Vol. 12, No. 1, September 2021, pp. 64 – 73
P-ISSN: 2089 – 0256, e-ISSN: 2598 – 3016

ANALISA PENERAPAN *FILTERING PROXY SERVER* PADA KEAMANAN JARINGAN KOMPUTER UNTUK MEMINIMALISR PENYEBARAN *MALWARE* (STUDI KASUS *CAKRABUANA CRUISESHIP & SCHOOL* CIREBON)

Rizky Maulana[1], Muhammad Hatta[2], Ilwan Syafrinal[3]

[1]Mahasiswa Teknik Informatika, Fakultas Teknologi Informasi, Universitas Catur Insan Cendekia
[23]Dosen Teknik Informatika, Fakultas Teknologi Informasi, Universitas Catur Insan Cendekia
rizkymaulll98@gmail.com[1], muhammad.hatta@cic.ac.id[2], ilwan.syafrinal@cic.ac.id[3]

Abstrak

Cakrabuana *Cruise Ship & Hotel School* Cirebon merupakan lembaga pendidikan & pelatihan yang jumlah akses *internet*nya cukup tinggi, namun karena kebiasaan buruk pengguna membuka situs-situs yang di dalamnya mengandung *malware*, maka komputer *client* yang sering mengakses situs-situs tersebut terinfeksi *malware.* Situs-situs yang dimaksud yaitu judi *online, scam,* ataupun situs yang biasanya menyediakan *keygen/crack*. Berdasarkan uraian di atas permasalahan tersebut dapat di atasi dengan salah satu cara yaitu menggunakan metode *filtering*. *Filtering* pada *website* berhasil membatasi situs *web* yang dapat diakses oleh pengguna. *Proxy server* yang di jalankan dengan sistem operasi *Linux Ubuntu* 16.04.6-*server* yang akan digunakan sebagai metode *filtering* pada penelitian ini. Selanjutnya *software* yang akan menjalankannya yaitu *software squid* yang merupakan *software* untuk menjalankan fungsi sebagai *proxy server*, dan melakukan *filtering website* yang di nilai mengandung *malware*. Hasil penelitian dari analisa penerapan *filtering website* dengan menggunakan *proxy server* yaitu terciptanya sistem keamanan jaringan komputer *client* untuk meminimalisir penyeberan *malware* di Cakrabuana *Cruise Ship & Hotel School* Cirebon. Dengan demikian akan menghasilkan keamanan jaringan yang lebih optimal.
Kata Kunci*: Filtering, Proxy Server, Malware*

Abstract

Cakrabuana Cruise Ship & Hotel School Cirebon is an educational & training institution that has a high number of internet access, but due to bad habits of users opening sites that contain malware, computers that frequently access these sites are infected with malware. The sites in question are online gambling, scams, or sites that usually provide keygen / crack. Based on the description above, this problem can be overcome by using the filtering method. Filtering on the website succeeds in limiting the websites that can be accessed by users. Proxy server that is run with the Linux Ubuntu 16.04.6-server operating system which will be used as a filtering method in this study. Furthermore, the software that will run it is the Squid software, which is software to function as a proxy server, and filter websites that are considered to contain malware. The results of the research from the analysis of the application of website filtering using a proxy server, namely the creation of a client computer network security system to minimize the spread of malware in Cakrabuana Cruise Ship & Hotel School Cirebon. This will result in more optimal network security.
***Keywords** : Filtering, Proxy Server, Malware*

1. Pendahuluan

Pada masa kini, pemakaian komputer dan *notebook* sudah sangat banyak. Ada banyak sistem operasi yang digunakan oleh perangkat-perangkat tersebut, contohnya adalah *Ubuntu*, *Debian*, dan *Windows*. Pada sistem operasi yang di gunakan banyak aplikasi yang dapat digunakan untuk membantu aktivitas tertentu. Contohnya adalah aplikasi pengolah kata, peramban *internet*, dan pengolah data. Terkadang, ada aplikasi berbahaya yang melakukan aktivitas-aktivitas membahayakan sistem yang berjalan, aktivitas tersebut bersifat

p-ISSN 2089-0265
e-ISSN 2598-3016

tersembunyi, seperti mengubah sebuah *file*, menduplikasi *file*, menghapus *file*, mengirim *file* melalui jaringan, mengakses jaringan tertentu atau situs tertentu tanpa sepengetahuan milik pengguna. Semua perangkat lunak yang melakukan aktivitas berbahaya tersebut di suatu sistem disebut dengan *malware* (Cahyanto et al., 2017) .

Malware adalah singkatan dari *Malicious Software*, yaitu perangkat lunak berbahaya, perangkat lunak ini bisa digunakan untuk mengganggu pengoperasian komputer, mengumpulkan informasi sensitif, atau mendapatkan akses ke sistem komputer (CSIRT, 2015). Saat ini penyebaran *malware* pada jaringan *internet* sudah sangat tidak terkendali. Hal tersebut yang saat ini menjadi masalah keamanan teknologi informasi karena dampak yang ditimbulkan oleh *malware* tidak main-main. Penyebaran *malware* melalui media jaringan *internet* salah satu diantaranya yaitu berawal dari kebiasaan buruk pengguna yang membuka situs-situs yang di dalamnya sudah terinfeksi *malware* atau bahkan sengaja di pasangkan *malware* oleh pemilik situs. Begitupun yang terjadi pada Cakrabuana *Cruise Ship & Hotel School* Cirebon.

Cakrabuana *Cruise Ship & Hotel School* Cirebon merupakan lembaga penyelenggara pendidikan & pelatihan yang mengembangkan karir di bidang perhotelan dan kapal pesiar Internasional. Jaringan komputer yang aman sangat dibutuhkan oleh karyawan Cakrabuana *Cruise Ship & Hotel School* Cirebon. Sistem kemanan jaringan yang akan dirancang kemudian dapat membantu dalam keamanan jaringan pada lembaga tersebut.

Berdasarkan hasil dari komunikasi langsung yang di lakukan oleh penulis dan *network administrator* pada lembaga tersebut, komputer *client* pada Cakrabuana *Cruise Ship & Hotel School* Cirebon sering terinfeksi *malware*, penyebabnya adalah membuka situs-situs yang mengandung *malware*. Sebagai contoh situs yang di maksud adalah situs yang mempunyai konten judi *online*, *scam*, ataupun situs yang biasanya menyediakan *keygen* atau *crack*. Situs-situs yang berpotensi untuk menyebarkan *malware* tersebut masih dapat di akses, karena belum adanya sistem keamanan jaringan komputer agar dapat meminimalisir penyebaran *malware*. Apabila hal ini terus terjadi, komputer yang terinfeksi *malware* akan menyebabkan beberapa program, aplikasi, *software*, dan bahkan data di dalam komputer akan rusak dan hilang dengan sendirinya. Akan menjadi masalah besar ketika data atau program yang rusak sangat penting dan berhubungan dengan pekerjaan Cakrabuana *Cruise Ship & Hotel School* Cirebon.

Maka penulis memberikan saran dengan melakukan *filtering website* dengan menggunakan *proxy server*. *Proxy Server* berfungsi untuk melakukan *filtering* terhadap situs-situs yang dinilai mengandung *malware* sehingga pada komputer *client* tidak dapat mengakses situs yang mengandung *malware* tersebut.

Berdasarkan latar belakang permasalahan yang telah di jelaskan di atas, maka di usulkan untuk dapat di lakukan penelitian dengan judul "Analisa & Penerapan *Filtering Proxy Server* Pada Keamanan Jaringan Komputer untuk Meminimalisir Penyebaran *Malware* (Studi Kasus : Cakrabuana *Cruise Ship & Hotel School* Cirebon)".

2. Metode Penelitian

Prosedur penelitian yang dilakukan dalam penelitian ini menggunakan metode PPDIOO (*Prepare, Plan, Design, Implementation, Operate, Optimize*) *network cycle* (Adhiwibowo & Mindatama, 2019).

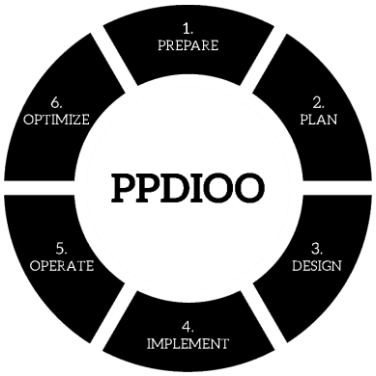
Tahap *prepare* ini penulis berkomunikasi dengan melakukan wawancara kepada *network administrator* di lembaga tersebut untuk memperoleh gambaran dan penjelasan mengenai kondisi jaringan *internet* yang ada di Cakrabuana *Cruise Ship* & Hotel *School* Cirebon.

Tahap *plan* dilakukan pemetaan kebutuhan pelaksanaan pengembangan jaringan baru dan rencana yang dibutuhkan untuk membuat sistem keamanan jaringan menggunakan *proxy server*. Tahap *design* dimana penulis melakukan desain topologi jaringan dan menyiapkan rencana instalasi jaringan sesuai kebutuhan. Tahap *Implementation* penulis memastikan seluruh proses sudah sesuai dengan desain dan kemudian melakukan instalasi dan konfigurasi pada *linux ubuntu*, yang akan di gunakan untuk membangun sistem kemanan jaringan komputer menggunakan *proxy server*.

p-ISSN 2089-0265
e-ISSN 2598-3016

Tahap *operate* penulis melakukan kegiatan pengamatan pada jaringan komputer dan memastikan sistem *filtering proxy server* dapat digunakan pada jaringan Cakrabuana *Cruise Ship* & Hotel *School* Cirebon.

Tahap *optimize* adalah tahap akhir peneliti melakukan pengujian pada system filtering *proxy server* apakah sudah maksimal dan sesuai dengan tujuan penelitian.

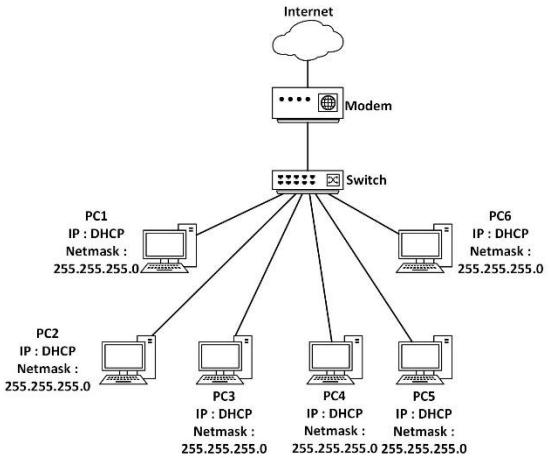


Gambar 1. Metode PPDIOO Network Cycle

3. Hasil dan Pembahasan

1. *Prepare*

penulis berkomunikasi dengan melakukan wawancara kepada *network administrator* di lembaga tersebut untuk memperoleh gambaran dan penjelasan mengenai kondisi jaringan *internet* yang ada di Cakrabuana *Cruise Ship* & Hotel *School* Cirebon. Berikut kondisi jaringan yang berjalan :



Gambar 2. Topologi Jaringan Berjalan

Topologi jaringan berjalan pada gambar 2 menjelaskan topologi jaringan berjalan di Cakrabuana *Cruise Ship & Hotel School* Cirebon menghubungkan setiap pengguna dan memudahkan pengguna untuk mengakses *internet* dengan bebas tanpa batasan di karenakan belum adanya sistem *proxy server* pada *internet* perusahaan.

2. *Plan*

Tahap pemetaan kebutuhan pelaksanaan kebutuhan peralatan perangkat lunak dan perangkat keras.

Tabel 1. Spesifikasi Perangkat Keras

Nama Perangkat	Spesifikasi
PC Server	*Processor Pentium® Dual-core CPU E5300 @2.60 GHz (2 CPUs)*
	RAM 8 GB
	Hardisk 500 GB
PC Client	*Intel Core duo*
	2 GB
	500 *GB* (*HDD SATA*)
	10/100/1000 *Mbps*

Spesifikasi perangkat keras pada tabel 1 merupakan spesifikasi yang akan digunakan pada Cakrabuana Cruise Ship & Hotel School Cirebon.

Tabel 2. Perangkat Lunak

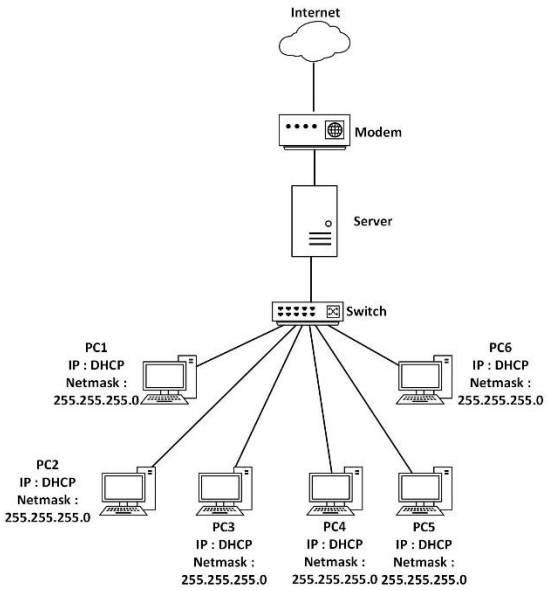
1	Ubuntu Server 16.04.46
2	Windows XP (Client)
3	*VirtualBox versi6.0.18-136238*

Perangkat lunak pada tabel 2 merupakan perangkat lunak yang akan digunakan pada Cakrabuana Cruise Ship & Hotel School Cirebon.

3. *Design*

Tahap berikutnya yaitu *design* dimana penulis melakukan desain topologi jaringan dan menyiapkan rencana instalasi jaringan sesuai kebutuhan.

p-ISSN 2089-0265
e-ISSN 2598-3016



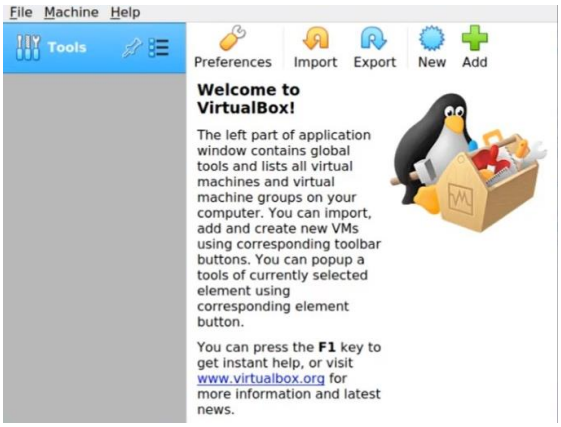
Gambar 3. Perancangan Topologi Usulan

Perancangan topologi fisik pada gambar 3 perancangan topologi usulan ini akan mengubah struktur topologi dan mekanisme kerja jaringan. Perubahan yang dilakukan adalah dengan menambahkan *server ubuntu* pada perusahaan yang akan di gunakan alat *filtering* atau *blok* situs - situs yang kemungkinan terkena *malware* dan pada *server ubuntu* akan di *install* aplikasi *DHCP server* dan *squid server*.

Server yang telah terhubung ke *internet*, kemudian *Server* tersebut telah di konfigurasikan dengan *service-service* yang dibutuhkan untuk pengamanan *proxy* yang dimaksudkan untuk dapat melakukan *filtering* akses *internet* terhadap situs-situs yang berpotensi mengandung *malware*, cara kerja pada *proxy server* yaitu saat *user* menggunakan layanan pada *server proxy* kemudian melakukan permintaan data atau file yang terdapat di *internet* (*public server*). Selanjutnya *proxy* akan meneruskan permintaan tersebut ke *internet* dengan seolah-olah *server* tersebutlah yang memintanya. *Client* akan mengakses *internet* melalui *switch* yang terhubung dengan *server*.

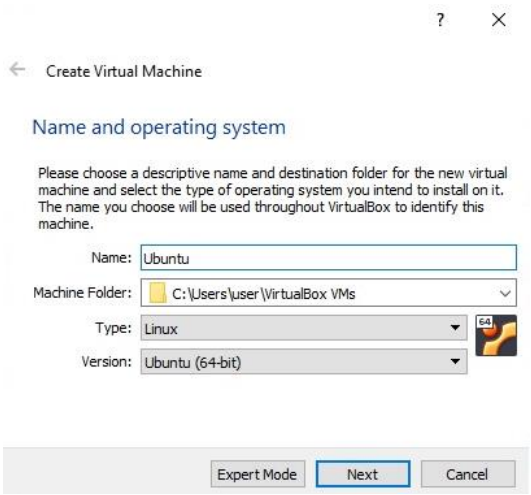
4. Implementation

Berikutnya adalah tahap *implementation* penulis memastikan seluruh proses sudah sesuai dengan desain dan kemudian melakukan instalasi dan konfigurasi pada *linux ubuntu*, yang akan di gunakan untuk membangun sistem kemanan jaringan komputer menggunakan *proxy server*.



Gambar 4. Instalasi Ubuntu Pada *Virtual Machine*

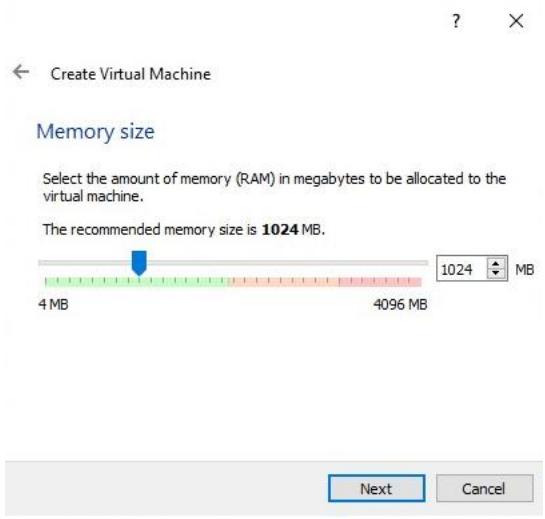
Pada gambar 4 hal yang pertama dilakukan adalah klik menu *file* dan pilih *new*



Gambar 5 Instalasi Ubuntu Pada *Virtual Machine*

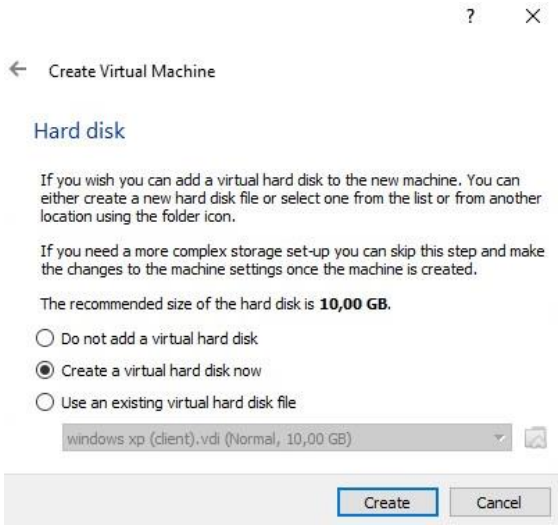
Pada gambar 5 kemudian isi *name* dengan nama *Ubuntu*, isi *type* dengan pilih *Linux*, dan pilih *version* sesuai spesifikasi *PC* atau *Laptop*, kemudian klik *next*

p-ISSN 2089-0265
e-ISSN 2598-3016



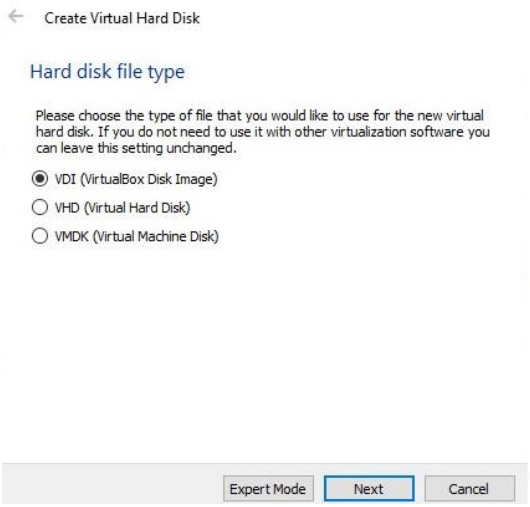
Gambar 6. Instalasi Ubuntu Pada *Virtual Machine*

Pada gambar 6 menentukan besaran memori pilih *next* karena *virtualbox* otomatis merekomendasikan besarnya memori



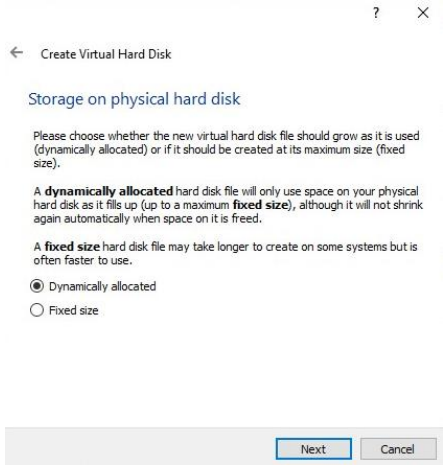
Gambar 7. Instalasi Ubuntu Pada *Virtual Machine*

Pada gambar 7 Menentukan ukuran *harddisk*, *klik create*



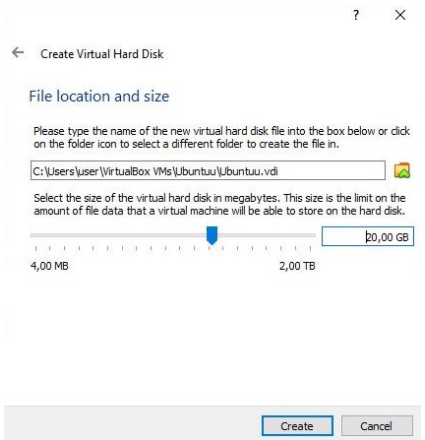
Gambar 8. Instalasi Ubuntu Pada *Virtual Machine*

Pada gambar 8 Menentukan *disk image* dan pilih VDI *(Virtual Disk Image)* kemudian *next*



Gambar 9. Instalasi Ubuntu Pada *Virtual Machine*

Pada gambar 9 menentukan penyimpanan *disk* dan pilih opsi *dynamically alocated* kemudian *next*



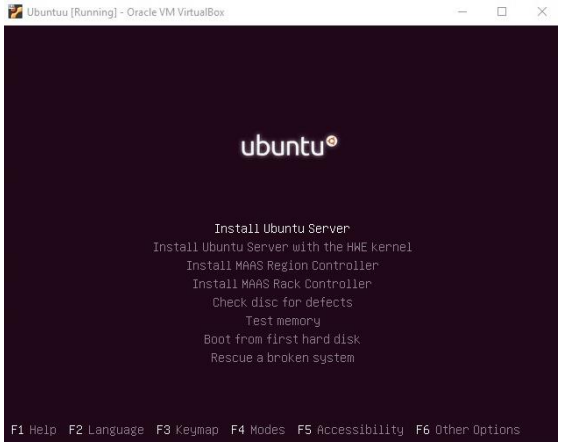
Gambar 10. Instalasi Ubuntu Pada *Virtual Machine*

p-ISSN 2089-0265
e-ISSN 2598-3016

Pada gambar 10 menentukan *location* dan *size* kemudian *create*

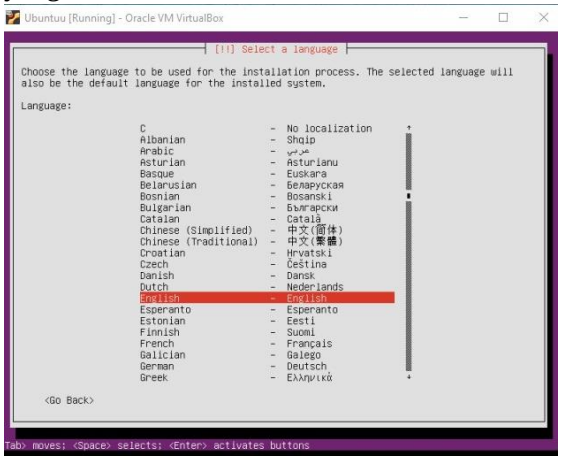
Gambar 11. Bahasa Instalasi

Pada gambar 11 menentukan bahasa yang akan digunakan kemudian *next*



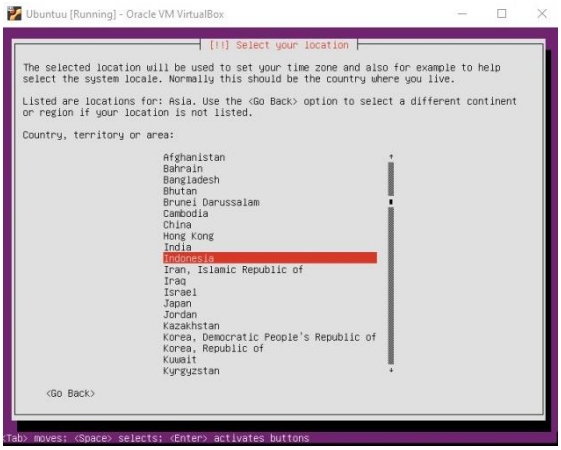
Gambar 12. *Mode* Instalasi

Pada gambar 12 menentukan *sistem operasi* yang akan di instal kemudian *next*



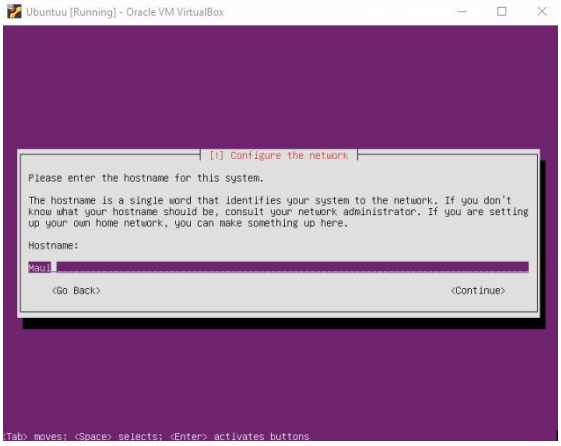
Gambar 13. *Mode* Instalasi

Pada gambar 13 menentukan bahasa instalas*i ubuntu server* kemudian *next*



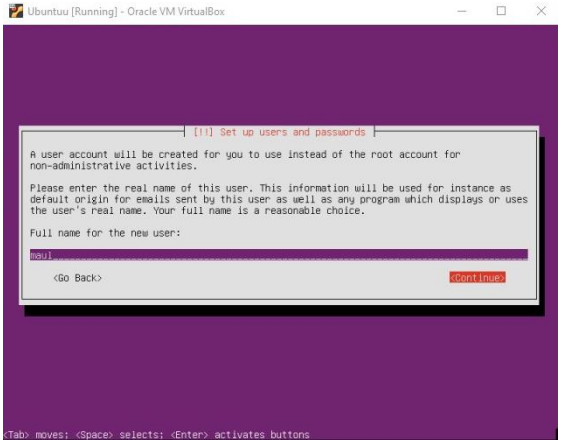
Gambar 14. *Time Zone*

Pada gambar 14 menentukan *time zone* kemudian *next*



Gambar 15. *Hostname Server*

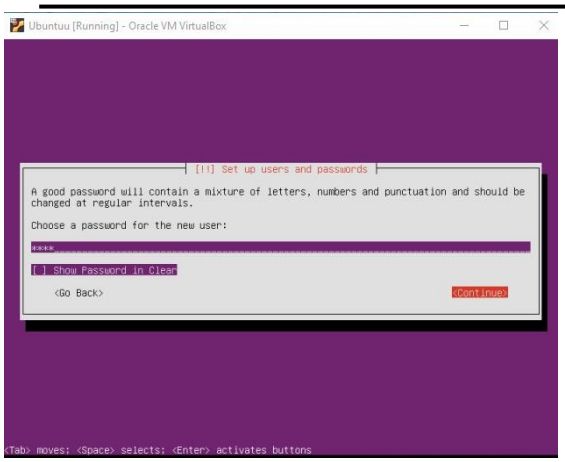
Pada gambar 15 menentukan *hostname* pada *server ubuntu* dan berikan nama *ubuntu* kemudian *next*



Gambar 16. *Name User*

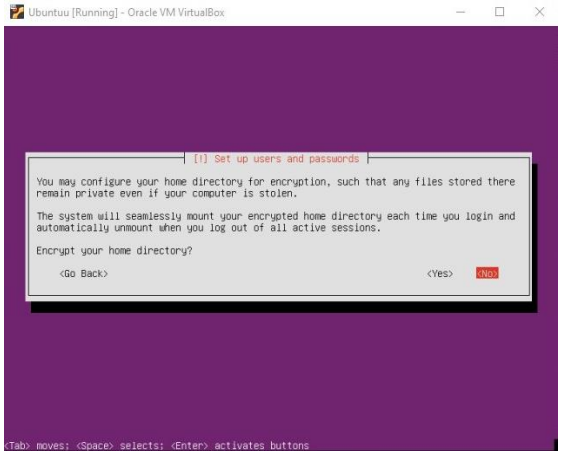
Pada gambar 16 menentukan *name user* dan berikan nama maul kemudian *next*

p-ISSN 2089-0265
e-ISSN 2598-3016



Gambar 17. *Create Password*

Pada gambar 17 membuat *password user* kemudian *next*

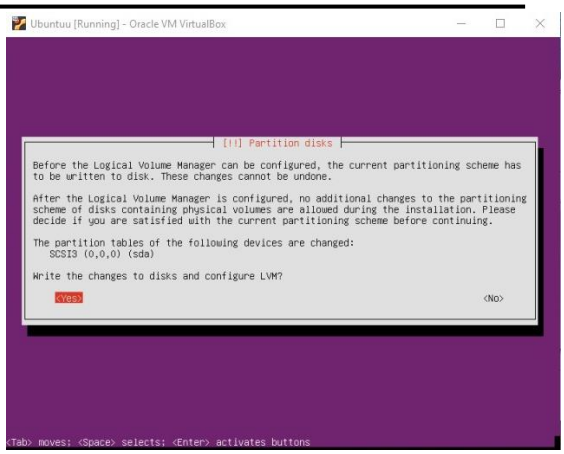


Gambar 18. *Encrypt Home Directory*

Pada gambar 18 pada *home directory* pilih opsi *no* kemudian *next*

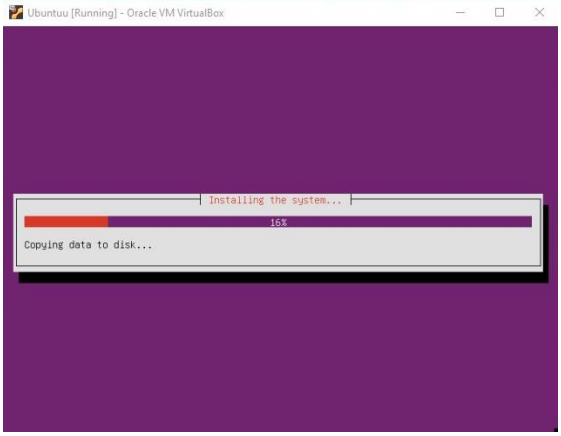
Gambar 19. *Format Disk*

Pada gambar 19 menentukan *format disk* dan pilih baru ke 2 yaitu *standart format disk* kemudian *next*



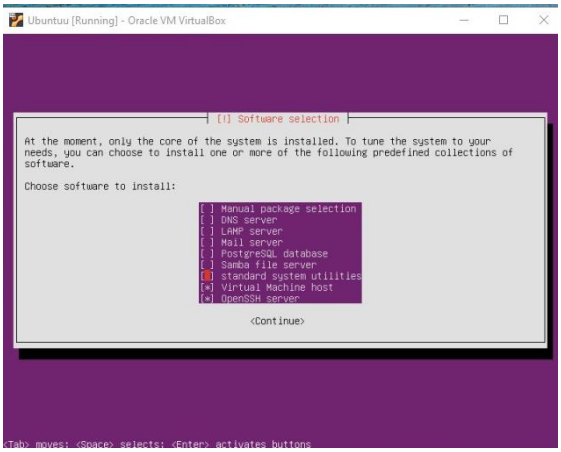
Gambar 20. *Format Disk*

Pada gambar 20 pilih opsi *yes*



Gambar 21. *Proses Instgalasi*

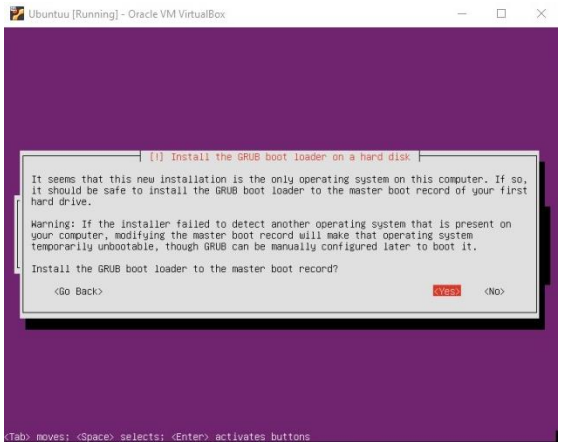
Pada gambar 21 menunggu proses instalasi selesai



Gambar 22. Pemilihan *Service Server*

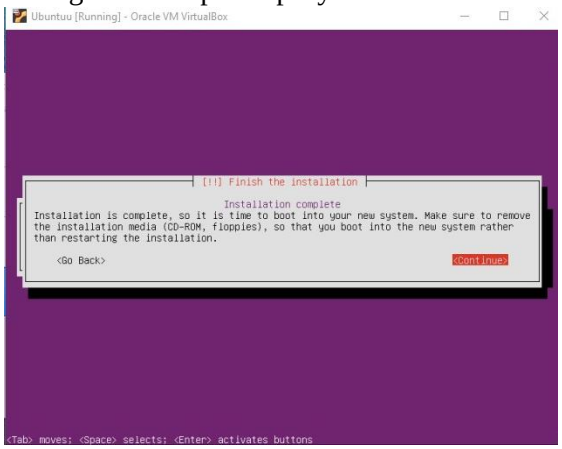
Pada gambar 22 menentukan *service* yang akan dibutuhkan *server dan* pilih *openSSH* dan *virtual machine host* kemudian *next.*

p-ISSN 2089-0265
e-ISSN 2598-3016



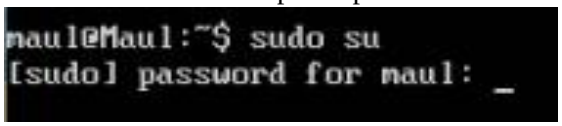
Gambar 23. *Instalasi Grup Loader*

Pada gambar 23 pilih opsi yes kemudian *next*



Gambar 24. *Instalasi Complete*

Pada gambar 24 proses instalasi *ubuntu server* telah selesai kemudian pilih opsi *continue*



Gambar 25. Perintah *Root*

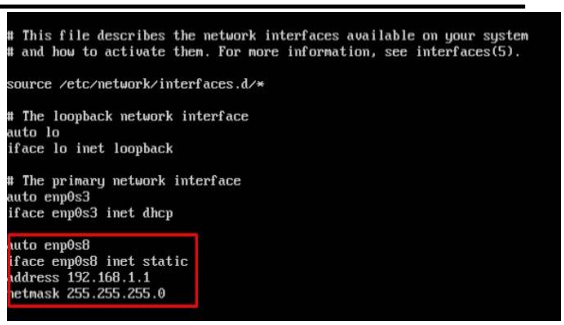
Pada gambar 25 masukan perintah *sudo su* dan *password user root*

Gambar 26. *Instalasi DHCP*

Pada gambar 26 *install DHCP* nya dengan mengetikkan perintah : ***apt-get install isc-dhcp-server***

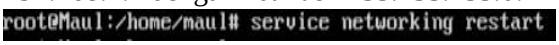
Gambar 27. *Network Interface*

Pada gambar 27 , tambahkan *enp0s8* pada *network interfaces* dengan perintah ***: nano /etc/network/interfaces***



Gambar 28. *Network Interface*

Pada gambar 28 masukan *IP address* 192.168.1.1 dengan *netmask* 255.255.255.0.

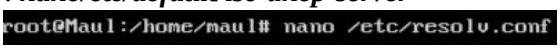


Gambar 29. Restart Service *Network Interface*

Pada gambar 29 lakukan *restart service network*

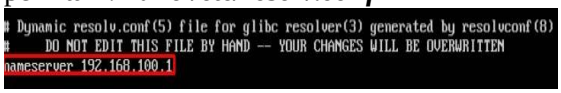
Gambar 30. *Default DHCP Server*

Pada gambar 30 memilih *interface* yang akan digunakan untuk DHCP *server* dengan perintah : ***nano/etc/default/isc-dhcp-server***



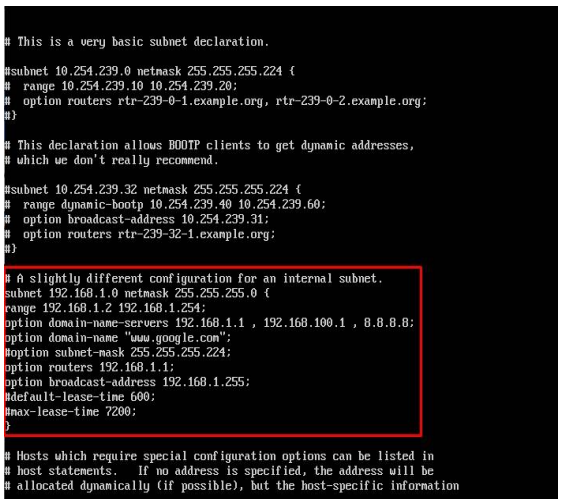
Gambar 31. *DNS Server*

Pada gambar 31 masukan *DNS Server* dengan perintah : ***nano /etc/resolv.conf***



Gambar 32. *Setting DNS Server*

Pada gambar 32 masukan *nameserver 192.168.100.1*



Gambar 33. *Setting DNS Server*

p-ISSN 2089-0265
e-ISSN 2598-3016

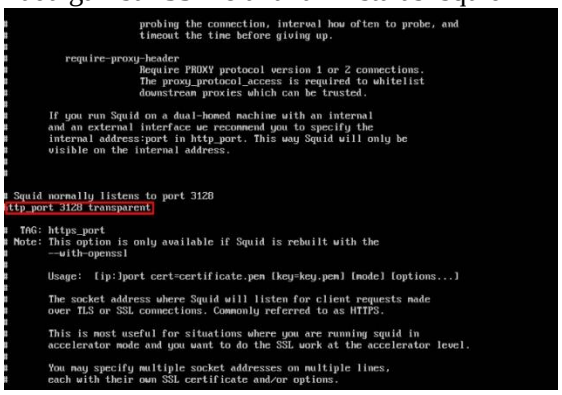
Pada gambar 33 masukan
subnet 192.168.1.0 netmask 255.255.255.0
range 192.168.1.2 192.168.1.254
option domain-name-server 192.168.1.1 , 192.168.100.1 , 8.8.8.8
option domain-name www.google.com
option routers 192.168.1.1
option broadcast-address 192.168.1.255

Gambar 34. Perintah *Root*

Pada gambar 34 lalukan *restart service* dhcp

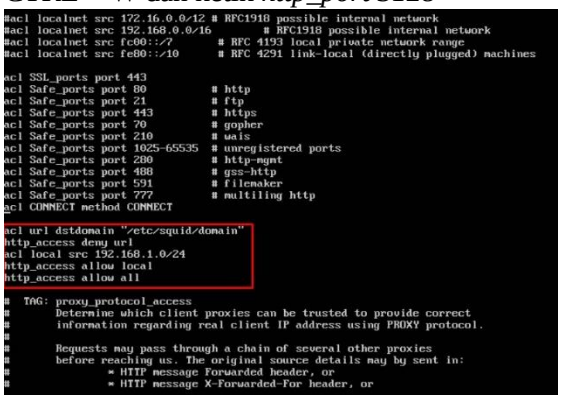
Gambar 35. *Install Squid*

Pada gambar 35 melakukan instalasi squid



Gambar 36. *Konfigurasi Squid*

Pada gambar 36 ketikan perintah : ***nano /etc/squid/squid.conf*** kemudian search dengan CTRL + W dan ketik *http_port 3128*

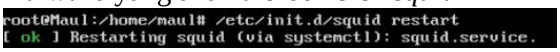


Gambar 37. *Konfigurasi Squid*

Pada gambar 37 ketikan perintah : ***acl connect*** kemudian ketik
Acl url dstdomain "/etc/squid/domain"
http_access deny url
acl local src 192.168.1.0/24
http_access allow local
http_access allow all

Gambar 38. *Konfigurasi Squid*

Pada gambar 38 ketik perintah : ***nano/etc/squid/domain*** kemudian masukan *domain / IP website* yang dinilai mengandung *malware* yang akan *diblock* oleh *squid*

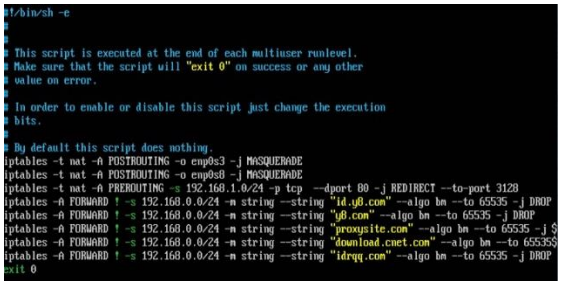


Gambar 39. *Konfigurasi Squid*

Pada gambar 39 kemudian *restart service squid*

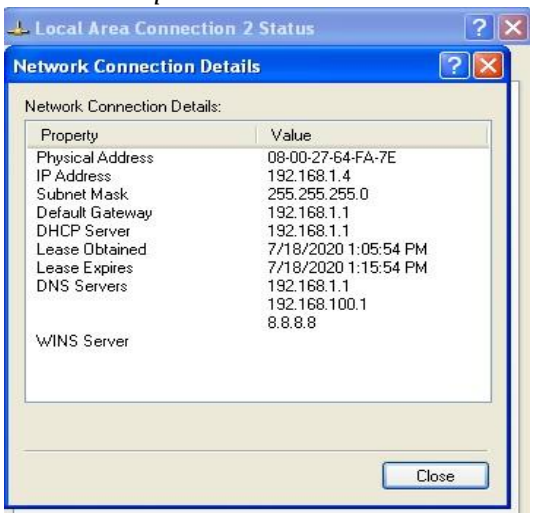
5. Operate

Melakukan kegiatan pengamatan pada jaringan komputer dan memastikan sistem *filtering proxy server* dapat digunakan pada jaringan Cakrabuana *Cruise Ship* & Hotel *School* Cirebon.



Gambar 40. Pengamatan Situs *Malware*

pada gambar 40 *situs* yang mengandung *malware* akan di *redirect* ke *port* 3128 yaitu *port* default *squid*.



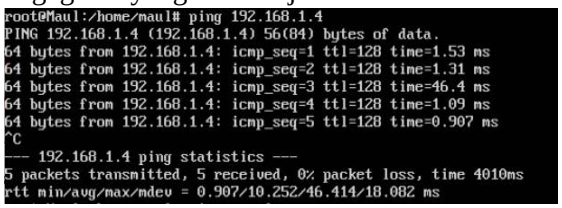
p-ISSN 2089-0265
e-ISSN 2598-3016

Gambar 41. Pengamatan *DHCP Client*

pada gambar 41 uji coba dhcp pada client dengan mendapatkan alamat *IP address 192.168.1.4* dengan *subnet 255.255.255.0*

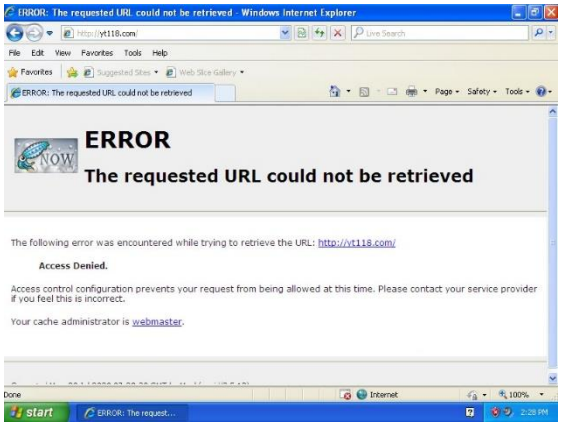
6. Optimize

Tahap akhir adalah *optimize* peneliti memprediksi dan meminimalisir masalah dan kegagalan yang akan terjadi



Gambar 42 Test Ping

Pada gambar 42 dilakukanya *test ping* untuk memastikan tidak ada *error*



Gambar 43 Test Website Proxy

Pada gambar 43 dilakukanya uji coba blokir *website* yang mengandung *malware*

4. Simpulan dan Saran

Berdasrkan pembahasan dari penelitian ini dapat disimpulkan bahwa dengan menerapkan *filtering proxy* dapat meningkatkan keamanan dan meminimalisirkan penyebaran *malware*.

Adapun saran dari pengembangan sistem ini kedepannya dapat menggunakan fitur lain yang terdapat di *squid* untuk memaksimalkan kecepetan maupun kinerja *server* dalam jaringan komputer.

5. Daftar Pustaka

Adhiwibowo, W., & Mindatama, W. (2019). Implementasi Sistem Voucher dengan Router Mikrotik. *Pengembangan Rekayasa Dan Teknologi*, *15*(2), 118–123. https://doi.org/http://dx.doi.org/10.26623/jprt.v15i2.1766

Cahyanto, T. A., Wahanggara, V., & Ramadana, D. (2017). Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis. *Justindo, Jurnal Sistem & Teknologi Informasi Indonesia*, *2*(1), 19–30. http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/1037

CSIRT. (2015). *Panduan Penanganan Insiden Keamanan Jaringan*. 1–49.