E-ISSN: 2829-0208

Jurnal Teknik Informatika dan Komputer

https://journal.uhamka.ac.id/index.php/jutikom

Penerapan Tools Fail2Ban Untuk Mencegah Serangan Brute Force Pada Web Server Online Learning Uhamka (OLU)

Yustika Ramadhani[1], Muchammad Sholeh[1*]
Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Prof. Dr. Hamka, Jakarta, Indonesia
[*]Correspondence: m.sholeh@uhamka.ac.id

ABSTRAK

Penelitian ini bertujuan untuk membantu tim *internal* BPTI UHAMKA dalam mengamankan *web server Online Learning* UHAMKA (OLU) sehingga krendensial *login* civitas akademik UHAMKA terlindungi dari percobaan serangan *brute force. Fail2Ban* adalah sebuah *tools* keamanan *server* dimana ia akan mendeteksi percobaan *login attempts* sesuai dengan nilai maksimal percobaan yang telah dikonfigurasi sebelumnya. Dalam penerapannya, *Fail2Ban* yang menggunakan bahasa pemograman python diinstal pada server Online Learning UHAMKA (OLU) yang menggunakan sistem operasi *CentOS 7 Server*. Pada cara kerjanya, *Fail2Ban* akan memblokir atau melakukan *ban* pada *ip address* yang melakukan percobaan *login attempts* berturut-turut dalam kurun waktu satu jam. Berdasarkan hasil perbandingan sebelum dan sesudah penerapannya, dapat dibuktikan bahwa *Fail2Ban* mampu untuk mendeteksi serangan *brute force* yang terjadi dan melakukan *ban* pada *ip address* penyerang.

Kata kunci : *brute force attacks, centOS7, fail2ban*

ABSTRACT

This study aims to assist the internal team of BPTI UHAMKA in making the Online Learning UHAMKA (OLU) web *server so that the login credentials of the UHAMKA academic community are protected from attempted brute force attacks. Fail2Ban is a server security tool where it detects login attempts according to the maximum pre-configured trial value. In its implementation, Fail2Ban which uses the python programming language is installed on the Online Learning UHAMKA (OLU) server that uses the CentOS 7 server operating system. In the way it works, Fail2Ban will block or ban IP addresses that try to log in consecutively within one hour. Based on the comparison before and before its implementation, it can be proven that Fail2Ban can detect brute force attacks that occur and ban the attacker's IP address.*

Keywords : *brute force attacks, centOS7, fail2ban*

1. PENDAHULUAN

Dalam rangka mendukung era digitalisasi pada penyelenggaran universitas yang baik *(good university governance)* di lingkungan Universitas Muhammadiyah Prof. DR. HAMKA, dilakukannya perubahan besar pada sistem informasi dimana seluruh kegiatan dapat dilakukan secara *blended-learning*, baik dalam perkuliahan belajar-mengajar maupun tata kelola penyelenggaraan administrasi. Dengan beroperasinya *Online Learning* UHAMKA (OLU), diharapkan mendukung perkuliahan pada sisi daring dengan harapan mahasiswa dan sivitas akademik dapat terbantu sehingga menjadi efektif dan efisien.

Berdasarkan hasil wawancara yang dilakukan dengan Kepala Bagian Jaringan dan *Server* di BPTI UHAMKA, dalam pengalamannya disebutkan bahwa beberapa sistem UHAMKA pernah mengalami serangan seperti *DDoS, deface injection, brute force*, dan lain lain. Hal ini menjadikan keamanan pada s*erver* perlu dilindungi dengan baik untuk menghindari terjadinya serangan, salah satunya yaitu *brute force attack.*

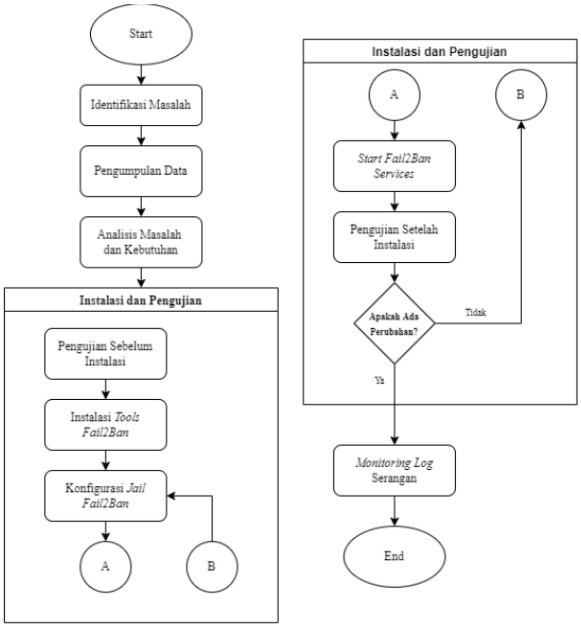
Fail2Ban merupakan aplikasi yang mendukung keamanan *web* aplikasi dengan dilakukannya deteksi intrusi

yang selanjutnya akan meminimalisir serangan dari luar seperti *login attempts* pada kredensial *login* OLU UHAMKA. Dan tindakan dasar *Fail2Ban* sebagai *monitor* serangan dari luar yaitu melarang *IP address* yang mencurigakan tersebut untuk masuk ke dalam aplikasi. Pada hasil akhir penelitian akan melihat perbandingan antara sebelum dan sesudah penerapan dari *tools Fail2Ban*.

Berdasarkan hasil wawancara tersebut menghasilkan fokus pada penelitian ini, yaitu bagaimana melakukan pendeteksian akan serangan *brute force* yang terjadi pada aplikasi *Online Learing* UHAMKA (OLU) dengan menggunakan *tools Fail2Ban,* sehingga keamanan aplikasi bukan lagi kendala yang harus dikhawatirkan.

2. METODOLOGI

Metodologi adalah tata cara yang disusun secara pasti, sistematis dan logis sebagai landasan untuk kegiatan tertentu. Metodologi yang digunakaan pada penelitian ini yaitu *Network Development Life Cycle* (NDLC). Network Development Life Cycle (NDLC) adalah satu metode pada pengembangan dalam jaringan (Sujadi & Mutaqin, 2017). Metode NDLC dinilai sesuai dalam penerapan keamanan server yang dilakukan pada penelitian ini. Tahapan-tahapan penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Diagram alir penelitian

a. Identifikasi Masalah

Proses identifikasi terkait dengan masalah pada aplikasi Online Learning UHAMKA (OLU). Tujuan yang didapatkan dari tahap identifikasi yaitu untuk melindungi kredensial login pengguna dari sistem tersebut.

b. Pengumpulan Data

Dilakukannya pengumpulan data bertujuan untuk memperkuat penelitian dan mempermudah jalannya penelitian. Pengumpulan data yang dilakukan dengan wawancara dan studi literatur. Pengumpulan data dengan wawancara didapatkan dari pihak pengelola server Universitas Muhammadiyah Prof. DR. HAMKA, yaitu Kepala Bagian Jaringan dan Server BPTI UHAMKA. Pengumpulan data dengan studi literatur data yang didapatkan diperoleh dengan mempelajari teori yang berkaitan dengan judul penelitian. Teori tersebut didapatkan dari berbagai sumber seperti jurnal, buku, dan sumber bacaan lainnya.

c. Analisis Masalah dan Kebutuhan

Pada tahap ini dilakukannya analisis terhadap masalah dan kebutuhan yang didapatkan setelah melakukan pengumpulan data. Analisis masalah berisikan rumusan masalah dan batasan masalah yang bertujuan agar penelitian yang dilakukan tidak keluar dari pembahasan. Sedangkan analisis kebutuhan yaitu identifikasi terhadap kebutuhan yang diperlukan dalam penerapan *tools* pencegahan serangan *brute force* agar sesuai dengan tujuan dari penelitian ini.

Brute force attack adalah metode serangan lama untuk menjadikan informasi menjadi mudah untuk dibaca dari pesan yang dienkripsi. Dengan menggunakan *trial-end error* untuk memiliki info *login*, *encrypt key*, atau bahkan mencari halaman web yang tersembunyi, penyerang mengambil semua kemungkinan kombinasi password hingga mendapatkan password yang valid, (Mulyanto et al., 2022). Metode ini dapat disebut sebagai pencarian yang rumit, dengan menggunakan 3 kombinasi karakter berbeda yaitu alfabet, alfabet dengan angka, dan gabungan alfabet, angka, juga simbol, (Laatansa et al., 2019).

Kebutuhan dari hasil dengan wawancara yang dilakukan dengan Kepala Bagian Jaringan dan *Server* BPTI UHAMKA, yaitu:

1) Narasumber ingin meminimalisir resiko serangan keamanan pada *server.*
2) Narasumber ingin dilakukannya *action ban* sementara waktu dengan batas jumlah percobaan *login* dalam waktu yang sudah ditentukan.
3) Narasumber ingin pemantauan keamanan pada sisi *server* sehingga memudahkan pekerjaan *network administrator.*

d. Instalasi dan Pengujian

Tahap ini adalah tahap dari implementasi *tools Fail2Ban* sebagai bentuk solusi dari pencegahan serangan *brute force*. *Fail2Ban* adalah aplikasi yang digunakan untuk mendeteksi kegagalan percobaan login yang kemudian akan memblokir *IP address* asalnya. *Fail2Ban* mengubah aturan konfigurasi dari *firewall* yaitu *IPTable* dengan konfigurasi miliknya sendiri, saat *Fail2Ban* mulai berjalan maka dilakukan pengambilan alih fungsi *firewall* yang ada pada server, dan *Fail2Ban* dapat mengamankan berbagai macam *server* juga memberikan hasil dari serangan ke dalam log data, (Muakhori & Fadlil, 2020). Perlindungan dari *firewall* dapat berupa penolakan, pembatasan akses dan penyaringan akses yang sudah dianggap aman. Peran dan fungsi lain dari *firewall* sendiri yaitu sebagai filter antara komputer internal dan eksternal, juga mengatur kontrol lalu lintas data untuk memberikan izin akses pada jaringan private, (Khadafi et al., 2021).

Adapun metode yang digunakan yaitu *Network Development Life Cycle (NDLC)* dan memiliki tahapan sebagai berikut:

1) Pengujian Sebelum Instalasi
Tahap awal dimana percobaan serangan *brute force* pada port ssh dilakukan dengan menggunakan *tools Medusa.* Melihat apakah celah pada *port* terbuka dan memungkinkan terjadinya serangan.

2) Instalasi *Tools Fail2Ban*
Tahapan selanjutnya dimana instalasi *tools Fail2Ban* dilakukan pada *server Online Learning* UHAMKA (OLU) untuk meminimalisir terjadinya serangan *brute force.*

3) Konfigurasi *Jail Fail2Ban*
Konfigurasi pada *file Jail* dilakukan untuk memilih jenis *service* yang akan digunakan maupun tidak digunakan. Dalam penelitian ini penulis menggunakan *service ssh IP Tables* dan tiap percobaan *login* yang gagal akan terekam dalam *log* direktori dan juga memilih aksi *action_mwl.*

4) *Start Fail2Ban Service*
Tahap ini dimana dilakukannya perintah untuk memulai *service* dari *Fail2Ban* yang dilanjutkan dengan mengecek status *service* apakah sudah *active* atau belum.

5) Pengujian Setelah Instalasi
Tahap ini dilakukannya pengujian setelah instalasi dengan menggunakan *attack tools Medusa* sebagai uji perbandingan sebelum dan sesudah proses instalasi. Dalam tahap ini juga menentukan apakah terjadinya pengulangan pada konfigurasi *file* atau tidak.

e. *Monitoring Log* Serangan

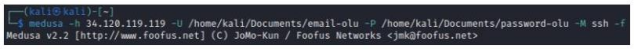
Konfigurasi *file* sebelumnya memiliki *rules* untuk mengirimkan *activity log* ke dalam database *MySQL* dengan merekam nama protokol, *port, ip address* dan waktu. *Fail2SQL* digunakan untuk mempermudah analisa setelah terjadinya penyerangan karena *Fail2SQL* mencatat segala log attacks yang berupa *IP address, port, protocol*, serta waktu saat terjadinya serangan tersebut secara *real time*, (Risqiwati et al., 2018).

3. HASIL DAN PEMBAHASAN

Pada bagian ini menjelaskan mengenai pembahasan dan hasil dari penerapan *tools Fail2Ban* pada *server* OLU UHAMKA. Beberapa tahapan dilakukan meliputi analisis kebutuhan lingkungan, pengujian sebelum penerapan *tools Fail2Ban*, penerapan *tools Fail2Ban*, pengujian setelah penerapan *tools Fail2Ban* dan *log activity*.

3.1 PENGUJIAN SEBELUM INSTALASI *TOOLS FAIL2BAN*

Pada tahap ini dilakukannya percobaan serangan *brute force* pada *target port* yang telah ditentukan sebelum melakukan tahapan instalasi *Fail2Ban.* Percobaan serangan dilakukan dengan *hacking tools Medusa* yang terinstal pada sistem operasi Kali Linux. Perintah yang dituliskan dalam *terminal* berisikan *hostname, file* yang berisikan *user email, file* yang berisikan percobaan *user password* dan *target module.* Perintah yang dijalankan pada terminal *Medusa* dapat dilihat pada Gambar 2.



Gambar 2. Perintah yang dijalankan pada terminal *medusa*

Pada prosesnya, *Medusa* akan mencocokan *file user email* dengan *file user password* satu persatu hingga kedua *file* tersebut cocok dengan kredensial yang ada pada *server* OLU UHAMKA. Apabila sudah ditemukan maka status akan berubah dari *account check* menjadi *account found* seperti pada Gambar 3.

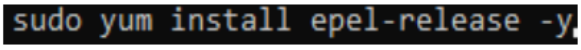
Gambar 3. Hasil percobaan dari serangan *brute force*

3.2 PENERAPAN *TOOLS FAIL2BAN*

Pada tahap ini dilakukan instalasi *tools Fail2Ban* menggunakan *remote access SSH*, berikut adalah langkah-langkah yang dilakukan:

1. *Update repository package*

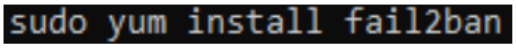
Langkah pertama yang dilakukan yaitu mendapatkan *update* dari *repository* pada *CentOS 7* menggunakan perintah *yum* dengan mengetik perintah pada *cli* seperti pada Gambar 4.



Gambar 4. *Command update repository*

2. *Instalasi tools Fail2Ban*

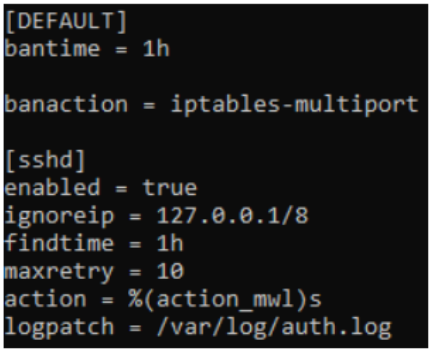
Setelah dilakukannya *update*, dilanjutkan dengan instalasi *Fail2Ban* yang sudah tersedia pada *repository* dengan mengetik perintah pada *cli* seperti pada Gambar 5.



Gambar 5. *Command install fail2ban*

3. Konfigurasi *Jail file* pada *Fail2Ban*

Setelah proses instalasi selesai, selanjutnya melakukan konfigurasi pada *file jail* yang terdapat pada direktori *Fail2Ban* dengan cara menyalin *file jail.conf* menjadi *jail.local.* Selanjutkan masuk ke dalam *editor* dari *file jail.local* dan menuliskan jenis *services* yang akan digunakan. Pada Gambar 6 dilakukan aturan pada *port SSH* dimana setelah percobaan kesepuluh, *iptables* akan melakukan aksi *ban* pada *ip address* penyerang selama 1 jam dan *Fail2Ban* akan menghitung kegagalan percobaan *login* selama 1 jam. Adapun rincian mengenai konfigurasi pada *file jail* dapat dilihat pada Tabel 1.



Gambar 5. Konfigurasi pada file *jail.local*

Tabel 1. Rincian Konfigurasi *Fail2Ban*

Perintah	Fungsi
Bantime = 1h	Melakukan *ban* selama satu jam
Banaction = iptables-multiport	Melakukan aksi *ban* menggunakan *iptables* untuk konfigurasi *firewall* pada setiap *port* yang tersedia
Enable = true	Mengaktifkan fungsi dari konfigurasi *file jail*
Ignoreip = 127.0.0.1/8	Melakukan pengecualian *ban* untuk *local ip address*
Findtime = 1h	Mendeteksi percobaan penyerangan dalam kurun waktu satu jam
Maxretry = 10	Batas maksimal dari serangan percobaan *login*
Action = %(action_mwl)s	Memberikan *alert* pada *administrator*
Logpath = /var/log/auth.log	Lokasi *file* untuk *monitoring* serangan yang telah terjadi

4. Menjalankan *tools Fail2Ban*

Setelah melakukan konfigurasi *file*, kemudian dilakukan perizinan *services Fail2Ban* dengan perintah seperti pada Gambar 6.

```
systemctl enable fail2ban
```

Gambar 6. *Command enable fail2ban*

Setelah memberikan perintah *enable, Fail2Ban* dapat dijalankan dengan perintah seperti pada Gambar 7.

```
systemctl status fail2ban
```

Gambar 7. *Command* menjalankan *fail2ban*

Apabila *Fail2Ban* berhasil dijalankan, status *active* dari *service* tersebut berwarna hijau dan bertuliskan *active (running).*

3.3 PENGUJIAN SETELAH PENERAPAN *TOOLS FAIL2BAN*

Setelah penerapan *tools Fail2Ban* berhasil dijalankan, dilakukan pengujian untuk melihat hasil dari penerapan *tools Fail2Ban* apakah berhasil atau tidak. Pengujian kembali dilakukan dengan menggunakan *hacking tools Medusa* dengan metode *brute force.* Perintah yang dilakukan tetap melakukan serangan *brute force* pada *port SSH* seperti pada Gambar 8.

```
┌──(kali㉿kali)-[~]
└─$ medusa -h 34.120.119.119 -U /home/kali/Documents/email-olu -P /home/kali/Documents/password-olu -M ssh -f
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
```

Gambar 8. Perintah *brute force* setelah penerapan *fail2ban*

Hasil yang didapatkan yaitu penyerang gagal melakukan *brute force* pada percobaan kesepuluh seperti yang terlihat pada Gambar 9. Target secara otomatis menghentikan koneksi antara penyerang dan sistem.

Gambar 9. Hasil pengujian setelah penerapan *tools fail2ban*

3.4 *LOG ACTIVITY*

Pada tahapan instalasi sebelumnya, dilakukan konfigurasi pada *file jail* dimana *log file* akan tersimpan dan masuk ke dalam database *MySQL*. Dapat dilihat pada Gambar 10 dimana terdapat percobaan *login* oleh *ip address* 103.87.60.86 atau penyerang. *Fail2Ban* menghentikan percobaan *login* yang gagal setelah dilakukan sebanyak 10 kali.

Gambar 10. *Log file* pada *fail2ban*

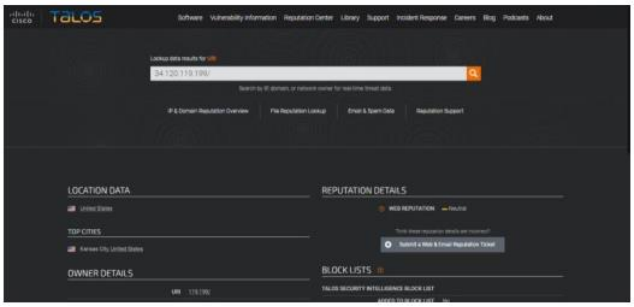
Kemudian setiap laporan percobaan *login* tersebut masuk ke dalam database *MySQL* yang telah dibuat sebelumnya dimana berisikan *port, ip address, count* dan *timestamp* yang terlihat pada Gambar 11 .

Gambar 11. *Report* pada *fail2sql*

3.5 PERBANDINGAN SEBELUM DAN SETELAH PENERAPAN *TOOLS FAIL2BAN*

Pada tahap terakhir yaitu perbandingan sebelum dan sesudah penerapan *tools Fail2Ban* guna mencegah serangan *brute force*. Sebelum menginstal *tools Fail2Ban, tools Medusa* berhasil mencocokan *user login* dan *password* pada *hostname* OLU yang kemudian dilakukan percobaan untuk *login* dan berhasil. Dan setelah menginstal *tools Fail2Ban* dan melakukan serangan *brute force* yang sama, *Fail2Ban* menghentikan koneksi setelah percobaan kesepeluh. Dapat dikatakan bahwa *Fail2Ban* berhasil mencegah serangan *brute force* yang dilakukan.

Setelah penerapan *tools Fail2Ban*, pengujian juga menggunakan alat berupa *website* untuk mendapatkan pengecekan reputasi *web* atau *IP reputation* yaitu Cisco Talos seperti pada Gambar 12. Cisco Talos digunakan karena merupakan alat *publick lookup* dimana kita dapat mengetahui informasi mengenai *ip address. Website* tersebut juga dapat digunakan untuk melihat tingkat reputasi *website (IP reputation)* dengan nilai *unknow, poor, neutral,* dan *good.* Pengecekan dilakukan dengan memasukan *ip address* dari OLU UHAMKA dan mendapatkan nilai *neutral.*



Gambar 12. *Command install fail2ban*

4. KESIMPULAN

Setelah dilakukannya implementasi dari *tools Fail2ban* dan pembahasan yang sudah diuraikan, maka didapatkan kesimpulan sebagai berikut:

1. Penelitian ini berhasil melakukan implementasi *tools Fail2Ban* untuk memproteksi *web* aplikasi *Onlne Learning* UHAMKA dengan dilakukannya pendeteksian sehingga dapat melindungi dan melakukan pencegahan terhadap kemungkinan terjadinya serangan *brute force*. Penerapan keamanan dari serangan *brute force* ini diharapkan dapat membantu untuk melindungi kredensial civitas akademik Universitas Muhammadiyah Prof. DR. HAMKA.
2. Penelitian ini berhasil menghasilkan *report* atas serangan yang telah terjadi kedalam bentuk *table database* menggunakan *PHP MySQL* sehingga mempermudah *system administrator* dalam mengetahui hasil dari pencegahan yang dilakukan *Fail2Ban.*
3. Penelitian ini berhasil menghasilkan pengujian perbandingan sebelum dan sesudah dilakukannya implementasi *tools Fail2Ban* dengan menggunakan *hacking tools Medusa*, dimana sebelum dilakukannya penerapan *tools Fail2Ban Medusa* dapat melakukan serangan *brute force* hingga mendapatkan kombinasi *email* dan *password* yang cocok. Kemudian setelah dilakukannya penerapan *tools Fail2Ban, Medusa* tidak berhasil mendapatkan kombinasi *email* dan *password. Fail2Ban* melakukan tindakan pemutusan koneksi dan *ban* apabila terjadinya pelanggaran pada aturan *Fail2Ban* yang sudah dikonfigurasi. Penulis juga melakukan pengecekan reputasi dari *website* OLU UHAMKA, dengan menggunakan alat pengecekan reputasi Cisco Talos, hasil yang didapatkan yaitu OLU UHAMKA mendapatkan reputasi *web neutral* yang berarti reputasi dianggap netral atau cukup baik

REFERENCES

Khadafi, S., Dian Pratiwi, Y., Alfianto, E., & Adhi Tama Surabaya, T. (2021). Keamanan Ftp Server Berbasiskan Ids Dan Ips Menggunakan Sistem Operasi Linux Ubuntu. In *Jurnal Ilmiah NERO* (Vol. 6, Issue 1).

Laatansa, Saputra, R., & Noranita, B. (2019). *Analysis of GPGPU-Based Brute-Force and Dictionary Attack on SHA-1 Password Hash*. IEEE.

Muakhori, I., & Fadlil, A. (2020). *Security Of Dynamic Domain Name System Servers Against DDOS Attacks Using IPTABLE And FAIL2BA* (Vol. 4, Issue 36).https://iocscience.org/ejournal/index.php/mantik/index

Mulyanto, Y., Herfandi, & Kirana, R. C. (2022). *Analisis Keamanan Wireless Local Area Network (WLAN) Terhadap Serangan Brute Force Dengan Metode Penetration Testing*. *JINTEKS (Jurnal Informatika Teknologi Dan Sains)*, *4*(1), 26–35.

Risqiwati, D., Ari Irawan, E., Teknik, F., & Studi Teknk Informatika, P. (2018). *Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server Realtime Prevention of Brute Force and DDOS Attacks On Ubuntu Server*. *17*(4), 347–354.

Sujadi, H., & Mutaqin, A. (2018). *Rancang Bangun Arsitektur Jaringan Komputer Teknologi Metropolitan Area Network (Man) Dengan Menggunakan MetodeNetwork Development Life Cycle (Ndlc) (Studi Kasus : Universitas Majalengka)*.