PERANCANGAN DAN IMPLEMENTASI SISTEM RESERVASI DAN PEMESANAN RESTORAN BERBASIS WEB DAN MOBILE

LAPORAN PROYEK AKHIR

Dibuat untuk memenuhi syarat menyelesaikan UTS

Oleh:

1. FAUZI RACHMAN (23416255 201205)
2. Gading agan (23416255 201220)
3. HIKAM WILDANI HAFIDZ (23416255201287)
4. Altaf Sultan Al Razan (23416255201269)
5. MUHAMMAD FAISAL AL GHIFARY (23416255201212)

TEKNIK INFORMATIKA FAKULTAS ILMU KOMPUTER UNIVERSITAS BUANA PERJUANGAN KARAWANG 2025

DAFTAR ISI

Pembagian tugas:

Fauzi Rachman: Kriteria 1

Gading agan: Kriteria nomer2

Hikam Wildani Hafidz: Kriteria nomer 2

Altaf Sultan Al Razan: Kriteria nomer 3

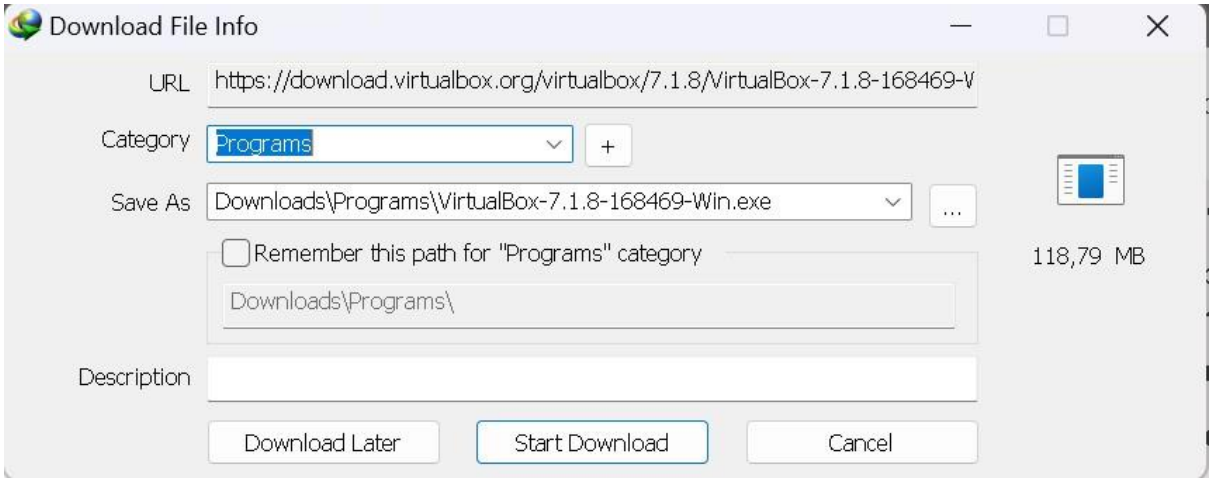
Muhammad Faisal Al Ghifary: Kesimpulan dan Evaluasi

Instalasi Sistem (Kriteria 1)

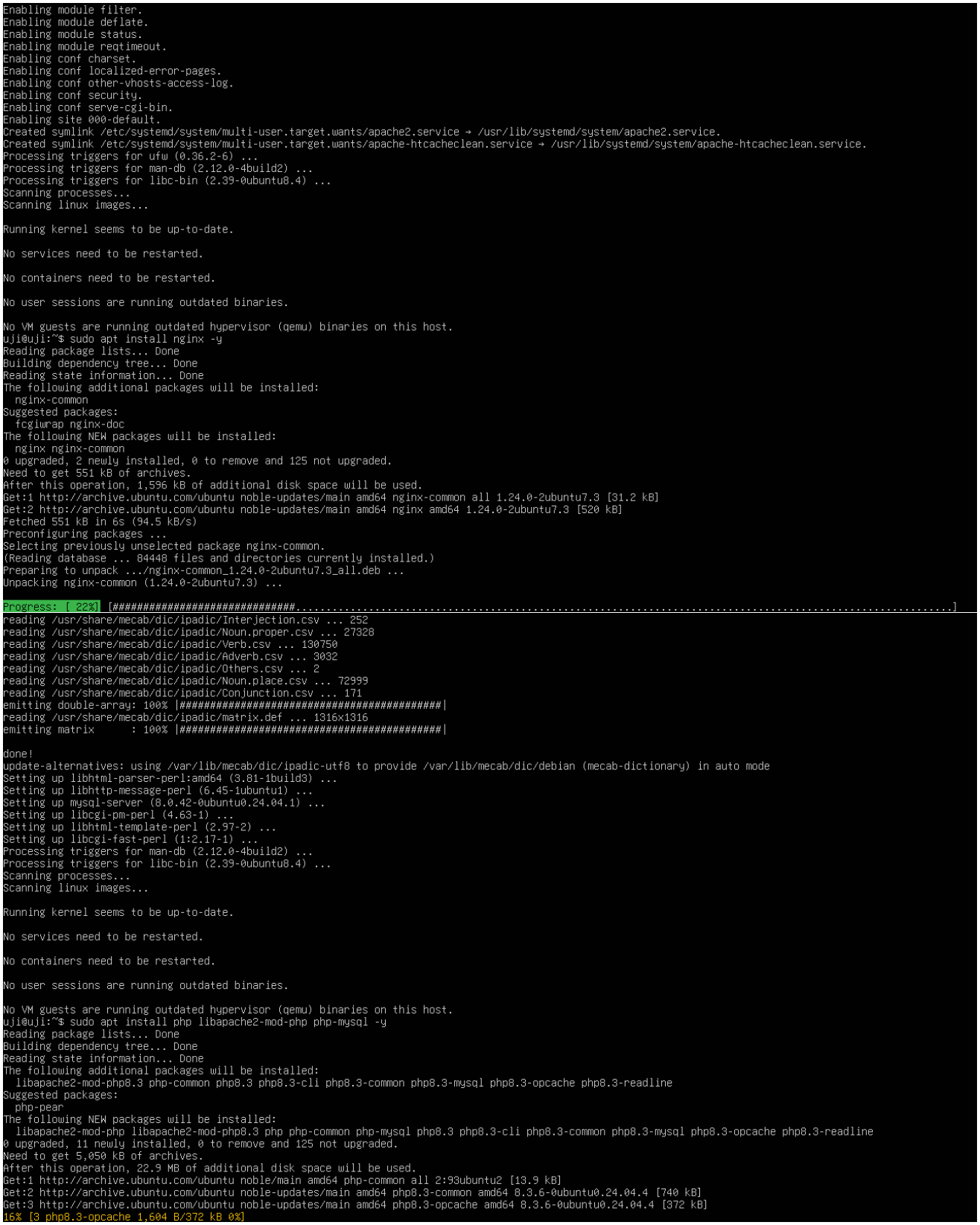
Intallasi VirtualBox dan Ubuntu(ubuntu-24.04.2-live-server-amd64_2)

Ubuntu 24.04.2 LTS Server di VirtualBox Alasan kami karena:

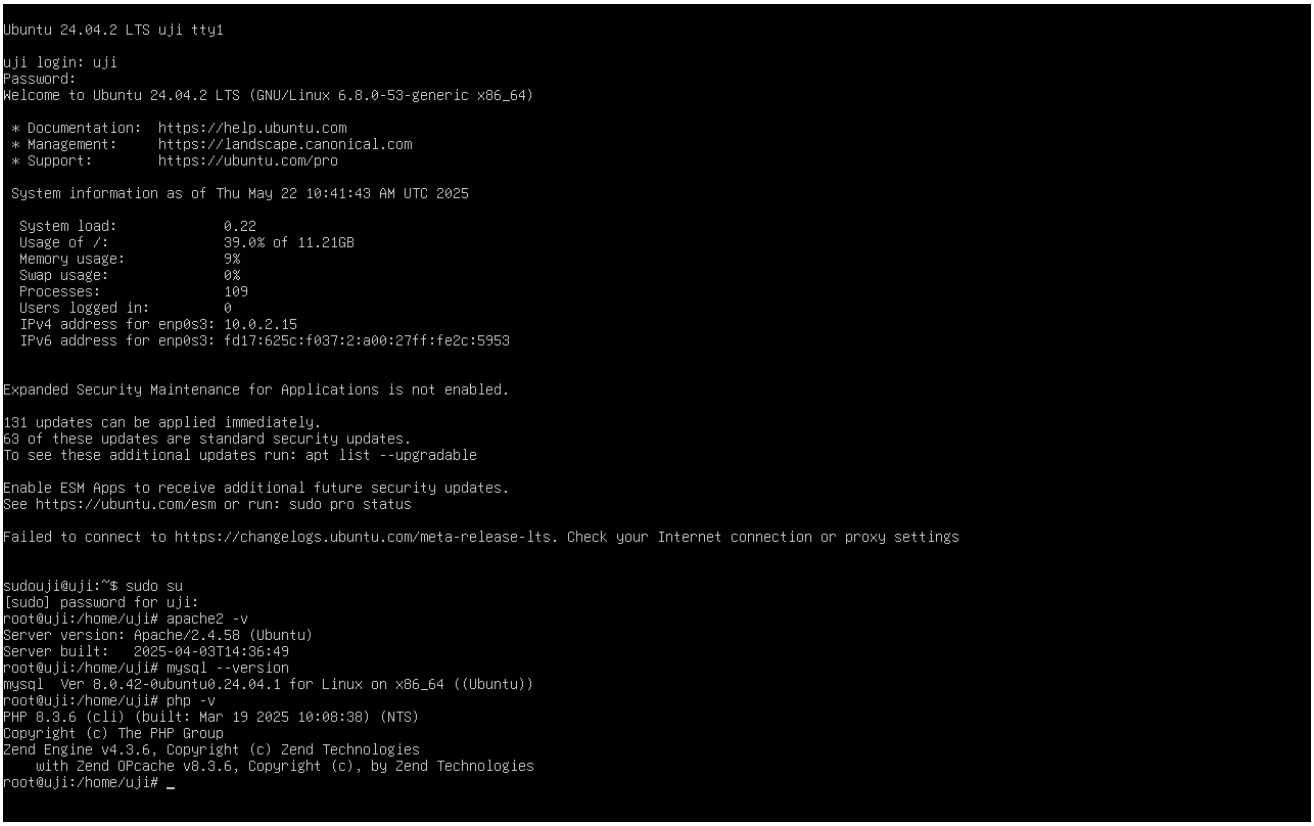
- Popularitas dan dukungan komunitas yang luas.
- Dokumentasi yang melimpah.
- Stabilitas (LTS = Long Term Support).
- Fokus pada penggunaan server (sesuai tugas UTS).
- Kemudahan instalasi Apache, MySQL, dan PHP (melalui apt).




```
Get:35 http://archive.ubuntu.com/ubuntu noble-backports/restricted amd64 c-n-f Metadata [116 B]
Get:36 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [27.1 kB]
Get:37 http://archive.ubuntu.com/ubuntu noble-backports/universe Translation-en [16.5 kB]
Get:38 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [16.4 kB]
Get:39 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [1,304 B]
Get:40 http://archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:41 http://archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:42 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [235 kB]
Get:43 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [208 B]
Get:44 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 c-n-f Metadata [468 B]
Get:45 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [840 kB]
Get:46 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [183 kB]
Get:47 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.3 kB]
Get:48 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [17.0 kB]
Get:49 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [17.7 kB]
Get:50 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [3,792 B]
Get:51 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:52 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [380 B]
Fetched 9,042 kB in 22s (402 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
125 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 125 not upgraded.
Need to get 2,084 kB of archives.
After this operation, 8,094 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2-3.1ubuntu0.1 [108 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7 [91.9 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.1ubuntu7 [11.2 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-ldap amd64 1.6.3-1.1ubuntu7 [9,116 B]
Get:5 http://archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3build2 [166 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-1ubuntu8.6 [1,330 kB]
Get:7 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-1ubuntu8.6 [163 kB]
Get:8 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-1ubuntu8.6 [97.2 kB]
Get:9 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2 amd64 2.4.58-1ubuntu8.6 [90.2 kB]
Get:10 http://archive.ubuntu.com/ubuntu noble/main amd64 ssl-cert all 1.1.2ubuntu1 [17.8 kB]
Fetched 2,084 kB in 8s (271 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libapr1t64:amd64.
(Reading database ... 75%
```



Details version apache, mysql dan php:

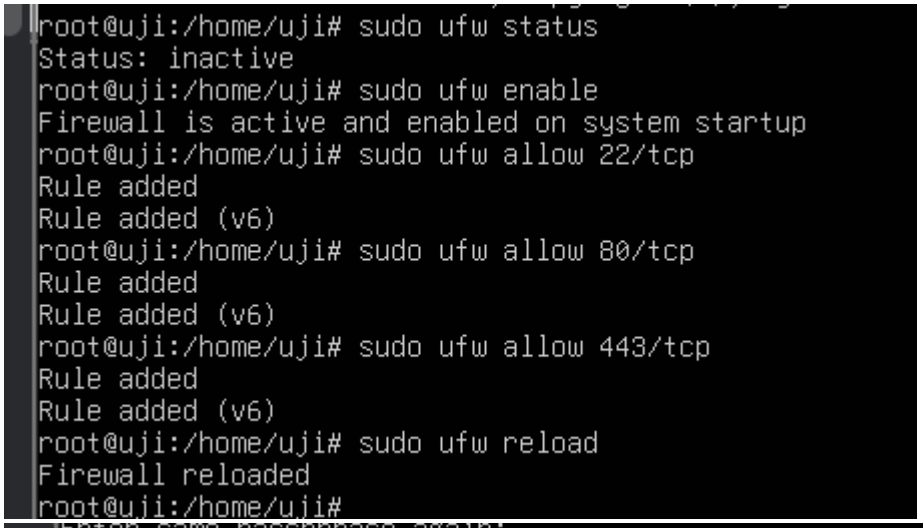


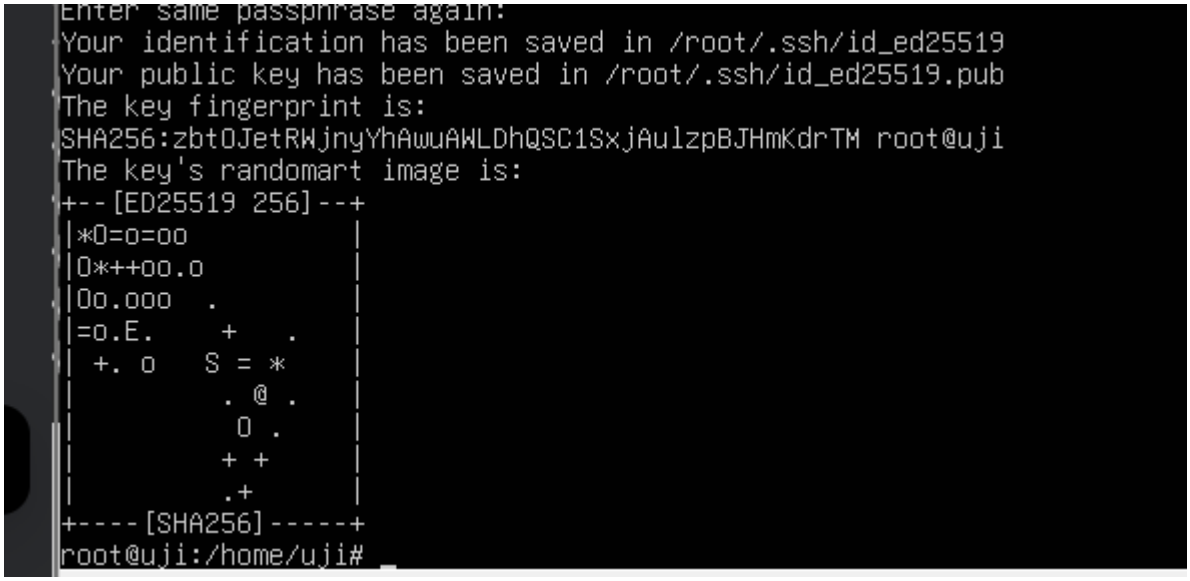
Pengamanan Sistem (Kriteria 2)

1. Daftar Port dan Alasan

Port	Protokol	Layanan	Alasan Teknis
22	TCP	SSH	Untuk remote administration server
80	TCP	HTTP	Untuk layanan web (apache/nginx)

443	TCP	HTTPS	Untuk layanan web dengan enskripsi SSL/TLS





```
root@uji:/home/uji# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2c:59:53 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 85623sec preferred_lft 85623sec
    inet6 fd17:625c:f037:2:a00:27ff:fe2c:5953/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86012sec preferred_lft 14012sec
    inet6 fe80::a00:27ff:fe2c:5953/64 scope link
       valid_lft forever preferred_lft forever
root@uji:/home/uji# ssh-copy-id -i /root/.ssh/id_ed25519.pub fauzi_rachman_205@10.0.2.15
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed

/usr/bin/ssh-copy-id: ERROR: ssh: connect to host 10.0.2.15 port 22: Connection refused

root@uji:/home/uji#
```

2. Konfigurasi Autentikasi Pengguna

Berikut adalah hasil dari sudo fw status :

```
root@uji:/home/uji# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
```

Berikut hasil dari sudo ss -tuln :

```
root@uji:/home/uji# sudo ss -tuln
Netid          State           Recv-Q          Send-Q                    Local Address:Port                    Peer Ad
udp            UNCONN          0               0                            127.0.0.54:53                         0.
udp            UNCONN          0               0                         127.0.0.53%lo:53                         0.
udp            UNCONN          0               0                      10.0.2.15%enp0s3:68                         0.
tcp            LISTEN          0               4096                         127.0.0.54:53                         0.
tcp            LISTEN          0               4096                      127.0.0.53%lo:53                         0.
tcp            LISTEN          0               151                          127.0.0.1:3306                       0.
tcp            LISTEN          0               511                            0.0.0.0:80                         0.
tcp            LISTEN          0               70                           127.0.0.1:33060                      0.
tcp            LISTEN          0               511                                [::]:80
root@uji:/home/uji#
```

Autentikasi SSH berbasis key lebih aman daripada password karena beberapa hal :

1. Key lebih panjang dan kompleks (biasanya 2048/4096 bit) dibandingkan dengan password
2. Tidak rentan terhadap brute force attack
3. Dapat dilindungi dengan passphrase tambahan
4. Memungkinkan revoke key tanpa mengubah password sistem

3. Penggunaan Enkripsi dan Efeknya

Sistem enkripsi ini sangat penting karena :

1. Kerahasiaan Data : Mencegah penyadapan data sensitif
2. Integritas Data : Memastikan data tidak diubah selama transmisi
3. Autentikasi : Memverifikasi identitas server (terutama dengan SSL/TLS)

Efek yang terjadi pada keamanan layanan :

1. Port 443 (HTTPS) lebih aman daripada port 80 (HTTP) karena enkripsi SSL/TLS
2. SSH dengan key lebih aman daripada password
3. Firewall membatasi akses hanya ke layanan yang diperlukan

Mitigasi (Kriteria 3)

Port Terbuka yang sebelum dan sesudah terbuka

```
root@uji:/home/uji# sudo ss -tuln
Netid          State           Recv-Q          Send-Q                    Local Address:Port
udp            UNCONN          0               0                            127.0.0.54:53
udp            UNCONN          0               0                         127.0.0.53%lo:53
udp            UNCONN          0               0                    10.0.2.15%enp0s3:68
tcp            LISTEN          0               511                            0.0.0.0:80
tcp            LISTEN          0               4096                      127.0.0.53%lo:53
tcp            LISTEN          0               70                           127.0.0.1:33060
tcp            LISTEN          0               4096                      127.0.0.54:53
tcp            LISTEN          0               151                          127.0.0.1:3306
tcp            LISTEN          0               511                             [::]:80
root@uji:/home/uji#
```

Tindakan yang dilakukan untuk menutup port 3306 dan 21 yaitu sebagai berikut:

sudo ufw deny 3306 sudo ufw

deny 21 sudo nano

/etc/ssh/sshd_config sudo

systemctl ssh

sudo ufw status (menampilkan status port tertutup dan terbuka)

```
root@uji:/home/uji# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
21/tcp                     DENY        Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
21/tcp (v6)                DENY        Anywhere (v6)

root@uji:/home/uji#
```

KESIMPULAN & EVALUASI

Kesimpulan

Paragraf Hasil Parafrase:

Lingkungan server dirancang menggunakan **Ubuntu Server 24.04.2 LTS** yang diinstal melalui platform virtualisasi VirtualBox. Distribusi ini dipilih karena menyediakan dukungan jangka panjang (LTS), dokumentasi teknis yang lengkap, serta komunitas pengguna yang aktif. Infrastruktur server dikonfigurasi dengan menginstal **Apache2** sebagai web server, **MySQL** untuk manajemen basis data, dan **PHP** sebagai bahasa pemrograman backend—semuanya dijalankan melalui manajer paket apt. Skema penamaan pengguna mengikuti format **namalengkap_NIM** untuk memudahkan identifikasi dan administrasi akun di dalam sistem. Proses instalasi berjalan sukses, dan server siap dioperasikan dalam simulasi lokal.

Dari sisi keamanan, **UFW (Uncomplicated Firewall)** dikonfigurasi untuk membuka akses hanya pada port esensial:

- **Port 22** (SSH) untuk manajemen jarak jauh,
- **Port 80** (HTTP) dan **443** (HTTPS) untuk layanan web.
  Port non-kritis seperti **21** (FTP) dan **3306** (Akses Remote MySQL) ditutup menggunakan perintah sudo ufw deny guna mengurangi risiko eksposur serangan eksternal. Validasi dilakukan melalui pemeriksaan status firewall (sudo ufw status) dan pemantauan port aktif (ss -tuln), yang mengonfirmasi hanya port vital yang terbuka.

Autentikasi SSH ditingkatkan dengan mengganti metode berbasis password menjadi **key-based authentication**. Modifikasi pada file /etc/ssh/sshd_config mencakup penonaktifan PasswordAuthentication dan PermitRootLogin untuk mencegah serangan brute-force. Kunci kriptografi **RSA 2048-bit** yang dipasangkan dengan passphrase digunakan untuk memastikan keamanan tambahan.

Pada tahap mitigasi, audit port dengan ss -tuln mengidentifikasi port tidak terpakai seperti **21** dan **3306**, yang kemudian ditutup secara permanen. Verifikasi pasca-tindakan menunjukkan port tersebut tidak lagi merespons koneksi eksternal. Langkah ini sejalan dengan prinsip **Least Privilege** dan **Defense in Depth**, di mana sistem dirancang untuk membatasi akses seminimal mungkin dan menerapkan proteksi berlapis. Hasil akhirnya adalah server dengan eksposur terbatas, autentikasi berbasis kriptografi, serta pengurangan risiko serangan melalui penutupan layanan non-esensial.

.

Evaluasi

Selama proses implementasi, tim menghadapi beberapa kendala teknis yang berhasil diselesaikan. Salah satunya adalah **konflik port antara Apache dan Nginx**, yang muncul ketika keduanya mencoba menggunakan port 80 secara bersamaan. Solusi yang diterapkan adalah menonaktifkan salah satu layanan melalui sudo systemctl stop nginx. Kendala lain adalah **gagalnya koneksi SSH** setelah PasswordAuthentication dinonaktifkan, yang diatasi dengan mengakses langsung console VirtualBox untuk memperbaiki file konfigurasi SSH dan merestart layanan menggunakan sudo systemctl restart ssh. Performa VirtualBox yang awalnya lambat karena RAM 2GB juga diatasi dengan menambah alokasi memori menjadi 4GB, yang meningkatkan stabilitas server secara signifikan.

Evaluasi terhadap keamanan menunjukkan bahwa sistem cukup terlindungi dari serangan dasar. Penggunaan SSH key-based, penutupan port yang tidak diperlukan, dan pembatasan akses firewall memberikan lapisan perlindungan kuat. Namun, **belum dilakukan pengujian penetrasi atau simulasi serangan** untuk menguji efektivitas konfigurasi secara menyeluruh. Selain itu, monitoring sistem real-time belum diterapkan sehingga serangan yang terjadi (jika ada) tidak dapat langsung dideteksi. Hal ini menjadi catatan penting untuk pengembangan lanjutan.

Rekomendasi Pengembangan

Agar sistem lebih aman dan efisien, kami merekomendasikan beberapa pengembangan ke depan. Pertama, penggunaan **Docker** dapat diterapkan untuk menjalankan layanan Apache, MySQL, dan PHP secara terisolasi, yang dapat mengurangi risiko antar-layanan dan meningkatkan kemudahan manajemen. Kedua, disarankan untuk menginstal tools seperti **Fail2Ban** guna mendeteksi dan memblokir IP yang melakukan brute-force login secara otomatis. Ketiga, implementasi **TLS/SSL** menggunakan sertifikat dari **Let's Encrypt** akan meningkatkan keamanan koneksi web secara signifikan. Keempat, mengganti port default SSH (22) ke port acak seperti 2222 dapat mengurangi kemungkinan pemindaian otomatis oleh bot. Terakhir, integrasi sistem monitoring dan logging seperti logwatch atau SIEM akan memperkuat pengawasan terhadap aktivitas mencurigakan.