

Nama : Asyrof Hafizh Maulana

Honeypot dan Honeynet

1. Pilih salah satu aplikasi HoneyPot berikut ini untuk Anda praktikkan install dan demonstrasikan cara menggunakannya:

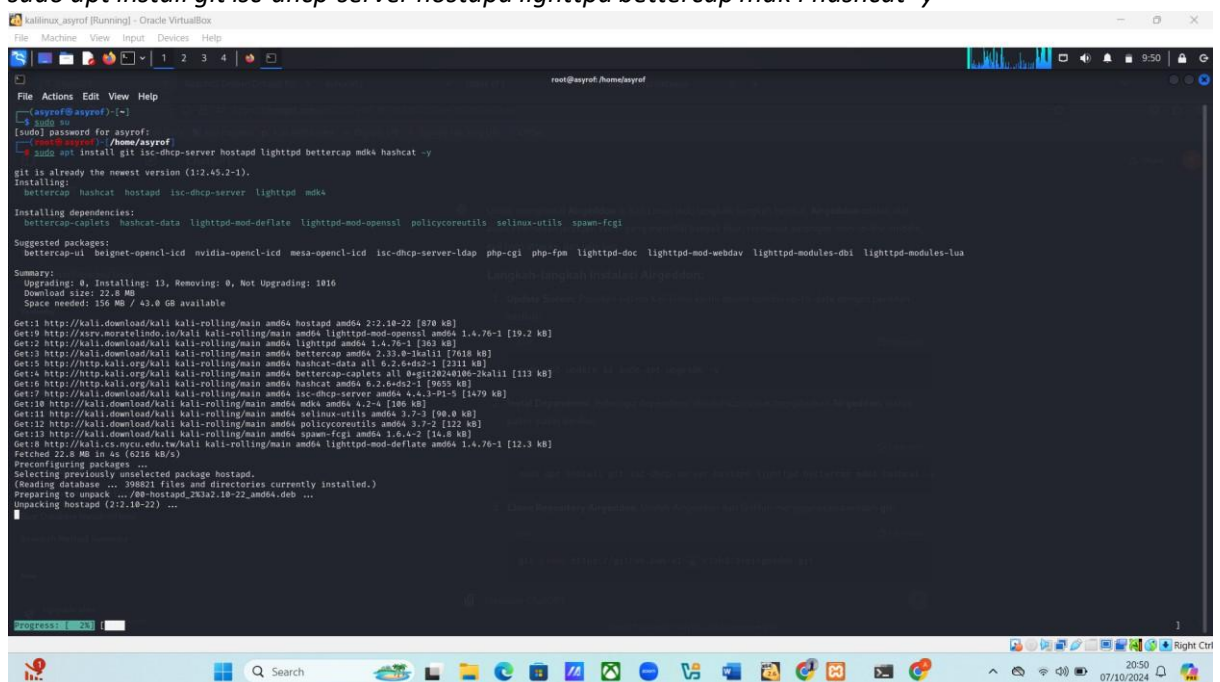
- ghost-usb-honeypot (<https://code.google.com/archive/p/ghost-usb-honeypot/>)
- wordpot (<http://brindi.si/g/projects/wordpot.html>)
- airgeddon (<https://github.com/v1s1t0r1sh3r3/airgeddon/>)

Jelaskan step by step yang anda lakukan untuk instalasi dan menjalankan aplikasi tersebut. Jelaskan masing masing fungsi fitur dan menu yang ada di aplikasi tersebut. Screenshot tiap menu atau hasil yang ingin Anda peroleh saat Instalasi dan menjalankan aplikasi tersebut.

Langkah instalasi airgeddon :

- Update Sistem: Pastikan sistem Kali Linux kamu dalam kondisi up-to-date dengan perintah berikut:
`sudo apt update && sudo apt upgrade -y`
- Instal Dependensi: Beberapa dependensi dibutuhkan untuk menjalankan Airgeddon. Install paket-paket berikut:

`sudo apt install git isc-dhcp-server hostapd lighttpd bettercap mdk4 hashcat -y`



```
root@asyrof:~/home/asyrof
File Actions Edit View Help
[asyrof@asyrof]~$ sudo apt install git isc-dhcp-server hostapd lighttpd bettercap mdk4 hashcat -y
[sudo] password for asyrof:
[sudo] apt install git isc-dhcp-server hostapd lighttpd bettercap mdk4 hashcat -y
git is already the newest version (1:2.45.2-1).
Installing:
bettercap hashcat hostapd isc-dhcp-server lighttpd mdk4
Installing dependencies:
bettercap-caplets hashcat-data lighttpd-mod-deflate lighttpd-mod-openssl polycoreutils selinux-utils spawn-fcgi
Suggested packages:
bettercap-ui bgnet-openssl-icd nvidia-openssl-icd mesa-openssl-icd isc-dhcp-server-ldap php-cgi php-fpm lighttpd-doc lighttpd-mod-webdav lighttpd-modules-dbi lighttpd-modules-lua
Summary:
Upgrading: 0, Installing: 13, Removing: 0, Not Upgrading: 1016
Download size: 22.0 MB
Space needed: 110 MB / 43.0 GB available
Get:0 http://kali.download/kali kali-rolling/main amd64 hostapd amd64 2:2.10-22 [870 kB]
Get:1 http://xrv.moratelindo.io/kali kali-rolling/main amd64 lighttpd-mod-openssl amd64 1.4.76-1 [19.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 lighttpd amd64 1.4.76-1 [363 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 bettercap amd64 2.33.0-3kali1 [7018 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 hashcat amd64 6.2.0-2kali1 [2311 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 hashcat-data all 6.2.0-2kali1 [2311 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 bettercap-caplets all 0git20240100-2kali1 [113 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 hashcat amd64 6.2.0-2kali1 [2311 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 isc-dhcp-server amd64 4.4.3-PI-5 [1479 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 mdk4 amd64 4.2-4 [100 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 selinux-utils amd64 3.7-3 [90.0 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 polycoreutils amd64 3.7-2 [122 kB]
Get:12 http://kali.download/kali kali-rolling/main amd64 spawn-fcgi amd64 1.6.4-2 [14.5 kB]
Get:13 http://kali.cs.nyu.edu.tw/kali kali-rolling/main amd64 lighttpd-mod-deflate amd64 1.4.76-1 [12.3 kB]
Fetched 22.0 MB in 4s (6216 kB/s)
Preconfiguring packages ...
Selecting previously unselected package hostapd.
(Reading database ... 39821 files and directories currently installed.)
Preparing to unpack .../80-hostapd_2k32-10-22_amd64.deb ...
Unpacking hostapd (2:2.10-22) ...
```

- Clone Repository Airgeddon: Unduh Airgeddon dari GitHub menggunakan perintah git:
`git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git`

```
kallinux_asyrof [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@asyrof:/home/asyrof/airgeddon

REMOVING:
hashcat-data polycycoreutils selinux-utills spawn-fcgi

Summary:
Upgrading: 0, Installing: 0, Removing: 4, Not Upgrading: 1016
Freed space: 31.2 MB

(Reading database ... 400683 files and directories currently installed.)
Removing hashcat-data (6.2.6+ds2-1) ...
Removing polycycoreutils (3.7-2) ...
Removing selinux-utills (3.7-3) ...
Removing spawn-fcgi (1.6.4-2) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

root@asyrof:/home/asyrof# git clone https://github.com/vis10r1sh3r3/airgeddon.git
fatal: destination path 'airgeddon' already exists and is not an empty directory.

root@asyrof:/home/asyrof# ls /home/asyrof
Desktop Documents Downloads Music Pictures Public Templates Videos airgeddon

root@asyrof:/home/asyrof# sudo rm -rf /home/asyrof/airgeddon

root@asyrof:/home/asyrof# ls /home/asyrof
Desktop Documents Downloads Music Pictures Public Templates Videos

root@asyrof:/home/asyrof# git clone https://github.com/vis10r1sh3r3/airgeddon.git
Cloning into 'airgeddon' ...
remote: Enumerating objects: 10329, done.
remote: Counting objects: 100% (683/683), done.
remote: Compressing objects: 100% (274/274), done.
remote: Total 10329 (delta 438), reused 648 (delta 406), pack-reused 9646 (from 1)
Receiving objects: 100% (10329/10329), 56.86 MiB | 2.19 MiB/s, done.
Resolving deltas: 100% (6508/6508), done.

root@asyrof:/home/asyrof# cd airgeddon

root@asyrof:/home/asyrof/airgeddon#
```

- Masuk ke Direktori Airgeddon: Setelah meng-clone repositori, masuk ke dalam direktori Airgeddon:
cd airgeddon

```
kallinux_asyrof [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@asyrof:/home/asyrof/airgeddon

REMOVING:
hashcat-data polycycoreutils selinux-utills spawn-fcgi

Summary:
Upgrading: 0, Installing: 0, Removing: 4, Not Upgrading: 1016
Freed space: 31.2 MB

(Reading database ... 400683 files and directories currently installed.)
Removing hashcat-data (6.2.6+ds2-1) ...
Removing polycycoreutils (3.7-2) ...
Removing selinux-utills (3.7-3) ...
Removing spawn-fcgi (1.6.4-2) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

root@asyrof:/home/asyrof# git clone https://github.com/vis10r1sh3r3/airgeddon.git
fatal: destination path 'airgeddon' already exists and is not an empty directory.

root@asyrof:/home/asyrof# ls /home/asyrof
Desktop Documents Downloads Music Pictures Public Templates Videos airgeddon

root@asyrof:/home/asyrof# sudo rm -rf /home/asyrof/airgeddon

root@asyrof:/home/asyrof# git clone https://github.com/vis10r1sh3r3/airgeddon.git
Cloning into 'airgeddon' ...
remote: Enumerating objects: 10329, done.
remote: Counting objects: 100% (683/683), done.
remote: Compressing objects: 100% (274/274), done.
remote: Total 10329 (delta 438), reused 648 (delta 406), pack-reused 9646 (from 1)
Receiving objects: 100% (10329/10329), 56.86 MiB | 2.19 MiB/s, done.
Resolving deltas: 100% (6508/6508), done.

root@asyrof:/home/asyrof# cd airgeddon

root@asyrof:/home/asyrof/airgeddon#
```

- Jalankan Airgeddon: Jalankan skrip Airgeddon dengan perintah berikut:
sudo bash airgeddon.sh

```
root@asyrof:~/home/asyrof/airgeddon

REMOVING:
policycoreutils selinux-utils spam-fcgi

Summary:
Upgrading: 0, Installing: 0, Removing: 4, Not Upgrading: 1016
Freed space: 31.2 MB

(Reading database ... 400683 files and directories currently installed.)
Removing hashcat-data (6.2.6+ds2-1) ...
Removing policycoreutils (3.7-2) ...
Removing selinux-utils (3.7-3) ...
Removing spam-fcgi (1.6.4-2) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

root@asyrof:~/home/asyrof/
# git clone https://github.com/vist0rsh3r3/airgeddon.git
fatal: destination path 'airgeddon' already exists and is not an empty directory.

root@asyrof:~/home/asyrof/
# ls /home/asyrof
Desktop Documents Downloads Music Pictures Public Templates Videos airgeddon

root@asyrof:~/home/asyrof/
# sudo rm -rf /home/asyrof/airgeddon

root@asyrof:~/home/asyrof/
# ls /home/asyrof
Desktop Documents Downloads Music Pictures Public Templates Videos

root@asyrof:~/home/asyrof/
# git clone https://github.com/vist0rsh3r3/airgeddon.git
Cloning into 'airgeddon' ...
remote: Enumerating objects: 10329, done.
remote: Counting objects: 100% (603/603), done.
remote: Compressing objects: 100% (274/274), done.
remote: Total 10329 (delta 430), reused 604 (delta 406), pack-reused 9646 (from 1)
Receiving objects: 100% (10329/10329), 56.86 MiB | 2.19 MiB/s, done.
Resolving deltas: 100% (6500/6500), done.

root@asyrof:~/home/asyrof/
# cd airgeddon

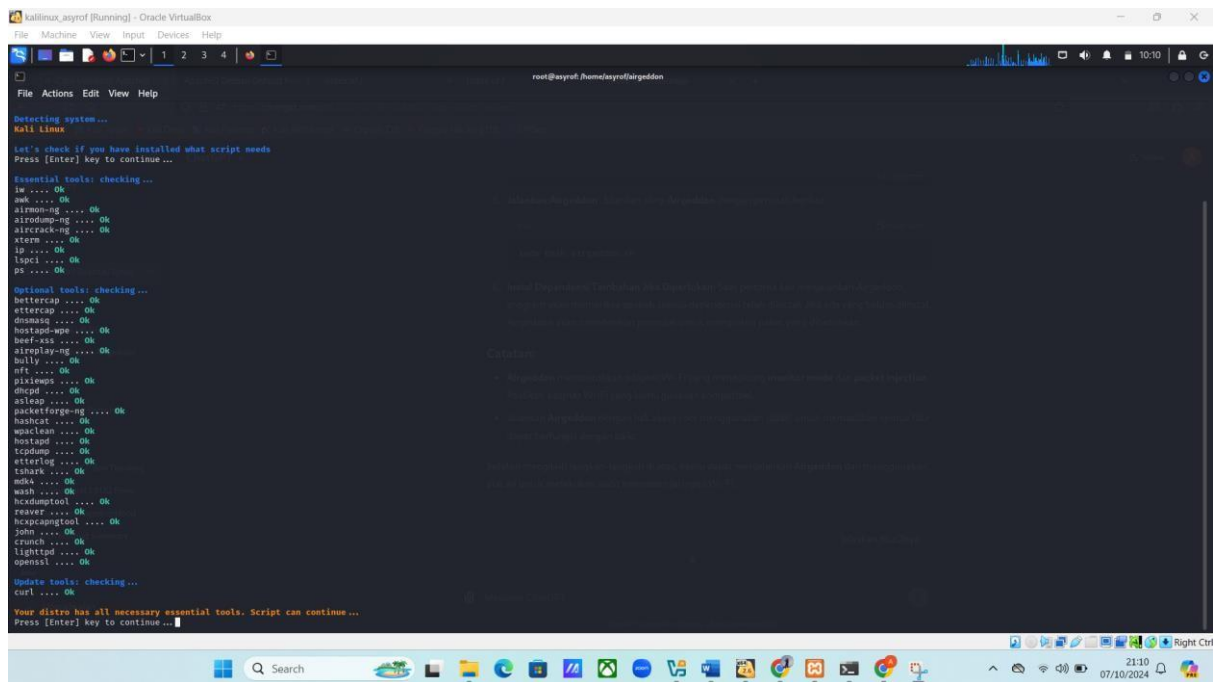
root@asyrof:~/home/asyrof/airgeddon/
# sudo ./airgeddon.sh

***** Welcom *****
Welcome to airgeddon script v11.31

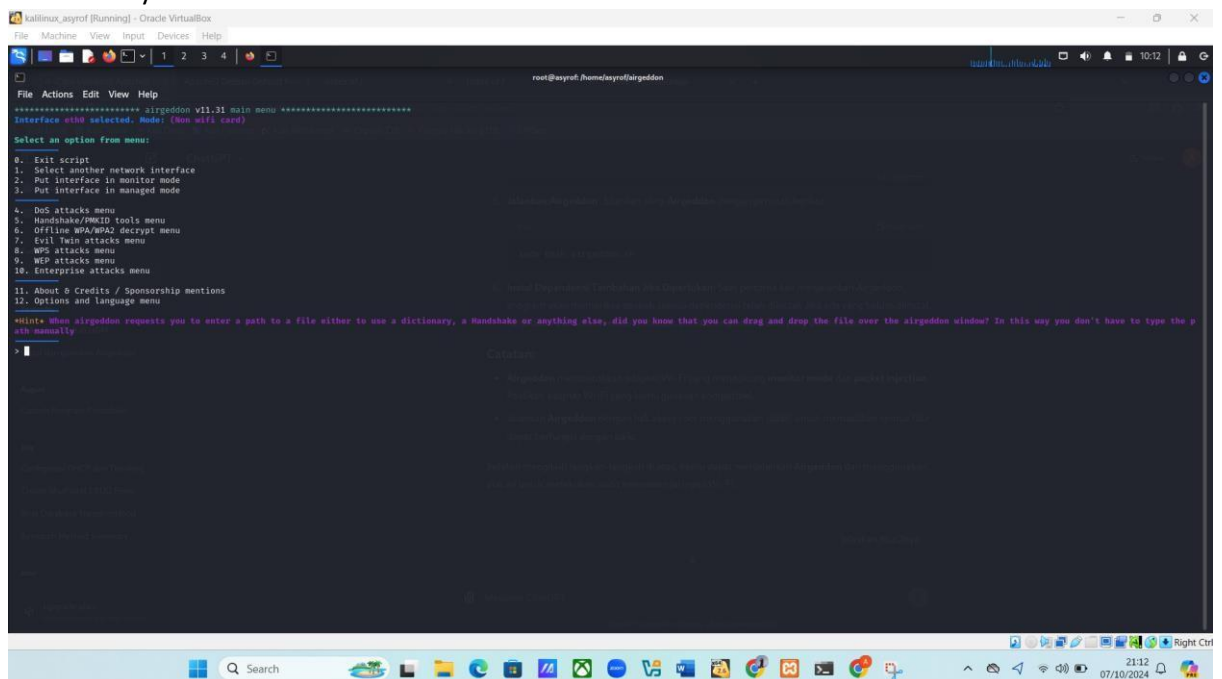
          _____
         /  ____  \
        /  /  __ \
       /  /  /  / \
      /  /  /  /  \
     /  /  /  /   \
    /  /  /  /     \
   /  /  /  /       \
  /  /  /  /         \
 /  /  /  /           \
/  /  /  /             \
\  \  \  \             /
 \  \  \  \           /
  \  \  \  /         /
   \  \  \ /       /
    \  \  \     /
     \  \  \   /
      \  \  \ /
       \  \  /
        \  /
         \ /
          \

Developed by vist0r
```

- Setelah selesai install airgeddon,install juga package nya :



- Fitur-fiturnya :



- Fitur Utama Aircraddon:
- Mode Monitor:
Menyediakan opsi untuk menempatkan adapter Wi-Fi dalam mode monitor (monitor mode), yang penting untuk menangkap paket data jaringan.
- DoS (Denial of Service) Attack:
Melakukan serangan death untuk memutuskan koneksi klien dari access point (AP), salah satu bentuk serangan Denial of Service (DoS).
- Handshake Capture:
Menangkap WPA/WPA2 handshakes yang bisa digunakan untuk melakukan serangan brute force dengan kamus password (password cracking).
- Offline WPA/WPA2 Decryption:

Menggunakan kamus untuk memecahkan WPA/WPA2 handshakes yang telah ditangkap secara offline.

- **WPS Attacks:**
Menjalankan serangan terhadap WPS (Wi-Fi Protected Setup) untuk mengakses jaringan Wi-Fi. Termasuk serangan brute force terhadap PIN WPS.
- **Evil Twin Attack:**
Membuat access point palsu yang meniru access point asli untuk menangkap informasi sensitif dari korban (seperti login ke halaman palsu).
- **PKMID Tools:**
Memungkinkan penggunaan teknik terbaru dalam memecahkan WPA/WPA2 tanpa memerlukan four-way handshake. Teknik ini memanfaatkan key exchange identifier (PMKID).
- **Enterprise Attacks:**
Mendukung serangan pada jaringan WPA/WPA2 Enterprise, yang merupakan jaringan Wi-Fi yang lebih aman, biasanya digunakan di lingkungan perusahaan.
- **MDK4/MDK3 DoS Tools:**
Menggunakan MDK4 atau MDK3 untuk melakukan serangan DoS yang lebih lanjut, seperti beacon flood, probe flood, atau serangan berbasis paket lainnya.
- **WEP Attacks:**
Mendukung serangan terhadap jaringan WEP, meskipun WEP sudah dianggap tidak aman dan jarang digunakan.
- **5Ghz Band Attack Support:**
Mendukung serangan di frekuensi Wi-Fi 5GHz.
- **MAC Address Spoofing:**
Mendukung spoofing alamat MAC untuk menyembunyikan identitas perangkat selama serangan.
- **Wi-Fi Jammer:**
Menyediakan opsi untuk menjamming semua perangkat yang terhubung ke jaringan Wi-Fi tertentu, mencegah mereka terhubung ke internet atau access point.
- **Network Mapping:**
Menampilkan peta jaringan yang berisi daftar access point, klien yang terhubung, dan informasi penting lainnya seperti kekuatan sinyal dan jenis enkripsi.
- **Cracking Handshakes with Different Tools:**
Mendukung berbagai alat untuk cracking handshake, seperti aircrack-ng, hashcat, atau john the ripper.
- **Support for External Plugins:**
Dapat menggunakan plugin eksternal untuk menambah fungsionalitas lebih lanjut seperti integrasi dengan tool lain.
- **Automatic Dependency Installation:**
Airedragon secara otomatis memeriksa dan menginstal semua dependensi yang dibutuhkan ketika pertama kali dijalankan.
- **Graphical and Text-based Interface:**
Menyediakan tampilan antarmuka berbasis teks dan grafis yang memudahkan navigasi dan penggunaan, bahkan untuk pengguna yang kurang familiar dengan command line.
- **Multi-language Support:**
Airedragon mendukung beberapa bahasa, memungkinkan pengguna dari berbagai latar belakang untuk mengoperasikannya dengan lebih mudah.

- Evil Twin + DoS Combo Attack:
Kombinasi dari Evil Twin dan DoS attack memungkinkan pelaku untuk membuat korban terputus dari jaringan asli dan bergabung dengan access point palsu.
- Advanced MITM (Man-In-The-Middle) Attacks:
Termasuk serangan MITM yang bisa digunakan untuk menangkap atau mengubah lalu lintas jaringan antara korban dan access point.
- Detection Evasion Techniques:
Menerapkan teknik untuk menghindari deteksi oleh sistem keamanan, seperti menggunakan MAC spoofing, serta kontrol yang lebih halus pada serangan deauth untuk menghindari deteksi oleh IDS/IPS (Intrusion Detection/Prevention Systems).

Kategori Menu dalam Aircrack-ng:

- DoS Attack Menu: Untuk melakukan serangan DoS melalui berbagai metode seperti deauthentication, deassociation, dan lain-lain.
- Handshake/PKID Tools Menu: Untuk menangkap dan mengolah WPA/WPA2 handshakes atau PMKID.
- Offline WPA/WPA2 Decrypt Menu: Untuk mendekripsi handshakes yang sudah ditangkap.
- Evil Twin Attacks Menu: Untuk membuat Evil Twin AP dan menangkap informasi dari korban.
- WPS Attacks Menu: Untuk brute force terhadap PIN WPS.
- WEP Attacks Menu: Untuk memecahkan jaringan WEP.
- Enterprise Attacks Menu: Untuk serangan terhadap jaringan WPA/WPA2 Enterprise.

Configuration Management (Hardening WebServer)

2. Pasang http/webserver berbasis Apache2 pada komputer Anda. Anda bebas memilih menggunakan Windows (XAMPP) atau Linux (Apache2) sebagai OS servernya.

Lakukan Hardening pada Webserver dengan meminimalkan informasi yang muncul di header web server (hilangkan informasi versi apache/php atau OS) maupun pada signature/footer webserver tersebut. Tunjukkan screenshot jika sudah berhasil melakukan hardening yang diminta diatas.

Pada DocumentRoot webserver tersebut, terdapat 4 folder aplikasi (buatkan 4 folder aplikasi) dan sesuai aturan/role/acl sebagai berikut

- publicapp (dapat diakses dari semua jaringan)
- privateapp (hanya dapat diakses dari jaringan private Anda misal: 192.168.1.0/24)
- specialapp (hanya IP hacker yang tidak dapat mengakses, misal: IP Hacker 192.168.1.100)
- protectapp (hanya dapat diakses dengan http authentication berbasis htaccess, misal user:admin password:rahasia)

Bagaimana konfigurasi pada webserver agar setiap folder aplikasi tersebut berjalan sesuai rule/aturan/acl yang disebutkan diatas. Jelaskan dan deskripsikan dengan screenshot saat menguji akses masing masing folder app melalui browser setelah konfigurasi sudah disetting.

Jawab :

- memasang apache2 pada linux

```

root@kali:~# apt update
Hit:1 http://kali.kali.org/kali kali-rolling InRelease
1826 packages can be upgraded. Run 'apt list --upgradable' to see them.

root@kali:~# apt install apache2
Installing:
  apache2

Installing dependencies:
  apache2-data  apache2-utils

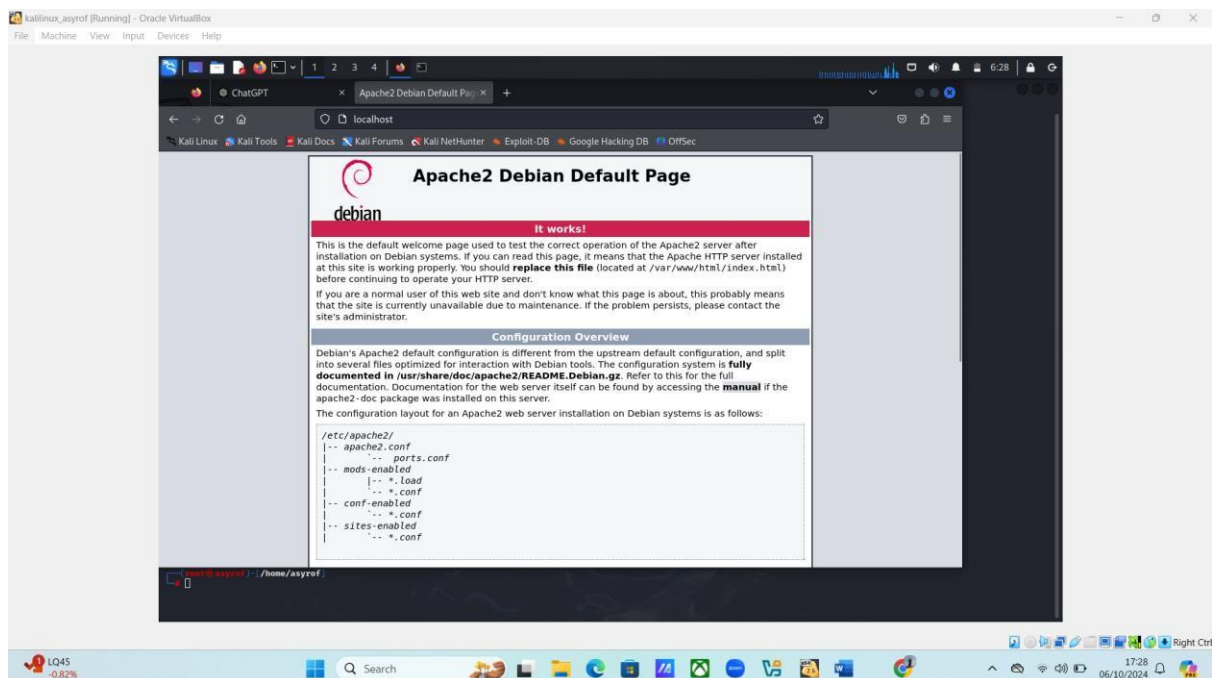
Suggested packages:
  apache2-doc  apache2-suexec-pristine | apache2-suexec-custom  ufw

Summary:
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 1826
  Download size: 587 kB
  Space needed: 1988 kB / 45.1 GB available

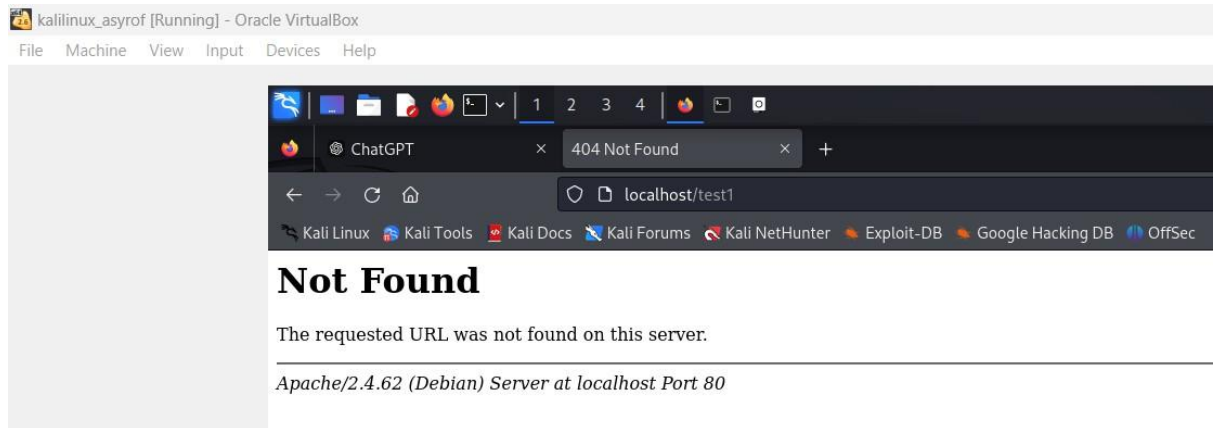
Continue? [Y/n] y
Get:1 http://kali.kali.org/kali kali-rolling/main amd64 apache2-data all 2.4.62-1 [161 kB]
Get:2 http://kali.kali.org/kali kali-rolling/main amd64 apache2-utils amd64 2.4.62-1 [218 kB]
Get:3 http://kali.kali.org/kali kali-rolling/main amd64 apache2 amd64 2.4.62-1 [217 kB]
Fetched 587 kB in 1s (557 kB/s)
Selecting previously unselected package apache2-data.
(Reading database ... 394625 files and directories currently installed.)
Preparing to unpack .../apache2-data_2.4.62-1_all.deb ...
Unpacking apache2-data (2.4.62-1) ...
Selecting previously unselected package apache2-utils.
Preparing to unpack .../apache2-utils_2.4.62-1_amd64.deb ...
Unpacking apache2-utils (2.4.62-1) ...
Selecting previously unselected package apache2.
Preparing to unpack .../apache2_2.4.62-1_amd64.deb ...
Unpacking apache2 (2.4.62-1) ...
Setting up apache2-data (2.4.62-1) ...
Setting up apache2-utils (2.4.62-1) ...
Setting up apache2 (2.4.62-1) ...
Enabling module mpm_event.
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.

```

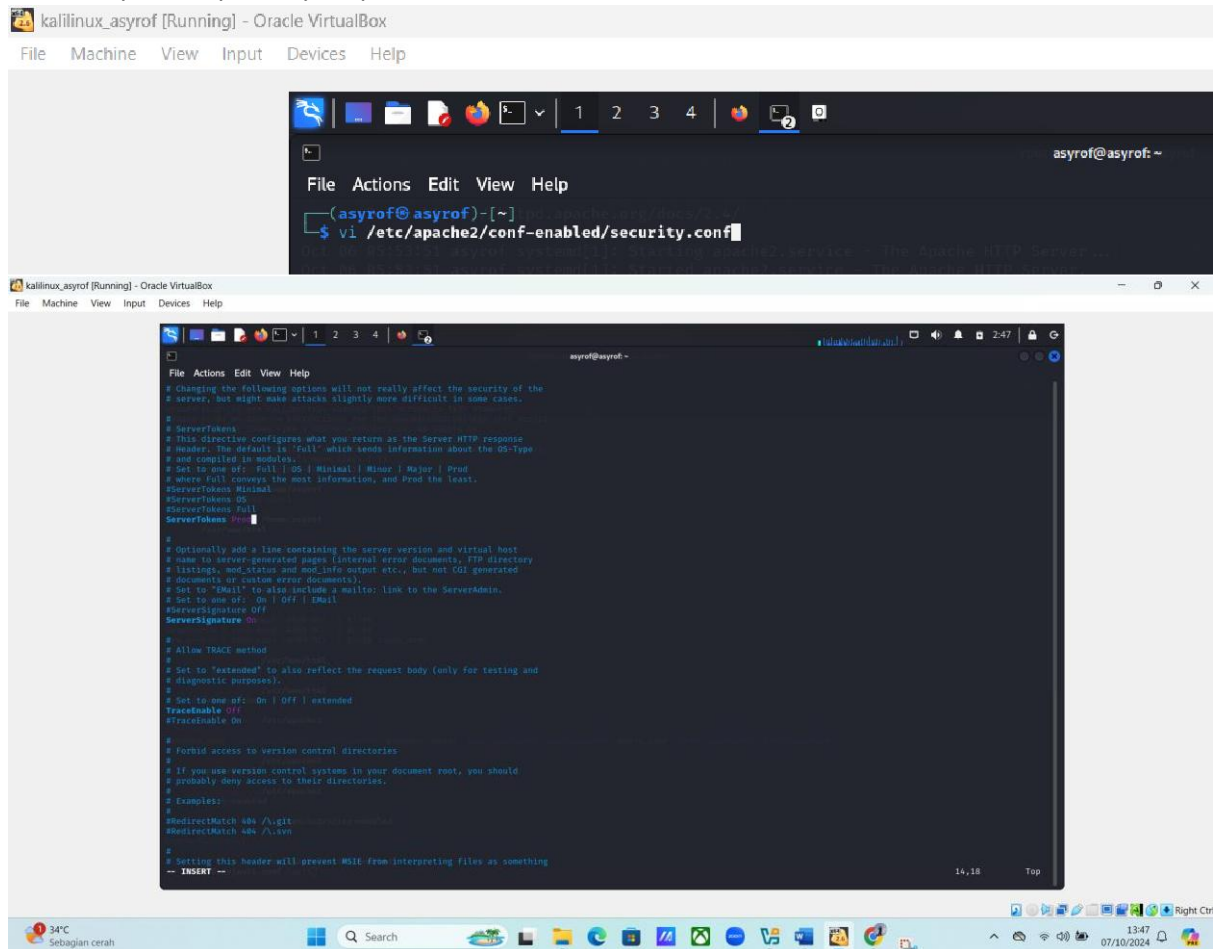
- setelah apache2 terpasang jalankan dengan perintah service apache 2 start
- cara cek status apache2 apakah sudah aktif atau belum dengan perintah service apache2 status
- setelah aktif masuk web apache Debian default page:



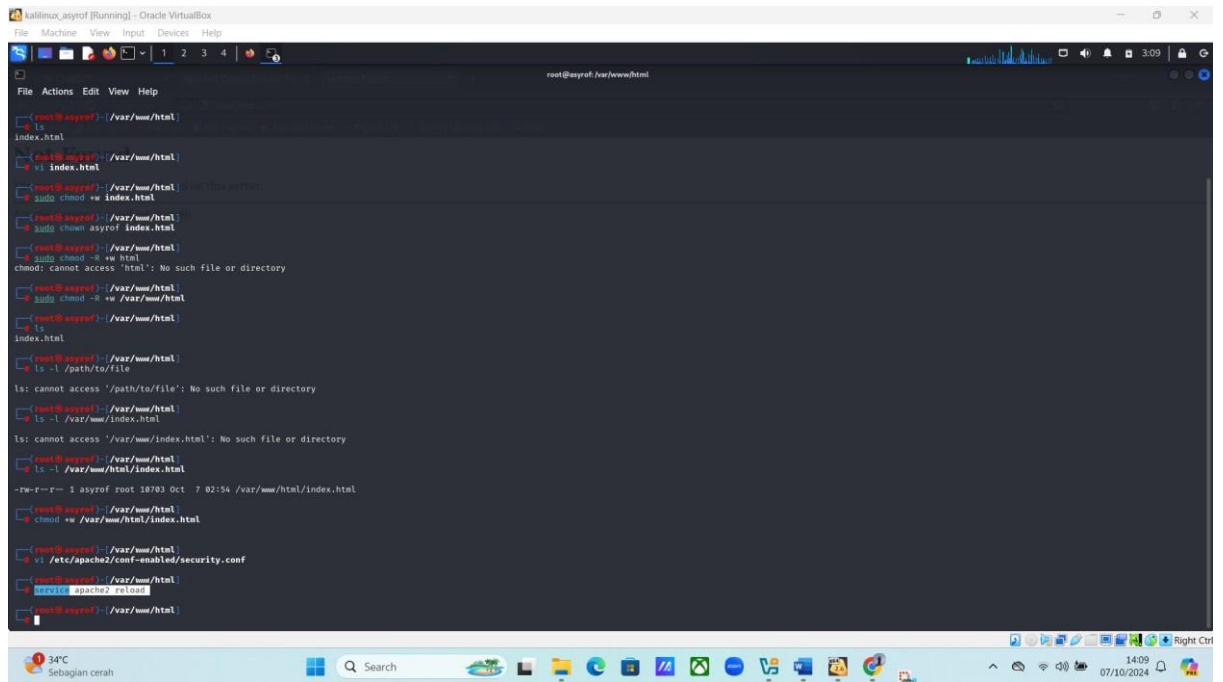
- setelah itu melakukan hardening atau menyembunyikan informasi



- cara menyembunyikan nya seperti ini :

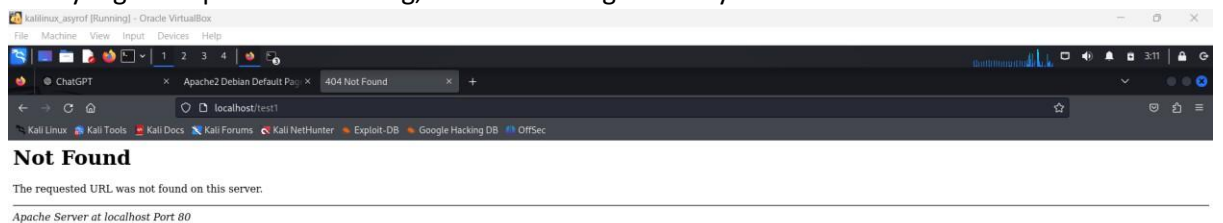


- setelah itu keluar dari vi dan lakukan reload pada apache2 untuk menyimpan perubahan:

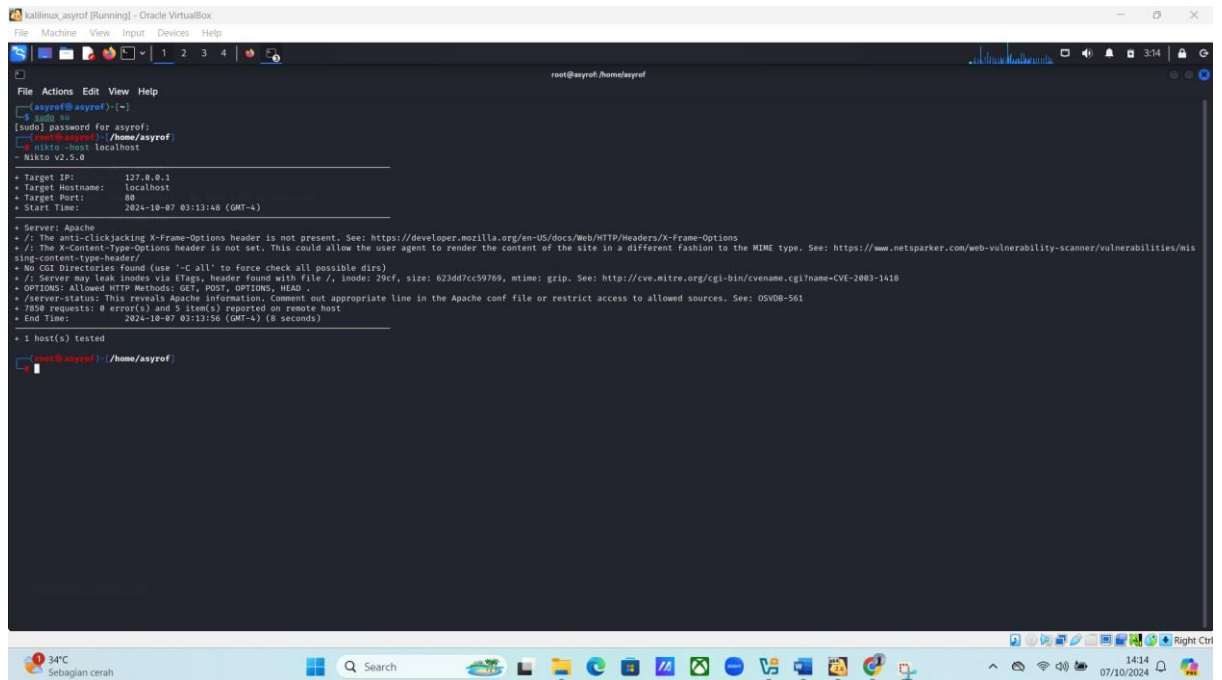


```
root@kali:~# cd /var/www/html
root@kali:~/www/html# ls
index.html
root@kali:~/www/html# mv index.html /var/www/html/
root@kali:~/www/html# chmod -R *w /var/www/html
root@kali:~/www/html# ls -l /path/to/file
ls: cannot access '/path/to/file': No such file or directory
root@kali:~/www/html# ls -l /var/www/index.html
ls: cannot access '/var/www/index.html': No such file or directory
root@kali:~/www/html# service apache2 reload
```

- versi yang ditampilkan akan hilang, masih tersisa signature nya:

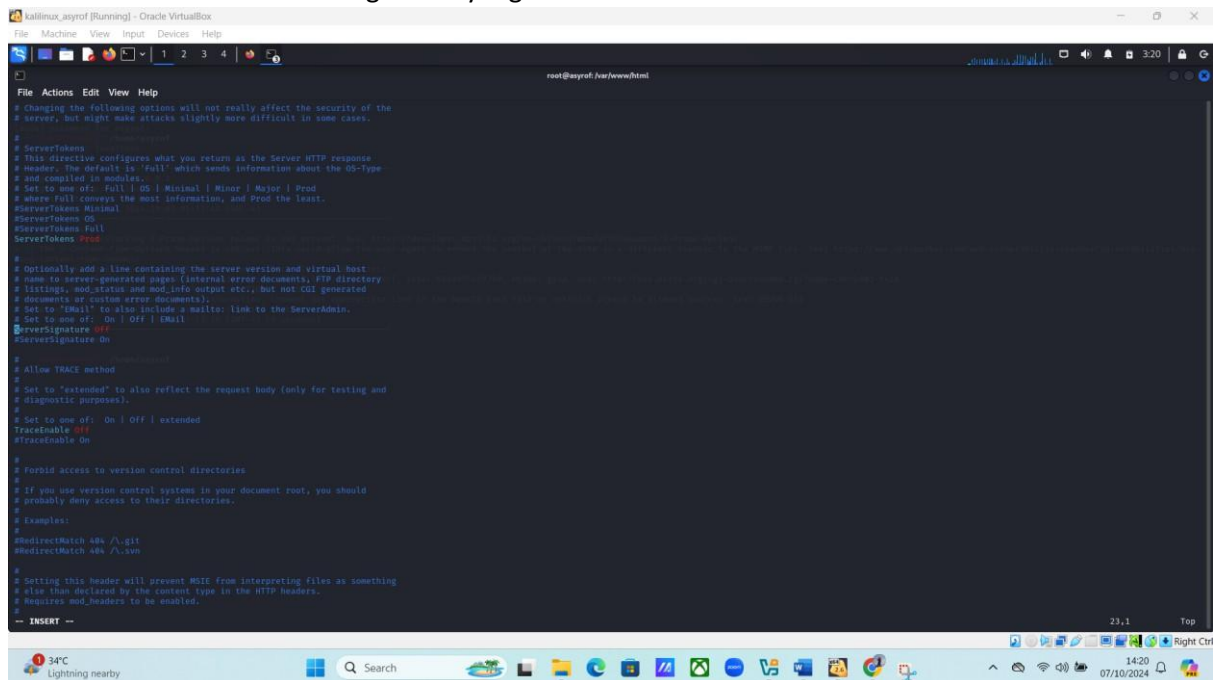


- hasil scan Nikto juga versinya akan tidak terlihat



```
kali@kali:~$ sudo nikto -h localhost
Nikto v2.5.0
+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-10-07 03:13:48 (GMT-4)
+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis-sing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cf, size: 623dd7cc59769, mtime: grip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ 7850 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2024-10-07 03:13:56 (GMT-4) (8 seconds)
+ 1 host(s) tested
```

- kemudian mematikan signature dengan cara menghapus tanda # pada signature yang off dan memberi tanda # untuk signature yang On :



```
# Changing the following options will not really affect the security of the
# server, but might make attacks slightly more difficult in some cases.
#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# header. The default is 'Full' which sends information about the OS-type
# and compiled-in modules.
# Set to one of: Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
ServerTokens Minimal
ServerTokens OS
ServerTokens Full
ServerTokens Prod

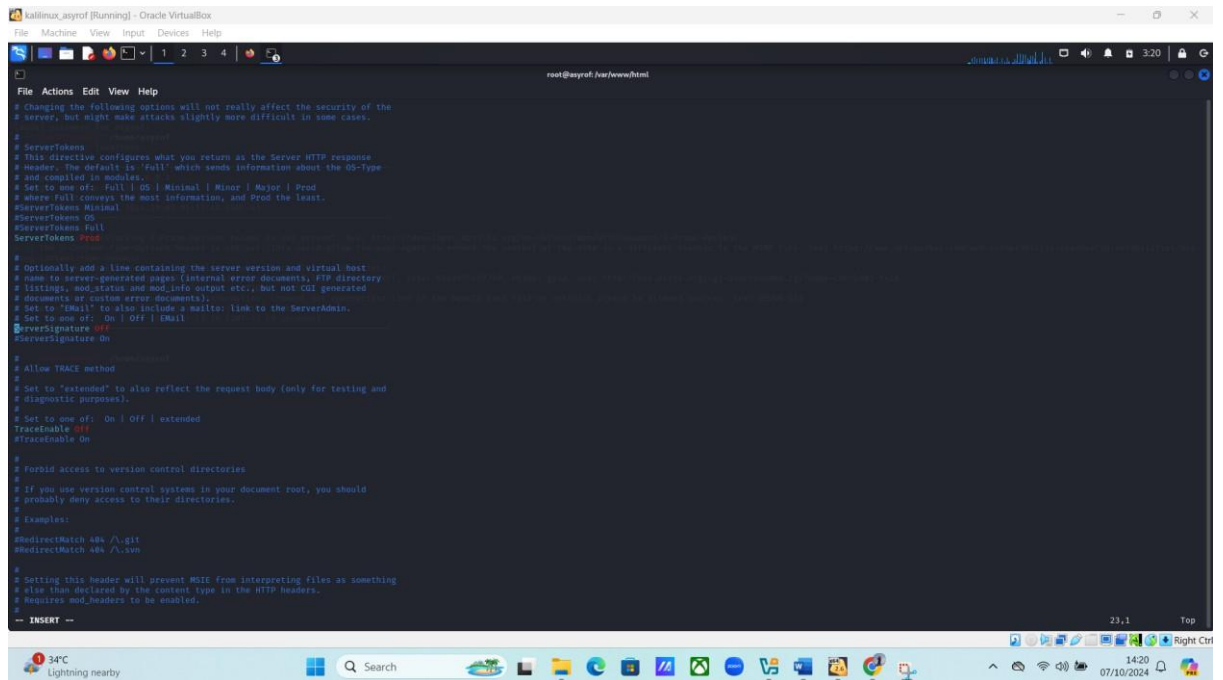
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, /P directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to 'Email' to also include a mailto: link to the ServerAdmin.
# Set to one of: On | Off | Email
ServerSignature On
ServerSignature Off

# Allow TRACE method
# Set to 'extended' to also reflect the request body (only for testing and
# diagnostic purposes).
# Set to one of: On | Off | extended
Traceable Off
Traceable On

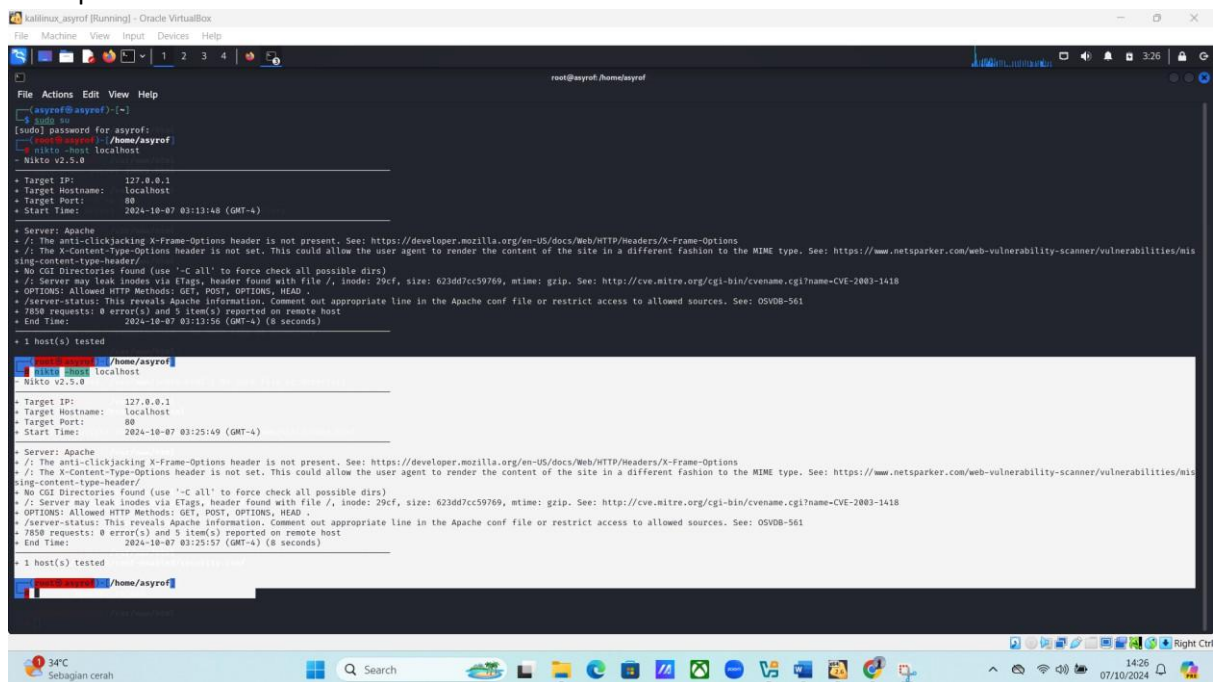
# Forbid access to version control directories
# If you use version control systems in your document root, you should
# probably deny access to their directories.
# Examples:
# #RedirectMatch 404 /\.git
# #RedirectMatch 404 /\.svn

# Setting this header will prevent MSIE from interpreting files as something
# else than declared by the content type in the HTTP headers.
# Requires mod_headers to be enabled.
```

- setelah mengubah signature nya,melakukan reload apache2 untuk melakukan penyimpanan yang sudah diubah,lalu refresh halaman localhost,maka signature nya akan hilang :



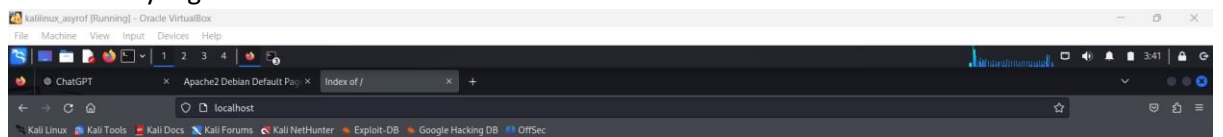
- perubahan yang sudah dibuat dilihat dengan nikto,signature nya pun juga sudah tidak ditampilkan :



- setelah proses hardening selesai,selanjutnya membuat 4 folder pada documentroot :

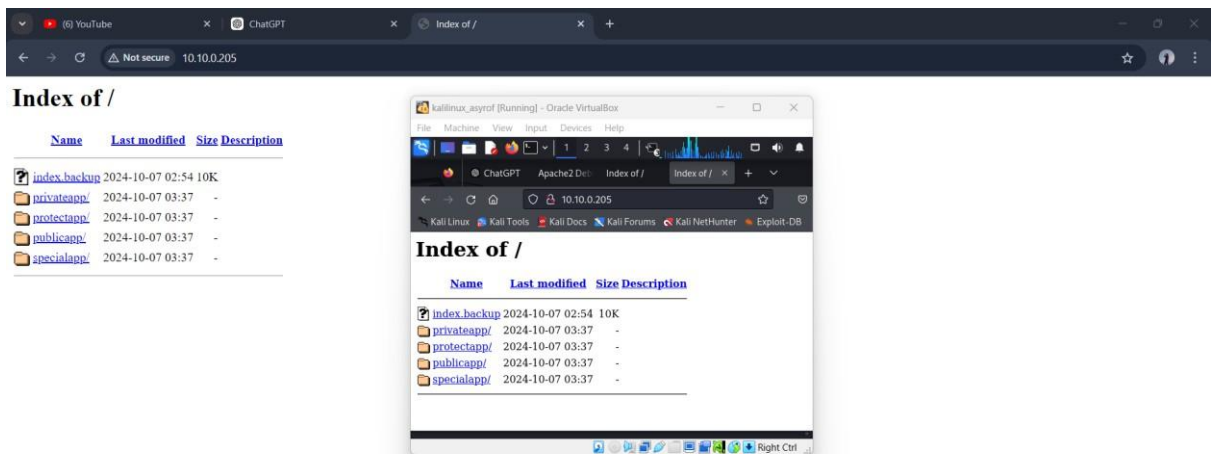
```
root@kali:~# cd /var/www/html
root@kali:/var/www/html# ls
index.html
root@kali:/var/www/html# ls -l /path/to/file
ls: cannot access '/path/to/file': No such file or directory
root@kali:/var/www/html# ls -l /var/www/index.html
ls: cannot access '/var/www/index.html': No such file or directory
root@kali:/var/www/html# ls -l /var/www/html/index.html
-rw-r--r-- 1 asyraf root 18703 Oct 7 02:54 /var/www/html/index.html
root@kali:/var/www/html# chmod +w /var/www/html/index.html
root@kali:/var/www/html# vi /etc/apache2/conf-enabled/security.conf
root@kali:/var/www/html# service apache2 reload
root@kali:/var/www/html# vi /etc/apache2/conf-enabled/security.conf
root@kali:/var/www/html# service apache2 reload
root@kali:/var/www/html# ls
index.html  privateapp  protectapp  publicapp  specialapp
```

- lihat folder yang sudah dibuat di index :

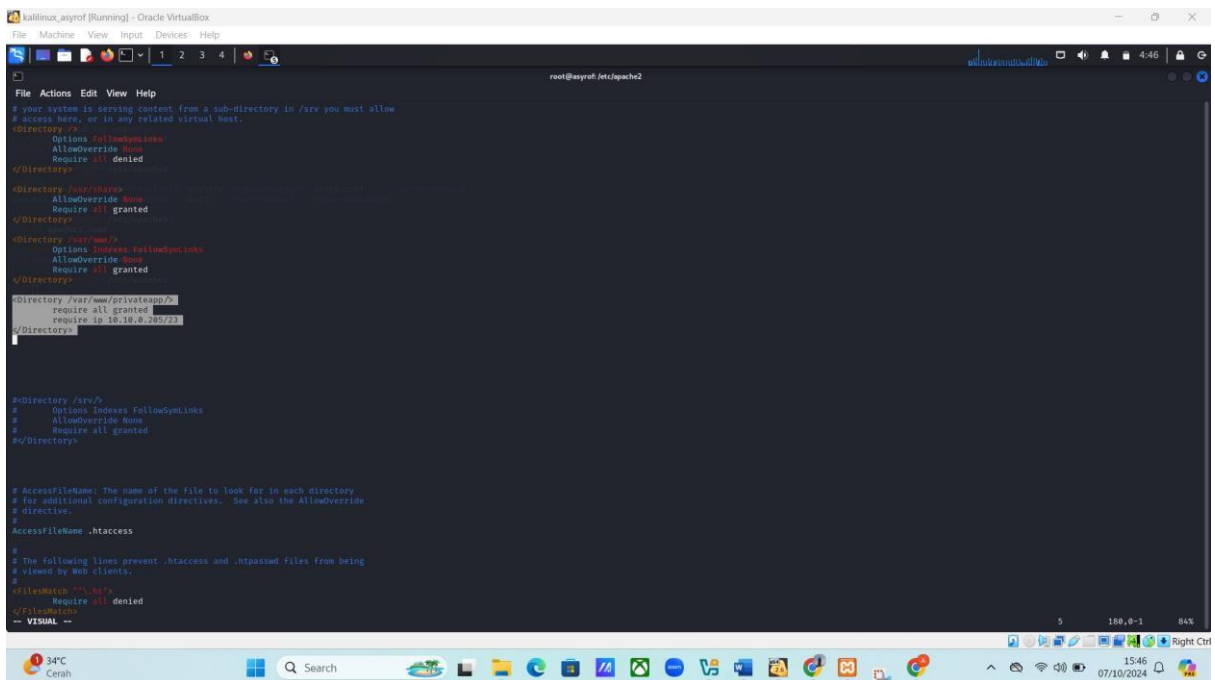


- selanjutnya membuat publicapp dapat diakses dari semua jaringan

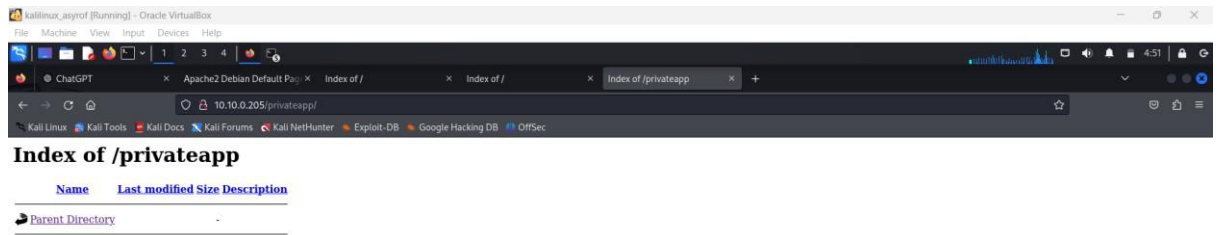
A screenshot of a Kali Linux desktop environment. The top panel shows the system menu with 'Wireless', 'Machine', 'VPN', 'Input', 'Devices', and 'Help' options. The main workspace contains a terminal window titled 'root@kali: /usr/www/html' and a file manager window showing the contents of the '/usr/www/html' directory. The terminal displays the output of several commands: 'service apache2 reload', 'cat /etc/apache2/conf-enabled/security.conf', 'mkdir publicapp privateapp specialapp', 'ls', 'cp index.html privateapp publicapp specialapp', 'cp index.html index.backup', 'ipconfig', and 'ifconfig'. The file manager shows a directory listing of the '/usr/www/html' directory, including files like 'index.html', 'privateapp', 'publicapp', 'specialapp', and 'index.backup'. The bottom panel shows the system status bar with the date '07/10/2024' and the time '14:57'.



- Selanjutnya membuat privateapp (hanya dapat diakses dari jaringan private dengan cara masuk ke vi apache2.conf, buat directory privateapp menggunakan ip yang sudah dicantumkan:



- Setelah itu keluar dan reload apache2 untuk menyimpan perubahan lalu cek melalui chrome :

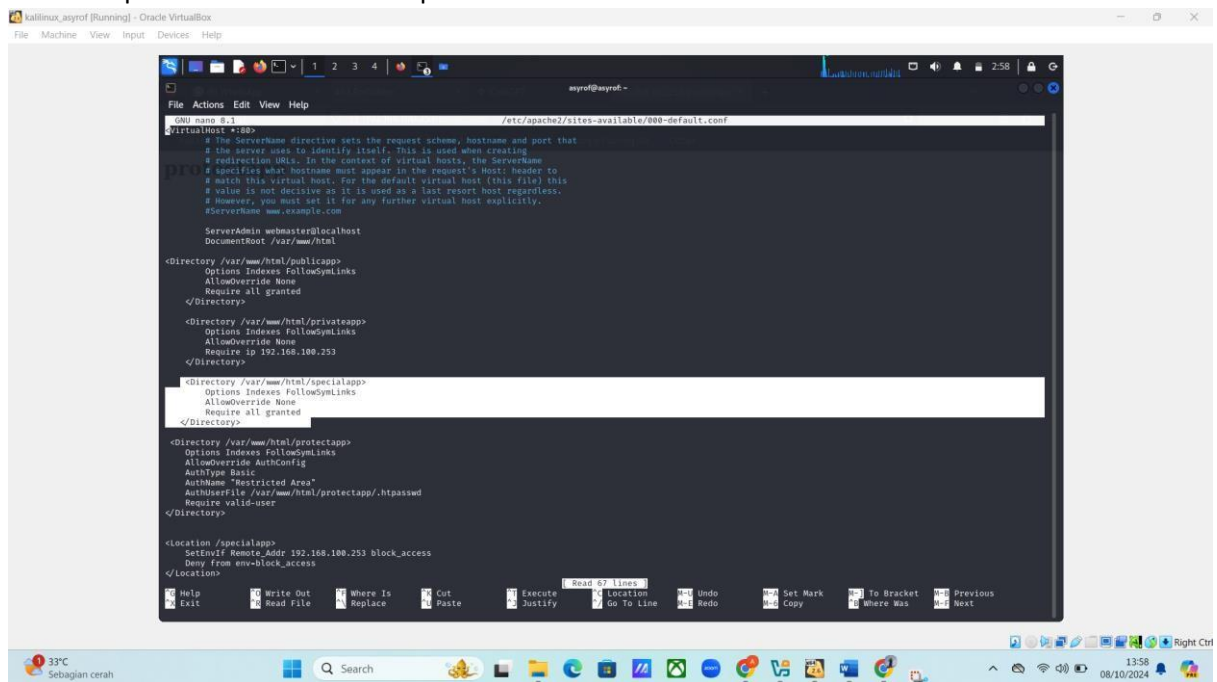


- Membuat specialapp (hanya IP hacker yang tidak dapat mengakses, misal: IP Hacker 192.168.1.100)

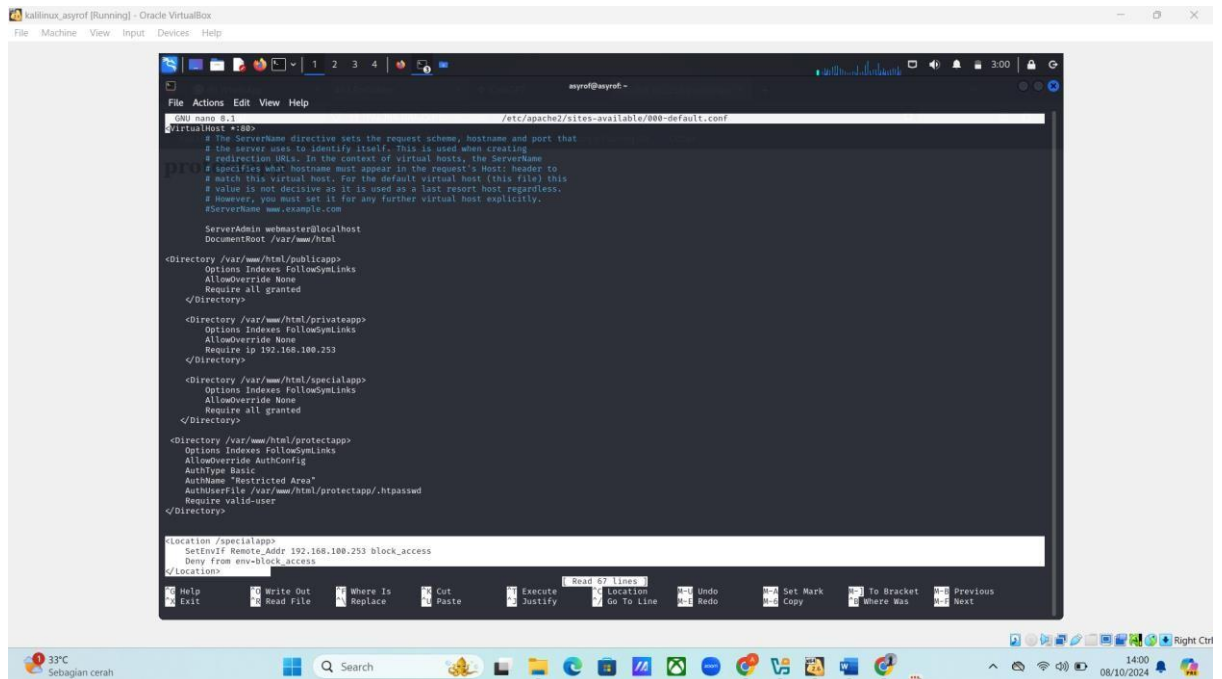
- Masukkan perintah ini :

```
(asyrof@asyrof)-[~]
$ sudo nano /etc/apache2/sites-available/000-default.conf
(asyrof@asyrof)-[~]
$
```

- Lalu buat pada GNU NANO buat seperti ini :



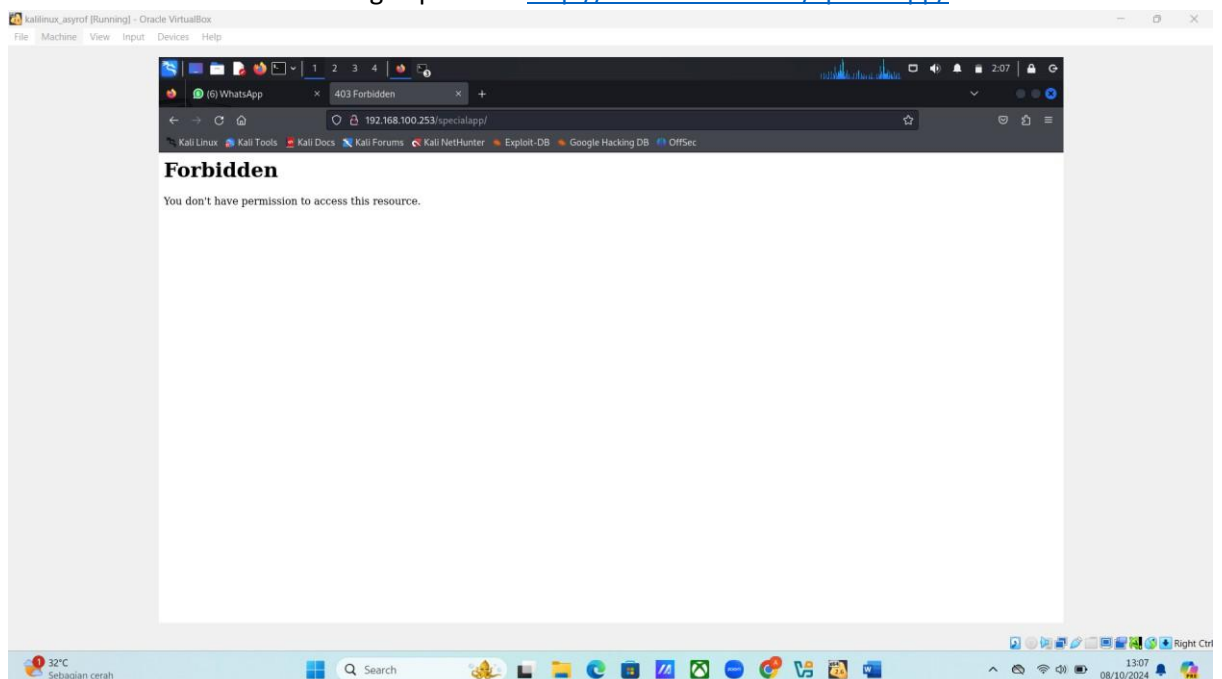
- Setelah itu buat perintah lag untuk mengatur IP yang tidak diperbolehkan akses :



Kenapa dibuat perintah baru?

Karena pada directory specialapp tidak diperbolehkan 2 perintah digabung menjadi satu contohnya "Require all granted" untuk perintah memperbolehkan semua akses, tidak bisa digabung dengan perintah "not IP 192.168.100.253(ip yang dilarang akses)" karena akan berbenturan perintahnya. maka dari itu dibuat perintah terpisah.

- Lalu akses melalui chrome dengan perintah <http://192.168.100.253/specialapp/>



- Terakhir membuat protectapp (hanya dapat diakses dengan http authentication berbasis htaccess, misal user:admin password:rahasia), pertama buat username dan passwordnya :

```
ayyraf@ayyraf:~$ chmod 644 /path/to/.htpasswd
chmod: cannot access '/path/to/.htpasswd': No such file or directory

ayyraf@ayyraf:~$ sudo htpasswd -c /var/www/html/protectedapp/.htpasswd ID
htpasswd: cannot create file /var/www/html/protectedapp/.htpasswd

ayyraf@ayyraf:~$ sudo htpasswd -c /var/www/html/protectedapp/.htpasswd ID
New password:
Re-type new password:
htpasswd: password verification error

ayyraf@ayyraf:~$ sudo nano /var/www/html/protectedapp/.htpasswd ID
New password:
Re-type new password:
Adding password for user ID

ayyraf@ayyraf:~$ sudo nano /var/www/html/protectedapp/.htaccess
ayyraf@ayyraf:~$ sudo systemctl restart apache2

ayyraf@ayyraf:~$ sudo nano /etc/apache2/sites-available/000-default.conf
ayyraf@ayyraf:~$ sudo systemctl restart apache2
```

- Pada GNU Nano buat perintah seperti ini :

```
ayyraf@ayyraf:~$ nano /etc/apache2/sites-available/000-default.conf
VirtualHost *:80
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    <Directory /var/www/html/publicapp>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
    </Directory>

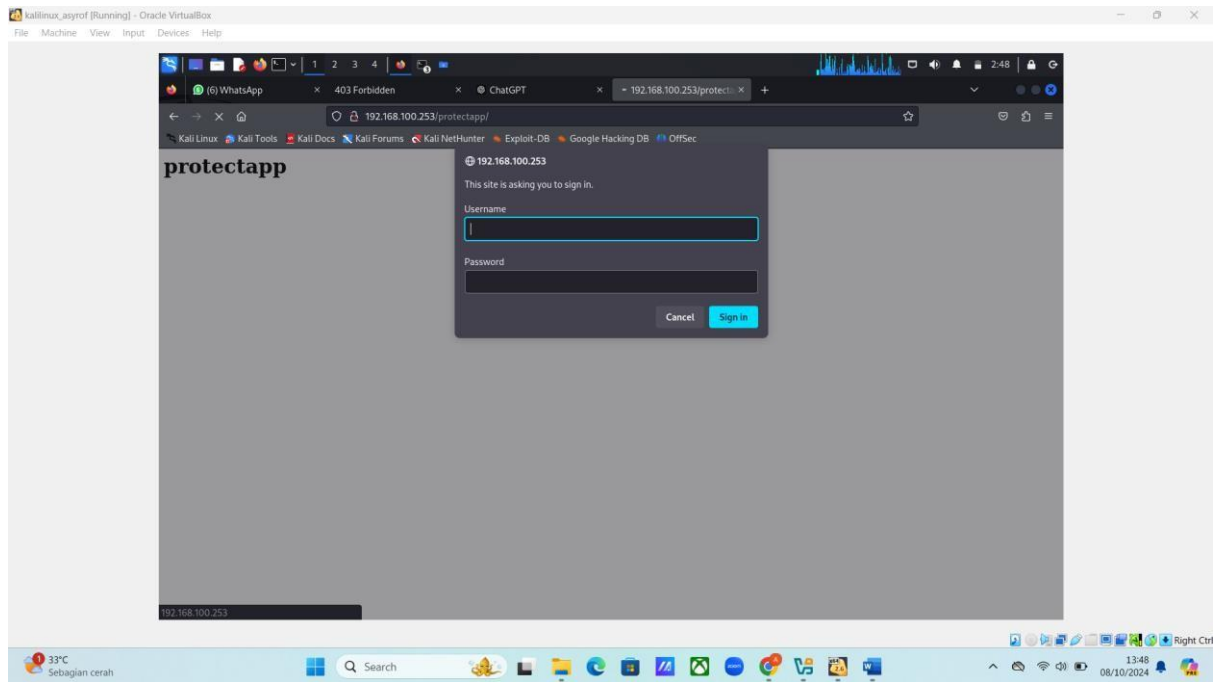
    <Directory /var/www/html/privateapp>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require ip 192.168.100.253
    </Directory>

    <Directory /var/www/html/specialapp>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
    </Directory>

    <Directory /var/www/html/protectedapp>
        Options Indexes FollowSymLinks
        AllowOverride AuthConfig
        AuthType Basic
        AuthName "Restricted Area"
        AuthUserFile /var/www/html/protectedapp/.htpasswd
        Require valid-user
    </Directory>

    <Location /specialapp>
        SetEnvIf Remote_Addr 192.168.100.253 block_access
        Deny from env=block_access
    </Location>
```

- Setelah membuat id,password,dan membuat pengaturan di GNU nano restart/reload apache2.lalu masuk ke chome untuk membuktikannya :



Penjelasan :

- Publicapp : web localhost bisa diakses semua IP
- Privateapp : web localhost hanya bisa diakses dengan alamat IP yang diizinkan akses
- Specialapp : web localhost tidak bisa diakses dengan alamat IP yang dilarang masuk,kebalikan dari privateapp
- Privateapp : web localhost bisa diakses semua alamat IP tetapi harus memasukkan ID dan Username

Keterangan : IP yang saya gunakan berbeda,karena saya mengerjakan tugasnya berbeda tempat