Σύγχρονες Εφαρμογές Ασφάλειας

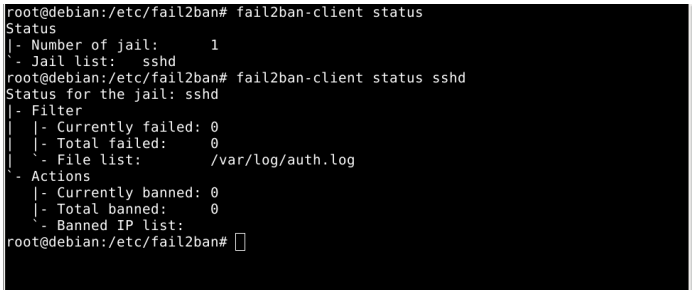
Μπουρλάκης Γεώργιος

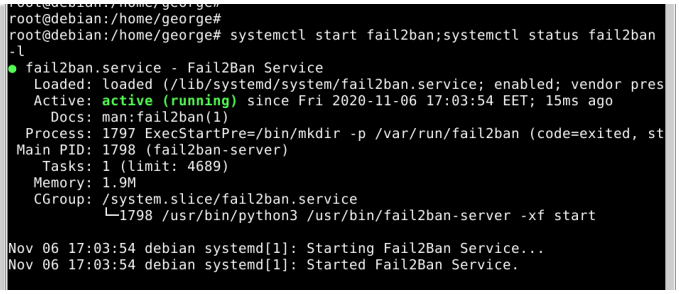
1054321

ssh-fail2ban

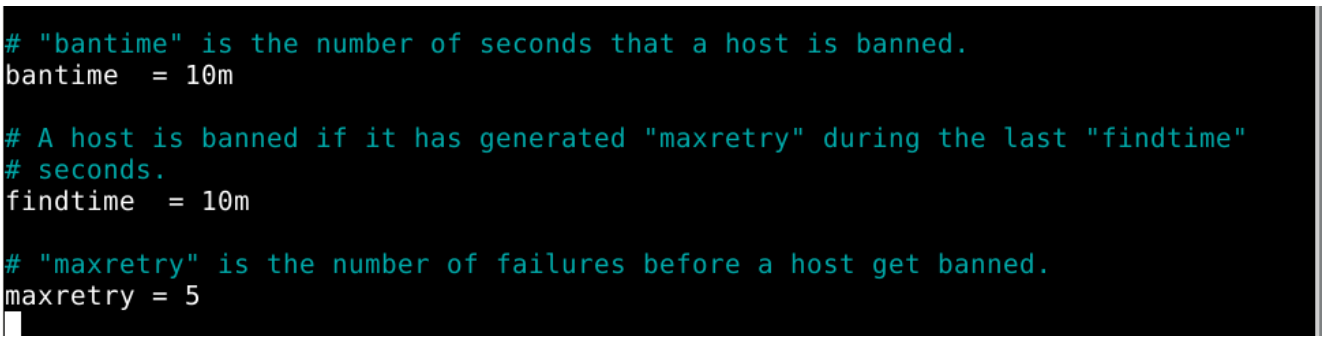
1) Προστασία ανεπιθύμητων επιθέσεων με χρήση του πακέτου fail2ban

- Για την κατάσταση των jails με τις εντολές fail2ban-client status και fail2ban-client status sshd:





- Μετά την τροποποίηση του αρχείου jail.conf να κλειδώνει τις συνδέσεις μετά από 5 λανθασμένες προσπάθειες τα τελευταία 10 λεπτά:



- Το αποτέλεσμα μετά από 5 αποτυχημένες προσπάθειες με λάθος κωδικό φαίνεται από την εντολή fail2ban-client status sshd:

```
root@debian:/home/george# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     6
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   10.0.2.6
root@debian:/home/george#
```

- Οι συνδέσεις καταγράφονται στο /var/log/fail2ban.log

```
2020-11-06 17:15:05,328 fail2ban.server        [1850]: INFO    Starting Fail2ban v0.10.2
2020-11-06 17:15:05,330 fail2ban.database      [1850]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2020-11-06 17:15:05,331 fail2ban.jail          [1850]: INFO    Creating new jail 'sshd'
2020-11-06 17:15:05,343 fail2ban.jail          [1850]: INFO    Jail 'sshd' uses pyinotify {}
2020-11-06 17:15:05,349 fail2ban.jail          [1850]: INFO    Initiated 'pyinotify' backend
2020-11-06 17:15:05,350 fail2ban.filter        [1850]: INFO      maxLines: 1
2020-11-06 17:15:05,380 fail2ban.server        [1850]: INFO    Jail sshd is not a JournalFilter instance
2020-11-06 17:15:05,381 fail2ban.filter        [1850]: INFO    Added logfile: '/var/log/auth.log' (pos = 51147, hash = 0f0476a37c36cfb7b2077c5ab114a08e2b9f4017)
2020-11-06 17:15:05,381 fail2ban.filter        [1850]: INFO      encoding: UTF-8
2020-11-06 17:15:05,381 fail2ban.filter        [1850]: INFO      maxRetry: 5
2020-11-06 17:15:05,382 fail2ban.filter        [1850]: INFO      findtime: 600
2020-11-06 17:15:05,382 fail2ban.actions       [1850]: INFO      banTime: 600
2020-11-06 17:15:05,383 fail2ban.jail          [1850]: INFO    Jail 'sshd' started
2020-11-06 17:19:08,794 fail2ban.filter        [1850]: INFO    [sshd] Found 10.0.2.6 - 2020-11-06 17:19:04
2020-11-06 17:19:08,795 fail2ban.filter        [1850]: INFO    [sshd] Found 10.0.2.6 - 2020-11-06 17:19:06
2020-11-06 17:19:14,709 fail2ban.filter        [1850]: INFO    [sshd] Found 10.0.2.6 - 2020-11-06 17:19:14
2020-11-06 17:19:19,868 fail2ban.filter        [1850]: INFO    [sshd] Found 10.0.2.6 - 2020-11-06 17:19:19
2020-11-06 17:19:40,518 fail2ban.filter        [1850]: INFO    [sshd] Found 10.0.2.6 - 2020-11-06 17:19:40
2020-11-06 17:19:41,100 fail2ban.actions       [1850]: NOTICE  [sshd] Ban 10.0.2.6
2020-11-06 17:19:42,415 fail2ban.filter        [1850]: INFO    [sshd] Found 10.0.2.6 - 2020-11-06 17:19:42
2020-11-06 17:20:41,499 fail2ban.server        [1850]: INFO    Shutdown in progress...
2020-11-06 17:20:41,499 fail2ban.server        [1850]: INFO    Stopping all jails
```

- Η διεύθυνση που απορρίφθηκε από το firewall φαίνεται στην προηγούμενη φωτογραφία και είναι η 10.0.2.6 (IP από άλλο VM στο ίδιο LAN):

```
root@debian:/home/george# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     6
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   10.0.2.6
root@debian:/home/george#
```

- Η εντολή για unban μιας ip είναι η εξής:

```
root@debian:/home/george# fail2ban-client set sshd unbanip 10.0.2.6
10.0.2.6
root@debian:/home/george# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     6
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
root@debian:/home/george#
```

και βλέπουμε ότι πλέον δεν είναι banned.

- Εκτελούμε την εντολή: sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
  για να φτιάξουμε ένα πανομοιότυπο αρχείο με το jail.conf δηλαδή το jail.local στο οποίο μπορούμε να κάνουμε αλλαγές και να βάλουμε σε whitelist πχ την ip 10.0.2.6 με την εντολή: ignoreip = 10.0.2.6

- Δεν κατάφερα να δουλέψω το sendmail παρόλες τις προσπάθειες και αλλαγές στο jail.local όπως θέτοντας στο destemail το email μου, στο mta το sendmail και αλλάζοντας την εντολή action = %(action_)s σε action = %(action_mwl)s

2) Χρήση Public Key Authentication

- Δημιουργία κλειδιού:
  ssh-keygen -t rsa -b 4096

```
root@debian:/etc/fail2ban# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:b0wR0lHs1kb0mysKbePjY77fDl8SMEYegMJL4EqEONU root@debian
The key's randomart image is:
+---[RSA 4096]----+
|.oo..o  .o+=+..  |
|+. .E + ...+.... |
| .. .. o  ..=o  .|
| . .  .    oooo o|
|  .     S .. ..o |
|         +.    ..|
|         .++ o...|
|         .++o =..|
|          +*=..+ |
+----[SHA256]-----+
root@debian:/etc/fail2ban#
```

- Αντιγραφή κλειδιού σε άλλο server:
  ssh-copy-id root@10.0.2.6
  Η αντιγραφή έγινε και κάνοντας: ssh root@10.0.2.6
  βλέπουμε το αρχείο με το δημόσιο κλειδί:nano /root/.ssh/authorized_keys

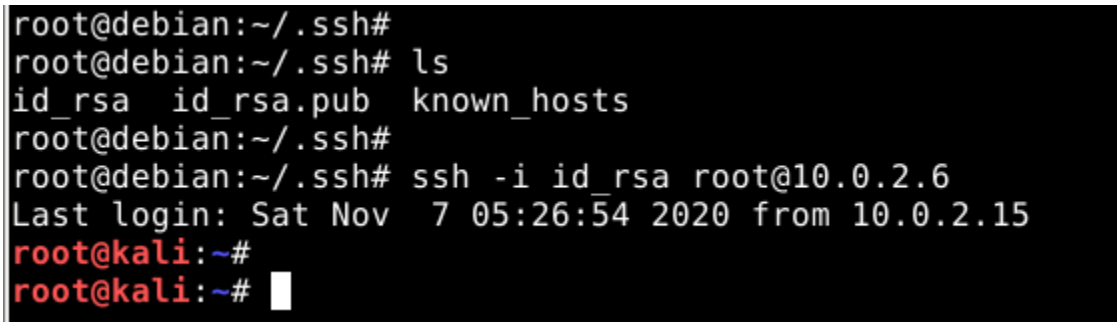
```
root@debian:/etc/fail2ban# ssh-copy-id root@10.0.2.6
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are
 already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to
install the new keys
root@10.0.2.6's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@10.0.2.6'"
and check to make sure that only the key(s) you wanted were added.

root@debian:/etc/fail2ban#
root@debian:/etc/fail2ban# ssh root@10.0.2.6
Linux kali 5.4.0-kali3-amd64 #1 SMP Debian 5.4.13-1kali1 (2020-01-20) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Nov  7 04:50:54 2020 from 10.0.2.15
root@kali:~#
root@kali:~#
root@kali:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  sslstrip.log  Templates  Videos
root@kali:~# cd /root/.ssh/
root@kali:~/.ssh# ls
authorized_keys  known_hosts
root@kali:~/.ssh# nano authorized_keys
root@kali:~/.ssh#
```

- Έγιναν κάποια configurations στο sshd_config:
  PubkeyAuthentication yes
  PasswordAuthentication no
  ChallengeResponseAuthentication no
  UsePAM no

```
PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
```

```
# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM no
```

- Επιτυχία δοκιμής σύνδεσης χωρίς κωδικό αλλά με το private key id_rsa:



3) Υλοποίηση νέων φίλτρων για χρήση στο πακέτο fail2ban

- failregex = lost input channel from .*\[<HOST>\] to MTA-v\d after (data|mail|rcpt)$

\[<HOST>\] did not issue MAIL/EXPN/VRFY/ETRN during connection to (MSP|MTA)-v\d$
\[<HOST>\], reject.*\.\.\. (Relaying denied)
\[<HOST>\]: Possible SMTP RCPT flood, throttling\.$
timeout waiting for input from \[<HOST>\] during server cmd read
rejecting commands from(.+)? \[<HOST>\] due to pre-greeting traffic
relay=([^]+)?\[<HOST>\], .* Domain of sender address [\w@.-]+ does not (exist|resolve)$

- ignoreregex = sm-mta\[\d+\]: \w+: (from|to)=
sm-mta\[\d+\]: \S+[[]\d[]]:
sm-mta\[\d+\]: STARTTLS=(client|server)
sm-mta\[\d+\]: STARTTLS: (read|write) error=(generic|syscall|timeout)
: timeout waiting for input from [\w.-]+ during server cmd read$
: collect: premature EOM: (unexpected close|Connection timed out with [\[\]\w.-]+|Connection reset by \S+)(, sender=\S+)?$
: collect: (I/O error|read timeout|unexpected close) on connection from
[\w.-]+ did not issue MAIL/EXPN/VRFY/ETRN during connection to MTA-v\d$

- Η εντολή για δοκιμάσουμε κάποια φίλτρα χωρίς να τα ενεργοποιήσουμε(πχ για φίλτρο sshd) είναι: fail2ban-regex /var/log/auth/log /etc/fail2ban/filter.d/sshd.conf

```
root@debian:/etc/fail2ban# fail2ban-regex /var/log/auth.log /etc/fail2ban/filter.d/sshd.conf

Running tests
=============

Use   failregex filter file : sshd, basedir: /etc/fail2ban
Use         maxlines : 1
Use      datepattern : Default Detectors
Use         log file : /var/log/auth.log
Use         encoding : UTF-8


Results
=======

Failregex: 98 total
|-  #) [# of hits] regular expression
|   4) [68] ^Failed \b(?!publickey)\S+ for (?P<cond_inv>invalid user )?<F-USER>(?P<cond_user>\S+
)|(?(cond_inv)(?:(?! from ).)*?|[^:]+)</F-USER> from <HOST>(?: port \d+)?(?: on \S+(?: port \d+)
?)?(?: ssh\d*)?(?(cond_user): |(?:(?:(?! from ).)*)$)
|  14) [30] ^pam_unix\(sshd:auth\):\s+authentication failure;\s*logname=\S*\s*uid=\d*\s*euid=\d*
\s*tty=\S*\s*ruser=<F-USER>\S*</F-USER>\s*rhost=<HOST>\s.*(?: \[preauth\])?\s*$
`-

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
|  [880] {^LN-BEG}(?:DAY )?MON Day %k:Minute:Second(?:\.Microseconds)?(?: ExYear)?
`-

Lines: 884 lines, 0 ignored, 98 matched, 786 missed
[processed in 0.16 sec]

Missed line(s): too many to print.  Use --print-all-missed to print all 786 lines
root@debian:/etc/fail2ban#
```

- fail2ban-regex --print-all-missed /var/log/mail.log /etc/fail2ban/filter.d/sendmail.conf /etc/fail2ban/filter.d/sendmail.conf | less

```
[sendmail]
enabled = true
port = smtp, submission
filter = sendmail
logpath = /var/log/mail.log
bantime = 5m
findtime = 5m
maxretry = 3
```