IMPLEMENTASI SISTEM *AUTENTIKASI* TERPUSAT PADA *WIFI ACCES POINT* DI KAMPUS UNHAS MENGGUNAKAN *LDAP*



TUGAS AKHIR

Disusun dalam rangka memenuhi salah satu persyaratan Untuk menyelesaikan program Strata-1 Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin

Makassar

Disusun Oleh:

<u>HANDRI</u>
D42114021

DEPARTEMEN TEKNIK INFORMATIKA FAKULTAS TEKNIK UNIVERSITAS HASANUDDIN

2019

LEMBAR PENGESAHAN SKRIPSI

"IMPLEMENTASI SISTEM AUTHENTIKASI TERPUSAT PADA WIFI ACCESS POINT DI KAMPUS UNHAS MENGGUNAAN LDAP"

OLEH:

HANDRI

D42114021

Skripsi ini telah dipertahankan pada Ujian Akhir Sarjana tanggal 21 Januari 2020. Diterima dan disahkan sebagai salah satu syarat memperoleh gelar Sarjana Teknik (ST.) pada Program Studi S1 Teknik Informatika Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.

Gowa, 27 Januari 2020

Pembimbing II,

NIP. 19830510 201404 1 001

Disetujui oleh:

Pembimbing I,

R., M.IT A. Ais Prayogi, S.T., M.Eng

Dr. Eng Muhammad Niswar, S.R., M.IT NIP. 19730922 199903 1 001



ii

ABSTRAK

Pada saat ini pengguna *wifi* dikampus Universitas Hasanuddin (UNHAS) sangatlah banyak mulai dari mahasiswa, staff hingga dosen. Dengan adanya *wifi* dapat menawarkan beragam kemudahan dalam berkomunikasi dan mencari informasi. Di kampus Universitas Hasanuddin (UNHAS) semua fakultas memiliki tersendiri server jaringannya sehingga cuman *client* di fakultas tersebut yang dapat menggunakan *wifi*.

Untuk meningkatkan kenyamanan dan efisiensi dari penggunaan *wifi* skala besar maka digunakan sistem autentikasi. Hal ini untuk meningkatkan keamanan dalam penggunaan *wifi* dalam meminimalisir resiko serangan, karena data yang terkirim saat melakukan *login* merupakan data *credential* pengguna.

Pada penelitian ini akan mengimplementasikan *authentikasi* terpusat menggunakan *Lightweight Directory Access Protocol (LDAP)*. Penelitian ini juga menyajikan kerangka pengukuran untuk mendukung berbagai tugas pengukuran system authetikasi yang dibuat, seperti *lathency authetikasi dan performansi CPU* pada 50 unit PC. Maka hasil analisis dari implementasi sistem *authentikasi* pada *wifi* unhas adalah *latency authentikasi* selama 232,6 detik dan performansi *CPU* sebesar 25,3%. Sehingga penerapan system berfungsi dengan baik dan *freeradius* digunakan sebagai metode *authentikasi client*.

Kata kunci : Wifi, authentikasi terpusat, Lightweight Directory Access Protocol (LDAP), FreeRADIUS

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas kehadirat TuhanYang Maha Esa karena berkat Rahmat dan Karunia-Nya sehingga Tugas Akhir yang berjudul "IMPLEMENTASI SISTEM AUTENTIKASI TERPUSAT PADA WIFI ACCES POINT DI KAMPUS UNHAS MENGGUNAKAN LDAP" ini dapat diselesaikan sebagai salah satu syarat dalam menyelesaikan jenjang Strata-1 pada Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.

Penyusunan penelitian ini disajikan hasil suatu penelitian yang menyangkut judul yang telah diangkat dan telah melalui proses pencarian dari berbagai sumber baik jurnal penelitian, *prosiding* pada seminar-seminar nasional/internasional, buku maupun dari situs-situs di internet.

Penulis menyadari bahwa dalam penyusunan dan penulisan skripsi ini tidak lepas dari bantuan, bimbingan serta dukungan dari berbagai pihak, dari masa perkuliahan sampai dengan masa penyusunan tugas akhir, sangatlah sulit untuk menyelesaikan tugas akhir ini. Oleh karena itu, penulis dengan senang hati menyampaikan terima kasih kepada:

- Kedua Orang tua penulis, Bapak Lukas Sampe Lapu. dan Alm. Ibu Katrina Masita serta saudara-saudara penulis yang selalu memberikan dukungan, doa, dan semangat serta selalu sabar dalam mendidik penulis sejak kecil;
- Bapak Dr.Eng. Muhammad Niswar, S.T., M.IT., selaku pembimbing I dan Bapak A. Ais Prayogi, ST., M.Eng, selaku pembimbing II yang selalu

menyediakan waktu, tenaga, pikiran dan perhatian yang luar biasa untuk mengarahkan penulis dalam penyusunan tugas akhir;

- Bapak Dr. Amil Ahmad Ilham, S.T., M.IT., selaku Ketua Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin atas bimbingannya selama masa perkuliahan penulis;
- 4) Bapak Dr. Amil Ahmad Ilham, S.T., M.IT., dan Ibu Elly Warni, S.T., M.T yang telah menyempatkan waktunya memberikan saran kepada penulis;
- Bapak Ady Wahyudi Paundu,S.T., M.T. yang yang telah menyempatkan waktunya memberikan saran kepada penulis;
- Pegawai PTIK, khususnya Bapak Lukman Hakim, Kak Ardyansah dan Kak Rendra yang telah membantu saya selama penelitian;
- Keluarga Departemen Teknik Informatika FT-UH angkatan 2014 atas semua bantuan dan semangat yang diberikan selama ini;
- Para teman-teman dan kakak-kakak lab CCIE, SEIS, CBS, IOT, AIMP yang telah memberikan begitu banyak bantuan selama penelitian, pengambilan data dan diskusi *progress* penyusunan Tugas Akhir;
- 9) Teman KMKT 2014 atas dukungan dan semangat yang diberikan selama ini;
- 10) Teman KMKO 2014 atas dukungan dan semangat yang diberikan selama ini;
- 11) Teman Alang Squad atas dukungan dan semangat yang diberikan selama ini;
- 12) Teman-teman Rectifier FT UH atas dukungan dan semangat yang diberikan selama ini;
- Teman KKN 99 TMMD Kepulauan Selayar atas dukungan dan semangat yang diberikan selama ini;

- 14) Segenap Staf Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin yang telah membantu penulis.
- Orang-orang berpengaruh lainnya yang tanpa sadar telah menolong dan menjadi inspirasi penulis.

Akhir kata, penulis berharap semoga Allah SWT. berkenan membalas segala kebaikan dari semua pihak yang telah banyak membantu. Semoga Tugas Akhir ini dapat memberikan manfaat bagi pengembangan ilmu. Aamiin.

Gowa, November 2019

Penulis

DAFTAR ISI

LEMBAR	PENGESAHAN SKRIPSI Error! Bookmark not defined.
ABSTRA	К і
KATA PH	ENGANTARii
DAFTAR	ISIv
DAFTAR	GAMBAR ix
DAFTAR	TABEL xi
BAB I	
1.1.	Latar Belakang 1
1.2.	Rumusan Masalah
1.3.	Tujuan Penelitian
1.4.	Batasan Masalah
1.5.	Manfaat Penelitian
1.6.	Sistematika Penulisan
BAB II	
2.1	Eduroam
2.2	Autentikasi Terpusat
2.3	<i>Wifi</i>
2.4	<i>Proxmox</i>
2.5	RADIUS (Remote Access Dial-in User Service

		2.6.1	. FreeRadius	10
	2.6	L	DAP (Lightweight Directory Access Protocol)	12
		2.6.1	. Fusion Directory	13
		2.6.2	PhpLdapAdmin	14
	2.7	V	Veb Service	14
		2.7.1	Apache	14
		2.7.2	PHP	15
	2.8	P	Putty	16
	2.9	K	Keamanan	17
		2.9.1	. EAP	17
		2.9.2	. TLS/ SSL	17
		2.9.3	EAP-TLS	18
		2.9.4	EAP-TTLS	19
		2.9.5	Protokol 802.1X	20
	2.10). V	Vireless LAN Controller (WLC)	20
BA	AB II	I		22
	3.1	L	okasi dan Waktu Penelitian	22
	3.2	I	nstrumen Penelitian	22
	3.3	Р	Prosedur Penelitian	23
	3.4	Р	Perancangan Sistem	25

3.4.1	Instalasi FreeRadius	. 28
3.4.2	Instalasi OpenLdap	. 32
3.4.3 \$	Setup Fusion Directory	. 35
3.4.4.	Testing	. 40
3.5 Sk	enario Pengujian	. 46
3.5.1	Pengujian Latency Authentikasi	. 46
3.5.2	Pengujian Penggunaan CPU	. 47
BAB IV		. 47
4.1 Ha	sil Penelitian	. 48
4.1.1	Hasil Pengujian Latency Authentikasi	. 48
4.1.2	Pengujian Penggunaan CPU	. 50
4.2 Pe	mbahasan	. 53
4.2.1	Lantency Authentikasi	. 53
4.2.2	Performansi CPU	. 53
BAB V		
5.1 Ke	esimpulan	. 55
5.2 Sa	ran	. 55
DAFTAR PUSTAKA		
LAMPIRAN		. 58

DAFTAR GAMBAR

Nomor	halaman
Gambar 2.1	. 11
Gambar 2.2	. 12
Gambar 2.3	. 14
Gambar 3.1	. 20
Gambar 3.2	. 22
Gambar 3.3	. 22
Gambar 3.4	. 23
Gambar 3.5	. 26
Gambar 3.6	. 26
Gambar 3.7	. 28
Gambar 3.8	. 28
Gambar 3.9	. 30
Gambar 3.10	. 31
Gambar 3.11	. 31
Gambar 3.12	. 32
Gambar 3.13	. 33
Gambar 3.14	. 33
Gambar 3.15	. 34
Gambar 3.16	. 35
Gambar 3.17	. 36
Gambar 3.18	. 37

Gambar 3.19	39
Gambar 3.20	39
Gambar 3.21	40
Gambar 3.22	40
Gambar 3.23	41
Gambar 3.24	42
Gambar 4.1	44
Gambar 4.2	45
Gambar 4.3	46
Gambar 4.4	47
Gambar 4.5	48

DAFTAR TABEL

Nomor	
Tabel 4.1	45
Tabel 4.2	48

BAB I

PENDAHULUAN

1.1. Latar Belakang

Saat ini banyak cara dilakukan untuk memanfaatkan jaringan internet seperti wifi dan menjadi salah satu bagian terpenting dalam dunia kampus. Pada saat ini pengguna wifi dikampus Universitas Hasanuddin (UNHAS) sangatlah banyak mulai dari mahasiswa, staff hingga dosen. Dengan adanya wifi dapat menawarkan beragam kemudahan dalam berkomunikasi dan mencari informasi. Kebanyakkan pengguna bila tiba dikampus mereka segera menyambungkan perangkat mereka dengan wifi kampus. Agar seluruh *client* di kampus Universitas Hasanuddin (UNHAS) dapat mengakses wifi maka dugunakan access point, sebuah access point bisa menjangkau satu atau beberapa ruangan tergantung radius jangkauannya. Pada kampus Universitas Hasanuddin (UNHAS) tiap-tiap fakultas memiliki tersendiri server jaringannya sehingga cuman client di fakultas tersebut yang dapat menggunakannya. Masih ada beberapa kelemahan yang terjadi pada wifi dikampus yang dimana seseorang dapat melihat lalu lintas data pada jaringan, sehingga orang tersebut dapat menangkap data seperti username dan password dan menggunakanya.

Untuk mengatasi beberapa kelemahan diatas maka diterapkan autentikasi terpusat menggunakan protokol *Lightweight Directory Access Protocol (LDAP). Lightweight Directory Access Protocol (LDAP)* adalah sebuah protocol *client-server* yang digunakan untuk mengakses suatu *directory service*. LDAP menggunakan model client-server, dimana client mengirimkan identifier data kepada server menggunakan protokol TCP/IP dan server mencoba mencarinya pada DIT (Directory Information Tree) yang tersimpan di server. Bila ditemukan maka *client* diperbolehkan terhubung ke jaringan *wifi* dan apabila tidak ditemukan maka *client* diminta memasukan ulang identifier data. Jadi dengan menggunakan *Lightweight Directory Access Protocol (LDAP)* pada autentikasi terpusat *wifi access point* kampus maka keamanannya lebih aman dan kita dapat terhubung ke *wifi* selama dalam jangkauan *access point* walaupun di fakultas mana berada.

1.2. Rumusan Masalah

Berdasarkan latar belakang, maka rumusan masalah pada tugas akhir ini adalah:

- Bagaimana menerapkan autentikasi terpusat pada akses wifi access point dengan menggunakan lightweight directory access protocol (LDAP) ?
- 2. Bagaimana kinerja dari sebuah *wifi access point* yang menggunakan *lightweight directory access protocol (LDAP)* ?
- 3. Apa keamanan yang diberikan apabila menggunakan *lightweight directory access protocol (LDAP)* ?

1.3. Tujuan Penelitian

- 1. Untuk mempelajari dan menerapkan sistem autentikasi terpusat pada *wifi access point* di kampus dengan menggunakan *lightweight directory access protocol (LDAP)*.
- 2. Untuk mengetahui kinerja *Lightweight Directory Access Protocol(LDAP)* pada *wfi access point* di kampus.
- 3. Untuk mengetahui keamanan apa yang di berikan menggunakan *lightweight directory access protocol (LDAP)*.

1.4. Batasan Masalah

Yang menjadi batasan masalah dalam tugas akhir ini adalah :

- Membuat autentikasi pengguna *wifi* yang berbasis *lightweight directory* access protocol (LDAP), yang mana Sistem ini akan deterapkan pada Sistem Operasi Linux Ubuntu 18.04.
- 2. Membuat *user* yang bisa *login* pada jaringan *wifi* yang dirancang.
- Perangkat yang digunakan dalam membuat sistem adalah Laptop Asus dengan memori RAM 2Gb dan *Processor Intel Core* i3 4030U *CPU* @1.90GH, *Access Point* Cisco dan *Switch*.

1.5. Manfaat Penelitian

Manfaat dari tugas akhir ini adalah :

1.5.1. Bagi Peneliti

Penelitian ini diharapkan mampu menambah pengetahuan peneliti dalam mengimplementasian sistem autentikasi terpusat menggunakan *lightweight directory access protocol (LDAP)*.

1.5.2. Bagi Client

Penelitian ini diharapkan memberikan kenyamanan dan keamanan bagi *Client* dalam menggunakan *wifi*.

1.5.3. Bagi Pendidikan

Penelitian ini diharapkan mampu menjadi acuan bagi penelitian selanjutnya terutama dalam keamanan *Wifi*.

1.6. Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan.

BAB II TINJAUN PUSTAKA

Pada bab ini akan dijelaskan teori-teori yang menunjang percobaan yang dilakukan.

BAB III METODOLOGI PENELITIAN

Bab ini berisi analisis kebutuhan sistem, perancangan sistem, dan skenario pengujian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi hasil penelitian dan pembahasan penjabaran dari penelitian yang dilakukan.

BAB V PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian dan saran.

BAB II

TINJAUAN PUSTAKA

2.1 Eduroam

Eduroam (education roaming) adalah layanan roaming WLAN antar lembaga akademis dan lembaga penelitian di seluruh dunia. Eduroam memberikan akses layanan internet yang aman kepada pengguna dari sebuah institusi yang berpartisipasi di dalam layanan eduroam ketika pengguna tersebut berkunjung ke institusi lain yang juga berpartisipasi di dalam layanan eduroam. Pengguna hanya perlu menggunakan kredensial dari institusi asalnya untuk proses *authentikasi*. Untuk proses otorisasi dilakukan oleh institusi tempat pengguna tersebut berkunjung. Setelah mendapatkan izin, maka pengguna tersebut akan mendapatkan ip dan dapat melakukan akses internet melalui firewall dan server proxy dari institusi tempat ia berkunjung (Ubaidillah).

Inisiatif eduroam awalnya dimulai pada tahun 2002. TFMobility Klaas Wierenga dari SURFnet yang merupakan bagian dari TERENA (Tran-European Research and Education Networking Association), yang saat ini berganti nama menjadi GÉANT, menyatukan sebuah infrastruktur berbasis RADIUS dengan protokol IEEE 802.1x untuk akses internet roaming antar institusi di Eropa. Tujuan dari berdirinya TERENA adalah untuk mempromosikan dan berpartisipasi dalam pengembangan infrastruktur informasi dan telekomunikasi internasional berkualitas tinggi untuk kepentingan penelitian dan pendidikan. Langkah apapun yang diperlukan akan diambil untuk menunjukkan bahwa infrastuktur yang akan di kembangkan didasarkan pada standar yang terbuka dan menggunakan teknologi paling canggih yang tersedia. Selama masa pengembangannya, pada tahun 2003 sudah mulai banyak institusi di Eropa yang mulai bergabung. Hingga pada tahun 2004, Australia menjadi negara non-Eropa pertama yang terhubung di dalam layanan eduroam. Sampai saat ini, sudah terdapat 89 operator roaming yang tersebar di seluruh dunia yang memberikan akses layanan eduroam (Ubaidillah).

2.2 Autentikasi Terpusat

Autentikasi yaitu proses pengesahan identitas pengguna (*end user*) untuk mengakses jaringan. Proses ini diawali dengan pengiriman kode unik misalnya, *username*, *password*, *pin*, sidik jari oleh pengguna kepada server. Di sisi server, sistem akan menerima kode unik tersebut, selanjutnya membandingkan dengan kode unik yang disimpan dalam *database* server. Jika hasilnya sama, maka server akan mengirimkan hak akses kepada pengguna. Namun jika hasilnya tidak sama, maka server akan mengirimkan pesan kegagalan dan menolak hak akses pengguna (Yesi Novaria Kunang, 2008).

2.3 Wifi

Wifi (Wireless Fidelity) merupakan salah satu varian teknologi komunikasi dan informasi yang bekerja pada jaringan dan perangkat Wireless Local Area Network (WLAN). Sesuai dengan namanya, perangkat yang dibutuhkan untuk mengakses internet dengan layanan ini juga nirkabel. Jika dibandingkan dengan internet lainnya, *Wifi* lebih mudah instalasinya. Namun, pastinya harus ada perangkat utama seperti wireless atau access point dan jaringan internet (Jori David Joseph,2016).

Layanan ini umumnya diperuntukan bagi tempat-tempat umum dengan aksesibilitas yang tinggi seperti pusat perbelanjaan, hotel, kafe, kampus, dan sebagainya. Layanan internet jenis ini dikenal pula dengan istilah hotspot. Untuk mengaksesnya diperlukan gadget yang memiliki fasilitas *Wifi* seperti laptop, netbook/notebook, PDA, atau ponsel (Jori David Joseph,2016).

Kecepatan akses internet wireless tergolong tinggi dan bisa mencapai 54 Mbps. Selain itu koneksi cenderung stabil sehingga proses pengaksesan layanan internet bisa dilakukan dengan lancer (Jori David Joseph,2016).

Jaringan Wifi memiliki standar yang digunakan pada jaringan lokal nirkabel Wireless Local Area Network dan Metropolitan Area Network (WLAN, MAN) yang didasari pada spesifikasi standar Institute of Electrical and Electronic Engineers (IEEE) 802.11, standarisasi jaringan Wifi menggunakan spesifikasi IEEE 802.11 a/b/g [2]. Terdapat tiga metode authentikasi keamanan jaringan Wifi antara lain Wired Equivalent Privacy (WEP), Wireless Protected Access-Pre Shared Key (WPA-PSK), dan WPA2-PSK (Jori David Joseph,2016).

Wifi memiliki kelebihan dan kekurangan. Kelebihan yang dimiliki oleh *wifi* antara lain adalah dengan menggunakan *wifi* kita lebih praktis

karena penggunaannya bisa berpindah-pindah tempat serta hampir semua perangkat teknologi sudah support dengan jaringan *wifi*. Kekurangannya adalah keamanan data yang harus lebih diperhatikan dan sekalipun anda bisa bebas bergerak namun perhatikan jangkauan *wifi*nya karena semakin jauh jangkauannya maka semakin lamban pula koneksinya (NH Sari,2018).

2.4 Proxmox

Proxmox adalah sebuah distro linux virtualisasi berbasis debian 64 bit yang mendukung Openvz dan KVM. Proxmox memungkinkan untuk melakukan manajemen terpusat dari banyak server fisik. Sebuah proxmox terdiri dari minimal satu master local dan beberapa node (Fadjrin,2013)

Proxmox merupakan software open source virtualization platform untuk menjalankan virtual appliance dan virtual machine. Proxmox VE (Virtual Environment) adalah distro khusus yang didekasikan secara khusus sebagai mesin virtualisasi yaitu KVM dan OpenVZ. (Suryono,2012).

Proxmox VE menggunakan Container Virtualization dan Full Virtualization:

• Container Virtualization (OpenVZ) merupakan teknologi yang disarankan untuk menjalankan server linux. OpenVZ membuat beberapa container yangsecure dan terisolasi (disebut juga CT,VE atau VPS). Setiap Container melakukan dan mengeksekusi persis seperti layaknya sebuah *stand alone server*, sebuah container dapat di-reboot secara independen dan memiliki akses *super user ,IP*

address, memori, proses,file, aplikasi, system library dan konfigurasi tersendiri (Suryono,2012).

Full Virtualization (KVM) merupakan singkatan dari (Kernel-based Virtual Machine) adalah solusi virtualisasi penuh untuk hardware berbasis x86 yang memiliki ekstensi virtualisasi (Intel VT datau AMDV *CPU*). Setiap virtual machine memiliki hardware pribadi yang virtual: network card,disk, adapter grafis,dll.KVM mirip dengan XEN akan tetapi KVM merupakan bagian dari Linux dan menggunakan system scheduler dan memory managemen regular dari Linux (Suryono,2012).

2.5 RADIUS (Remote Access Dial-in User Service

RADIUS (*Remote Access Dial-in User Service*) adalah salah satu mekanisme untuk melakukan akses kontrol dalam mengecek dan melakukan autentikasi (*authentication*) *user* atau pengguna yang bedasarkan pada mekanisme autentikasi yang sebelumnya sudah banyak dilakukan, yaitu menggunakan metode *response/challenge*. *Remote Access Dial-in User Service* (RADIUS) dikembangkan pada pertengahan tahun 1990 oleh Livingstone Enterprise (sekarang Lucent Technologies). Pada awal perkembangannya RADIUS mengunakan *port* 1645, namun port tersebut bentrok dengan layanan *datametrics*. Sehingga *port* RADIUS diganti dan sekarang port yang digunakan oleh RADIUS adalah *port* 1812 dengan format standarnya ditetapkan pada RFC (*Request for Command*) 2138 (Muhammad Asfiandi,2014). Server RADIUS memiliki mekanisme keamanan utuk melakukan autentikasi dan autorisasi kepada pengguna sebelum melakukan koneksi. Pada saat computer client ingin melakukan koneksi ke jaringan, maka server RADIUS akan melakukan autentikasi terlebih dahulu dengan meminta identitas pengguna yang merupakan *username* dan *password* untuk dicocokkan dengan data yang terdapat dalam database server RADIUS. Selanjutnya RADIUS akan menentukan apakah pengguna dapat menggunakan layanan jaringan komputer atau tidak. Jika proses autentikasi suksek dilakukan maka akan dilakukan proses pelaporan, yaitu mencatat semua aktivitas koneksi yang dilakukan oleh pengguna di jaringan, baik menghitung durasi waktu koneksi dan jumlah transfer data yang dilakukan oleh pengguna didalam jaringan. Proses pelaporan server RADIUS terhadap pengguna jaringan bias dalam bentuk waktu (detik, menit, jam) maupun dilakukan dalam bentuk besar transfer data (*Byte, Kbyte, Mbyte*) (Muhammad Asfiandi,2014).

2.6.1. FreeRadius

FreeRADIUS merupakan modular yang dikembangkan untuk dapat bekerja dengan performa tinggi dan didistribusikan dibawah lisensi GNU (*General Public License*). *FreeRADIUS* bisa diuduh dan digunakan secara gratis. Meskipun gratis, didalam *FreeRADIUS* sudah mengandung RADIUS server, PAM, module Apache dan banyak tambahan *tool* lainnya (Muhammad Asfiandi,2014). *FreeRADIUS* adalah RADIUS server yang paling banyak digunakan didunia dan menjadi RADIUS server yang paling popular dikalangan Open Source. *FreeRADIUS* suport dengan semua protokol autentikasi dan dilengkapi dengan web administrasi pengguna berbasis PHP yang disebut *dialupadmin. FreeRADIUS* juga mengandung AAA yang dibutuhkan oleh banyak perusahan seperti perusahaan telekomunikasi. *FreeRADIUS* juga merupakan server yang cepat dan memiliki banyak fitur (Muhammad Asfiandi,2014).

Alasan utama banyak yang memilih *FreeRADIUS* adalah mahalnya harga RADIUS server komersial. Sebagai contoh: harga *Interlink's Secure* XS mulai dari \$2375 untuk 250 pengguna, *Funk Odyssey* server \$2500, VOP Radius *Small Business* mulai dari \$995 untuk 100 pengguna. Harga RADIUS server komersial tersebut tidak akan terjangkau untuk pengguna hotspot, terutama untuk kampus (Muhammad Asfiandi,2014).



Gambar 2.1. Alur kerja Radius

Pada gambar 2.1 dimana *user* akan diminta identitas, seperti *username* dan *password*, untuk dapat dicocokkan dengan identitas yang telah dimasukan pada server Radius pada waktu sebelumnya, apabila identitas tersebut terdapat pada server Radius dan identitas yang dimasukan benar maka *user* langsung dapat mengakses internet dengan menggunakan jaringan *wireless (hotspot)* tersebut.

2.6 LDAP (Lightweight Directory Access Protocol)

LDAP adalah sebuah protokol yang mengatur mekanisme pengaksesan layanan direktori (Directory Service) yang dapat digunakan untuk mendeskripsikan banyak informasi seperti informasi tentang people, organizations, roles, services dan banyak entitas lainnya (Aprilia Ayu Mahardani, 2017).

LDAP menggunakan model client-server, dimana client mengirimkan identifier data kepada server menggunakan protokol TCP/IP dan server mencoba mencarinya pada DIT (Directory Information Tree) yang tersimpan di server. Bila di temukan maka hasilnya akan dikirimkan ke client tersebut namun bila tidak maka hasilnya berupa pointer ke server lain yang menyimpan data yang di cari (Aprilia Ayu Mahardani, 2017).

LDAP tersebut memiliki bentuk struktur yang berhirarki, bukannya berformat kolom dan baris, seperti halnya database normal, sehingga memudahkan untuk memasukkan sejumlah besar detail yang mirip dalam bentuk yang terorganisir. Awalnya, server LDAP merupakan sesuatu yang terdapat diantara LDAP client dan sebuah server DAP (X 500), jadi untuk mengurangi resource yang dibutuhkan menjalankan client (Aprilia Ayu Mahardani, 2017).



Gambar 2.2. Alur kerja Ldap

Perancangan dari Gambar 2.2 dapat dilihat hubungan antara LDAP dengan RADIUS. Saat user akan mengakses perangkat, user harus memasukkan ID (username dan password) yang akan diproses oleh RADIUS. RADIUS akan mengambil data dari LDAP saat melakukan otentikasi ID user. Setelah ID terotentikasi, RADIUS akan melakukan proses otorisasi pemberian izin akses untuk user.

2.6.1. Fusion Directory

Fusion Directory adalah aplikasi web di bawah lisensi *GNU* (*General Public License*) dikembangkan di PHP untuk dengan mudah mengelola direktori *LDAP* dan semua layanan terkait (Samsyul Hdidayat, 2012).

2.6.2. PhpLdapAdmin

PhpLDAPAdmin adalah sfotware opensource yang digunakan untuk mempermudah dalam pembuatan database di server LDAP. Dengan phpLDAPAdmin kita tidak perlu bersusah payah mondarmandir ke terminal, sehingga cukup dengan membuka browser dan hanya sesekali melakukan chek ulang via terminal untuk memastikan apakah data yang kita masukkan benar atau salah (Samsyul Hdidayat, 2012).

2.7 Web Service

Web Service adalah aplikasi yang dibuat agar dapat dipanggil dan diakses oleh aplikasi lain melalui internet dengan menggunakan format pertukaran data sebagai format pengiriman pesan, menurut (Yusrizal, 2017).

Web services merupakan sebuah sistem terdistribusi memiliki komponen yang dapat di-deploy dan diakses menggunakan protokol HTTP (Hyper Text Transport Protocol) maupun HTTPS (HTTP Secure). Layanan web dapat di program dalam berbagai bahasa pemograman yang ada. Pada web services sekurang-kurangnya terdapat sebuah web server (jaringan penyedia layanan) dan sebuah klien. Klien meminta layanan yang ditawarkan oleh web server bisa melaui desktop/PC maupun mobile (Yusrizal, 2017).

2.7.1 Apache

Apache merupakan salah satu server web yang paling banyak digunakan di dunia, beberapa keunggulan Apache dibandingkan dengan web server yang lain seperti IIS (Internet Information Service) dari Microsoft adalah kemampuannya untuk mendukung berbagai bahasa script paling populer seperti PHP (Personal Home Page) dan JSP (Java Server Pages). Hal lain yang membuat Apache lebih diminati adalah sistem lisensinya yang gratis sehingga mengurangi biaya yang perlu dikeluarkan dalam membangun situs web dinamis (Andi Wahju,2014).

Apache Web Server merupakan program untuk menjalankan web dalam sebuah komputer. Web service ini akan melayani setiap permintaan dari web browser dan mengirimkan data dalam bentuk html yang bisa dibaca oleh web browser dari pengguna computer (Andi Wahju,2014).

2.7.2 PHP

PHP ialah bahasa skrip dalam server (*server-side embedded scripting language*). Artinya, PHP bekerja di dalam HTML dengan tugas membuat isi dokumen sesuai permintaan.



Gambar 2.3. Diagram Alur Kerja PHP

Pada gambar di atas tampak alur kerja *engine* PHP. Pertamatama, sebuah komputer pengunjung web melakukan HTTP request terhadaphalaman tertentu. Jika halaman yang di*request* tersebut ialah halaman PHP, maka Web Server *Apache* akan meneruskan halaman PHP tersebut ke PHP *engine*. PHP *engine* akan melakukan interpretasi terhadap *source* PHP dalam halaman tersebut, dengan bantuan dari *database* jika perlu. Setelah interpretasi selesai, maka PHP akan mengembalikan hasilnya yang berupa HTML murni (tanpa adanya *source* PHP sama sekali) kepada Web Server *Apache*. Setelah itu Web Server *Apache* akan meneruskannya kepada komputer pengunjung web tadi dalam bentuk HTML yang dapat ditampilkan oleh internet browser (Ihsan Naskah, 2011).

2.8 Putty

Putty adalah sebuah program open source yang dapat Anda gunakan untuk melakukan protokol jaringan SSH, Telnet dan R*login*. Aplikasi ini merupakan aplikasi portable sehingga tidak perlu di install. Protokol ini dapat digunakan untuk menjalankan sesi remote pada sebuah komputer melalui sebuah jaringan, baik itu LAN, maupun internet. Program ini banyak digunakan oleh para pengguna komputer tingkat menengah ke atas, yang biasanya digunakan untuk menyambungkan, mensimulasi, atau mencoba berbagai hal yang terkait dengan jaringan. Program ini juga dapat Anda gunakan sebagai tunnel di suatu jaringan (Andi,2010).

2.9 Keamanan

2.9.1. EAP

EAP adalah sebuah *framework* autentikasi hasil pengembangan IEEE yang berfungsi secara fleksibel. EAP sendiri bukanlah mekanisme autentikasi secara spesifik, EAP hanya menyediakan fungsi *transport* untuk membawa informasi autentikasi yang disediakan oleh *EAP method*. Dengan begitu, jika ada mekanisme autentikasi (*EAP method*) baru, tidak perlu melakukan *upgrade* pada semua peralatan jaringan. Saat ini terdapat lebih dari 40 *EAP method*, namun yang memenuhi standar untuk bekerja di jaringan nirkabel sebagaimana yang dijelaskan pada *Request For Comments* (RFC) 4017 dan telah disertifikasi oleh Wi-Fi Alliance hanya ada tujuh saja, termasuk di antaranya adalah EAP-TLS, EAPTTLS, dan EAP-PEAP (Azhari Harahap, 2011).

2.9.2. TLS/ SSL

TLS (*Transport Security Layer*) dan pendahulunya SSL (*Secure Socket Layer*) adalah protokol kriptografi yang menyediakan keamanan dalam berkomunikasi melalui jaringan. Dalam RFC 2246, dinyatakan bahwa TLS menyediakan keamanan dalam tiga hal :

 Mutual authentication antara klien dan server dengan public key cryptography berdasarkan digital signatures. Dengan ini identitas klien/ server dapat dibuktikan dan pemalsuan pesan dapat dihindari. Algoritme kriptografi kunci publik yang sering digunakan adalah RSA (Rivest, Shamir, Adleman) dan DSA (*Digital Signature Algorithm*).

- Menjaga kerahasiaan data dengan fungsi kriptografi simetrik untuk melakukan enkripsi/ dekripsi data sehingga mencegah pihak ketiga untuk melakukan *eavesdropping*. Algoritme kunci simetrik yang sering digunakan adalah AES (*Advanced Encryption Standard*) dan 3DES (*Triple* DES).
- Menghasilkan Message Authentication Code (MAC) melalui fungsi hash untuk mendeteksi adanya gangguan dan menjaga integritas data. Algoritme hash yang sering digunakan adalah MD5 (Message-Digest Algorithm) dan SHA-1 (Secure Hash Algorithm) (Azhari Harahap, 2011).

2.9.3. EAP-TLS

EAP-TLS merupakan standar EAP *method* pertama yang digunakan dalam jaringan nirkabel serta menyediakan banyak dukungan dari *vendor*. Menurut Sankar e*t al* (2004), pada implementasinya EAP-TLS membutuhkan sertifikat digital dari sisi klien dan juga server. Perlunya sertifikat digital di sisi klien merupakan kelebihan sekaligus kekurangan dari EAP-TLS, karena setiap klien membutuhkan sertifikat digital ke semua klien membutuhkan sumber daya adaministrasi tambahan. Di lain pihak, kelebihannya adalah pada sisi keamanan dimana pihak ketiga

tidak akan bisa melakukan penyerangan tanpa adanya sertifikat digital (Azhari Harahap, 2011).

2.9.4. EAP-TTLS

Sama seperti EAP-TLS, EAP-TTLS (EAPTunneled TLS) juga menggunakan protocol TLS. EAP-TTLS dikembangkan oleh Funk Software dan Certicom. Walaupun memiliki banyak dukungan di berbagai *platform* system operasi seperti Linux dan Mac OS, namun Microsoft Windows tidak memiliki dukungan secara *default*, dibutuhkan aplikasi *third party* agar EAP-TTLS bisa dijalankan. Pada EAP-TTLS, sertifikat digital di sisi klien bersifat *optional*, artinya tidak harus ada. Proses autentikasi dalam EAP-TTLS terbagi dalam dua langkah utama (Azhari Harahap, 2011):

- 1. Pembentukan *secure tunnel*, melalui sertifikat digital dari server, proses ini mirip dengan EAP-TLS.
- 2. Proses autentikasi, yang sering disebut juga *inner authentication*. Autentikasi menggunakan metode autentikasi lain seperti PAP (*Password Authentication Protocol*), CHAP (*Challenge-Handshake Authentication Protocol*), MS-CHAP (Microsoft-CHAP), atau bahkan EAP *method* lain. Data yang dikirim akan di enkripsi oleh *secure tunnel* yang dibentuk di langkah 1. EAP-TTLS mendukung penyembunyian identitas karena data dilewatkan melalui *secure tunnel* (Azhari Harahap, 2011).

2.9.5. Protokol 802.1X

Institute of Electrical and Electronics Engineers (IEEE) 802.1X merupakan standar yang digunakan untuk memberikan autentikasi dan otorisasi ke perangkat yang telah terhubung melalui port Local Area Network (LAN) secara fisik untuk menetapkan autentikasi pointtopoint. Sehingga keamanan jaringan berbasis kabel dalam perusahaan atau organisasi dapat ditingkatkan (CISCO, 2011). Ada banyak implementasi yang telah dilakukan dengan metode autentikasi yang berbeda yang digunakan di standar IEEE 802.1X salah satunya menggunakan EAP-PEAP yang pengimplementasiannya cukup mudah dan memiliki tingkat keamanan yang cukup baik. Adanya implementasi autentikasi pengguna jaringan bertujuan untuk mencegah dan mengurangi adanya tindak kejahatan di jaringan

2.10. Wireless LAN Controller (WLC)

Wireless LAN Controller (WLC) adalah sebuah perangkat yang mengarahkan atau mengatur lalu lintas pada jaringan wireless. WLC biasanya digunakan pada jaringan yang berskala menengah ke besar. Tujuannya adalah untuk memudahkan pengontrolan banyak access point. Split MAC adalah kemampuan untuk membagi tugas antara AP dan WLC. AP bertugas untuk menyediakan layanan 802.11 secara realtime, misalnya menyebarkan beacon, ssid, dan merespon request. Tugas AP berikutnya adalah mengirim ACK kepada client ketika client mengirim data. Tugas WLC pada split MAC adalah authentication, authorization, policy, dan sebagainya.

AP dan WLC berkomunikasi menggunakan protokol *CAPWAP*. CAPWAP adalah singkatan dari *Control and Provisioning of Wireless Access Point*. Ketika client mengirimkan data melalui wireless, frame 802.11 yang diterima AP dari client akan di enkapsulasi kedalam CAPWAP untuk diteruskan ke WLC. WLC juga memiliki kemampuan untuk merubah kekuatan sinyal dari AP untuk mengakomodasi coverage hole detection.

BAB III

METODOLOGI PENELITIAN

3.1 Lokasi dan Waktu Penelitian

Proses penelitian dilakukan sejak bulan Maret 2019. Dan lokasi penelitian dilakukan di Pusat Teknologi Informasi dan Komunikasi Universitas Hasanuddin dan LAB Cloud Computing.

3.2 Instrumen Penelitian

Instrumen yang digunakan pada penelitian ini terdiri dari Hardware dan Software.

1) Hardware

Hardware atau perangkat keras yang dibutuhkan untuk mengimplementasikan rancangan sistem adalah :

- a) Server
- b) WLC (Wireless LAN Controller)
- c) Access Point
- d) PC
- e) Laptop
- 2) Software
 - a) Proxmox
 - b) Ubuntu Server 18.04
 - c) Windows 10
 - d) Freeradius

- e) LDAP (Lightweight Directory Access Protocol)
- f) Fusion Directory
- g) PhpLdapAdmin
- h) Web Service
- i) Apache
- j) Putty

3.3 **Prosedur Penelitian**

Tahapan pada penelitian ditunjukkan pada gambar 3.1



Gambar 3. 1. Diagram Tahapan Penelitian

Tahapan secara garis besar dijelaskan sebagai berikut.:

- Pada studi literatur dilakukan pencarian penelitian terkait dengan LDAP (*Lightweight Directory Access Protocol*) dan juga penelitian sebelumnya yang berkaitan dengan topik penelitian yang dapat menunjang kegiatan penelitian.
- 2. Pada tahap ini, dilakukan desain rancangan sistem yang akan dibuat mulai dari perancangan alur kerja sistem dan perancangan basis data

sistem.

- 3. Pada tahap ini, dilakukan persiapan berbagai jenis instrument yang dibutuhkan dalam penelitian, berupa software maupun hardware.
- 4. Pada tahap ini, desain sistem yang telah dirancang kemudian di implementasikan dan dibangun menggunakan instrument yang sudah disiapkan berupa server, access point, WLC (Wireless LAN Controller), Proxmox, Ubuntu 18.04
- Pada tahap ini, setelah sistem telah dibangun maka dilakukan testing WLC (Wireless LAN Controller) ke LDAP untuk mengetahui apakah konfigurasi yang dilakukan berhasil atau tidak.
- Pada tahap ini setelah sistem telah dibangun maka dilakukan pengambilan data berupa *latency authentikasi* berapa lama selesai *authentikasi* dan performansi *CPU* untuk menlihat kerja *CPU* untuk 50 unit PC.
- 7. Setelah dilakukan pengambilan data, maka data yang diperoleh akan dianalisis untuk mengetahui kinerja dari system yang diterapkan.
3.4 Perancangan Sistem



Gambar 3.2. Rancangan system yang saat ini digunakan

Gambar 3.2 adalah topologi jaringan internet yang ada di kampus UNHAS sekarang. Contoh pada gambar 3.2 terdapat dua fakultas yaitu fakultas A dan fakultas B. Bisa dilihat bahwa fakultas A dan fakultas B memiliki tersendiri routernya maka *login* pengguna hanya dapat dilakukan dimasing-masing fakultas. Pada router tiap fakultas disitu akan terjadi *authentikasi* terhadapa pengguna *wifi* yang ingin *login*. Apabila pengguna dari fakultas A berkunjung ke fakultas B dan ingin menggunakan jaringan *wifi*nya maka pengguna fakultas A tersebut tidak bisa *login* dikarenakan pengguna dari fakultas A tidak terdaftar di fakultas B, begitupun sebaliknya. Pengguna yang dimaksud disini adalah dosen, pegawai, serta mahasiswa yang ada difakultas tersebut. Sehingga pada penelitian ini diterapkan system *authentikasi* terpusat untuk mengatasi masalah diatas.



Gambar 3.3. Rancangan system yang akan diterapkan

Gambar 3.3 adalah rancangan system yang akan dibuat. Pada kotak yang berwarna merah adalah system yang akan *diinstalasi* pada penelitian ini. *Instalasi*nya dapat dilihat pada poin **3.4.1** – **3.4.3**. Setelah system di*instalasi* maka selanjutnya pada *WLC* di*konfigurasi* agar system yang di*instalasi* tadi dapat digunakan dan siap dipancarkan oleh *access point* sehingga pengguna dapat menggunakannya. Konfigurasi tersebut dapat dilihat pada poin **3.4.4**. Apabila system sudah rampung maka jumlah acces point diperbanyak sesuai dengan kebutuhan yang akan digunakan.



Gambar 3.4 Alur proses login

Gambar 3.4 adalah penggambaran dari alur proses terhadap system yang dibuat. Mulai dari pengguna memasukan username dan password. Kemudian dicek apakah kolom username dan password sudah terisi atau tidak. Jika system mendekteksi bahwa salah satu dari kolom username dan password tidak terisi maka akan kembali pada menu inputan. Dan jika kolom inputan telah terisi system akan melanjutkan pada proses pengecekkan kedatabase dimana dalam proses ini terjadi proses validasi atas username dan password yang dimasukkan, yang mana jika salah akan kembali lagi pada menu inputan awal. Tetapi jika benar maka alur proses *login* berhasil.

Perancangan sistem dilakukan sesuai desain rancangan yang telah ditentukan. Dengan beberapa hal yang perlu disiapkan untuk menerapkan sistem, antara lain mempersiapkan perangkat keras yang akan digunakan dan juga instalasi perangkat lunak diperlukan.

Implementasi *LDAP* dan *FreeRadius* pada jaringan *Wifi* kampus UNHAS yang akan dimulai dengan pemasangan server pada pada rak server. Spesifikasi dari server tersebut adalah *CPU* Intel Xeon 8 core, RAM 32GB dan hardisk 2TB. Jika sudah dilakukan pemasangan maka dilanjutkan dengan mebuat virtualisasi LDAP dan FreeRadius pada server. Kemudian install Ubuntu 18.04 pada virtualisasi LDAP dan FreeRadius.

3.4.1 Instalasi FreeRadius

FreeRadius digunakan untuk menangani *authentikasi* dan otorisasi koneksi yang dilakukan user. Pada saat komputer client akan menghubungkan diri dengan jaringan maka server Radius akan meminta identitas user (username dan password) untuk kemudian dicocokkan dengan data yang ada dalam database server untuk kemudian ditentukan apakah user diijinkan untuk menggunakan layanan dalam jaringan komputer. Jika proses *authentikasi* dan otorisasi berhasil maka proses pelaporan dilakukan, yakni dengan mencatat semua aktifitas koneksi user, menghitung durasi waktu dan jumlah transfer data dilakukan oleh user. Install Ubuntu server 18.04 pada virtualisasi FreeRadius yang ada pada server, lalu install FreeRadius pada ubuntu server yang telah terinstall tadi dengan perintah :

a) Instalasi FreeRadius dengan perintah :

sudo apt-get install freeradius freeradius-ldap freeradiusconfig freeradius-mysql freeradius-common freeradius-utils nmap

Fungsi dari perintah diatas untuk menginstall freeradius yang akan digunakan sebagai otentikasi

b) Membuat akun dan sandi test dengan perintah :

nano /etc/freeradius/3.0/users

Fungsi dari perintah diatas untuk membuat akun yang akan

dikoneksikan antara freeradius dengan ldap

c) Mengedit konfigurasi ldap dengan perintah :

```
nano /etc/freeradius/3.0/mods-available/ldap
# isi server dengan alamat ip ke ldap
server = 10.1.2.36
identity = 'cn=admin,dc=unhas,dc=ac,dc=id'
password = *****
base_dn = 'dc=unhas,dc=ac,dc=id'
```

Fungsi perintah diatas untuk membuat identitas ldap

d) Mengcopy file ke mods-enabled dengan perintah :

ln -s /etc/freeradius/3.0/mods-available/ldap

/etc/freeradius/3.0/mods-enabled/ldap

Fungsi diatas untuk menyalin konfigurasi

e) Membuat user baru di FusionDirectory

- → C (0	Not secure 103,195.1	42.175/fusiondirectory/main.php?plug=27	<u>(\$</u>
Users and groups			uid=unhas,ou=people,dc=tdap.dc=unhas,dc=ac.d
Departments	User Unix Groups	s and roles Freeradius References	
Users		Personal information	Progenizational contact information
Groups and roles			
CL roles		Last name* tester	Location
tor, acorgiamento	1000	First name* tester	State
Systems		Description	Address
lystems		Picture Change File Inte Standbarra	
eployment queue		Choose File Ind lie chosen La O	Room No.
Configuration		T Account information	Phone
configuration		in proceed and interest	Mobile
DAP import/export	Base	/	Pager
Reporting	Login*	unhas	Fax
achboard	Preferred language	•	Homepage
200100010	Password method*	ssha 💌	
My account	Password		gE Personal contact information
Jser	Password again		Display name
inix			
reeradius		P Organizational information	Home address
		*	Private phone
	1.000		
	Title	*	
		Add Delete	
	Organization		
	Department		
	Department No		
	England No.		
	Employee No.		Ok Apply Cancel

Gambar 3. 5. Membuat user baru di Fusion Directory

f) Masukkan settingan freeradius

G seb remove taskba	r/dock - Go: 🗙 🛞 FusionDire	ectory X G Id	dap fusiondirectory group bas 🗙 📔 🛞 Plugi	ns - FusionDirecto	ry is the \times 😵 Setting up an LDAP directory v. \times +	- 0	\times
← → C (0	Not secure 103.195.142.175	5/fusiondirectory/main.php?pl	lug=27			\$) :
	ain 🗖 Sign out	8 Manage users				Signed in: fd	d-admin
Users and groups					uid=unhas,ou=peo	ple,dc=ldap,dc=unhas,dc=	ac,dc=id
Departments	User Unix Groups and re	oles Freeradius References	\$				
Users	This account has Freeradius	settings enabled. You can disab	ie them by clicking below.				
Groups and roles ACL roles	Remove Freeradius settings						
ACL assignments		Support 802.1x			Groups		
Systems	Tunnel medium type*	IEEE-802				A	
Systems	Tunnel type*	VIAN	-				
Deployment queue	VI AN M			Groups		w	
Configuration	Evolution data	MM			tester tester V Add Delete		
Configuration	Expiration date						
LDAP import/export		User preferences	\$				
Reporting	Protocol	PPP					
Dashboard	IP Addrose	102 105 142 174					
My account	IP Notress	103.163.142.174					
User	Framed-MTU	1500					
Unix	Compression	Van Jacobean TCR IR					
Groups and roles	Compression	Fremed Lines					
Freeradius	Service type	Framed-User					
	Idle Timeout	10					
	Port limit	2					
	- or min	-					
					0	K Apply Car	ncel

Gambar 3. 6. Masukan settingan FreeRadius

- g) Mengetest koneksi radius ke ldap.
 - 1) Melihat radius bekerja tanpa masalah dengan perintah :

freeradius -X

2) Test koneksi radius ke ldap denfgan perintah :

radtest 'user' 'pass' 'ip' '18120 testing123

h) Freeradius Terhubung dengan LDAP

root@srv-ldap:/# radtest unhas ***** 127.0.0.1 18120

testing123 Sent Access-Request Id 146 from 0.0.0.0:47194 to

127.0.0.1:1812 length 75

User-Name = "unhas"

User-Password = "*****"

NAS-IP-Address = 10.1.2.9

NAS-Port = 18120

Message-Authenticator = 0x00

Cleartext-Password = "*****"

Received Access-Accept Id 146 from 127.0.0.1:1812 to

0.0.0.0:0 length 20

Fungsi diatas untuk *testing* dari *freeradius* ke *ldap* apakah sudah bisa terhubung atau belum.

3.4.2 Instalasi OpenLdap

OpenLdap digunakan oleh program email dan beberapa aplikasi lain untuk mencari dan mengambil informasi dari sebuah direktori yang disimpan pada sebuah server.

Install Ubuntu server 18.04 pada virtualisasi LDAP yang ada pada server, lalu install openldap pada ubuntu server yang telah terinstall tadi dengan perintah :

a) sudo apt-get install -y slapd ldap-utils libarchive-zip-perl

3	10.1.2.35 - PuTTY –	×
Pac	kage configuration	
	Configuring slapd	
	Please enter the password for the admin entry in your LDAP directory.	
	Administrator password:	
	<0k>	

Gambar 3.7. Instalasi openldap

b) Memastikan port Ldap ada dan berjalan dengan perintah :

nmap localhost

P 10.1.2.35 - PuTTY	_		×
e /usr/lib/x86_64-linux-gnu/libblas.so.3 (libblas.so.3-x86_64-linux mode	(-gnu)	in	auto /
Processing triggers for libc-bin (2.27-3ubuntul)			
Processing triggers for man-db (2.8.3-2)			
Setting up liblinear3:amd64 (2.1.0+dfsg-2)			
Setting up liblua5.3-0:amd64 (5.3.3-lubuntu0.18.04.1)			
Setting up nmap (7.60-lubuntu5)			
Processing triggers for libc-bin (2.27-3ubuntul)			
\$ namp localhost			
-sh: 5: namp: not found			
\$ nmap localhost			
Starting Nmap 7.60 (https://nmap.org) at 2019-04-30 06:27 UTC			
Nmap scan report for localhost (127.0.0.1)			
Host is up (0.00023s latency).			
Other addresses for localhost (not scanned): ::1			
rDNS record for 127.0.0.1: localhost.localdomain			
Not shown: 998 closed ports			
PORT STATE SERVICE			
22/tcp open ssh			
389/tcp open ldap			
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds			
			· · · · · · · · · · · · · · · · · · ·

Gambar 3.8. Memastikan port ldap berjalan

c) Membuat base_domain Top lovel domain =unhas.ac.id dengan

perintah:

my_base_dn=
$$(echo "unhas.co.id" | sed -e 's/\./,dc=/g;s/^/dc=/"$$

\$ echo "\$my_base_dn" dc=unhas,dc=co,dc=id

- d) Memasukkan file settingnan
- 1) root@srv-ldap: sed -ie "s/olcSuffix:.*/olcSuffix:

\$my_base_dn/"

 $/etc/ldap/slapd.d/cn\=config/olcDatabase\=\\{1\}mdb.ldif$

2) root@srv-ldap: sed -ie "s/olcRootDN:.*/olcRootDN:

cn=admin,\$my_base_dn/"

 $/etc/ldap/slapd.d/cn\=config/olcDatabase\=\\{1\}mdb.ldif$

- 3) root@srv-ldap: tail -n +3 /etc/ldap/slapd.d/cn\=conf ig/olcDatabase\= $\{1\}$ mdb.ldif > /tmp/db.ldif
- 4) root@srv-ldap: cat /tmp/db.ldif >> /etc/ldap/slapd.d /cn\=config/olcDatabase\=\{1\}mdb.ldif
- e) Install Fusion Directory dan plugin-pluginnya seperti : phpmbstring, fusiondirectory, fusiondirectory-plugin-freeradius, fusiondirectory-plugin, freeradius-schema, fusiondirectoryplugin-ldapmanager,fusiondirectory-plugin-systems,

fusiondirectory-plugin-systems-schema dengan perintah sebagai berikut :

apt-get install -y php-mbstring fusiondirectory fusiondirectoryplugin-freeradius fusiondirectory-plugin-freeradius-schema fusiondirectory-plugin-ldapmanager fusiondirectory-pluginsystems fusiondirectory-plugin-systems-schema

f) Menginstal skema direktori fusion dengan perintah :

sudo fusiondirectory-insert-schema

g) Mengubah skema untuk menentukan jenis objek tambahan

dalam LDAP dan konfigurasi FreeRadius dengan perintah :

sudo fusion
directory-insert-schema -i -c $-\mathrm{y}$

/etc/ldap/schema/fusiondirectory/*

3.4.3 Setup Fusion Directory

a) Di browser masukkan, http://<your VMs IP address/fusiondirectory.

Disini IP dari VMs yaitu http://10.1.2.36/fusiondirectory/

FusionDirectory	× +	– ø ×
← → C () Not se	2cure 103.195.142.174/fusiondirectory/setup.php	☆ 🏟 🗄
• FUSION DIRECTORY	Welcome to FusionDirectory setup wizard	1.0.19
FusionDirectory Setup	This seems to be the first time you start FusionDirectory - we didn't find any configuration right now. This simple wizard intends to help you w	hile setting it up.
Welcome The welcome message	What will the wizard do for you? • Create a basic, single site configuration • Tries to find problems within your PHP and LDAP setup	
Language setup	Let you choose from a set of basic and advanced configuration switches Guided migration of existing LDAP trees	
Installation check	What will the wizard NOT do for you?	
LDAP setup	Find every possible comguration error Migrate every possible LDAP setup - create backup dumps!	
Configuration	To continue: For security reasons you need to authenticate for the installation by creating the file 'Var/cache/fusiondirectory/fusiondirectory auth', contain down bursy-ruling the following command:	ning the current session ID on the servers local filesystem. This can be
LDAP inspection	echo -n vvk4qto2netqun45aqmjpo9ndq > /var/cache/fusiondirectory/fusiondirectory.auth	
Finish	Click the 'Next' button when you've finished.	
		Back Next

Gambar 3.9. Tampilan fusion directory

Kemudian jalankan echo command dari header To Continue dan klik next

b) Language Setting FusionDirectory × + - a × ← → C (Not secure | 103.195.142.174/fusiondirectory/setup.php 🖈) 🍪 🗄 FUSION 📮 Language setup 1.0.19 FusionDirectory Setup Preferred language At this point, you can select the site wide default language. Choosing "automatic" will use the language requested by the browser. This setting can be overn Arabic (%-p-) forzalian (Cotabia) Colombian Spanish (Espeñol Colombiano) Colombian Spanish (Espeñol Colombiano) Colombian Spanish (Espeñol Colombiano) Experied (Nederlands) Dutch (Nederlands) Experied (Nederlands) Preferred language Velcome Language setup is step allows you to ur preferred languag Dutch (Nederlands) Einnish (Suomi) Finnish (Suomi) French (Français) German (Deutsch) Greek (CJANYIKÖ) Italian (Italiano) Norwegian Bokmål (Norsk bokmål) Norwegian Bokmål (Norsk Persian (בע-ב) Polish (Polski) Portuguese (Portuguese) Russian (русский язык) Spanish (Español) Back Next



← → C (① Not secu	are 103.195.142.174/fusiondirectory/setup.php			\$) 🛯) :
FUSION RECTORY	Installation check				1	.0.1
FusionDirectory Setup	PHP module and extension checks		PHP setup configuration (show information))			
Velcome	Checking PHP version	Ok	register_globals = off			Ok
	Checking for LDAP support	Ok	session.gc_maxiifetime >= 86400			Ok
🖌 Language setup	Checking for gettext support	Ok	session.auto_start = Off			Ok
	Checking for curl support	Ok	memory_limit >= 128			Ok
Installation check	Checking for json support	Ok	implicit_flush = Off			Ok
Basic checks for PHP compatibility and extensions	Checking for filter support	Ok	max_execution_time >= 30			
	Checking for iconv support	Ok	expose_php = Off			Ok
LDAP setup	Checking for hash method support	Ok	zend.ze1_compatibility_mode = Off			Ok
	Checking for IMAP support	Ok				
Configuration	Checking for mbstring support	Ok				
	Checking for imagick support	Ok				
LDAP inspection	Checking for compression module support.	Ok				
Theorem						

Gambar 3. 11. Installation check

d) Ldap Setup

* FUSION DIRECTORY	LDAP connection	n setup				1.0.19
FusionDirectory Setup		LDAP connection		Āi	uthentication	
✓ Welcome ✓ Language setup	Location name* Connection URI* TLS connection Base*	IdapUnhas Idap.//localhost 389 C++++++++++++++++++++++++++++++++++++	Admin DN Admin password*	cn=admin	.dc=ac,dc=id	
LDAP setup This dialog performs the basic configuration of the LDAP connectivity for FusionDirectory.	Current status Bind as	Status user 'on-admin,dc-ac.dc-id' failed [Retry]				
Configuration LDAP Inspection Finish						

Gambar 3.12. Setting ldap

*Ldap Connection

Location name : ldapUnhas

Connection URI : ldap://localhost:389

Base : dc=unhas,dc=ac,dc=id

*Authentication

Admin DN : cn=admin

Admin Password : *****

e) Configuration

← → C (Nots	ecure 103.195.14	2.174/fusiondirecto	prv/setup.php				0 7 ☆	6	
	Configur	ration screen o	f FusionDirector	У				1.0.19	
FusionDirectory Setup			Look and feel			Schema setup			
✓ Welcome ✓ Language setup	Language Theme* Timezone*	English (English) breezy 🔻 Asia/Makassar	•	•	Schema validation	×			
Installation check			Password setting	js		Core settings			
V LDAP setup FusionDirectory configuration Configuration screen of FusionDirectory LDAP inspection	Password de Force defaull Password mi Use account SASL Realm SASL Exop	fault hash" t hash Inimum length Inimum differs expiration	ssha Ø		Display summary in listings Edit locking Enable logging LDAP size limit	entryCSN			
Finish	Login attribut Enforce encr Warn if sessi Session iffetti HTTP Basic HTTP Heade Header name	te* ypted connections ion is not encrypted me* authentication r authentication e	Login and session	un	Enable snapshots Snapshot base	Snapshots			
			S.SL.			CAS	Back	Next	

Gambar 3. 13. Configuration screen of FusionDirectory

FusionDirectory	× +					- 0	\times
← → C ① Not secure	103.195.142.174/fusiondirector	y/setup.php				야 ☆ 🧐	÷
	Header name	AUTH_USER					
		\$5L			CAS		
	Key path /etc	/ssl/private/fd.key		Enable CAS			
	Certificate path /etc	/ssl/certs/fd.cert		CA certificate path	/etc/ssl/certs/ca.cert		
	CA certificate path /etc	/ssl/certs/ca.cert		Host	localhost		
				Port	443		
	People and group storage (editing this can break your LDAP)			CAS context	/cas		
	People DN attribute*	uid 🔻					
	CN pattern*	%givenName% %sn%					
	Strict naming policy						
	Group/user min id	100					
	Next id hook						
	Base number for user id	1100					
	Base number for group id	1100					
	Users RDN*	ou=people					
	Groups RDN*	ou=groups					
	ACL role RDN*	ou=aciroles					
	Id allocation method*	Traditional •					
	Pool user id min	10000					
	Pool user id max	40000					
	Pool group id min	10000					
	Pool group id max	40000					
	Restrict role members						
						Back Next	

Gambar 3. 14. Configuration screen of FusionDirectory

Timezone : Asia/Makassar

Password Default hash : ssha

Force default hash: centang ya

f) Ldap Inspection

"Inspecting object classis in root object" pilih "Migrate"

	e 103.195.142.174/tusiondirectory/setup.pnp	ः 🖤 (म
• FUSION RECTORY	LDAP Inspection	1.0.1
FusionDirectory Setup	PHP module and exter	ision checks
Velcome	During the LDAP inspection, we're going to check for several common pitfalls that may occur when migration provide smooth services.	to FusionDirectory base LDAP administration. You may want to fix the problems below, in order to
Language setup	Inspecting object classes in root object Migrate	Failed
	Checking permission for LDAP database	Ok
V LDAP setup	Checking for invisible users	Ok
 FusionDirectory configuration 	Checking for super administrator There is no FusionDirectory administrator account inside your LDAP. Create	Failed
LDAP inspection Analyze your current LDAP for	Checking for default ACL roles and groups Migrate	Default ACL roles have not been inserted
PostonDirectory compatibility	Checking for users outside the people tree	Ok
Finish	Checking for groups outside the groups tree	Ok
	Checking for invisible departments	Ok
	Checking for duplicated UID numbers	Ok
	Checking for duplicated GID numbers	Ok
	Check again	

Gambar 3. 15. Ldap Inpection

Back Next

- Dihalaman selanjutnya pilih "Migrate" lagi
- "Checking for super administrator" pilih "Create"
- Akun super user untuk fusiondirectory

User ID : fd-admin

Password : *****

- Kemudian "Apply"
- "Checking for default ACL roles and groups" pilih 'Migrate'
- Next

g) Finish

FusionDirectory	× +	-	٥	×
← → C (① Not sec	ure 103.195.142.174/fusiondirectory/setup.php	\$:
FUSION	inish - write the configuration file		1.(D. 1 9
FusionDirectory Setup	Create your configuration file			
Velcome	After downloading and placing the file under /eto/fusiondirectory/, please make sure that the user the webserver is running with is able to read fusiondirectory.conf, while other users shouldn't. Run fusiondirectory-setupcheck-config to put the correct right on fusiondirectory conf			
Installation check	Upwindee configuration Status: The configuration is currently not readable or it does not exists.			
V LDAP setup				
configuration				
LDAP inspection				
Write configuration file				
Waiting for cs.gssprt.jp		Bac	k Ne	ext

Gambar 3. 16. Finish setup FusionDirectory

Pilih "Download configuration"

scp file /etc/fusiondirectory di VM(you may need to scp it to your

home directory, and then copy it over)

jalankan "fusiondirectory-setup --check-config"

h) Kemudian Login ke FusionDirectory

<VM ip>/fusiondirectory> = http://10.1.2.36/fusiondirectory/

Masukkan user dan password yang dibuat sebelumnya

FusionDirectory	× +				- 0 ×
← → C (0 M	lot secure 103.195.142.17	5/fusiondirectory/main.php?global_check=1			• 🖈 🧐 :
FUSION	in 📑 Sign out	Welcome System Administra	ator!		Signed in: fd-admin
Users and groups	Users and groups				
Departments Users Groups and roles ACL roles	Departments	(C) Users	Groups and roles	ACL roles	ACL assignments
ACL assignments	Systems				
Systems					
Systems Deployment queue	Systems	Deployment queue			
Configuration	Configuration				
Configuration LDAP import/export	comgutation				
Reporting	Configuration	LDAP import/export			
Dashboard					
My account	Reporting				
User Unix Groups and roles	Dashboard				
Freeradius	My account				
	User	Onix 🛞	Groups and roles	Freeradius	
					@ 2002-2019 The FusionDirectory team, 1.0.19

Gambar 3. 17. Tampilan *login* setelah setting FusionDirectory

3.4.4. Testing

Pada tahap ini kita melakukan pengujian terhadap LDAP dengan WLC untuk mengetahui system yang dirancang dapat terhubung dan siap digunakan. Adapun langkah-langkah sebagai berikut :

a) Membuat User baru di fusiondirectory

A 1411 C D T 1404				D: .						9	~
WLC-PTIKOT			× 🖲 Fusi	onDirectory	×	+			_		
← → C ①	Not s	ecui	re 103.195.142.	175/fusiondirect	ory/main.php	p?plug=27&reset=1			☆	6	:
	in		Sign out	😕 Man	age users	3			Signed	in: fd-ad	Imin
Users and groups	U	ser	5					Filter			
Departments Users	К	<	© © Base [4	Actions -		 Show templates Show functional users 			
Groups and roles			Surname -	Given name	Login	Properties	Actions	Show POSIX users			
ACL assignments		8	Administrator	System	fd-admin	27	x D & A D B 🕇	Search in subtrees			
Systems		8	eduroam	eduroam	eduroam	2 ²	x D 0 2 C 🛱 🖥	Q			
Systems		8	tester	tester	unhas	2 ² (0)	x D & A D B 🕇			Apply filte	ar
Deployment queue	8	3									
Configuration											
Configuration											
LDAP import/export											
Reporting											
Dashboard											
My account											
User											
Unix Groups and roles											
Freeradius											

Gambar 3.18. Membuat user

User : handri Pass : *****

b) Koneksi Radius Dengan WLC

nano /etc/freeradius/3.0/clients.conf
#koneksi ke radius
client 10.1.2.35 {
 ipaddr = 10.1.2.35
 secret =*****
}

```
#koneksi ke ldap
client 10.1.2.36 {
    ipaddr = 10.1.2.36
    secret = *****
}
#koneksi ke wlc
client 10.0.1.23 {
    ipaddr = 10.0.1.23
    secret = *****
}
```

Fungsi diatas untuk memasukkan alamat ip dan sandi pada setiap perangkat yang digunakan dalam penerapan system sehingga perangkat yang digunakan saling terhubung.

c) Memasukkan tipe otentikasi

vi /etc/freeradius/3.0/mods-enabled/eap

eap {

}

default_eap_type = eap_ttls

Fungsi diatas untuk memasukkan tipe otentikasi yang akan digunakan. Pada langkah ini kita akan mengatur keamanan otentikasi terhadap system yang telah dibuat. Bisa dilihat bahwa keamanan yang digunakan yaitu eap terlebih khusus eap_ttls. Proses otentikasi menggunakan eap-ttls terbagi dalam dua langkah utama, yaitu:

- 1. Pembentukan *secure tunnel* melalui sertifikat server.
- 2. Data yang dikirim akan di enkripsi oleh *secure tunnel* yang dibentuk di langkah 1. EAP-TTLS mendukung penyembunyian identitas karena data dilewatkan melalui *secure tunnel*. Sehingga data identitas *client* sangat aman. Data tersebut hanya diketahui oleh *client* dan *server*.

d) Manajemen WLC Security Radius

S WLC-PTIK01	× 🖲 FusionDirectory	× +					-	٥	×
← → C ▲ Not se	ecure https://10.0.1.23/screens/frame	eset.html					1	2 🚳	:
ı. cısco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY	MANAGEMENT	COMMANDS HE	LP FEEDBAC	Sa <u>v</u> e	Configuration Ping L	ogout B n	efresh <u>H</u> ome
Security	RADIUS Authentication Server	rs > Edit					< Back	App	ly
 AAA General RADIUS Authentication Accounting Pallback Downloaded AVP TACACS+ LOAP Local Ho Users Ap Policies Password Policies I Cocal EAP Advanced EAP Priority Order Access Control Lists Wireless Protection Policies Accas CSXP Local Policies Access Control Lists Wireless Protection Policies Accas CSXP Local Policies Accas CSXP Local Policies Accas CSXP Local Policies Advanced 	Server Index Server Address(Ipv4/Ipv6) Shared Secret Pormat Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RPC 3576 Server Timeout Network User Management Retransmit Timeout Tunnel Proxy Realm List IPSec	3 10.1.2.35 ASCII • ••• ••• ••• ••• ••• ••• •••	ners and requires a ke	ay wrap compliant RA	DIUS server)				

Gambar 3. 19. Manajemen WLC

Ip : 10.1.2.35 //ip radius srv

SharedSecret : ***** // /etc/freeradius/3.0/clients.conf

WLC-PTIK01	× 😨 FusionDirectory	× +				-	. 0	×
	secure https://10.0.1.23/screens/fi	rameset.html					\$ 6	
cisco	MONITOR WLANS CONTROL	LER WIRELESS SECUR	ITY MANAGEMENT	COMMANDS	HELP FEEDBACK	Saye Configuration Ping	Logout B	efresh <u>H</u> ome
WLANs	WLANs > Edit 'Eduroam-I	Demo'				< Back	Apply	1
 WLANS WLARS Advanced 	General Security Qo Profile Name Type SSID SSID Status Security Policies Radio Policy Interface/Interface Group(G) Multicast Vian Feature Broadcast SSID NAS-ID NAS-ID Foot Notes I Web Policy cannot be used in of 2(a) FlowComment Local Switching 2(b) Wine Reconnect Local Switching 4 Citers Wine Reconnect Local Switching 4 Citers Wine Resonance Local Switching 4 Citers Wine Resonance Local Switching 4 Citers Wine Resonance Local Switching 2(b) Wine Reconnect Local Switching 10 Wine Reconnect Local Switching 4 Citers Wine Resonance Local Switching 10 Wine Reconnect Local Switching 10 Wine Reconnech	Policy-Mapping Eduroam-Demo VVLAN Eduroam-demo Enabled (WPA2](Auth(802.1X)) (Modifications done under sec All Charter and the sec All Ch	Advanced unity tab will appear aft word AP on connected nected rode will says	ter applying the che or standalane moa WLC as InAB and A	nges.) • ACLs • the AP will act as NAS P as NAS while its on standalor mode to reade excluded Orientic	re mode		

e) Membuat SSID Eduroam-demo

Gambar 3. 20. Membuat SSID

S WLC-PTIK01	X 😨 FusionDirectory X +	- 0 ×
← → C 🔺 Not se	ecure https://10.0.1.23/screens/frameset.html	☆ 🎯 :
սիսիս		Sage Configuration Ping Logout Befresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	A Home
WLANs	WLANs > Edit 'Eduroam-Demo'	< Back Apply
▼ WLANS	General Security Qos Policy-Mapping Advanced	
WLANS	Laura 2 Laura 2 AAA Commer	
P Advanced	Layer 2 Layer 3 AAA Servers	
	Fast Transition	
	Protected Management Frame	
	PME Dicabled Y	
	WPA+WPA2 Parameters	
	WPA Policy	
	WPA2 Forgerition	
	OUZ.12 IN Enable	
	FT R02 1Y Enable	
	FT PSK Enable	
	WPA off-randomize State	
	14 Disable V	
	Foot Notes	
	I Web Policy cannot be used in combination with IPsec. CRANITE authentication, Override Interface ACLs 2(a) Fieckment Local Switching in on supported with IPsec. CRANITE authentication, Override Interface ACLs 2(b) When Rexonnect Local authentication is enabled, irrespective of AP on connected or standalone mode the AWII act as NAS 2(c) When Rexonnect Local authentication is enabled, are on connected mode will use WUC as NAS and AP as NAS while its on standalone mode 3 When client exclusion is enabled, ar Timesul Value of zero means infinity (will require administrative override to reset excluded clients) 4 Client NPF is not active unies WPA2 is configured	

f) Mengatur Security WAP+WAP2, dan mengaktifkan 802.1x

Gambar 3. 21. Mengatur security

g) Memilih radius server yang telah dibuat.

S WLC-PTIK01	× 🔅 FusionDirect	tory × +			-	o ×
← → C ▲ Not se	cure https://10.0.1.23/scr	reens/frameset.html				☆ 🍪 :
uluili. cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> O	NTROLLER WIRELESS SECU	rity m <u>a</u> nagement c <u>o</u> mmand	S HE <u>L</u> P <u>F</u> EEDBACK	Sa <u>v</u> e Configuration <u>P</u> ing	Logout <u>R</u> efresh
WLANs	WLANs > Edit 'Edur	'oam-Demo'			< Back	Apply
▼ WLANs	General Security	QoS Policy-Mapping	Advanced			
Advanced	Layer 2 Layer 3	AAA Servers				
	Select AAA servers bel Radius Servers Radius Server Overw Authentic Problem Server 1 [P10.1.2 Server 2 None Server 3 None Server 3 None Server 6 None Radius Server Account Interim Update LOAP Servers Foot Notes I Web Policy cannot be us 2(a) FlexConnect Local 2(b) When flexconnect to 3 When clant exclusion is 4 Clent Whep Son converted	low to override use of default ser rite interface Enabled cation Servers Accounting Server d	CRANTE authentication, Override Inter CRANTE authentication, Override Inter tive of AP on connected mode standalone anexter mode will use WLC as INAS an anexter mode will use WLC as INAS and anexter mode will use WLC as INAS and and and and an and and and and and and and an and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and and	face ACLs mode the A will act as NAS d AP as NAS while its on standelone moc override to reset excluded clients)	đe	

Gambar 3. 22. Memilih radius server yang telah dibuat

h) Menguji coba koneksi

radtest handri@uhas.ac.id ****** 10.1.2.35 18120 testing123

Fungsi diatas untuk menguji koneksi dari *client* ke server

i) Koneksi Perangkat Mobile dengan LDAP

	奈 × ₄ 🛛 90% 🖬 09.58	8
~		
v	eduroam	
	Metode EAP	
	TTLS 👻	
	Otentikasi tahap 2	
	PAP 👻	
	Sertifikat CA	
	Jangan validasi 👻	
	Sertifikat tidak ditentukan. Sambungan tidak bersifat pribadi.	
	Identitas	
	handri@unhas.ac.id	
	Identitas anonim	
	handri@unhas.ac.id	
	Sandi	
	BATAL SAMBUNGKAN	
10	olodikost	

Gambar 3. 23. Menghubungkan client menggunakan perangkat mobile



Gambar 3. 24. Perangkat mobile sudah terhubung

3.5 Skenario Pengujian

Pengujian dilakukan dengan menggunakan parameter sebagai berikut:

3.5.1 Pengujian Latency Authentikasi

- 1. Menyiapkan 50 unit PC digunakan sebagai *client*
- 2. Menghubungkan 1 unit PC ke jaringan wifi yang telah dibuat untuk melihat berapa lama waktu otentikasinya.
- Setelah data waktu otentikasinya didapat, catat data tersebut untuk dianalisis.
- 4. Ulangi langkah 2 dan 3 dengan jumlah user bertambah satu demi satu sampai dengan 50 unit PC yang harus dikoneksikan secara bersamaan.

 Data yang diperoleh kemudian dianalisis untuk mengetahui waktu yang dibutuhkan setiap PC yang akan terhubung ke jaringan wifi dibuat.

3.5.2 Pengujian Penggunaan CPU

Cara pengujian ini sama dengan langkah pengujian latency otentikasi.

- 1. Menyiapkan 50 unit PC digunakan sebagai client
- 2. Menghubungkan 1 unit PC ke jaringan wifi yang telah dibuat untuk melihat berapa persen penggunaan CPU.
- 3. Setelah data persenan penggunaan CPU didapat, catat data tersebut untuk dianalisis.
- 4. Ulangi langkah 2 dan 3 dengan jumlah user bertambah satu demi satu sampai dengan 50 unit PC yang harus dikoneksikan secara bersamaan.
- Data yang diperoleh kemudian dianalisis untuk mengetahui waktu yang dibutuhkan setiap PC yang akan terhubung ke jaringan wifi dibuat.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Hasil Penelitian

Bab ini menjelaskan keseluruhan hasil pengujian dan analisa dari penerapan sistem yang telah dibuat, dengan demikian akan diketahui performansi dari *latemcy authentikasi* dan penggunaan *CPU*.

4.1.1 Hasil Pengujian Latency Authentikasi

Pada pengujian ini dilakukan menggunakan 50 unit PC yang akan dihubungkan ke jaringan yang telah dibuat. Dibutuhkan 1 unit PC sebagai *monitoring* terhadap 50 unit PC yang akan terhubung. Untuk melihat lantency *Authentikasi* yang diinginkan maka kita mengetikan perintah *freeradius* –*X* di *Command Line Interface (CLI)* pada putty.



Gambar 4.1. User yang terhubung

Fungsi perintah *freeradius* -X adalah untuk menjalankan *authentikasi freeradius* dan sekaligus dapat melihat detail terhadap user yang terhubung, dapat dilihat pada gambar 4.1.

User	Latency Authentikasi (s)
1	4,9
5	24
10	47,9
15	71,4
20	95,5
25	118,3
30	141,3
35	163,8
40	186,4
45	209,9
50	232,6

Tabel 4.1. Hasil pengujian latency pada 1-50 unit PC

Hasil pengujian latency authentikasi dapat dilihat pada table 4.1

dan untuk lebih jelasnya dapat dilihat pada grafik gambar 4.1.



Gambar 4.2. Grafik Latency Authentikasi pada 1-50 unit PC

Berdasarkan gambar 4.2., grafik yang diperoleh dari masingmasing percobaan mulai dari 1 hingga 50 unit PC yang dikoneksikan secara bersamaan maka menunjukan bahwa latency *authentikasi* yang dihasilkan semakin besar. Hal ini dikarena user yang dikoneksikan terus bertambah sehingga waktu yang dibutuhkan juga akan terus bertambah.

4.1.2 Pengujian Penggunaan CPU

Pada pengujian ini dilakukan menggunakan 50 unit PC yang akan dihubungkan ke jaringan yang telah dibuat. Dibutuhkan 1 unit PC sebagai *monitoring* terhadap 50 unit PC yang akan terhubung. Untuk memperoleh penggunaan *CPU* secara *realtime* dapat mengetikan perintah "top -b -n (...) -p (*ID*) / grep (command) > nama_file.txt" di *Command Line Interface* (*CLI*) pada putty. Fungsi *top* yaitu fungsi yang dapat melihat semua fungsi yang sedang berjalan di system, dapat dilihat

🧬 roo	ot@radiusuh: /										- C) ×	(
top - Tasks	13:46:47 : 111 tota	up 1 1,	day, 2 ru	, 4:33, unning,	2 use 69 sle	ers, lo eping,	oad	d avera O stop	ge: ped,	0.07, 0.03, 0 zombie	, 0.00 ≘		^
೪Cpu (Ց	s): 0.0 u	s,	0.2	sy, 0.0) ni, 99	.8 id,	(0.0 wa,	0.	0 hi, 0.0	si, O	.0 st	
KiB Me	em : 4039	432	tota	1, 2826	5812 fre	e, 14	409	976 use	d,	1071644 but	ff/cach	le	
KiB Sv	wap: 4038	652	tota	1, 4038	8652 fre	e,		0 use	d.	3643668 ava	ail Mem	L	
PID	USER	PR	NI	VIRT	RES	SHR	s	%CPU	%MEM	TIME+	COMMAN	ID	
17544	www-data	20		526532	17832	10652	S	0.0	0.4	0:00.00	apache	2	
17545	www-data	20		526532	17756	10588	S	0.0	0.4	0:00.00	apache	2	
17546	www-data	20		526968	18072	10700	S	0.0	0.4	0:00.00	apache	2	
17547	www-data	20		526532	17832	10652	S	0.0	0.4	0:00.00	apache	2	
18174	www-data	20		526532	16772	9640	S	0.0	0.4	0:00.00	apache	2	
23892	root	20					Ι	0.0	0.0	0:00.25	kworke	r/0:0	
24001	root	20					Ι	0.0	0.0	0:00.14	kworke	r/u4+	
24206	root	20					Ι	0.0	0.0	0:00.05	kworke	r/u4+	
24314	root	20					Ι	0.0	0.0	0:00.00	kworke	r/1:1	
24363	root	20		105684	6948	5960	S	0.0	0.2	0:00.03	sshd		
24365	handri	20		76628	7500	6464	S	0.0	0.2	0:00.04	system	ıd	_
24366	handri	20		259388	2720	60	S	0.0	0.1	0:00.00	(sd-pa	im)	
24484	handri	20		107984	5680	4676	S	0.0	0.1	0:00.03	sshd		
24485	handri	20		4628	776	712	S	0.0	0.0	0:00.00	sh		
24494	root	20		66696	4420	3792	S	0.0	0.1	0:00.01	sudo		
24496	root	20		61756	3664	3216	S	0.0	0.1	0:00.00	su		
24497	root	20	0	20312	3884	3332	S	0.0	0.1	0:00.01	bash		~

Gambar 4.3. Tampilan perintah top

Maksud dari perintah "top -b -n (...) -p (*ID*) / grep (command) > nama_file.txt" yaitu " -b" untuk pengiriman ouput yang berasal dari fungsi "top", "-n" untuk menentukan jumlah output yang inginkan, "p" untuk monitor terhadap proses dengan ID yang ditentukan, "|" untuk memberikan input dari suatu output proses yang lain, "grep" untuk mencari kata kunci yang diinginkan, ">" untuk menyimpan *output* ke file yang diinginkan. Pada pengujian ini menggunakan perintah "top -b-n 20 -p 22711 / grep freeradius $-X > Data_skripsi.txt$ " dapat dilihat pada gambar 4.4.

🛃 roo	ot@radiusuh: /								_		Х	_
GNU	nano 2.9.	3		Da	ta_skripsi	.txt						^
GNU 22711 22711 22711 22711 22711 22711 22711 22711 22711 22711 22711 22711 22711 22711	nano 2.9. freerad freerad freerad freerad freerad freerad freerad freerad freerad freerad freerad freerad freerad freerad freerad	3 20 20 20 20 20 20 20 20 20 20 20 20 20	211424 211424 211424 211424 211424 211424 211424 211424 211424 211424 211424 211424 211424 211424 211424 211424 211424	Da 18564 18564 18564 18564 18564 18564 18564 18564 18564 18564 18564 18564 18564	ta skripsi 10524 S 10524 S	txt 0.0 0.7 0.0 1.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0	0.5 0.5 0.5 0.5 0.5 0.5 0.5 0.5 0.5 0.5	0:09.13 0:09.15 0:09.15 0:09.18 0:09.18 0:09.18 0:09.18 0:09.18 0:09.18 0:09.18 0:09.18 0:09.18 0:09.18 0:09.18 0:09.18 0:09.18	freerad freerad freerad freerad freerad freerad freerad freerad freerad freerad freerad freerad	ius ius ius ius ius ius ius ius ius ius		^
22711	freerad	20	211424	18564	10524 S	0.0	0.5	0:09.18	freerad	ius		
22711 22711 22711	freerad freerad freerad	20 20 20	211424 211424 211424	18564 18564 18564	10524 S 10524 S 10524 S	0.0 0.0 0.0	0.5 0.5 0.5	0:09.18 0:09.18 0:09.18	freerad freerad freerad	ius ius ius		

Gambar 4.4. Tampilan capture secara realtime

Untuk pengujian performansi *CPU*, dilakukan pengujian langsung pada 50 unit PC. Pengujian dilakukan secara bertahap mulai dari 1 unit PC hingga 50 unit PC dihubungkan ke jaringan secara bersamaan. Hasil pengujian ditampilkan pada gambar 4.2 berdasarkan data tabel pada halaman lampiran 1.

User	Performasi CPU (%)
1	0,7
5	2,7
10	5
15	7,9
20	11,1
25	15
30	16,6
35	19
40	21,7
45	23,3
50	25,3

Tabel 4.2. Hasil pengujian performansi CPU pada 1-50 unit PC

Hasil pengujian performansi CPU dapat dilihat pada table 4.2

dan untuk lebih jelasnya dapat dilihat pada grafik gambar 4.5.



Gambar 4.5. Grafik rata-rata CPU pada 1-50 unit PC

Berdasarkan gambar 4.5, grafik yang diperoleh dari percobaan 1-50 PC yang dikoneksikan secara bersamaan maka menunjukan bahwa performansi *CPU* memiliki presentase yang terus naik. Hal ini disebabkan karena permintaan dari user yang ingin terhubung terus bertambah sehingga kinerja *CPU* juga akan bertambah. Sehinggga menunjukkan bahwa semakin banyak user yang ingin terhubung maka semakin besar juga jumlah performansi *CPU* yang dihasilkan.

4.2 Pembahasan

4.2.1 Lantency Authentikasi

Berdasarkan tabel 4.1, besar waktu yang dibutuhkan dari 1 – 50 unit PC agar terhubung ke jaringan adalah 4,8 detik – 232,6 detik. *Latency authentikasi* dipengaruhi oleh berapa banyak pengguna yang akan terhubung secara bersamaan. Dengan banyaknya pengguna yang akan terhubung secara bersamaan maka semakin besar waktu yang dibutuhkan. Pada uji coba 50 unit PC secara bersamaan system akan memvalidasi satu per satu pengguna dari setiap 50 unit PC sehingga membutuhkan waktu yang cukup lama untuk menyelesaikan semuanya. Total waktu yang dibutuhkan untuk menyelesaikan proses validasi dari 50 unit PC yaitu 232,6 detik. Sehingga rata-rata untuk menyelesaikan per unit PC dari 50 unit PC yaitu 4,6 detik.

4.2.2 Performansi CPU

Berdasarkan tabel 4.2, besar penggunaan CPU yang dibutuhkan saat 1 – 50 unit PC terhubung ke jaringan adalah 0,7% -25,3%. Penggunaan CPU yang meningkat dipengaruhi oleh berapa banyak pengguna yang akan terhubung secara bersamaan. Dengan banyaknya pengguna yang akan terhubung secara bersamaan maka semakin meningkat *CPU* yang digunakan. Pada uji coba 50 unit PC yang dihubungkan secara bersamaan performansi *CPU* meningkat sampai dengan 25,3%. Jika dirata-ratakan per unit PC membutuhkan 0,5% penggunaan *CPU*.

BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil analisis yang telah dilakukan dalam pengujian sistem *authentikasi* terpusat menggunakan LDAP maka dapat disimpulkan bahwa:

- 1. Penerapan system *authentikasi* terpusat menggunakan LDAP dapat mempermudah client dalam mengakses *wifi* dilingkup kampus UNHAS.
- Semakin banyak pengguna yang terhubung secara bersamaan maka semakin banyak pula waktu yang diperlukan untuk *authentikasi* sehingga semakin lama juga pengguna menuggu.
- Penggunaan LDAP sangat meningkatkan keamanan dimana paket yang dikirim terenkripsi sehingga sulit untuk mengetahuinya.

5.2 Saran

Sehubungan dengan selesainya proses pembuatan skripsi ini, penulis bermaksud menyampaikan beberapa saran kepada para pembaca yakni:

- Sebelum penerapan system yang akan dibuat alangkah baiknya lebih dulu pahami system yang dibuat.
- Perlu adanya pengembangan terhadap otoritas akses sehingga pengguna mempunyai hak akses lebih.

 Untuk pengembangan berikutnya untuk proses *auntentikasi* dengan berbasis freeradius ini jangan hanya diterapkan pada jaringan *wireless*, melainkan juga pada jaringan LAN.

DAFTAR PUSTAKA

Ubaidillah. "Analisis Eduroam Indonesia"

- Yesi Novaria Kunang, 2008. "Autentikasi pengguna wireless LAN berbasis Radius server".
- Jori David Joseph, 2016. "Analisis Trafik Jaringan Wireless Fidelity (*Wifi*) menggunakan Network Protocol Analyzer pada *Authentikasi* WEP".
- Fadjrin, Akbar, Jahnsen Gultom. 2013. "Cloud Computing Server Menggunakan Proxmox Pada CV. Cipta Solusi Sejahtera. STMIK PalComTech Palembang."
- Suryono, 2012. "Pembuatan Prototype Virtual Server Menggunakan Proxmox Ve Untuk Optimalisasi Resource Hardware Di Noc FKIP UNS".
- Muhammad Asfiandi, 2014. "Konfigurasi Freeradius sebagai Radius Server Menggunakan Centos 6.5 di PT. Telekomunikasi Seluler Department IT Operation Regional Sumbagut".
- Aprilia Ayu Mahardani, 2017. "Implementasi Openvpn Menggunakan Ldap Sebagai Manajemen User Pada Sistem Operasi Ubuntu".
- Yusrizal, 2017. "Rancang Bangun Layanan Web (Web Service) Untuk Aplikasi Rekam Medis Praktik Pribadi".
- Azhari Harahap, 2011. "Perbandingan Kinerja Eap-Tls, Eap-Ttls Dan Eap-Peap Sebagai Protokol Autentikasi Pada Jaringan Nirkabel"
- Andre Rizal Sinaga dkk, 2018. "Implementasi Autentikasi Mode Multi-Auth Pada Jaringan Local Area Network Berbasis Kabel Menggunakan Protokol IEEE 802.1X Dan Radius Server"

LAMPIRAN

LAMPIRAN 1

• Hasil proses masukan settingan pada perintah,

cat /tmp/db.ldif >> /etc/ldap/slapd.d

 $/cn=config/olcDatabase=\{1\}$ mdb.ldif :

AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.

CRC32 d2700c21

dn: olcDatabase={1}mdb

objectClass: olcDatabaseConfig

objectClass: olcMdbConfig

olcDatabase: {1}mdb

olcDbDirectory: /var/lib/ldap

olcSuffix: ,dc=unhas,dc=ac,dc=id

olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none

olcAccess: {1}to attrs=shadowLastChange by self write by * read

olcAccess: {2}to * by * read

olcLastMod: TRUE

olcRootDN: cn=admin,dc=unhas,dc=ac,dc=id

olcRootPW::

e1NTSEF9NUZCaHVkWGREMndHWWg1OXVCbTVxUnkyc0VW NlhoOTE= olcDbCheckpoint: 512 30

olcDbIndex: objectClass eq

olcDbIndex: cn,uid eq

olcDbIndex: uidNumber,gidNumber eq

olcDbIndex: member,memberUid eq

olcDbMaxSize: 1073741824

structuralObjectClass: olcMdbConfig

entryUUID: aba9ac0a-ff5c-1038-94e4-5be379cd044a

creatorsName: cn=config

createTimestamp: 20190430062645Z

entryCSN: 20190430062645.289435Z#000000#000#000000

modifiersName: cn=config

modifyTimestamp: 20190430062645Z

dn: olcDatabase={1}mdb

objectClass: olcDatabaseConfig

objectClass: olcMdbConfig

olcDatabase: {1}mdb

olcDbDirectory: /var/lib/ldap

olcSuffix: dc=unhas,dc=ac,dc=id

olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none

olcAccess: {1}to attrs=shadowLastChange by self write by * read olcAccess: {2}to * by * read olcLastMod: TRUE

olcRootDN: cn=admin,dc=unhas,dc=ac,dc=id

olcRootPW::

e1NTSEF9NUZCaHVkWGREMndHWWg1OXVCbTVxUnkyc0VW

NlhoOTE=

olcDbCheckpoint: 512 30

olcDbIndex: objectClass eq

LAMPIRAN 2

• Hasil proses pada perintah, sudo fusiondirectory-insert-schema :

SASL/EXTERNAL authentication started

SASL username:

gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

executing 'ldapadd -Y EXTERNAL -H ldapi:/// -f

/etc/ldap/schema/fusiondirectory/core-fd.ldif'

SASL/EXTERNAL authentication started

SASL username:

gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

adding new entry "cn=core-fd,cn=schema,cn=config"

SASL/EXTERNAL authentication started

SASL username:

gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0

executing 'ldapadd -Y EXTERNAL -H ldapi:/// -f

/etc/ldap/schema/fusiondirectory/core-fd-conf.ldif'

SASL/EXTERNAL authentication started

SASL username:

gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

adding new entry "cn=core-fd-conf,cn=schema,cn=config"

SASL/EXTERNAL authentication started

SASL username:

gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

executing 'ldapadd -Y EXTERNAL -H ldapi:/// -f

/etc/ldap/schema/fusiondirectory/ldapns.ldif'

SASL/EXTERNAL authentication started

SASL username:

gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

adding new entry "cn=ldapns,cn=schema,cn=config"

SASL/EXTERNAL authentication started

SASL username:

gidNumber = 0 + uidNumber = 0, cn = peercred, cn = external, cn = auth

SASL SSF: 0

executing 'ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/fusiondirectory/template-fd.ldif' SASL/EXTERNAL authentication started SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth SASL SSF: 0

adding new entry "cn=template-fd,cn=schema,cn=config"

LAMPIRAN 3

 Hasil proses pada perintah, sudo fusiondirectory-insert-schema -i -c -y /etc/ldap/schema/fusiondirectory/* :

SASL SSF: 0

executing 'ldapadd -Y EXTERNAL -H ldapi:/// -f

/etc/ldap/schema/fusiondirectory/systems-fd.ldif'

SASL/EXTERNAL authentication started

SASL username:

gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

adding new entry "cn=systems-fd,cn=schema,cn=config"

SASL/EXTERNAL authentication started

SASL username:

gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

template-fd already exists in the LDAP, skipping...

LAMPIRAN 4

Hasil proses menguji coba koneksi pada perintah,

radtest handri@uhas.ac.id ****** 10.1.2.35 18120 testing123

(0) Received Access-Request Id 59 from 10.1.2.35:49891 to

10.1.2.35:1812 length 77

- (0) User-Name = "<u>handri@uhas.ac.id</u>"
- (0) User-Password = "*****"
- (0) NAS-IP-Address = 10.1.23
- (0) NAS-Port = 18120

(0) Sent Access-Accept Id 59 from 10.1.2.35:1812 to 10.1.2.35:49891

length 0

(0) Finished request

Waking up in 4.9 seconds.

(0) Cleaning up request packet ID 59 with timestamp +15

LAMPIRAN 5

Hasil dari menguji koneksi Perangkat Mobile dengan LDAP

(8) Received Access-Request Id 29 from 10.0.1.23:32771 to

10.1.2.35:1812 length 313

(8) User-Name = "handri@unhas.ac.id"

- (8) Chargeable-User-Identity = 0x00
- (8) Location-Capable = Civic-Location
- (8) Calling-Station-Id = "0c-98-38-c2-f2-b3"
- (8) Called-Station-Id = "10.0.1.23"
- (8) NAS-Port = 1
- (8) Cisco-AVPair = "audit-session-id=0a000117000ad77b5ce765ea"
- (8) Acct-Session-Id = "5ce765ea/0c:98:38:c2:f2:b3/6286"
- (8) Cisco-AVPair = "mDNS=true"
- (8) NAS-IP-Address = 10.0.1.23
- (8) NAS-Identifier = "WLC-PTIK01"
- (10) Finished request

Waking up in 4.9 seconds.

- (1) Cleaning up request packet ID 22 with timestamp +180
- (2) Cleaning up request packet ID 23 with timestamp +180
- (3) Cleaning up request packet ID 24 with timestamp +180
- (4) Cleaning up request packet ID 25 with timestamp +180
- (5) Cleaning up request packet ID 26 with timestamp +180
- (6) Cleaning up request packet ID 27 with timestamp +180

(7) Cleaning up request packet ID 28 with timestamp +180
(8) Cleaning up request packet ID 29 with timestamp +180
(9) Cleaning up request packet ID 30 with timestamp +180
(10) Cleaning up request packet ID 31 with timestamp +180

LAMPIRAN 6

User	Latency Authentikasi (s)
1	4,8
2	9,7
3	14,5
4	19,2
5	24
6	28,8
7	33,5
8	38,3
9	43,1
10	47,9
11	52,8
12	57,1
13	62
14	66,6
15	71,4
16	76,2
17	81,1
18	85,7

Tabel 4.1. Hasil pengujian latency pada 1-50 unit PC

10	00.6
19	90,6
20	95,5
21	100,3
22	104,6
23	109,2
24	113,6
25	118,3
26	123
27	127,4
28	132
29	136,5
30	141,3
31	145,6
32	150,3
33	154,7
34	159,3
35	163,8
36	168,1
37	172,8
38	177,7
39	182,1
40	186,4
41	191
42	195,9
43	200,6
44	205,1
45	209,9
46	214,3
47	219
48	223,6
1	

49	228,2
50	232,6

LAMPIRAN 7

User	Kinerja CPU (%)
1	0,7
2	1,4
3	1,7
4	2
5	2,7
6	3,4
7	3,7
8	4,3
9	4,7
10	5
11	5,7
12	6,4
13	6,7
14	7
15	7,9
16	8,3
17	9,2
18	10
19	10,6
20	11,1
21	12,4
22	14,3
23	14,4

Tabel 4.2. Hash pengujian Cr 0 1-50 unit rC	Tabel 4.2. Hasi	l pengujian	<i>CPU</i> 1-50) unit PC
----------------------------------------------------	-----------------	-------------	-----------------	-----------

24	14,9
25	15
26	15,3
27	15,7
28	16
29	16,3
30	16,6
31	17
32	17,7
33	18,7
34	18.6
35	19
36	19,5
37	20
38	20,6
39	21,1
40	21,7
41	22
42	22,3
43	22,5
44	23
45	23,3
46	23,9
47	24,4
48	24,7
49	24,9
50	25,3