Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

2η Εργασία
Ονοματεπώνυμο: Αγησίλαος Κολλιόπουλος
Αριθμός Μητρώου: 1072803
Τμήμα: ΗΜΤΥ

Ερωτήσεις κατανόησης και Εργασία για το μάθημα:
Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

1) Προστασία ανεπιθύμητων επιθέσεων με χρήση του πακέτου fail2ban

Εγκαθιστούμε το πακέτο fail2ban και το ενεργοποιούμε.

- Ελέγχουμε την κατάσταση των jails με την εντολή **fail2ban-client status** και **fail2ban-client status sshd**.

```
agiskallas@debian-agis:~$ sudo fail2ban-client status
[sudo] password for agiskallas:
Status
|- Number of jail:      1
`- Jail list:   sshd
agiskallas@debian-agis:~$ 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:
```

Εικόνα 1: Τα αποτελέσματα των εντολών

- τροποποιούμε το αρχείο για το φίλτρο ssh ώστε να κλειδώνει τις συνδέσεις μετά από5 λανθασμένες προσπάθειες στα τελευταία 10 λεπτά.

  Αφού ορίσουμε το αρχείο **/etc/fail2ban/jail.local**, επεξεργαζόμαστε την ετικέτα [sshd] και θέτουμε findtime = 600, maxretry = 5, όπου findtime είναι ο χρόνος μεταξύ αποτυχημένων προσπαθειών και maxretry, ο μέγιστος αριθμός αποτυχημένων προσπαθειών για να γίνει ban.

```
# SSH servers
#

[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode   = normal
enabled = true
port    = ssh
maxretry = 5
findtime = 600
bantime = 3600
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

Εικόνα 2: Καθορισμός παραμέτρων sshd jail

- Έχοντας δύο τερματικά ανοικτά, πραγματοποιούμε 5 προσπάθειες με λάθος κωδικό και βλέπουμε το αποτέλεσμα με την εντολή **fail2ban-client status sshd**.

```
kolli@192.168.1.7's password:
Permission denied, please try again.
kolli@192.168.1.7's password:
Permission denied, please try again.
kolli@192.168.1.7's password:
kolli@192.168.1.7: Permission denied (publickey,password).

C:\Users\kolli>ssh 192.168.1.7
kolli@192.168.1.7's password:
ssh_dispatch_run_fatal: Connection to 192.168.1.7 port 22: Connection
 timed out

C:\Users\kolli>ssh 192.168.1.7

C:\Users\kolli>ssh 192.168.1.7
ssh: connect to host 192.168.1.7 port 22: Connection timed out
```

Εικόνα 3: Αποτυχημένες προσπάθειες σύνδεσης

```
agiskallas@debian-agis:~$ 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:   192.168.1.27
agiskallas@debian-agis:~$ _
```

Εικόνα 4: Το status(banned IP) μετά τις αποτυχίες

- Το log συνδέσεων για το fail2ban βρίσκεται στο **/var/log/fail2ban.log** και κάνοντας **cat** τα logs βλέπουμε τις 5 αποτυχημένες προσπάθειες που κάναμε και την IP που το κάναμε και στην συνέχεια φαίνεται η διαδικασία του ban.

```
2023-11-02 15:56:54,079 fail2ban.filtersystemd  [495]: INFO    [sshd] Jail is in operation now (proc
ess new journal entries)
2023-11-02 16:10:15,713 fail2ban.filter         [495]: INFO    [sshd] Found 192.168.1.27 - 2023-11-0
2 16:10:15
2023-11-02 16:10:21,416 fail2ban.filter         [495]: INFO    [sshd] Found 192.168.1.27 - 2023-11-0
2 16:10:20
2023-11-02 16:10:25,164 fail2ban.filter         [495]: INFO    [sshd] Found 192.168.1.27 - 2023-11-0
2 16:10:24
2023-11-02 16:10:29,123 fail2ban.filter         [495]: INFO    [sshd] Found 192.168.1.27 - 2023-11-0
2 16:10:28
2023-11-02 16:10:34,664 fail2ban.filter         [495]: INFO    [sshd] Found 192.168.1.27 - 2023-11-0
2 16:10:34
2023-11-02 16:10:34,677 fail2ban.actions        [495]: NOTICE  [sshd] Ban 192.168.1.27
```

Εικόνα 5: Το log των συνδέσεων

- Κοιτώντας και το firewall μας, βλέπουμε πως το fail2ban πρόσθεσε κανόνα που κάνει όλα τα πακέτα από την banned IP REJECT(εδώ αντί για IP, έχει το LAPTOP)

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-sshd (1 references)
target     prot opt source               destination
REJECT     all  --  LAPTOP-AE1O84HI.router.wind  anywhere             reject-with icmp-port-unreacha
ble
RETURN     all  --  anywhere             anywhere
```

Εικόνα 6: Ανανέωση του firewall από το fail2ban

- Για να κάνουμε unban μια IP χρησιμοποιούμε την εντολή:

  sudo fail2ban-client set JAIL unbanip IP,

  Όπου **JAIL** είναι το όνομα της φυλακής, στην δικιά μας περίπτωση είναι **sshd** και **IP** είναι η IP που θέλουμε να κάνουμε unban, δηλαδή 192.168.1.27.

```
agiskallas@debian-agis:~$ sudo fail2ban-client set sshd unbanip 192.168.1.27
1
agiskallas@debian-agis:~$ 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:
agiskallas@debian-agis:~$ 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
```

Εικόνα 7: Μετά το unban

- Για να κάνουμε Whitelist IP που δεν θέλουμε να γίνονται ban αλλάζουμε το **/etc/fail2ban/jail.local** και κάτω από το [sshd] μπορούμε να ορίσουμε ignoreip = 192.168.1.1/24 . Με αυτόν τον τρόπο επιτρέπουμε όλες τις IP στο τοπικό δίκτυο να κάνουν προσπάθειες σύνδεσης με ssh χωρίς να γίνονται ban

- Εγκαθιστούμε το πακέτο **sendmail** ώστε το fail2ban να μας στέλνει email όταν μπλοκάρεται μια IP διεύθυνση. Μετά την εγκατάσταση του πακέτου **sendmail** και βάζοντας στο αρχείο **/etc/mail.rc** τα credentials για το gmail, αλλάζουμε τα παρακάτω settings στο **jail.local**:

```
[Default]
destemail = upXXXXXXX@ac.upatras.gr
sender = example@gmail.com
mta = sendmail
action = %(action mwl) s

[sshd]
enabled = true
filter = sshd
```

Στην συνέχεια κάνουμε restart το fail2ban.service

---

2) Χρήση Public Key Authentication

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

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

  Χρησιμοποιήσαμε την εντολή: **ssh-keygen -t rsa -b 4096**

- την αντιγραφή του κλειδιού στο host υπολογιστή μας

  Αντιγράφουμε το **id_debian.pub** αρχείο με **scp** στο αρχείο **~/.ssh/authorized_keys** του VM μας, ενώ στο host machine ορίζουμε το **.ssh/config** για να προτιμάει τη σύνδεση με public key ως εξής:

```
Host debian

    HostName 192.168.1.10
    User agiskallas
    PreferredAuthentications publickey
    IdentityFile ~/.ssh/id_debian
```

- τροποποίηση του αρχείου **sshd_config** για πρόσβαση μόνο με το δημόσιο κλειδί.

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

```
PasswordAuthentication no
```

- την επιτυχή δοκιμή σύνδεσης (χωρίς την χρήση συνθηματικού password).

```
PS C:\Users\kolli> ssh debian
Linux debian-agis 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.
You have mail.
Last login: Fri Nov  3 09:50:24 2023
agiskallas@debian-agis:~$
```

Εικόνα 8: Επιτυχής σύνδεση με public key

---

3) Υλοποίηση 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 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"}*

- Υλοποιούμε το “regular expression” για δύο νέα φίλτρα στο fail2ban, που να λαμβάνει υπόψιν του το παραπάνω αρχείο καταγραφής.

Joomla = ^.* INFO <HOST> joomlafailure .*$
Nextcloud = ^{.*reqId.*nextcloud.*message.*Login failed.*Remote IP: <HOST>.*version.*}$

^ κάνει match την αρχή string
.* χαρακτήρας 0 ή πολλές φορές
$ κάνει match το τέλος string
<HOST> για match από το fail2ban

- Μπορούμε να δοκιμάσουμε (dry run) τα παραπάνω φίλτρα χωρίς να τα ενεργοποιήσουμε με την παρακάτω εντολή:

fail2ban-regex file.log "regex code"

- Αποθηκεύουμε στον φάκελο **/etc/fail2ban/filter.d/** με τα αντίστοιχα ονόματα regex ως εξής:

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

Ορίζουμε στο αρχείο jail.local για τα παραπάνω φίλτρα τα: ports, protocols, iptable chain, findtime, bantime και retries.

```
[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
```

Τέλος, κάνουμε restart το fail2ban.service για να δεχτεί τις νέες αλλαγές.