UNIVERSITAS AMIKOM YOGYAKARTA

LAPORAN 5

SISTEM ADMINISTRATOR & LAYANAN JARINGAN

INSTALASI LAMP PADA CENTOS 7

Dibuat oleh :

Nama : Nurhalis Jusman

NIM : 17.83.0079

Kelas : 17-S1TK-02

A. TUJUAN

1. Mahasiswa da[at memahami apa itu Samba server
2. Mahasiswa dapat memahami fungsi dari Samba Server
3. Mahasiswa dapat mengkonfigurasi Samba Server secara dasar

B. PERALATAN

1. Laptop atau PC
2. Virtual Machine dengan VMware atau Virtual Box
3. VM ber-Sistem Operasi Linux CentOS

C. TEORI SINGKAT

LAMP, adalah sebuah kata yang mengacu pada kombinasi perangkat lunak open source (singkatan). Secara khusus mengacu OS Linux, Web server Apache, database MySQL, pemrograman Perl, PHP, dan Python. Dan LAMP yang mengambil inisial ini. Keduanya cocok untuk pembangunan situs web, termasuk konten dinamis dalam database terkait, dan apa popularitas tinggi. Dalam distribusi OS menjabat sebagai Linux, tetapi beberapa dari LAMP ini telah didistribusikan dalam satu set. software kelompok tersebut, atau tidak lebih murah karena merupakan perangkat lunak open source, karena biaya yang sangat rendah bahkan jika dibutuhkan, adalah mungkin untuk mengurangi biaya, memiliki keuntungan dari Ikaseru yang sangat disesuaikan. sisi lain, jaminan, seperti tidak ada dukungan, risiko besar di bidang manajemen operasional, pengembang, manajer operasi akan dibutuhkan keterampilan sesuai. LAPP Jika Anda ingin menggunakan PostgreSQL ke basis data melalui mesin scan, seperti LASP Jika Anda ingin menggunakan SQLite, kata-kata serupa akan melimpah untuk mengubah singkatan tergantung pada konfigurasi. Selain itu, ada WISA sebagai relatif, ini dimaksudkan untuk menggunakan OS Windows Sever, server Web IIS, database SQL Server, pemrograman ASP.NET, merujuk ke server Web yang dibangun dalam penawaran Microsoft untuk teknologi Anda.

PRAKTEK LAMPP

1. Pertama install Apache

```
[root@localhost ~]# yum install httpd_
```

2. Setelah itu konfigurasi dahulu pada httpd.conf

```
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf
```

Pada file httpd.conf edit seperti pada gambar dibawah ini

```
#Listen 12.34.56.78:80
Listen 192.168.1.1:80_
```

```
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed.  This address appears on some server-generated pages, such
# as error documents.  e.g. admin@your-domain.com
#
ServerAdmin admin@halis.com
```

```
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName halis.com:80
```

3. Kemudian restart httpd nya

```
[root@localhost ~]# systemctl start httpd.service
```

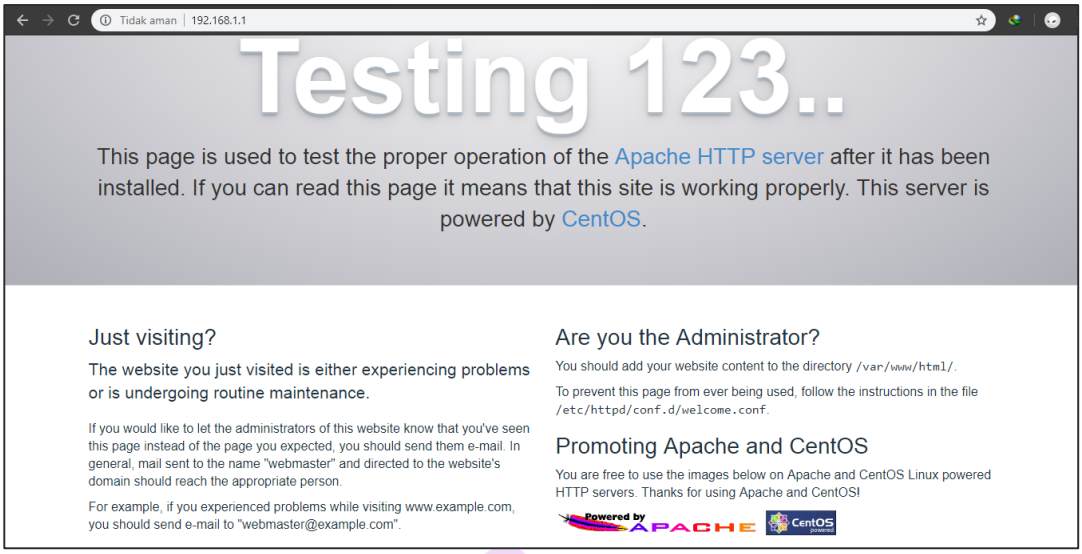
4. Setelah menyalakan service apache, mengenablekan akses http firewallnya

```
[root@localhost ~]# firewall-cmd --permanent --add-service=http
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# _
```

5. Kemudian enable/aktifkan httpdnya

```
[root@localhost ~]# systemctl enable httpd.service
```

6. Kemudian coba akses web browser dengan menggunakan ip public address untuk memastikan service berhasil



7. Selanjutnya melakukan proses installsi MariaDB

```
[root@localhost ~]# yum install mariadb-server
```

8. Kemudian aktifkan service mariaDbnya

```
[root@localhost ~]# systemctl start mariadb
[root@localhost ~]#
```

9. Jangan lupa aktifkan konfigurasi firewallnya

```
[root@localhost ~]# firewall-cmd  --permanent --add-service=mysql
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# _
```

10. Karena setingan awal dari mariadb tidak aman sama sekali makan kita harus amakan dulu dengan menghapus anonymous user dan test database dan menyeting beberapa konfigurasi

```
[root@localhost ~]# mysql_secure_installation
```

```
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] Y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] Y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] Y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] Y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

11. Kemudian aktifkan mariadbnya

```
[root@localhost ~]# systemm enabled mariadb.service
```

12. Selanjutnya penginstalan php

```
[root@localhost ~]# yum install php php-mysql
```

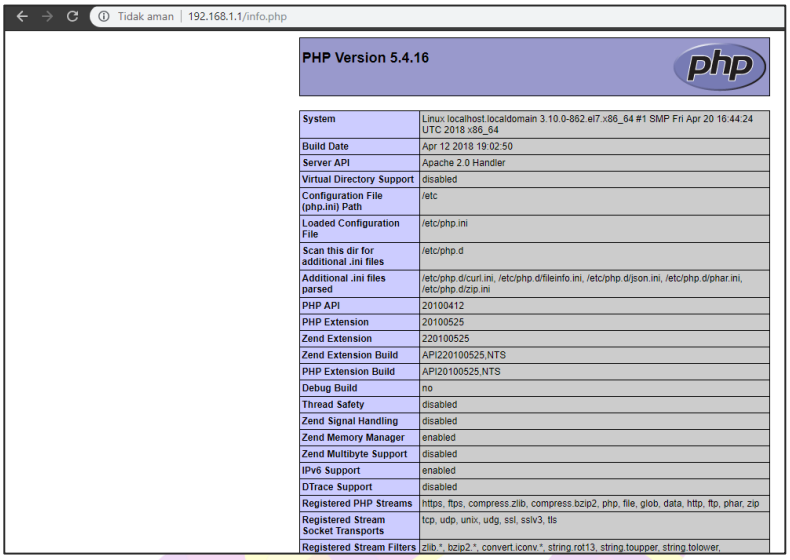
13. Sebelum menggunakan php restart service apache terlebih dahulu

```
[root@localhost ~]# systemctl enable httpd.service
```

14. Kemudian kita melakukan pengetesan PHP, Apache secara default akan membuat directory yaitu '/var/www/html/'. Jadi untuk mencoba PHP nya kita harus menaruh file.php nya di folder tersebut. Dengan cara "# vi /var/www/html/info.php"
Lalu tulisakan kode berikut

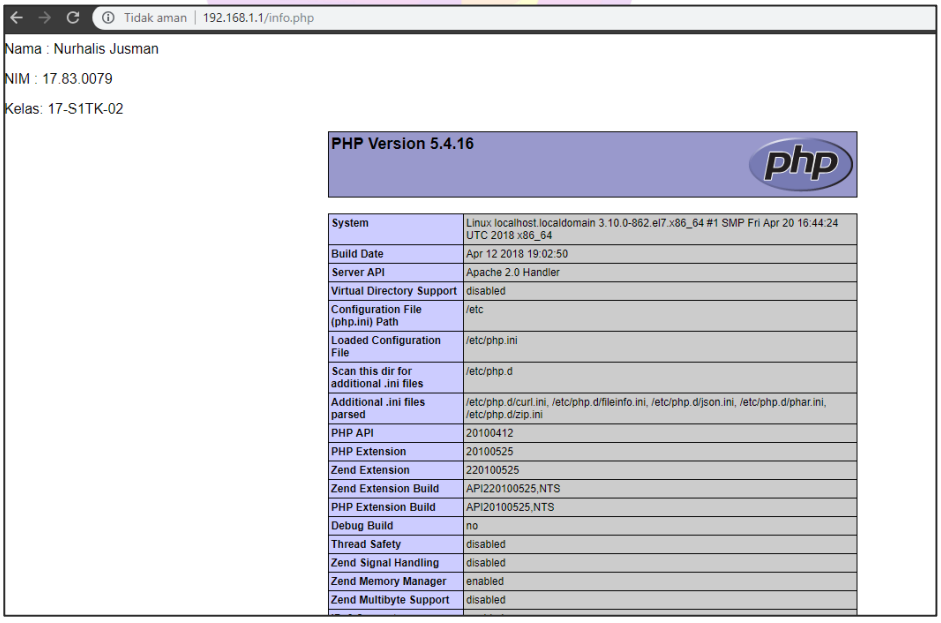
```
<?php
        phpinfo();
?>
~
~
~
~
~
```

15. Untuk mengakses file yang kita buat tadi bisa dengan menuliskan alamat urlnya di browser kita masing – masing, dengan cara **http://ip_address/info.php.** Jika berhasil tanpa ada problem, maka kita akan melihat tampilan webpage-nya seperti berikut ini, Kemudian kita akan mengubah tampilan homepage nya pada file info.php, yang didalam file tersebut berisi nama, nim, dan kelas kita masing – masing



System	Linux localhost.localdomain 3.10.0-862.el7.x86_64 #1 SMP Fri Apr 20 16:44:24 UTC 2018 x86_64
Build Date	Apr 12 2018 19:02:50
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/phar.ini, /etc/php.d/zip.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS
PHP Extension Build	API20100525,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower,

```
<p>Nama  : Nurhalis Jusman<p>
<p>NIM   : 17.83.0079<p>
<p>Kelas: 17-S1TK-02<p>
<?php
        phpinfo();
?>
```



System	Linux localhost.localdomain 3.10.0-862.el7.x86_64 #1 SMP Fri Apr 20 16:44:24 UTC 2018 x86_64
Build Date	Apr 12 2018 19:02:50
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/phar.ini, /etc/php.d/zip.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS
PHP Extension Build	API20100525,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled

Tipe-tipe penyerangan pada web server

1. **DoS:**
   Dalam sebuah serangan Denial of Service (DoS), penyerang mengirimkan sebuah arus permintaan layanan pada mesin server dengan harapan dapat melemahkan semua sumber daya seperti "memory" atau melakukan konsumsi kapasitas processor. Serangan DoS meliputi:
   - Kemacetan jaringan
   - membanjiri service port
   - Melakukan perubahan konfigurasi Routers
   - membanjiri mail server
2. **DDoS:**
   Pada serangan Distributed DoS (DDoS), penyerang melakukan instalasi suatu agent atau daemon pada beberapa host yang telah berhasil dimasuki. Hacker mengirimkan perintah pada bagian master, yang mengakibatkan terkirimnya perintah pada beberapa host slave. Master melakukan komunikasi kepada agent yang berada pada server lain untuk melakukan perintah serangan. DDoS sulit dihalau karena pada umumnya melakukan blokir pada suatu alamat IP single atau jaringan tidak akan menghentikan serangan. Traffic berjalan mulai dari ratusan atau sampai ribuan jumlahnya , pada system server atau komputer individu seringkali tidak mengetahui bahwa komputer-komputernya merupakan bagian dari serangan tersebut.

3. ***FTP Bounce Attack***
   FTP (File Transfer Protocol) digunakan untuk melakukan transfer dokumen dan data secara anonymously dari mesin local ke server dan sebaliknya. Idealnya seorang administrator ftp server mengerti bagaimana serangan ini bekerja. FTP bounce attack digunakan untuk melakukan slip past application-based firewalls.
   dalam sebuah bounce attack, hacker melakukan upload sebuah file aplikasi atau script pada ftp server dan kemudian melakukan request pada file ini dikirim ke server internal. File tersebut dapat terkandung di dalamnya malicious software atau suatu skript yang simple yang membebani server internal dan menggunakan semua memory dan sumberdaya CPU.
   Untuk menghindarkan diri dari serangan ini, FTP daemon pada web server seharusnya melakukan update sercara regular. Site FTP seharusnya dimonitor secara teratur untuk melakukan check apakah terdapat file yang tidak dikenal ditransfer ke web server. Firewall juga membantu dengan cara melakukan filter untuk melakukan blok pada ekstensi file tertentu, sebuah teknik yang dapat melakukan blok terhadap teruploadnya malicious software.

4. ***Port Scanning Attack***
   sebuah port scan adalah ketika seseorang menggunakan software untuk secara sistematik melakukan scan bagian-bagian dari sistem mesin komputer orang lain. hal yang dibolehkan dalam penggunaan software ini adalah untuk manajemen network.
   kebanyakan hacker masuk ke komputer lain untuk meninggalkan sesuatu ke dalamnya, melakukan capture terhadap password atau melakukan perubahan konfigurasi set-up.. metode pertahanan dari serangan ini, melakukan monitor network secara teratur. Ada beberapa free tools yang dapat melakukan monitor terhadap scan port dan aktivitas yang berhubungan dengannya.

5. **Ping Flooding Attack**
   Ping melibatkan satu komputer mengirim sinyal ke anothercomputer mengharapkan respon balik. Penanggungjawab penggunaan ping providesinformation pada ketersediaan layanan tertentu. Ping Flooding adalah theextreme mengirimkan ribuan atau jutaan ping per detik. Ping Banjir cancripple sistem atau bahkan shut down seluruh situs. Meniru Banjir korban banjir Attack jaringan atau mesin dengan IP Pingpackets. Minimal 18 sistem operasi yang rentan terhadap serangan ini, tetapi dapat themajority ditambal. Ada juga banyak router dan printer yang arevulnerable. Patch saat ini tidak dapat diterapkan di seluruh networkeasily global.

6. **Smurf Attack**
   Smurf Attack merupakan modifikasi dari "serangan ping" dan bukannya mengirimkan ping langsung ke sistem menyerang, mereka akan dikirim ke alamat abroadcast korban alamat. Berbagai addressesfrom IP sistem setengah jadi akan mengirimkan ping kepada korban, membombardir thevictim mesin atau sistem dengan ratusan atau ribuan ping. Salah satu solusinya adalah untuk mencegah dari server Web yang usedas broadcast. Router harus dikonfigurasi untuk menolak broadcast IP-Sutradara fromother jaringan ke jaringan. Lain yang sangat membantu mengukur adalah untuk mengkonfigurasi therouter untuk memblokir IP spoofing dari jaringan yang akan disimpan. Router dikonfigurasi assuch akan memblokir setiap paket yang berasal dari donor Network.To ini akan efektif harus dilakukan untuk semua router pada jaringan.

7. **SYN Flooding Attack**
   Serangan ini memanfaatkan kerentanan dalam TCP / IP protokol komunikasi. Serangan ini membuat mesin korban menanggapi kembali ke sistem tidak ada. Korban dikirim paket dan diminta untuk menanggapi sebuah sistem atau mesin dengan alamat IP yang salah. Seperti menjawab, itu dibanjiri dengan permintaan. Permintaan menunggu tanggapan sampai paket mulai waktu keluar dan menjatuhkan. Selama masa tunggu, sistem korban dikonsumsi oleh permintaan dan tidak bisa menanggapi permintaan yang sah. Ketika sebuah koneksi TCP yang normal dimulai, tuan rumah tujuan menerima SYN (menyinkronkan / start) paket dari host sumber dan mengirim kembali SYN ACK (menyinkronkan mengakui) respons. Tujuan host harus yang mendengar pengakuan, atau paket ACK, dari SYN ACK sebelum sambungan dibuat. Ini disebut sebagai "TCP three-way handshake".
   Penurunan batas waktu masa tunggu untuk tiga way handshake dapat membantu untuk mengurangi banjir SYN therisk dari serangan, seperti yang akan meningkatkan ukuran antrian koneksi (ACK SYN antrian). Menerapkan service pack untuk meng-upgrade sistem operasi yang lebih tua juga merupakan tindakan balasan yang baik. Sistem operasi baru-baru ini tahan terhadap serangan ini.

8. **IPFragmentation/Overlapping Fragment Attack**
   Memfasilitasi IP relatif sesak pengiriman melalui jaringan. Paket IP dapat dikurangi dalam ukuran atau pecah menjadi paket yang lebih kecil. Dengan membuat paket-paket yang sangat kecil, router dan sistem deteksi intrusi tidak dapat mengidentifikasi isi paket dan akan membiarkan mereka melewati tanpa pemeriksaan. Ketika sebuah paket disusun kembali pada ujung yang lain, itu buffer overflows. Mesin akan hang, reboot atau mungkin tidak menunjukkan efek sama sekali.
   Dalam Fragmen Tumpang Tindih Attack, paket yang disusun kembali dimulai di tengah paket lain. Sebagai sistem operasi tersebut menerima paket yang tidak valid, itu

mengalokasikan memori untuk menahan mereka. Ini akhirnya menggunakan semua sumber daya memori dan menyebabkan mesin untuk reboot atau menggantung.

9. **IPSequence Prediction Attack**
   Using the SYN Flood method, a hacker can establish connection with a victim machineand obtain the IP packet sequence number in an IP Sequence Prediction Attack.With this number, the hacker can control the victim machine and fool it into believing it's communicating with another network machines. The victim machine will provide requested services. Most operating systems now randomize their sequence numbers to reduce the possibility of prediction.

10. **DNSCache Poisoning**
    DNS menyediakan informasi host didistribusikan digunakan untuk pemetaan nama domain, dan alamat IP. Untuk meningkatkan produktivitas, server DNS cache data yang terbaru untuk pencarian cepat. Cache ini bisa diserang dan informasi palsu untuk mengarahkan sambungan jaringan atau memblokir akses ke situs Web), sebuah taktik licik yang disebut cache DNS keracunan.
    Pertahanan terbaik terhadap masalah seperti keracunan cache DNS adalah dengan menjalankan versi terbaru dari perangkat lunak DNS untuk sistem operasi yang digunakan. Lagu versi baru tertunda dan cerita bersambung mereka untuk membantu mencegah penipuan.

11. **SNMP Attack**
    Kebanyakan dukungan jaringan perangkat SNMP karena aktif secara default. Sebuah Serangan Serangan SNMP dapat mengakibatkan dapat mengakibatkan jaringan yang dipetakan, dan lalu lintas dapat dipantau dan diarahkan.
    Pertahanan terbaik terhadap serangan ini adalah upgrade ke SNMP3, yang mengenkripsi password dan pesan. Sejak SNMP berada pada hampir semua perangkat jaringan, router, hub, switch, Server dan printer, tugas upgrade sangat besar. Beberapa vendor kini menawarkan alat Manajemen SNMP yang meliputi distribusi upgrade untuk jaringan global.

12. **UDP Flood Attack**
    Serangan Banjir UDP sebuah link Serangan dua sistem yang tidak curiga. Oleh Spoofing, banjir UDP hook up sistem UDP satu layanan (yang untuk tujuan pengujian aseries menghasilkan karakter untuk setiap paket yang diterimanya) dengan sistem lain layanan echo UDP (yang gemanya setiap karakter yang diterimanya dalam upaya untuk menguji program jaringan). Akibatnya non-stop banjir data yang tidak berguna betweentwo lewat sistem.

13. **Send Mail Attack**
    Dalam serangan ini, ratusan dari ribuan pesan dikirim dalam waktu yang singkat; load normal biasanya hanya berkisar 100 atau 1000 pesan per jam. Serangan melawan pengiriman email mungkin tidak ber dampak pada bagian depan, tetapi waktu down sebuah pada beberapa website akan terjadi.
    bagi perusahaan yang reputasinya bergantung pada reliablenya dan keakuratan transaksi pada transaksi pada base web, sebuah serangan DoS dapat menjadi pemicu utama dan merupakan ancaman yang serius untuk berjalannya bisnis.