

Perancangan Sistem Keamanan Server Linux Ubuntu 18.04 dengan Metode Ufw Firewall, Hardening, Chmod dan Chown pada UNUSIA Jakarta

Fezan Nabawi¹, Agung Budi Susanto², Mardiyanto³

^{1,2,3}Jurusan Teknik Informatika, Fakultas Teknik, Universitas Pamulang

E-mail : ¹fezan@unusia.ac.id, ²dosen02680@unpam.ac.id

Submitted Date: Juli 7, 2022
Revised Date: Agustus 6, 2022

Reviewed Date: Juli 19, 2022
Accepted Date: Agustus 28, 2022

Abstrak

Keamanan sistem operasi server di jaringan sebagai bagian dari keamanan sistem informasi sangat penting untuk menjaga keutuhan data serta menjamin ketersediaan layanan bagi *client*. Keamanan data sangat penting, terutama di area *DeMilitarization Zone (DMZ)* komputer. Namun kadang perlindungan data atau keamanan data, sering dianggap kurang begitu penting dan kurang diperhatikan. Ini menjadi penting diterapkan ketika data telah diserang ataupun dicuri. Seharusnya mengantisipasi sebelum kejadian atau preventif. Sebagai tindakan *preventif* disini menggunakan metode *hardening*, menerapkan *firewall* ufw dan pengaturan hak akses user dan file dengan *chown* dan *chmod*. Komputer server di Unusia terkoneksi dengan jaringan sehingga terdapat ancaman serangan keamanan yang lebih besar dari komputer yang tidak terhubung ke jaringan, dengan keamanan server jaringan maka resiko ancaman kejahatan dapat diminimalisir, sehingga diperlukan perancangan sistem operasi server yang aman. *Firewall* Ufw adalah aplikasi atau alat untuk memfilter paket-paket yang lewat, baik yang akan masuk atau meninggalkan jaringan internal ke publik atau sebaliknya. Akses LAN ke Server DMZ dan ke Internet seharusnya hanya diperbolehkan melalui *firewall*, sehingga dengan *firewall* dapat mengontrol sistem keamanan di jaringan komputer lokal terutama di pusat data server. Metodologi yang digunakan untuk menyusun penelitian adalah menggunakan metode eksperimental dan studi pustaka. langkah awal dalam penelitian ini adalah analisis kebutuhan yang berguna untuk menentukan kebutuhan dalam penelitian. Setelah langkah analisis kebutuhan, desain sistem *hardening server* yaitu dengan cara menerapkan *rule* di *firewall* ufw dan memberikan hak akses user pada masing-masing file dengan *chmod* dan *chown*. Sehingga dengan menerapkan *hardening*, *firewall* ufw, *chmod*, dan *chown* diatas ini dapat memberikan keamanan dan manajemen data yang baik.

Kata Kunci: Sistem Operasi *Server*, *Hardening*, dan *Firewall*

Abstract

Server operating system security on the network as part of information system security is very important to maintain data security and ensure the availability of services for clients. Data security is very important, especially in the *DeMilitarization Zone (DMZ)* area of the computer. However, sometimes data protection or data security is often considered less important and less attention is paid to it. This becomes important when data has been attacked or stolen. Must anticipate before the incident or preventive. As a preventive measure, here we use the *hardening* method, implement a *ufw* firewall and set user and file access rights with *chown* and *chmod*. Computer servers at Unusia are connected to the network so that there is a greater threat of attack from computers that are not connected to the network, with a security server network, the threat of crime can be minimized, so it is necessary to design a secure server operating system. Firewall is



an application or tool to filter the packets that pass, whether that will enter or leave the internal network to the public or vice versa. LAN access to the DMZ Server and to the Internet is only allowed through the firewall, so that the firewall can control the security system on the local computer network, especially in the server data center. The methodology used to organize the research is to use experimental methods and literature study. The first step in this research is a needs analysis which is useful for determining needs in research. After the requirements analysis step, the server hardening system design is implemented by applying the rules in the ufw firewall and granting user access rights to each file with chmod and chown. So by implementing hardening, firewall ufw, chmod, and chown above can provide security and good data management..

Keywords: Server Operating System, Hardening, and Firewall

1. Pendahuluan

Kemajuan perkembangan teknologi komputer dan jaringan dewasa ini sangatlah cepat, dan perangkat tersebut menjadi hal yang sangat penting bagi organisasi untuk pengolahan transaksi data, transfer file, dan lain sebagainya. Pada perkantoran ataupun instansi penggunaan komputer dan internet sudah bukan hal yang asing, apalagi yang bisnis utamanya via internet seperti *e-commerce*, *startup*, dan seterusnya. Jadi perangkat komputer dan Jaringan merupakan kebutuhan yang tidak dapat dielakkan lagi, karena dengan jaringan komputer mereka dapat mengambil data dari komputer lain tanpa mereka harus beranjak dari tempat duduknya, dan dengan jaringan komputer juga kita dapat menyimpan ke banyak perangkat untuk keperluan backup, dimana ini merupakan salah satu bentuk keamanan data. Misalnya, semua file dapat disimpan atau dicopy ke dua, tiga atau lebih komputer yang terkoneksi ke jaringan. Sehingga bila salah satu mesin rusak, maka salinan di mesin yang lain bisa digunakan. Secara umum Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan. Pihak yang meminta/menerima layanan disebut *client* dan yang memberikan/mengirim layanan disebut *server*. Desain ini disebut dengan sistem *client-server* [1]. Jadi pada dasarnya, konektivitas jaringan ini menggunakan komputer server dan

komputer client yang saling terhubung satu sama lain, sehingga dapat saling berbagi file.

Server adalah sebuah sistem komputer yang menyediakan jenis layanan (*service*) tertentu dalam sebuah jaringan komputer. *Server* didukung dengan prosesor yang bersifat scalable dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan [2]. Sistem operasi jaringan yang umum digunakan yakni Linux Server.

Dengan terhubungnya server ke jaringan internet maka serangan dari dunia maya akan semakin meningkat, dan berbagai teknik serangan terus berkembang, sehingga tidak dapat diabaikan. Sebagai tindakan preventif, maka perlu disiapkan keamanan untuk melindungi dan meminimalkan ancaman terhadap *server* Linux yaitu dengan metode *hardening*. *Hardening* bertujuan untuk menambahkan tingkat keamanan pada server. Linux telah menjadi pilihan selain Windows Server, banyak orang IT maupun organisasi untuk menjadikan Linux sebagai sistem operasi server, hal ini dikarenakan salah satu kelebihanannya yakni *open sources*, *secure*, stabil sampai gratis. Kita ketahui pula bahwa *Internet* sebenarnya adalah jaringan komputer besar yang memiliki akses sangat terbuka di dunia, dari situ kita bisa mengakses website, informasi berita, tutorial, video, sampai transaksi pembelian sekarangpun sudah menggunakan internet. namun demikian dalam pengelolaan jaringan memiliki banyak permasalahan diantaranya yang berhubungan dengan keamanan jaringan dan server. Perkembangan teknologi



jaringan komputer, selain banyak manfaat juga memiliki banyak sisi buruk. Salah satunya adalah serangan terhadap sistem komputer yang terhubung ke *Internet*. Sebagai akibat dari serangan tersebut, banyak sistem komputer di organisasi yang terganggu bahkan data-data bisa hilang, rusak dan sebagainya. Oleh karena itu keamanan Jaringan saat ini menjadi tren isu yang sangat penting, karena hampir semua organisasi sudah terkoneksi dengan jaringan komputer dan internet di setiap transaksi bisnis nya, jadi perlu ada pengamanan yang khusus untuk melindungi transaksi-transaksi yang berlangsung. Untuk menanggulangi hal tersebut, diperlukan sistem keamanan yang dapat mencegah kegiatan-kegiatan yang mungkin menyerang server jaringan internal yakni dengan menerapkan firewall. Di dalam firewall semua komunikasi yang keluar dan masuk akan difilter atau dikontrol, port-port yang rentan servisnya dapat di tutup atau diblokir, sehingga hanya pihak yang diizinkan saja yang boleh lewat. Cara ini merupakan salah satu pengamanan jaringan yang sering digunakan. Jadi keamanan terhadap komputer server menjadi perhatian utama, ketika pada saat kita membangun sebuah infrastruktur jaringan. Keamanan jaringan juga dapat dikontrol dengan cara menyesuaikan *network sharing properties* pada masing-masing komputer, yang dapat membatasi *folder* dan *file* untuk dapat diakses oleh pengguna tertentu pada sistem jaringan. Walaupun demikian masih banyak institusi atau organisasi tidak peduli dengan masalah keamanan. Namun, ketika sistem jaringan diserang dan sistem masalah, baru mulai adanya perhatian dan itu sudah terlambat biaya perbaikan sistem akan menjadi tinggi. Oleh karena itu, diperlukan perhatian pada investasi keamanan jaringan untuk tindakan preventif. Disini pengelolaan keamanan server linux akan diuji cobakan di UNUSIA Jakarta sebagai studi kasus dalam penelitian ini. Dalam penelitian ini tidak dapat dipisahkan dari hasil penelitian terdahulu. Dari hasil penelusuran penelitian yang didapat oleh peneliti dan dirasa sangat penting dan memiliki pendekatan terbaik terhadap penelitian ini adalah:

- a. Jurnal dengan judul “Implementasi *Firewall* dan *Port Knocking* Sebagai Keamanan Data Transfer Pada *FTP Server* Berbasis Linux *Ubuntu Server*” (Shah Khadafi, dkk, 2019), penelitian yang dilakukan membahas tentang server menyediakan service FTP dalam sebuah jaringan yang diamankan menggunakan metode firewall dan port knocking di sistem operasi linux ubuntu server. FTP menggunakan port 21 untuk layanan file transfer antara komputer server dengan client. Hasil dari pengujian, dengan mengaktifkan firewall dan port knocking membuat peretas tidak dapat mengetahui port berapa yang aktif. Menggunakan sistem otentifikasi port knocking dapat melindungi hak akses penggunaan layanan FTP [3].
- b. Jurnal dengan judul “Pemanfaatan *IPTables* Sebagai *Intrusion Detection System (IDS)* dan *Intrusion Prevention System (IPS)* Pada *Linux Server*” (Atmadji, E. S. J., dkk, 2017), penelitiannya membahas tentang firewall iptables sebagai IPS pada system operasi linux. Iptables mampu memblokir serangan. Dengan iptables diharapkan bisa mengamankan server dengan lebih optimal [4].
- c. Jurnal dengan judul “Perancangan *Filtering Firewall* Menggunakan *Iptables* di *Jaringan Pusat Teknologi Informasi Unsrat*” (Glend Sondakh, dkk, 2014), penelitian yang dilakukan membahas tentang jaringan kampus unsrat yang dikelola oleh Pusat Teknologi dan Informasi menyediakan layanan pertukaran informasi baik dari dalam (intranet) maupun dari luar (internet). Aliran informasi ini khususnya yang berasal dari luar, sangat rentan terhadap keamanan atau isi informasi yang tidak diinginkan. Perangkat lunak (software) *Iptables* yang merupakan software bawaan dari sistem operasi linux dapat digunakan sebagai firewall didalam suatu jaringan [5].



Kesimpulan tinjauan pustaka diatas rata-rata hanya menggunakan dua variabel atau dua metode untuk solusi penyelesaian masalah, sedangkan untuk pembaharuan di penelitian saya menggunakan lebih dari dua variabel.

2. Metodologi Penelitian

Metodologi yang digunakan untuk menyusun penelitian “Perancangan Sistem Keamanan Server Linux Ubuntu 18.04 dengan metode *Hardening*, *Ufw Firewall*, *Chmod* dan *Chown* pada UNUSIA Jakarta” ini yaitu menggunakan metode eksperimental dan studi pustaka. Metode eksperimen merupakan penelitian yang digunakan untuk mencari pengaruh perlakuan tertentu terhadap dampaknya dalam kondisi yang terkendalikan (Jaedun, 2011)[6].

A. Analisis Kebutuhan

Sebelum pelaksanaan kegiatan penelitian perlu dilakukannya analisa terhadap kebutuhan. Analisa kebutuhan yang tepat dapat memudahkan berjalannya penelitian guna mencapai tujuan. Jadi langkah awal dalam penelitian ini adalah analisis kebutuhan yang berguna untuk menentukan kebutuhan dalam penelitian. *Server* tersebut direncanakan untuk menyimpan data yang berkaitan dengan data administrasi kampus, serta master program. Dikarenakan data tersebut *vital*, maka peneliti memprioritaskan pengamanan pada sisi *server* tersebut agar tidak di serang oleh pihak asing. Peneliti juga membatasi koneksi untuk akses ke *server* agar lebih terorganisir. Hanya *host* yang didaftarkan saja yang bisa akses ke data tersebut. *Host* yang tidak terdaftar akan ditolak. Berikut daftar perangkat lunak (software) dan perangkat keras (hardware) yang diperlukan.

- Server Dell PowerEdge T40 Tower (Intel Xeon 4 Core, RAM 16GB, Harddisk 1TB, DVDRW)
- Virtualbox (Linux dan Windows Server)
- Tools Built-in di Linux Ubuntu Server (ufw firewall, chmod, dan chown)
- Nmap, dan Wireshark
- Putty & WinsCP

Pengumpulan data dilakukan di kampus Universitas Nahdlatul Ulama Indonesia Jakarta. Adapun data yang terkumpul adalah sebagai berikut :

- Spesifikasi pada *server* yang eksis
- Topologi infrastruktur jaringan yang berjalan.

B. Teknik Pengumpulan Data

1. Teknik Observasi

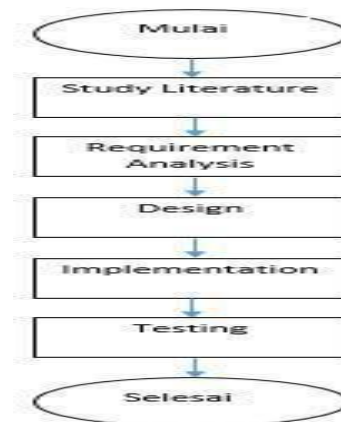
Observasi ini dilakukan untuk melihat secara langsung sistem keamanan diserver data yang ada di Unusia Jakarta. Pengamatan ini dilakukan guna mendapatkan informasi atau gambaran yang objektif, sehingga dapat diketahui apa saja yang perlu diusulkan untuk membangun sistem keamanan di kampus tersebut agar dapat memberikan keamanan pada data-data penting yang ada di server tersebut.

2. Studi Literatur

Pengumpulan data dilakukan melalui dua cara yaitu:

Data primer yakni data yang diperoleh secara langsung dari sumber kampus Unusia Jakarta. Data sekunder yakni data yang diperoleh dari sumber tidak langsung seperti melalui artikel, buku, jurnal, dan sumber data lainnya yang menunjang bahasan.

C. Tahapan Penelitian



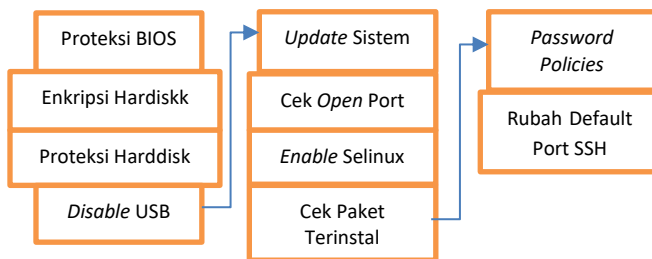
Gbr 1. Tahapan Penelitian

Jadi dari diagram alur tersebut, langkah awal dalam penelitian ini adalah menganalisa

kebutuhan sampai pada akhirnya ditesting atau diuji.

3. Hasil Dan Pembahasan A. Perancangan Penelitian

Untuk perancangan dan implementasi penelitian akan mengikuti *flowchart* sebagaimana yang tertera pada gambar di tahapan penelitian. Setelah menyelesaikan langkah analisis kebutuhan, desain dibutuhkan untuk memperjelas cara kerja sistem *hardening* server, yang dapat dilihat pada tahapan berikut ini:



Gbr 2. Perancangan Penelitian

Adapun skema sistem perancangan *hardening* server seperti diatas (tapi tidak harus berurutan, dan tidak harus semua proses dilakukan, tapi disesuaikan dengan kebutuhan). Tujuannya yaitu melindungi *server* yang mencakup layanan *file server* dimana dapat mencegah dari serangan *attacker* yang memanfaatkan celah pada *port*. Dalam skema ini terdapat empat lapisan keamanan yang diterapkan yaitu *firewall*, *hardening*, *privilege user* dan *file*. Keempat lapisan tersebut memberikan layanan keamanan berupa pendeteksi *open port*, pemblokiran *IP address*, sistem buka-tutup port, mengetahui *IP* penyerang dan pengaturan akses pada *user* dan *file*. Untuk untuk mengakses server diperlukan izin akses yang dimana akses khusus itu diberikan kepada admin. Gambar skenario terkait manajemen file dan user seperti berikut:

Proses pembangunan keamanan *server* terdiri dari beberapa langkah. Langkah pertama adalah menerapkan *hardening* dimulai dengan *patching* yang berguna untuk menambal dan

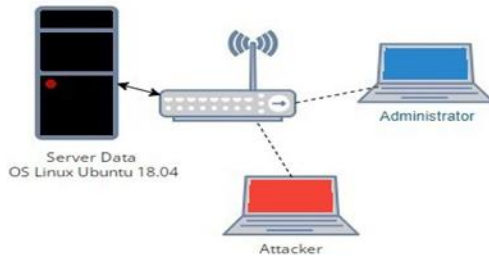
mengupdate aplikasi, dan system, serta menjaga *kernel linux* dan *software* tetap *up to date*. Hal Ini akan mencegah penyerang menggunakan kerentanan yang diketahui untuk masuk ke sistem. Setelah proses *hardening* selesai, langkah berikutnya yaitu menerapkan *management user* dan *file* dengan membuat atau menghapus user yang tidak perlu dan memberikan *privilege* terhadap *folder/file* dengan *chmod* dan *chown*. Langkah ketiga yaitu menginstal *ufw* sebagai dasaran untuk menerima *rule-rule* keamanan, konfigurasi yang diterapkan berupa pembatasan koneksi ke *port telnet, ssh, ftp*, dan *http*. Langkah terakhir yaitu *management icmp request* pada sistem *kernel* guna untuk pencegahan serangan *ddos*, seperti gambar dibawah ini.

```
Administrator: Command Prompt - ping 10.61.52.97 -t
Microsoft Windows [Version 10.0.18240]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Windows\system32>ping 10.61.52.97 -t
Pinging 10.61.52.97 with 32 bytes of data:
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
Reply from 10.61.52.97: bytes=32 time<1ms TTL=64
```

Gbr 3. pencegahan serangan ddos

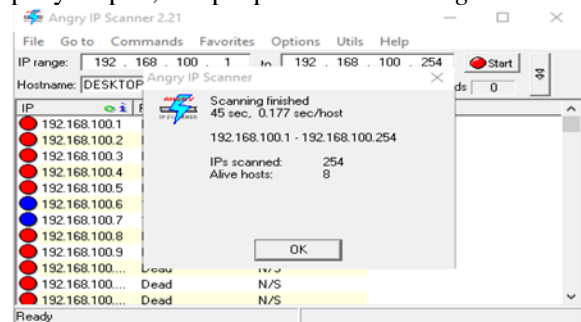
B. Teknik Analisis

Penjabaran teknik analisis menggunakan metode *hardening*, *firewall* *ufw* dan *privilege user* dan *file* dengan *chmod* dan *chown*. Pengujian dalam penelitian ini berbentuk client yang mencoba masuk via *ssh* ke sistem server *hardening* yang telah diamankan. Server yang sudah diamankan adalah dapat mengenali *IP address* penyerang. Penelitian ini dalam simulasinya menggunakan sebuah virtual mesin (*virtualbox*), didalamnya terdapat sebuah PC Server dan PC attacker seperti gambar berikut:

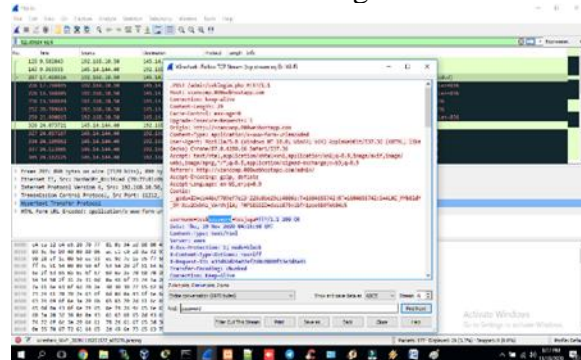


Gbr 4. Skenario Pc Server dan PC

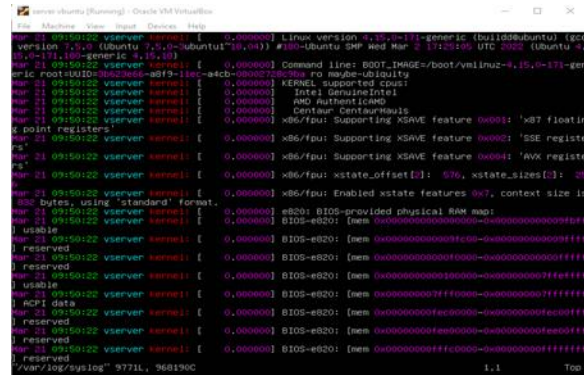
Skenario dari gambar diatas PC server sengaja akan dibuka beberapa port service seperti http, ftp, ssh, icmp dan telnet untuk tes sejauh mana keamanan bisa di lihat oleh penyusup dan administrator, kemudian ada sebuah PC attacker difungsikan melakukan *scanning* target untuk mencari informasi terkait *vulnerability* yang ada di target, hingga penyerangan dengan bantuan tools seperti nmap dan wireshark. Dari hasil penyusupan berlangsung, diperoleh sebuah file log yang berisikan segala aktifitas yang dilakukan oleh orang yang tidak berhak seperti penyusup untuk dianalisa oleh administrator. Berikut ini lampiran gambar mulai dari scanning, penyusupan, sampai pada informasi *log* di sistem.



Gbr 5. Informasi log di sistem



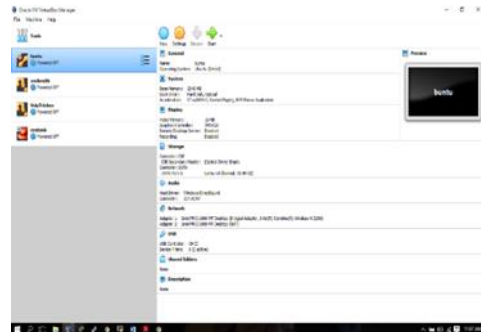
Gbr 6. Informasi log di sistem 2



Gbr 7. Informasi log di sistem 3

1. Instalasi dan Konfigurasi Perangkat Lunak yang dibutuhkan

Proses instalasi sistem operasi disertai dengan konfigurasi jaringan (konfigurasi IP address, subnet mask) pada PC Server dan PC Attacker mutlak dilakukan agar penulis dapat melakukan implementasi, simulasi dan analisis pada tesis ini. Instalasi ini nantinya dilakukan dalam sebuah perangkat lunak virtual dan kedua sistem operasi harus bisa saling terhubung dalam sebuah jaringan LAN agar dapat saling berkomunikasi dalam sebuah jaringan virtual host.

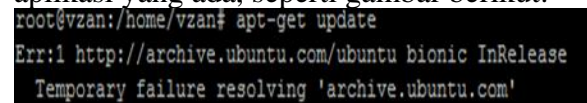


Gbr 8. Jaringan virtual host

C. Pengamanan Server

1. Patching

Langkah ini dimaksudkan untuk menambal celah-celah keamanan atau memperbaiki kekurangan system dan aplikasi yang ada, seperti gambar berikut:



Gbr 9. Tampilan Patching

Patching dapat dilakukan dengan menggunakan perintah *apt-get update* dan *apt-get dist-upgrade*. Untuk menjalankan perintah tersebut hanya dapat dilakukan jika user memiliki akses *root*. Perintah untuk masuk ke *root* dengan *sudo su*, dengan “*sudo su*” akan memberikan kewenangan agar *user* biasa dapat bertindak seperti *super user*, sehingga *user* biasa pun dapat leluasa menguasai sistem.

2. Management User dan file

Proses pembuatan *user* dan penghapusannya. Apabila ada salah satu *user* yang sudah tidak terpakai alangkah baiknya dihilangkan untuk keefektifan *management user*. Atau apabila dibutuhkan *user* tambahan dapat dilakukan. Perintah yang dapat digunakan untuk menambahkan *user* adalah *adduser* dimana *adduser* mencakup pembuatan *group*, direktori *home* dan informasi pribadi. Untuk menghapus *user* dapat menggunakan *deluser*. Dan untuk menghapus direktori yang tersisa, perintah yang digunakan ialah *rm -r* [10].

3. Konfigurasi Ufw sebagai Firewall Rules

Pengamanan server dan sistem operasi jaringan di linux Ubuntu 18.04 dapat menggunakan firewall yang secara default sudah terpasang di linux. Jika belum ada bisa lakukan langkah-langkah install dan konfigurasinya sebagai berikut :

- Instal firewall ufw dengan perintah
`#sudo apt-get install ufw`
- Lakukan blok port sesuai kebutuhan, misal ingin blok port 23 (remote dari luar server dengan telnet yang tidak bisa diakses) bisa dengan perintah
`#sudo ufw deny 23`, dan berikut hasilnya.

```
root@vsrver:/home/vzan# ufw status
Status: active

To Action From
--
21 DENY Anywhere
23 DENY Anywhere
22 ALLOW Anywhere
80 ALLOW Anywhere
21 (v6) DENY Anywhere (v6)
23 (v6) DENY Anywhere (v6)
22 (v6) ALLOW Anywhere (v6)
80 (v6) ALLOW Anywhere (v6)

root@vsrver:/home/vzan# _
```

Gbr 10. Remote dari luar server

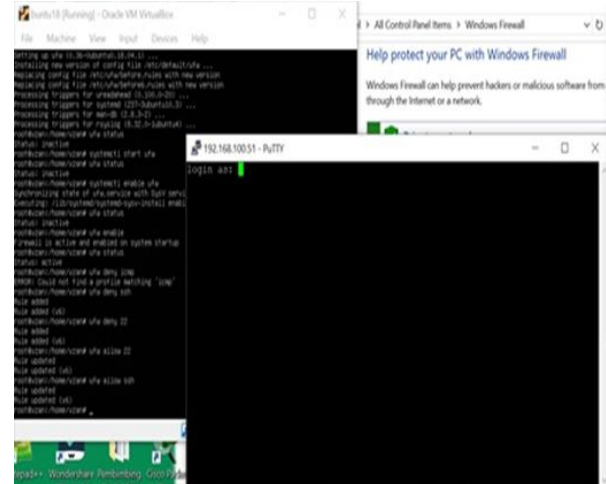
Jika ingin service ssh di allow atau di *open*, perintahnya sebagai berikut:

```
#sudo ufw allow 22
```

Atau dengan *allow* nama

```
#sudo ufw allow ssh
```

Dengan perintah tersebut, maka server bisa diakses dengan putty yang hasilnya akan tampak seperti gambar dibawah ini:



Gbr 11. Perintah service ssh di allow atau di open

Berikut ini perintah-perintah firewall Ufw di Ubuntu 18.04 :

-Memasang *firewall* UFW

```
#apt install ufw
```

-Menghapus UFW

```
#apt-get remove ufw
```

-Mengaktifkan UFW

```
#ufw enable
```

-Cek status dan *rules* UFW

```
#ufw status verbose
```

-Menonaktifkan atau *Reset* UFW

```
#ufw disable
```

```
#ufw reset
```

-Membolehkan akses

```
#ufw allow ssh
```

atau `ufw allow 22`

```
#ufw allow 80
```

-Membolehkan *Specific Port Ranges*

```
#ufw allow 6000:6007/tcp
```

-*Specific IP Addresses*



```
#ufw allow from 203.0.113.4
#ufw allow from 203.0.113.4 to any port 22
-Allow berdasarkan Subnets
#ufw allow from 203.0.113.0/24
-Menolak koneksi
#ufw deny http
#ufw deny from 203.0.113.4
-Menghapus Rules
#ufw delete allow http atau ufw delete allow 80
```

4. ICMP

Dilakukan penambahan rule yang digunakan untuk pemblokiran IP address yang tidak terdaftar, yang dapat berpotensi menimbulkan *denial of service*, sehingga dapat menghambat kinerja sistem.

Berikut tabel kegiatan dan hasil akhir yang direncanakan

Kelas Uji	Skenario Uji	Input	Respon Server	Hasil	Keterangan
Patching	Melakukan update/pembaruan system	#Apt-get update #apt-get upgrade #lsb-releases -a	Menampilkan versi system	Valid	System telah berhasil terupdate dengan versi terbaru
Ufw	Blok port yang rentan terhadap kejahatan	#Nmap ip_address_server #ufw deny 22	Menampilkan port-port yang terbuka dan memblokir service ftp	valid	System telah berhasil mengubah status port 22 dari allow ke deny
Chmod	Memberikan priviledg	#chmod go-wx	Menghapus	Valid	File atau folder berubah

	e ke user tamu hanya baca tidak bisa edit		wewenang write dan execute terhadap file		status permissio nnya
Icmp	Melakukan tes ping	Ping ip_address_server	Mem blokir permintaan icmp	V alid	System berhasil menolak permintaan ping

1. Konfigurasi Chmod pada Pada file dan folder

Konfigurasi ini dilakukan terkait kebutuhan *permission* masing-masing folder tersebut. Berikut ini contoh penjelasan penggunaan atribut file di Linux.

```
(masarie@SparkFly ~)$ ls -l /opt/vnc/
total 7936
-rwxr-xr-x 1 masarie users 6120920 Dec 21 2016 VNC-Viewer-6.0.1-Linux-x64
-rwxr-xr-x 1 masarie users 1995504 Aug 18 2011 vncviewer.exe
(masarie@SparkFly ~)$
```

Gbr 12. Konfigurasi Chmod

Ada 3 segmen atribut untuk setiap file dan folder di linux yaitu :

Segmen A merupakan User/Owner permission (-RWX)

segmen B merupakan Group Permission (R-X)

dan segmen C merupakan Other Permission (R-X).

→ Tanda minus atau strip (-) merupakan indikasi kalau ada permission yang tidak diterapkan/berikan untuk user,group atau other.

Contoh pada kasus diatas pada segmen B (*group permission*) dengan permission R-X (W nya gak ada) itu artinya user yang tergabung dalam group 'users'[D]



hanya bisa membaca(read) dan menjalankan file(executable) "VNC-Viewer-6.0.1-Linux-x64" dan tidak bisa mengedit,menghapus dan memodifikasi (write)

-Ubah Hak Akses File Dengan Symbolic/Huruf

r – Read **w** – Write **x** – Execute

Adapun simbol untuk mengeset permission yang kita maksud,kamu bisa gunakan simbol:

u – Owner ->Mengeset Owner permission
g – Group ->Mengeset Group permission
o – Others ->Mengeset Other permission

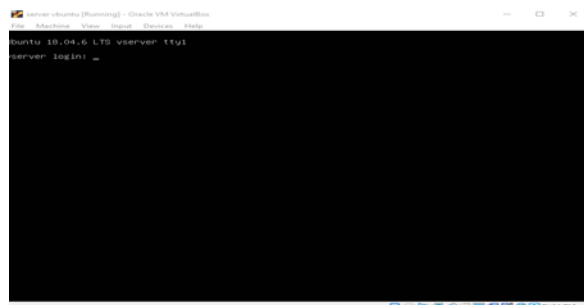
Tanda + (plus) dan – (minus) digunakan sebagai operator untuk menambahkan atau menghapus *permission*.

Contoh : misal sebelum nya beratribut rwxrw-r- pada file dokumen.doc Kita ingin ubah group permission menjadi read only (**r-**) dengan menghapus permission write (**w**) menggunakan perintah # `chmod g-w dokumen.doc` [7].

D. Hasil

1. Hasil Instalasi Server Ubuntu 18

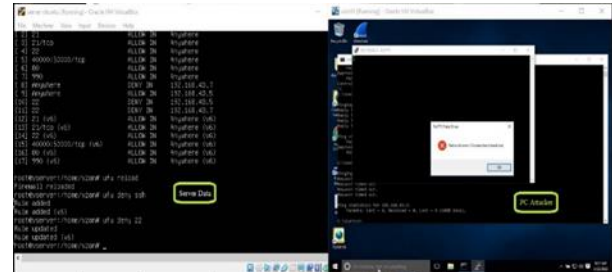
Hasil instalasi server ubuntu berupa CLI (Command Line Interface), adalah antarmuka pengguna berbasis teks seperti gambar dibawah:



Gbr 13. Instalasi Server Ubuntu 18

2. Hasil Konfigurasi Firewall

Berikut tampilan hasil konfigurasi firewall ufw, dimana status port yang di *deny* dan di *allow* terlihat dan akses ssh diblokir.



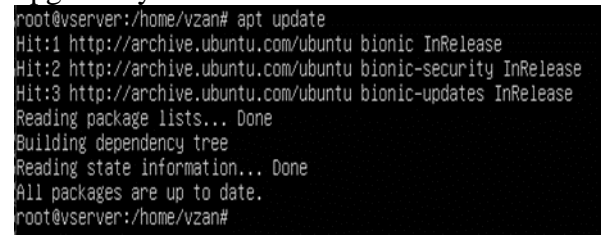
Gbr 14. Konfigurasi Server Ubuntu 18

3. Hasil Hardening

Berikut ini hasil-hasil dari konfigurasi hardening yang diantaranya sebagai berikut:

a) Hasil Patching (Update Sistem)

Berikut tampilan hasil update dan upgrade system server Ubuntu 18



Gbr 19. Hasil Patching

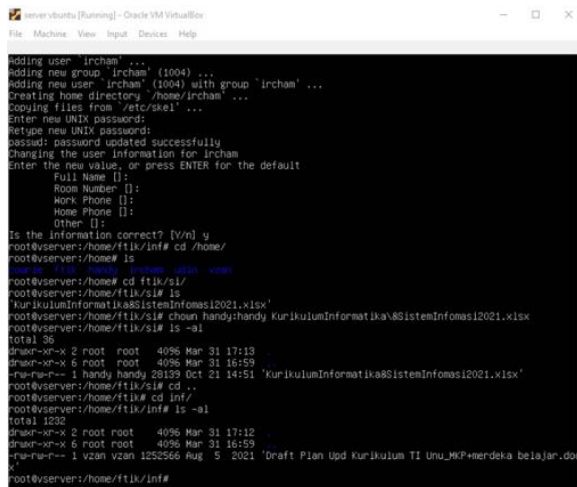
b) Hasil Password Policies



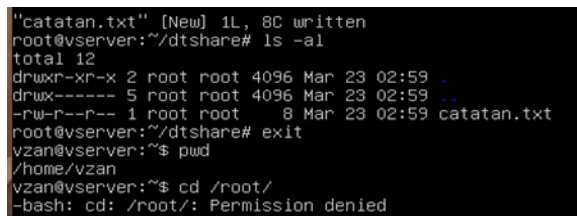
Gbr 20. Hasil Patching

4. Hasil Konfigurasi Manajemen Akses File dan User

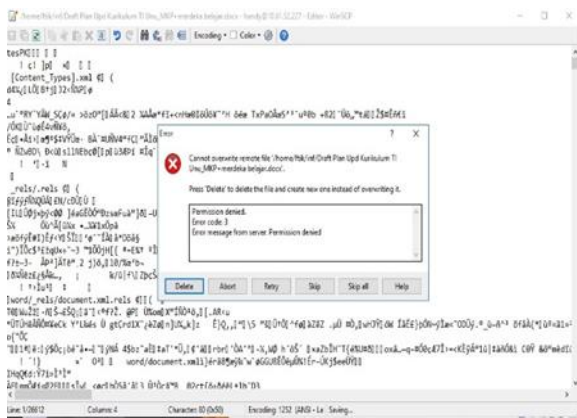
Pada tampilan berikut ini bisa melihat folder tercipta sesuai rencana di skenario diatas, dimana sub folder program studi dibawah struktur folder fakultas, dan masing-masing folder mempunyai hak akses tersendiri beserta gambar lampiran hasil tes akses.



Gbr 21. Lampiran Hasil Tes Akses



Gbr 22. Lampiran Hasil Tes Akses 2



Gbr 23. Lampiran Hasil Tes Akses 3

E. Analisa Serangan

Penganalisaan terhadap serangan bertujuan untuk mendeteksi tindakan-tindakan pengujian dari sistem yang telah dibuat. Dari analisis yang diperoleh dari log, menginformasikan aktivitas atau tindakan yang dapat digunakan administrator untuk dapat menentukan kebijakan atau memberi aturan dalam pengamanan sistem server jaringan. Hasil

pengujian ini berhasil dilakukan dengan menunjukkan hasil tindakan atau aktivitas serangan yang telah terjadi beserta pencegahannya. Metode seperti ini dapat memberikan solusi yang baik. Adapun hasil dari pengujian akan dimonitoring dan direview oleh administrator secara berkala.

4. Kesimpulan Dan Saran

Dari penelitian berupa implementasi pada sistem keamanan server jaringan yang telah dilakukan, maka dapat ditarik kesimpulan bahwa:

1. Implementasi firewall ufw pada sistem keamanan di server jaringan dapat membantu keamanan pada server tersebut dan dapat membantu administrator dalam menganalisa, melakukan tindakan pencegahan hingga membuat kebijakan.
2. Dari rancangan dan implementasi hardening server tersebut akan menghasilkan keamanan server data yang minim pencurian dari kejahatan komputer.
3. Manajemen akses file dan user dengan chmod dan chown juga dapat membantu dalam mengamankan data dari orang yang tidak berhak terutama folder atau file privat yang bukan public.
4. File log yang ada pada sistem dapat memberikan informasi detail baik IP address attacker, dan apa saja yang dilakukan oleh attacker untuk selanjutnya dilakukan analisa untuk pengambilan keputusan terkait kebijakan yang akan diterapkan.

Untuk saran berdasarkan dari penelitian yang telah dilakukan ini adalah:

1. Implementasi *firewall* Ufw, hardening dan manajemen file akses dengan chmod dan chown pada server Ubuntu 18.04 bisa meminimalisir resiko terhadap keamanan pada server dan untuk memaksimalkan bisa menambahkan metode honeypot, dan port knocking yang bisa dijalankan secara bersamaan dengan tujuan mengamankan server secara keseluruhan, membuat server tiruan, dan mengetahui *log traffic* dan sebagainya secara grafis.
2. Penelitian ini masih memiliki banyak kekurangan, jadi harus perlu dikembangkan



sistem secara menyeluruh dengan menambahkan metode lain seperti menambahkan *firewall* jaringan dan *endpoint security* agar keamanan lebih kuat.

DAFTAR PUSTAKA

- [1] Wikipedia. 2021. Jaringan Komputer. https://id.wikipedia.org/wiki/Jaringan_komputer. Halaman ini terakhir diubah pada 6 Agustus 2021, pukul 13.10.
- [2] Efendi, Ilham. Apa Yang di Maksud Dengan Server. <https://www.it-jurnal.com/apa-yang-di-maksud-dengan-server/>.
- [3] Khadafi, S., Pratiwi, Y. D., & Alfianto, E. (2021). Keamanan FTP Server Berbasiskan IDS dan IPS Menggunakan Sistem Operasi Linux Ubuntu. *Network Engineering Research Operation*, 6(1), 11-24.
- [4] Atmadji, E. S. J., Susanto, B. M., & Wiratama, R. (2017). Pemanfaatan IPTables Sebagai Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) Pada Linux Server. *Teknika*, 6(1), 19-23.
- [5] Sondakh, G., Najoan, M. E., & Lumenta, A. S. (2014). Perancangan filtering firewall menggunakan iptables di jaringan pusat teknologi informasi Unsrat. *Jurnal Teknik Elektro dan Komputer*, 3(4), 19-27.
- [6] A Jaedun (2011). Metodologi penelitian eksperimen – Jurnal Fakultas Teknik UNY.
- [7] Arianto. 2020. Cara Mengatur Hak Akses & Kepemilikan File di Linux <https://www.belajarlinux.org/memahami-dan-mengatur-hak-akses-serta-kepemilikan-file-folder-linux/> Diperbarui 4 April 2020

