

Συγχρονες εφαρμογες Ασφαλειας

Ονοματεπώνυμο : Νικόλας Φιλίππας

AM: 1072754

Εργασία: 3η

1. Προστασία ανεπιθύμητων επιθέσεων με χρήση του πακέτου fail2ban.

Εγκαταστήστε το πακέτο fail2ban στην εικονική μηχανή που έχετε φτιάξει. Ανατρέξτε στα φίλτρα (/etc/fail2ban/filter/d/) και στα αρχεία διαμόρφωσης fail2ban.conf και jail.conf που εγκαταστάθηκαν.

Installing the fail2ban :

```
sudo apt install fail2ban
```

```
don@debian:/etc/fail2ban$ ls
action.d      filter.d      jail.local    paths-debian.conf
fail2ban.conf jail.conf     paths-arch.conf paths-opensuse.conf
fail2ban.d    jail.d        paths-common.conf
```

Το fail2ban πακέτο με την εγκατάσταση του αυτόματα ενεργοποιεί το φίλτρο προστασίας για ssh επιθέσεις.

1. Ελέγξτε την κατάσταση των jails με την εντολή fail2ban-client status και fail2banclient status sshd.

```
don@debian:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:  sshd
```

```
don@debian:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:    0
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
  |- Currently banned: 0
  |- Total banned:    0
  `-- Banned IP list:
```

2. τροποποιήστε το αρχείο για το φίλτρο ssh ώστε κλειδώνει τις συνδέσεις μετά από 5 λανθασμένες προσπάθειες στα τελευταία 10 λεπτά.

Δημιουργούμε το αρχείο jail.local στον φακελο /etc/fail2ban.

Προσθετούμε τις γραμμες

```
maxretry = 5 # five wrong tries
findtime = 10m # if it has generated maxretry during the last "findtime"
```

Και ενεργοποιούμε το jail για το sshd

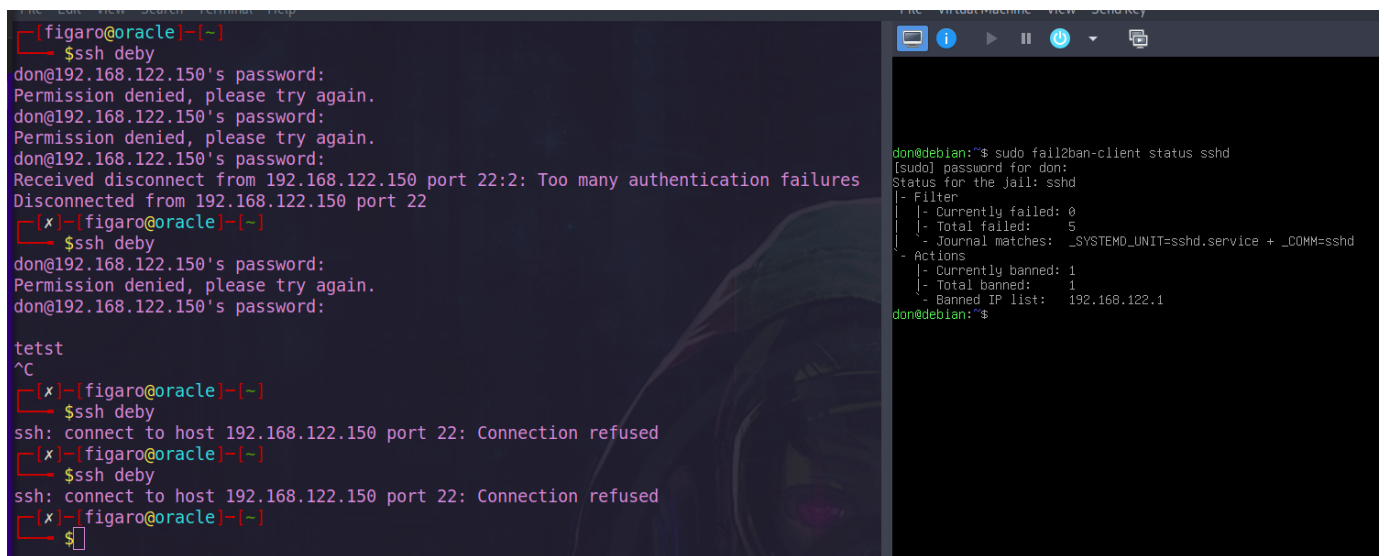
```
# [sshd]
enabled = true
```

Αλλάζουμε και το backend σε systemd που χρησιμοποιουν τα debian για να μπορεί να κάνει monitor τα log files.

3. Έχοντας δύο τερματικά ανοικτά, πραγματοποιείστε 5 προσπάθειες με λάθος κωδικό και δείτε το αποτέλεσμα με την εντολή `fail2ban-client status sshd`.

Το debby για διευκόλυνση των συνδέσεων, σύμφωνα με το ssh config file είναι :

```
Host debby
    HostName 192.168.122.150
    User don
```



The image shows two terminal windows. The left window is a terminal on the 'figaro@oracle' host. It shows a user 'don' attempting to SSH into '192.168.122.150' five times with incorrect passwords, resulting in 'Permission denied' and 'Received disconnect from 192.168.122.150 port 22: Too many authentication failures'. After a 'tst' command, the user 'figaro' attempts to SSH into '192.168.122.150' three times, resulting in 'Connection refused'. The right window is a terminal on the 'don@debian' host. It shows the command 'sudo fail2ban-client status sshd' being executed, displaying the status of the fail2ban service for the 'sshd' jail, including the number of failed attempts (5) and the current banned IP (192.168.122.1).

4. Σε ποιο log αρχείο καταγράφονται οι συνδέσεις? Ανοίξτε και δείτε τις τελευταίες γραμμές που δείχνουν την ανεπιτυχή σύνδεση.

Στο `/var/log/fail2ban.log` καταγραφονται οι συνδέσεις.

```
2023-11-02 17:38:13,003 fail2ban.server [494]: INFO Starting Fail2ban v1.0.2
2023-11-02 17:38:14,001 fail2ban.server [494]: INFO Observer start...
2023-11-02 17:38:14,004 fail2ban.observer [494]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/sqlite3'
2023-11-02 17:38:14,102 fail2ban.database [494]: INFO Creating new jail 'sshd'
2023-11-02 17:38:14,150 fail2ban.jail [494]: INFO Jail 'sshd' uses systemd {}
2023-11-02 17:38:14,383 fail2ban.jail [494]: INFO Initiated 'systemd' backend
2023-11-02 17:38:14,407 fail2ban.jail [494]: INFO maxLines: 1
2023-11-02 17:38:14,408 fail2ban.filter [494]: INFO [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
2023-11-02 17:38:14,418 fail2ban.filtersystemd [494]: INFO maxRetry: 5
2023-11-02 17:38:14,418 fail2ban.filter [494]: INFO findtime: 600
2023-11-02 17:38:14,419 fail2ban.filter [494]: INFO banTime: 600
2023-11-02 17:38:14,419 fail2ban.actions [494]: INFO encoding: UTF-8
2023-11-02 17:38:14,431 fail2ban.filtersystemd [494]: INFO [sshd] Jail is in operation now (process new journal)
2023-11-02 17:38:14,444 fail2ban.jail [494]: INFO Jail 'sshd' started
2023-11-02 19:10:23,356 fail2ban.filter [494]: INFO [sshd] Found 192.168.122.1 - 2023-11-02 19:10:22
2023-11-02 19:10:27,775 fail2ban.filter [494]: INFO [sshd] Found 192.168.122.1 - 2023-11-02 19:10:27
2023-11-02 19:10:33,073 fail2ban.filter [494]: INFO [sshd] Found 192.168.122.1 - 2023-11-02 19:10:32
2023-11-02 19:10:34,323 fail2ban.filter [494]: INFO [sshd] Found 192.168.122.1 - 2023-11-02 19:10:34
2023-11-02 19:10:42,073 fail2ban.filter [494]: INFO [sshd] Found 192.168.122.1 - 2023-11-02 19:10:41
2023-11-02 19:10:42,231 fail2ban.actions [494]: NOTICE [sshd] Ban 192.168.122.1
```

```

2023-11-02 17:38:13,983 fail2ban.server [494]: INFO -----
-----
2023-11-02 17:38:14,001 fail2ban.server [494]: INFO Starting Fail2ban v1.0.2
2023-11-02 17:38:14,004 fail2ban.observer [494]: INFO Observer start...
2023-11-02 17:38:14,102 fail2ban.database [494]: INFO Connected to fail2ban
persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2023-11-02 17:38:14,150 fail2ban.jail [494]: INFO Creating new jail 'sshd'
2023-11-02 17:38:14,383 fail2ban.jail [494]: INFO Jail 'sshd' uses systemd
{}
2023-11-02 17:38:14,407 fail2ban.jail [494]: INFO Initiated 'systemd'
backend
2023-11-02 17:38:14,408 fail2ban.filter [494]: INFO maxLines: 1
2023-11-02 17:38:14,418 fail2ban.filtersystemd [494]: INFO [sshd] Added journal
match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
2023-11-02 17:38:14,418 fail2ban.filter [494]: INFO maxRetry: 5
2023-11-02 17:38:14,419 fail2ban.filter [494]: INFO findtime: 600
2023-11-02 17:38:14,419 fail2ban.actions [494]: INFO banTime: 600
2023-11-02 17:38:14,419 fail2ban.filter [494]: INFO encoding: UTF-8
2023-11-02 17:38:14,431 fail2ban.filtersystemd [494]: INFO [sshd] Jail is in
operation now (process new journal entries)
2023-11-02 17:38:14,444 fail2ban.jail [494]: INFO Jail 'sshd' started
2023-11-02 19:10:23,356 fail2ban.filter [494]: INFO [sshd] Found
192.168.122.1 - 2023-11-02 19:10:22
2023-11-02 19:10:27,775 fail2ban.filter [494]: INFO [sshd] Found
192.168.122.1 - 2023-11-02 19:10:27
2023-11-02 19:10:33,073 fail2ban.filter [494]: INFO [sshd] Found
192.168.122.1 - 2023-11-02 19:10:32
2023-11-02 19:10:34,323 fail2ban.filter [494]: INFO [sshd] Found
192.168.122.1 - 2023-11-02 19:10:34
2023-11-02 19:10:42,073 fail2ban.filter [494]: INFO [sshd] Found
192.168.122.1 - 2023-11-02 19:10:41
2023-11-02 19:10:42,231 fail2ban.actions [494]: NOTICE [sshd] Ban 192.168.122.1

```

5. Δείτε ξανά την έξοδο της *fail2ban-client status sshd* και ελέγξτε το *firewall* σας εάν απορρίπτει την IP διεύθυνση από την οποία κάνατε τις ανεπιτυχές συνδέσεις.

```

don@debian:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed:     5
|   \- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
  |- Currently banned: 1
  |- Total banned:     1
  \- Banned IP list:   192.168.122.1

```

Συμφωνα με τα iptables απορριπτεται η διευθυνση μας για συνδεσεις

```

don@debian:~$ sudo !!
sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            multiport dports ssh
f2b-sshd    tcp  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain f2b-sshd (1 references)
target     prot opt source                destination
REJECT     all  --  192.168.122.1         anywhere              reject-with icmp-port-unreachable
RETURN     all  --  anywhere              anywhere

```

6. Με ποια εντολή κάνουμε “unban” την IP?

Μπορούμε να κάνουμε unban με την εντολή :

```
sudo fail2ban-client set JAILNAME unbanip IPADDRESS
```

Στην δικιά μας περίπτωση έχουμε JAILNAME=sshd και IPADDRESS=192.168.122.1

```

don@debian:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 5
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`-- Actions
    |- Currently banned: 0
    |- Total banned: 1
    `-- Banned IP list:

```

```

don@debian:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            multiport dports ssh
f2b-sshd    tcp  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain f2b-sshd (1 references)
target     prot opt source                destination
RETURN     all  --  anywhere              anywhere

```

7. Σε ποιο αρχείο μπορούμε να προσθέσουμε IP που δεν επιθυμούμε να φιλτράρονται? Πχ (τις IP διευθύνσεις από το εσωτερικό LAN).

Στο αρχείο jail.local βάζουμε χωρισμένες με κενό τις διευθύνσεις που θέλουμε να είναι whitelisted.

```
ignoreip = 192.169.0.0/16 192.168.0.0/16
```

Επειδή το virtual machine κάνει bridge στο εσωτερικό virtual network 192.168.0.0/16 πρέπει να το κάνουμε και αυτό whitelist.

Για να ισχύσει το καινούργιο jail.local κάνουμε restart

```
sudo systemctl restart fail2ban.service
```

Κάνουμε τον έλεγχο και βλέπουμε ότι δεν κάνει ban την ip μας οσες φορές και αν κάνουμε λάθος τον κωδικό

```
└─ $ssh deby
don@192.168.122.150s password:
Permission denied, please try again.
don@192.168.122.150s password:
Permission denied, please try again.
don@192.168.122.150s password:
Received disconnect from 192.168.122.150 port 22:2: Too many authentication failures
Disconnected from 192.168.122.150 port 22
```

```
└─ [X]─[figaro@oracle]─[~]
└─ $ssh deby
don@192.168.122.150s password:
Permission denied, please try again.
don@192.168.122.150s password:
Permission denied, please try again.
don@192.168.122.150s password:
Received disconnect from 192.168.122.150 port 22:2: Too many authentication failures
Disconnected from 192.168.122.150 port 22
```

```
└─ [X]─[figaro@oracle]─[~]
└─ $ssh deby
don@192.168.122.150s password:
Permission denied, please try again.
don@192.168.122.150s password:
Permission denied, please try again.
don@192.168.122.150s password:
Received disconnect from 192.168.122.150 port 22:2: Too many authentication failures
Disconnected from 192.168.122.150 port 22
```

8. **Εγκαταστήστε και ρυθμίστε το πακέτο sendmail ώστε το fail2ban να σας στέλνει email όταν μπλοκάρει μια IP διεύθυνση. Οδηγίες για την εγκατάσταση και ρύθμιση του sendmail μπορείτε να βρείτε εδώ.**

Εγκατάσταση των απαραίτητων πακετων :

```
sudo apt install -y sendmail sendmail-cf mailutils sendmail-bin
```

Επομενο βημα ειναι η δημιουργια ενος auth file για το email απο το οποιο θα στελνει :

```
sudo -i
mkdir -m 700 /etc/mail/authinfo
cd /etc/mail/authinfo
vim gmail-auth
```

Μεσα στο αρχειο gmail-auth βαζουμε τις εξης πληροφοριες

```
AuthInfo: "U:root" "I:YOUR GMAIL EMAIL ADDRESS" "P:YOUR PASSWORD"
```

Δημιουργουμε ενα hash map για το authentication file

```
makemap hash gmail-auth<gmail-auth
```

Επειτα επεξεργαζόμαστε το αρχείο `/etc/mail/sendmail.mc` και βάζουμε κατω απο το MAILER :

```
define(`SMART_HOST',`[smtp.gmail.com]')dn!
define(`RELAY_MAILER_ARGS', `TCP $h 587')dn!
define(`ESMTP_MAILER_ARGS', `TCP $h 587')dn!
define(`confAUTH_OPTIONS', `A p')dn!
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dn!
define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dn!
FEATURE(`authinfo',`hash -o /etc/mail/authinfo/gmail-auth.db')dn!
```

Ξαναχτιζουμε τα configurations του sendmail με το

```
make -C /etc/mail
```

κανουμε restart την υπηρεσια sendmail

```
systemctl restart sendmail
```

Check for status

```
systemctl status sendmail
• sendmail.service - LSB: powerful, efficient, and scalable Mail Transport Agent
   Loaded: loaded (/etc/init.d/sendmail; generated)
   Active: active (running) since Sun 2023-11-05 16:56:07 EET; 14s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 462 ExecStart=/etc/init.d/sendmail start (code=exited, status=0/SUCCESS)
    Tasks: 1 (limit: 1099)
   Memory: 11.3M
      CPU: 311ms
    CGroup: /system.slice/sendmail.service
            └─639 "sendmail: MTA: accepting connections"
```

Παραδειγμα αποστολης email :

```
echo "Just testing my sendmail gmail relay" | mail -s "Sendmail gmail Relay"
filippatos.nikolaos@ac.upatras.gr
```

Τελος προσθετουμε τις παρακατω γραμμες στο jail.local :

```
[DEFAULT]

desemail = filippatos.nikolaos@ac.upatras.gr
sender=nickdevelopingtester@gmail.com
sendername=root
mta = sendmail
action = %(action_mwl)s}
```

2. Χρήση Public Key Authentication

Στην εικονική μηχανή που τρέχει *debian* ενεργοποιείτε την *ssh* πρόσβαση μόνο με χρήση δημόσιου κλειδιού. Τα βήματα περιλαμβάνουν :

1. **την δημιουργία του κλειδιού (*ssh-keygen*) με τις σωστές παραμέτρους.**

```
ssh-keygen -t rsa -b 4096
```

Το αποθηκεύουμε στο αρχείο *laptop*

2. **την αντιγραφή του κλειδιού σε άλλο *server* (πχ το *host* υπολογιστή σας)**

Με την εντολή

```
ssh-copy-id -i laptop deby
```

Όπου *-i* είναι το flag για να κάνουμε specify ποια ταυτότητα θέλουμε να συνδεστούμε με το connection *deby* (*debian headless*) .

Τροποποιούμε και το *.ssh/config* αρχείο για να προτιμάει την σύνδεση με *publickey*

```
Host deby
    HostName 192.168.122.150
    User don
    PreferredAuthentications publickey
    IdentityFile ~/.ssh/laptop
```

Εναλλακτικός τρόπος ήταν να αντιγράψουμε το *laptop.pub* αρχείο με *scp* στο αρχείο *authorized_keys* του *vm* μας.

3. **τροποποίηση του αρχείου *sshd config* για πρόσβαση μόνο με το δημόσιο κλειδί.**

Στο φακέλο */etc/ssh/sshd_config.d* θα δημιουργήσουμε ένα αρχείο με τις παρακάτω ρυθμίσεις :

```
PasswordAuthentication no
```

4. **την επιτυχή δοκιμή σύνδεσης (χωρίς την χρήση συνθηματικού *password*).**

```
[figaro@oracle]--[~]
└─ $ssh deby
Linux debian 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov  2 21:36:09 2023 from 192.168.122.1
```

3. Υλοποιήσει νέων φίλτρων για χρήση στο πακέτο fail2ban

Το log αρχείο δύο εφαρμογών joomla και nextcloud είναι όπως παρακάτω:

```
> 2020-10-06T16:27:16+00:00 INFO 150.140.139.252 joomlafailure Username
and password do not match or you do not have an account yet.
> {"reqId":"VDEzZE0K2wITbT4fNrs1","level":2,"time":"2020-10-
26T16:04:26+02:00","remoteAddr":"150.140.139.252","user":"--","app":"no app in
Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών
context","method":"POST","url":"/nextcloud/index.php/login","message":"Login
failed: username (Remote IP: 150.140.139.143)","userAgent":"Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:82.0) Gecko/20100101
Firefox/82.0","version":"19.0.4.2"}
```

1. Υλοποιήστε το “regular expression” για δύο νέα φίλτρα στο fail2ban που να λαμβάνει υπόψιν του τα παραπάνω αρχείο καταγραφής. Μπορείτε να χρησιμοποιήσετε το site αυτό: <https://regex101.com/>

```
# Joomla
^.* INFO <HOST> joomlafailure .*$

# Next cloud
^{.*reqId.*nextcloud.*message.*Login failed.*Remote IP: <HOST>.*version.*}$
```

- ^ beginning of sentence
- .* any characters 0 to many times
- \$ end of sentence
- <HOST> for fail2ban

2. Με ποια εντολή μπορούμε να δοκιμάσουμε (dry run) τα παραπάνω φίλτρα χωρίς να τα ενεργοποιήσουμε?

```
fail2ban-regex file.log "regex code"
```

3. Φτιάξτε το αρχείο jail.local και ορίστε για τα παραπάνω φίλτρα τα: ports, protocols, iptable chain, findtime, bantime και retries.

Αποθηκεύουμε στον φακέλο filters.d/ με τα αντιστοιχα ονοματα

```
[ Definition ]
failregex = <regex code >
```

```
[joomla]
enabled=true
filter=joomla

port=http,https
protocol=all
chain=INPUT
findtime=10m
bantime=10m
maxretry=5
```



```
[nextcloud]
enabled=true
filter=joomla

port=http,https
protocol=all
chain=INPUT
findtime=10m
bantime=10m
maxretry=5
```

Και κανουμε για να δεχτει τις νεες αλλαγες

```
systemctl restart fail2ban.service
```