# Keamanan Siber

**Pertemuan 5 Hardening System**

I Wayan Ardiyasa-ITB STIKOM Bali 2023

*Always The First*

# Pendahuluan

- Keamanan sistem komputer yaitu untuk menjamin sumber daya tidak digunakan atau dimodifikasi oleh orang yang tidak bertanggung jawab.
- Dibagi menjadi tiga bagian antara lain :
  1. Keamanan eksternal (external security).
  2. Keamanan interface pemakai (user interface security).
  3. Keamanan internal (internal security).
- Pentingnya menjaga keamanan jaringan maupun komputer server harus dipahami oleh semua elemen didalamnya;
- Sehingga timbulnya "**awareness**" terhadap permasalahan keamanan dann kerentanan terhadap sistem keamanan.

# Definisi Hardening System

- Proses memperkuat keamanan suatu sistem komputer, jaringan, atau perangkat lunak untuk mengurangi kerentanan terhadap ancaman keamanan.
- Proses ini melibatkan penerapan serangkaian tindakan yang dirancang untuk menutup celah keamanan, mengamankan konfigurasi, dan mengurangi celah serangan.

# Tujuan Hardening

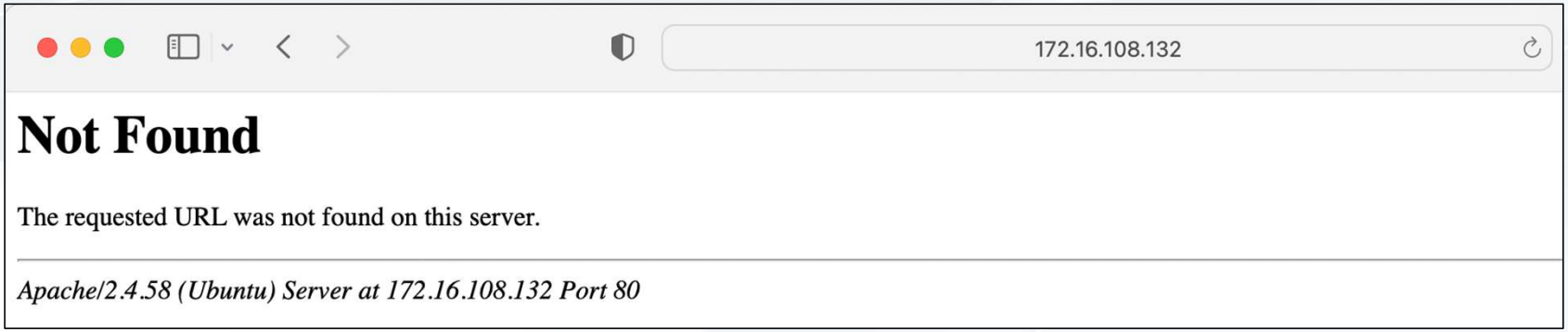
- Pada umumnya sistem operasi linux pada saat diimplementasikan atau baru diinstall, masih menggunakan konfigurasi standard meskipun sudah aman ada baiknya tetap dilakukan hardening, teruatama jika server tersebut akan diakses melalui internet atau IP Public.
- Untuk menerapkan standard keamanan (security policy) dari sistem operasi linux.
- Menutupi celah keamanan (security vulnerability) yang terdapat pada konfigurasi standar pada sistem operasi tersebut.

# Langkah-langkah Hardening

- Update sistem
- Pengelolaan pengguna
- Pengaturan keamanan aplikasi
- Monitoring dan Respon insiden
- Kebijakan keamanan

# Menyembunyikan Informasi Apache dan OS

- Pengujian akses pada apache, untuk melihat informasi apache dan OS



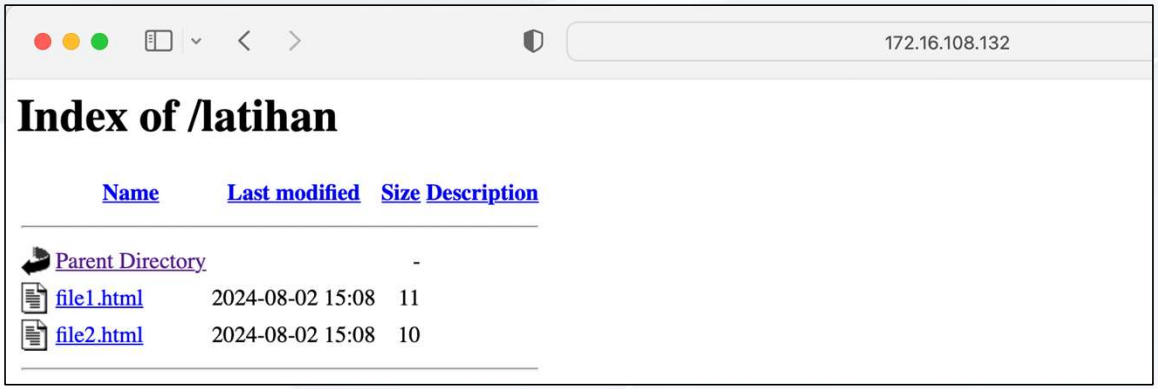
# Menyembunyikan Informasi Apache dan OS

- Masuk terminal dengan mode root :
  - **#nano /etc/apache2/conf-enabled/security.conf**
- Cari baris berikut pada file security.conf
  - **ServerSignature Off**
  - **ServerTokens Prod**
- Hasil pengujian, informasi apache tidak muncul.

# Menonaktifkan list direktori

- Secara default apache akan menampilkan semua isi directory pada htdocs atau **/var/www/html/**, secara implementasi hal ini tidak diperkenankan karena tidak aman sebab attacker dapat mengetahui seluruh folder yang ada pada htdocs atau **/var/www/html.** Seperti gambar berikut :

Jika diakses direktori, maka akan menampilkan isi pada direktori tersebut Dalam hal ini ada 2 file yang di skenariokan



# Menonaktifkan list direktori

- Ketik command berikut diterminal **#nano /etc/apache2/apache2.conf**
- Kemudian ubah pada baris **<Directory /var/www/html>** seperti berikut ini:

```
<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted_
</Directory>
```

Menjadi

```
<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
        Options -Indexes
</Directory>
```

# Menonaktifkan list direktori

- Setelah ditambahkan baris pada **<Directory /var/www/html>**, lakukan restart apache2 dengan command : **#systemctl restart apache2**
- Lakukan akses ke ip server melalui browser, dan apabila berhasil maka menampilkan gambar seperti dibawah ini :

# Mod Security Apache

- **Mod Security** yaitu berfungsi sebagai firewall untuk web server dan digunakan untuk memantau lalu lintas secara real time. **Mod Security** melindungi web server dari serangan **brute force**.
- Berikut cara menginstall Mod Security pada ubuntu server, yaitu :
  - Untuk menjalankan Mod Security pada apache yaitu install modul libapache2-modsecurity. Dengan command **#apt install libapache2-mod-security2**
  - Klik **Y** untuk menyetujui dan tunggu hingga selesai proses instalasi. Seperti gambar berikut :

```
root@mesinserver:/# apt install libapache2-mod-security2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required
  libwrap0 tcpd
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  liblua5.1-0 libyajl2 modsecurity-crs
Suggested packages:
  lua geoip-database-contrib ruby python
The following NEW packages will be installed:
  libapache2-mod-security2 liblua5.1-0 libyajl2 modsecurity-crs
0 upgraded, 4 newly installed, 0 to remove and 60 not upgraded.
Need to get 510 kB of archives.
After this operation, 2,701 kB of additional disk space will be used.
Do you want to continue? [Y/n] y_
```

# Membatasi Request pada Apache

- By Default Apache tidak memiliki batasan pada ukuran request service HTTP dan ketika system mengizinkan request yang besar pada web server, ada kemungkinan bahwa system bisa menjadi korban serangan DoS (Denialof service).
- Apache dapat membatasi besar ukuran request dengan **"LimitRequestBody"** di file konfigurasi apache2.conf. Yang dapat mengatur nilai besar request dalam byte dari 0 (tidak terbatas) hingga 2147483647 (2GB). Adapun caranya sebagai berikut :
- Bukan terminal, ketik command berikut: #nano /etc/apache2/apache2.conf
- tambahkan script berikut :
  - `<Directory /var/www/html/upload/>`
  - `#Pembatasan hanya pada direktori upload saja`
  - `LimitRequestBody 512000`
  - `</Directory>`

# Membatasi **request pada apache**

- **Menggunakan mod_evasive untuk Mitigasi Serangan DoS**
- mod_evasive adalah modul lain digunakan untuk membatasi dan mencegah serangan DoS dengan cara mendeteksi dan memblokir IP yang melakukan request terlalu banyak dalam waktu singkat.
- Berikut instalasi dan konfigurasinya :
- Lakukan instalasi terlebih dahulu pada mode root: **`#apt-get install libapache2-mod-evasive`**
- Buka terminal pada mode root dan gunakan command berikut untuk merubah konfigurasi: **`#nano/etc/apache2/mods-available/evasive.conf`** lalu tambahkan konfigurasi berikut :

# Membatasi request pada apache

- Lalu tambahkan konfigurasi berikut ini :

```
<IfModule mod_evasive20.c>
    DOSHashTableSize    3097
    DOSPageCount        2
    DOSSiteCount        50
    DOSPageInterval     1
    DOSSiteInterval     1
    DOSBlockingPeriod   10
    DOSEmailNotify      ardi@example.com
    DOSSystemCommand    "sudo /sbin/iptables -A INPUT -s %s -j DROP"
    DOSLogDir           "/var/log/mod_evasive"
</IfModule>
```

- Setelah dilakukan penambahan konfigurasi, lakukan restart :

**#sudo systemctl restart apache2**

# Membatasi request pada apache

Keterangan :

- **DOSPageCount**: Jumlah request per halaman yang diizinkan dalam interval yang ditentukan.
- **DOSSiteCount**: Jumlah request yang diizinkan dari satu IP dalam interval yang ditentukan.
- **DOSPageInterval dan DOSSiteInterval**: Interval waktu dalam detik.
- **DOSBlockingPeriod**: Waktu dalam detik untuk memblokir IP yang terdeteksi.
- **DOSEmailNotify**: Alamat email untuk menerima notifikasi saat terjadi serangan.
- **DOSSystemCommand**: Perintah sistem yang dijalankan saat terjadi serangan (misalnya, untuk memblokir IP dengan iptables).
- **DOSLogDir**: Direktori untuk menyimpan log dari mod_evasive.

# Keamanan Akses SSH

- User root adalah user default dimana Attacker telah mengetahui user tersebut. Sehingga Attacker dapat melakukan Brute Force untuk mendapatkan passworddari user root tersebut.
- Untuk mengamankan akses SSH salah satunya adalah menonaktifkan user root dengan cara sebagai berikut :

  Buka terminal ketik command berikut: **`nano /etc/ssh/sshd_config`**
  Cari baris berikut :

```
PermitRootLogin no
PubkeyAuthentication yes
PasswordAuthentication no
ChallengeResponseAuthentication no
```

  Setelah itu lakukan restart : **`systemctl restart sshd`**

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI

Kampus Merdeka INDONESIA JAYA

**Single Degree Program**

**S2 - Sistem Informasi (M.Kom.)**
**S1 - Sistem Komputer (S.Kom.)**
**S1 - Sistem Informasi (S.Kom.)**
**S1 - Teknologi Informasi (S.Kom.)**
**S1 - Bisnis Digital (S.Bns.)**
**D3 - Manajemen Informatika (A.Md.Kom.)**

**Dual Degree International Program**

**S1 - Sistem Informasi (S.Kom., B.IT.)**
(collaboration with HELP University)
**S1 - Bisnis Digital (S.Bns., B.M.)**
(collaboration with DNUI University)

**Dual Degree National Program**

**S1 - Sistem Informasi (S.Kom., S.Ds.)**
(collaboration with Universitas Teknologi Bandung)


www.stikom-bali.ac.id info@stikom-bali.ac.id (0361) 244445

STIKOMERS TV STIKOM Bali @stikombali


*Always The First*