Fail2ban

“Now go away or I shall taunt you a second time…”

CIALUG
December 2016
Andrew Denner

Welcome to lug

Slides will be posted later tonight on http://denner.co

Email: denner@gmail.com

Twitter: @adenner

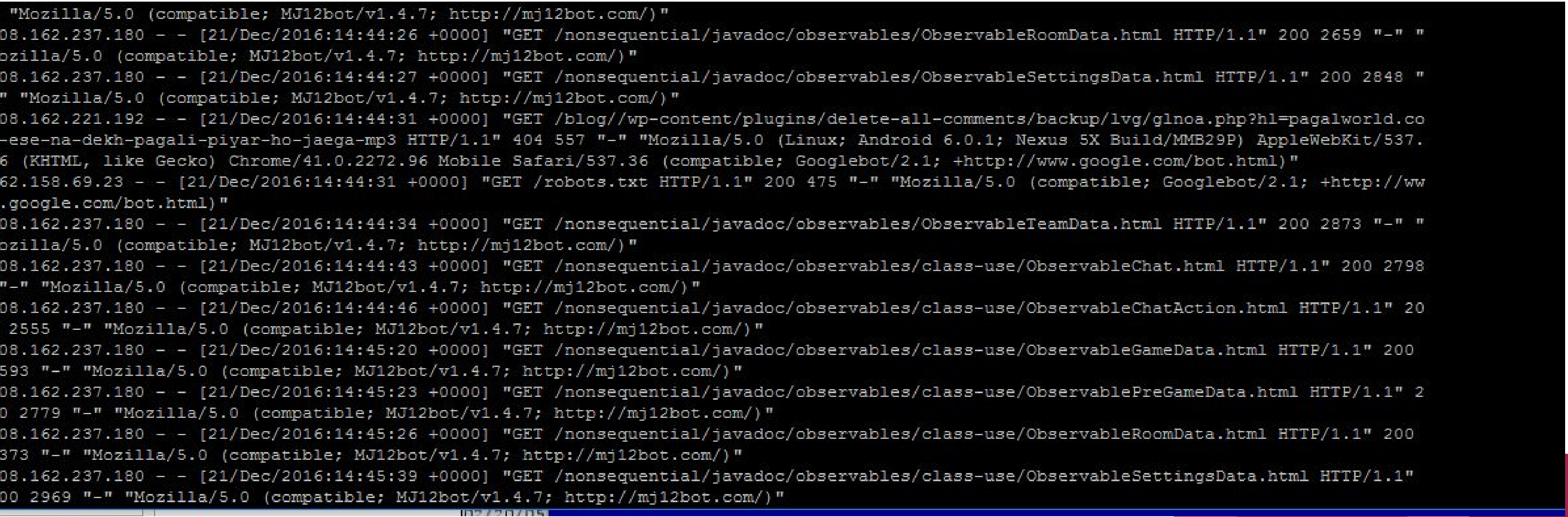
18 76
G.H. BASS

FAIL

Fail2ban

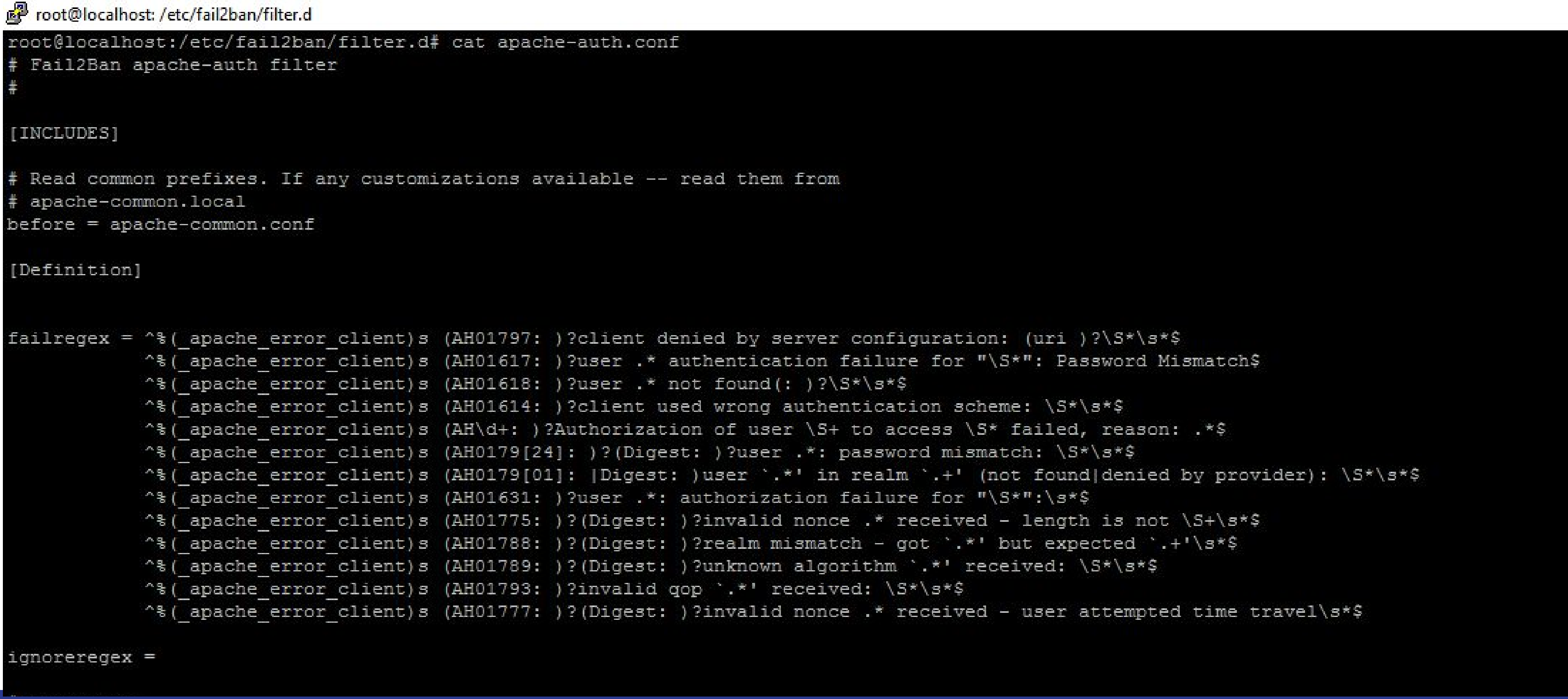
“Fail2ban scans log files (e.g. /var/log/apache/error_log) and bans IPs that show the malicious signs -- too many password failures, seeking for exploits, etc. Generally Fail2Ban is then used to update firewall rules to reject the IP addresses for a specified amount of time, although any arbitrary other action (e.g. sending an email) could also be configured. Out of the box Fail2Ban comes with filters for various services (apache, courier, ssh, etc).” --http://www.fail2ban.org/

Looks at log files like apache access



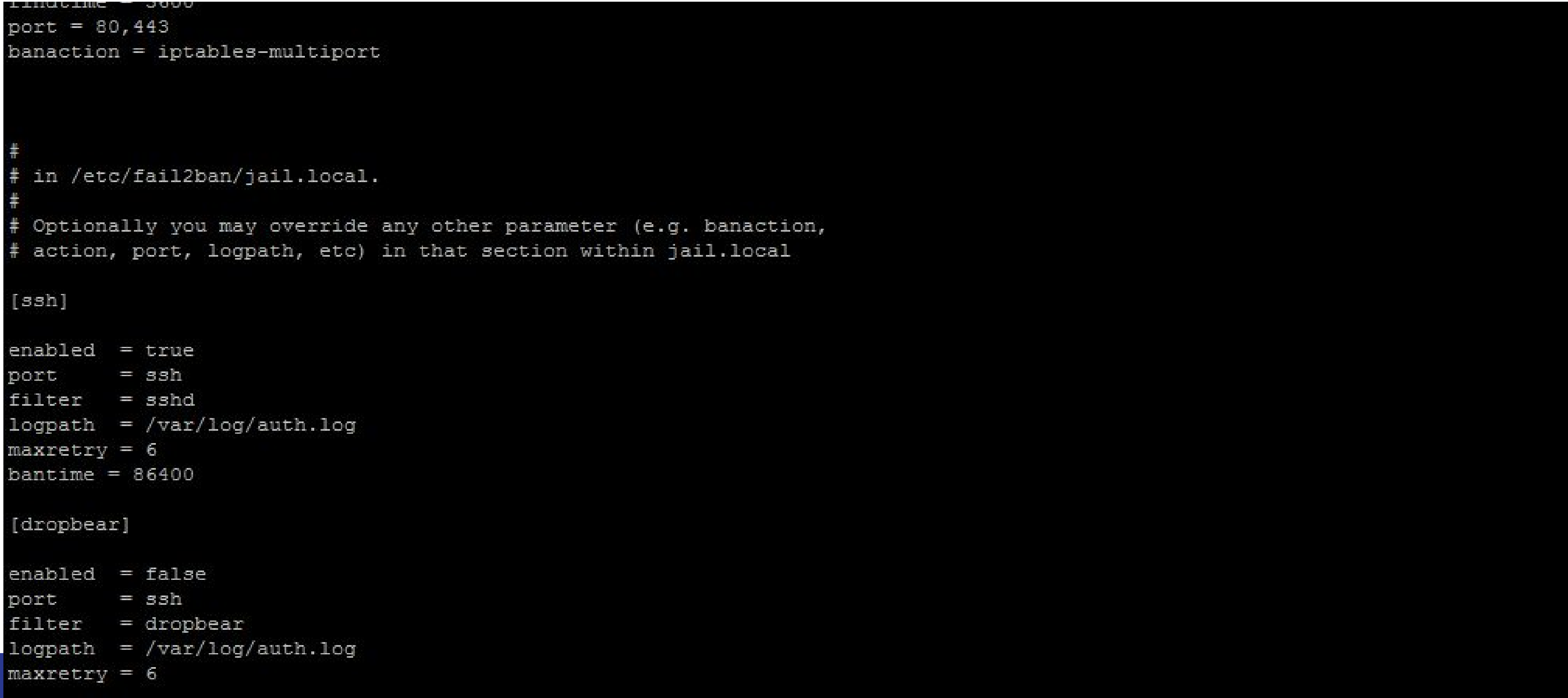
```
 "Mozilla/5.0 (compatible; MJ12bot/v1.4.7; http://mj12bot.com/)"
08.162.237.180 - - [21/Dec/2016:14:44:26 +0000] "GET /nonsequential/javadoc/observables/ObservableRoomData.html HTTP/1.1" 200 2659 "-" "
ozilla/5.0 (compatible; MJ12bot/v1.4.7; http://mj12bot.com/)"
08.162.237.180 - - [21/Dec/2016:14:44:27 +0000] "GET /nonsequential/javadoc/observables/ObservableSettingsData.html HTTP/1.1" 200 2848 "
" "Mozilla/5.0 (compatible; MJ12bot/v1.4.7; http://mj12bot.com/)"
08.162.221.192 - - [21/Dec/2016:14:44:31 +0000] "GET /blog//wp-content/plugins/delete-all-comments/backup/lvg/glnoa.php?hl=pagalworld.co
-ese-na-dekh-pagali-piyar-ho-jaega-mp3 HTTP/1.1" 404 557 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.
6 (KHTML, like Gecko) Chrome/41.0.2272.96 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
62.158.69.23 - - [21/Dec/2016:14:44:31 +0000] "GET /robots.txt HTTP/1.1" 200 475 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://ww
.google.com/bot.html)"
08.162.237.180 - - [21/Dec/2016:14:44:34 +0000] "GET /nonsequential/javadoc/observables/ObservableTeamData.html HTTP/1.1" 200 2873 "-" "
ozilla/5.0 (compatible; MJ12bot/v1.4.7; http://mj12bot.com/)"
08.162.237.180 - - [21/Dec/2016:14:44:43 +0000] "GET /nonsequential/javadoc/observables/class-use/ObservableChat.html HTTP/1.1" 200 2798
"-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.7; http://mj12bot.com/)"
08.162.237.180 - - [21/Dec/2016:14:44:46 +0000] "GET /nonsequential/javadoc/observables/class-use/ObservableChatAction.html HTTP/1.1" 20
 2555 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.7; http://mj12bot.com/)"
08.162.237.180 - - [21/Dec/2016:14:45:20 +0000] "GET /nonsequential/javadoc/observables/class-use/ObservableGameData.html HTTP/1.1" 200
593 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.7; http://mj12bot.com/)"
08.162.237.180 - - [21/Dec/2016:14:45:23 +0000] "GET /nonsequential/javadoc/observables/class-use/ObservablePreGameData.html HTTP/1.1" 2
0 2779 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.7; http://mj12bot.com/)"
08.162.237.180 - - [21/Dec/2016:14:45:26 +0000] "GET /nonsequential/javadoc/observables/class-use/ObservableRoomData.html HTTP/1.1" 200
373 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.7; http://mj12bot.com/)"
08.162.237.180 - - [21/Dec/2016:14:45:39 +0000] "GET /nonsequential/javadoc/observables/class-use/ObservableSettingsData.html HTTP/1.1"
00 2969 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.7; http://mj12bot.com/)"
```

Using regex files found in /etc/fail2ban/filter.d



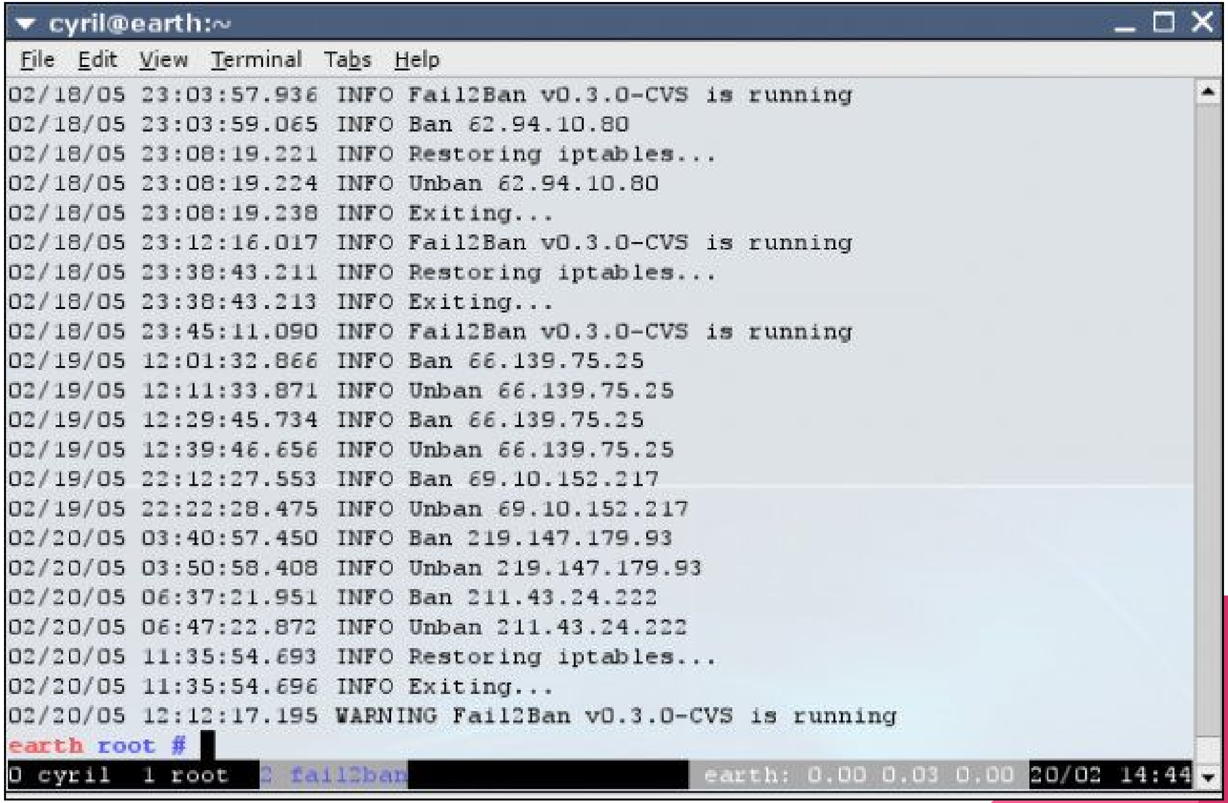
```
root@localhost:/etc/fail2ban/filter.d# cat apache-auth.conf
# Fail2Ban apache-auth filter
#

[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# apache-common.local
before = apache-common.conf

[Definition]


failregex = ^%(_apache_error_client)s (AH01797: )?client denied by server configuration: (uri )?\S*\s*$
            ^%(_apache_error_client)s (AH01617: )?user .* authentication failure for "\S*": Password Mismatch$
            ^%(_apache_error_client)s (AH01618: )?user .* not found(: )?\S*\s*$
            ^%(_apache_error_client)s (AH01614: )?client used wrong authentication scheme: \S*\s*$
            ^%(_apache_error_client)s (AH\d+: )?Authorization of user \S+ to access \S* failed, reason: .*$
            ^%(_apache_error_client)s (AH0179[24]: )?(Digest: )?user .*: password mismatch: \S*\s*$
            ^%(_apache_error_client)s (AH0179[01]: |Digest: )user `.*' in realm `.+' (not found|denied by provider): \S*\s*$
            ^%(_apache_error_client)s (AH01631: )?user .*: authorization failure for "\S*":\s*$
            ^%(_apache_error_client)s (AH01775: )?(Digest: )?invalid nonce .* received - length is not \S+\s*$
            ^%(_apache_error_client)s (AH01788: )?(Digest: )?realm mismatch - got `.*' but expected `.+'\s*$
            ^%(_apache_error_client)s (AH01789: )?(Digest: )?unknown algorithm `.*' received: \S*\s*$
            ^%(_apache_error_client)s (AH01793: )?invalid qop `.*' received: \S*\s*$
            ^%(_apache_error_client)s (AH01777: )?(Digest: )?invalid nonce .* received - user attempted time travel\s*$

ignoreregex =
```

Rules in /etc/fail2ban/jail.conf

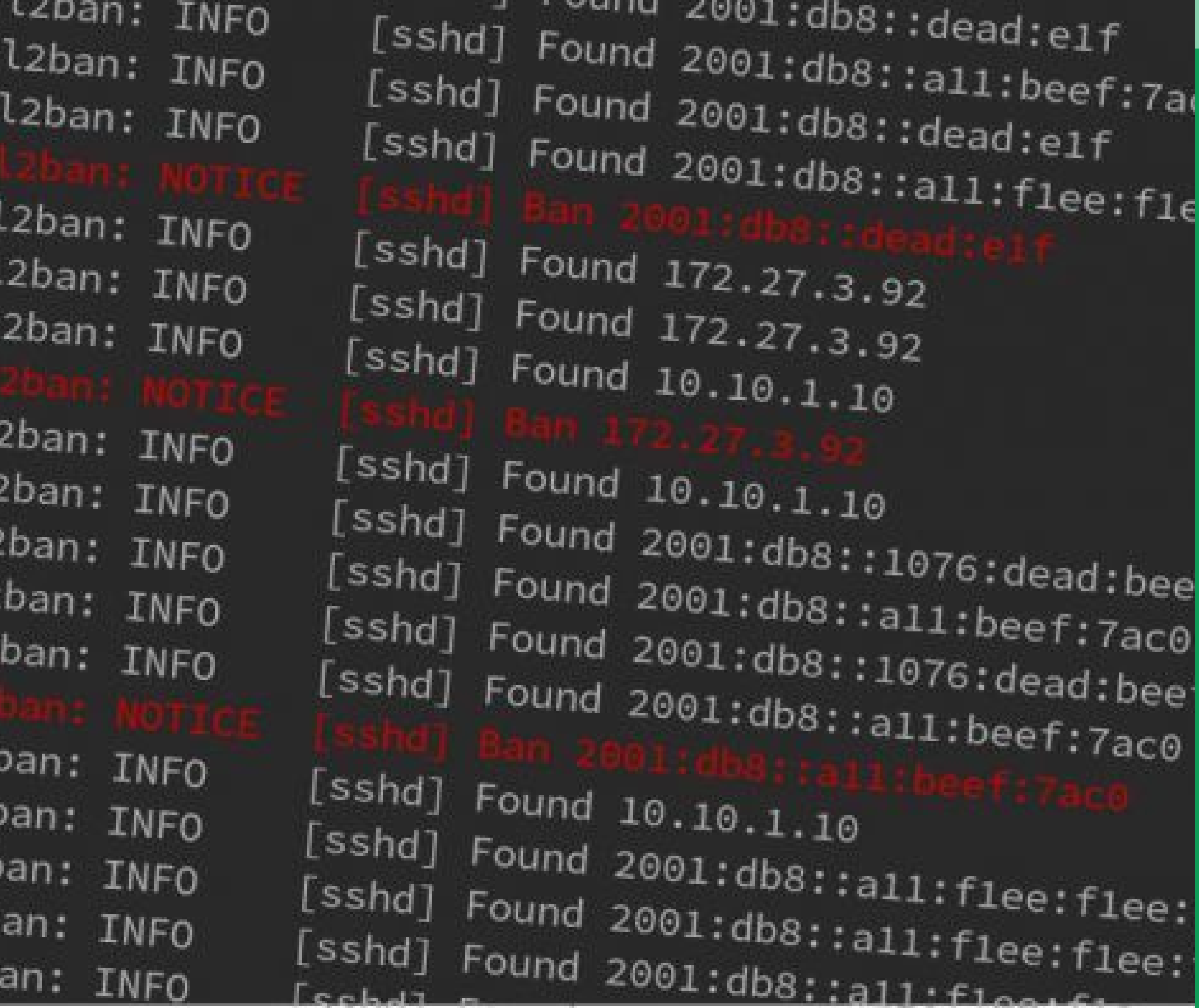


```
findtime = 3600
port = 80,443
banaction = iptables-multiport



#
# in /etc/fail2ban/jail.local.
#
# Optionally you may override any other parameter (e.g. banaction,
# action, port, logpath, etc) in that section within jail.local

[ssh]

enabled  = true
port     = ssh
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 6
bantime = 86400

[dropbear]

enabled  = false
port     = ssh
filter   = dropbear
logpath  = /var/log/auth.log
maxretry = 6
```

Actions logged in /var/log/fail2ban.log



```
02/18/05 23:03:57.936 INFO Fail2Ban v0.3.0-CVS is running
02/18/05 23:03:59.065 INFO Ban 62.94.10.80
02/18/05 23:08:19.221 INFO Restoring iptables...
02/18/05 23:08:19.224 INFO Unban 62.94.10.80
02/18/05 23:08:19.238 INFO Exiting...
02/18/05 23:12:16.017 INFO Fail2Ban v0.3.0-CVS is running
02/18/05 23:38:43.211 INFO Restoring iptables...
02/18/05 23:38:43.213 INFO Exiting...
02/18/05 23:45:11.090 INFO Fail2Ban v0.3.0-CVS is running
02/19/05 12:01:32.866 INFO Ban 66.139.75.25
02/19/05 12:11:33.871 INFO Unban 66.139.75.25
02/19/05 12:29:45.734 INFO Ban 66.139.75.25
02/19/05 12:39:46.656 INFO Unban 66.139.75.25
02/19/05 22:12:27.553 INFO Ban 69.10.152.217
02/19/05 22:22:28.475 INFO Unban 69.10.152.217
02/20/05 03:40:57.450 INFO Ban 219.147.179.93
02/20/05 03:50:58.408 INFO Unban 219.147.179.93
02/20/05 06:37:21.951 INFO Ban 211.43.24.222
02/20/05 06:47:22.872 INFO Unban 211.43.24.222
02/20/05 11:35:54.693 INFO Restoring iptables...
02/20/05 11:35:54.696 INFO Exiting...
02/20/05 12:12:17.195 WARNING Fail2Ban v0.3.0-CVS is running
earth root #
0 cyril  1 root  2 fail2ban                    earth: 0.00 0.03 0.00 20/02 14:44
```

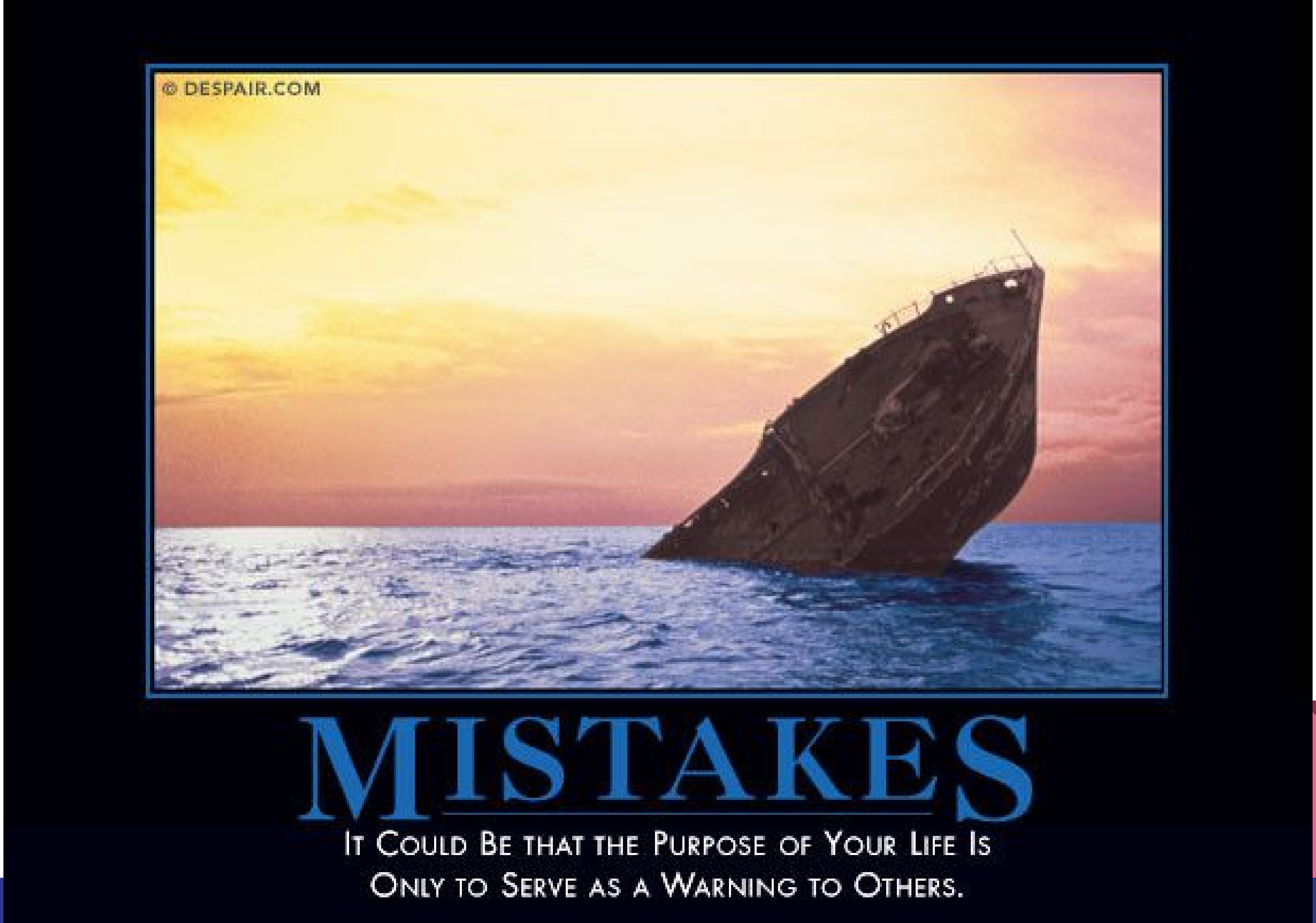


```
                   Found 2001:db8::dead:e1f
l2ban: INFO     [sshd] Found 2001:db8::a11:beef:7ac
l2ban: INFO     [sshd] Found 2001:db8::dead:e1f
l2ban: INFO     [sshd] Found 2001:db8::a11:f1ee:f1e
l2ban: NOTICE   [sshd] Ban 2001:db8::dead:e1f
l2ban: INFO     [sshd] Found 172.27.3.92
2ban: INFO      [sshd] Found 172.27.3.92
2ban: INFO      [sshd] Found 10.10.1.10
2ban: NOTICE    [sshd] Ban 172.27.3.92
2ban: INFO      [sshd] Found 10.10.1.10
2ban: INFO      [sshd] Found 2001:db8::1076:dead:bee
2ban: INFO      [sshd] Found 2001:db8::a11:beef:7ac0
ban: INFO       [sshd] Found 2001:db8::1076:dead:bee
ban: INFO       [sshd] Found 2001:db8::a11:beef:7ac0
ban: NOTICE     [sshd] Ban 2001:db8::a11:beef:7ac0
ban: INFO       [sshd] Found 10.10.1.10
ban: INFO       [sshd] Found 2001:db8::a11:f1ee:f1ee:
an: INFO        [sshd] Found 2001:db8::a11:f1ee:f1ee:
an: INFO        [sshd] Found 2001:db8::a11:f1ee:f1ee:
an: INFO        [sshd]
```

Shortcomings

Before the latest version fail2ban didn’t support ipv6

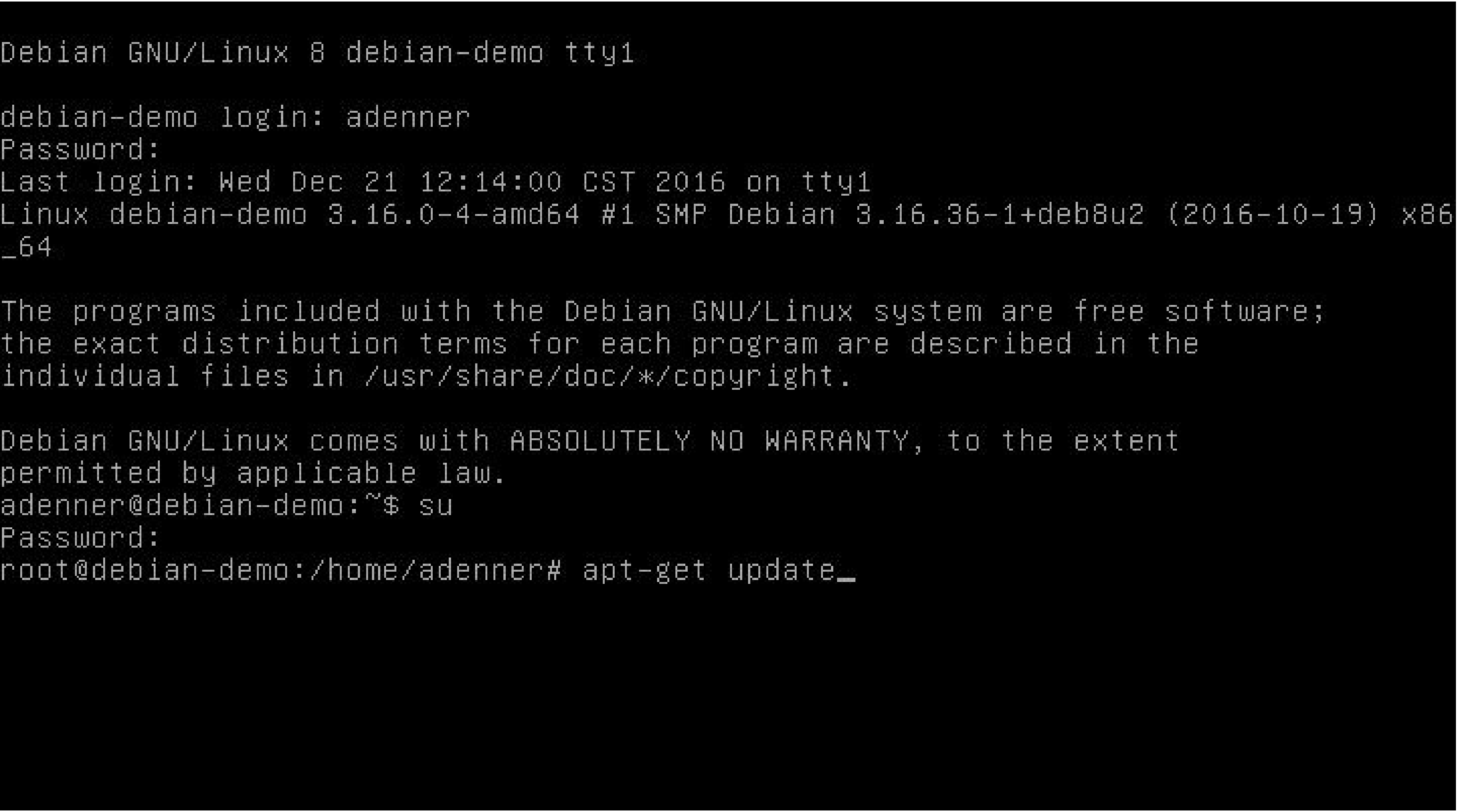
It now does…


© DESPAIR.COM
MISTAKES
It Could Be that the Purpose of Your Life Is
Only to Serve as a Warning to Others.

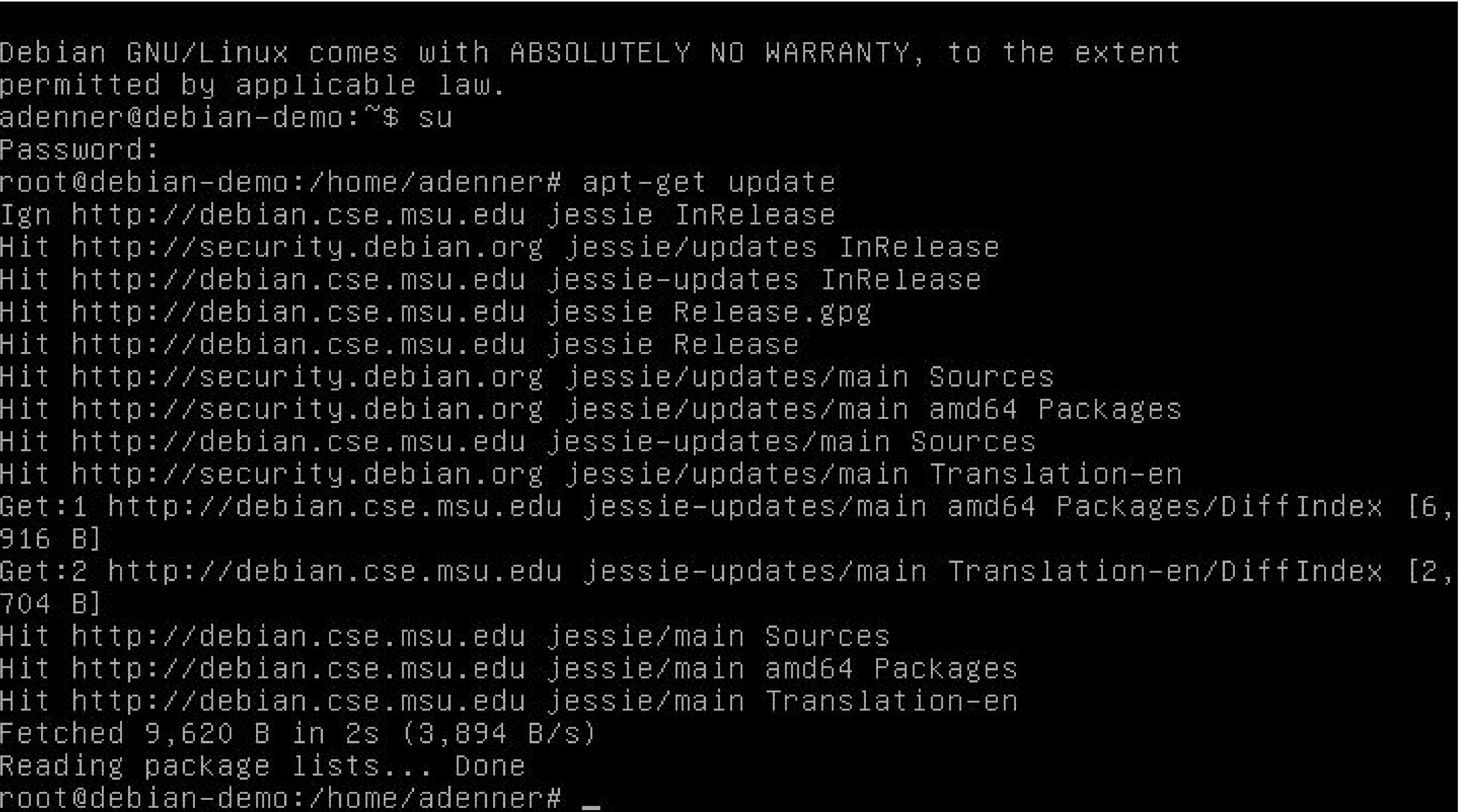
Ssh keys or a password manager is your friend

“I wrote them down in my diary so that I wouldn't *have* to remember.”

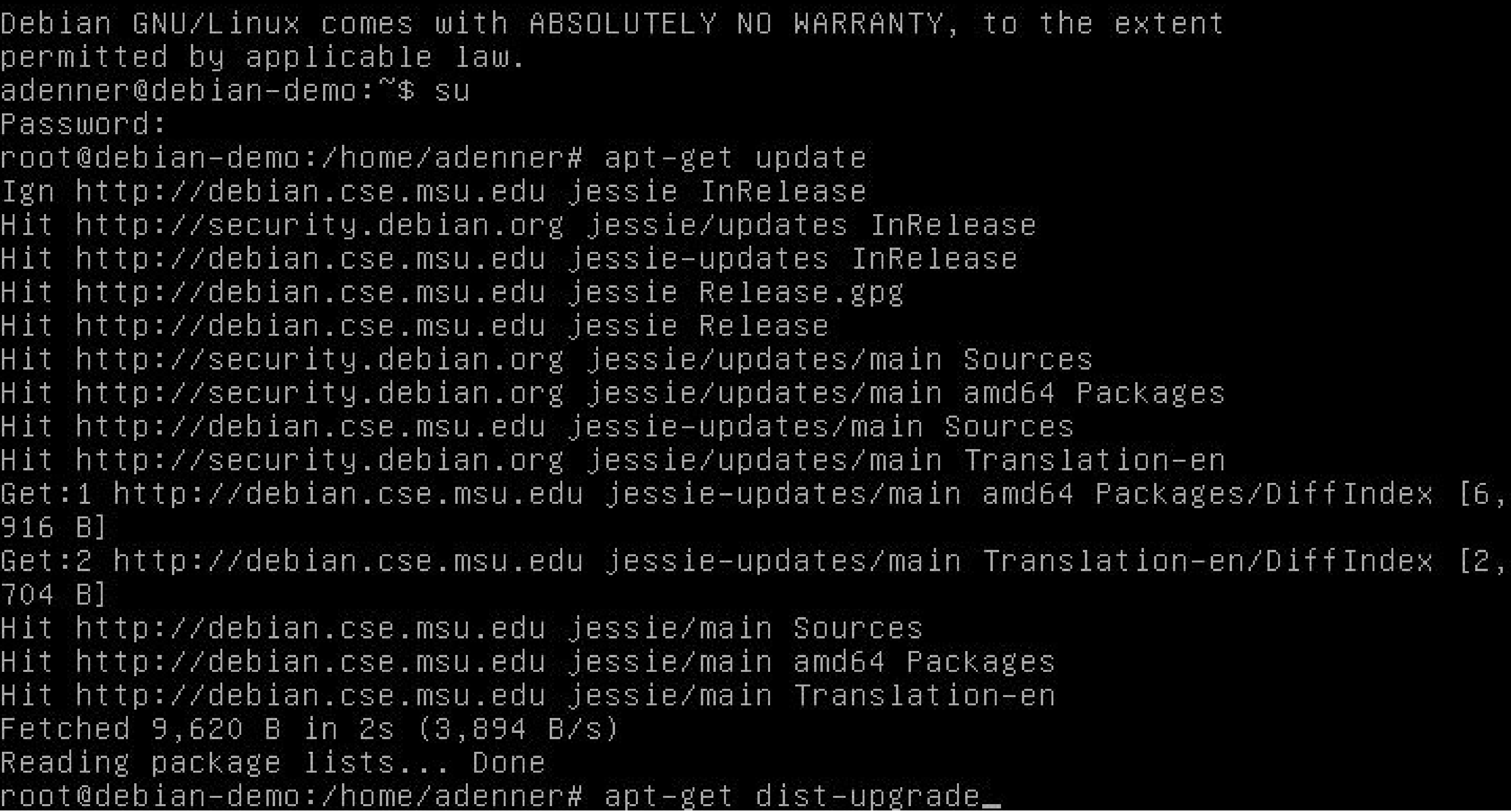
Now for the install



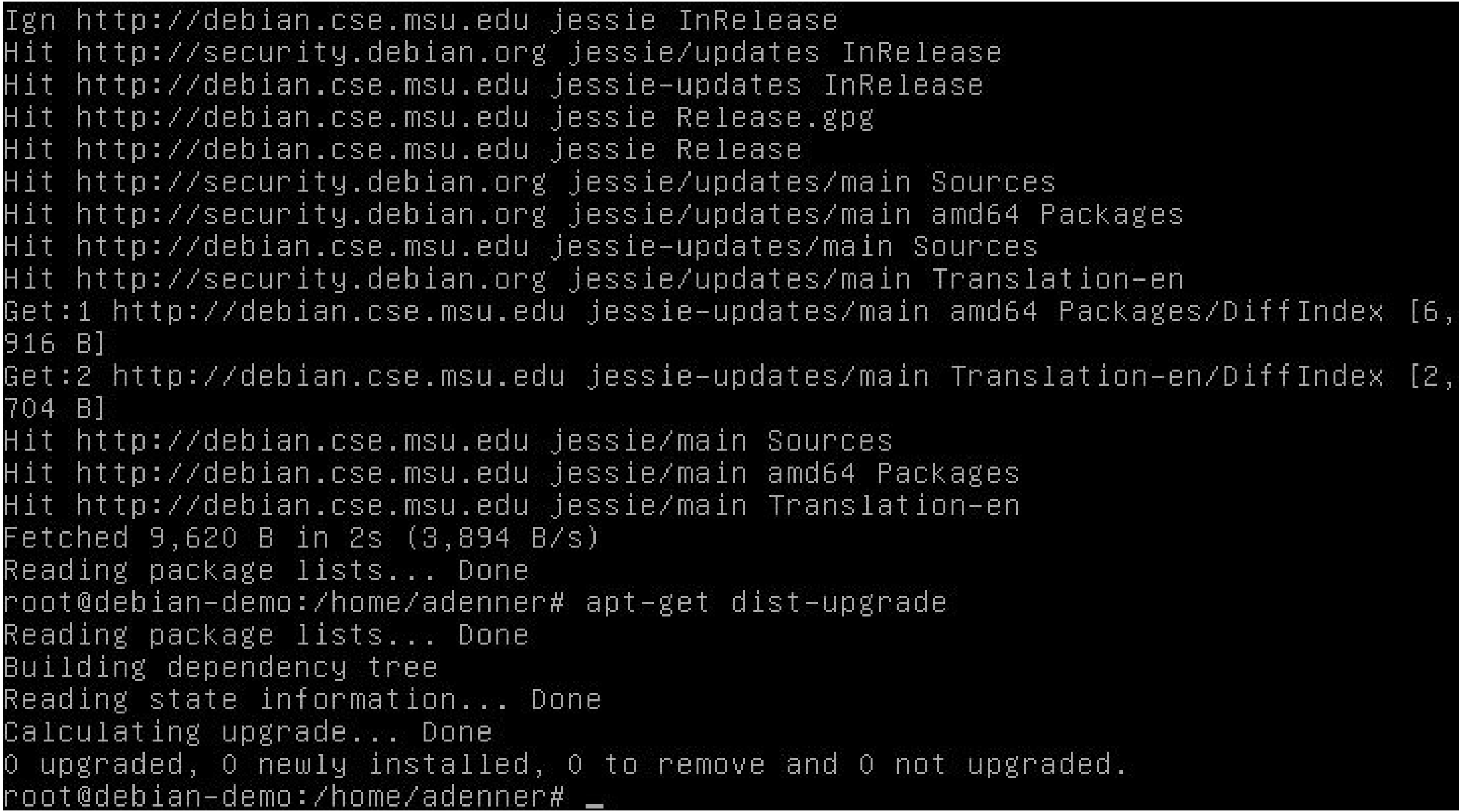
```
Debian GNU/Linux 8 debian-demo tty1

debian-demo login: adenner
Password:
Last login: Wed Dec 21 12:14:00 CST 2016 on tty1
Linux debian-demo 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) 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.
adenner@debian-demo:~$ su
Password:
root@debian-demo:/home/adenner# apt-get update_
```



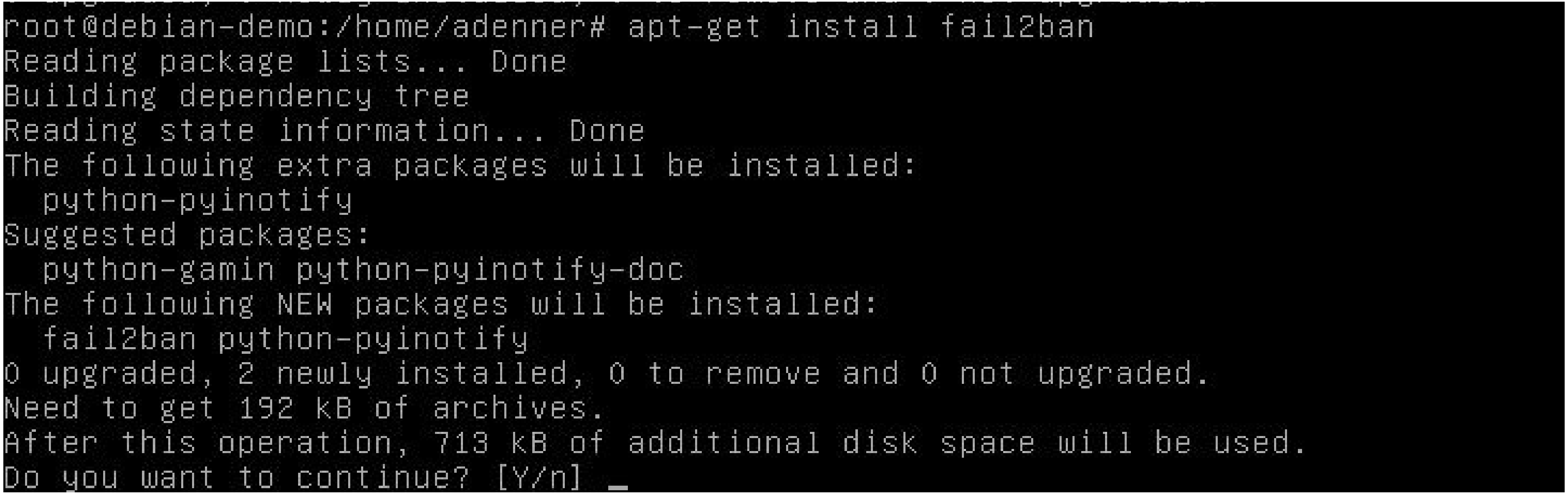
```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
adenner@debian-demo:~$ su
Password:
root@debian-demo:/home/adenner# apt-get update
Ign http://debian.cse.msu.edu jessie InRelease
Hit http://security.debian.org jessie/updates InRelease
Hit http://debian.cse.msu.edu jessie-updates InRelease
Hit http://debian.cse.msu.edu jessie Release.gpg
Hit http://debian.cse.msu.edu jessie Release
Hit http://security.debian.org jessie/updates/main Sources
Hit http://security.debian.org jessie/updates/main amd64 Packages
Hit http://debian.cse.msu.edu jessie-updates/main Sources
Hit http://security.debian.org jessie/updates/main Translation-en
Get:1 http://debian.cse.msu.edu jessie-updates/main amd64 Packages/DiffIndex [6,
916 B]
Get:2 http://debian.cse.msu.edu jessie-updates/main Translation-en/DiffIndex [2,
704 B]
Hit http://debian.cse.msu.edu jessie/main Sources
Hit http://debian.cse.msu.edu jessie/main amd64 Packages
Hit http://debian.cse.msu.edu jessie/main Translation-en
Fetched 9,620 B in 2s (3,894 B/s)
Reading package lists... Done
root@debian-demo:/home/adenner# _
```



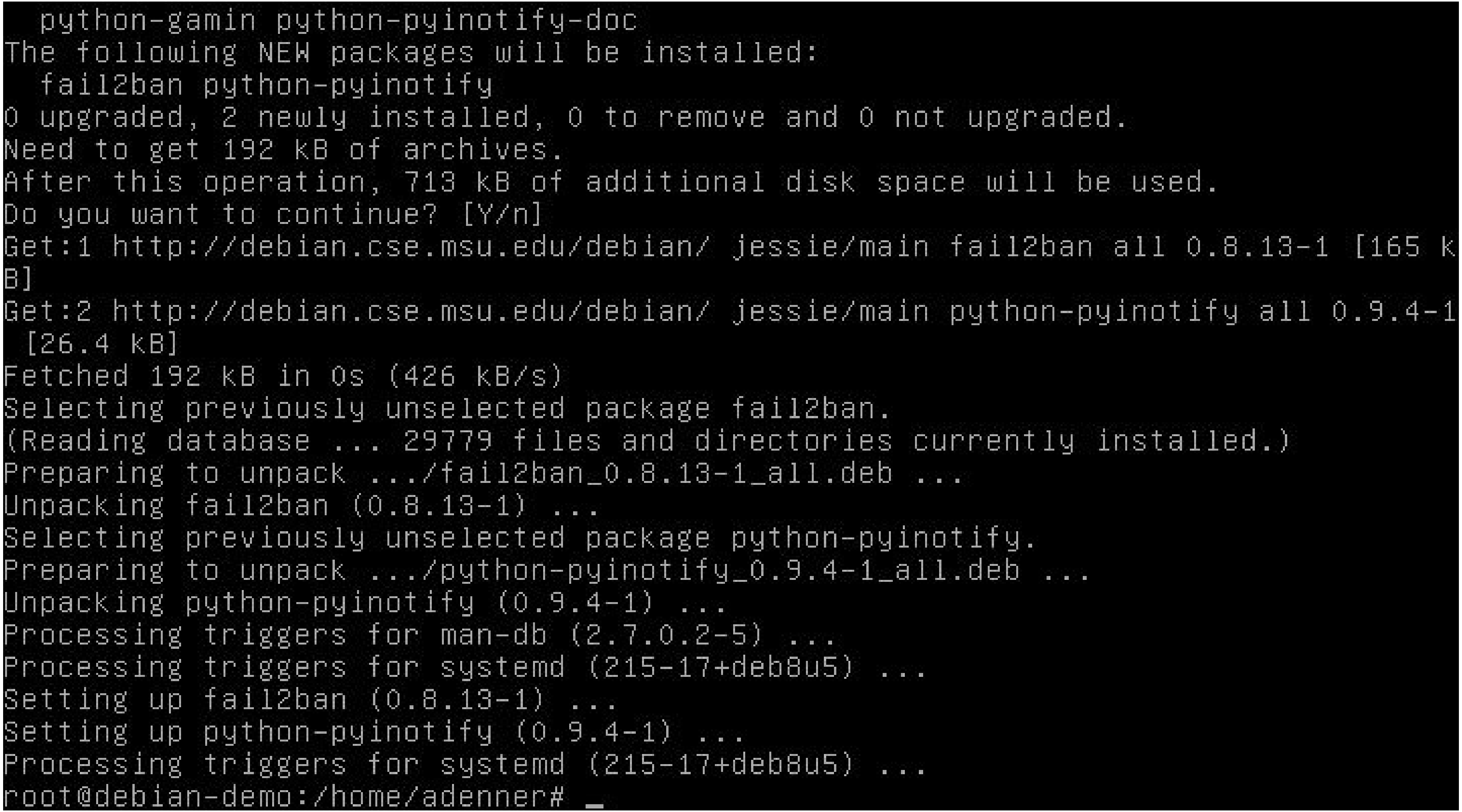
```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
adenner@debian-demo:~$ su
Password:
root@debian-demo:/home/adenner# apt-get update
Ign http://debian.cse.msu.edu jessie InRelease
Hit http://security.debian.org jessie/updates InRelease
Hit http://debian.cse.msu.edu jessie-updates InRelease
Hit http://debian.cse.msu.edu jessie Release.gpg
Hit http://debian.cse.msu.edu jessie Release
Hit http://security.debian.org jessie/updates/main Sources
Hit http://security.debian.org jessie/updates/main amd64 Packages
Hit http://debian.cse.msu.edu jessie-updates/main Sources
Hit http://security.debian.org jessie/updates/main Translation-en
Get:1 http://debian.cse.msu.edu jessie-updates/main amd64 Packages/DiffIndex [6,
916 B]
Get:2 http://debian.cse.msu.edu jessie-updates/main Translation-en/DiffIndex [2,
704 B]
Hit http://debian.cse.msu.edu jessie/main Sources
Hit http://debian.cse.msu.edu jessie/main amd64 Packages
Hit http://debian.cse.msu.edu jessie/main Translation-en
Fetched 9,620 B in 2s (3,894 B/s)
Reading package lists... Done
root@debian-demo:/home/adenner# apt-get dist-upgrade_
```



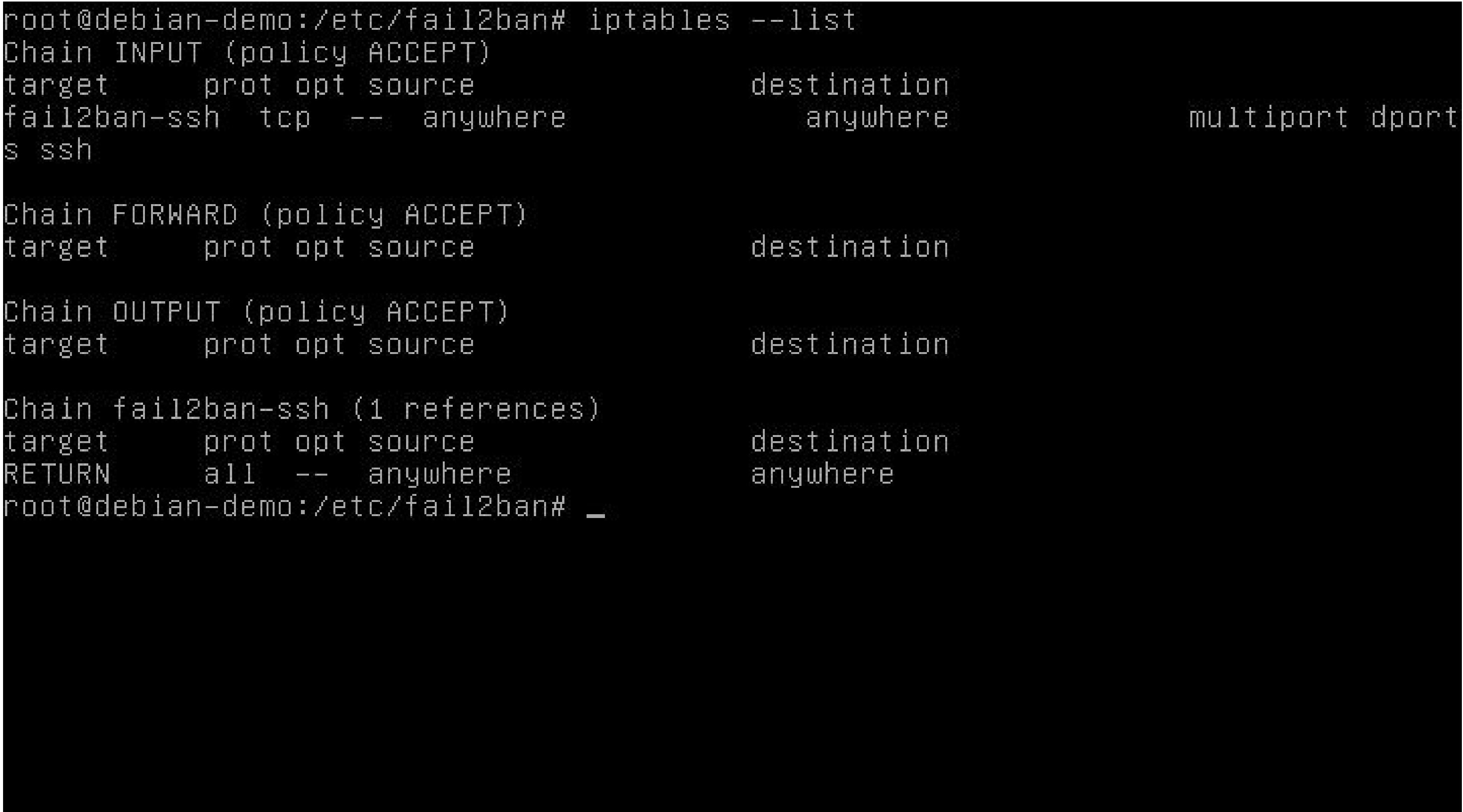
```
Ign http://debian.cse.msu.edu jessie InRelease
Hit http://security.debian.org jessie/updates InRelease
Hit http://debian.cse.msu.edu jessie-updates InRelease
Hit http://debian.cse.msu.edu jessie Release.gpg
Hit http://debian.cse.msu.edu jessie Release
Hit http://security.debian.org jessie/updates/main Sources
Hit http://security.debian.org jessie/updates/main amd64 Packages
Hit http://debian.cse.msu.edu jessie-updates/main Sources
Hit http://security.debian.org jessie/updates/main Translation-en
Get:1 http://debian.cse.msu.edu jessie-updates/main amd64 Packages/DiffIndex [6,
916 B]
Get:2 http://debian.cse.msu.edu jessie-updates/main Translation-en/DiffIndex [2,
704 B]
Hit http://debian.cse.msu.edu jessie/main Sources
Hit http://debian.cse.msu.edu jessie/main amd64 Packages
Hit http://debian.cse.msu.edu jessie/main Translation-en
Fetched 9,620 B in 2s (3,894 B/s)
Reading package lists... Done
root@debian-demo:/home/adenner# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@debian-demo:/home/adenner# _
```



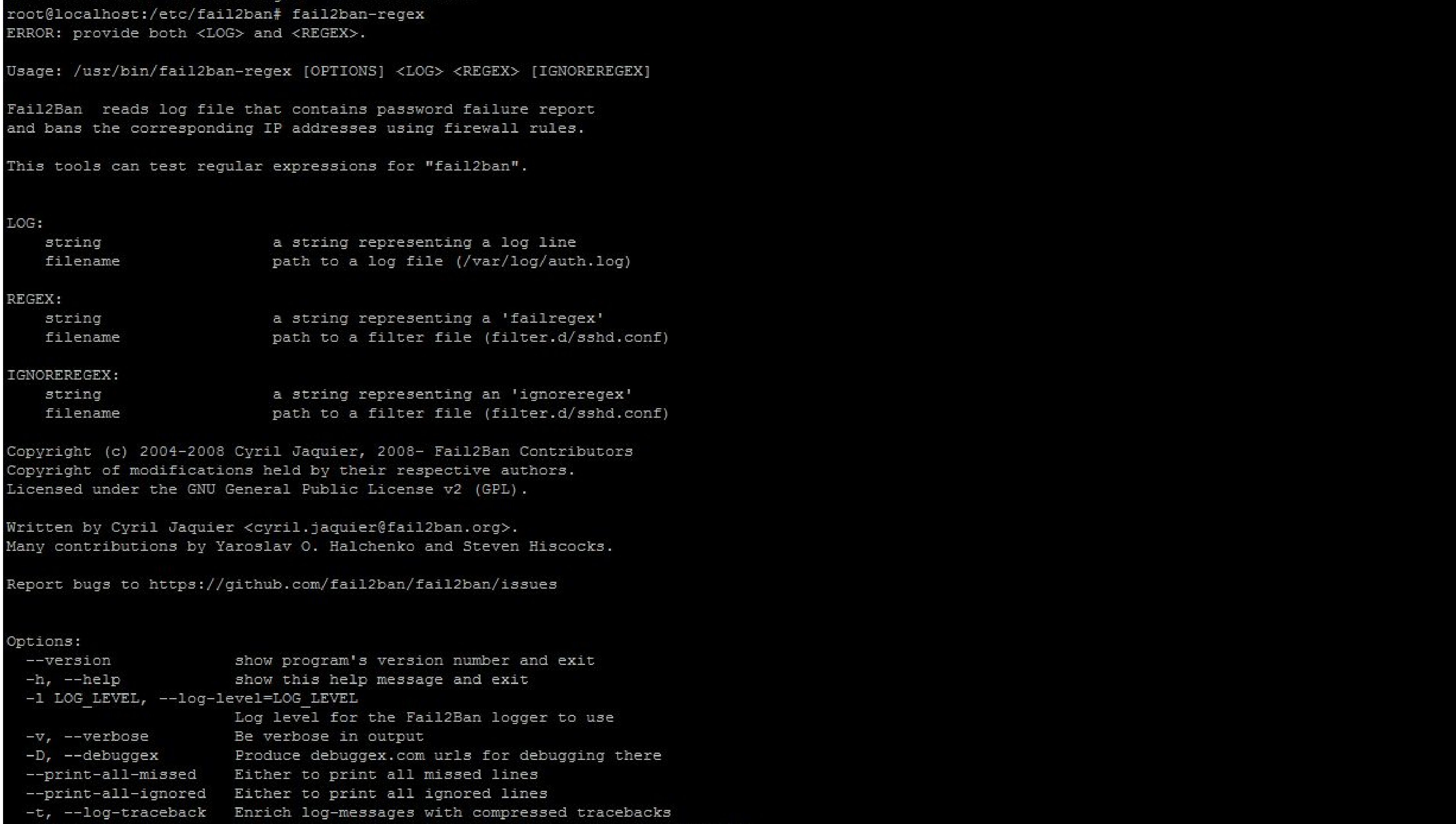
```
root@debian-demo:/home/adenner# apt-get install fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  python-pyinotify
Suggested packages:
  python-gamin python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python-pyinotify
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 192 kB of archives.
After this operation, 713 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
```



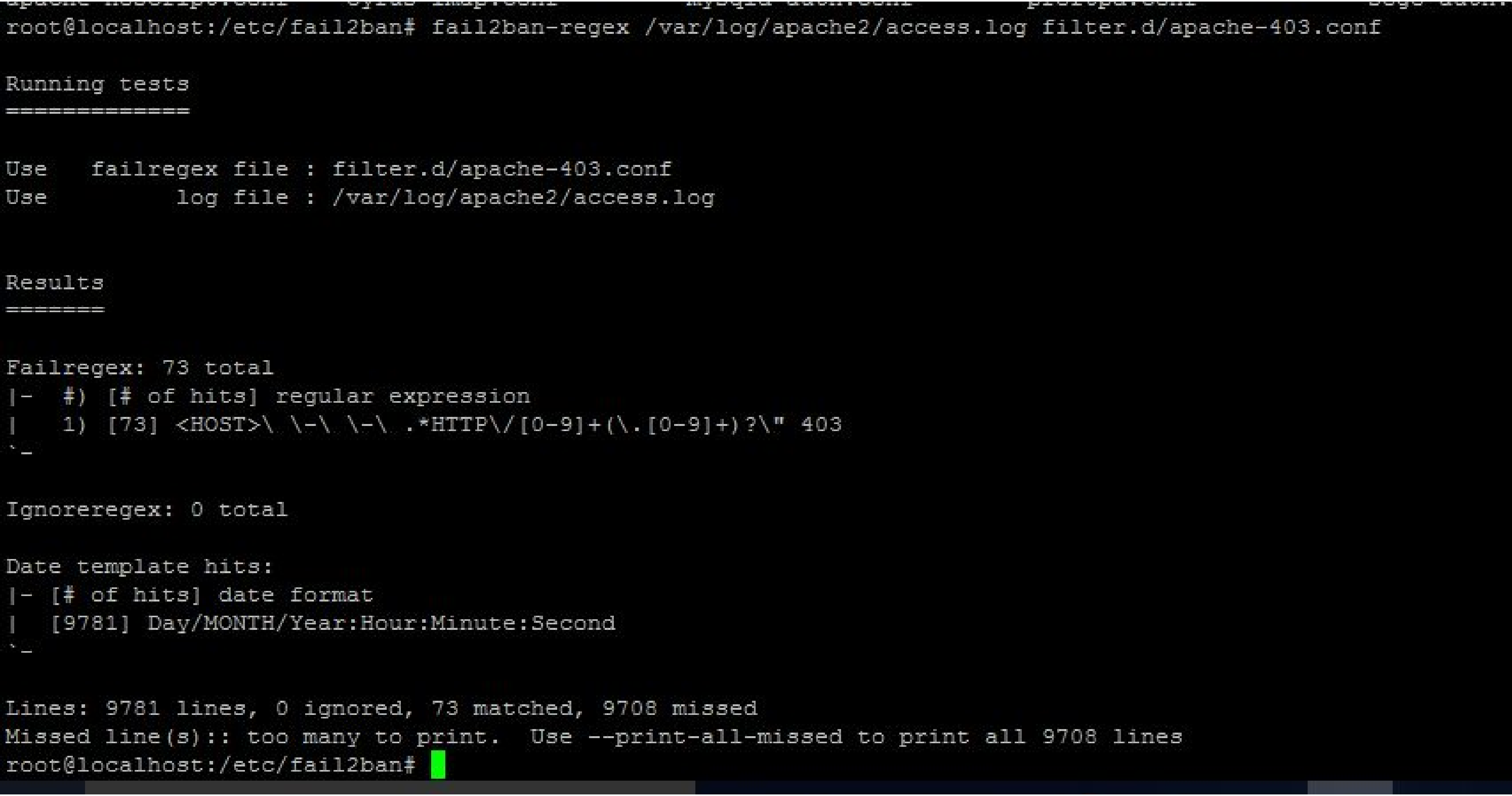
```
  python-gamin python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python-pyinotify
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 192 kB of archives.
After this operation, 713 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://debian.cse.msu.edu/debian/ jessie/main fail2ban all 0.8.13-1 [165 k
B]
Get:2 http://debian.cse.msu.edu/debian/ jessie/main python-pyinotify all 0.9.4-1
 [26.4 kB]
Fetched 192 kB in 0s (426 kB/s)
Selecting previously unselected package fail2ban.
(Reading database ... 29779 files and directories currently installed.)
Preparing to unpack .../fail2ban_0.8.13-1_all.deb ...
Unpacking fail2ban (0.8.13-1) ...
Selecting previously unselected package python-pyinotify.
Preparing to unpack .../python-pyinotify_0.9.4-1_all.deb ...
Unpacking python-pyinotify (0.9.4-1) ...
Processing triggers for man-db (2.7.0.2-5) ...
Processing triggers for systemd (215-17+deb8u5) ...
Setting up fail2ban (0.8.13-1) ...
Setting up python-pyinotify (0.9.4-1) ...
Processing triggers for systemd (215-17+deb8u5) ...
root@debian-demo:/home/adenner# _
```



```
root@debian-demo:/etc/fail2ban# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
fail2ban-ssh  tcp  --  anywhere             anywhere             multiport dport
s ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain fail2ban-ssh (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
root@debian-demo:/etc/fail2ban# _
```



```
root@localhost:/etc/fail2ban# fail2ban-regex
ERROR: provide both <LOG> and <REGEX>.

Usage: /usr/bin/fail2ban-regex [OPTIONS] <LOG> <REGEX> [IGNOREREGEX]

Fail2Ban  reads log file that contains password failure report
and bans the corresponding IP addresses using firewall rules.

This tools can test regular expressions for "fail2ban".



LOG:
    string                  a string representing a log line
    filename                path to a log file (/var/log/auth.log)

REGEX:
    string                  a string representing a 'failregex'
    filename                path to a filter file (filter.d/sshd.conf)

IGNOREREGEX:
    string                  a string representing an 'ignoreregex'
    filename                path to a filter file (filter.d/sshd.conf)

Copyright (c) 2004-2008 Cyril Jaquier, 2008- Fail2Ban Contributors
Copyright of modifications held by their respective authors.
Licensed under the GNU General Public License v2 (GPL).

Written by Cyril Jaquier <cyril.jaquier@fail2ban.org>.
Many contributions by Yaroslav O. Halchenko and Steven Hiscocks.

Report bugs to https://github.com/fail2ban/fail2ban/issues



Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -l LOG_LEVEL, --log-level=LOG_LEVEL
                        Log level for the Fail2Ban logger to use
  -v, --verbose         Be verbose in output
  -D, --debuggex        Produce debuggex.com urls for debugging there
  --print-all-missed    Either to print all missed lines
  --print-all-ignored   Either to print all ignored lines
  -t, --log-traceback   Enrich log-messages with compressed tracebacks
```



```
root@localhost:/etc/fail2ban# fail2ban-regex /var/log/apache2/access.log filter.d/apache-403.conf

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

Use   failregex file : filter.d/apache-403.conf
Use         log file : /var/log/apache2/access.log


Results
=======

Failregex: 73 total
|-  #) [# of hits] regular expression
|   1) [73] <HOST>\ \-\ \-\ .*HTTP\/[0-9]+(\.[0-9]+)?\" 403
`-

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
|  [9781] Day/MONTH/Year:Hour:Minute:Second
`-

Lines: 9781 lines, 0 ignored, 73 matched, 9708 missed
Missed line(s):: too many to print.  Use --print-all-missed to print all 9708 lines
root@localhost:/etc/fail2ban#
```

Resources

http://www.fail2ban.org

https://www.slightfuture.com/security/fail2ban-ipv6

https://www.netfilter.org/

https://httpd.apache.org/docs/1.3/logs.html