

Αναφορά Εργασίας 3: Προστασία Εξυπηρετητών με χρήση ssh και fail2ban

Γρηγόρης Καπαδούκας (ΑΜ: 1072484)

3 Νοεμβρίου 2022

1 Προστασία ανεπιθύμητων επιθέσεων με χρήση του πακέτου fail2ban


Αρχικά θα εγκαταστήσουμε το πακέτο fail2ban μέσω του package manager του debian11 headless machine μέσω της εξής εντολής

```
sudo apt install fail2ban -y
```

1.1

Αφού εγκαταστήσαμε το fail2ban μπορούμε πλέον να εκτελέσουμε τις εντολές "fail2ban-client status" και "fail2ban-client status sshd" όπως μας ζητείται. Παρακάτω φαίνεται το output αυτών:

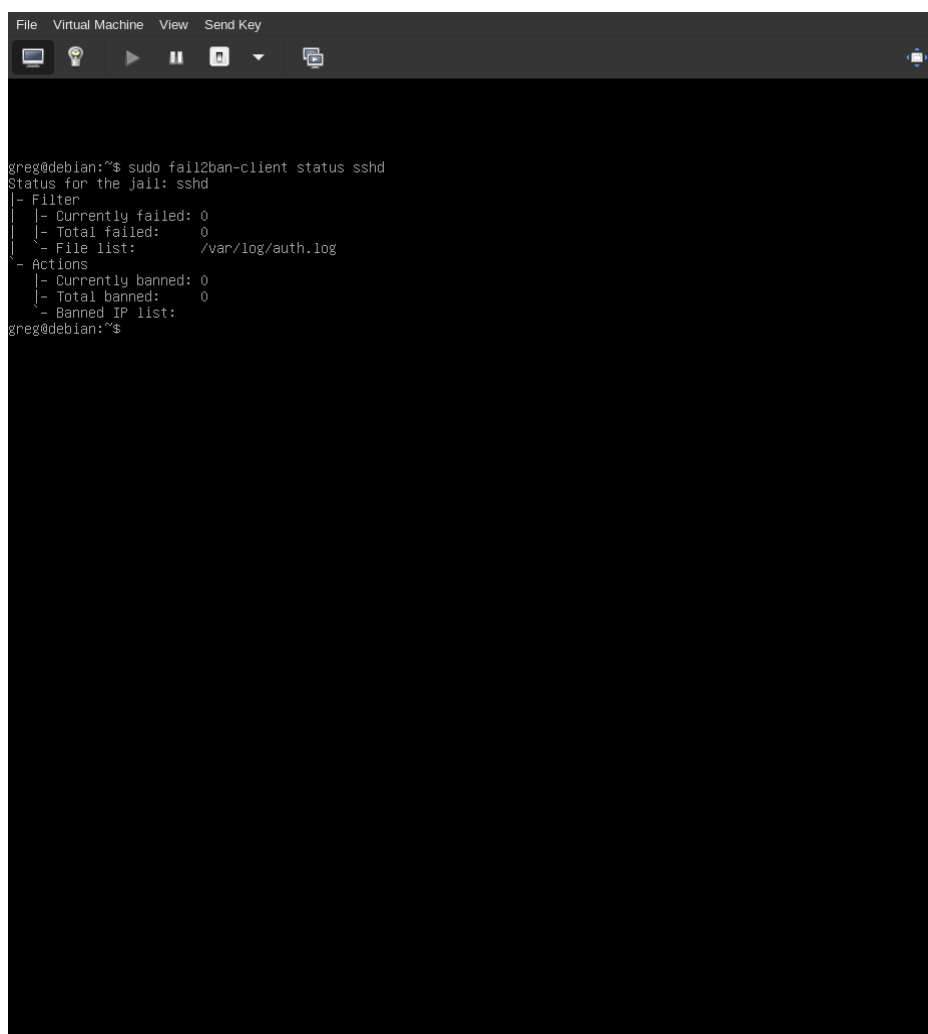
1. fail2ban-client status



The image shows a terminal window within a Virtual Machine. The window has a dark theme and a menu bar at the top with options: File, Virtual Machine, View, and Send Key. Below the menu bar is a toolbar with icons for running, pausing, and other VM controls. The terminal text is as follows:

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

2. fail2ban-client status sshd



```
File Virtual Machine View Send Key
greg@debian:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |-- Currently failed: 0
|  |-- Total failed: 0
|  |-- File list: /var/log/auth.log
|- Actions
|  |-- Currently banned: 0
|  |-- Total banned: 0
|  |-- Banned IP list:
greg@debian:~$
```

1.2

Αρχικά για να ρυθμίσουμε τον fail2ban θα εκτελέσουμε την εξής εντολή:

```
"sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Με αυτή την εντολή δημιουργούμε ένα configuration file το οποίο έχει προτεραιότητα επί του fail.conf και δεν θα γίνει overwritten από το package manager όταν γίνει upgrade στο fail2ban.

Έπειτα θα ανοίξουμε το αρχείο jail.local σε έναν editor και θα κάνουμε un-comment στην γραμμή 23 και 24 τα [sshd] και enabled = true. Με αυτόν

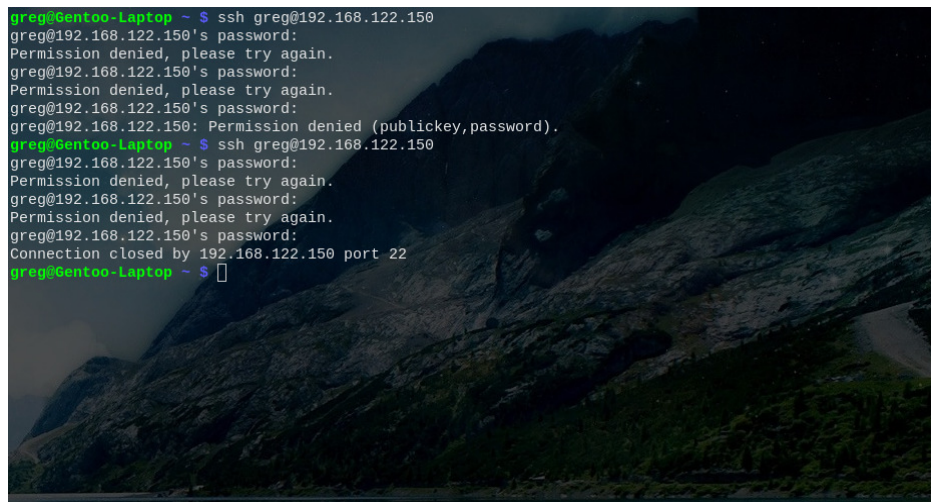
τον τρόπο ενεργοποιούμε το φίλτρο ssh ώστε να κάνουμε ban την σύνδεση στο ssh μετά από αριθμό προσπαθειών ίσο με την τιμή της μεταβλητής maxretry στη σειρά 108 (default τιμή είναι 5, όπως ζητάει η εκφώνηση) και το fail2ban θα βλέπει για αποτυχημένες προσπάθειες σε χρονικό περιθώριο ίσο με την τιμή της μεταβλητής findtime στη σειρά 103 (default τιμή είναι 10 λεπτά, όπως ζητάει η εκφώνηση). Τέλος επισημαίνουμε ότι το ban θα ισχύει για όσο χρόνο αναφέρει η μεταβλητή bantime στη σειρά 101 (default τιμή είναι 10 λεπτά).

Άρα με αυτόν τον τρόπο έχουμε πετύχει τον σκοπό μας. Παρακάτω δίνουμε ένα screenshot του configuration file με τα modifications από το default καθώς και screenshot 5 απετυχημένων προσπαθειών σύνδεσης με ssh που οδηγούν σε ban.

1. jail.local

```
File Virtual Machine View Send Key
1 #
2 # WARNING: heavily refactored in 0.9.0 release. Please review and
3 # customize settings for your setup.
4 #
5 # Changes: in most of the cases you should not modify this
6 # file, but provide customizations in jail.local file,
7 # or separate .conf files under jail.d/ directory, e.g.:
8 #
9 # HOW TO ACTIVATE JAILS:
10 #
11 # YOU SHOULD NOT MODIFY THIS FILE.
12 #
13 # It will probably be overwritten or improved in a distribution update.
14 #
15 # Provide customizations in a jail.local file or a jail.d/customisation.local.
16 # For example to change the default bantime for all jails and to enable the
17 # ssh-iptables jail the following (uncommented) would appear in the .local file.
18 # See man 5 jail.conf for details.
19 #
20 # [DEFAULT]
21 # bantime = 1h
22 #
23 [sshd]
24 enabled = true
25 #
26 # See jail.conf(5) man page for more information
27
28
29
30 # Comments: use '#' for comment lines and ';' (following a space) for inline comments
31
32
33 [INCLUDES]
34
35 #before = paths-distrow.conf
36 before = paths-debian.conf
37
38 # The DEFAULT allows a global definition of the options. They can be overridden
39 # in each jail afterwards.
40
41 [DEFAULT]
42
43 #
44 # MISCELLANEOUS OPTIONS
45 #
46
47 # "bantime.increment" allows to use database for searching of previously banned ip's to increase a
48 # default ban time using special formula, default it is banTime * 1, 2, 4, 8, 16, 32...
49 #bantime.increment = true
```

2. Ssh ban μετά από 5 αποτυχημένες προσπάθειες:

A terminal window with a dark background featuring a mountain landscape. The text in the terminal shows a series of failed SSH login attempts. The user 'greg' is trying to connect to '192.168.122.150'. The first attempt fails with 'Permission denied, please try again.' after entering a password. The second attempt also fails with the same message. The third attempt fails with 'Permission denied (publickey,password).' after entering a password. The fourth attempt fails with 'Permission denied, please try again.' after entering a password. The fifth attempt fails with 'Permission denied, please try again.' after entering a password. The sixth attempt fails with 'Permission denied, please try again.' after entering a password. The seventh attempt fails with 'Permission denied, please try again.' after entering a password. The eighth attempt fails with 'Permission denied, please try again.' after entering a password. The ninth attempt fails with 'Permission denied, please try again.' after entering a password. The tenth attempt fails with 'Permission denied, please try again.' after entering a password. The connection is closed by 192.168.122.150 port 22. The prompt returns to 'greg@Gentoo-Laptop ~ \$'.

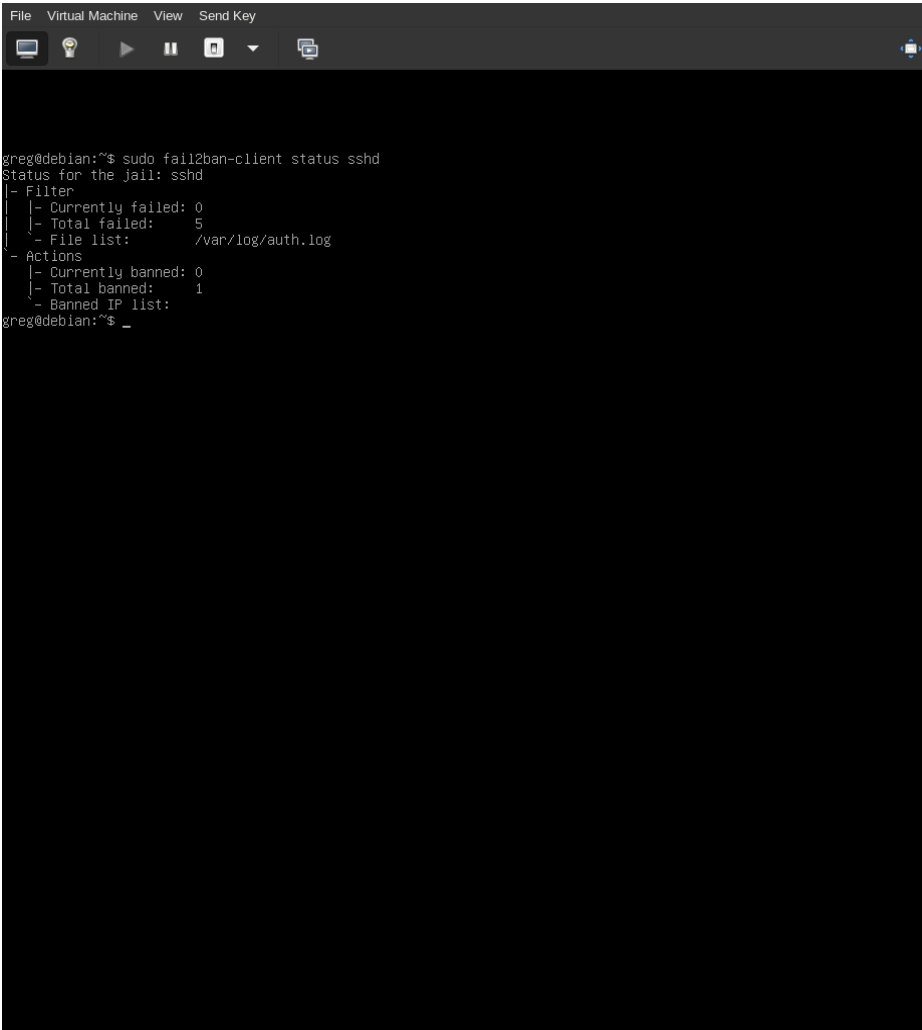
Σημειώνω εδώ ότι το background είναι διαφορετικό στο πάνω screenshot επειδή χρησιμοποιώ το τερματικό του host, ενώ προηγουμένως όλα τα screenshots ήταν από το virt-manager.

Εδώ παρατηρούμε ότι στην 6η προσπάθεια ο server δεν έδωσε error message αν το password είναι σωστό ή όχι, επειδή είχε ήδη κλείσει η σύνδεση, το οποίο ο host machine που χρησιμοποιήσαμε για να κάνουμε το testing το αντιλήφθηκε σύντομα μετά.

1.3

Έχοντας κάνει προηγουμένως 5 προσπάθειες με λάθος κωδικό για να φτιάξουμε το screenshot όπου δείχνουμε την επιτυχή λειτουργία του fail2ban banning στο ssh, παρακάτω θα δείξουμε μόνο screenshot με το αποτέλεσμα της εντολής "fail2ban-client status sshd".

- fail2ban-client status sshd



```
File Virtual Machine View Send Key
greg@debian:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
- Filter
|- Currently failed: 0
|- Total failed: 5
- File list: /var/log/auth.log
- Actions
|- Currently banned: 0
|- Total banned: 1
- Banned IP list:
greg@debian:~$ _
```

Ο λόγος που παραπάνω βλέπουμε ότι τα currently failed και currently banned πεδία είναι ίσα με 0, είναι επειδή έχουν περάσει πλέον τα 10 λεπτά από τη στιγμή που κάναμε τις 5 ανεπιτυχημένες προσπάθειες στο προηγούμενο ερώτημα μέχρι τότε που εκτελέσαμε την εντολή "fail2ban-client status sshd"

1.4

Καταρχάς όλες οι συνδεσεις του υπολογιστή καταγράφονται στο /var/log/syslog αρχείο, το οποίο είναι και το αρχείο που κάνει parse το fail2ban για να λειτουργήσει. Υποθέτω όμως ότι η εκφώνηση εννοεί για το /var/log/fail2ban.log αρχείο, στο οποίο καταγράφονται οι ανεπιτυχείς συνδέσεις και οι IP διευθύνσεις από όπου προήλθαν, καθώς και πότε το fail2ban κάνει ban ή unban

κάποια διεύθυνση. Παρακάτω συμπεριλαμβάνω screenshot το fail2ban.log αρχείου μου που δείχνουν τις ανεπιτυχείς συνδέσεις που έγιναν.

- fail2ban.log

```

File Virtual Machine View Send Key
[Icons: Desktop, Home, Play, Pause, Stop, Window, Search, Print]

2022-10-29 21:18:55,830 fail2ban.server [1152]: INFO -----
2022-10-29 21:18:55,830 fail2ban.server [1152]: INFO Starting Fail2ban v0.11.2
2022-10-29 21:18:55,831 fail2ban.observer [1152]: INFO Observer start...
2022-10-29 21:18:55,841 fail2ban.database [1152]: INFO Connected to fail2ban persistent database '/var/lib/
2022-10-29 21:18:55,842 fail2ban.database [1152]: WARNING New database created, Version '4'
2022-10-29 21:18:55,843 fail2ban.jail [1152]: INFO Creating new jail 'sshd'
2022-10-29 21:18:55,858 fail2ban.jail [1152]: INFO Jail 'sshd' uses pyinotify {}
2022-10-29 21:18:55,859 fail2ban.jail [1152]: INFO Initiated 'pyinotify' backend
2022-10-29 21:18:55,860 fail2ban.filter [1152]: INFO maxlines: 1
2022-10-29 21:18:55,875 fail2ban.filter [1152]: INFO maxRetry: 5
2022-10-29 21:18:55,875 fail2ban.filter [1152]: INFO findtime: 600
2022-10-29 21:18:55,875 fail2ban.actions [1152]: INFO banTime: 600
2022-10-29 21:18:55,875 fail2ban.filter [1152]: INFO encoding: UTF-8
2022-10-29 21:18:55,875 fail2ban.filter [1152]: INFO Added logfile: '/var/log/auth.log' (pos = 0, hash =
2022-10-29 21:18:55,879 fail2ban.jail [1152]: INFO Jail 'sshd' started
2022-10-30 00:04:33,579 fail2ban.filter [1152]: INFO [sshd] Found 192.168.122.1 - 2022-10-30 00:04:33
2022-10-30 00:04:38,391 fail2ban.filter [1152]: INFO [sshd] Found 192.168.122.1 - 2022-10-30 00:04:38
2022-10-30 00:04:41,096 fail2ban.filter [1152]: INFO [sshd] Found 192.168.122.1 - 2022-10-30 00:04:40
2022-10-30 00:04:46,318 fail2ban.filter [1152]: INFO [sshd] Found 192.168.122.1 - 2022-10-30 00:04:46
2022-10-30 00:04:49,347 fail2ban.filter [1152]: INFO [sshd] Found 192.168.122.1 - 2022-10-30 00:04:49
2022-10-30 00:04:49,856 fail2ban.actions [1152]: NOTICE [sshd] Ban 192.168.122.1
2022-10-30 00:14:49,196 fail2ban.actions [1152]: NOTICE [sshd] Unban 192.168.122.1
2022-10-30 00:30:18,075 fail2ban.filter [1152]: INFO [sshd] Found 192.168.122.1 - 2022-10-30 00:30:17
2022-10-30 01:35:05,896 fail2ban.filter [1152]: INFO [sshd] Found 192.168.122.1 - 2022-10-30 01:35:05

"fail2ban.log" 24L, 2415B

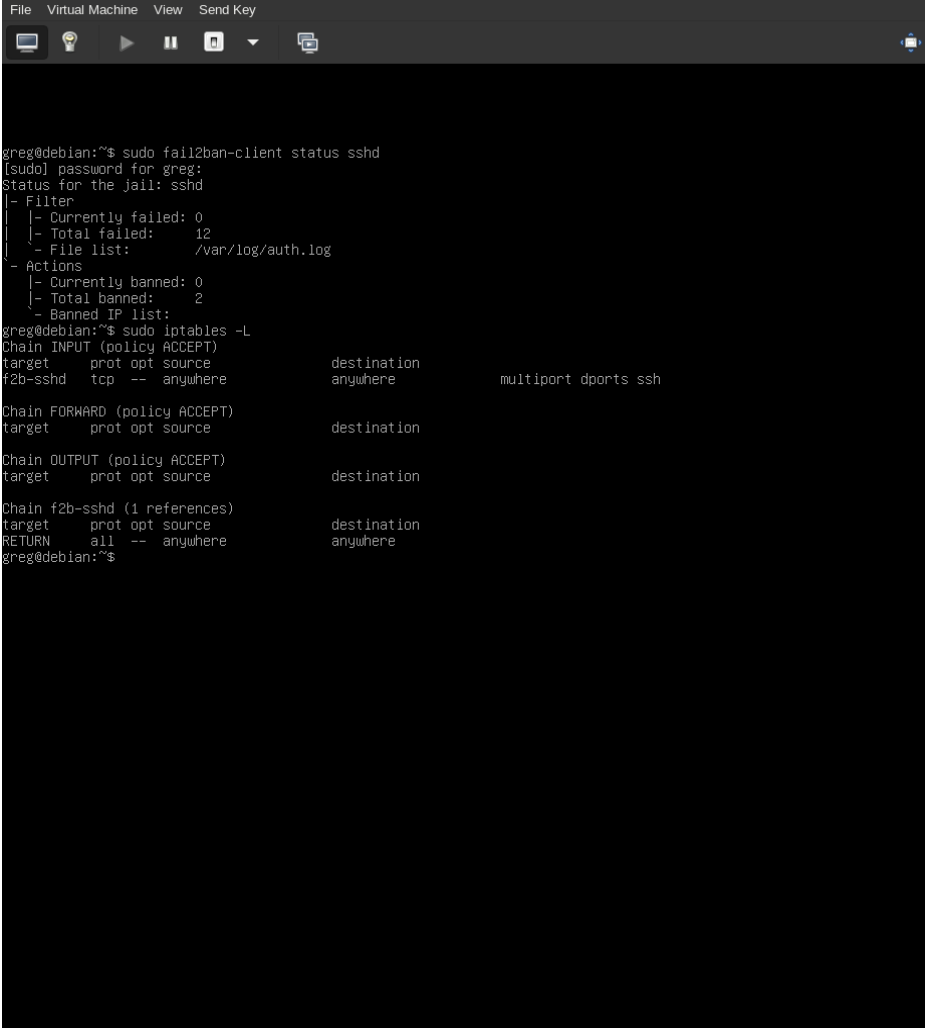
```

Εδώ παρατηρούμε τις αρχικές 5 ανεπιτυχείς συνδέσεις που οδήγησαν στο ban, και δέκα λεπτά μετά το unban που έγινε. Τέλος παρατηρούμε δύο ακόμα ανεπιτυχείς συνδέσεις που έγιναν αργότερα καταλάθος.

1.5

Παρακάτω δείχνουμε το output των της εντολής που μας ζητήθηκε και τους σχετικούς κανόνες του firewall όταν δεν υπάρχει κανένα ban:

- fail2ban-client status sshd και iptables -L χωρίς κανένα ban:



```
File Virtual Machine View Send Key
greg@debian:~$ sudo fail2ban-client status sshd
[sudo] password for greg:
Status for the jail: sshd
|- Filter
| - Currently failed: 0
| - Total failed: 12
| - File list: /var/log/auth.log
|- Actions
| - Currently banned: 0
| - Total banned: 2
| - Banned IP list:
greg@debian:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
f2b-sshd tcp -- anywhere anywhere multiport dports ssh

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
greg@debian:~$
```

Παρακάτω δείχνουμε το output των της εντολής που μας ζητήθηκε και τους σχετικούς κανόνες του firewall όταν υπάρχει ban:

- fail2ban-client status sshd και iptables -L με ban:

```
File Virtual Machine View Send Key
[Icons]

greg@debian:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |-- Currently failed: 0
|  |-- Total failed: 17
|  |-- File list: /var/log/auth.log
|- Actions
|  |-- Currently banned: 1
|  |-- Total banned: 3
|  |-- Banned IP list: 192.168.122.1
greg@debian:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
f2b-sshd tcp -- anywhere anywhere multiport dports ssh

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
greg@debian:~$
```

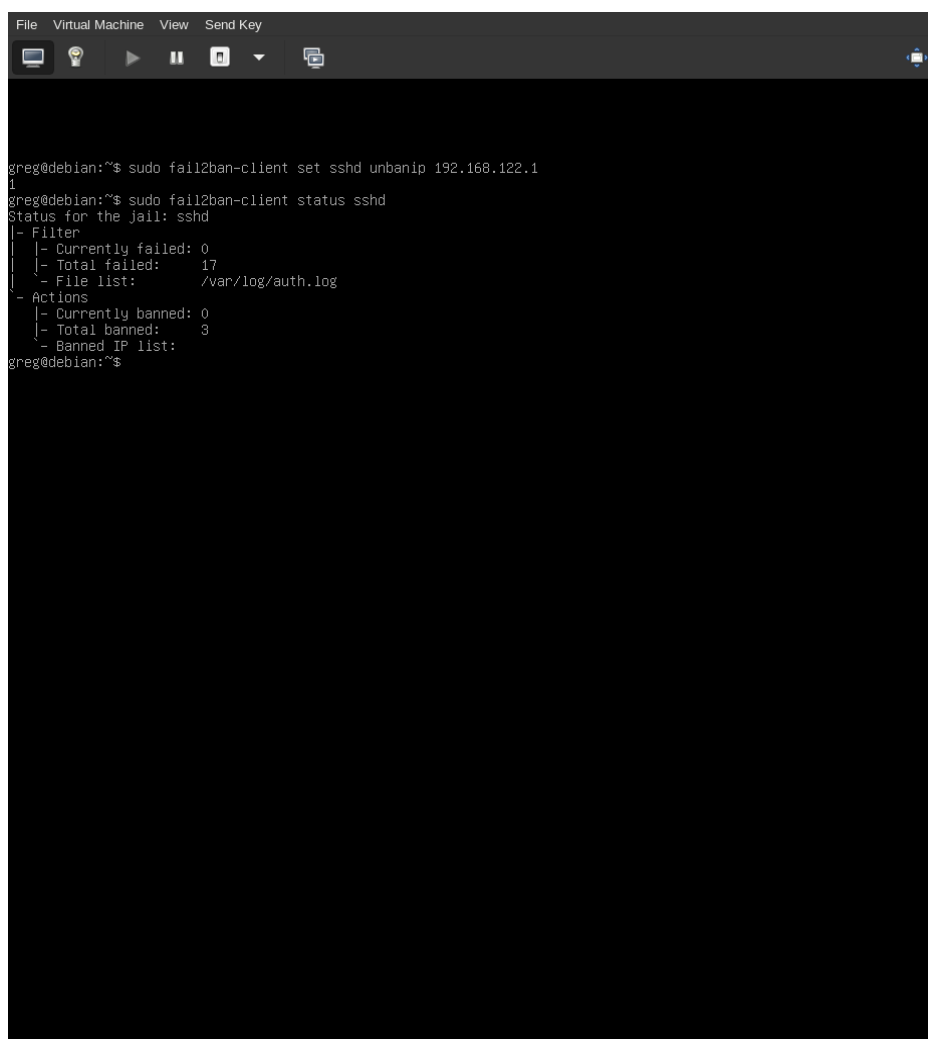
1.6

Για να κάνουμε unban μια IP εκτελούμε την εξής εντολή:

```
"fail2ban-client set <jail name> unbanip <IP address>
```

Σε αυτή τη περίπτωση για να κάνουμε unban την IP του host εκτελούμε την εντολή "fail2ban-client set sshd unbanip 192.168.122.1". Παρακάτω φαίνεται το output της εντολής αυτής σε συνδυασμό με το "fail2ban-client status sshd" για να δούμε ότι το unban έγινε με επιτυχία:

- fail2ban-client set sshd unbanip 192.168.122.1 και fail2ban-client status sshd:

A screenshot of a terminal window with a dark background. The window has a title bar with 'File', 'Virtual Machine', 'View', and 'Send Key' menus. Below the title bar are icons for a terminal, a lightbulb, a play button, a pause button, a stop button, a dropdown menu, and a copy icon. The terminal shows the following commands and output:

```
greg@debian:~$ sudo fail2ban-client set sshd unbanip 192.168.122.1
1
greg@debian:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed: 17
|  - File list: /var/log/auth.log
- Actions
  |- Currently banned: 0
  |- Total banned: 3
  - Banned IP list:
greg@debian:~$
```

1.7

Μπορούμε να προσθέσουμε τις IP διευθύνσεις που δεν επιθυμούμε να φιλτράρονται στο `jail.local` αρχείο στη μεταβλητή `ignoreip` στη γραμμή 92 (όπως είναι το default configuration file). Παρακάτω δείχνω screenshot όπου έχω απενεργοποιήσει το φιλτράρισμα για το virtual LAN που δημιουργεί το KVM στον υπολογιστή μου:

- Απενεργοποίηση φιλτραρίσματος - `ignoreip` μεταβλητή:

```
File Virtual Machine View Send Key
68 #bantime.formula = ban.Time * math.exp(float(ban.Count+1)*banFactor)/math.exp(1*banFactor)
69
70 # "bantime.multipliers" used to calculate next value of ban time instead of formula, corresponding
71 # previously ban count and given "bantime.factor" (for multipliers default is 1):
72 # following example grows ban time by 1, 2, 4, 8, 16 ... and if last ban count greater as multipliers count,
73 # always used last multiplier (64 in example), for factor '1' and original ban time 600 - 10.6 hours
74 #bantime.multipliers = 1 2 4 8 16 32 64
75 # following example can be used for small initial ban time (bantime=60) - it grows more aggressive at begin,
76 # for bantime=60 the multipliers are minutes and equal: 1 min, 5 min, 30 min, 1 hour, 5 hour, 12 hour, 1 day, 2
77 #bantime.multipliers = 1 5 30 60 300 720 1440 2880
78
79 # "bantime.overalljails" (if true) specifies the search of IP in the database will be executed
80 # cross over all jails, if false (default), only current jail of the ban IP will be searched
81 #bantime.overalljails = false
82
83 # -----
84
85 # "ignoreself" specifies whether the local resp. own IP addresses should be ignored
86 # (default is true). Fail2ban will not ban a host which matches such addresses.
87 #ignoreself = true
88
89 # "ignoreip" can be a list of IP addresses, CIDR masks or DNS hosts. Fail2ban
90 # will not ban a host which matches an address in this list. Several addresses
91 # can be defined using space (and/or comma) separator.
92 ignoreip = 127.0.0.1/8 ::1 192.168.122.0/24
93
94 # External command that will take an tagged arguments to ignore, e.g. <ip>,
95 # and return true if the IP is to be ignored. False otherwise.
96 #
97 # ignorecommand = /path/to/command <ip>
98 ignorecommand =
99
100 # "bantime" is the number of seconds that a host is banned.
101 bantime = 10m
102
103 # A host is banned if it has generated "maxretry" during the last "findtime"
104 # seconds.
105 findtime = 10m
106
107 # "maxretry" is the number of failures before a host get banned.
108 maxretry = 5
109
110 # "maxmatches" is the number of matches stored in ticket (resolvable via tag <matches> in actions).
111 maxmatches = %(maxretry)s
112
113 # "backend" specifies the backend used to get files modification.
114 # Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
115 # This option can be overridden in each jail as well.
116 #
117 :
```

1.8

Αρχικά θα κάνουμε configure το fail2ban μέσω του jail.local, όπως φαίνεται παρακάτω:

- jail.local για email sending:

```
File Virtual Machine View Send Key
164 # "filter" defines the filter to use by the jail.
165 # By default jails have names matching their filter name
166 #
167 filter = %(__name__)s(mode=%(mode)s)
168
169 #
170 #
171 # ACTIONS
172 #
173
174 # Some options used for actions
175
176 # Destination email address used solely for the interpolations in
177 # jail.{conf,local,d/*} configuration files.
178 destemail = up1072484@upnet.gr
179
180 # Sender email address used solely for some actions
181 sender = gregkap12@gmail.com
182 sendername = Fail2ban on Debian11
183
184 # E-mail action. Since 0.8.1 Fail2Ban uses sendmail MTA for the
185 # mailing. Change mta configuration parameter to mail if you want to
186 # revert to conventional 'mail'.
187 mta = sendmail
188 action = %(action_mwl)s
189
190 # Default protocol
191 protocol = tcp
192
193 # Specify chain where jumps would need to be added in ban-actions expecting parameter chain
194 chain = <known/chain>
195
196 # Ports to be banned
197 # Usually should be overridden in a particular jail
198 port = 0:65535
199
200 # Format of user-agent https://tools.ietf.org/html/rfc7231#section-5.5.3
201 fail2ban_agent = Fail2Ban/%(fail2ban_version)s
202
203 #
204 # Action shortcuts. To be used to define action parameter
205
206 # Default banning action (e.g. iptables, iptables-new,
207 # iptables-multiport, shorewall, etc) It is used to define
208 # action_* variables. Can be overridden globally or per
209 # section within jail.local file
210 banaction = iptables-multiport
211 banaction_allports = iptables-allports
212
213 :set number
```

Οι αλλαγές που έχουν γίνει σε σύγκριση με το αρχικό configuration file είναι αρχικά να ρυθμίσουμε το destmail στη γραμμή 170, το οποίο είναι το email address παραλήπτης. Επίσης αλλάζουμε το sender στη γραμμή 181 το οποίο είναι το email address αποστολέας, καθώς και το sendername στη γραμμή 182 το οποίο είναι το όνομα που θα έχει το email σαν αποστολέα. Τέλος ελέγχουμε ότι το mta στη γραμμή 187 είναι ίσο με sendmail, που είναι η default λειτουργία και ότι το action στη γραμμή 188 είναι ίσο με %(action_mwl)s (το action κανονικά είναι στη σειρά 269 αλλά το μετακίνησα στην 188). Το sendmail είναι το email relay utility που χρησιμοποιείται για να σταλθούν τα mail και το %(action_mwl)s δηλώνει να σταλθούν οι πιθανές επιθέσεις μαζί με τα logs (χωρίς το l δεν στέλνονται τα logs).

Έπειτα πρέπει να κάνουμε configure το sendmail. Για να το κάνουμε αυτό αρχικά θα κάνουμε configure το authentication του Gmail λογαριασμού που θα χρησιμοποιήσουμε, εκτελώντας τις εξής εντολές σε elevated shell:

1. `"apt install sendmail mailutils sendmail-bin -y"`
2. `"mkdir -m 700 /etc/mail/authinfo/"`
3. `"cd /etc/mail/authinfo/"`
4. `"vim gmail-auth"` όπου στο περιεχόμενο του αρχείου βάζουμε το εξής:
"AuthInfo: "U:root" "I:gregkap12@gmail.com" "P:Ένα App password που έφτιαξα""
5. `"makemap hash gmail-auth < gmail-auth"`
6. `"rm gmail-auth"`

Έπειτα θα κάνουμε configure το sendmail με τις εξής εντολές:

1. `"vim /etc/mail/sendmail.mc"` όπου στο τέλος στη γραμμή 101 θα προσθέσουμε από κάτω τις γραμμές 102 έως 108 όπως φαίνεται στο παρακάτω screenshot:

```

59 DAEMON_OPTIONS( Family=inet, Name=MSP-v4, Port=submission, M-Ea, Addr=127.0.0.1')dnl
60 dnl #
61 dnl # Be somewhat anal in what we allow
62 define( confPRIVACY_FLAGS, dnl
63 'needmailhelo, needdsnhehlo, needvfyhelo, restrictgrub, restrictexpand, nobodyreturn, authwarnings')dnl
64 dnl #
65 dnl # Define connection throttling and window length
66 define( confCONNECTION_RATE_THROTTLE, 15)dnl
67 define( confCONNECTION_RATE_WINDOW_SIZE, 100)dnl
68 dnl #
69 dnl # Features
70 dnl #
71 dnl # use /etc/mail/local-host-names
72 FEATURE( 'use_cw_file')dnl
73 dnl #
74 dnl # The access db is the basis for most of sendmail's checking
75 FEATURE( 'access_db', , 'skip')dnl
76 dnl #
77 dnl # The greet_pause feature stops some automail bots - but check the
78 dnl # provided access db for details on excluding localhosts...
79 FEATURE( 'greet_pause', 1000)dnl 1 seconds
80 dnl #
81 dnl # Delay_checks allows sender->recipient checking
82 FEATURE( 'delay_checks', 'friend', 'n')dnl
83 dnl #
84 dnl # If we get too many bad recipients, slow things down...
85 define( confBAD_RCPT_THROTTLE, 3!)dnl
86 dnl #
87 dnl # Stop connections that overflow our concurrent and time connection rates
88 FEATURE( 'conncontrol', 'nodelay', 'terminate')dnl
89 FEATURE( 'ratecontrol', 'nodelay', 'terminate')dnl
90 dnl #
91 dnl # If you're on a dialup link, you should enable this - so sendmail
92 dnl # will not bring up the link (it will queue mail for later)
93 dnl define( confCON_EXPENSIVE, 'True')dnl
94 dnl #
95 dnl # Dialup/LAN connection overrides
96 dnl #
97 include( '/etc/mail/m4/dialup.m4')dnl
98 include( '/etc/mail/m4/provider.m4')dnl
99 dnl #
100 dnl # Default Mailer setup
101 MAILER_DEFINITIONS
102 define( 'SMART_HOST', '[smtp.gmail.com]')dnl
103 define( 'RELAY_MAILER_ARGS', 'TCP $h 587')dnl
104 define( 'ESMTP_MAILER_ARGS', 'TCP $h 587')dnl
105 define( 'confAUTH_OPTIONS', 'A p')dnl
106 TRUST_AUTH_MECH( 'EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
107 define( 'confAUTH_MECHANISMS', 'EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
108 FEATURE( 'authinfo', 'hash -o /etc/mail/authinfo/gmail-auth.db')dnl
109 MAILER( 'local')dnl
110 MAILER( 'smtp')dnl
111
~
~
"/etc/mail/sendmail.mc" 111L, 4442B written
108,65 Bot

```

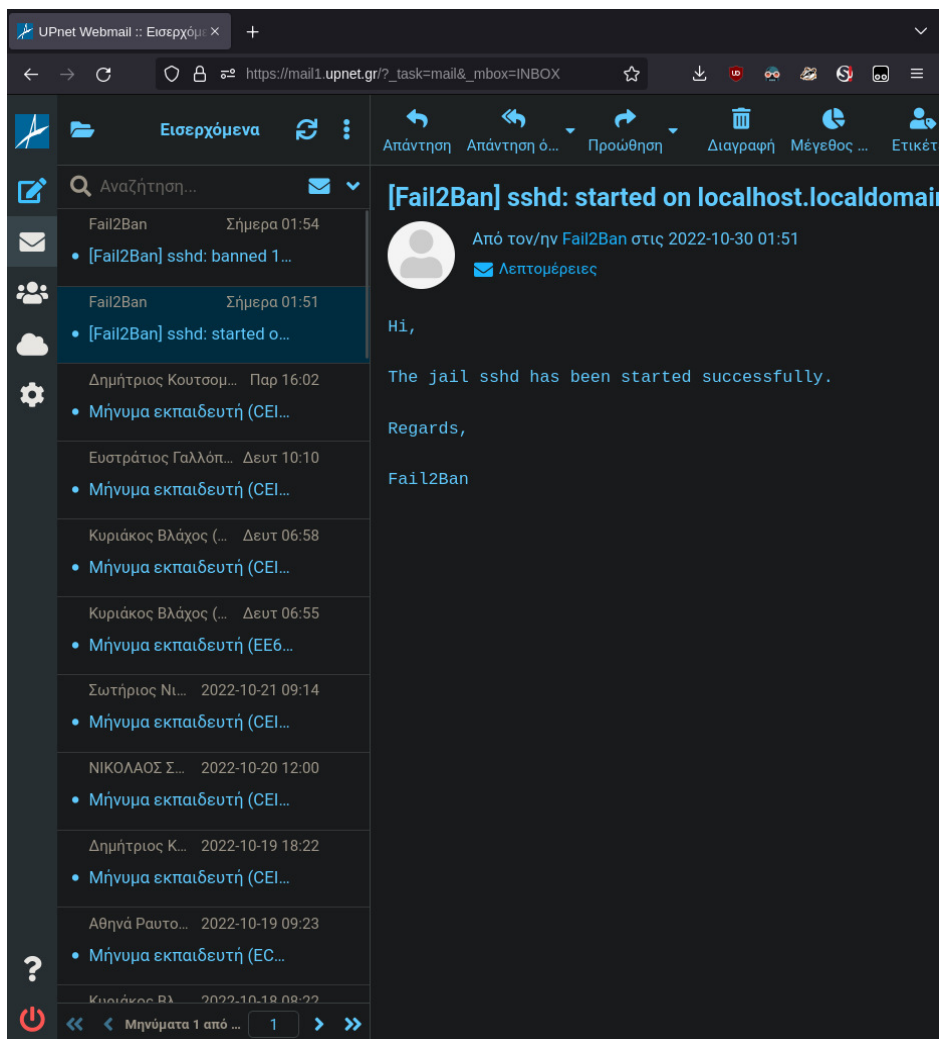
2. "make -C /etc/mail"
3. "systemctl restart sendmail"
4. "systemctl status sendmail" όπου παρατηρούμε ότι το sendmail τρέχει χωρίς κανένα error"

Τώρα το configuration πρέπει να είναι έτοιμο! Για να δοκιμάσουμε το email sending functionality του fail2ban κάνουμε τα εξής:

1. Εκτελούμε την εντολή: "systemctl restart fail2ban"
2. Εκτελούμε την εντολή: "systemctl status fail2ban" και βλέπουμε ότι έχει error, επειδή το default domain name debian δεν είναι fully

qualified domain name, όπως αυτό απαιτεί. Αυτό το διορθώνουμε φτιάχνοντας ένα fully qualified domain name μέσω το duckdns.org και αλλάζοντας το hostname στο debian box και το /etc/hosts file του, αλλά δεν θα μπω σε λεπτομέρεια εφ' όσον δεν είναι ο σκοπός της άσκησης.

3. Βλέπουμε το εξής email στο inbox:



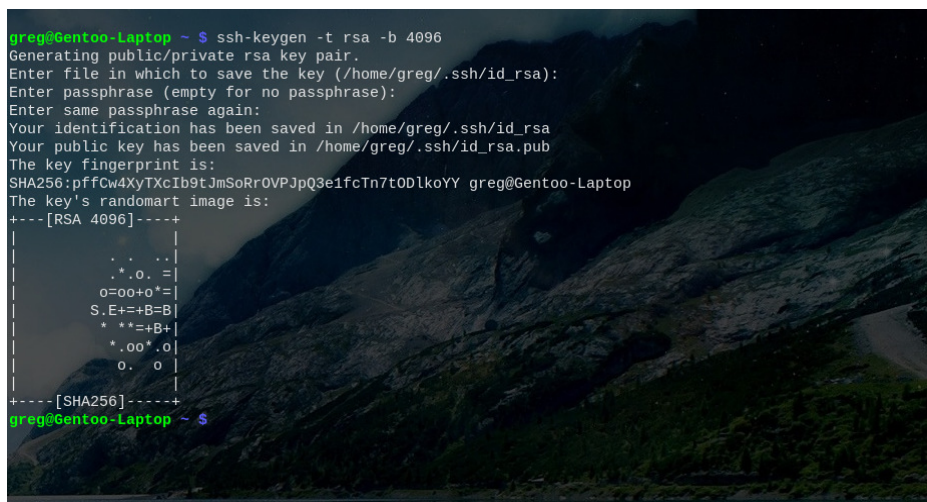
Άρα συμπεραίνουμε ότι το fail2ban σε συνδυασμό με το sendmail λειτουργούν σωστά.

2 Χρήση Public Key Authentication

2.1

Υποθέτουμε πως με τις σωστές παραμέτρους εννοείται να δημιουργήσουμε κλειδί μέσω του ssh-keygen που να είναι τύπου RSA, με μέγεθος 4096. Για να επιτευχθεί αυτό θα εκτελέσουμε την εντολή που φαίνεται στο παρακάτω screenshot:

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

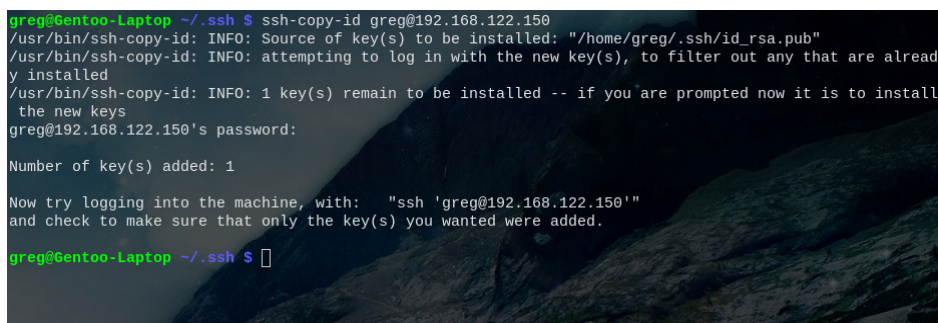


```
greg@Gentoo-Laptop ~ $ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/greg/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/greg/.ssh/id_rsa
Your public key has been saved in /home/greg/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:pffCw4XyTXcIb9tJmSoRr0VPJpQ3e1fcTn7t0DlkoYY greg@Gentoo-Laptop
The key's randomart image is:
+---[RSA 4096]---+
|
|. . .
|. . o. =|
|o=oo+o*=|
|S.E+=B=B|
|* **+=B+|
|*.oo*.o|
|o. o|
+---[SHA256]-----+
greg@Gentoo-Laptop ~ $
```

2.2

Για να μεταφέρουμε το public κλειδί από τον host στον debian server, ώστε να μπορεί αργότερα να γίνει σύνδεση του host στον debian machine χωρίς χρήση συνθηματικού θα χρησιμοποιήσουμε το utility ssh-copy-id, όπως φαίνεται στο screenshot παρακάτω:

- `ssh-copy-id greg@192.168.122.150`



```
greg@Gentoo-Laptop ~/.ssh $ ssh-copy-id greg@192.168.122.150
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/greg/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
greg@192.168.122.150's password:

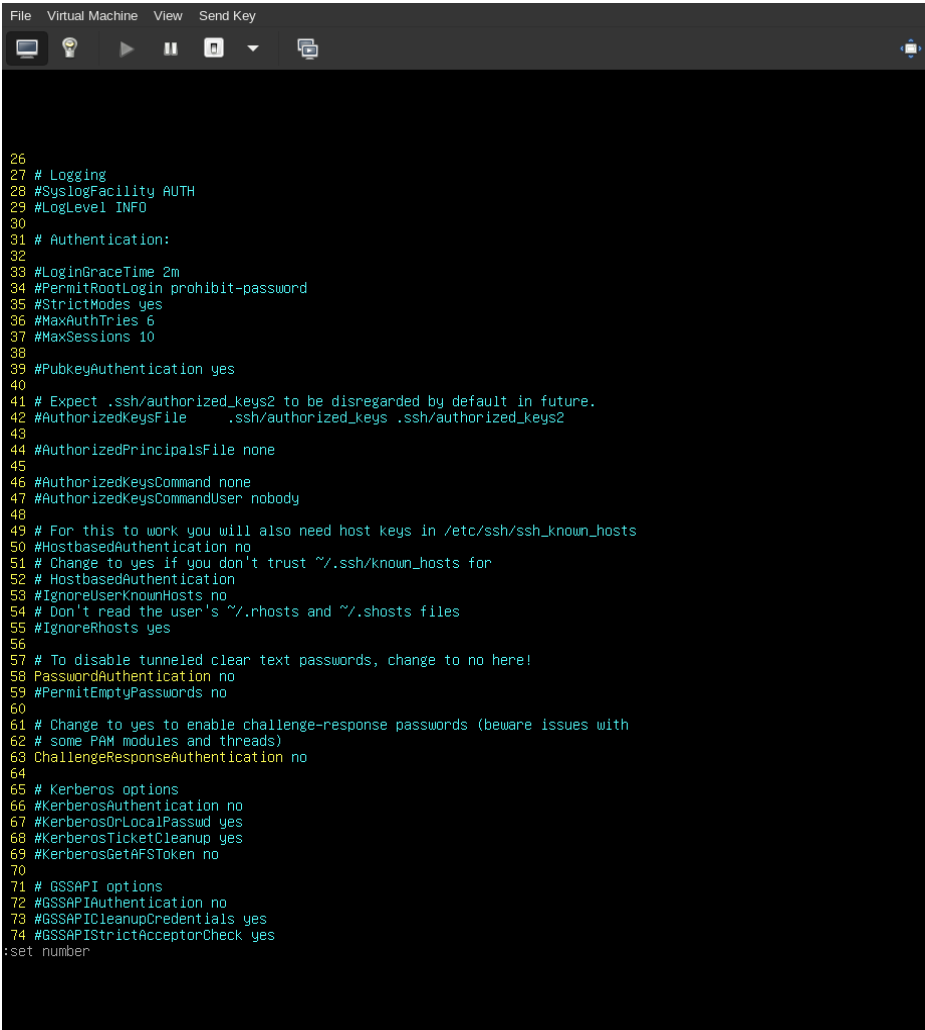
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'greg@192.168.122.150'"
and check to make sure that only the key(s) you wanted were added.
greg@Gentoo-Laptop ~/.ssh $
```

2.3

Για να απενεργοποιήσουμε τον πρόσβαση με χρήση συνθηματικού θα εκτελέσουμε την εντολή "sudo vim /etc/ssh/sshd_config" για να τροποποιήσουμε το αρχείο ώστε στη γραμμή 58 να κάνουμε uncomment το PasswordAuthentication και να το αλλάξουμε από yes σε no, όπως φαίνεται στο screenshot παρακάτω:

- sshd_config



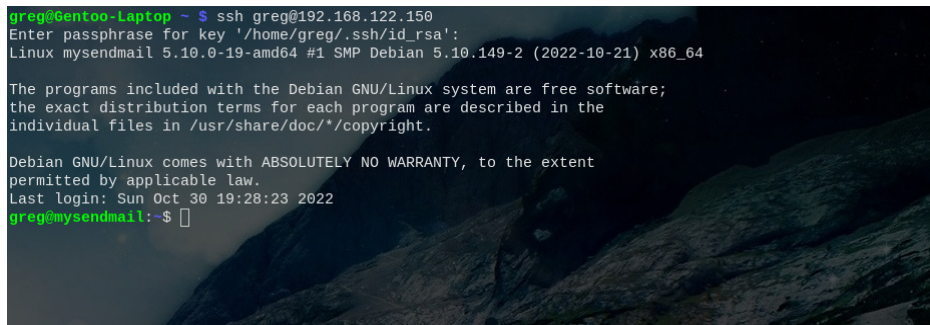
```
26
27 # Logging
28 #SyslogFacility AUTH
29 #LogLevel INFO
30
31 # Authentication:
32
33 #LoginGraceTime 2m
34 #PermitRootLogin prohibit-password
35 #StrictModes yes
36 #MaxAuthTries 6
37 #MaxSessions 10
38
39 #PubkeyAuthentication yes
40
41 # Expect .ssh/authorized_keys2 to be disregarded by default in future.
42 #AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
43
44 #AuthorizedPrincipalsFile none
45
46 #AuthorizedKeysCommand none
47 #AuthorizedKeysCommandUser nobody
48
49 # For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
50 #HostbasedAuthentication no
51 # Change to yes if you don't trust ~/.ssh/known_hosts for
52 # HostbasedAuthentication
53 #IgnoreUserKnownHosts no
54 # Don't read the user's ~/.rhosts and ~/.shosts files
55 #IgnoreRhosts yes
56
57 # To disable tunneled clear text passwords, change to no here!
58 PasswordAuthentication no
59 #PermitEmptyPasswords no
60
61 # Change to yes to enable challenge-response passwords (beware issues with
62 # some PAM modules and threads)
63 ChallengeResponseAuthentication no
64
65 # Kerberos options
66 #KerberosAuthentication no
67 #KerberosOrLocalPasswd yes
68 #KerberosTicketCleanup yes
69 #KerberosGetAFSToken no
70
71 # GSSAPI options
72 #GSSAPIAuthentication no
73 #GSSAPICleanupCredentials yes
74 #GSSAPIStrictAcceptorCheck yes
:set number
```

Τώρα εκτελούμε την εντολή "sudo systemctl restart sshd" για να κάνουμε restart το sshd και να σιγουρευτούμε ότι πέρασαν οι αλλαγές.

2.4

Πλέον μένει μόνο να εκτελέσουμε την εντολή "ssh greg@192.168.122.150" από τον host υπολογιστή για να δούμε ότι ήταν επιτυχής η σύνδεση με χρήση του RSA κλειδιού. Το output της εντολής φαίνεται παρακάτω:

- ssh greg@192.168.122.150



```
greg@gentoo-Laptop ~ $ ssh greg@192.168.122.150
Enter passphrase for key '/home/greg/.ssh/id_rsa':
Linux mysendmail 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) 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: Sun Oct 30 19:28:23 2022
greg@mysendmail:~$
```

Παρατηρούμε πως το μόνο συνθηματικό που ζητήθηκε είναι το συνθηματικό του κλειδιού και όχι συνθηματικό για τον χρήστη greg, άρα το configuration είναι σωστό. Αν επιθυμούσα θα μπορούσα να είχα δημιουργήσει το κλειδί χωρίς συνθηματικό, οπότε δεν θα μου ζητούσε καθόλου συνθηματικό η σύνδεση πλέον.

3 Υλοποίηση νέων φίλτρων για χρήση στο πακέτο fail2ban

3.1

Στη περίπτωση του joomla, για να ταυτοποιήσουμε κάθε log που προέκυψε από λάθος password κατά το authentication, αρκεί το regular expression να ταιριάζει το "INFO", να αντιληφθεί η IP και μετά το "joomlafailure Username and password do not match or you do not have an account yet." Άρα το regular expression που προκύπτει είναι το εξής:

- `^.*INFO <HOST>.*joomlafailure.*Username and password do not match or you do not have an account yet\.$`

Αυτό το regular expression με το ^ δηλώνει ότι αρχίζουμε από την αρχή του string. Επισημαίνουμε επίσης πως το fail2ban αυτόματα καταλαβαίνει και αφαιρεί την ημερομηνία από το log στο τελικό string στο οποίο εφαρμόζεται

το regex. Έπειτα με το . εννοείται οποιοσδήποτε χαρακτήρας εκτός το new line και * σημαίνει 0 ή περισσότερες φορές. Άρα με το .* εννοούμε πως οτιδήποτε κάνει match, μέχρι να φτάσουμε στο επόμενο μέρος του κανόνα, το joomlafailure. Άρα εκεί κάνουμε match έναν έναν τους χαρακτήρες. Τέλος έχουμε ξανά .* και το τελικό substring που χρειάζεται να αναγνωρίσουμε από το log, το 'Username and password do not match or you do not have an account yet\.' Τέλος με το \$ αναγνωρίζεται το τέλος του string και με το <HOST> αναγνωρίζεται η IP διεύθυνση που χειρίζεται το fail2ban όταν αποφασίζει αν θα την κάνει ban ή όχι.

Στην περίπτωση του nextcloud ήταν αδύνατο να καταλάβω ποιά κομμάτια του log είναι πάντα παρούσα στη περίπτωση λανθασμένου κωδικού, αλλά αναζητώντας στο διαδίκτυο κατέληξα στο εξής. Για να σιγουρευτούμε ότι ένα log προέκυψε από failed user authentication, αρκεί το log να έχει αναγνωρίσουμε τα "Login failed: " ... "(Remote IP: <IP διεύθυνση>)" στο log ή εναλλακτικά να αναγνωρισθεί ""remoteAddr":<IP διεύθυνση>" ... "Trusted domain error.". Οπότε το regular expression στο οποίο κατέληξα είναι το εξής:

- `^.*Login failed: '?.*'? \ (Remote IP: '?<HOST>'?\).*$ ||
^.*\ "remoteAddr":\ ".*<HOST>\ ".*Trusted domain error.*$`

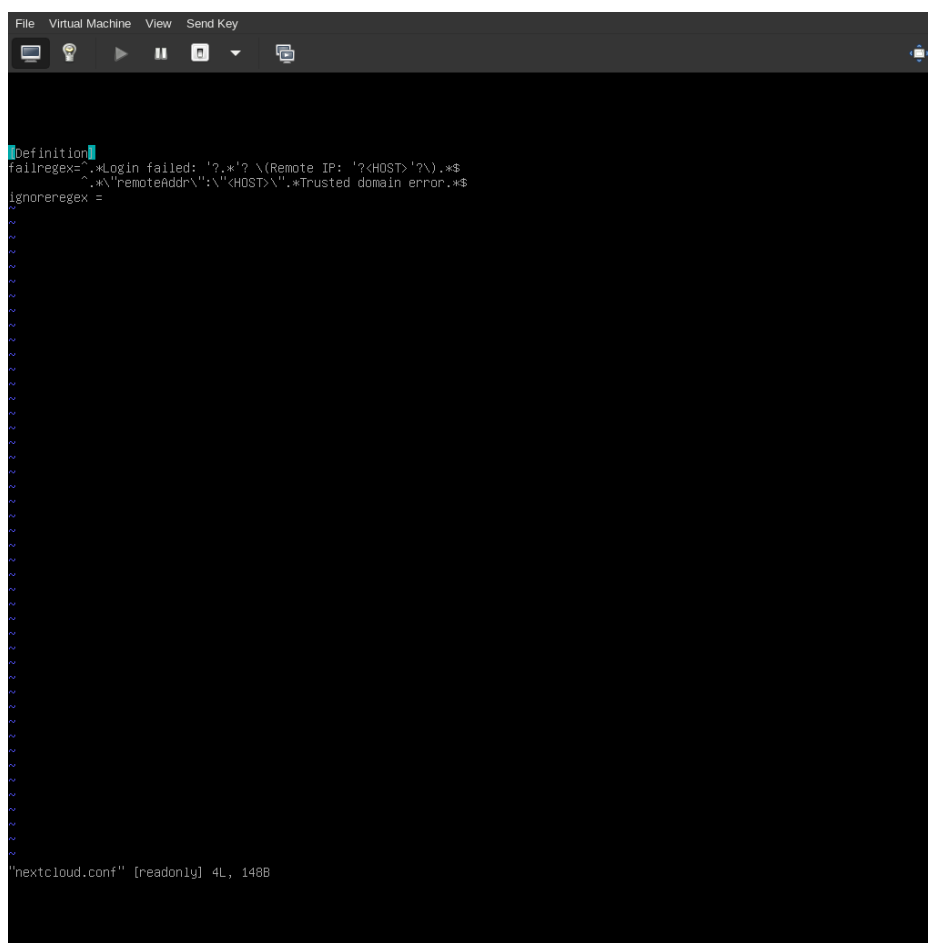
Συμπληρώνοντας στα προηγούμενα, το ? σημαίνει ότι το προηγούμενο σύμβολο είτε δεν υπάρχει είτε εμφανίζεται μια φορά. Επίσης το || δηλώνει ότι μπορεί να ισχύει το regex στη πρώτη γραμμή ή το regex στη δεύτερη.

3.2

Μπορούμε να δοκιμάσουμε τα φίλτρα μέσω της χρήσης του fail2ban-regex utility. Η σύνταξη της εντολής είναι "fail2ban-regex <log string ή log αρχείο> <regex ή filter configuration αρχείο>". Εγώ προτίμησα να χρησιμοποιήσω τα log αρχεία και filter configuration αρχείο, επειδή κατά τη δημιουργία του regex δεν ήθελα να κάνω πολλές φορές copy και paste στο τερματικό, καθώς και τα filter configuration αρχεία θα χρειαστούν για το ερώτημα 3 (και ας μην τα ζητάει).

Άρα αρχικά έβαλα το δοθέν log του joomla σε ένα αρχείο example_joomla.log και το log του nextcloud σε ένα άλλο αρχείο example_nextcloud.log. Επίσης έφτιαξα στον φάκελο /etc/fail2ban/filter.d/ δύο νέα αρχεία, τα joomla.conf και nextcloud.conf, που έχουν την εξής δομή:

- /etc/fail2ban/filter.d/joomla.conf



The screenshot shows a terminal window within a virtual machine. The window has a menu bar with 'File', 'Virtual Machine', 'View', and 'Send Key'. Below the menu bar is a toolbar with icons for running, pausing, and other VM controls. The terminal content shows the configuration of fail2ban. It starts with a comment '#definition', followed by 'failregex=' and two regex patterns for login failures. Then 'ignoreregex =' is shown. The terminal is mostly black with some blue and white text. At the bottom, it says 'nextcloud.conf' [readonly] 4L, 148B.

```
#definition
failregex='.*Login failed: '?.*'? \(Remote IP: '?<HOST>'?\).*$
.*\''remoteAddr\':"'\<HOST>'\'".*Trusted domain error.*$
ignoreregex =

'nextcloud.conf' [readonly] 4L, 148B
```

Έπειτα θα εκτελέσουμε την εντολή `fail2ban-regex` και θα δούμε τα αποτελέσματα, τα οποία φαίνονται παρακάτω:

- `fail2ban-regex /home/greg/example_joomla.log /etc/fail2ban/filter.d/joomla.conf`

```
File Virtual Machine View Send Key
Running tests
=====
Use failregex filter file : joomla, basedir: /etc/fail2ban
Use log file : /home/greg/example_joomla.log
Use encoding : UTF-8

Results
=====
Failregex: 1 total
|- #) [# of hits] regular expression
| 1) [1] ^.*INFO <HOST>.*joomlafailure.*Username and password do not match or you do not have an account yet\.$
|-

Ignoreregex: 0 total

Date template hits:
Lines: 1 lines, 0 ignored, 1 matched, 0 missed
[processed in 0.02 sec]
greg@mysendmail:~$
```

- fail2ban-regex /home/greg/example_nextcloud.log /etc/fail2ban/filter.d/nextcloud.conf

```
File Virtual Machine View Send Key
Running tests
=====
Use failregex filter file : nextcloud, basedir: /etc/fail2ban
Use log file : /home/greg/example_nextcloud.log
Use encoding : UTF-8

Results
=====
Failregex: 1 total
|- [# of hits] regular expression
|_ 1) [1] ^.*Login failed: '?.*'? \(\Remote IP: '?<HOST>'?\).*$
-

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
|_ 1) ExYear(?P<_sep>[-/.])Month(?P=_sep)Day(?:T| ?)24hour:Minute:Second(?:[.,]Microseconds)?(?:\s*Zone offset)?
-

Lines: 1 lines, 0 ignored, 1 matched, 0 missed
(processed in 0.02 sec)
greg@mysendmail:~$ _
```

Άρα τα regular expressions του ερωτήματος 1 είναι σωστά.

3.3

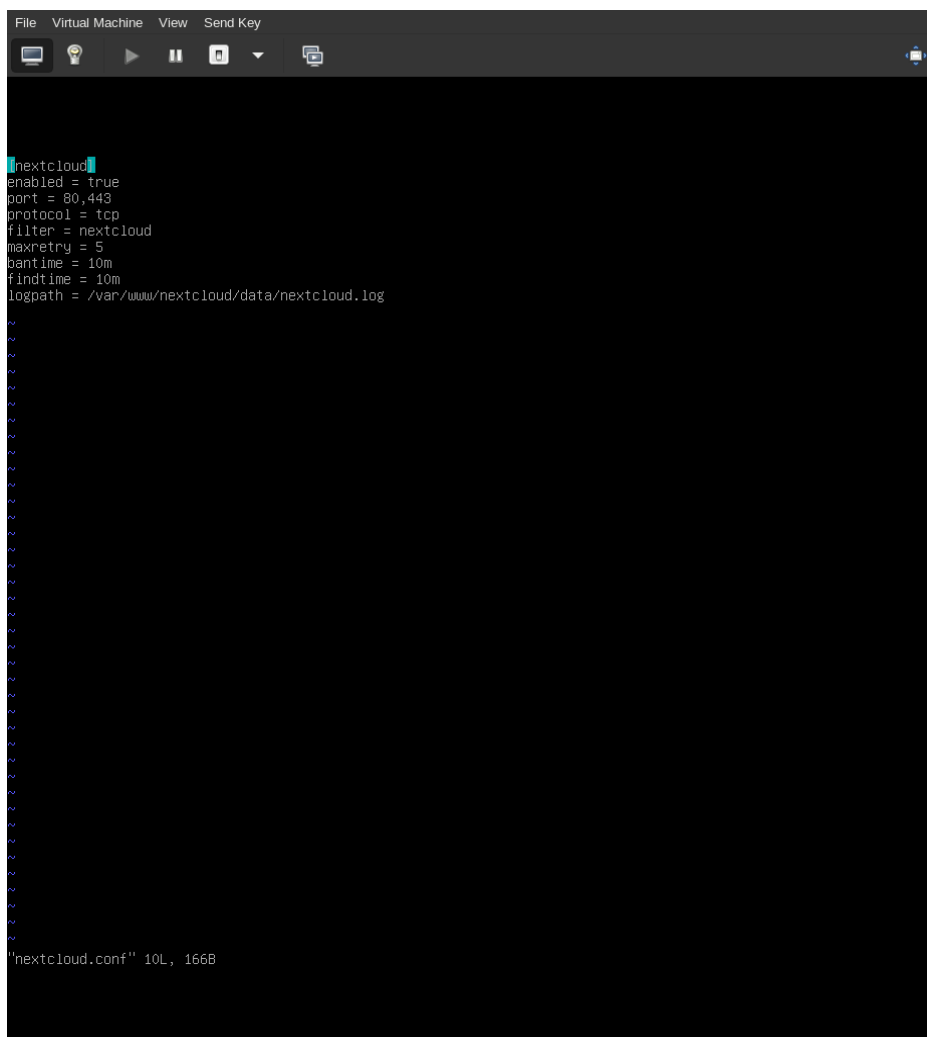
Σε αυτό το ερώτημα αντί να αλλάξουμε το αρχείο jail.local προτιμήσαμε να προσθέσουμε στον φάκελο /etc/fail2ban/jail.d/ δύο αρχεία, ένα joomla.conf και ένα nextcloud.conf που να υλοποιούν με ισοδύναμο τρόπο τις φυλακές. Το περιεχόμενο των αρχείων αυτών φαίνεται παρακάτω:

- /etc/fail2ban/jail.d/joomla.conf


```
[joomla]
enabled = true
filter = joomla
port = http,https
protocol = tcp,udp
maxentry = 5
findtime = 10m
bantime = 10m
logpath = /var/www/joomla/tmp/*error.php
          /var/www/joomla/htdocs/tmp/*error.php
          /var/www/joomla/htdocs/logs/*error.php
          /var/www/joomla/apps/logs/*error.php
          /var/www/joomla/htdocs/administrator/logs/*error.php
          /var/www/joomla/apps/*/administrator/logs/*error.php

"joomla.conf" 14L, 395B
```

- /etc/fail2ban/jail.d/nextcloud.conf



```
File Virtual Machine View Send Key
nextcloud
enabled = true
port = 80,443
protocol = tcp
filter = nextcloud
maxretry = 5
bantime = 10m
findtime = 10m
logpath = /var/www/nextcloud/data/nextcloud.log

"nextcloud.conf" 10L, 166B
```

Εδώ σημειώνω ότι πληροφορίες όπως τα port, protocols και logpath τα βρήκα στο διαδίκτυο, επειδή δεν χρησιμοποιώ ούτε joomla ούτε nextcloud στον προσωπικό μου υπολογιστή ή στο debian server για να τα γνωρίζω.

Επίσης σημειώνω ότι λόγω της απουσίας των logfiles στο logpath, αφού δεν έχω εγκατεστημένο τα joomla και nextcloud μου δημιουργήθηκε αρχικά θέμα, όπου με την χρήση των νέων jail το fail2ban κράσαρε αμέσως όταν ξεκινούσε. Ο τρόπος που έλυσα το θέμα αυτό ήταν να φτιάξω τα log αρχεία σε κάθε logpath μέσω της εντολής touch, και μέχρι και κενά να ήταν το fail2ban πλέον ξεκινούσε κανονικά.