Monitoring Penggunaan CPU Server

1. Monitoring dilakukan menggunakan webmin. diperoleh penggunakan CPU server berlebihan (96%)

dari hasil **ps aux | grep php** diketahui adalah:

www-data 912356 99.6 0.1 85792 25116 ? R 05:51 247:50 php /tmp/.sessions/.L3Zhci93d3cvaHRtbC9wcmVzZW5zaS1hcGkvLmdpdC9pbmZvZXJyb3JfNDA0LWhhbmRsZXI=
www-data 912364 99.6 0.1 85792 25032 ? R 05:51 247:49 php /tmp/.sessions/.L3Zhci93d3cvaHRtbC9wcmVzZW5zaS1hcGkvLmdpdC9pbmZvZXJyb3JfNDA0LWhhbmRsZXI=
www-data 912372 99.6 0.1 85792 25124 ? R 05:51 247:48 php /tmp/.sessions/.L3Zhci93d3cvaHRtbC9wcmVzZW5zaS1hcGkvLmdpdC9pbmZvZXJyb3JfNDA0LWhhbmRsZXI=
www-data 912378 99.8 0.1 85792 25044 ? R 05:53 246:47 php /tmp/.sessions/.L3Zhci93d3cvaHRtbC9wcmVzZW5zaS1hcGkvdmVuZG9yL2ZydWl0Y2FrZS9waHAtY29ycy9zcmMvRXhjZXB0aW9uc2Vycm9yXzQwNC1oYW5kbGVy
www-data 912386 99.8 0.1 85792 25048 ? R 05:53 246:46 php /tmp/.sessions/.L3Zhci93d3cvaHRtbC9wcmVzZW5zaS1hcGkvdmVuZG9yL2ZydWl0Y2FrZS9waHAtY29ycy9zcmMvRXhjZXB0aW9uc2Vycm9yXzQwNC1oYW5kbGVy
www-data 912395 99.8 0.1 85792 25144 ? R 06:03 236:04 php /tmp/.sessions/.L3Zhci93d3cvaHRtbC9wcmVzZW5zaS1hcGkvdmVuZG9yL3JhbXNleS91dWlkL3NyYy9HZW5lcmF0b3JlcnJvcl80MDQtaGFuZGxlcg==
www-data 912403 99.8 0.1 85792 25340 ? R 06:03 236:04 php /tmp/.sessions/.L3Zhci93d3cvaHRtbC9wcmVzZW5zaS1hcGkvdmVuZG9yL3JhbXNleS91dWlkL3NyYy9HZW5lcmF0b3JlcnJvcl80MDQtaGFuZGxlcg==

setelah dilakukan pengecekan pada salah satu file tmp sessions tersebut

sudo cat /tmp/.sessions/.L3Zhci93d3cvaHRtbC9wcmVzZW5zaS1hcGkvdmVuZG9yL2ZydWl0Y2FrZS9waHAtY29ycy9zcmMvRXhjZXB0aW9uc2Vycm9yXzQwNC1oYW5kbGVy

melakukan akses terhadap file error_404.php dimana file tersebut adalah backdoor yang ditanamkan untuk menyisipkan coding lain pada website.

lalu kill sesuai PID nya

sudo kill -9 912356
sudo kill -9 912364
sudo kill -9 912372
sudo kill -9 912378
sudo kill -9 912386
sudo kill -9 912395
sudo kill -9 912403

Hasilnya CPU server normal kembali

2. Pemeriksaan Terhadap File Mencurigakan

Kata kunci: **error_404.php**, **.htaccess**, **html**
cari file tersebut pada lokasi yang **folder public**, **vendor** dan **system** dimana seharusnya file tersebut tidak seharusnya berada di lokasi tersebut.

cek rutin **tail -f /var/log/apache2/error.log**
untuk memantau aktivitas ip yang mengakses server mencurigakan.
lakukan blok ip tersebut jika fail2ban tidak mendeteksinya, dengan cara:

1. Blok IP dengan IPTABLES

untuk tambah ip yang diblok
sudo iptables -A INPUT -s 36.70.12.0/24 -j DROP

untuk menghapus ip yang diblok
sudo iptables -D INPUT -s 36.70.12.0/24 -j DROP

untuk menghapus ip yang diblok dalam daftar
contoh:
5 DROP all -- 192.168.1.100 0.0.0.0/0
7 DROP all -- 203.0.113.45 0.0.0.0/0
sudo iptables -D INPUT 7
sudo iptables -D INPUT 5

untuk melihat ip yang sudah diblok
sudo iptables -L INPUT -n
sudo iptables -L -n
sudo iptables -L INPUT -n --line-numbers | grep DROP

2. Blok IP dengan UFW

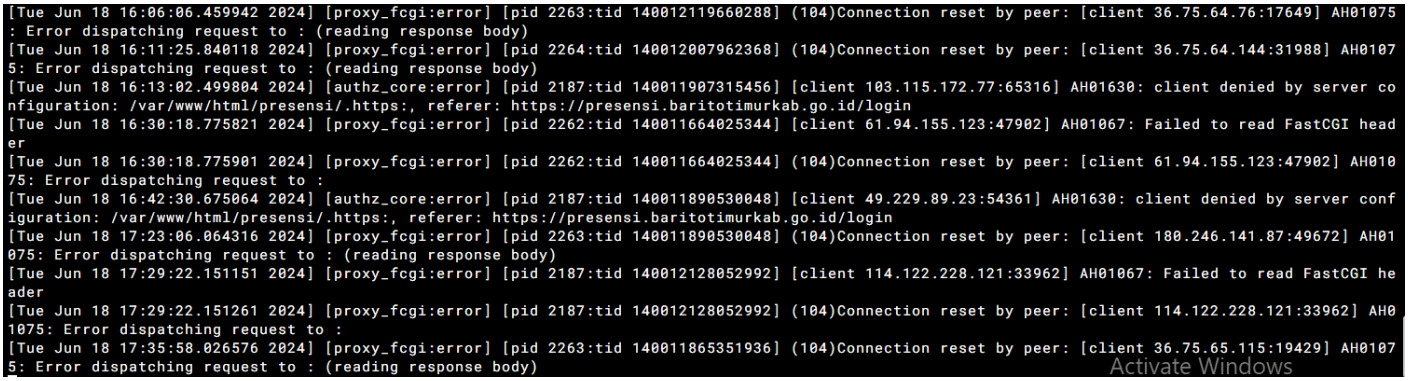
untuk tambah ip yang diblok
ufw deny from 36.70.12.0/24

untuk menghapus ip yang diblok
ufw status numbered
ufw delete <number>

untuk melihat ip yang sudah diblok
ufw status

3. Pemeriksaan Terhadap Log Apache

tail -f /var/log/apache2/error.log ditemukan koneksi seperti gambar berikut:



dari log diatas akses yang tidak normal adalah:
[Tue Jun 18 16:42:30.675064 2024] [authz_core:error] [pid 2187:tid 140011890530048] [client 49.229.89.23:54361] AH01630: client denied by server configuration:

/var/www/html/presensi/.https:, referer: https://presensi.baritotimurkab.go.id/login

Jaringan ip 49.229.89.23 wajib diblok:
ufw deny from 349.229.0.0/16

sedangkan, log lain seperti:

[Tue Jun 18 17:35:58.026576 2024] [proxy_fcgi:error] [pid 2263:tid 140011865351936] (104)Connection reset by peer: [client 36.75.65.115:19429] AH01075: Error dispatching request to : (reading response body)
adalah log koneksi normal dimana pengguna sedang mengakses page aplikasi ATEI.

4. Batasi Akses ke bin/sh

Batas ke bin/sh agar pengguna lain selain root tidak bisa mengaksesnya (kemungkinkan pengguna exploit):
chmod 700 /bin/sh

dan menambah rule pada .htaccess pada root web, untuk mencegah metode traversal directoy:
 # Prevent directory traversal attacks
RewriteCond %{REQUEST_URI} \.\. [NC]
RewriteRule ^ - [F]

5. Buat rule untuk serve-cgi-bin.conf

serve-cgi-bin.conf terletak pada /etec/apache2/conf-available. Tambahkan aturan berikut:

```
ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
<Directory "/usr/lib/cgi-bin">
        AllowOverride None
        Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
        Require all granted

        # Menambahkan aturan untuk mencegah serangan traversal direktori
        RewriteEngine On
        RewriteCond %{REQUEST_URI} \.\. [NC]
        RewriteRule ^ - [F]
</Directory>
```

Revisi #16
Dibuat 17 Juni 2024 10:03:53 oleh Friscia Anthony
Diperbaharui 11 Desember 2025 08:22:39 oleh Friscia Anthony