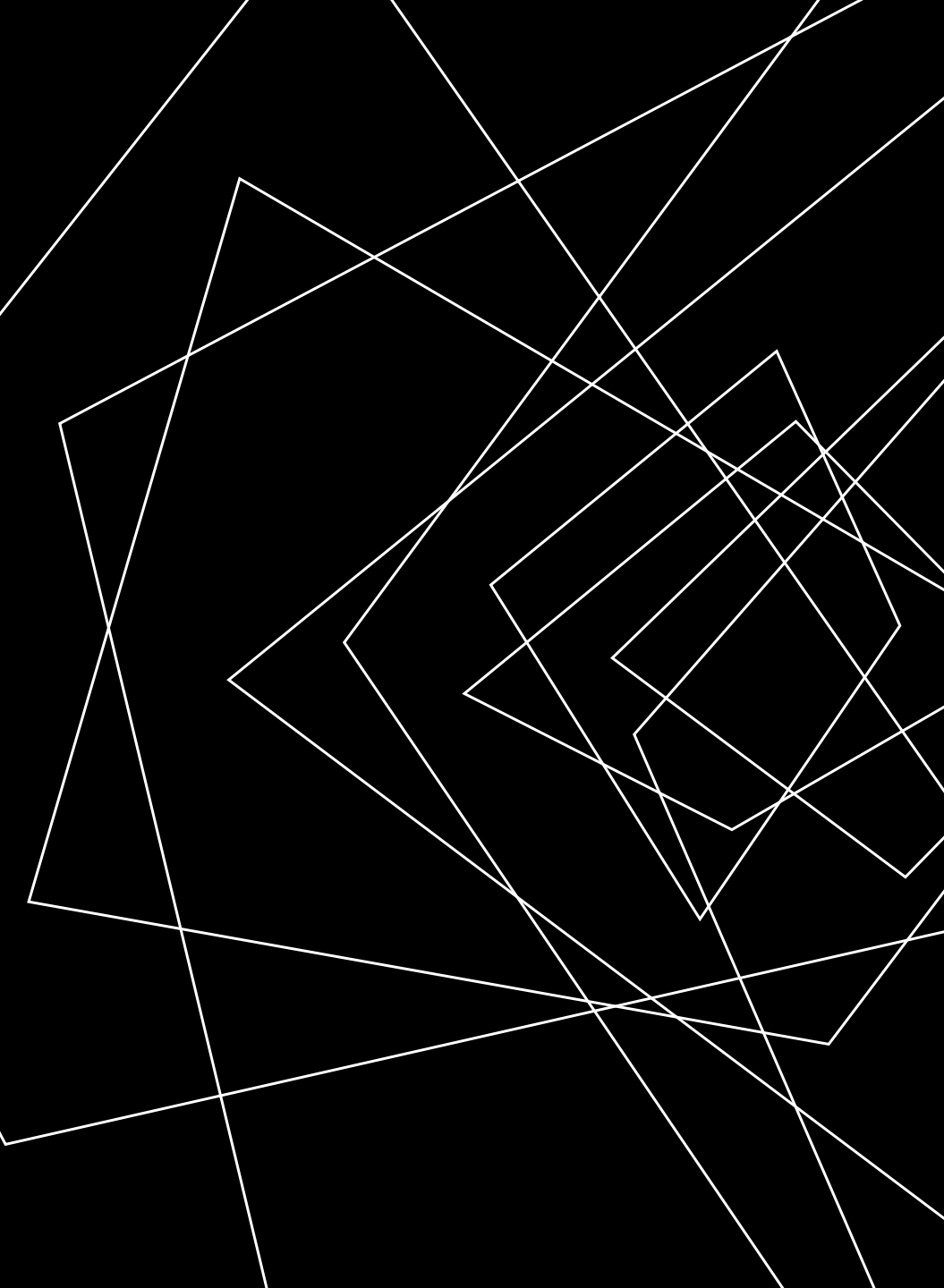


FAIL2BAN

Emrecañ Atlıhan

FAIL2BAN NEDİR?

Fail2Ban, belirli log dosyalarındaki şüpheli etkinlikleri tespit eden ve belirli koşullara dayalı olarak bu etkinliklerin gerçekleştiren IP adreslerini geçici olarak engelleyen bir güvenlik aracıdır. Genellikle, **brute force** saldırıları, **sisteme giriş** denemeleri, **doS/DDoS saldırıları**, **kimlik doğrulama hataları** gibi durumu izler.



LOG DOSYASI
İZLEME

Fail2Ban, sunucuların log dosyalarını (örneğin /var/log/auth.log, /var/log/nginx/error.log) izler.

REGEX TABANLI
FİLTRELEME:

Bir olay meydana geldiğinde (örneğin bir kullanıcı başarısız giriş yaparsa), Fail2Ban bu olayı regex (regular expressions) kullanarak tespit eder.

BANLAMA

Eğer bir IP, belirli bir sayıda hatalı giriş denemesi yaparsa, Fail2Ban bu IP'yi bir süreliğine (örneğin 10 dakika) banlar.

IP ENGELLEME

Banlanan IP'ler, ağ seviyesinde engellenir (IPtables veya FirewallD kullanılarak).

FAIL2BAN BİLEŞENLERİ

Filter (Filtreler)

Fail2Ban, log dosyasındaki hatalı girişleri tespit etmek için filtreler kullanır.

Filtreler, log dosyalarındaki belirli desenleri (regex) arar.

Jails

Jail, Fail2Ban'in güvenlik önlemi olarak IP'yi banlama kararını verdiği yapıdır.

Jail belirli bir servis için filtreyi uygular ve hata arar.

Actions

Banlama eylemi genellikle IP adreslerinin engellenmesini içerir.

KURULUM

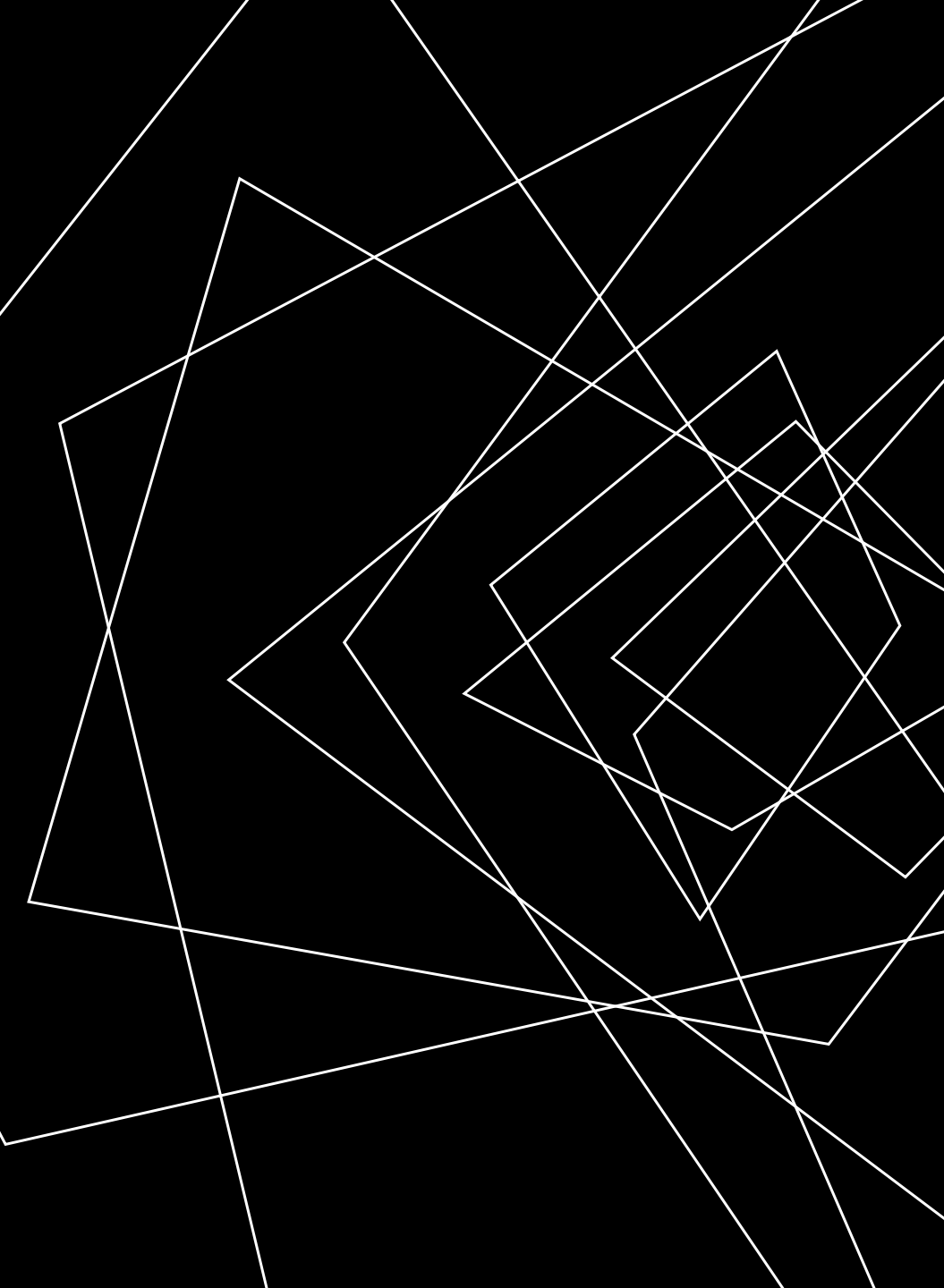
Apt install fail2ban yeterli olacaktır.

Bunun dışında fail2ban herhangi bir ban atılması durumunda mail atma hizmetine de sahiptir bunun için Postfix, Exim veya **Sendmail** gibi **SMTP** sunucusu çeşit gerekir. Aşağıdaki komutu kullanarak kendiniz Postfix indirebilirsiniz.

Apt-get install postfix -y

KONFIGÜRASYON

Konfigürasyon kısmında jail.conf karşımıza çıkar fakat ana dosyayı bozmamak için bunu kopyalayıp jail.local şeklinde kaydetmek en iyisi olacaktır. Dosyanın içinde yazanlar aslında bize bir nevi yol göstericidir. Filtrelerin hazırlanışı ve kullanılan terimler hakkında bize bilgi verirler. Bu bilgiler nelerdir peki?



KONFIGÜRASYON

ignoreip: Bu listedeki bir adres veya adresler için fail2ban kısıtlamaları etkilenmeyecektir. İlgili alanda *CIDR Netmask* veya tek *IP* eklenebilir.

bantime: Fail2ban tarafından engellenen IP için saniye cinsinden ne kadar bloke kalacağını belirten alandır. Varsayılan 600 saniyedir (10 dakika)

maxretry: Maksimum kaç başarısız işlem'den sonra “*bantime*” süresi kadar erişimin kısıtlanacağını tanımlandığı alandır. Varsayılan “3” olarak ayarlıdır.

destemail: Fail2ban işlemleri ile ilgili uyarıların gönderileceği e-postanın tanımlandığı alandır.

logpath: Fail2ban 'ın dikkate alacağı servisin log dosyasıdır.

```
# "bantime" is the amount of time that a host is banned, integer in seconds or
# time abbreviation format (m - minutes, h - hours, d - days, w - weeks, mo - months, y - years).
# This is to consider as an initial time if bantime.increment gets enabled.
bantime = 10m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 10m

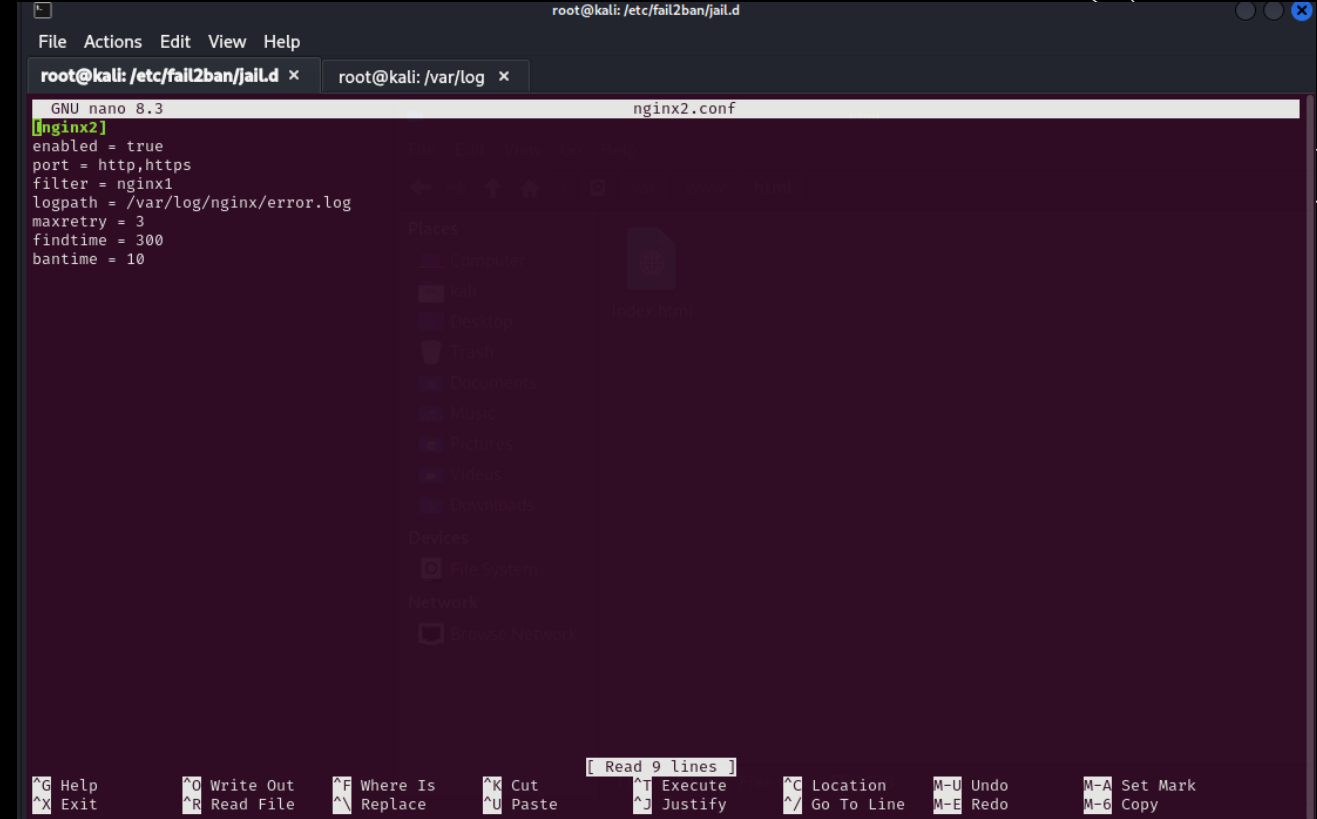
# "maxretry" is the number of failures before a host get banned.
maxretry = 5

# "maxmatches" is the number of matches stored in ticket (resolvable via tag <matches> in actions).
maxmatches = %(maxretry)s

# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "polling", "systemd" and "auto".
# This option can be overridden in each jail as well.
#
```

ÖRNEK BİR .CONF DOSYASI

Burda nginx brute force tespiti ile ilgili bir konfigürasyon dosyası var. Geçen sayfa olup burda olmayan şey ise filter. Kendiliğinden gelen filtreler olsa bile log örneğine bakarak filtre oluşturmak asıl nokta burada. Tabiki de işe yaramaz diyemeyiz fakat bu nokta konfigürasyon yapılırken unutulmamalı.



The screenshot shows a terminal window with the title bar "root@kali: /etc/fail2ban/jail.d". The window contains a nano editor editing the file "nginx2.conf". The configuration file content is as follows:

```
enabled = true
port = http,https
filter = nginx1
logpath = /var/log/nginx/error.log
maxretry = 3
findtime = 300
bantime = 10
```

The nano editor interface includes a menu bar at the top with "File", "Actions", "Edit", "View", and "Help". Below the menu bar, there are two tabs: "root@kali: /etc/fail2ban/jail.d" and "root@kali: /var/log". The nano editor status bar at the bottom shows various keyboard shortcuts: ^G Help, ^X Exit, ^O Write Out, ^R Read File, ^F Where Is, ^N Replace, ^K Cut, ^U Paste, ^T Execute, ^J Justify, ^C Location, ^_ Go To Line, M-U Undo, M-E Redo, M-A Set Mark, and M-6 Copy. A small tooltip "Read 9 lines" is visible over the "Execute" and "Justify" shortcuts.

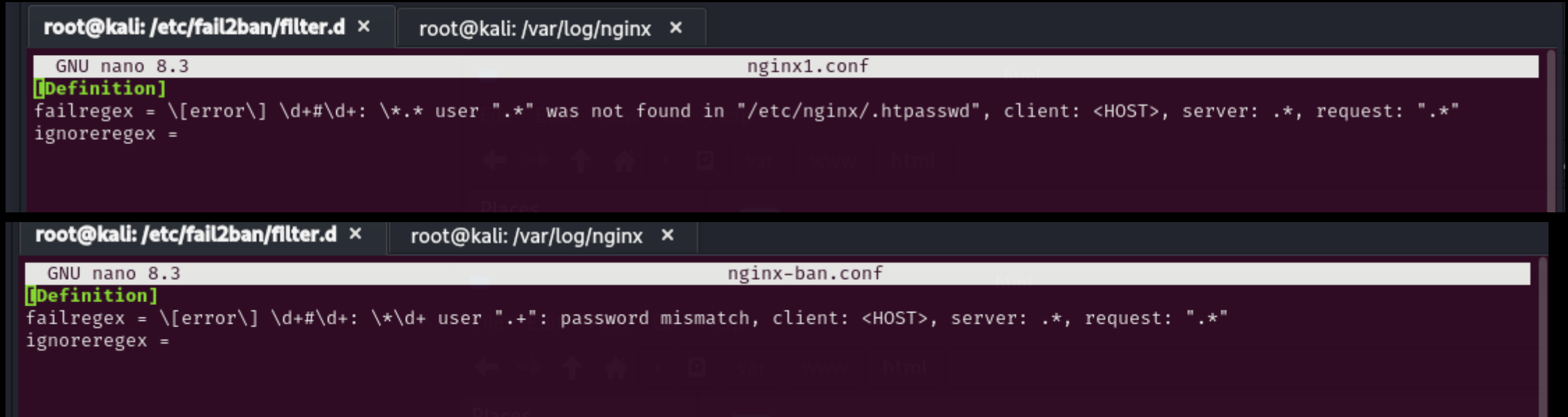
ÖRNEK BİR FİLTRE DOSYASI NASIL OLMALI

Aşağı tarafta yanlış giriş yapıldığında düşen filtreleri görmektesiniz. Diğer sayfada da oluşturulan filtreleri göstereceğim.

```
2025/03/28 23:25:25 [error] 25376#25376: *2 open() "/var/www/html/favicon.ico" failed (2: No such file or directory), client: 192.168.6.158, server: localhost
2025/03/28 23:30:08 [error] 29150#29150: *1 user "a" was not found in "/etc/nginx/.htpasswd", client: 192.168.6.158, server: localhost
2025/03/28 23:33:26 [error] 29152#29152: *3 user "a" was not found in "/etc/nginx/.htpasswd", client: 192.168.6.158, server: localhost
2025/03/28 23:33:28 [error] 29152#29152: *3 user "a" was not found in "/etc/nginx/.htpasswd", client: 192.168.6.158, server: localhost
2025/03/28 23:33:30 [error] 29152#29152: *3 user "a" was not found in "/etc/nginx/.htpasswd", client: 192.168.6.158, server: localhost
2025/03/28 23:33:32 [error] 29152#29152: *3 user "a" was not found in "/etc/nginx/.htpasswd", client: 192.168.6.158, server: localhost
2025/03/28 23:33:33 [error] 29152#29152: *3 user "a" was not found in "/etc/nginx/.htpasswd", client: 192.168.6.158, server: localhost
2025/03/28 23:33:36 [error] 29152#29152: *3 user "a" was not found in "/etc/nginx/.htpasswd", client: 192.168.6.158, server: localhost
2025/03/28 23:34:45 [error] 29150#29150: *5 user "altay": password mismatch, client: 192.168.6.158, server: localhost, request: "GET /"
2025/03/28 23:34:48 [error] 29150#29150: *5 user "altay": password mismatch, client: 192.168.6.158, server: localhost, request: "GET /"
2025/03/28 23:34:51 [error] 29150#29150: *5 user "altay": password mismatch, client: 192.168.6.158, server: localhost, request: "GET /"
2025/03/28 23:34:56 [error] 29150#29150: *5 user "altay": password mismatch, client: 192.168.6.158, server: localhost, request: "GET /"
2025/03/28 23:35:28 [error] 29150#29150: *5 user "altay": password mismatch, client: 192.168.6.158, server: localhost, request: "GET /"
2025/03/28 23:35:55 [error] 29150#29150: *7 user "altay a" was not found in "/etc/nginx/.htpasswd", client: 192.168.6.158, server: localhost
2025/03/28 23:40:54 [error] 29150#29150: *8 user "a" was not found in "/etc/nginx/.htpasswd", client: 192.168.6.158, server: localhost
```

Bir önceki sayfada oluşan aslında 2 tip log vardı.

1. Kullanıcı adı yanlış olan giriş denemesi
2. Kullanıcı doğru fakat şifresi yanlış olan giriş denemesi.



```
root@kali: /etc/fail2ban/filter.d x root@kali: /var/log/nginx x
GNU nano 8.3 nginx1.conf
[Definition]
failregex = \[error\] \d+\d+: \*.~ user ".~" was not found in "/etc/nginx/.htpasswd", client: <HOST>, server: .~, request: ".~"
ignoreregex =

root@kali: /etc/fail2ban/filter.d x root@kali: /var/log/nginx x
GNU nano 8.3 nginx-ban.conf
[Definition]
failregex = \[error\] \d+\d+: \*\d+ user ".+": password mismatch, client: <HOST>, server: .~, request: ".~"
ignoreregex =
```

SORUNLAR VE ÇÖZÜM OLABİLECEKLER

Saldırganlar her zaman aynı IP den saldırmazlar. Hatta saldırı yapıldıktan sonra genelde raporlarda IP'ler kiralık sunucu çıkar. Peki bunu önlemi alınabilir mi? Bunun için yapılması gereken abuseIP den api olarak kontrol etmektir.

FTP Brute-Force	Port Scan	Hacking	Brute-Force	Bad Web Bot	SSH	Web App Attack
5	14	15	18	19	22	21

SORUNLAR VE ÇÖZÜM OLABİLECEKLER

