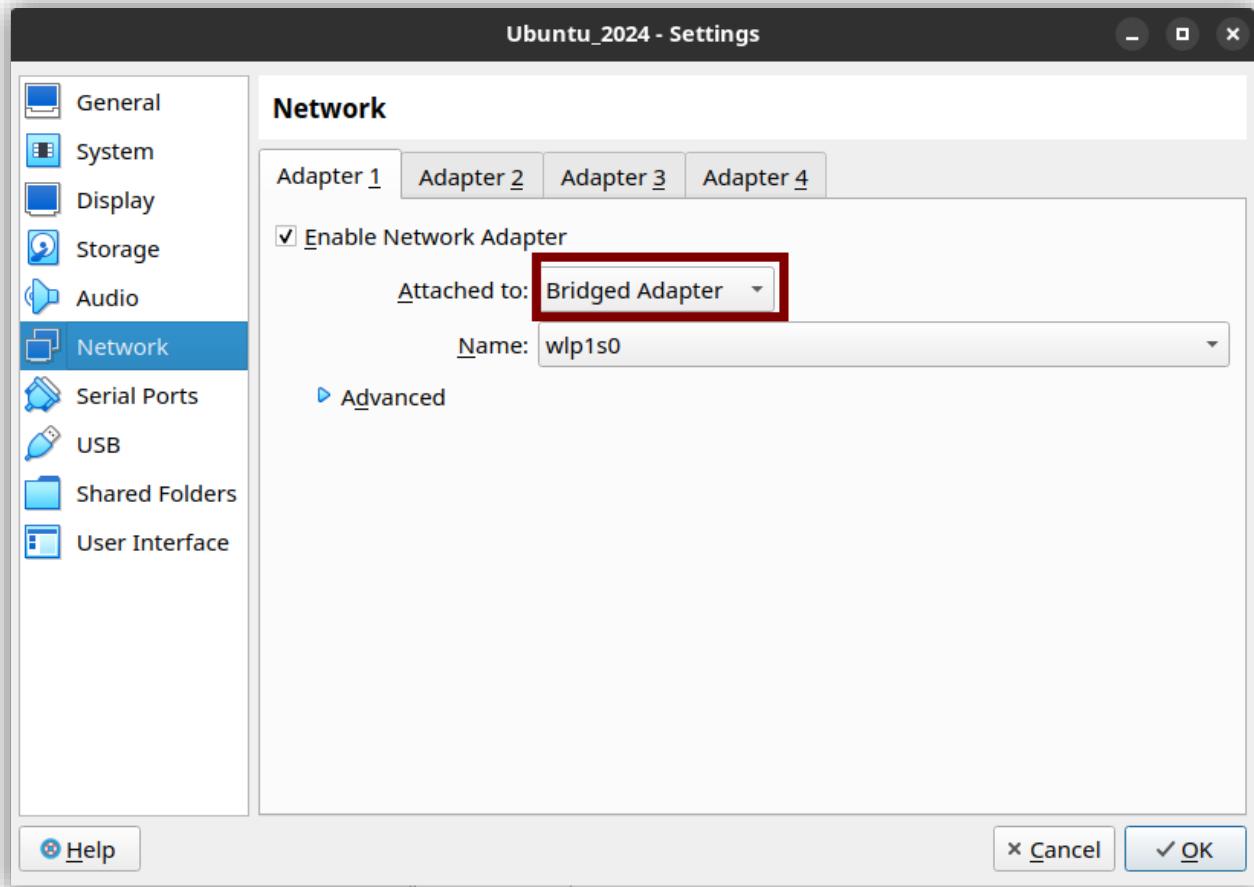
```
GNU nano 6.2 .zshrc
autoload -U colors && colors      # Load colors
PS1="%B${fg[red]}%[%{fg[green]}%]%n%{fg[red]}@%{fg[blue]}%)%M %{fg[magenta]}%~%{fg[white]}%#"
print-time() print -P '%F{yellow}%D{%FT%.2.%z}%f'
preexec_functions+=(print-time)
setopt autocd          # Automatically cd into typed directory.
stty stop undef        # Disable ctrl-s to freeze terminal.
setopt interactive_comments

#History in cache directory:
HISTSIZE=10000000
SAVEHIST=10000000
HISTFILE=~/.zsh_history
#To retrieve the history file everytime history is called upon.
setopt share_history

# Basic auto/tab complete:
autoload -U compinit
zstyle ':completion:*' menu select
zmodload zsh/complist
compinit
_comp_options+=(globdots)           # Include hidden files.
```

A2. Ρυθμίστε το δίκτυο στον εξυπηρετητή και παραμετροποιήστε αρχικά το ανάχωμα ασφαλείας ώστε να μην επιτρέπεται καμία εξωτερική σύνδεση στον εξυπηρετητή σας, εκτός από συνδέσεις SSH. Για το σκοπό αυτό μπορείτε να χρησιμοποιήσετε εργαλεία όπως iptables ή nftables.

Προαπαιτούμενο για τη ρύθμιση του SSH είναι η ρύθμιση της static ip μέσω του netplan configuration (**192.168.1.29**) εντός του Ubuntu και η επιλογή της ρύθμισης Bridged Adapter στο Virtual Box. Έπειτα γίνεται εγκατάσταση του πακέτου Open SSH Server και ενεργοποίηση της υπηρεσίας ssh.service μέσω του systemctl (ένα εργαλείο διαχείρισης του systemd, το οποίο είναι το προεπιλεγμένο σύστημα διαχείρισης διαδικασιών και υπηρεσιών σε πολλές διανομές Linux). Χρησιμοποιείται για την εκκίνηση, την παύση, την επανεκκίνηση και τον έλεγχο των διαφόρων υπηρεσιών του συστήματος, καθώς και για τη διαχείριση των διάφορων άλλων πτυχών του συστήματος, όπως οι ενότητες εκκίνησης (unit files), τα logs και άλλες διαμορφώσεις).



```
[terminator@skynet ~]$ cd /etc/netplan  
2024-03-16T16:42:08.50+0200  
[terminator@skynet /etc/netplan]$ sudo nano 00-installer-config.yaml
```



```
GNU nano 6.2                               00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.1.29/24]
      routes:
        - to: default
          via: 192.168.1.1
      nameservers:
        addresses: [1.0.0.1,1.1.1.1]
```

```
[terminator@skynet ~]$ sudo apt install openssh-server
2024-03-16T16:45:39.38+0200
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:8.9p1-3ubuntu0.6).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```



```
[terminator@skynet ~]$ sudo systemctl start ssh.service
2024-03-16T16:46:56.73+0200
[terminator@skynet ~]$ sudo systemctl enable ssh.service
2024-03-16T16:47:04.68+0200
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-
-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
[terminator@skynet ~]$ sudo systemctl status ssh.service
2024-03-16T16:47:12.01+0200
● ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
      Active: active (running) since Sat 2024-03-16 16:35:22 EET; 11min ago
        Docs: man:sshd(8)
               man:sshd_config(5)
        Main PID: 819 (sshd)
          Tasks: 1 (limit: 4181)
         Memory: 6.7M
            CPU: 104ms
           CGroup: /system.slice/ssh.service
                   └─819 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 16 16:35:21 skynet systemd[1]: Starting OpenBSD Secure Shell server...
Mar 16 16:35:22 skynet sshd[819]: Server listening on 0.0.0.0 port 22.
Mar 16 16:35:22 skynet sshd[819]: Server listening on :: port 22.
Mar 16 16:35:22 skynet systemd[1]: Started OpenBSD Secure Shell server.
Mar 16 16:36:11 skynet sshd[1118]: Accepted password for terminator from 192.168.1.14 por>
Mar 16 16:36:11 skynet sshd[1118]: pam_unix(sshd:session): session opened for user termin>
lines 1-18/18 (END)
```

```
[konstantman@arch ~]$ ssh -p 101 terminator@192.168.1.29
terminator@192.168.1.29's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-100-generic x86_64)
```

*Bonus: Όπως βλέπουμε στο screenshot φροντίσαμε να αλλάξουμε τη προεπιλεγμένη θύρα από 22 στο 101 (matrix reference) με σκοπό να αποτρέψουμε τυχόν επιθέσεις από bots που δρούν αυτοματοποιημένα στη προεπιλεγμένη θύρα.*

Αφού ενεργοποιήσαμε το SSH φροντίσαμε να ασφαλίσουμε το server με την εγκατάσταση ενός firewall. Εγκαταστήσαμε το πακέτο iptables και με τα flags -L και -v



είδαμε τους default κανόνες και πήραμε τα κατάλληλα μέτρα ώστε να τους αλλάξουμε. Χρησιμοποιώντας το ufw (Uncomplicated Firewall) που λειτουργεί στην ουσία ως “front end” τρέξαμε την εντολή **sudo ufw default deny incoming** που χρησιμοποιείται για την προσθήκη μιας προεπιλεγμένης απόρριψης για εισερχόμενη κίνηση στο ufw στο σύστημά μας . Αυτό σημαίνει ότι όλα τα εισερχόμενα πακέτα προς το σύστημά μας θα απορρίπτονται από προεπιλογή, ενισχύοντας την ασφάλεια του συστήματός μας, καθώς αποτρέπει την ανεπιθύμητη εισερχόμενη πρόσβαση στον υπολογιστή μας εκτός από το SSH το οποίο και θα ορίσουμε τώρα.

```
[terminator@skynet ~]$ sudo apt install iptables
2024-03-16T17:15:21.20+0200
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.7-1ubuntu5.2).
iptables set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
[terminator@skynet ~]$ sudo iptables -L -v
2024-03-16T17:58.64+0200
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source          destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source          destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out      source          destination
[terminator@skynet ~]$
```

```
[terminator@skynet ~]$ sudo ufw default deny incoming
2024-03-16T18:45:09.24+0200
```

```
[terminator@skynet ~]$ sudo ufw enable
2024-03-16T18:45:59.78+0200
```



Με την εντολή ***sudo iptables -A INPUT -p tcp --dport 101 -j ACCEPT*** προσθέτουμε έναν νέο κανόνα στο τείχος προστασίας iptables σε ένα σύστημα Linux για εισερχόμενα πακέτα:

```
[terminator@skynet ~]$ sudo iptables -A INPUT -p tcp --dport 101 -j ACCEPT
2024-03-16T18:49:17.47+0200
```

Αντίστοιχα για τα εξερχόμενα με την εντολή ***sudo iptables -A OUPUT -p tcp --dport 101 -j ACCEPT***:

```
[terminator@skynet ~]$
[terminator@skynet ~]$ sudo iptables -A OUPUT -p tcp --dport 101 -j ACCEPT
```

Και τέλος για τη δρομολόγηση των πακέτων μεταξύ διεπαφών ***sudo iptables -A FORWARD -p tcp --dport 101 -j ACCEPT***:

```
[terminator@skynet ~]$ sudo iptables -A FORWARD -p tcp --dport 101 -j ACCEPT
2024-03-16T18:49:00.12+0200
```

```
[terminator@skynet ~]$ sudo apt-get install iptables-persistent
2024-03-16T18:53:01.77+0200
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables-persistent is already the newest version (1.0.16).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```



Αναλυτικά τα μέρη της εντολής:

- **-A INPUT:** Ο πίνακας INPUT χρησιμοποιείται για τον έλεγχο της εισερχόμενης κίνησης προς το σύστημα.
- **-A OUTPUT:** Ο πίνακας OUTPUT χρησιμοποιείται για τον έλεγχο της εξερχόμενης κίνησης από το σύστημά μας.
- **-A FORWARD:** Ο πίνακας FORWARD χρησιμοποιείται όταν το σύστημά μας δρομολογεί πακέτα μεταξύ διεπαφών, όπως σε έναν δρομολογητή ή έναν server που λειτουργεί ως πύλη (gateway).
- **-p tcp:** Αυτό καθορίζει το πρωτόκολλο TCP για τον κανόνα.
- **--dport 101:** Αυτός είναι ο προορισμός πόρτας (destination port) προς την οποία επιτρέπεται η εισερχόμενη σύνδεση. Στη συγκεκριμένη περίπτωση, η πόρτα είναι η 101.
- **-j ACCEPT:** Αυτό καθορίζει την ενέργεια που θα πραγματοποιηθεί αν ένα πακέτο αντιστοιχεί στον κανόνα. Στην περίπτωση αυτή, το πακέτο θα γίνει δεκτό.

*Bonus Πρόταση: μπορούμε να διαμορφώσουμε τον τοίχο προστασίας (firewall) έτσι ώστε να αποδέχεται συνδέσεις SSH μόνο από συγκεκριμένες διευθύνσεις IP που θα είναι στην ουσία οι IPs των χρηστών που συνδέονται με τον server.*

A3. Προχωρήστε στην απεγκατάσταση όλων των υπηρεσιών, εφαρμογών και πρωτοκόλλων δικτύου (π.χ. IPv4, IPv6) που δεν είναι απαραίτητες στον εξυπηρετητή σας και έχουν εγκατασταθεί κατά τη αρχική εγκατάσταση του λειτουργικού συστήματος. Απενεργοποιήστε όσες υπηρεσίες δεν απαιτούνται για την λειτουργία του εξυπηρετητή αλλά δεν μπορούν να απεγκατασταθούν.



```
[terminator@skynet ~]$ sudo apt autoremove rsyslog
2024-04-06T18:24:20.23+0300
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
libbson-1.0-0 libdbi1 libesmtp6 libestr0 libfastjson4 libhiredis0.14 libivykis0
libmongoc-1.0-0 libmongocrypt0 libnet1 libprotobuf-c1 librabbitmq4 librdkafka1
libriemann-client0 libsensors-config libsensors5 libsnappy1v5 libsnmp-base libsnmp40
rsyslog
0 upgraded, 0 newly installed, 20 to remove and 0 not upgraded.
After this operation, 10.7 MB disk space will be freed.
Do you want to continue? [Y/n] y
```

### Vulnerability Details : CVE-2019-17042

An issue was discovered in Rsyslog v8.1908.0. contrib/prmcisconames/prmcisconames.c has a heap overflow in the parser for Cisco log messages. The parser tries to locate a log message delimiter (in this case, a space or a colon), but fails to account for strings that do not satisfy this constraint. If the string does not match, then the variable lenMsg will reach the value zero and will skip the sanity check that detects invalid log messages. The message will then be considered valid, and the parser will eat up the nonexistent colon delimiter. In doing so, it will decrement lenMsg, a signed integer, whose value was zero and now becomes minus one. The following step in the parser is to shift left the contents of the message. To do this, it will call memmove with the right pointers to the target and destination strings, but the lenMsg will now be interpreted as a huge value, causing a heap overflow.

Published 2019-10-07 16:15:12 Updated 2021-12-06 18:12:36 Source [MITRE](#)

[View at NVD](#), [CVE.org](#)

Vulnerability category: Input validation

#### Exploit prediction scoring system (EPSS) score for CVE-2019-17042

Probability of exploitation activity in the next 30 days: 0.67%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 78 % [EPSS Score History](#) [EPSS FAQ](#)

#### CVSS scores for CVE-2019-17042

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	6.4	NIST
9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	NIST

Με την εντολή **sudo apt remove rsyslog** αφαιρέσαμε το rsyslog επειδή στην έκδοση 20.04 η εντολή `syslog()` μπορεί να γεμίσει την μνήμη του rsyslog deamon και να προκαλέσει πρόβλημα στο file system όπως φαίνεται στο CVE (Common Vulnerabilities and Exposures).



```
[terminator@skynet ~]$ sudo apt remove telnet
2024-03-16T19:22:15.95+0200
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  telnet
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 158 kB disk space will be freed.
Do you want to continue? [Y/n] ■
```

Αφαίρεση telnet με την με την εντολή **sudo apt remove telnet** που είναι ένα πρωτόκολλο δικτύου που χρησιμοποιείται για την απομακρυσμένη πρόσβαση σε άλλους υπολογιστές, αλλά λόγω των σοβαρών προβλημάτων ασφαλείας που σχετίζονται με τη χρήση τουκαι την έλλειψη κρυπτογράφησης , συνήθως δεν συνιστάται η χρήση του.

```
[terminator@skynet ~]$ sudo apt remove snapd
2024-03-16T19:24:35.89+0200
Reading package lists... done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  squashfs-tools
Use 'sudo apt autoremove' to remove it.
The following packages will be REMOVED:
  snapd
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 102 MB disk space will be freed.
Do you want to continue? [Y/n] ■
```

Αφαίρεση του snap με την εντολή **sudo apt remove snapd** γιατί ως μη "native" package manager αυξάνει το attack surface ακόμα και αν ανήκει στην Canonical την εταιρεία δηλαδή πίσω από την Ubuntu διανομή .

```
[terminator@skynet ~]$ sudo modprobe -r ip6_tunnel
2024-03-16T19:35:54.07+0200
[sudo] password for terminator:
```



Εκτελούμε την εντολή **sudo modprobe -r ip6\_tunnel** για να αφαιρέσουμε το module πυρήνα με το ίδιο όνομα από το σύστημα Linux που στο Linux χρησιμοποιείται για τη δημιουργία, την παραμετροποίηση και τη διαχείριση των τούνελ IPv6 στο σύστημα που εφόσον χρησιμοποιούμε IPv4 κάτι τέτοιο περισσεύει και μπορεί να χρησιμοποιηθεί κακόβουλα.

```
[terminator@skynet ~]$ sudo systemctl stop plymouth
2024-03-16T19:40:48.99+0200
[terminator@skynet ~]$ sudo systemctl disableplymouth
2024-03-16T19:40:57.05+0200
Unknown command verb disableplymouth.
[terminator@skynet ~]$ sudo systemctl disable plymouth
2024-03-16T19:41:00.07+0200
Synchronizing state of plymouth.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable plymouth
[terminator@skynet ~]$ sudo systemctl status plymouth
2024-03-16T19:41:10.67+0200
● plymouth-quit.service - Terminate Plymouth Boot Screen
   Loaded: loaded (/lib/systemd/system/plymouth-quit.service; static)
   Active: inactive (dead) since Sat 2024-03-16 19:40:49 EET; 21s ago
     Main PID: 841 (code=exited, status=1/FAILURE)
        CPU: 2ms

Mar 16 19:31:04 skynet systemd[1]: Starting Terminate Plymouth Boot Screen...
Mar 16 19:31:04 skynet systemd[1]: Finished Terminate Plymouth Boot Screen.
Mar 16 19:40:49 skynet systemd[1]: plymouth-quit.service: Deactivated successfully.
Mar 16 19:40:49 skynet systemd[1]: Stopped Terminate Plymouth Boot Screen.
[terminator@skynet ~]$
```

Με την εντολή **sudo systemctl disable plymouth** απενεργοποιούμε την υπηρεσία που χρησιμοποιείται για το "splash screen" κατά την φόρτωση του λειτουργικού.



```
[terminator@skynet ~]$ sudo systemctl stop plymouth-log
2024-03-16T19:46:57.11+0200
[terminator@skynet ~]$ sudo systemctl disable plymouth-log
2024-03-16T19:47:04.01+0200
Synchronizing state of plymouth-log.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable plymouth-log
[terminator@skynet ~]$ sudo systemctl status plymouth-log
2024-03-16T19:47:11.18+0200
● plymouth-read-write.service - Tell Plymouth To Write Out Runtime Data
    Loaded: loaded (/lib/systemd/system/plymouth-read-write.service; static)
    Active: inactive (dead) since Sat 2024-03-16 19:46:57 EET; 14s ago
      Main PID: 673 (code=exited, status=1/FAILURE)
        CPU: 3ms

Mar 16 19:30:56 skynet systemd[1]: Starting Tell Plymouth To Write Out Runtime Data...
Mar 16 19:30:56 skynet systemd[1]: Finished Tell Plymouth To Write Out Runtime Data.
Mar 16 19:46:57 skynet systemd[1]: plymouth-read-write.service: Deactivated successfully.
Mar 16 19:46:57 skynet systemd[1]: Stopped Tell Plymouth To Write Out Runtime Data.
[terminator@skynet ~]$ █
```

Με την εντολή **service --status-all** βλέπουμε όλες τις υπηρεσίες που έχουμε στο σύστημα μας. Όσες έχουν [ - ] από δίπλα, είναι απεγκατεστημένες.



```
[terminator@skynet ~]$ service --status-all
2024-03-16T19:58:37.14+0200
[ + ] apparmor
[ + ] apport
[ - ] console-setup.sh
[ + ] cron
[ - ] cryptdisks
[ - ] cryptdisks-early
[ + ] dbus
[ - ] grub-common
[ - ] hwclock.sh
[ + ] irqbalance
[ - ] iscsid
[ - ] keyboard-setup.sh
[ + ] kmod
[ - ] lvm2
[ - ] lvm2-lvmpolld
[ + ] netfilter-persistent
[ - ] open-iscsi
[ - ] open-vm-tools
[ - ] openvswitch-switch
[ + ] plymouth
[ + ] plymouth-log
[ + ] procps
[ - ] rsync
[ - ] screen-cleanup
[ + ] ssh
[ + ] udev
[ + ] ufw
[ + ] unattended-upgrades
[ - ] uuidd
```

	masked	enabled
rescue.service	static	-
rsync.service	masked	enabled
rsyslog.service	enabled	enabled
screen-cleanup.service	masked	enabled
secureboot-db.service	enabled	enabled
serial-getty@.service	disabled	enabled
setvtrgb.service	enabled	enabled
snapd.aa-prompt-listener.service	masked	enabled
snapd.apparmor.service	masked	enabled
snapd.autoimport.service	masked	enabled
snapd.core-fixup.service	masked	enabled
snapd.recovery-chooser-trigger.service	masked	enabled
snapd.seeded.service	masked	enabled
snapd.service	masked	enabled
snapd.system-shutdown.service	masked	enabled



Και με την εντολή **systemctl list-unit-files --type=service** καταγράφουμε όλες τις υπηρεσίες που είναι ενεργοποιημένες και απενεργοποιημένες στο σύστημα μας.

UNIT FILE	STATE	VENDOR PRESET
apparmor.service	enabled	enabled
apport-autoreport.service	static	-
apport-forward@.service	static	-
apport.service	generated	-
apt-daily-upgrade.service	static	-
apt-daily.service	static	-
apt-news.service	static	-
autovt@.service	alias	-
blk-availability.service	enabled	enabled
bolt.service	static	-
cloud-config.service	enabled	enabled
cloud-final.service	enabled	enabled
cloud-init-hotplugd.service	static	-
cloud-init-local.service	enabled	enabled
cloud-init.service	enabled	enabled
console-getty.service	disabled	disabled
console-setup.service	enabled	enabled
container-getty@.service	static	-
cron.service	enabled	enabled
cryptdisks-early.service	masked	enabled
cryptdisks.service	masked	enabled

A4. Ενεργοποιήστε την αυτόματη εγκατάσταση ενημερώσεων για την διόρθωση κενών ασφαλείας του συστήματος. Αυτό γίνεται με εργαλεία όπως "unattended-upgrades" στο Ubuntu/Debian και "dnf-automatic" στις διανομές Fedora και Red Hat Enterprise Linux (RHEL).

Επαληθεύστε την ακεραιότητα και την αυθεντικότητα των πακέτων λογισμικού που εγκαθιστάτε στο σύστημα σας ενεργοποιώντας GPG (GNU Privacy Guard) ελέγχους στους διαχειριστές πακέτων λογισμικού όπως είναι ο apt, yum, dnf κλπ.



Έπειτα προχωρήσαμε στην αυτόματη εγκατάσταση ενημερώσεων με την εγκατάσταση του πακέτου **sudo apt install unattended-upgrades** και το αντίστοιχο configuratiopn , για τη διόρθωση κενών ασφαλείας οι ενημερώσεις λογισμικού αποτελούν κρίσιμο μέρος της διαδικασίας διατήρησης ασφαλείας του συστήματος. Καθώς αναπτύσσονται συχνά για να διορθώσουν ευπάθειες και κενά ασφαλείας που μπορεί να εκτίθενται σε κακόβουλες επιθέσεις.

Η αυτόματη εγκατάσταση ενημερώσεων ασφαλείας επιτρέπει στο σύστημά μας να εγκαθιστά αυτόματα αυτές τις ενημερώσεις χωρίς την παρέμβαση του χρήστη. Αυτό εξασφαλίζει ότι το σύστημά μας παραμένει ενημερωμένο και προστατευμένο από γνωστά κενά ασφαλείας.

```
[terminator@skynet ~]$ sudo apt install unattended-upgrades
2024-03-16T20:01:00.55+0200
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unattended-upgrades is already the newest version (2.8ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
GNU nano 6.2          /etc/apt/apt.conf.d/50unattended-upgrades
// Automatically upgrade packages from these (origin:archive) pairs
//
// Note that in Ubuntu security updates may pull in new dependencies
// from non-security sources (e.g. chromium). By allowing the release
// pocket, these get automatically pulled in
Unattended-Upgrade::Allowed-Origins {
    "${distro_id}:${distro_codename}";
    "${distro_id}:${distro_codename}-security";
```



```
GNU nano 6.2          /etc/apt/apt.conf.d/20auto-upgrades
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
```

Εδώ τροποποιήσαμε κατάλληλα το config file ώστε να φροντίσουμε να γίνονται ενημερώσεις σε ένα συγκεκριμένο χρονικό διάστημα.

```
[terminator@skynet ~]$ sudo systemctl restart unattended-upgrades.service
2024-03-16T20:12:21.92+0200
[terminator@skynet ~]$
```

```
Packages blacklist due to conffile prompts: []
No packages found that can be upgraded unattended and no pending auto-removals
Package libdw1 has a higher version available, checking if it is from an allowed origin and is not pinned down.
Package libelf1 has a higher version available, checking if it is from an allowed origin and is not pinned down.
Extracting content from /var/log/unattended-upgrades/unattended-upgrades-dpkg.log since 2024-03-16 20:14:17
```

```
[terminator@skynet ~]$ sudo unattended-upgrades
2024-03-16T20:14:46.31+0200
[terminator@skynet ~]$
```



```
[terminator@skynet ~]$ sudo apt install debian-archive-keyring
2024-04-05T18:43:18.82+0300
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
debian-archive-keyring is already the newest version (2021.1.1ubuntu2).
The following packages were automatically installed and are no longer required:
  libestr0 libfastjson4
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
[terminator@skynet ~]$ apt-key list
2024-04-05T18:43:22.54+0300
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
/etc/apt/trusted.gpg
-----
pub    rsa4096 2012-05-11 [SC]
      790B C727 7767 219C 42C8  6F93 3B4F E6AC C0B2 1F32
uid            [ unknown] Ubuntu Archive Automatic Signing Key (2012) <ftpmaster@ubuntu.com>
/etc/apt/trusted.gpg.d/ubuntu-keyring-2012-cdimage.gpg
-----
pub    rsa4096 2012-05-11 [SC]
      8439 38DF 228D 22F7 B374  2BC0 D94A A3F0 EFE2 1092
uid            [ unknown] Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>
/etc/apt/trusted.gpg.d/ubuntu-keyring-2018-archive.gpg
-----
pub    rsa4096 2018-09-17 [SC]
      F6EC B376 2474 EDA9 D21B  7022 8719 20D1 991B C93C
uid            [ unknown] Ubuntu Archive Automatic Signing Key (2018) <ftpmaster@ubuntu.com>
```

Κατά την εγκατάσταση λογισμικού, είναι σημαντικό να επιβεβαίσουμε ότι τα πακέτα που εγκαθίστανται είναι ακέραια και αυθεντικά. Οι διαχειριστές πακέτων λογισμικού χρησιμοποιούν συνήθως το GPG (GNU Privacy Guard) για την υπογραφή των πακέτων τους, επιτρέποντας στο σύστημα να επαληθεύει την αυθεντικότητα και την ακεραιότητά τους. Το οποίο και κάναμε με την εγκατάσταση και ενεργοποίηση του πακέτου **sudo apt install debian-archive-keyring**.



## B. Διαμόρφωση και Διαχείριση Χρηστών Συστήματος

B1. Καταργήστε/απενεργοποιήστε τους περιττούς λογαριασμούς χρηστών. Η προεπιλεγμένη διαμόρφωση του λειτουργικού συστήματος συχνά περιλαμβάνει λογαριασμούς επισκεπτών ή και λογαριασμούς χρηστών που σχετίζονται με τοπικές υπηρεσίες και υπηρεσίες δικτύου. Συνήθως τα ονόματα και οι κωδικοί πρόσβασης για αυτούς τους λογαριασμούς είναι γνωστά. Καταργήστε (εάν είναι δυνατό) ή απενεργοποιήστε τους περιττούς λογαριασμούς για να εξαλείψετε τη χρήση τους από κακόβουλους χρήστες.

Καταργήσαμε κάποιους περιττούς λογαριασμούς και τα “home directories” που μπορούν να λειτουργήσουν ως απειλή για το σύστημα μας αν αξιοποιηθούν κατάλληλα από κάποιο κακόβουλο χρήστη με σκοπό το “privilege escalation”.

```
[terminator@skynet ~]$ sudo userdel games
2024-03-22T18:52:47.34+0200
[sudo] password for terminator:
[terminator@skynet ~]$ sudo rm -r /home/games
2024-03-22T18:53:12.47+0200
rm: cannot remove '/home/games': No such file or directory
```

```
[terminator@skynet ~]$ sudo userdel mail
2024-03-22T18:58:42.92+0200
[terminator@skynet ~]$ sudo rm -r /home/mail
2024-03-22T18:58:50.28+0200
rm: cannot remove '/home/mail': No such file or directory
[terminator@skynet ~]$
```



```
[terminator@skynet ~]$ sudo userdel news  
2024-03-22T19:00:01.59+0200  
[terminator@skynet ~]$ sudo rm -r /home/news  
2024-03-22T19:00:07.67+0200  
rm: cannot remove '/home/news': No such file or directory  
[terminator@skynet ~]$
```

B2. Δημιουργήστε ενδεικτικούς χρήστες στο σύστημα σας και κατάλληλες ομάδες χρηστών. Στα πλαίσια της εργασίας δημιουργήστε έναν διαχειριστή του συστήματος (διαφορετικό λογαριασμό από το root), και κάποιους πρόσθετους απλούς χρήστες. Δημιουργήστε προσωπικό χώρο (home directory) για κάθε χρήστη. Διαμορφώστε το σύστημα διαχείρισης αρχείων έτσι ώστε κάθε χώρος να δημιουργείται στην κατάλληλη θέση του δίσκου ανάλογα με τον ρόλο του χρήστη, δηλαδή σε διαφορετική διαδρομή φακέλων θα πρέπει να βρίσκεται ο προσωπικός χώρος των απλών χρηστών από των διαχειριστών. Αντιστοιχίστε τους χρήστες σε κατάλληλες ομάδες. Δώστε στους χρήστες τα απαραίτητα δικαιώματα (στους φακέλους και υπηρεσίες) ανάλογα με τους ρόλους τους.

Έπειτα προχωρήσαμε στη δημιουργία των κατάλληλων groups για τους αντίστοιχους χρήστες (user,admin).



```
[terminator@skynet ~]$ sudo groupadd admins
```

2024-03-22T19:21:36.68+0200

```
[terminator@skynet ~]$ sudo groupadd users
```

2024-03-22T19:21:42.16+0200

```
[terminator@skynet ~]$ sudo useradd -m -d /home/user1 -s /bin/bash -G users user1
2024-03-22T19:26:54.00+0200
[terminator@skynet ~]$ sudo useradd -m -d /home/user2 -s /bin/bash -G users user2
2024-03-22T19:26:59.97+0200
[terminator@skynet ~]$ 
```

Μετά δημιουργήσαμε τους λογαριασμούς και τα αντίστοιχα home directories φροντίζοντας ο καθένας να έχει πρόσβαση μόνο στα απαραίτητα αρχεία με βάση την αρχή του ελάχιστου προνομίου.

```
[terminator@skynet ~]$ id admin
2024-04-06T19:23:25.76+0300
uid=1003(admin) gid=1004(admin) groups=1004(admin),4(adm),24(cdrom),25(sudo),30(dip),46(pl
ugdev),110(lxd),1001(admins)
[terminator@skynet ~]$ id user1
2024-04-06T19:23:31.10+0300
uid=1001(user1) gid=1002(user1) groups=1002(user1),100(users)
[terminator@skynet ~]$ id user2
2024-04-06T19:23:35.20+0300
uid=1002(user2) gid=1003(user2) groups=1003(user2),100(users)
[terminator@skynet ~]$ 
```



```
[terminator@skynet /home]$ ls  
2024-03-22T19:28:34.31+0200  
terminator user1 user2
```

```
user1@skynet:~$ ls -la  
total 24  
drwxr-x--- 2 user1 user1 4096 Mar 22 19:36 .  
drwxr-xr-x 5 root root 4096 Mar 22 19:26 ..  
-rw----- 1 user1 user1 45 Mar 22 19:36 .bash_history  
-rw-r--r-- 1 user1 user1 220 Jan 6 2022 .bash_logout  
-rw-r--r-- 1 user1 user1 3771 Jan 6 2022 .bashrc  
-rw-r--r-- 1 user1 user1 807 Jan 6 2022 .profile  
user1@skynet:~$ sudo apt update  
[sudo] password for user1:  
user1 is not in the sudoers file. This incident will be reported.  
user1@skynet:~$
```

```
user2@skynet:~$ ls -la  
total 24  
drwxr-x--- 2 user2 user2 4096 Mar 22 19:26 .  
drwxr-xr-x 5 root root 4096 Mar 22 19:26 ..  
-rw-r--r-- 1 user2 user2 220 Jan 6 2022 .bash_logout  
-rw-r--r-- 1 user2 user2 3771 Jan 6 2022 .bashrc  
-rw-r--r-- 1 user2 user2 807 Jan 6 2022 .profile  
user2@skynet:~$ sudo apt update  
[sudo] password for user2:  
user2 is not in the sudoers file. This incident will be reported.  
user2@skynet:~$
```

Και όπως παρατηρούμε οι χρήστες user1, user2 δεν μπορούν να περιηγηθούν πέραν του δικού τους home directory και να χρησιμοποιήσουν την εντολή sudo για escalated privileges.



```
user1@skynet:~$ ls -la
total 20
drwxr-x--- 3 user1 user1 4096 Apr  5 18:19 .
drwxr-xr-x  6 root  root  4096 Mar 22 21:24 ..
-rw------- 1 user1 user1   73 Mar 22 19:39 .bash_history
-rw-r--r--  1 user1 user1  220 Jan  6  2022 .bash_logout
-rw-r--r--  1 user1 user1 3771 Jan  6  2022 .bashrc
drwx----- 2 user1 user1 4096 Apr  5 18:19 .cache
-rw-r--r--  1 user1 user1  807 Jan  6  2022 .profile
user1@skynet:~$ cd
user1@skynet:/home$ ls
admin terminator user1 user2
user1@skynet:/home$ cd admin
-bash: cd: admin: Permission denied
user1@skynet:/home$ cd user2
-bash: cd: user2: Permission denied
user1@skynet:/home$ cd user1
user1@skynet:~$ _
```

B3. Απενεργοποιήστε τη σύνδεση ως root χρήστης στο σύστημα (ακόμα και με ssh σύνδεση). Για την εκτέλεση εντολών ως root μπορεί να χρησιμοποιηθεί η εντολή sudo η οποία επιτρέπει τον καλύτερο έλεγχο των δικαιωμάτων.

Χρησιμοποιήσαμε την εντολή **sudo passwd -l root** για να κλειδώσουμε τον λογαριασμό του root στο σύστημα μας (το flag **-l** στην εντολή **passwd** σημαίνει "lock").

Όταν ο λογαριασμός root είναι κλειδωμένος, δεν είναι δυνατή η σύνδεση ή η είσοδος στο σύστημα ως χρήστης root, ούτε μέσω του τερματικού ή άλλων μεθόδων. Αυτό αποτελεί έναν επιπρόσθετο μηχανισμό προστασίας, καθώς αποτρέπει την ανεπιθύμητη χρήση του λογαριασμού root.



```
[terminator@skynet ~]$ sudo passwd -l root
```

```
2024-03-22T20:01:36.23+0200
passwd: password expiry information changed.
[terminator@skynet ~]$ su - root
2024-03-22T20:01:42.05+0200
Password:
su: Authentication failure
```

Τέλος φροντίσαμε να κλειδώσουμε τη σύνδεση με root ακόμα και μέσω ssh.

```
[terminator@skynet ~]$ sudo nano /etc/ssh/sshd_config
2024-03-22T20:14:19.44+0200
```

```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```



**B4.** Επιβάλλετε ισχυρές πολιτικές κωδικών πρόσβασης χρησιμοποιώντας τη διαμόρφωση PAM (Pluggable Authentication Modules) (/etc/pam.d/common-password). Εφαρμόστε πολιτικές πολυπλοκότητας και εναλλαγής κωδικού πρόσβασης.

Σε αυτό το παράδειγμα, η πολιτική πολυπλοκότητας κωδικού πρόσβασης εφαρμόζεται με τα ακόλουθα χαρακτηριστικά:

**obscure:** Ορίζει ότι οι κωδικοί πρόσβασης πρέπει να είναι δυσδιάκριτοι.

**yescrypt:** Άλγοριθμος κρυπτογράφησης και hash που έχει σχεδιαστεί για να παρέχει ασφαλή αποθήκευση κωδικών και ελέγχους ταυτότητας.

**sha512:** Χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης SHA-512 για την αποθήκευση των κωδικών πρόσβασης.

**minlen=8:** Ορίζει ότι οι κωδικοί πρόσβασης πρέπει να έχουν τουλάχιστον 8 χαρακτήρες.

**remember=5:** Ορίζει ότι οι προηγούμενοι 5 κωδικοί πρόσβασης θα αποθηκευτούν για αντιστροφή ελέγχου.

```
[terminator@skynet ~]$ sudo nano /etc/pam.d/common-password
```

```
2024-03-22T21:11:17.28+0200
```

```
[terminator@skynet ~]$
```

```
# here are the per-package modules (the "Primary" block)
password      [success=1 default=ignore]      pam_unix.so obscure yescrypt sha512 minlen=8 remember=5
# here's the fallback if no module succeeds
password      requisite                  pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password      required                  pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
```



B5. Ρυθμίστε το επιτρεπτό όριο αποθηκευτικού χώρου για κάθε χρήστη (disk quotas) και ότι άλλους περιορισμούς προτείνετε (χρήση επεξεργαστή, μνήμης κλπ.). Πιο συγκεκριμένα, οι απλοί χρήστες θα πρέπει να έχουν αποθηκευτικό χώρο μέχρι 500 MB και απεριόριστη χρήση οι διαχειριστές του συστήματος.

Για αυτό το ερώτημα αρχικά εγκαταστήσαμε το quota (σύστημα περιορισμού αποθηκευτικού χώρου σε έναν υπολογιστή ή σε ένα δίκτυο) και έπειτα με την κατάλληλη τροποποίηση του fstab (file systems table: αρχείο με πληροφορίες σχετικά με τα πώς οργανώνονται και προσαρμόζονται τα διάφορα συστήματα αρχείων στο σύστημα) και τις εντολές **sudo quota -vs user1 && sudo quota -vs user2 && sudo quota -vs admin** φροντίσαμε να δώσουμε στους χρήστες 500MB αποθηκευτικού χώρου και στον admin απεριόριστο (δώσαμε το μέγιστο δυνατό όριο).

```
[terminator@skynet ~]$ sudo apt install quota
2024-03-22T21:44:51.36+0200
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
quota is already the newest version (4.06-1build2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
[terminator@skynet ~]$
```

```
GNU nano 6.2
/etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/ubuntu-vg/ubuntu-vg during curtin installation
/dev/disk/by-1d/dm-uuid-LVM-hBZCHkIIIZfwGmj3XJfuKsmzUjQR3SQ4wUzmm2seg9kPhkwSP5P3D8stDptG8zC / ext4 defaults,usrquota 0 1
```



```
[terminator@skynet ~]$ sudo quota -vs user1
2024-03-22T21:47:18.39+0200
Disk quotas for user user1 (uid 1001):
  Filesystem   space  quota  limit  grace  files  quota  limit  grace
/dev/mapper/ubuntu--vg-ubuntu--lv
          20K    500M   500M           5      0      0
[terminator@skynet ~]$ █ █
```

```
[terminator@skynet ~]$ sudo quota -vs user2
2024-03-22T21:48:56.70+0200
Disk quotas for user user2 (uid 1002):
  Filesystem   space  quota  limit  grace  files  quota  limit  grace
/dev/mapper/ubuntu--vg-ubuntu--lv
          20K    500M   500M           5      0      0
[terminator@skynet ~]$ █ █
```

```
[terminator@skynet ~]$ sudo quota -vs admin
2024-03-22T21:56:42.45+0200
Disk quotas for user admin (uid 1003):
  Filesystem   space  quota  limit  grace  files  quota  limit  grace
/dev/mapper/ubuntu--vg-ubuntu--lv
          16K   23552M  23552M           4      0      0
[terminator@skynet ~]$ █ █
```

B6. Ενεργοποίηση ελέγχου ταυτότητας που βασίζεται σε κλειδί για το πρωτόκολλο SSH (SSH key-based authentication). Χρησιμοποιήστε την ssh-keygen για τη δημιουργία κλειδιών και την ssh-copy-id για την εγκατάσταση των κλειδιών στον εξυπηρετητή. Απενεργοποιήστε την αυθεντικοποίηση των χρηστών με χρήση συνθηματικών (σχετική παραμετροποίηση του αρχείου /etc/ssh/sshd\_config).

Για την ενεργοποίηση ελέγχου ταυτότητας SSH με SSH key-based authentication. Φροντίσαμε να δημιουργήσουμε ένα ζευγάρι private key-public key όπου το δημόσιο κλειδί το στείλαμε στο “host machine” με τη χρήση του ssh-copy-id και τέλος κλειδώσαμε τη σύνδεση με password.



```
[terminator@skynet ~]$ ssh-keygen
2024-03-22T22:09:06.26+0200
Generating public/private rsa key pair.
Enter file in which to save the key (/home/terminator/.ssh/id_rsa):
```

```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes
PasswordAuthentication no
```



B7. Διαμορφώστε τον εξυπηρετητή ώστε να αποτρέπεται τους κακόβουλους χρήστες που δεν έχουν νόμιμα λογαριασμό σύνδεσης στο σύστημα, να δοκιμάζουν επαναληπτικά συνθηματικά χρηστών.

Όπως βλέπουμε ορίσαμε τις μέγιστες προσπάθειες που μπορεί να κάνει ένας χρήστης έως 3 και κλέισαμε τη πρόσβαση στο root μεσω του sudoers file.

```
GNU nano 6.2                               /etc/sudoers.tmp *
```

```
# Ditto for GPG agent
Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
#root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

## Allow a user to attempt to enter a password 3 times
Defaults        passwd_tries=3
# See sudoers(5) for more information on "@include" directives:

@includefile /etc/sudoers.d
```



```
2024-04-05T19:13:20.97+0300
[sudo] password for terminator:
Sorry, try again.
[sudo] password for terminator:
Sorry, try again.
[sudo] password for terminator:
sudo: 3 incorrect password attempts
```

```
*****  
WARNING: This is a private system. Unauthorized access is prohibited.  
*****  
Ubuntu 22.04.4 LTS skynet tty4  
skynet login: admin ←  
Password:  
Login incorrect ←  
skynet login: admin ←  
Password:  
Login incorrect ←  
skynet login: admin ←
```

B8. Ελέγξτε τακτικά τους λογαριασμούς χρηστών και τα δικαιώματα τους με εντολές του συστήματος όπως "getent passwd" και "getent group", διασφαλίζοντας ότι δεν υπάρχουν μη εξουσιοδοτημένοι λογαριασμοί.

Συγκεκριμένα η εντολή "getent passwd" χρησιμοποιείται για να εμφανίσει όλους τους λογαριασμούς χρηστών στο σύστημά σας. Κάθε χρήστης έχει έναν αντίστοιχο εγγραφόμενο λογαριασμό στο αρχείο **/etc/passwd** και κάθε γραμμή σε αυτό το αρχείο περιέχει πληροφορίες για ένα χρήστη, όπως το όνομα χρήστη, τον αριθμό του UID (User ID), τον αριθμό του GID (Group ID), το ονομαστικό πλήρες όνομα του χρήστη, τον κατάλογο του χρήστη και το κέλυφος (shell) που χρησιμοποιεί ο χρήστης όταν συνδέεται στο σύστημα.



Συμπληρωματικά η εντολή "getent group" εμφανίζει όλες τις ομάδες χρηστών στο σύστημά μας. Κάθε ομάδα έχει μια εγγραφή στο αρχείο **/etc/group**. Κάθε γραμμή σε αυτό το αρχείο περιέχει πληροφορίες για μια ομάδα, όπως το όνομα της ομάδας, τον αριθμό του GID (Group ID) και τα ονόματα των μελών της ομάδας.

Χρησιμοποιώντας αυτές τις εντολές για να ελέγξουμε τους λογαριασμούς χρηστών και τα δικαιώματα τους, θα μπορέσουμε να επιβεβαιώσουμε ότι δεν υπάρχουν μη εξουσιοδοτημένοι λογαριασμοί στο σύστημά σας και ότι οι ομάδες και οι χρήστες έχουν τα σωστά δικαιώματα πρόσβασης στους αντίστοιχους καταλόγους και αρχεία.

## Γ. Καταγραφή και Παρακολούθηση Συστήματος

Γ1. Ρυθμίστε ποιες πληροφορίες θα καταγράφονται στα αρχεία καταγραφής του συστήματος και πόσο συχνά θα επανεγγράφονται τα αρχεία αυτά (log rotation). Για τον λόγο αυτό, παραμετροποιήστε και χρησιμοποιήστε εργαλεία όπως είναι το rsyslog και το syslog-ng.

Όπως παρατηρούμε στα screenshots με την εντολή sudo nano /etc/syslog-ng/syslog-ng.conf αρχικά επιλέξαμε από ποιά “events”, χρήστες και λειτουργικά μέρη του συστήματος θέλουμε να κρατάμε logs.

*Bonus: Αποφασίσαμε πως θα ήταν μία καλή πρακτική ασφαλείας να ρυθμίσουμε το config file με τέτοιο τρόπο ώστε να στέλνει τα logs στον “host machine” με σκοπό να ελέγχονται ανά τακτά χρονικά διαστήματα από το προσωπικό.*



```
#####
# Destinations
#####
# First some standard logfile
#
destination d_auth { file("/var/log/auth.log"); };
destination d_cron { file("/var/log/cron.log"); };
destination d_daemon { file("/var/log/daemon.log"); };
destination d_kern { file("/var/log/kern.log"); };
destination d_lpr { file("/var/log/lpr.log"); };
destination d_mail { file("/var/log/mail.log"); };
destination d_syslog { file("/var/log/syslog"); };
destination d_user { file("/var/log/user.log"); };
destination d_uucp { file("/var/log/uucp.log"); };
```

```
# Send the messages to an other host
#
destination d_net { tcp("192.168.1.14" port(1000) log_fifo_size(1000)); };
```

```
[terminator@skynet ~]: sudo nano /etc/syslog-ng/syslog-ng.conf
2024-03-23T17:47:23.73+0200
[terminator@skynet ~]: sudo systemctl restart syslog-ng
2024-03-23T17:52:18.05+0200
[terminator@skynet ~]: sudo systemctl status syslog-ng
2024-03-23T17:52:30.31+0200
● syslog-ng.service - System Logger Daemon
    Loaded: loaded (/lib/systemd/system/syslog-ng.service; enabled; vendor preset: enabled)
    Active: active (running) since Sat 2024-03-23 17:52:18 EET; 12s ago
      Docs: man:syslog-ng(8)
      Main PID: 2290 (syslog-ng)
         Tasks: 2 (limit: 4181)
        Memory: 4.4M
           CPU: 53ms
          CGroup: /system.slice/syslog-ng.service
                  └─2290 /usr/sbin/syslog-ng -F
```

Τέλος επιλέξαμε πως θα κρατιούνται τα logs και θα ενημερώνονται ανάλογα με τις ακόλουθες ρυθμίσεις.



```
GNU nano 6.2                               /etc/logrotate.d/syslog-ng
/var/log/syslog
{
    rotate 7
    daily
    missingok
    notifempty
    delaycompress
    compress
    postrotate
        invoke-rc.d syslog-ng reload > /dev/null
    endscript
}
```

**rotate 7:** Αυτή η οδηγία καθορίζει τον αριθμό των περιστρεφόμενων αρχείων καταγραφής που θα διατηρούνται. Σε αυτή την περίπτωση, ορίζεται σε 7, πράγμα που σημαίνει ότι το logrotate θα κρατά το τρέχον αρχείο καταγραφής και 6 περιστρεφόμενα αρχεία καταγραφής. Όταν δημιουργείται ένα νέο αρχείο καταγραφής, το παλαιότερο αρχείο διαγράφεται.

**daily:** Αυτή η οδηγία ρυθμίζει το logrotate να "περιστρέψει" τα αρχεία καταγραφής καθημερινά. Ότι θα δημιουργηθεί δηλαδή ένα νέο αρχείο καταγραφής κάθε μέρα, ανεξάρτητα από το μέγεθός του.

**missingok:** Αυτή η οδηγία λέει στο logrotate να μη δημιουργεί σφάλμα αν το αρχείο καταγραφής λείπει. Είναι χρήσιμο σε περιπτώσεις που το αρχείο καταγραφής είναι προαιρετικό ή μπορεί να μην υπάρχει κατά τη στιγμή της περιστροφής.

**notifempty:** Με αυτή την οδηγία, το logrotate δε θα "περιστρέψει" το αρχείο καταγραφής αν είναι κενό.

**delaycompress:** Αυτή η οδηγία καθυστερεί τη συμπίεση των περιστρεφόμενων αρχείων καταγραφής μέχρι την επόμενη περιστροφή.

**compress:** Αυτή η οδηγία ενεργοποιεί τη συμπίεση των αρχείων καταγραφής. Τα συμπιεσμένα αρχεία καταγραφής συνήθως έχουν την κατάληξη **.gz**.



**postrotate ... endscript:** Αυτά περικλείουν τις εντολές που εκτελούνται μετά την περιστροφή των αρχείων καταγραφής. Σε αυτή την περίπτωση, το **/usr/lib/rsyslog/rsyslog-rotate** εκτελείται μετά την περιστροφή. Αυτό μπορεί να χρησιμοποιηθεί για εργασίες όπως το refresh ή το restart της υπηρεσίας καταγραφής για να διασφαλίσει ότι ξεκινά να γράφει στο νέο αρχείο καταγραφής.

**Γ2. Χρησιμοποιήστε την εντολή auditd για λεπτομερή καταγραφή συμβάντων του συστήματος καθώς και ενεργειών των χρηστών. Ορίστε τους κατάλληλους κανόνες στο αρχείο "/etc/audit/audit.rules".**

Χρησιμοποιώντας το πρόγραμμα audit ένα εργαλείο διαχείρισης συμβάντων που μας παρέχει τη δυνατότητα να καταγράψουμε λεπτομερώς διάφορα γεγονότα που συμβαίνουν στο σύστημα, όπως αλλαγές σε αρχεία και καταλόγους, προσπάθειες σύνδεσης χρηστών, ενέργειες διαχείρισης προνομίων και άλλα.

Και όπως φαίνεται και στο screenshot εμείς ορίσαμε πως θέλουμε να ελέγχει τα εξής :

- Τις ενέργειες του χρήστη
- Άλλαγές στο file system
- Ενέργειες του admin
- Άλλαγές στα network/system configurations

```
GNU nano 6.2          /etc/audit/audit.rules *
##Monitor all user actions (execve, fork, etc.)
-a always,exit -F arch=b64 -S execve -F key=user-actions ←

##Monitor file system events (read, write, create, delete, etc.)
-w /etc/passwd -p wa -k etc-passwd-changes ←
-w /etc/shadow -p wa -k etc-shadow-changes ←

##Monitor system administrator actions using sudo
-w /var/log/sudo.log -k sudo-activity ←

##Monitor changes to network configuration files
-w /etc/network/ -p wa -k network-config-changes ←

##Monitor changes to system configuration files
-w /etc/sysconfig/ -p wa -k sysconfig-changes ←
```



```
[terminator@skynet ~]$ sudo systemctl status auditd
2024-03-23T18:06:28.57+0200
● auditd.service - Security Auditing Service
  Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
  Active: active (running) since Sat 2024-03-23 18:06:14 EET; 13s ago
    Docs: man:auditd(8)
          https://github.com/linux-audit/audit-documentation
  Process: 2669 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
  Process: 2673 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
 Main PID: 2670 (auditd)
   Tasks: 2 (limit: 4181)
  Memory: 472.0K
     CPU: 65ms
    CGroup: /system.slice/auditd.service
              └─2670 /sbin/auditd

Mar 23 18:06:14 skynet augenrules[2686]: enabled 1
Mar 23 18:06:14 skynet augenrules[2686]: failure 1
Mar 23 18:06:14 skynet augenrules[2686]: pid 2670
Mar 23 18:06:14 skynet augenrules[2686]: rate_limit 0
Mar 23 18:06:14 skynet augenrules[2686]: backlog_limit 8192
Mar 23 18:06:14 skynet augenrules[2686]: lost 0
Mar 23 18:06:14 skynet augenrules[2686]: backlog 3
Mar 23 18:06:14 skynet augenrules[2686]: backlog_wait_time 60000
Mar 23 18:06:14 skynet augenrules[2686]: backlog_wait_time_actual 0
Mar 23 18:06:14 skynet systemd[1]: Started Security Auditing Service.
[terminator@skynet ~]$
```

Η καταγραφή αυτή επιτρέπει στους διαχειριστές να ελέγχουν και να αναλύουν τις διάφορες ενέργειες που λαμβάνονται στο σύστημα, προστατεύοντας το κατα αυτό το τρόπο από επιθέσεις, παράνομες ενέργειες ή ακόμη και απλές ανεπιθύμητες ενέργειες. Επιπρόσθετα η καταγραφή των διαφόρων “events” αποτελεί σημαντικό εργαλείο για την αποτελεσματική διερεύνηση και αντίδραση σε πιθανές παραβιάσεις ασφαλείας.



Γ3. Εγκαταστήστε και παραμετροποιήστε το εργαλείο Fail2Ban. Το Fail2Ban είναι ένα λογισμικό πρόληψης και αποτροπής εισβολής, υλοποιημένο σε python. Παρακολουθεί τα αρχεία καταγραφής και αποκλείει τις διευθύνσεις IP που εμφανίζουν σημάδια κακόβουλης δραστηριότητας.

Το Fail2Ban είναι ένα πολύ χρήσιμο εργαλείο για την προστασία ενός συστήματος από επιθέσεις brute-force και άλλες μορφές κακόβουλης δραστηριότητας. Αφού το εγκαταστήσαμε δημιουργήσαμε ένα copy του σε ένα αρχείο με την επέκταση .local και πραγματοποιήσαμε τις αλλαγές σε αυτό.

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 600
```

**enabled = true:** Ενεργοποιεί το Fail2Ban για αυτή την υπηρεσία.

**port = ssh:** Προσδιορισμός της πόρτας που παρακολουθείται.

**filter = sshd:** Κανόνας φιλτράρισματος που χρησιμοποιείται για τον έλεγχο των καταγραφών.

**logpath = /var/log/auth.log:** Η διαδρομή του αρχείου καταγραφής που παρακολουθείται.



**maxretry = 3:** Το μέγιστο αριθμό αποτυχημένων προσπαθειών πριν μπει στη λίστα αποκλεισμού.

**bantime = 600:** Ο χρόνος σε δευτερόλεπτα για τον οποίο ένας διευθυντής IP θα παραμείνει στη λίστα αποκλεισμού (εδώ, 600 δευτερόλεπτα = 10 λεπτά).

```
[terminator@skynet ~]$ sudo nano /etc/fail2ban/jail.local
2024-03-23T18:19:25.65+0200
[terminator@skynet ~]$ sudo systemctl restart fail2ban
2024-03-23T18:23:02.21+0200
[terminator@skynet ~]$ sudo systemctl status fail2ban
2024-03-23T18:23:03.89+0200
● fail2ban.service - Fail2Ban Service
    Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
    Active: active (running) since Sat 2024-03-23 18:23:02 EET; 1s ago
      Docs: man:fail2ban(1)
      Main PID: 3152 (fail2ban-server)
         Tasks: 5 (limit: 4181)
        Memory: 12.1M
          CPU: 350ms
        CGroup: /system.slice/fail2ban.service
                 └─3152 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Mar 23 18:23:02 skynet systemd[1]: Started Fail2Ban Service.
Mar 23 18:23:02 skynet fail2ban-server[3152]: Server ready
lines 1-13/13 (END)
```



Γ4. Εγκαταστήστε και παραμετροποιήστε το Σύστημα Ανίχνευσης Εισβολών (IDS) AIDE (Advanced Intrusion Detection Environment) για έλεγχο ακεραιότητας των αρχείων του συστήματος. Δοκιμάστε με απλές «κακόβουλες» ενέργειες ότι εντοπίζει τις μεταβολές που έχουν γίνει στο σύστημα.

Το AIDE (Advanced Intrusion Detection Environment) είναι ένα εργαλείο ανίχνευσης εισβολών που σχεδιάστηκε για να παρακολουθεί την ακεραιότητα των αρχείων σε ένα σύστημα. Χρησιμοποιεί διάφορους μηχανισμούς για να δημιουργήσει και να διατηρήσει μια βάση δεδομένων με τις κανονικές καταστάσεις των αρχείων, όπως checksums, χρονοσφραγίδες και άλλες πληροφορίες ακεραιότητας. Στη συνέχεια, συγκρίνει την παρούσα κατάσταση των αρχείων με τις αποθηκευμένες κανονικές τους τιμές και ειδοποιεί εάν εντοπιστεί οποιαδήποτε αλλαγή. Έτσι λοιπόν και εμείς αρχικά δημιουργήσαμε μία βάση με την εντολή **sudo aideinit** και έπειτα τρέξαμε το **sudo aide –check –config /etcv/aide/aide.conf** τη μία φορά στην αρχή της δημιουργίας του server και την άλλη μετά το πέρας της εργασίας και όπως παρατηρούμε εμφανίζονται οι αντίστοιχες αλλαγές που είχαμε κάνει στο σύστημα μας.



```
[terminator@skynet ~] $ sudo aideinit
2024-03-23T18:56:36.57+0200
Overwrite existing /var/lib/aide/aide.db.new [Yn]? y
Running aide --init...
Start timestamp: 2024-03-23 18:56:39 +0200 (AIDE 0.17.4)
AIDE initialized database at /var/lib/aide/aide.db.new
Ignored e2fs attributes: EIh

Number of entries: 124288

-----
The attributes of the (uncompressed) database(s):
-----

/var/lib/aide/aide.db.new
SHA256 : k09tF5er9gl/lC47qBplI93ClDD3mpe9
TJgDZVxIbu0=
```

```
[terminator@skynet ~] $ sudo aide --check --config /etc/aide/aide.conf
2024-03-23T19:04:24.52+0200
Start timestamp: 2024-03-23 19:04:24 +0200 (AIDE 0.17.4)
AIDE found differences between database and filesystem!!
Ignored e2fs attributes: EIh

Summary:
Total number of entries: 124288 ←
Added entries: 0
Removed entries: 0
Changed entries: 5

-----
Changed entries:
-----

f =.... ....H... : /aquota.user
d =.... mc.... : /home/terminator
f >.... mc..H... : /home/terminator/.zsh_history
f =.... mc..H... : /var/lib/fail2ban/fail2ban.sqlite3
f >b... mc..H... : /var/log/audit/audit.log
```



```
d+*****: /var/www
d+*****: /var/www/html
f+*****: /var/www/html/index.html
d+*****: /var/www/sec_team
f+*****: /var/www/sec_team/index.html

-----
The attributes of the (uncompressed) database(s):
-----

/var/lib/aide/aide.db.new
SHA256   : 47DEQpj8HBSa+/TImW+5JCeuQeRkm5NM
            pJWZG3hSuFU=
SHA512   : z4PhNX7vuL3xVChQ1m2AB9Yg5AULVxXc
            g/SpIdNs6c5H0NE8XYXysP+DGNKHFuwv
            Y7kxvUdBeoGlODJG+SfaPg==
RMD160    : nBGFpcXp/FRhKAiXfuj1SLlIjTE=
TIGER     : JPATDG0skzIWfM52sbuSX/Nz3i1JWE56
CRC32     : AAAAAA== 
HAVAL     : T2k4Ux8LyJkfYtp7vW994/rURWK4xvTr
            8UbVt0RvfBc=
WHIRLPOOL : Gfph11UiPGabR00cHS4XJsUwIyEw1Af4
            mv7glkmX96c+g75piyiP68+I4+A8TwDX
            6oIk5Ztj2TcIsTjMQqZusw==
GOST      : zoW5nMRnUv/+41yrmnsCeKu0wtIFXP9o
            WvSRLElJD40= 

End timestamp: 2024-04-05 19:49:29 +0300 (run time: 8m 0s)
```



## Δ. Εγκατάσταση υπηρεσιών στον εξυπηρετητή

**Δ1.** Εγκαταστήστε και παραμετροποιήστε με γνώμονα την ασφάλεια του ΛΣ, τις υπηρεσίες «Φιλοξενίας Ιστοσελίδων» (Web Service) και «Database Service». Σίγουρα δεν εγκαθιστούμε ποτέ πολλές υπηρεσίες μαζί σε έναν μόνο εξυπηρετητή στο δίκτυο μας αλλά κάνουμε την επιλογή αυτή για τις ανάγκες της συγκεκριμένης εργασίας. Ελέγχετε και επιδείξτε τη λειτουργικότητα των παρεχόμενων υπηρεσιών μετά την εγκατάσταση τους.

Στην αρχή της δημιουργίας του web server απαραίτητο εργαλείο είναι το apache το οποίο και εγκαταστήσαμε και φροντίσαμε να ελεγχουμε ότι τρέχει σωστά με την εντολή **sudo systemctl status apache2**. Έπειτα προσθέσαμε το απαραίτητο rule στο firewall μας έτσι ώστε να επιτρέπεται η επικοινωνία από και πρός τον apache server.

```
[terminator@skynet ~]$ sudo apt install apache2
2024-03-30T17:42:10.38+0200
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libestr0 libfastjson4
use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.3-0 mailcap mime-support
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser bzip2-doc
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.3-0 mailcap mime-support
  upgraded 12 newly installed, 0 to remove and 3 not upgraded
```



```
[terminator@skynet ~]$ sudo systemctl start apache2
2024-03-30T17:43:51.62+0200
[terminator@skynet ~]$ sudo systemctl status apache2
2024-03-30T17:43:58.71+0200
● apache2.service - The Apache HTTP Server
    Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
      Active: active (running) since Sat 2024-03-30 17:42:24 EET; 1min 33s ago
        Docs: https://httpd.apache.org/docs/2.4/
       Main PID: 3519 (apache2)
          Tasks: 55 (limit: 4181)
         Memory: 5.2M
            CPU: 61ms
           CGroup: /system.slice/apache2.service
                   ├─3519 /usr/sbin/apache2 -k start
                   ├─3520 /usr/sbin/apache2 -k start
                   ├─3521 /usr/sbin/apache2 -k start
```

```
[terminator@skynet ~]$ sudo ufw allow 'Apache'
2024-03-30T17:48:09.18+0200
Rule added
Rule added (v6)
[terminator@skynet ~]$ sudo ufw status
2024-03-30T17:48:13.72+0200
Status: active

To                         Action      From
--                         -----      ---
Apache                      ALLOW      Anywhere
Apache (v6)                  ALLOW      Anywhere (v6)

[terminator@skynet ~]$
```

Τέλος αφου σιγουρευτήκαμε ότι το configuration του apache λειτουργεί σωστά δημιουργήσαμε ένα template site το οποίο και επισκευτήκαμε με το αντίστοιχο domain και εκεί μας περίμενε ένα ιδιαίτερο μήνυμα.



The screenshot shows a web browser window with the URL `192.168.1.29`. The page is titled "Apache2 Default Page". It features a red arrow pointing to the Ubuntu logo and another red arrow pointing to the "It works!" button. Below the title, there is a message about the default welcome page and configuration files. A section titled "Configuration Overview" provides a tree view of the Apache configuration directory:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.load
|   '-- *.conf
|-- conf-enabled
|   '-- *.conf
|-- sites-enabled
|   '-- *.conf
```

```
GNU nano 6.2          /etc/apache2/sites-available/sec_team.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    ServerName sec_team
    ServerAlias www.sec_team
    DocumentRoot /var/www/sec_team
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

The screenshot shows a web browser window with the URL `www.sec_team/`. The page displays a large red arrow pointing upwards. The content of the page is:  
**To ptixio me kiniga alla parameno protos !!!**  
**O Leoutsakos einai o Thanasis Vegos tou MPES**



Όσον αφορά το database server αρχικά εγκαταστήσαμε το πακέτο mysql-server και αφού σιγουρευτήκαμε ότι τρέχει σωστά ξεκινήσαμε το απαραίτητο configuration όπου και δημιουργήσαμε ένα admin χρήστη με τα απαραίτητα δικαιώματα και φροντίσαμε να αφαιρέσουμε τους υπόλοιπους ανώνυμους users και την πρόσβαση του root remotely.

```
[terminator@skynet ~]$ sudo apt install mysql-server
2024-04-07T17:44:35.88+0300
[sudo] password for terminator:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
mysql-server is already the newest version (8.0.36-0ubuntu0.22.04.1).
```

```
[terminator@skynet ~]$ sudo systemctl start mysql.service
2024-03-30T18:32:27.19+0200
[terminator@skynet ~]$ sudo systemctl enable mysql.service
2024-03-30T18:32:33.56+0200
Synchronizing state of mysql.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable mysql
[terminator@skynet ~]$ sudo systemctl status mysql.service
2024-03-30T18:32:40.14+0200
● mysql.service - MySQL Community Server
   Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2024-03-30 18:31:42 EET; 57s ago
       Main PID: 5477 (mysqld)
          Status: "Server is operational"
         Tasks: 38 (limit: 4181)
        Memory: 365.6M
          CPU: 1.255s
         CGroup: /system.slice/mysql.service
                   └─5497 /usr/sbin/mysqld

Mar 30 18:31:41 skynet systemd[1]: Starting MySQL Community Server...
Mar 30 18:31:42 skynet systemd[1]: Started MySQL Community Server.
[terminator@skynet ~]$
```



```
[terminator@skynet ~]$ sudo mysql_secure_installation
2024-03-30T18:47:32.83+0200
[sudo] password for terminator:

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: y

There are three levels of password validation policy:

LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary
      file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 1
```

```
Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
Success.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : n
```

```
mysql> CREATE USER 'admin'@'localhost' IDENTIFIED BY 'root';
Query OK, 0 rows affected (0.02 sec)

mysql>
```



```
mysql> GRANT CREATE, ALTER, DROP, INSERT, UPDATE, INDEX, DELETE, SELECT, REFERENCES, RELOAD  
ON *.* TO 'admin'@'localhost' WITH GRANT OPTION;  
Query OK, 0 rows affected (0.01 sec)
```

Kai πράγματι βλέπουμε ότι με την εντολή **sudo mysqladmin -p -u admin version** η βάση μας τρέχει κανονικά.

```
[terminator@skynet ~]$ sudo mysqladmin -p -u admin version  
2024-03-30T19:16:25.16+0200  
Enter password:  
mysqladmin Ver 8.0.36-0ubuntu0.22.04.1 for Linux on x86_64 ((Ubuntu))  
Copyright (c) 2000, 2024, Oracle and/or its affiliates.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Server version      8.0.36-0ubuntu0.22.04.1  
Protocol version    10  
Connection          Localhost via UNIX socket  
UNIX socket         /var/run/mysqld/mysqld.sock  
Uptime:             13 min 52 sec  
  
Threads: 3  Questions: 21  Slow queries: 0  Opens: 171  Flush tables: 3  Open tables: 90  
Queries per second avg: 0.025
```



Δ2. Περιγράψτε αναλυτικά τις ρυθμίσεις που κάνατε για την ασφαλή παροχή των παραπάνω υπηρεσιών (π.χ. απενεργοποίηση default λογαριασμών, δημιουργία διαχειριστών για πρόσβαση στις υπηρεσίες με συγκεκριμένα δικαιώματα, ορισμός κανόνων ελέγχου πρόσβασης, καταγραφή/παρακολούθηση ενεργειών για απόπειρες μη εξουσιοδοτημένης πρόσβασης και άλλες ύποπτες δραστηριότητες). Εφαρμόστε την αρχή του ελάχιστου προνομίου στις παραμετροποιήσεις των υπηρεσιών. Δοκιμάστε μετά τις αλλαγές που κάνατε την ορθή λειτουργία των υπηρεσιών. Για καθεμία από τις αλλαγές που κάνατε τεκμηριώστε τη σκοπιμότητα της αλλαγής και τι ακριβώς επιτυγχάνεται με αυτήν.

Αρχικά για να διασφαλίσουμε την ασφαλή λειτουργία του server φροντίσαμε να εγκαταστήσουμε το bind9 (διακομιστής DNS) και να το ρυθμίσουμε κατάλληλα με το DNSSEC (DNS Security Extensions) με σκοπό την επαλήθευση και την επιβεβαίωση της ακεραιότητας των απαντήσεων DNS, διασφαλίζοντας ότι οι αντιστοιχίες διευθύνσεων IP που επιστρέφονται από το DNS είναι αυθεντικές και δεν έχουν τροποποιηθεί κατά τη μετάβαση από τον διακομιστή DNS στον τελικό χρήστη και βασίζεται στη χρήση κρυπτογραφίας δημόσιου κλειδιού (public-key cryptography)

```
[terminator@skynet ~]$ sudo apt install bind9
2024-04-05T21:15:32.36+0300
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bind9 is already the newest version (1:9.18.18-0ubuntu0.22.04.2).
The following packages were automatically installed and are no longer required:
  libestr0 libfastjson4
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```



```
[terminator@skynet ~] $ sudo systemctl status bind9
2024-04-05T21:23:50.40+0300
● named.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2024-04-05 21:23:42 EEST; 7s ago
    Docs: man:named(8)
 Process: 8101 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 8102 (named)
   Tasks: 8 (limit: 4181)
  Memory: 6.2M
    CPU: 77ms
   CGroup: /system.slice/named.service
           └─8102 /usr/sbin/named -u bind

Apr 05 21:23:42 skynet named[8102]: configuring command channel from '/etc/bind/rndc.key'
Apr 05 21:23:42 skynet named[8102]: command channel listening on ::1#953
Apr 05 21:23:42 skynet named[8102]: managed-keys-zone: loaded serial 2
Apr 05 21:23:42 skynet named[8102]: zone 0.in-addr.arpa/IN: loaded serial 1
Apr 05 21:23:42 skynet named[8102]: zone 255.in-addr.arpa/IN: loaded serial 1
Apr 05 21:23:42 skynet named[8102]: zone 127.in-addr.arpa/IN: loaded serial 1
Apr 05 21:23:42 skynet named[8102]: zone localhost/IN: loaded serial 2
Apr 05 21:23:42 skynet named[8102]: all zones loaded
Apr 05 21:23:42 skynet named[8102]: running
Apr 05 21:23:42 skynet systemd[1]: Started BIND Domain Name Server.
[terminator@skynet ~]$
```



```
listen-on-v6 { any; };
dnssec-enable yes;
dnssec-validation auto;

include "/etc/bind/keys/sec_team.com.*.key";
```

Έπειτα όσον αφορά τον database server αρχικά εγκαταστήσαμε το ModSecurity (σύστημα ανίχνευσης και πρόληψης εισβολών (IDS/IPS) και φροντίσαμε να ελέγξουμε τη σωστή λειτουργία του. Επιπρόσθετα δημιουργήσαμε το datauser1 στον οποίο φροντίσαμε να δώσουμε μόνο τα απολούτως απαραίτητα δικαιώματα (σύμφωνα με την αρχή του ελάχιστου προνομίου) και πράγματι όπως βλέπουμε παρατηρήσαμε ότι δεν μπορούμε να κάνουμε drop το table.

```
[terminator@skynet ~]$ sudo apt-get install libapache2-mod-security2
2024-04-07T17:59:25.57+0300
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

```
[terminator@skynet ~]$ sudo a2enmod security2
2024-04-07T18:00:57.97+0300
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
[terminator@skynet ~]$
```



```
[terminator@skynet ~]$ sudo mysqladmin -p -u datauser1 version
2024-03-30T19:33:22.36+0200
[sudo] password for terminator:
Enter password:
mysqladmin Ver 8.0.36-0ubuntu0.22.04.1 for Linux on x86_64 ((Ubuntu))
Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Server version      8.0.36-0ubuntu0.22.04.1
Protocol version    10
Connection          Localhost via UNIX socket
UNIX socket         /var/run/mysqld/mysqld.sock
Uptime:              9 min 6 sec

Threads: 2  Questions: 9  Slow queries: 0  Opens: 148  Flush tables: 3  Open tables: 67  Q
ueries per second avg: 0.016
```



```
[terminator@skynet ~]$ mysql -u datauser1 -p -e "SHOW TABLES FROM mysql;"  
2024-03-30T19:37:11.55+0200  
Enter password:  
+-----+  
| Tables_in_mysql |  
+-----+  
| columns_priv   |  
| component      |  
| db             |  
| default_roles  |  
| engine_cost    |  
| func           |  
| general_log    |  
| global_grants  |  
| gtid_executed  |  
| help_category  |  
| help_keyword   |  
| help_relation  |  
| help_topic     |  
| innodb_index_stats |  
| innodb_table_stats |  
| password_history |  
| plugin          |  
| procs_priv     |  
| proxies_priv   |  
| replication_asynchronous_connection_failover |  
| replication_asynchronous_connection_failover_managed |  
| replication_group_configuration_version |  
| replication_group_member_actions |  
| role_edges      |  
| server_cost     |  
| servers          |  
| slave_master_info |  
| slave_relay_log_info |  
| slave_worker_info |  
| slow_log         |  
| tables_priv     |  
| time_zone       |  
| time_zone_leap_second |  
| time_zone_name  |  
| time_zone_transition |  
| time_zone_transition_type |  
| user            |  
+-----+  
[terminator@skynet ~]$
```

```
mysql> GRANT INDEX, SELECT, REFERENCES, RELOAD on *.* TO 'datauser1'@'localhost' WITH GRAN  
T OPTION;  
Query OK, 0 rows affected (0.01 sec)
```



```
[terminator@skynet ~]$ mysql -u datauser1 -p -e "DROP TABLES mysql.columns_priv;"  
  
2024-03-30T19:38:56.55+0200  
Enter password:  
ERROR 1142 (42000) at line 1: DROP command denied to user 'datauser1'@'localhost' for table 'columns_priv'
```



## E. Ενδυνάμωση του Λειτουργικού Συστήματος

Ενεργοποιήστε το Security-enhanced Linux (SELinux). Το SELinux αποτελεί μια υλοποίηση αναφοράς της αρχιτεκτονικής ασφάλειας Flask για ευέλικτο έλεγχο πρόσβασης – flexible mandatory access control (MAC). Ρυθμίστε το SELinux σε "permissive" λειτουργία. Η λειτουργία permissive είναι μία από τις τρεις καταστάσεις στις οποίες λειτουργεί το SELinux, δηλαδή Enforcing, Permissive και Disabled. Κάθε φορά που είναι ενεργοποιημένο το SELinux, είτε θα λειτουργεί στη κατάσταση enforcing είτε στη κατάσταση permissive. Η κατάσταση enforcing λειτουργεί εφαρμόζοντας όλους τους κανόνες που αναφέρονται στην πολιτική ασφαλείας SELinux. Αποκλείει την πρόσβαση όλων των χρηστών που δεν επιτρέπεται να έχουν πρόσβαση σε ένα συγκεκριμένο αντικείμενο στην πολιτική ασφαλείας. Επιπλέον, αυτή η δραστηριότητα καταγράφεται επίσης στο αρχείο καταγραφής SELinux.

Στη κατάσταση permissive, το λειτουργικό σύστημα είναι διαμορφωμένο με SELinux, αλλά σε περιπτώσεις παράκαμψης των πολιτικών ασφάλειας προκαλεί μόνο την εμφάνιση ενός μηνύματος σφάλματος. Συνεπώς καμία δραστηριότητα δεν τίθεται σε περιορισμό όταν το SELinux εγκαθίσταται σε αυτή τη κατάσταση. Δοκιμάστε να παρακάμψετε κάποιες πολιτικές ασφαλείας και ελέγχετε ότι εμφανίστηκαν τα κατάλληλα μηνύματα λάθους.

Στο ερώτημα αυτό, ζητείται να ενεργοποιήσουμε το Security-enhanced Linux (SELinux) σε λειτουργία "permissive" σε ένα λειτουργικό σύστημα. Το SELinux είναι ένα σύστημα ασφαλείας που παρέχει ένα ευέλικτο έλεγχο πρόσβασης (flexible mandatory access control - MAC), βασισμένο στην αρχιτεκτονική ασφάλειας Flask.



Συγκεκριμένα, η λειτουργία "permissive" επιτρέπει στο SELinux να εκτελείται, αλλά δεν επιβάλλει τους κανόνες ασφαλείας του.

```
[terminator@skynet ~]$ getenforce
2024-04-07T19:00:26.01+0300
Permissive

[terminator@skynet ~]$ sestatus
2024-04-07T19:00:37.95+0300
SELinux status:                      enabled
SELinuxfs mount:                     /sys/fs/selinux
SELinux root directory:              /etc/selinux
Loaded policy name:                  default
Current mode:                        permissive
Mode from config file:              permissive
Policy MLS status:                  enabled
Policy deny_unknown status:         allowed
Memory protection checking:         requested (insecure)
Max kernel policy version:          33
[terminator@skynet ~]$
```

Αντίθετα, απλώς καταγράφει τις ενέργειες που θα είχαν απορριφθεί στο αρχείο καταγραφής SELinux. Αυτό επιτρέπει στους διαχειριστές συστημάτων να δοκιμάσουν διάφορες πολιτικές ασφαλείας χωρίς να περιορίζουν τη λειτουργικότητα του συστήματος. Όπως πράγματι βλέπουμε παρακάτω με την εντολή **audit2why < /var/log/audit/audit.log**

```
[terminator@skynet ~]$ audit2why < /var/log/audit/audit.log
```



Όπου βλέπουμε μια πληθώρα μυνημάτων με χαρακτηριστικό παράδειγμα το συγκεκριμένο στο οποίο π αναφέρει ότι μια ενέργεια απορρίφθηκε λόγω των κανόνων ασφαλείας SELinux. Συγκεκριμένα, η ενέργεια που απορρίφθηκε ήταν η αναζήτηση (search) στον κατάλογο / από τη διεργασία με τον αριθμό PID 1938, που εκτελείται με την εντολή systemd-user-r. Η απόρριψη αυτή προκύπτει επειδή η πρόσβαση δεν επιτρέπεται από τους κανόνες SELinux.

```
type=AVC msg=audit(1712505342.847:350): avc: [denied] { setattr } for pid=1988 comm="systemd-tmpfile" name="/" dev="cgroup2" ino=1 scontext=system_u:system_r:systemd_tmpfiles_t:s0 tcontext=system_u:object_r:cgroup_t:s0 tclass=filesystem permissive=1  
Was caused by:  
Missing type enforcement (TE) allow rule.  
You can use audit2allow to generate a loadable module to allow this access
```

Έτσι λοιπόν βλέπουμε ότι η λειτουργία permissive μας επιτρέπει να χειριζόμαστε σωστά και με ασφάλεια τον server καθώς μποτρούμε να ελέγξουμε οποιαδήποτε κακόβουλη κίνηση έχει γίνει χωρίς αυτό να μας περιορίζει στο βαθμό που το κάνει το enforcing που είναι η κατάσταση όπου οι κανόνες ασφαλείας SELinux εφαρμόζονται ενεργά και επιβάλλονται αυστηρά στο σύστημα. Αυτό σημαίνει ότι το SELinux ελέγχει και περιορίζει τις ενέργειες που μπορούν να πραγματοποιηθούν από τις εφαρμογές και τους χρήστες, βάσει των κανόνων ασφαλείας που έχουν οριστεί.

Σε λειτουργία "enforcing", αν μια ενέργεια παραβιάζει τους κανόνες ασφαλείας SELinux, τότε αυτή η ενέργεια απορρίπτεται και καταγράφεται στο αρχείο καταγραφής SELinux. Το SELinux ενεργεί ως ένα είδος φράγματος που προστατεύει το σύστημα από πιθανές επιθέσεις ή κακόβουλες ενέργειες.

Η λειτουργία "enforcing" προσφέρει υψηλό επίπεδο ασφάλειας, καθώς εξασφαλίζει ότι οι πολιτικές ασφαλείας SELinux τηρούνται αυστηρά. Ωστόσο, αυτή η λειτουργία μπορεί να οδηγήσει σε περιορισμούς στη λειτουργικότητα του συστήματος, καθώς ορισμένες ενέργειες μπορεί να απορρίπτονται λόγω των αυστηρών κανόνων ασφαλείας.



## ΣΤ. Αντίγραφα ασφαλείας και αποκατάσταση μετά από καταστροφή

Προτείνετε ένα σχέδιο για δημιουργία αντιγράφων ασφαλείας με βάση τις ανάγκες και τις παρεχόμενες υπηρεσίες του εξυπηρετητή. Μπορείτε να χρησιμοποιήσετε εργαλεία όπως rsync, bacula, ή borgbackup για αυτοματοποιημένες λύσεις δημιουργίας αντιγράφων.

Για να κρατήσουμε τα δεδομένα μας ασφαλή και διαθέσιμα σε περίπτωση προβλήματος με τον εξυπηρετητή, πρέπει να φτιάξουμε ένα καλό σχέδιο αντιγράφων ασφαλείας και αποκατάστασης. Ας δούμε ένα απλό σχέδιο που χρησιμοποιεί τα εργαλεία rsync, Bacula και BorgBackup, τα οποία κάνουν την διαδικασία πιο εύκολη και αυτοματοποιημένη. Το σχέδιο αυτό θα μας βοηθήσει να φροντίσουμε ώστε τα δεδομένα μας να είναι ασφαλή και προσβάσιμα.

### 1. Ανάλυση και Προετοιμασία

- Αναγνώριση Κρίσιμων Δεδομένων:** Αρχικά πρέπει να αναγωνρίσουμε ποια δεδομένα είναι κρίσιμα για τη σωστή λειτουργία του συστήματος και πρέπει να προστατεύονται.
- Κατηγοριοποίηση Δεδομένων:** Έπειτα πρέπει να κατηγοριοποιήσουμε αυτά τα δεδομένα βάσει της σημαντικότητάς τους και του πόσο συχνά αλλάζουν. Για παράδειγμα δεδομένα που αλλάζουν κάθε μέρα και είναι απαραίτητα για την καθημερινή λειτουργία της επιχείρησης, ενώ υπάρχουν και άλλα που είναι σταθερά και δεν αλλάζουν τόσο συχνά.
- Επιλογή Μεθόδου Backup:** Τέλος, πρέπει να επιλέξουμε την κατάλληλη μέθοδο αντιγράφου ασφαλείας για τα δεδομένα μας. Αυτό μπορεί να είναι ένα πλήρες αντίγραφο που περιλαμβάνει όλα τα δεδομένα, ένα διαφορικό αντίγραφο που περιλαμβάνει μόνο τις αλλαγές από το τελευταίο πλήρες αντίγραφο, ή ένα αυξητικό αντίγραφο που περιλαμβάνει μόνο τις νέες αλλαγές από το τελευταίο αντίγραφο (είτε πλήρες είτε διαφορικό).



## 2. Επιλογή Εργαλείων

- **Rsync:** Είναι ένα εργαλείο που μας βοηθάει να κάνουμε αυτόματο συγχρονισμό και αντίγραφα ασφαλείας των δεδομένων μας σε πραγματικό χρόνο.
- **Bacula:** Χρησιμοποιείται συνήθως σε περιβάλλοντα με μεγάλο όγκο δεδομένων και παρέχει λεπτομερή διαχείριση και ανάκτηση δεδομένων.
- **BorgBackup:** Είναι μια εξαιρετική επιλογή για αποδοτική συμπίεση και αποθήκευση αντιγράφων ασφαλείας σε απομακρυσμένες τοποθεσίες.

## 3. Καθορισμός Συχνότητας και Χρονοδιαγραμμάτων

- **Συχνότητα Αντιγράφων:** Πρέπει να αποφασίσουμε πόσο συχνά θα κάνουμε αντίγραφα ασφαλείας βασιζόμενοι στη σημασία και τη σημαντικότητα των δεδομένων.
- **Αυτοματισμός:** Μπορούμε να ρυθμίσουμε προγραμματισμένες εργασίες με τη χρήση cron jobs ή παρόμοιων εργαλείων για την αυτόματη εκτέλεση των αντιγράφων ασφαλείας.

## 4. Αποθήκευση και Διαχείριση Αντιγράφων

- **Πολλαπλές Τοποθεσίες:** Είναι σημαντικό να αποθηκεύουμε τα αντίγραφα σε διαφορετικές τοποθεσίες για να προστατεύμαστε από τοπικές καταστροφές.
- **Ασφάλεια:** Χρησιμοποιούμε κρυπτογράφηση και ασφαλή πρωτόκολλα μεταφοράς δεδομένων για την ασφαλή αποθήκευση των αντιγράφων ασφαλείας.

## 5. Δοκιμή και Επαναφορά

- **Δοκιμαστικές Επαναφορές:** Πρέπει να πραγματοποιούμε τακτικά δοκιμαστικές επαναφορές για να εξασφαλίσουμε ότι τα αντίγραφα ασφαλείας είναι λειτουργικά.
- **Αξιολόγηση και Βελτίωση:** Αναθεωρούμε το σχέδιο ανάλογα με τις αλλαγές στο περιβάλλον και τις ανάγκες της επιχείρησης.



## 6. Πρόσθετες Ενέργειες/Ρυθμίσεις

- **Παρακολούθηση:** Κάνουμε εγκατάσταση συστημάτων παρακολούθησης για να ανιχνεύουμε έγκαιρα προβλήματα στη διαδικασία backup.
- **Εκπαίδευση Προσωπικού:** Εκπαιδεύουμε το προσωπικό σχετικά με τη σωστή χρήση των εργαλείων και τις διαδικασίες ασφαλείας.

Ελέγξτε το σύστημα σας για τρωτά σημεία χρησιμοποιώντας κατάλληλα εργαλεία. Έχουν αναπτυχθεί εργαλεία τα οποία ανιχνεύουν το σύστημα για τυχόν επικίνδυνες για την ασφάλεια ρυθμίσεις και ενημερώνουν για ελλείψεις κρίσιμων ενημερώσεων που αφορούν πρωτίστως την ασφάλεια.

Όπως λοιπόν μας υποδείχθηκε αξιοποιήσαμε τα εργαλεία lynis και nmap και έχουμε τα παρακάτω αποτελέσματα.

Όσον αφορά το nmap παρατηρούμε πως το αρχικό με το τελικό screenshot δεν διαφέρουν σε μεγάλο βαθμό κάτι που μας χαροποιεί ιδιαιτέρως, καθώς πέραν του ανοικτού port για το http το οποίο θα μπορούσε πολύ εύκολα να ασφαλιστεί με την αγορά ενός domain name και τη χρήση https δεν παρατηρούμε κάποια άλλη σοβαρή αλλαγή στα αποτελέσματα.



```
[konstantman@arch ~]$ sudo nmap -Pn -A -sS -O -sV 192.168.1.29
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-07 05:43 EEST
Nmap scan report for 192.168.1.29 (192.168.1.29)
Host is up (0.00027s latency).
All 1000 scanned ports on 192.168.1.29 (192.168.1.29) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:BA:B5:6E (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.27 ms  192.168.1.29 (192.168.1.29)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 2.19 seconds
[konstantman@arch ~]$
```

```
[konstantman@arch ~]$ sudo nmap -Pn -A -sS -O -sV 192.168.1.29
[sudo] password for konstantman:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-07 05:38 EEST
Nmap scan report for www.sec_team (192.168.1.29)
Host is up (0.00023s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: PTIXIO
MAC Address: 08:00:27:BA:B5:6E (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose/storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), Synology DiskStation Manager 5.X (90%), Netgear RAIDiator 4.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/a:synology:diskstation_manager:5.2 cpe:/o:netgear:raidiator:4.2.28
Aggressive OS guesses: Linux 4.15 - 5.8 (97%), Linux 5.0 - 5.4 (97%), Linux 5.0 - 5.5 (95%), Linux 2.6.32 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.9 (91%), Linux 3.4 - 3.10 (91%), Linux 5.1 (91%), Linux 2.6.32 - 3.10 (91%), Linux 2.6.32 - 3.13 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.23 ms  www.sec_team (192.168.1.29)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 19.92 seconds
(konstantman@arch ~]$
```

Όσον αφορά το lynis παρατηρούμε με χαρά και δέος πως το score που πετύχαμε στο πρώτο scan είναι **78**.



```
[terminator@skynet ~/lynis]$ ./lynis audit system
2024-04-07T04:17:24.14+0300

[ Lynis 3.1.2 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2021, CISOfy - https://cisofty.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----

#####
#                                     #
#   NON-PRIVILEGED SCAN MODE          #
#                                     #
#####
```

```
=====
Lynis security scan details:

Hardening index : 78 [#####
Tests performed : 267
Plugins enabled : 2

Components:
- Firewall           [V]
- Malware scanner    [V]

Scan mode:
Normal [ ] Forensics [ ] Integration [ ] Pентest [V] (running non-privileged)
```

Προφανώς βέβαια μπορούμε να εκμεταλλευτούμε τα ερωτήματα που δίνει το lynis για να ασφαλίσουμε το server και κατ' επέκταση να αυξήσουμε και το score.

Συλλήβδην, μετά το πέρας της εργασίας αντιλαμβανόμαστε πως η δημιουργία και η ασφάλιση ενός server είναι κρίσιμης σημασίας και απαιτεί αρκετά βήματα πέραν από αυτά που μας ζητούνται τα οποία καθόλη την διάρκεια σας έχουμε προτείνει με την χρήση του όρου "Bonus" και επιπροσθέτως προτείνουμε και τα παρακάτω:



Πρωταρχικό κομμάτι του compartmentalization είναι ο διαχωρισμός των βασικών κομματιών του server σε partitions, με σκοπό και να αποφύγουμε τη καταστροφή όλων των αρχείων ώστε να μειώσουμε το impact μιας πιθανής επίθεσης και να κάνουμε πιο εύκολη τη λειτουργία backup, όπως μα προτείνεται και από το lynis.

```
* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls(FILE-6310)

* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls(FILE-6310)

* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls(FILE-6310)
```

Έπειτα καλό είναι να χρησιμοποιούμε ένα “malware scanner” στη συγκεκριμένη περίπτωση το rkhunter στο οποίο αρχικά κάνουμε manually ένα πρώτο scan και έπειτα το ρυθμίζουμε να γίνεται αυτοματοποιημένα με τη χρήση cron jobs.



```
[terminator@skynet ~]$ sudo rkhunter --check
```

```
2024-04-07T19:50:34.03+0300
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

Performing 'strings' command checks
  Checking 'strings' command [ OK ]

Performing 'shared libraries' checks
  Checking for preloading variables [ None found ]
  Checking for preloaded libraries [ None found ]
  Checking LD_LIBRARY_PATH variable [ Not found ]

Performing file properties checks
  Checking for prerequisites [ OK ]
  /usr/sbin/adduser [ OK ]
  /usr/sbin/chroot [ OK ]
  /usr/sbin/cron [ OK ]
  /usr/sbin/depmod [ OK ]
  /usr/sbin/fsck [ OK ]
  /usr/sbin/groupadd [ OK ]
  /usr/sbin/groupdel [ OK ]
  /usr/sbin/groupmod [ OK ]
```

Τέλος για να είμαστε και νομικά καλυμμένοι μπορούμε να προσθέσουμε ένα banner κατα την έισοδο του χρήστη στο server το οποίο θα υποδεικνύει ότι είναι μέρος ατομικής ιδιοκτησίας.

```
*****
WARNING: This is a private system. Unauthorized access is prohibited. ←
*****
Ubuntu 22.04.4 LTS skynet tty4
```



## Βιβλιογραφία

- [https://www.youtube.com/watch?v=04pAiANkr\\_s](https://www.youtube.com/watch?v=04pAiANkr_s)
- [https://www.youtube.com/watch?v=lm\\_4hoe-K7U](https://www.youtube.com/watch?v=lm_4hoe-K7U)
- [https://www.youtube.com/watch?v=Kq\\_JOGX0MW4](https://www.youtube.com/watch?v=Kq_JOGX0MW4)
- <https://superuser.com/questions/802894/ubuntu-server-how-to-make-a-domain-point-to-it>
- <https://www.nuharborsecurity.com/blog/ubuntu-server-hardening-guide-2>
- <https://github.com/arch-installer/setup>
- <https://stackoverflow.com/questions/40076573/adding-timestamp-to-each-line-on-zsh>
- <https://www.tecmint.com/ss-command-examples-in-linux/>
- <https://linuxize.com/post/how-to-configure-static-ip-address-on-ubuntu-18-04/>
- <https://motorscript.com/cleanup-ubuntu-server/>
- <https://www.maketecheasier.com/how-to-set-up-firewall-linux/>
- <https://www.hostinger.com/tutorials/iptables-tutorial>
- <https://kinsta.com/knowledgebase/ssh-connection-refused/>
- <https://www.geeksforgeeks.org/add-a-user-in-linux-using-python-script/>
- <https://phoenixnap.com/kb/install-ftp-server-on-ubuntu-vsftpd>
- <https://support.tigertech.net/ftp-errors>
- [https://wiki.archlinux.org/title/Very\\_Secure\\_FTP\\_Daemon](https://wiki.archlinux.org/title/Very_Secure_FTP_Daemon)