**LAPORAN PENELITIAN**

# RANCANG BANGUN LABORATORIUM *CYBERSECURITY VIRTUAL* MENGGUNAKAN PROXMOX VIRTUAL ENVIRONMENT PADA *SERVER* PRODI TEKNOLOGI INFORMASI


## Peneliti:

**Miskatur Rahman**

NIM. 180705045


| | |
|---|---|
| **Jenis Penelitian** | **Terapan** |
| **Bidang Ilmu Kajian** | **Cybersecurity** |
| **Dosen Peneliti** | **Malahayati, M.T** |


**UNIVERSITAS ISLAM NEGERI BANDA ACEH**

**FAKULTAS SAINS DAN TEKNOLOGI**

**PRODI. TEKNOLOGI INFORMASI**

**APRIL 2023**

**LEMBARAN IDENTITAS DAN PENGESAHAN LAPORAN PENELITIAN**
**PUSAT PENELITIAN DAN PENERBITAN LP2M UIN AR-RANIRY**
**TAHUN 2023**

| | | | |
|---|---|---|---|
| 1. a. | Judul | : | Rancang Bangun Laboratorium *Cybersecurity Virtual* Menggunakan Promox Virtual Environment Pada Server Prodi Teknologi Informasi |
| b. | Klaster | : | Penelitian Inter Disipliner |
| c. | No. Registrasi | : | - |
| d. | Bidang Ilmu yang diteliti | : | Sains dan Teknologi |
| 2. | Peneliti | | |
| a. | Nama Lengkap | : | Miskatur Rahman |
| b. | Jenis Kelamin | : | Laki Laki |
| c. | NIM | : | 18705045 |
| h. | Fakultas/Prodi | : | Sains dan Teknologi / Teknologi Informasi |
| i. | Anggota Peneliti 1 | | |
| | Nama Lengkap | : | Malahayati, M.T |
| | Jenis Kelamin | : | Perempuan |
| | Fakultas/Prodi | : | Sains dan Teknilogi/ Teknologi Informasi |
| j. | Anggota Peneliti 2 *(Jika Ada)* | | |
| | Nama Lengkap | : | Mulkan Fadhli, S.T, M.T |
| | Jenis Kelamin | : | Laki laki |
| | Fakultas/Prodi | : | Sains dan Teknilogi/ Teknologi Informasi |
| 3. | Lokasi Kegiatan | : | Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh |
| 4. | Jangka Waktu Pelaksanaan | : | 6 (Enam) Bulan |
| 5. | Tahun Pelaksanaan | : | 2023 |
| 6. | Jumlah Anggaran Biaya | : | - |
| 7. | Sumber Dana | : | Mandiri |
| 8. | *Output* dan *Outcome* | : | - |

Mengetahui,
Pembimbing 1

**Dr. Malahayati. M.T**
NIP. 198301272015032003

Banda Aceh, 11 April 2023
Pelaksana,

**Miskatur Rahman**
NIM. 180705045

Menyetujui:

Ketua Prodi. Teknologi Informasi

**Ima Dwitawati**

NIP. 198210132014032002

# ABSTRAK


| | | |
|---|---|---|
| Nama | : | Miskatur Rahman |
| Nim | : | 180705045 |
| Program Studi | : | Teknologi Informasi |
| Judul | : | Rancang Bangun Laboratorium *Cybersecurity* Virtual Menggunakan Proxmox *Virtual Environment* pada *Server* Prodi Teknologi Informasi |
| Tanggal Sidang | : | 11 April 2023 |
| Jumlah Halaman | : | 80 Halaman |
| Pembimbing I | : | Malahayati, M.T |
| Pembimbing II | : | Mulkan Fadhli, S.T., M.T |
| Kata Kunci | : | *Cybersecurity*, Proxmox, *Server* |



Prodi Teknologi Informasi (TI) semakin berkembang setiap tahunnya, mulai dari hal pengadaan perlengkapan untuk kebutuhan praktikum maupun dalam hal mahasiswa yang terus bertambah setiap tahunnya. Kebutuhan pada laboratorium komputer semakin meningkat dan komputer pada laboratorium sangat terbatas sedangkan mahasiswa setiap unitnya melebihi jumlah komputer pada laboratorium. Maka dari itu, dibutukan komputer tambahan untuk memenuhi kebutuhan mahasiswa karena, ruang laboratorium terbatas maka penelitian ini memiliki target untuk membangun sebuah laboratorium *cybersecurity* virtual dengan tujuan untuk memenuhi kebutuhan penggunaan komputer pada laboratorium. Namun, pengadaan peralatan dan infrastruktur yang dibutuhkan untuk menyiapkan laboratorium *cybersecurity* dapat menjadi sangat mahal. Oleh karena itu, rancang bangun laboratorium *cybersecurity* virtual menggunakan Proxmox *Virtual Environment* (VE) pada *server* Prodi Teknologi Informasi dapat menjadi solusi yang efektif dikarenakan, hanya membutuhkan *server* dan sebuah platform *open source* yaitu proxmox VE yang dapat digunakan untuk mengelola dan membuat virtualisasi *server*. Dengan menggunakan proxmox, kita dapat dengan mudah membuat dan mengelola berbagai macam sistem operasi dan aplikasi dalam satu *server* fisik. Metode yang digunakan adalah metode NDCL yang terdiri dari analisis, desain, implementasi, dan monitoring. Hasil yang di dapatkan saat melakukan uji ketahanan *server* pada laboratorium *cybersecurity virtual* dengan menjalankan lima VM secara bersamaan terjadinya delay sebanyak 6,14% saat digunakan untuk menginstal aplikasi secara bersamaan. Kemudian kegunaan RAM menjadi meningkat dan juga *swap usage* meningkat hingga 54,90%. Lalu dari praktikum yang dilakukan pada laboratorium *cybersecurity* virtual memiliki hasil yang bagus.



Kata Kunci: *Cybersecurity*, Proxmox, *Server*

# DAFTAR ISI

# DAFTAR GAMBAR

# DAFTAR TABEL

# BAB I
# PENDAHULUAN

## I.1 Latar Belakang

Prodi Teknologi Informasi (TI) semakin berkembang setiap tahunnya, mulai dari hal pengadaan perlengkapan untuk kebutuhan praktikum maupun dalam hal mahasiswa yang terus bertambah setiap tahunnya. Kebutuhan praktikum pada laboratorium komputer semakin meningkat akan tetapi komputer pada laboratorium sangat terbatas sedangkan mahasiswa setiap unitnya melebihi jumlah komputer pada laboratorium. Maka dari itu, dibutuhkan komputer tambahan untuk memenuhi kebutuhan mahasiswa, akan tetapi ruang laboratorium sangat terbatas maka penelitian ini memiliki target untuk memaksimalkan laboratorium Prodi Teknologi Informasi.

Seperti penelitian yang dilakukan oleh (Uramová et al., 2021) bahwa dibutuhkan laboratorium virtual di universitas selama pandemi untuk memudahkan dalam mengajar langsung maupun online dengan menggunakan GNS3. Tujuannya untuk mengenalkan siswa dengan tugas analisis keamanan siber dan konsep manajemen keamanan siber. Kemudian siswa juga diminta untuk mempraktekkan dalam bentuk berupa tugas.

Selanjutnya pada penelitian yang dilakukan oleh (Robles-Gómez et al., 2020) yaitu mengevaluasi laboratorium jarak jauh yang diberi nama (VIRE-Lab) dibuat untuk keamanan siber dan dihosting pada cloud menggunakan teknologi virtualisasi. Laboratorium tersebut dibangun di atas teknologi Emulated Virtual Enviroment – Next Genera (EVE-NG). Hasil yang diperoleh dari penilaian laboratorium dibagi dalam beberapa bagian yaitu, dalam hal interaksi dengan laboratorium, kepuasan menggunakannya, dan penerimaan siswa terhadap teknologi.

Laboratorium pada prodi teknologi informasi memiliki peran yang sangat penting dalam mendukung proses belajar mengajar dan penelitian di bidang teknologi informasi. Karena mahasiswa membutuhkan pengalaman praktikum untuk menerapkan konsep-konsep dan teknik-teknik yang dipelajari dalam kuliah. Namun dengan adanya laboratorium dapat membuat mahasiswa melatih

pengembangan keterampilan agar dapat lebih berkembang dan lebih leluasa saat belajar.

Pengadaan peralatan dan infrastruktur yang dibutuhkan untuk menyiapkan laboratorium komputer dapat menjadi sangat mahal. Oleh karena itu, rancang bangun laboratorium *cybersecurity* virtual menggunakan Proxmox Virtual Environment (VE) pada *server* Prodi Teknologi Informasi dapat menjadi solusi yang efektif dikarenakan, hanya membutuhkan *server* dan sebuah *platform open source* yaitu Proxmox VE yang dapat digunakan untuk mengelola dan membuat virtualisasi *server*.

Laboratorium *cybersecurity* virtual ini selesai di bangun, maka akan dilakukannya uji coba ketahanan *server* tersebut, berguna untuk mengetahui seberapa sanggup *server* itu menghandle laboratorium *cybersecurity* virtual itu bekerja dalam waktu bersamaan.

## I.2 Rumusan Masalah

Merujuk dari latar belakang tersebut, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana merancang sebuah laboratorium *cybersecurity* virtual di *server* Prodi Teknologi Informasi ?
2. Bagaimana menginstall Proxmox VE di *server* Prodi Teknologi Informasi?
3. Bagaimana menguji laboratorium *cybersecurity* virtual agar dapat berjalan dengan baik?

## I.3 Tujuan Penelitian

Berdasakan latar belakang dan rumusan masalah yang telah di uraikan, maka tujuan penelitian ini adalah :

1. Merancang laboratorium *cybersecurity* virtual.
2. Menginstall proxmox VE pada *server* Teknologi Informasi.
3. Menguji laboratorium *cybersecurity* virtual dapat berjalan dengan baik.

## I.4 Batasan Masalah

Agar pembahasan dari penelitian ini sesuai dengan judul dan latar belakang yang telah di uraikan, maka untuk membatasi masalah yang akan dibahas pada penelitian ini sebagai berikut :

1. Membuat Laboratorium *cybersecurity* virtual
2. Menggunakan proxmox VE
3. Menggunakan *server* DELL PowerEdge R440

## I.5 Manfaat Penelitian

Berdasarkan latar belakang, rumusan masalah dan tujuan penelitian yang telah di uraikan maka manfaat dari penelitian ini yaitu:

1. Dapat digunakan oleh mahasiswa Prodi Teknologi Informasi.
2. Dapat menjadi referensi kepustakaan bagi UIN Ar-raniry.

# BAB II
# LANDASAN TEORI

## II.1 Laboratorium

Laboratorium adalah tempat yang digunakan untuk melakukan penelitian ilmiah, eksperimen, dan tes. Selain itu, laboratorium juga dapat diartikan sebagai tempat pembelajaran untuk konsentrasi keilmuan tertentu, seperti kampus atau kelas, alam atau lingkungan, lembaga sosial kemasyarakatan, atau bahkan masyarakat itu sendiri. Laboratorium tidak hanya terbatas pada sebuah ruangan atau gedung, tetapi juga mencakup peralatannya (Muhajarah & Sulthon, 2020).

## II.2 Laboratorium Virtual

Laboratorium virtual adalah laboratorium yang berada di dalam perangkat computer/laptop yang digunakan siswa dalam melakukan eksperimen dengan aplikasi tanpa memerlukan adanya alat-alat laboratorium nyata (Gunawan 2017).

Laboratorium virtual adalah sebuah sistem yang memungkinkan seseorang untuk melakukan simulasi atau mengalami suatu kegiatan sama seperti di laboratorium fisik, namun tidak perlu berada di tempat yang sama. Laboratorium virtual bisa diakses melalui komputer atau perangkat mobile yang terhubung ke internet.

Laboratorium virtual memiliki banyak manfaat, diantaranya:

1. Menghemat biaya: Laboratorium virtual dapat menghemat biaya yang dibutuhkan untuk membeli peralatan dan menyewa ruangan laboratorium.
2. Akses mudah: Laboratorium virtual dapat diakses dari mana saja, selama terhubung ke internet. Ini memudahkan para pengguna untuk belajar di waktu yang fleksibel.
3. Pembelajaran yang lebih efektif: Laboratorium virtual memungkinkan para pengguna untuk melakukan simulasi dan mengalami kegiatan secara langsung, sehingga membantu mereka memahami konsep dengan lebih baik.
4. Keamanan: Laboratorium virtual juga lebih aman karena tidak perlu menggunakan bahan kimia atau peralatan yang berbahaya.

Meskipun laboratorium virtual memiliki banyak manfaat, ada beberapa kekurangan yang perlu dipertimbangkan. Salah satunya adalah bahwa laboratorium virtual tidak selalu dapat menyediakan pengalaman yang sama dengan laboratorium

fisik. Selain itu, laboratorium virtual juga mungkin tidak dapat menyediakan semua peralatan yang dibutuhkan untuk setiap kegiatan.

Namun demikian, laboratorium virtual merupakan alternatif yang sangat bermanfaat bagi para pengguna yang ingin belajar dan mengalami kegiatan di laboratorium, tetapi tidak memiliki akses ke laboratorium fisik atau tidak memiliki cukup dana untuk membeli peralatan yang dibutuhkan.

### *II.3* Pengertian *Server*

Menurut jurnal yang berjudul *"Design of a Scalable Multi-Server Architecture for Cloud Storage Services"* karya Haibin Zhang dan Jianqiang Luo (2015), *server* dapat diartikan sebagai sebuah komputer atau sistem yang memiliki perangkat keras dan perangkat lunak yang berfungsi untuk menyediakan berbagai layanan kepada pengguna melalui jaringan. *Server* dapat melakukan tugas-tugas seperti menyimpan dan memproses data, mengelola akses pengguna ke berbagai aplikasi dan layanan, serta menjaga keamanan data dan jaringan.

*Server* ialah seperangkat komputer yang terdiri atas program-program dengan fungsi sebagai tempat penyimpanan informasi dan kemudian mendistribusikan informasi tersebut pada komputer client yang mengaksesnya. Jadi, *server* merupakan perangkat keras yang yang terdiri dari beberapa layanan aplikasi tetapi bila jaringannya lebih komplek, maka sever tersebut bisa diatur satu atau untuk beberapa layanan saja. Kemudian layanan lainnya akan diberikan pada *server* yang lain, jika terjadi kolaborasi dan kerjasama dari beberapa *server* untuk memberikan layanan dan informasi kepada beberapa client. Umumnya, organisasi terkemuka seperti perusahaan-perusahaan kelas atas yang menerapkan *server* dengan konfigurasi yang kompleks, sedangkan *server* yang lebih sederhana yang menggunakan satu buah perangkat komputer dengan fungsi melayani beberapa layanan umumnya digunakan untuk ruang lingkup yang lebih kecil contohnya, dalam dunia pendidikan, kantor dan usaha kecil menengah (UKM).

*Server* merupakan bagian terpenting dari jaringan dikarenakan sever inti dari berbagai macam data dan aplikasi. *Server* berfungsi untuk memenuhi semua kepentingan. Sebagian besar *server* saat ini adalah web *server* dikarenakan terdapat database dan aplikasi web, dan dipakai juga untuk melayani aplikasi dari klien yang diakses melalui *browser*.

Sekarang ini *server* bukan hanya sebagai tempat aplikasi web saja, namun *server* menjadi lebih maju seperti *database server*, *mail server,* dll. Banyaknya aplikasi berpengaruh pada jumlah kebutuhan sumber daya pendukung, artinya semakin banyak aplikasi maka kebutuhan sumber daya pendukung juga berkembang, seperti kebutuhan sumber daya listrik, ruangan, dll. Solusi yang dapat diambil dari masalah tersebut adalah dengan menggunakan virtualisasi *server* yang menggunakan beberapa mesin *server* digabung menjadi satu. Mulai dengan adanya *cloud computing*.

Seperti sistem operasi *online*, berupa aplikasi *online* seperti *google docs*, *google slide,* dropbox dll. Pemakaian *server* yang semakin bermacam-macam membutuhkan sumber daya yang cukup sehingga dana yang dikeluarkan menjadi lebih besar, hal ini dikarenakan dalam membuat sebuah *server* setiap fungsinya harus dipisahkan agar tetap berjalan dengan stabil. Contoh aplikasi yang dapat dipakai dalam membuat virtualisasi *server* seperti Open Virtuozzo (VZ) dan proxmox.

## II.4 Pengertian Virtualisasi

Virtualisasi adalah suatu teknologi pada sebuah perangkat lunak yang memungkinkan satu perangkat keras untuk menjalankan beberapa sistem operasi dan servis pada saat yang sama. Layanan-layanan *server* dijalankan pada mesin-mesin *server* virtual di dalam mesin *server* fisik Saat ini, ada berbagai macam *server* produk virtualisasi. Proxmox adalah salah satunya produk, tetapi memiliki keunggulan utama pesaing dengan memiliki lisensi gratis dan mempunyai fitur yang sama dengan pesaing (Abdurrahman et al., 2019).

Ada beberapa jenis virtualisasi yang umum digunakan, di antaranya:

1. Virtualisasi Level Sistem Operasi (OS-level Virtualization): Jenis virtualisasi ini memungkinkan beberapa sistem operasi berjalan pada satu kernel OS yang sama. Contoh teknologi virtualisasi level sistem operasi adalah LXC (Linux Containers) dan OpenVZ. Kelebihan dari jenis virtualisasi ini adalah sangat cepat dan efisien dalam penggunaan sumber daya sistem, namun hanya dapat mendukung sistem operasi yang sama dengan kernel OS yang digunakan.
2. Virtualisasi Level Hypervisor (Hypervisor-level Virtualization): Jenis virtualisasi ini memungkinkan beberapa sistem operasi berjalan pada satu

hardware yang sama, dengan menggunakan hypervisor sebagai mediator antara hardware dan sistem operasi. Contoh teknologi virtualisasi level hypervisor adalah KVM (*Kernel-based Virtual Machine*), VMware, dan Xen. Kelebihan dari jenis virtualisasi ini adalah dapat mendukung berbagai jenis sistem operasi, namun penggunaan sumber daya sistem lebih besar dibandingkan virtualisasi level sistem operasi.

3. Virtualisasi Desktop (Desktop Virtualization): Jenis virtualisasi ini memungkinkan pengguna untuk menjalankan desktop pada *server* dan mengaksesnya melalui jaringan. Contoh teknologi virtualisasi desktop adalah VirtualBox dan VMware Workstation. Kelebihan dari jenis virtualisasi ini adalah memungkinkan pengguna untuk menjalankan desktop pada sistem operasi yang berbeda, namun penggunaan sumber daya sistem lebih besar dibandingkan virtualisasi level sistem operasi atau hypervisor.
4. Virtualisasi Aplikasi (Application Virtualization): Jenis virtualisasi ini memungkinkan aplikasi dijalankan dalam lingkungan terisolasi pada satu mesin fisik. Contoh teknologi virtualisasi aplikasi adalah Docker dan App-V. Kelebihan dari jenis virtualisasi ini adalah memungkinkan pengguna untuk menjalankan aplikasi pada berbagai jenis sistem operasi, namun penggunaan sumber daya sistem lebih kecil dibandingkan jenis virtualisasi lainnya.

Secara keseluruhan, virtualisasi adalah teknologi yang sangat berguna dalam mengoptimalkan penggunaan sumber daya sistem dan memungkinkan pengguna untuk menjalankan berbagai jenis sistem operasi dan aplikasi pada satu hardware yang sama. Ada beberapa jenis virtualisasi yang dapat digunakan, tergantung pada kebutuhan dan tujuan penggunaannya.

## II.5 Pengertian Proxmox

Proxmox Virtual Environment *(VE)* adalah sebuah mesin virtual yang dapat menvirtualisasi *server* dan dapat membuat penggunaan *server* menjadi lebih simple, proxmox sudah banyak digunakan oleh pengguna teknologi virtualisasi, sepetri contohnya *server* pada kampus, perkantoran, bisnis, dan *server* pada pemerintahan Sebagian juga sudah menggunakan proxmox. Proxmox sebuah sitem turunan dari linux Debian dengan kernel RHEL namun dimodifikasi untuk membuat, menjalankan, dan mengelola mesin virtualisasi (Semarang, 2014).

Proxmox VE memiliki fungsi khusus sebagai virtualisasi *Operating System* maupun *Appliance*. Berikut beberapa teknologi virtulaisasi yang bisa digunakan pada Proxmox VE.

1. *Kernel Virtual Machine* (KVM)

   Merupakan kernel-based virtual *machine* yang ditambahkan pada linux berguna untuk membuat full virtualisasi. KVM juga bagian integral daro Linux sejak tahun 2017.

2. Linux Container (LXC)

   Sering disebut sebagai virtualisasi *Operatig System* (OS), LXC adalah virtualisasi yang menggunakan *Container*. Virtualisasi ini memiliki tingkat efisiensi yang tinggi dan juga kecepatan aksesnya menjadi XC berkembang dengan cepat.

3. QEMU

   QEMU (Quick EMUlator) adalah sebuah program perangkat lunak yang berfungsi sebagai emulator dan virtualisasi sistem komputer. Dengan QEMU, pengguna dapat menjalankan sistem operasi dan aplikasi pada platform yang berbeda dari sistem host yang sedang digunakan. QEMU dapat menjalankan berbagai jenis arsitektur dan platform, seperti x86, ARM, PowerPC, SPARC, dan lain-lain.

### *II.6* Pratikum *Cybersecurity*

*Cybersecurity* adalah teknologi yang menemukan, melindungi, dan menjamin segala sesuatu yang berkaitan dengan keamanan perusahaan dari ancaman luar. Di dalamnya, *cyber security* memiliki bentuk implikasi pengendalian pada keamanan dan kekuatan sistem, yaitu operating system security yang terdiri dari *authentication and authorization*, *file system permissions*, *access privileges*, *logging and system monitoring*, dan *system services*. Keamanan sistem memiliki hubungan dengan tingkat keamanan bertransaksi. Untuk mengukur keamanan bertransaksi di e-commerce dapat dilihat dari dua indikator, yaitu reputasi dan *perceive risk* (Setiawan, 2019).

Macam-macam *cybersecurity* yang umum ditemukan:

1. Keamanan jaringan (Network Security) Network Security adalah upaya untuk melindungi jaringan komputer dari akses yang tidak sah, perusakan, atau

pencurian data. Contoh dari teknologi keamanan jaringan antara lain firewall, VPN, IDS, IPS, dan lain-lain.

2. Keamanan sistem (System Security) System Security adalah upaya untuk melindungi sistem komputer dari serangan dan ancaman yang berasal dari perangkat lunak jahat, virus, dan malware. Contoh teknologi keamanan sistem antara lain antivirus, anti-malware, encryption, dan lain-lain.
3. Keamanan aplikasi (Application Security) Application Security adalah upaya untuk melindungi aplikasi komputer dari serangan dan ancaman yang berasal dari perangkat lunak jahat, virus, dan malware. Contoh teknologi keamanan aplikasi antara lain testing keamanan aplikasi, penggunaan kode sumber terbuka, dan lain-lain.
4. Keamanan data (Data Security) Data Security adalah upaya untuk melindungi data komputer dari akses yang tidak sah, perusakan, atau pencurian data. Contoh teknologi keamanan data antara lain enkripsi, back up data, dan lain-lain.
5. Keamanan fisik (Physical Security) Physical Security adalah upaya untuk melindungi infrastruktur komputer dari serangan dan ancaman yang berasal dari lingkungan fisik, seperti pencurian perangkat keras atau akses fisik yang tidak sah ke perangkat keras. Contoh teknologi keamanan fisik antara lain penggunaan sistem kunci dan sensor, pemantauan video, dan lain-lain.
6. Keamanan internet (Internet Security) Internet Security adalah upaya untuk melindungi penggunaan internet dari serangan dan ancaman yang berasal dari internet, seperti phishing, spam, dan penipuan. Contoh teknologi keamanan internet antara lain antivirus, firewall, VPN, dan lain-lain.
7. Keamanan sosial (Social Engineering Security) Social Engineering Security adalah upaya untuk melindungi dari serangan dan ancaman yang berasal dari penipuan sosial, seperti phishing dan teknik rekayasa sosial. Contoh teknologi keamanan sosial antara lain penggunaan teknologi keamanan pada media sosial, pelatihan keamanan, dan lain-lain.

## II.7 Prodi Teknologi Informasi

Program Studi Teknologi Informasi adalah program studi yang mempelajari tentang pengembangan dan pemanfaatan teknologi informasi dalam menyelesaikan

masalah bisnis dan organisasi. Mahasiswa yang mengambil Program Studi Teknologi Informasi akan belajar tentang berbagai teknologi yang digunakan dalam pengolahan dan pemanfaatan data, termasuk basis data, jaringan komputer, keamanan informasi, dan pengembangan aplikasi.

Mereka juga akan belajar tentang cara mengelola proyek teknologi informasi dan mengembangkan solusi untuk masalah yang dihadapi oleh perusahaan dan organisasi. Program Studi Teknologi Informasi dapat ditemukan di universitas atau institut teknologi di seluruh dunia.

## II.8 Penelitian Terdahulu

Berkaitan dengan penelitian yang dilakukan pada *server*. Dibutuhkan acuan atau penelitian terkait guna untuk terhindar dari duplikasi dan plagiarisme, sehingga dapat mengembangkan sesuatu hal yang berbeda pada penelitian ini. Berikut penelitian terkait yang berkenaan dengan penelitian ini.

Pertama, penelitian mengenai "Merancang Praktikum Teknik Telekomunikasi Dasar melalui Laboratorium Virtual yang Memanfaatkan Teknologi Informasi Komunikasi (TIK)" (Bonok et al., 2022). Tujuan penelitian ini adalah merancang laboratorium virtual teknik telekomunikasi dasar yang digunakan dalam praktikum teknik telekomunikasi dasar. Adapun langkah yang diambil untuk perancangan laboratorium virtual ini dibuat dengan melakukan simulasi laboratorium berbentuk virtual pada teknik telekomunikasi dasar. Dengan memanfaatakan pemrograman komputer seperti Javascript, pemrograman *Personal Home Page* (PHP), Chart js dan basis data MySql. Hasil dari penelitian ini adalah bahwa laboratorium virtual ini berhasil dirancang simulator percobaan proses modulasi amplitudo dan modulasi frekuensi untuk mata kuliah praktikum teknik telekomunikasi dasar serta sistem informasi dari manajemen laboratorium virtual yang telah dapat diakses melalui web.

Kedua, penelitian mengenai "Optimalisasi Penggunaan VirtualBox Sebagai *Virtual Computer Laboratory* untuk Simulasi Jaringan dan Praktikum pada sekolah menengah kejuruan (SMK) Taruna Mandiri Pekanbaru" (Anam et al., 2020). Dalam penelitian ini Laboratorium komputer dengan perangkat komputer yang memiliki spesifikasi tinggi merupakan salah satu syarat yang harus dipenuhi oleh SMK Taruna Mandiri banyak pihak sekolah yang masih belum dapat untuk memenuhi

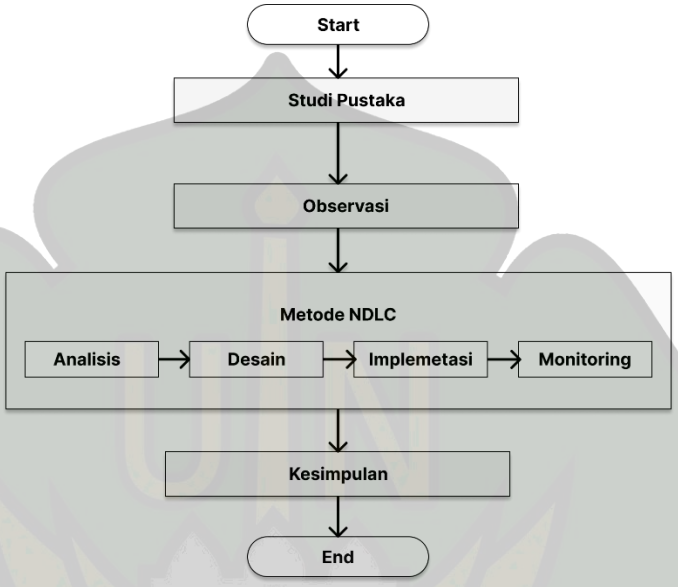
ketentuan tersebut. Sehingga proses belajar mengajar bagi siswa Teknik Komputer Jaringan (TKJ) akan terganggu. Untuk mengatasi hal tersebut, maka dapat digunakan pendekatan *Virtual Laboratory* atau Laboratorium Virtual sehingga siswa dapat memanfaatkan sumber daya yang ada dalam proses belajar mengajar. Hasil yang diperoleh pada kegiatan ini adalah siswa dapat menerapkan sistem pembelajaran yang efektif dengan menggunakan laptop ataupun *Personal Computer* (PC).

Ketiga, penelitian mengenai "Optimalisasi Sumber Daya Komputer Dengan Virtualisasi *Server* Menggunakan Proxmox Ve" (Abdurrahman et al., 2019). Dalam penelitian ini, akan diteliti performa dari virtualisasi *server* menggunakan Proxmox VE. Penelitian ini dimaksudkan untuk mengetahui beban penggunaan memory, *Central Processing Unit* (CPU) pada saat dijalankan semua *server* yang ada di dalam proxmox tesebut dan meneliti *Throughput*, *PacketLoss, Delay* dan *Jitter* yang ada pada *server*.

# BAB III
# METODE PENELITIAN

## III.1 Tahapan Penelitian

Tahapan penelitian mencakup langkah-langkah pelaksanaan dari pertama hingga terakhir, berikut langkah-langkah yang dilakukan dapat dilihat pada gambar 3.1.




Gambar 3.1 Bagan Alir Tahapan Penelitian

Pada gambar 3.1 menunjukkan tahapan penelitian dan setiap tahapan tersebut akan menjelaskan lebih rinci apa-apa saja yang akan dikerjakan. Tahapannya sebagai berikut :

### III.1.1 Studi Pustaka

Studi pustaka diawali dengan mengumpulkan informasi dengan cara mencari dan membaca. Kemudian menggabungkan semua dokumen menjadi satu untuk dijadikan sebagai referensi seperti buku, jurnal, artikel yang berkaitan dengan penelitian ini.

### III.1.2 Observasi

Pada langkah ini melakukan observasi terhadap Prodi Teknologi Informasi bertujuan untuk mengetahui sumber daya yang ada pada Prodi tersebut apa sudah dimenejemen dengan baik.

### III.1.3 Metode Network Development Life Cycle

Metode *Network Development Life Cycle* (NDLC) merupakan sebuah proses rancangan atau pengembangan pada system jaringan computer (Kurniawan, 2016). Metode ini memiliki bagian yang merumuskan setiap tahapan atau mekanisme suatu cara yang jelas. Cycle merupakan kata kunci deskriptif dari siklus hidup pengembangan sistem jaringan yang menggambarkan keseluruhan tahapan dan proses pengembangan sistem jaringan yang bersambung-sambung. ada empat tahapan yang di gunakan untuk penelitian ini yaitu:

**a. Analisis**

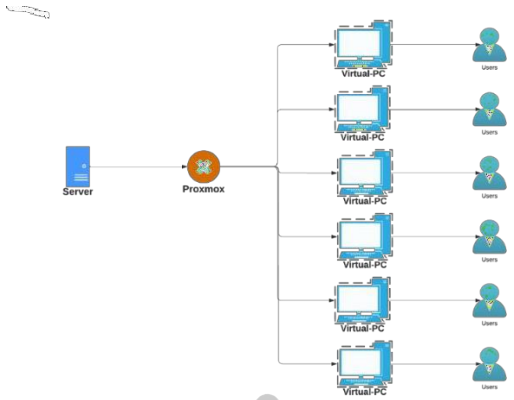
Analisis merupakan tahapan awal penelitian, melakukan analisis terhadap *server* pada Prodi Teknologi Informasi dilakukan konfigurasi terhadap *server* tersebut agar dapat berjalan dengan normal, dan spesifikasi *server* yang digunakan dapat di lihat pada Tabel 3.1.

Tabel 3.1 Spesifikasi *Server* Pada Prodi Teknologi Informasi

| Parameter | Nilai |
|---|---|
| Processor | Intel Xeon Silver 4208 2.1G, 8C |
| RAM | 8GB RDIMM, 2666MT |
| Harddisk | 2TB |

**b. Desain**

Desain merupakan tahapan kedua dari penelitian ini, yang akan di lakukan adalah mendesain atau rancangan gambar yang akan dibuat agar mengetahui bagaimana gambaran sistem itu bekerja, sistem yang akan dibuat tampak pada gambar 3.2.

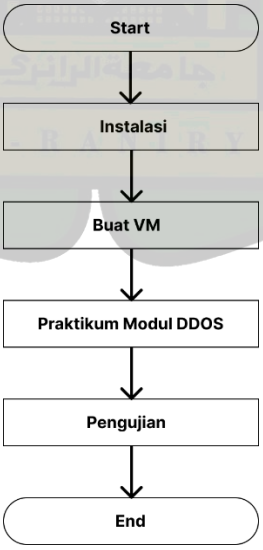



Gambar 3.2 Tampilan Laboratorium *Cybersecurity* Virtual

Pada gambar 3.2 menunjukan sistem yang akan dibuat pada *server,* akan di install proxmox untuk dapat lebih mudah memenejemen *server* karna proxmox berfungsi untuk menvirtualisasikan *server* terserbut, setelah menginstall proxmox dilakukan konfigurasi jaringan terhadap router atau sumber jaringan. Setelah itu mulai untuk membuat laboratorium *cybersecurity* virtual yang dimana harus membagi *storage* dan mengistall sistem operasi di dalam *server* tersebut.

**c. Implementasi**

Tahapan-tahapan yang perlu dilakukan dalam proses instalasi, Pembuatan VM, Konfigurasi Modul Praktikum, dan Pengujian merupakan proses penting dalam pengembangan atau pengoperasian sistem.




Gambar 3.3 Implementasi

1. Instalasi: tahapan ini dilakukan untuk menginstal perangkat lunak yaitu proxmox VE yang dibutuhkan untuk pengembangan atau pengoperasian sistem. Instalasi yang baik dan benar akan memastikan sistem dapat berjalan dengan lancar dan sesuai dengan kebutuhan.

   Proxmox VE adalah platform virtualisasi yang fleksibel dan dapat diandalkan untuk mengelola mesin virtual dan kontainer. Berikut adalah beberapa kegunaan dari instalasi Proxmox VE:

   - Konsolidasi Server: Proxmox VE, dapat menggabungkan beberapa server fisik menjadi satu server virtual yang dapat memudahkan manajemen dan penghematan biaya infrastruktur.
   - Manajemen Mesin Virtual: Proxmox VE memungkinkan untuk membuat, mengelola, dan menghapus mesin virtual dengan mudah dan cepat melalui antarmuka web yang intuitif.
   - Isolasi Aplikasi: Dengan menggunakan kontainer, Proxmox VE memungkinkan untuk menjalankan beberapa aplikasi dalam lingkungan yang terisolasi satu sama lain, yang dapat meningkatkan keamanan dan stabilitas sistem.
   - Skalabilitas: Proxmox VE dapat dengan mudah diskalakan sesuai dengan kebutuhan bisnis Anda, baik itu dalam hal kapasitas pemrosesan, memori, maupun penyimpanan.
   - Ketersediaan Tinggi: Proxmox VE menyediakan fitur ketersediaan tinggi (high availability) yang memastikan layanan tetap berjalan meskipun terjadi kegagalan pada satu atau beberapa node.
   - Backup dan Restore: Proxmox VE menyediakan fitur backup dan restore yang dapat membantu mengamankan dan memulihkan data yang penting dengan cepat dan mudah.

2. *Create* VM: Membuat Virtual Machine (VM) di Proxmox adalah proses membuat mesin virtual baru pada platform virtualisasi Proxmox. VM dapat digunakan untuk menjalankan sistem operasi dan aplikasi pada lingkungan virtualisasi yang terisolasi dari lingkungan fisik yang sebenarnya. Dalam pembuatan VM di Proxmox, pengguna harus memilih jenis sistem operasi, memilih jumlah memori, CPU dan disk yang akan dialokasikan untuk VM,

serta konfigurasi jaringan dan penyimpanan yang akan digunakan untuk VM. Setelah VM berhasil dibuat, pengguna dapat mengelola dan memantau VM melalui Proxmox VE GUI.VM dapat digunakan untuk mengisolasi aplikasi atau sistem operasi yang berbeda pada satu mesin fisik. Hal ini memungkinkan pengguna untuk mengoptimalkan sumber daya *hardware* yang tersedia, menghemat biaya pengadaan *hardware* baru, serta meningkatkan efisiensi dan skalabilitas sistem.

3. Konfigurasi Modul Praktikum: tahapan ini dilakukan untuk mengkonfigurasi atau menyiapkan modul praktikum atau bagian sistem yang akan diuji. Konfigurasi yang baik dan benar akan memastikan bahwa modul praktikum siap untuk diuji dan dapat berjalan dengan lancar.
4. Pengujian: tahapan ini dilakukan untuk menguji atau mengevaluasi sistem atau modul praktikum yang telah dikonfigurasi. Pengujian yang baik dan benar akan memastikan bahwa sistem atau modul praktikum berfungsi sesuai dengan spesifikasi dan memenuhi kebutuhan.

Melalui tahapan-tahapan ini, diharapkan sistem atau modul praktikum dapat dikembangkan atau dioperasikan dengan lebih baik dan sesuai dengan kebutuhan.

**d. Monitoring**

Pada tahapan ini melakukan uji coba pada *server* berguna untuk mengetahui seberapa kuat *server* menghandle 5 Virtual Machine (VM) dan tahapan ini juga melakukan praktikum terkait *cybersecurity* untuk mengetahui laboratorium *cybersecurity* virtual dapat berjalan dengan baik.

**e. Kesimpulan**

Tahapan ini merupakan tahapan akhir dari penelitian yang menyimpulkan tentang penelitian laboratorium *cybersecurity* virtual yang dimana dapat digunakan untuk menunjang pembelajaran mahasiswa Prodi Teknologi Informasi.

## III.2 Alat

Dalam melakukan penelitian ini, memerlukan beberapa alat penunjang berbentuk perangkat keras (*hardware*) dan perangkat lunak (*software*). Berikut perincian alat:

1. Perangkat Keras (*Hardware*)

a. Perangkat keras yang digunakan selama penelitian ini adalah laptop Asus TUF Gaming FC504 Series dengan prosesor Intel Core i7-8750H (2.2GHz, 9MB cache) 8GB DDR4-2666 RAM.
b. *Server* DELL PowerEdge R440 (Xeon Silver 4208 2.1G, 8C, 8GB, 2TB)

2. Perangkat Lunak (*Software*)

Perangkat lunak yang digunakan selama penelitan ini adalah :

a. Proxmox Virtual Environment
b. Sistem Operasi Linux Ubuntu versi 20.04.4.
c. Slowloris
d. Apache

# BAB IV
# HASIL DAN PEMBAHASAN

## *IV.1 Server*

*Server* yang digunakan pada penelitian ini adalah *server* DELL PowerEdge R440 dengan spesifikasi processor Intel Xeon, kapasitas HDD 2 TB dan RAM 8 GB. Gambar 4.1 di bawah ini merupakan *server* pada Prodi Teknologi Informasi.

Gambar 4.1 *Server* Prodi Teknologi Informasi

## IV.2 Konfigurasi Proxmox

Proxmox *Virtual Environment (VE)* adalah sebuah mesin virtual yang dapat menvirtualisasi *server* dan dapat membuat penggunaan *server* menjadi lebih simple, proxmox sudah banyak digunakan oleh pengguna teknologi virtualisasi, seperti contohnya *server* pada kampus, perkantoran, bisnis, dan *server* pada pemerintahan sebagian juga sudah menggunakan proxmox. Proxmox sebuah sitem turunan dari linux Debian dengan kernel RHEL namun dimodifikasi untuk membuat, menjalankan, dan mengelola mesin virtualisasi (Semarang, 2014).

Berikut merupakan langkah-langkah yang dilakukan pada *server* yang ditunjukkan pada gambar 4.2:

1. Install proxmox

Langkah pertama yaitu melakukan penginstalan proxmox pada *server* Prodi TI yang berguna untuk menvirtualisasikan *server* agar dapat menjalankan beberapa

sistem operasi pada *server* fisik. Proxmox juga memberikan kontrol penuh atas sumber daya *server*, termasuk CPU, RAM, dan penyimpanan.

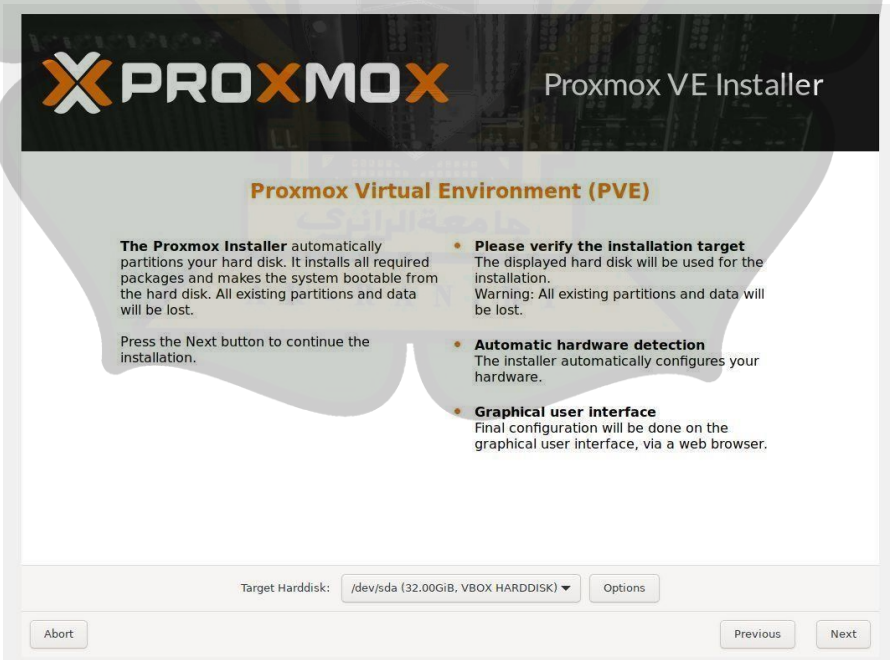
Proxmox juga menyediakan fitur *high availability* yang memungkinkan untuk menjaga uptime yang tinggi dan menjamin *server* tetap berjalan meskipun ada kegagalan perangkat keras atau perangkat lunak. Berikut tata cara penginstalan Proxmox yang harus dilakukan :


Gambar 4.2 Tampilan Awal Penginstalan Proxmox

Pada gambar 4.2 menampilkan menu awal penginstalan proxmox, pilih install Proxmox VE unutk melanjutkan penginstalan ke langkah selanjutnya.


Gambar 4.3 Tampilan Persetujuan Persyaratan

Gambar di atas menampilkan apa saja persyaratan yang harus diterima untuk dapat melanjutkan proses penginstalan Proxmox VE, jika persyaratan di terima maka pilih *I agree* untuk melanjutkan ke proses selanjutnya.




Gambar 4.4 Pemilihan *Storage*

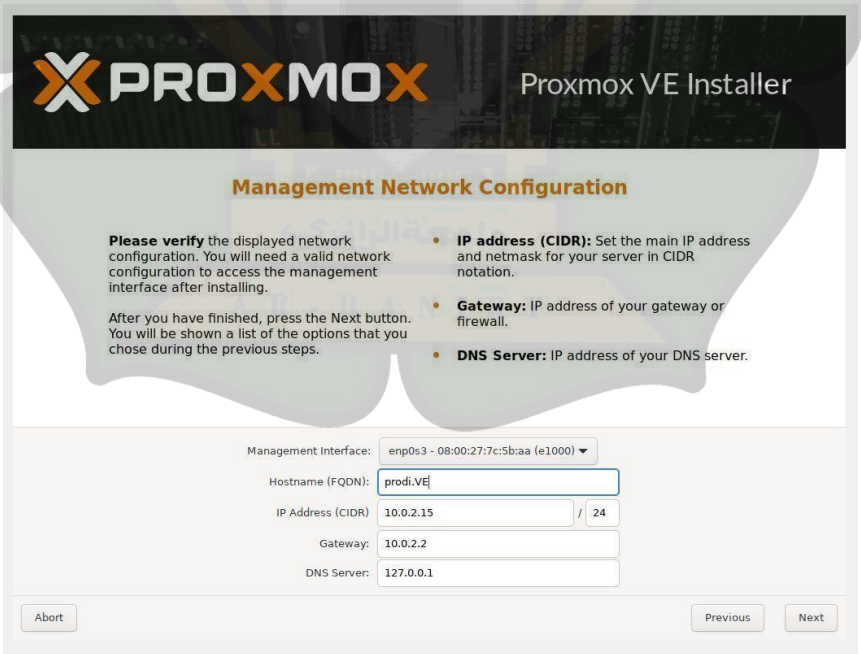
Tahapan pada gambar di atas menampilkan target *harddisk* yang akan digunakan untuk penginstalan Proxmox VE jika sudah memilih hardisk yang ingin digunakan untuk install proxmox VE maka pilih *Next* untuk melanjutkan langkah selanjutnya.


Gambar 4.5 Pemilihan Waktu dan Lokasi

Pada gambar 4.5 menampilkan halaman pemilihan lokasi, waktu dan tata letak *keyboard*. Jika sudah sesuai dengan pilihan maka untuk melanjutkan ke tahap selanjutnya maka pilih *Next*.


Gambar 4.6 Administrasi Email dan *Password*

Pada gambar 4.6 menampilkan *administration password* dan email yang harus di isi, *password* tersebut berguna untuk login pada saat mengakses Proxmox di browser untuk melanjutkan ke langkah selanjutnya pilih *Next*.

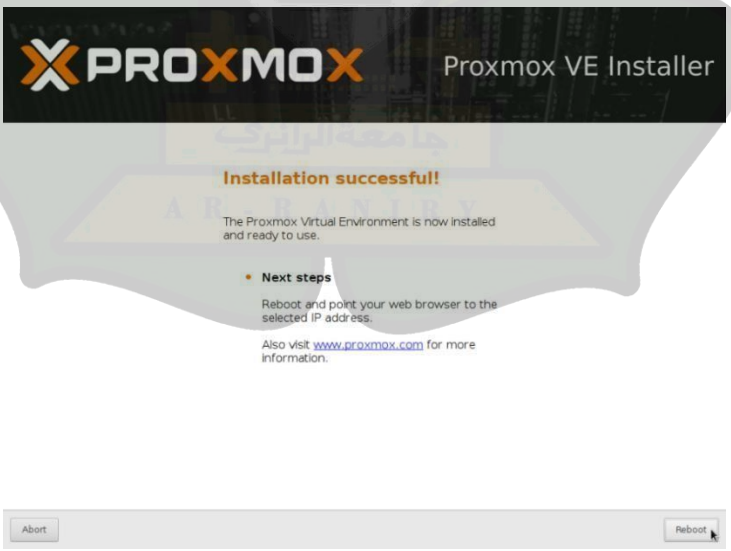



Gambar 4.7 Konfigurasi Jaringan

Pada gambar 4.7 di atas merupakan konfigurasi jaringan yang harus dilakukan yang bertujuan untuk saat mengakses Proxmox melalui browser membutuhkan ip tersebut jika sudah setting ip maka pilih *Next* untuk melanjutkan.


Gambar 4.8 Tampilan Proses Instalasi

Gambar 4.8 menampilkan proses instalasi berjalan, pada tahapan ini instalasi berjalan hingga sekitar 10 menit atau lebih.

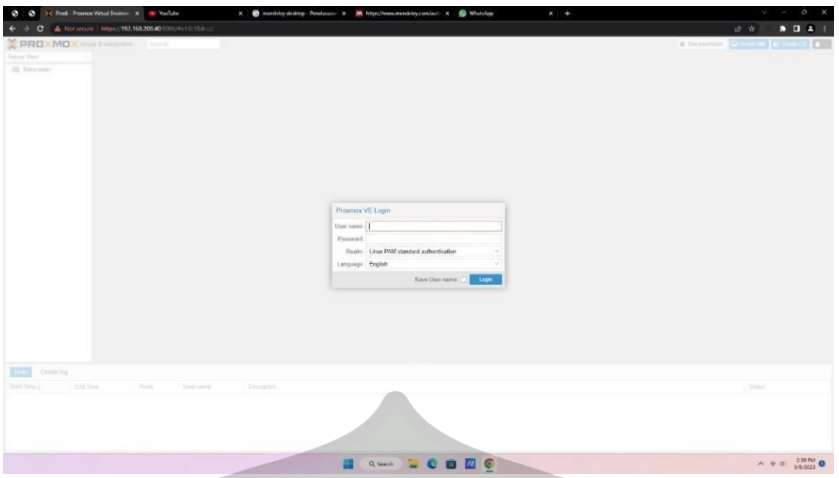



Gambar 4.9 Tampilan Instalasi Berhasil

Pada gambar 4.9 menampilkan bahwa instalasi berhasil dan instalasi selesai maka langkah selanjutnya pilih *Reboot* untuk merestart *server* karena pada saat proses instalasi berjalan ada beberapa konfigurasi yang berubah untuk memastikan sistem berjalan dengan benar, dan tujuan lainnya *Reboot* adalah untuk memuat *driver* baru, karena saat proses install ada driver baru yang di install, maka dibutuhkan *Reboot* untuk dapat menjalankannya.

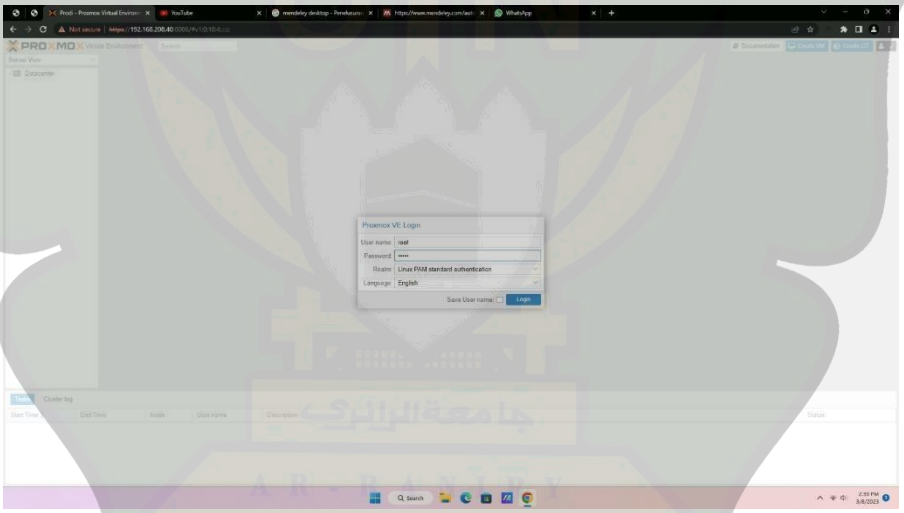

Gambar 4.10 Tampilan Proxmox Setelah Di *Install*

Pada gambar 4.10 menampilkan hasil dari instalasi proxmox yang sudah berhasi dilakukan, di halaman tersebut terdapat link https://192.168.100.2 untuk mengakses proxmox melalui browser.



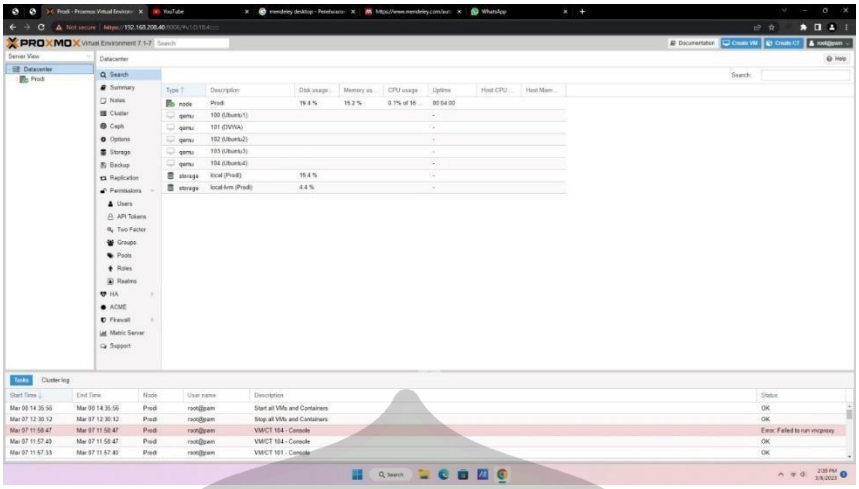
Gambar 4.11 Tampilan Login Proxmox Pada *Browser*

Pada gambar di atas menampilkan Proxmox dalam bentuk *console*. Untuk mengakses Proxmox menggunakan *browser* dapat dilakukan dengan menuliskan alamat IP https://192.168.100.2:8006 yang tertera pada gambar 4.10.



Gambar 4.12 Tampilan *Login*

Gambar di atas menampilkan tampilan halaman *login* untuk dapat masuk ke dalam *dasboard* Proxmox harus mengisi *username* dan *password* yang sudah di atur pada proses penginstallan.



Gambar 4.13 Tampilan Proxmox Setelah *Login*

2. Membuat *virtual machine*

Alasan mengapa pada penelitian ini menggunakan VM karena Isolasi yang lebih ketat pada VM merujuk pada tingkat isolasi yang lebih tinggi antara mesin virtual yang berbeda yang berjalan pada host fisik yang sama. Dalam konteks laboratorium cybersecurity virtual, ini berarti bahwa setiap VM memiliki lingkungan operasi yang terisolasi sepenuhnya, termasuk kernel, sistem operasi, dan ruang alamat memori.

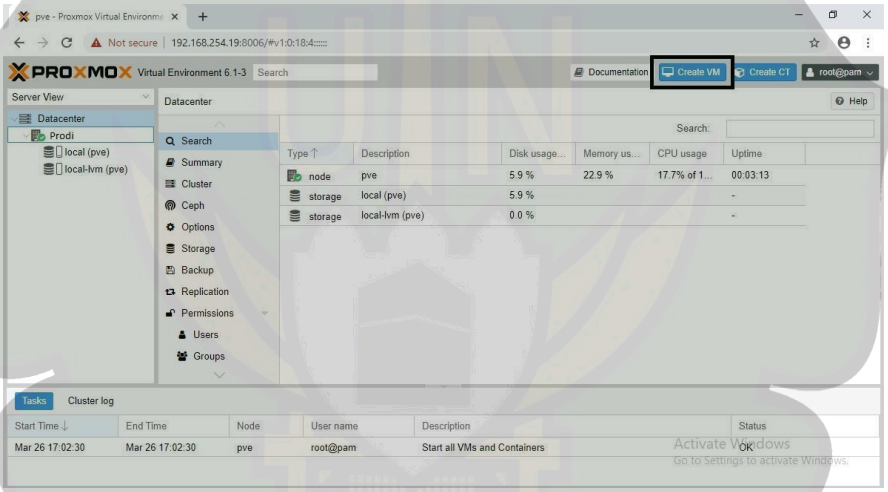
Berikut adalah beberapa contoh isolasi yang lebih ketat yang dimiliki oleh VM:

a. Isolasi Sistem Operasi: Setiap VM pada host fisik dapat menjalankan sistem operasi yang berbeda secara independen. Dapat memiliki beberapa VM dengan sistem operasi yang berbeda, seperti Windows, Linux, atau macOS, yang berjalan pada host yang sama, masing-masing dengan instalasi, konfigurasi, dan aplikasi yang terpisah.
b. Isolasi Kernel: VM memiliki kernel sistem operasi sendiri yang terisolasi sepenuhnya dari kernel host fisik. Hal ini memungkinkan pengujian dan eksperimen pada level kernel secara lebih terpisah, yang dapat berguna dalam skenario lab cybersecurity virtual yang memerlukan pengujian pada kerentanan atau eksploitasi pada level kernel.
c. Isolasi Ruang Alamat Memori: VM memiliki ruang alamat memori yang terpisah, yang berarti bahwa memori yang digunakan oleh satu VM tidak dapat diakses oleh VM lain atau oleh host fisik. Ini memberikan isolasi yang

lebih ketat antara VM, melindungi data dan konfigurasi dari akses yang tidak diizinkan.

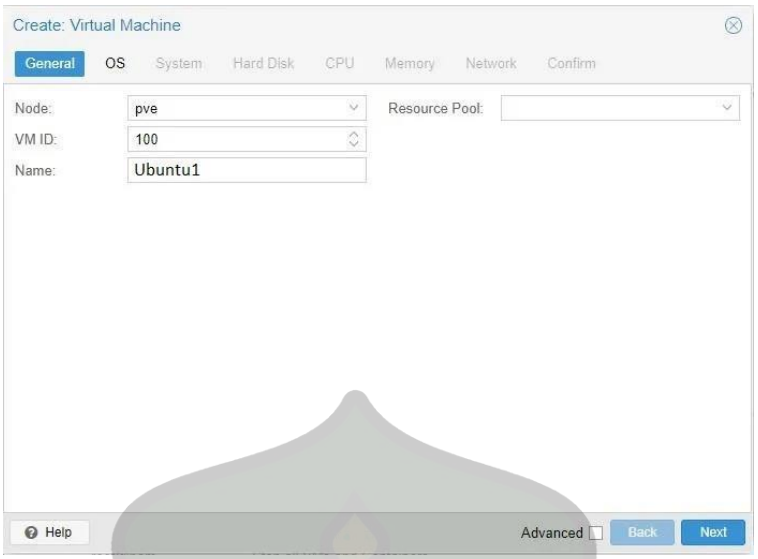
d. Firewall dan Jaringan yang Terpisah: Anda dapat mengkonfigurasi firewall dan jaringan secara terpisah untuk setiap VM, yang memungkinkan isolasi jaringan yang ketat antara VM. Anda dapat mengatur kebijakan akses jaringan yang lebih granular untuk mencegah akses yang tidak diizinkan antara VM, atau untuk mengatur skenario uji coba jaringan yang spesifik dalam lab cybersecurity virtual Anda.

Untuk membangun laboratorium *cybersecurity* virtual menggunakan Proxmox, perlu untuk install *Operating system* (OS) terlebih dahulu berikut langkah-langkah membuat VM:



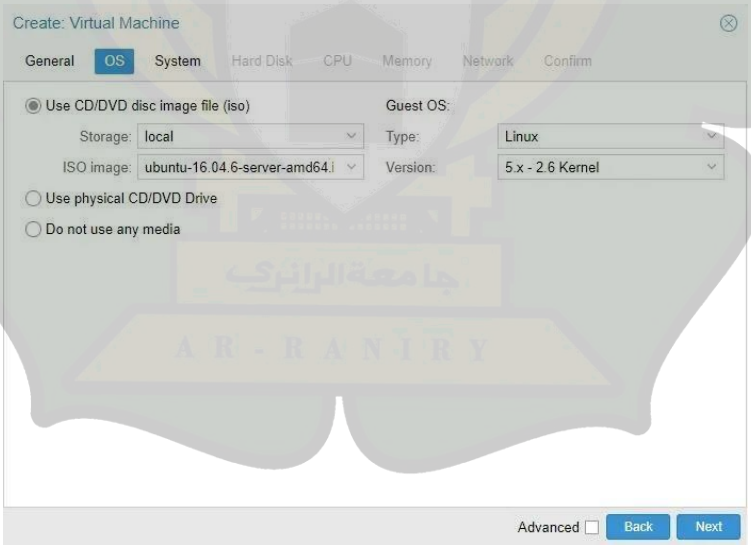

Gambar 4.14 Tampilan Proses Awal Pembuatan VM

Pada gambar 4.14 merupakan tahapan awal dalam membuat VM dengan mengklik *create* VM yang ada pada *dasboard* Proxmox disudut kanan atas.



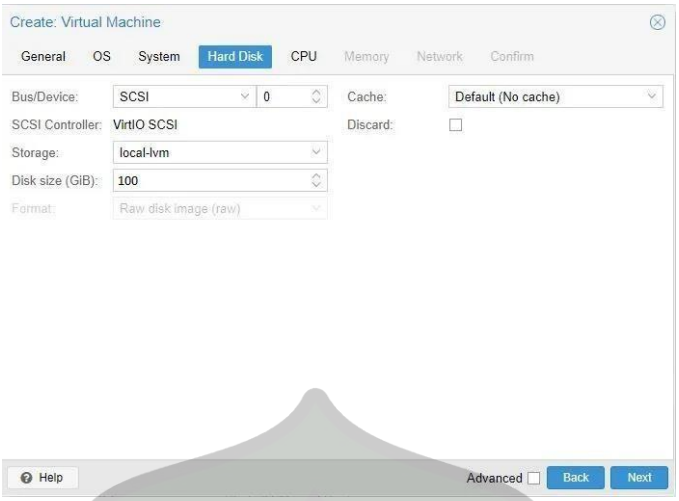

Gambar 4.15 Tampilan Awal Pembuatan VM

Selanjutnya pada gambar 4.15 menampilkan general pada proses setting awal pembuatan VM pada general tersebut terdapat *Node*, VM ID, *Name*, dan *Resource Pool*. Di tahapan ini hanya di wajibkan mengisi nama VM yang akan dibuat jika sudah klik *Next*.



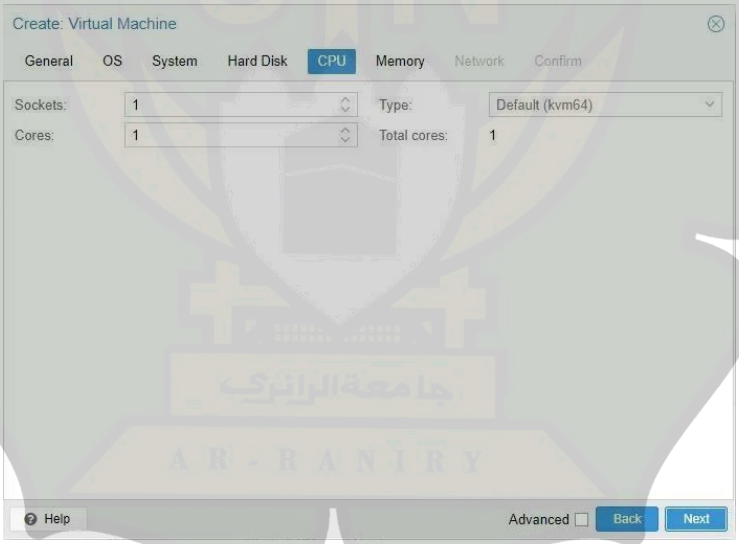

Gambar 4.16 Tampilan Pemilihan Iso OS

Pada gambar 4.16 menampilkan halaman OS, pada halaman tersebut harus memilih iso Ubuntu yang sudah di *upload* di Proxmox jika sudah memilih iso yang ingin digunakan maka selanjutnya klik *Next* pada sudut kanan bawah.



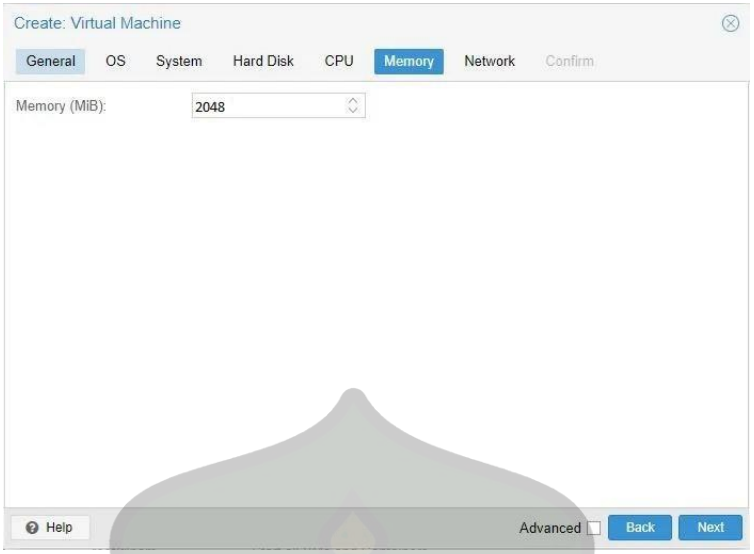

Gambar 4.17 Pengisian Ukuran *Harddisk* Yang Akan Digunakan

Selanjutnya pada gambar 4.17 menampilkan pada bagian *Hard Disk* pada tahap ini di wajibkan untuk menyesuaikan kapasitas *Hard Disk* yang akan digunakan untuk menginstall, jika sudah maka klik *Next.*



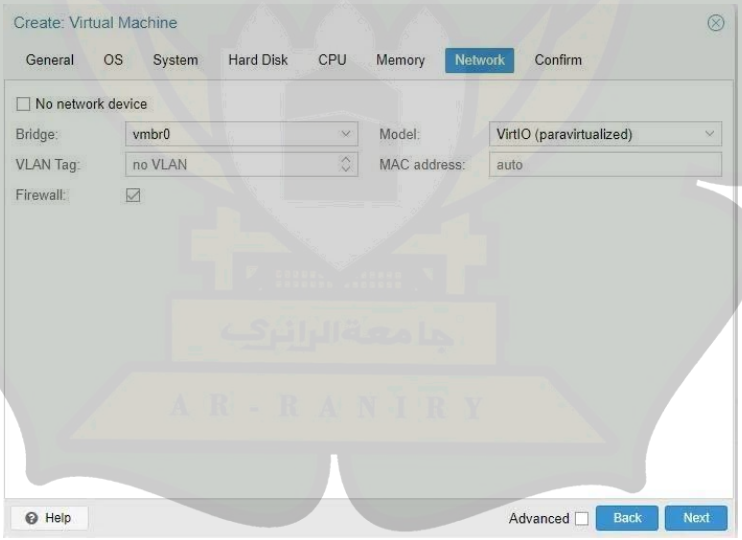

Gambar 4.18 Tampilan CPU Yang Akan Digunakan Oleh VM

Gambar 4.18 menampilkan halaman setting CPU pada halaman tersebut terdapat *Sockets*, *Cores*, *Type*, dan Total *cores*. Jika sudah melakukan setting pada tahapan ini maka klik *Next* pada sudut kanan bawah.



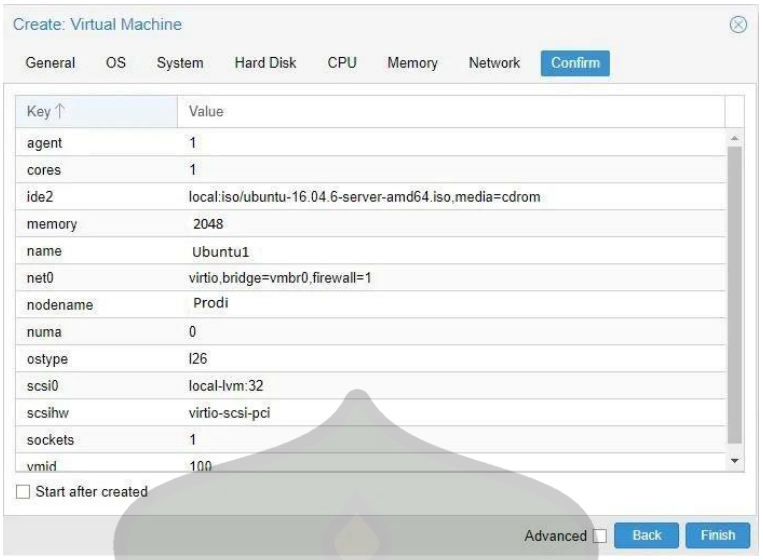

Gambar 4.19 Tampilan Isi Memory Yang Akan Digunakan VM

Gambar 4.19 menampilkan halaman setting Memory atau RAM yang akan di gunakan untuk OS yang akan di install, sesuaikan dengan kebutuhan dan jika sudah klik *Next.*




Gambar 4.20 Tampilan Pemilihan Network Yang Akan Digunakan

Selanjutnya pada gambar 4.20 menampilkan halaman *Network* pada tahapan ini sesuaikan jaringan yang ingin digunakan sesuai kebutuhan jika sudah setting sesuai yang diinginkan maka klik *Next* untuk melanjutkannya.

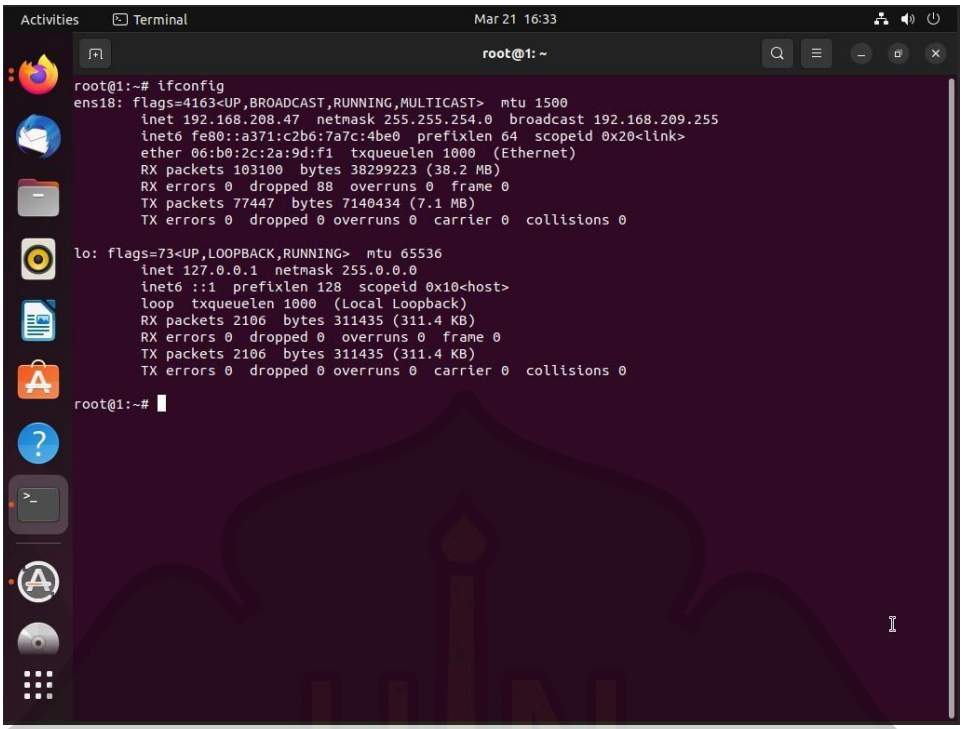



Gambar 4.21 Konfirmasai Penginstalan

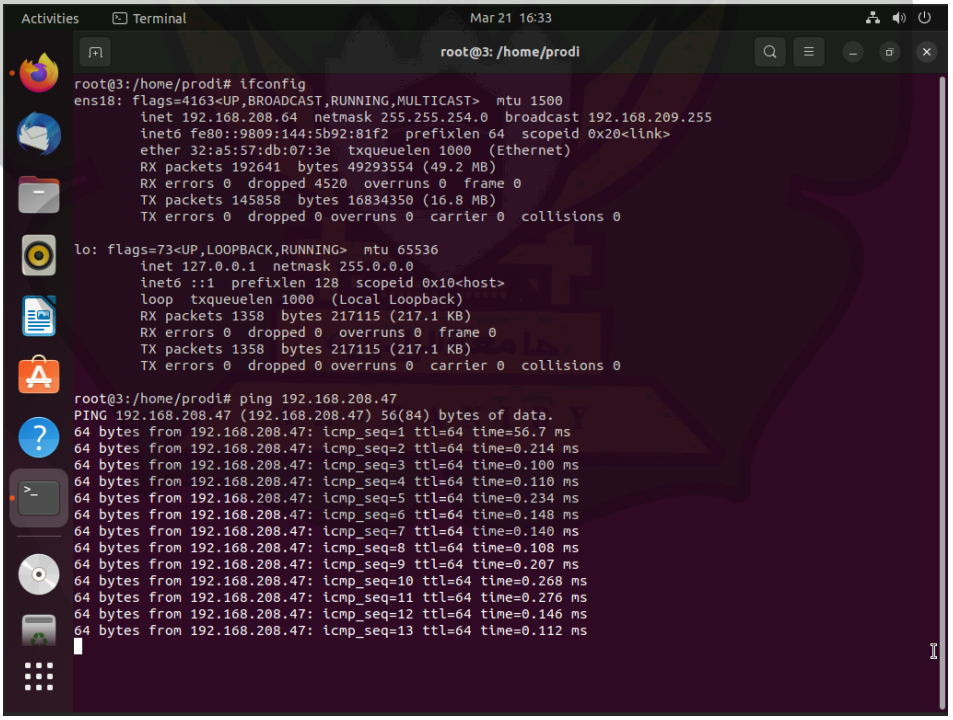
Pada gambar 4.21 menampilkan halaman konfirmasi kembali yang sudah di setting sebelumnya, berguna untuk pengecekan ulang agar tidak ada kesalahan pada saat penginstalan berlangsung, jika sudah sesuai maka klik *Finish* unutk menyelesaikan settingan dan selanjutnya install Ubuntu seperti biasa.

3. Pengujian *Virtual Machine* (VM)

Setelah melakukan penginstalan VM kemudian dilanjutkan dengan pengujian jaringan antar setiap VM agar dapat mengetahui bahwa setiap VM saling terhubung satu sama lain. Pengujian di lakukan dengan cara mencoba Ping ip dari VM ke VM yang lainnya gambar 4.2 menampilkan uji coba Ping.




Gambar 4.22 IP Dari Ubuntu Prodi 192.168.208.47



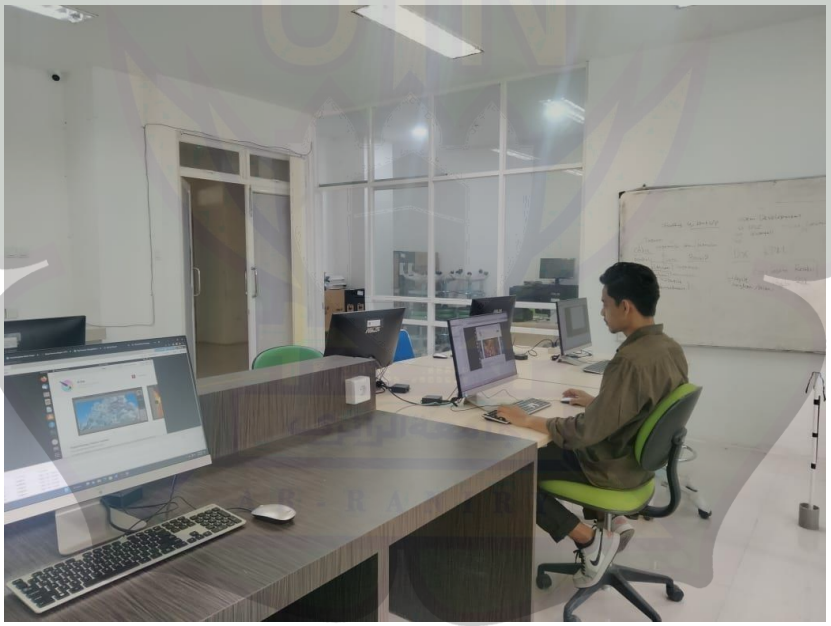

Gambar 4.23 Percobaan Ping Ke IP 192.168.208.47

Hasil dari pengujian Ping IP antar VM dapat dikatakan berhasil terlihat pada gambar 4.23 yang menampilkan ping ip dari gambar 4.22, fungsi dari ping ip antar VM berguna untuk mengetahui jaringan pada VM yang berbeda dapat berkomunikasi satu sama lain.

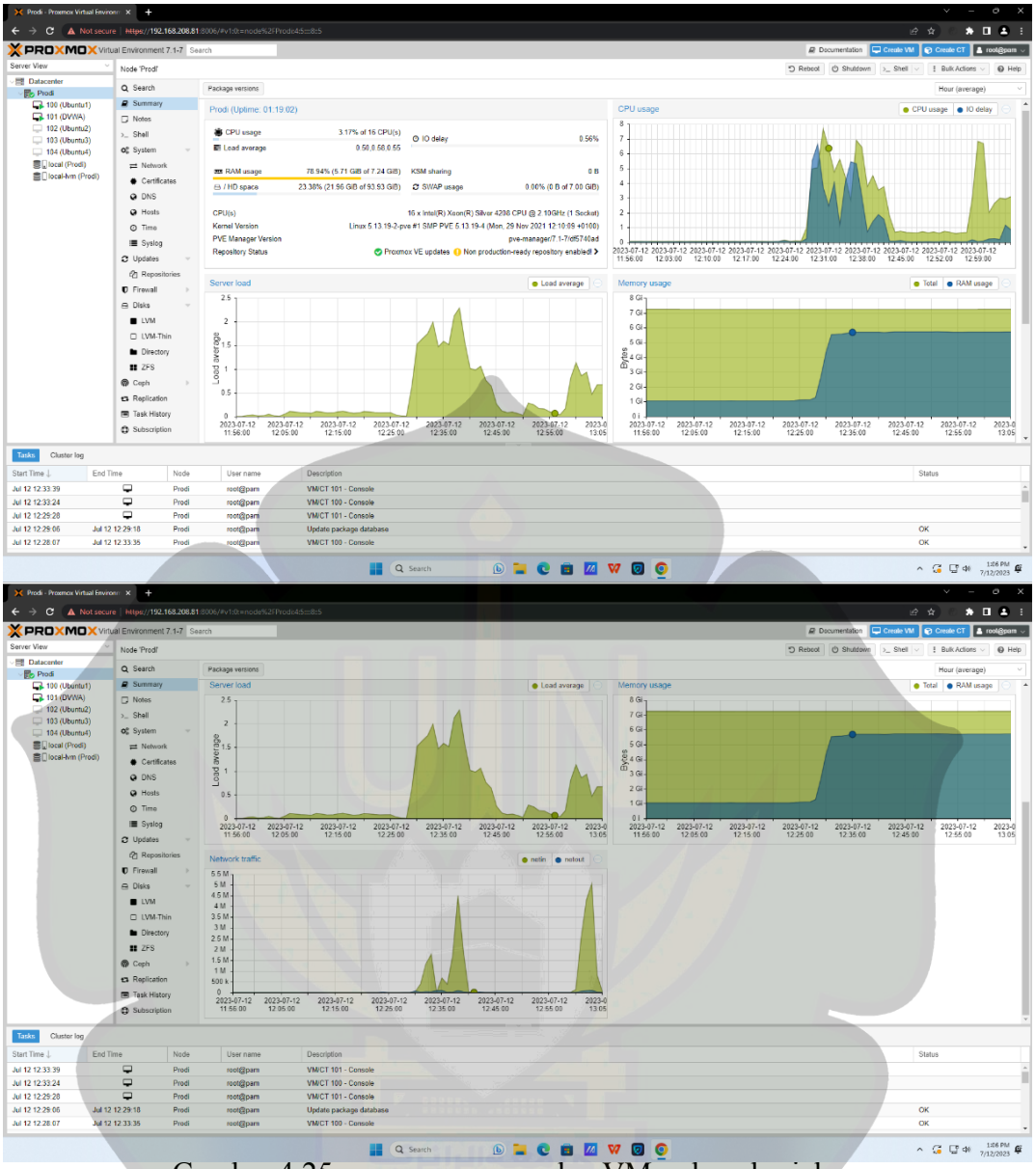
4. Pengujian kinerja *server*

Pengujian kinerja server bertujuan untuk mengetahui apakah server dapat menjalankan lima VM yang sedang menjalankan aplikasi Visual Studio Code secara bertahap. Tujuan lainnya adalah unutk mengetahui bahwa laboratorium cybersecurity virtual tidak hanya di gunakan untuk kebutuhan praktikum cybersecurity saja, akan tetapi dapat gunakan untuk mata kuliah lainnya contohnya seperti mata kuliah pemograman, *Big Data,* desain grafis dan lain-lain.

Pada tahapan ini dilakukan pengujian server secara bertahap, mulai dari dua VM terlebih dahulu lalu dilanjutkan dengan menghidupkan VM lainnya.

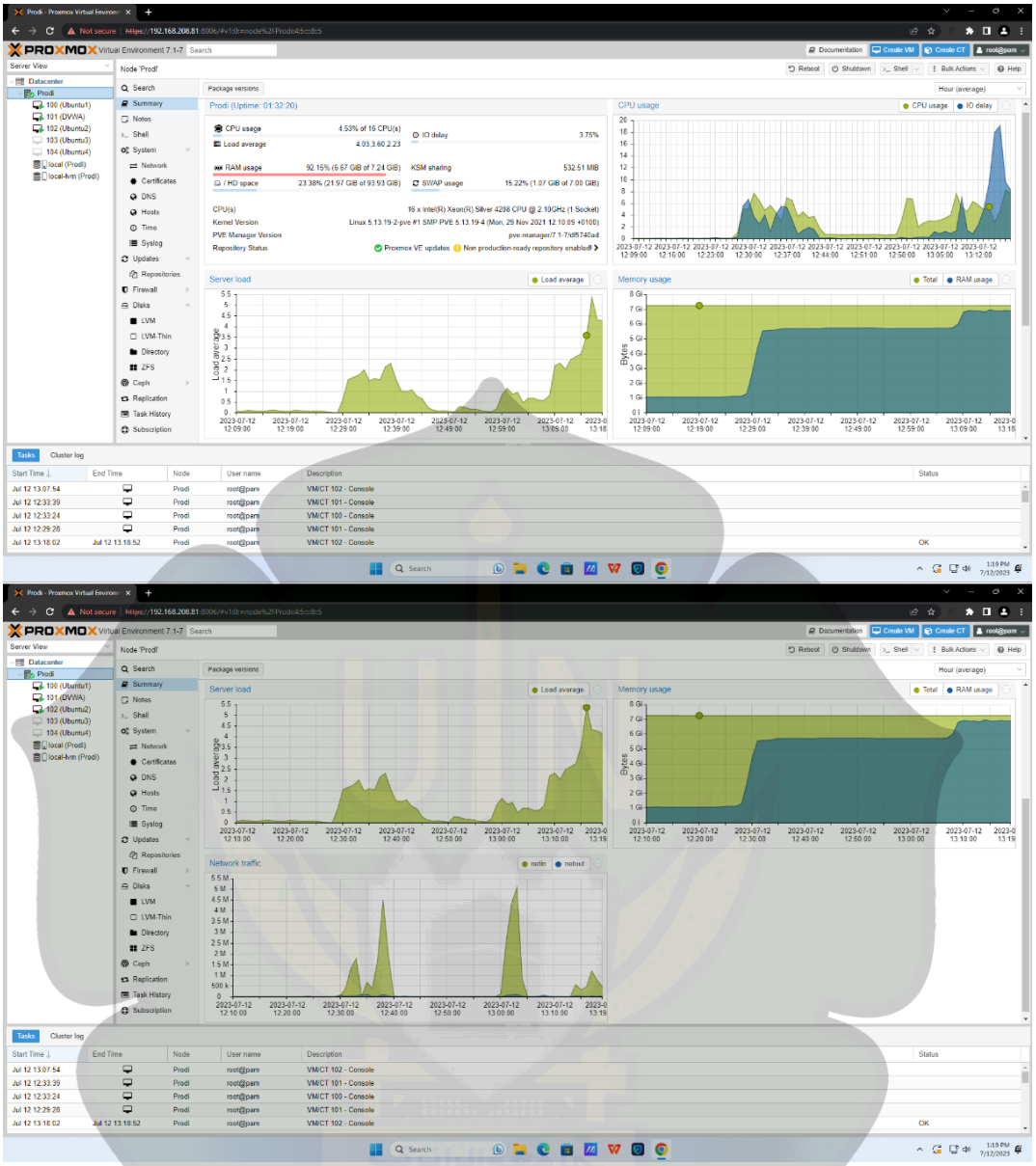


Gambar 4.24 Sedang Melakukan Pengujian



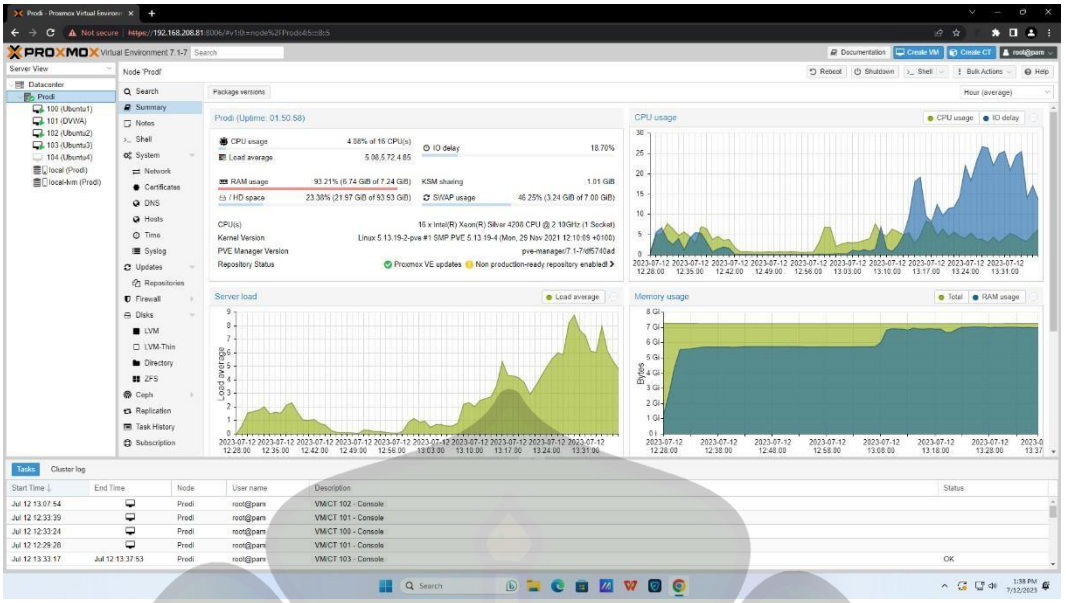
Gambar 4.25 *resources* server dua VM sedang berjalan

Gambar 4.25 menampilkan resources server yang digunakan oleh dua VM yang sedang berjalan, tampak server masih mampu unutk menjalankan dua VM tersebut.



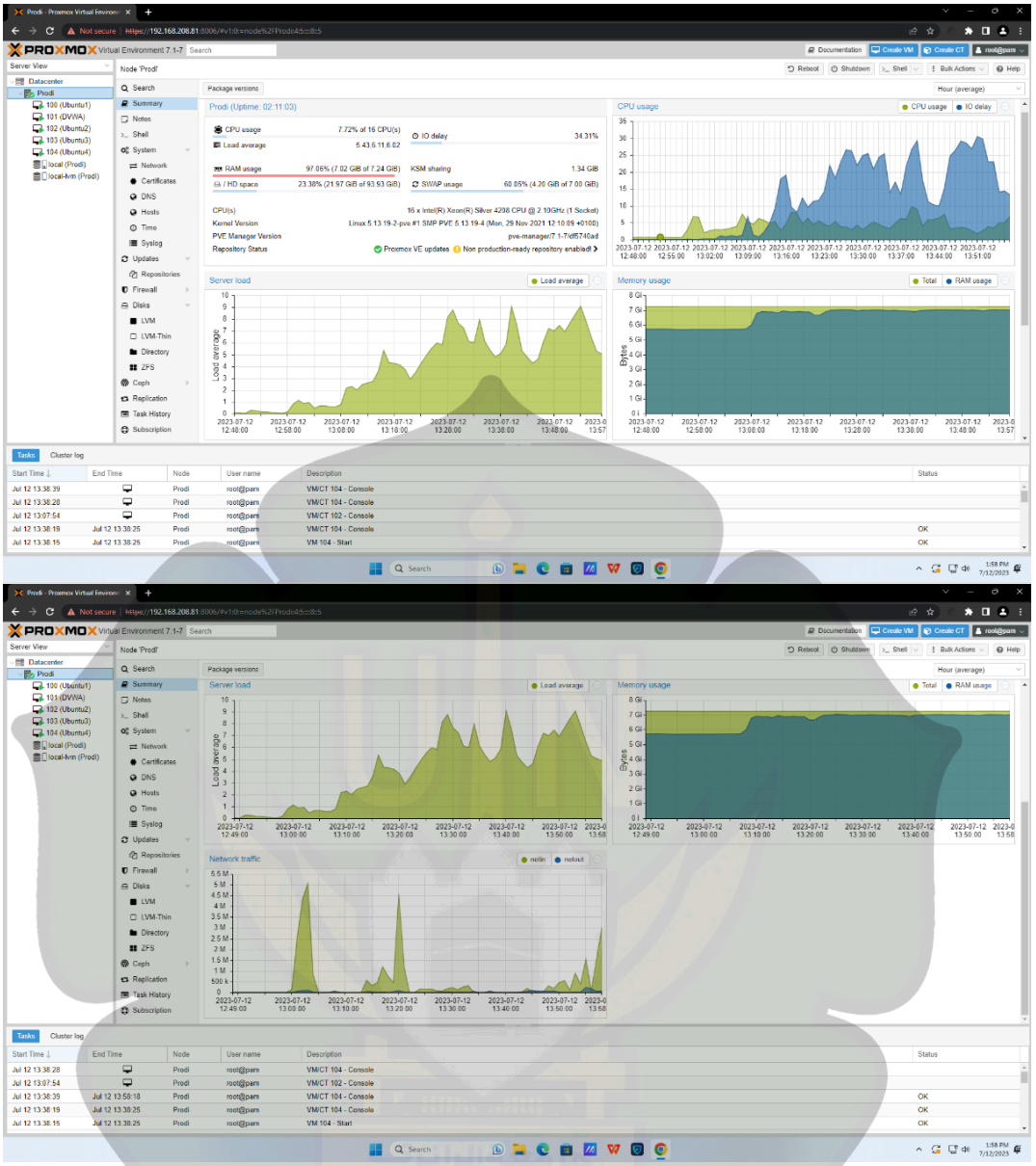
Gambar 4.26 *resources* server tiga VM sedang berjalan

Gambar 4.26 menampilkan *resources* server yang sedang digunakan unutk menjalankan tiga VM, pada tahap ini tampak RAM server mengalami peningkatan penggunaan.



Gambar 4.27 *resources* server empat VM sedang berjalan

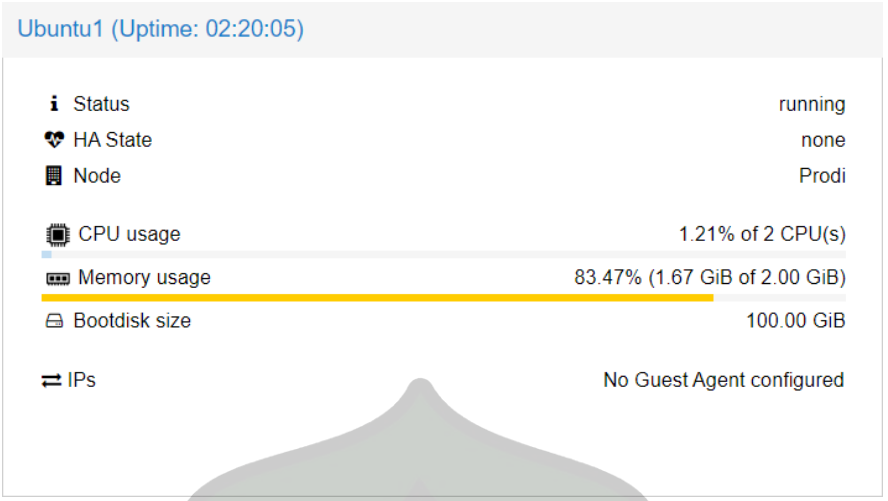
Gambar 4.27 menampilkan *resources* server yang digunakan untuk menjalankan empat VM, tampak input dan output delay meningkat yang sebelumnya hanya 3,75% saat menjalankan empat VM menjadi 18,70% efekny penggunaan VM agak melambat.



Gambar 4.28 *resources* server lima VM sedang berjalan

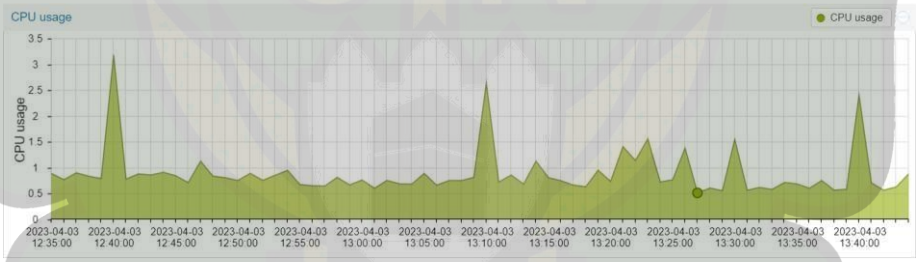
Gambar 4.28 menampilkan *resources* server yang digunakan untuk menjalankan lima VM, tampak input dan output delay meningkat dari tiga VM hanya 3,75% saat menjalankan empat VM menjadi 18,70% dan Ketika VM ke lima di hidupkan peningkatan lebih signifikan mencapai 34,31% menyebabkan penggunaan VM yang digunakan melambat.

Sedangkan untuk pemakaian pervirtual machine ditampilkan pada gambar berikut :



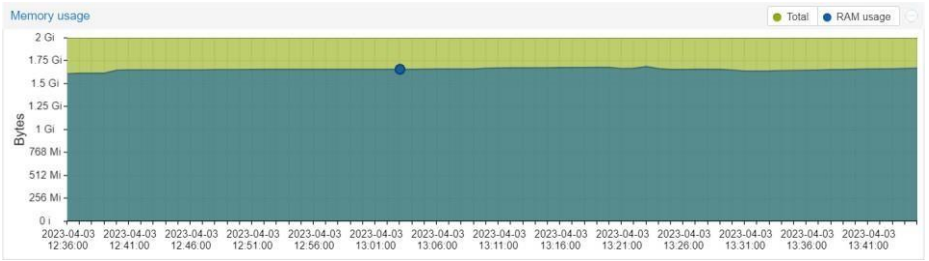

Gambar 4.29 Tampilan Penggunaan Resource Pada Salah Satu VM

Pada gambar di atas menampilkan penggunaan RAM pada VM hingga 83,47% penyebab penggunaan RAM meningkat disebabkan proses penginstalan aplikasi sedang berjalan.



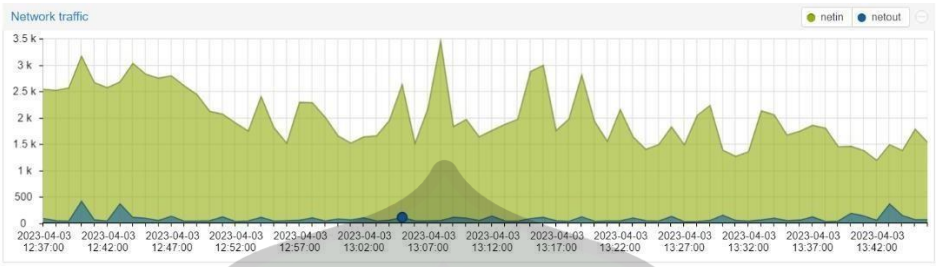

Gambar 4.30 Penggunaan CPU Pada Salah Satu VM

Pada gambar 4.30 tampak menampilkan grafik CPU yang di gunakan VM ada yang melonjak naik dan turun, saat grafik melonjak naik adanya proses instalasi yang sedang berjalan awal dari proses isntall berjalan maka grafik akan naik dan setelahnya akan normal dan sesekali akan naik jika prosesnya agak berat.



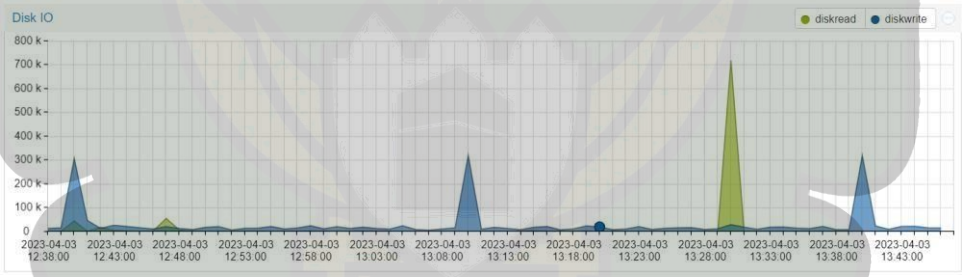

Gambar 4.31 Penggunaan Memori Pada Salah Satu VM

Pada gambar 4.31 menampilkan grafik ram yang digunakan pada VM pada grafik yang berwarna hijau menampilkan total RAM sedangkan yang berwarna biru RAM yang sedang digunakan, nampak pada grafik RAM terlihat normal.




Gambar 4.32 Lalu Lintas Jaringan

Pada gambar 4.32 menampilkan *network traffic* yang dimana nampak grafik yang naik turun disebabkan karena banyaknya data yang diterima sehinga membuat grafik tidak menentu.




Gambar 4.33 Disk Input dan Output

Pada gambar 4.33 menampilkan dua grafik yang memiliki warna yang berbeda pada grafik biru menampilkan *DiskWrite* adalah perintah atau operasi pada sistem operasi komputer yang digunakan untuk menulis data ke hard disk atau media penyimpanan lainnya. Sedangkan grafik hijau *DiskRead* adalah perintah atau operasi pada sistem operasi komputer yang digunakan untuk membaca data dari hard disk atau media penyimpanan lainnya.

## IV.3 Praktikum DDOS

Praktikum DDoS adalah kegiatan belajar yang dilakukan untuk mempelajari dan memahami bagaimana serangan DDoS dilakukan, bagaimana cara

mencegahnya, serta bagaimana cara memperkuat keamanan jaringan. Kegiatan ini melibatkan penggunaan perangkat lunak atau tools tertentu untuk melakukan serangan simulasi pada sistem target, dengan tujuan membantu orang memahami bagaimana cara melakukan serangan DDoS secara simulasi dan menguji keamanan jaringan mereka sendiri. Namun, perlu diingat bahwa praktikum DDoS hanya boleh dilakukan dengan izin dan pengawasan yang tepat dari pihak yang berwenang, dan melakukan serangan DDoS secara ilegal dapat mengakibatkan kerugian yang signifikan bagi korban serta melanggar undang-undang keamanan siber.

Praktikum kali ini menggunakan dua VM yang sudah ada pada laboratorium *cybersecurity* vitual dan menggunakan satu laptop. VM pertama digunakan unutk menjadi server dari web apache, sedangkan VM kedua sebagai penyerang menggunakan DDOS dan laptop digunakan untuk mengakses webiste apache. berikut langkah-langkah yang harus di lakukan:

1. Instalasi Apache

Apache merupakan software web server yang memungkinkan user untuk mengupload website di internet. Software ini gratis dan bersifat *open source* sehingga dapat digunakan bebas bahkan untuk kepentingan umum seperti bisnis, pembelajaran dan lainnya. Apache berfungsi sebagai penghubung antara server dan browser (seperti Google Chrome, Firefox, dll).

Software dengan nama resmi Apache HTTP Server ini pertama kali dirilis pada tahun 1995 oleh Apache Software Foundation. Apache merupakan *software* lintas *platform* sehingga dapat berfungsi dengan baik di server Unix dan server Windows. Beberapa kelebihan Apache dibanding software web server lain yaitu kemudahan konfigurasi, fleksibel karena memiliki struktur berbasis modul, stabil, dan sistem keamanan yang terus diperbarui. Namun Apache dapat mengalami gangguan performa jika suatu website menerima traffic dengan jumlah yang tinggi.

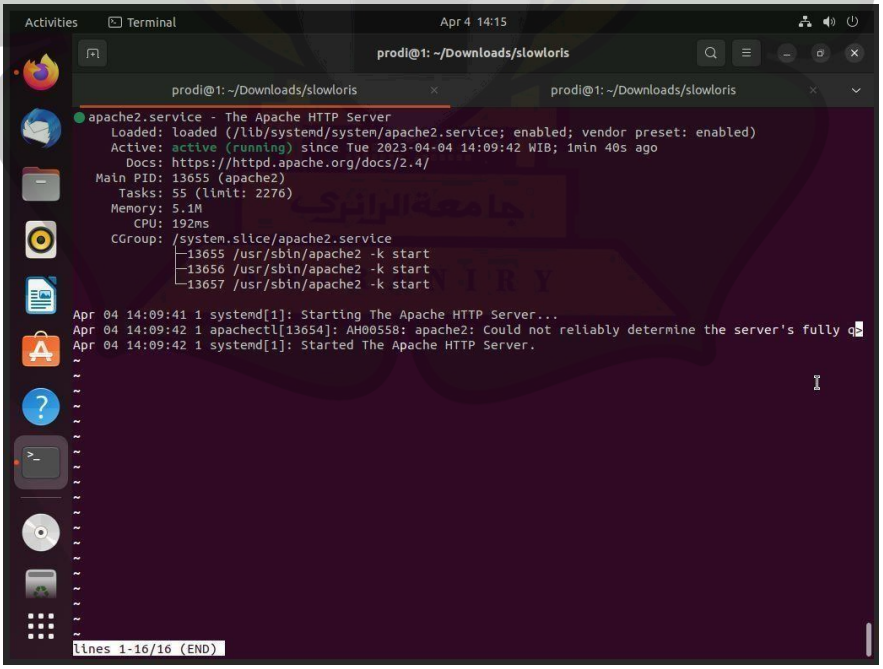
Salah satu penyebab meningkatnya traffic pada server Apache karena adanya penyerangan pada server. Slowloris adalah jenis serangan DDoS pada lapisan aplikasi yang menggunakan permintaan HTTP parsial untuk membuka koneksi antara satu komputer dan server Web yang ditargetkan, kemudian menjaga koneksi tersebut tetap terbuka selama mungkin, sehingga membebani dan memperlambat kinerja target (Netscout, 2020). Singkatnya Slowloris akan terus menerus mengirim

permintaan http dalam jumlah besar yang berakibat pada menurunnya performa server dan website menjadi error.

Pada modul ini akan dijabarkan langkah-langkah mulai dari instalasi Apache, instalasi slowloris, dan cara penyerangannya pada server Apache. Praktikum ini menggunakan tiga komputer yang sudah diinstalasi Ubuntu, komputer satu digunakan untuk instalasi Apache, komputer dua untuk akses website Apache, dan komputer tiga untuk akses slowloris. Sebelum lanjut ke tahap instalasi, perlu diketahui bahwa praktikum ini tidak untuk ditiru dan hanya digunakan sebagai bahan penelitian.

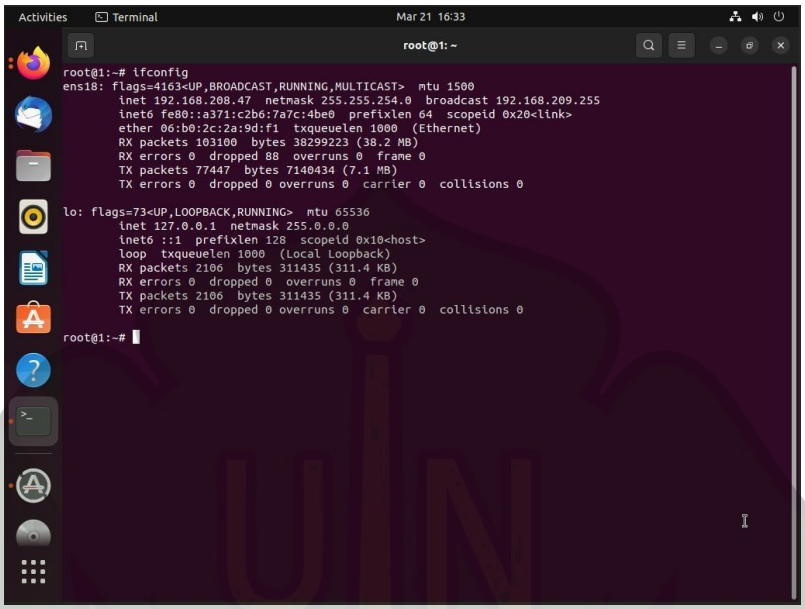
Berikut langkah-langkah instalasi Apache yang dilakukan pada komputer satu. Pertama, buka terminal di Ubuntu, ketik perintah *sudo apt install apache2,* masukkan sandi lalu *enter*. Tunggu sampai proses instalasi selesai.

Setelah proses instalasi selesai, ketik perintah *sudo systemctl start apache2* untuk memulai menghidupkan Apache kemudian enter. Untuk memastikan status Apache sudah aktif, ketik perintah *sudo systemctl status apache2,* lalu *enter*. Jika statusnya adalah "*active (running)*", maka Apache sudah aktif. Lebih jelasnya dapat dilihat pada gambar 4.34 dibawah ini.




Gambar 4.34 Status Apache Aktif

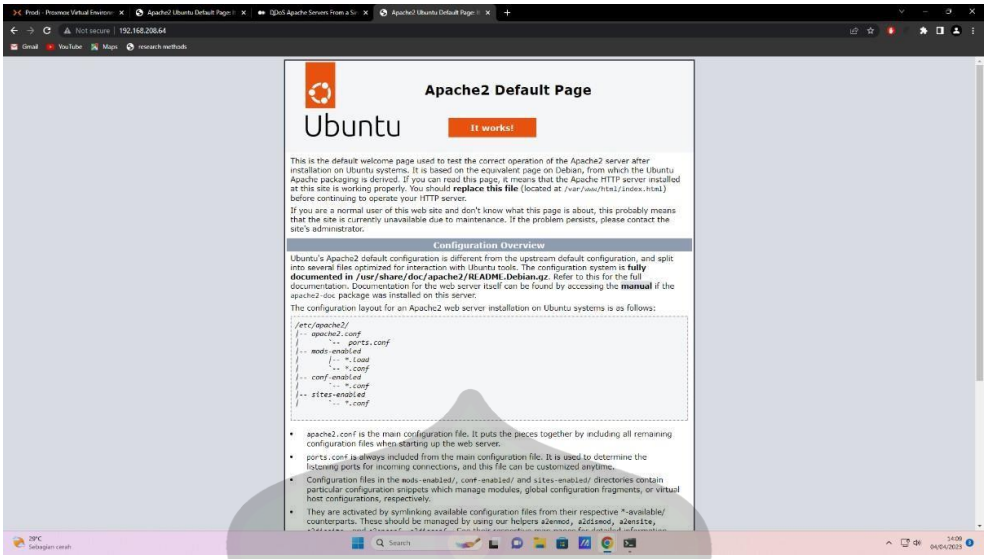
Setelah melakukan cek status, ketik *ifconfig* pada terminal kemudian klik enter. Perintah ini bertujuan untuk mendapatkan ip pada komputer satu dan selanjutnya akan digunakan saat melakukan akses web Apache pada komputer dua.




Gambar 4.35 IP komputer Satu yang Digunakan Untuk Web Apache

2. Akses Web Apache

Pada komputer dua untuk mengakses web server Apache. Lakukan pencarian menggunakan ip 192.168.208.72 yang sudah diperoleh pada langkah sebelumnya menggunakan browser. Gambar dibawah merupakan tampilan website Apache yang berhasil di akses menggunakan komputer ke dua.

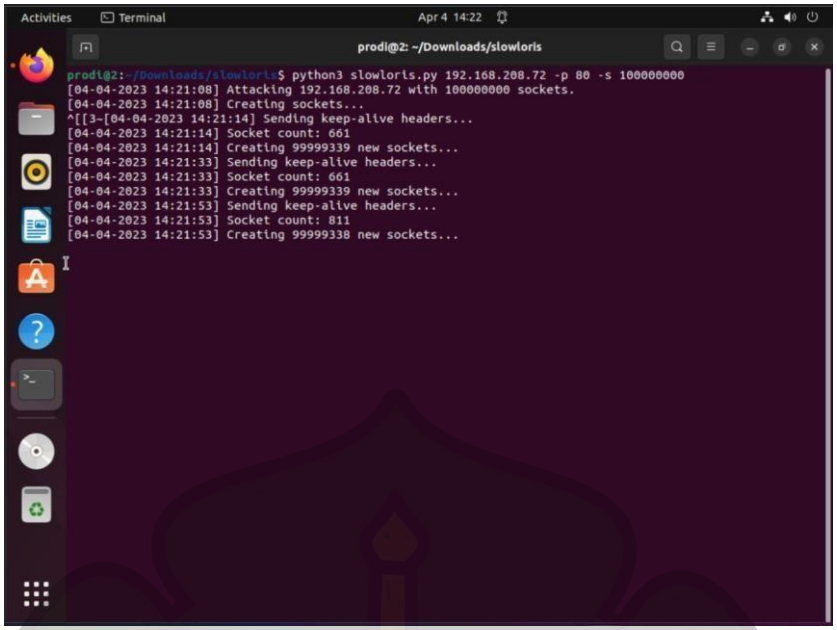



Gambar 4.36 Tampilan Web Default Apache

3. Instalasi dan penyerangan slowloris

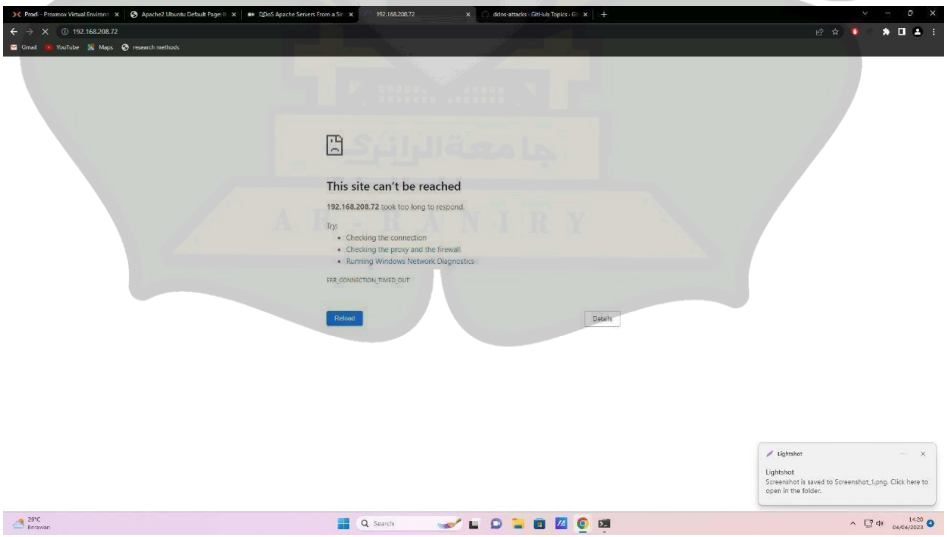
Proses instalasi slowloris dilakukan pada komputer tiga. Pertama, buka terminal pada Ubuntu lalu ketik *git clone* https://github.com/gkbrk/slowloris.git, kemudian enter. Tunggu hingga proses download selesai.

Kedua, ketik perintah *cd/Downloads/slowloris* untuk masuk ke direktori slowloris, lalu enter. Setelah masuk ke direktori Slowloris, ketik perintah *python3 slowloris.py 192.168.208.72 -p 80 -s 100000000,* lalu enter. Pada tahap ini DDOS menyerang server komputer satu dengan mengirim 100000000 permintaan secara terus menerus seperti terlihat pada gambar dibawah.




Gambar 4.37 Tampilan Proses Penyerangan DDOS

Akibat dari penyerangan ini server menjadi lambat dan website susah untuk di akses. Hasilnya, pada komputer dua yang digunakan untuk akses website Apache mengalami *error* akibat banyaknya permintaan yang masuk dalam waktu yang bersamaan. Gambar dibawah memperlihatkan tampilan website setelah dilakukan penyerangan DDOS.




Gambar 4.38 Tampilan Website Saat Terkena DDOS

# KESIMPULAN DAN SARAN

## V.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan beberapa hal sebagai berikut:

1. Pembuatan laboratorium *cybersecurity* virtual menggunakan proxmox VE pada *server* Prodi Teknologi Informasi menggunakan metode NDCL yang meliputi tahapan sebagai berikut :
   a. Analisis
   b. Desain
   c. Implementasi
   d. Monitoring
2. Hasil yang diperoleh saat melakukan uji ketahanan *server* pada laboratorium *cybersecurity* virtual dengan menjalankan lima VM secara bersamaan, ada beberapa kendala yaitu :
   a. Terjadi delay sebanyak 6,14% saat digunakan VM unutk menginstall aplikasi secara bersamaan.
   b. Pengunaan RAM meningkat.
   c. *Swap usage* meningkat hingga 54,90%
3. Dari praktikum DDOS yang dilakukan pada laboratorium *cybersecurity* virtual memiliki hasil yang bagus, yaitu praktikum berjalan sesuai yang diharapkan.

Dengan demikian laboratorium *cybersecurity* virtual dapat digunakan oleh mahasiswa TI untuk keperluan praktikum berguna untuk membuat mahasiswa TI dapat lebih berkembang dan memiliki wadah untuk berkreasi dalam bidang TI.

## V.2 Saran

Berdasarkan kesimpulan yang telah di uraikan maka berikut adalah beberapa saran pada penelitian ini :

1. RAM pada *server* Prodi TI dapat di-*upgrade* berguna untuk memaksimalkan kinerja *server* dalam menjalankan lima VM secara bersamaan.
2. Laboratorium *cybersecurity* virtual dapat dikembangkan lagi sesuai kebutuhan kedepannya.

جامعة الرانري
AR-RANIRY

# DAFTAR PUSTAKA


Abdurrahman, Soni, & Hafid, A. (2019). Optimalisasi Sumber Daya Komputer Dengan Virtualisasi *Server* Menggunakan Proxmox Ve. *Jurnal Fasilkom*, *9*(2), 369–376.

Anam, M. K., Sudyana, D., Noviciatie, A., & Lizarti, N. (2020). Optimalisasi Penggunaan VirtualBox Sebagai Virtual Computer Laboratory untuk Simulasi Jaringan dan Praktikum pada SMK Taruna Mandiri Pekanbaru. *Http://Jurnal.Sar.Ac.Id/Index.Php/J-PEMAS Optimal*, *vol 1*(2), 37–44.

Bonok, Z., Dako, R. D. R., & Lakoro, F. (2022). Merancang Praktikum Teknik Telekomunikasi Dasar melalui Laboratorium Virtual yang Memanfaatkan TIK. *Jambura Journal of Electrical and Electronics Engineering*, *4*(1), 38–41. https://doi.org/10.37905/jjeee.v4i1.10612

Kurniawan, R. (2016). Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode NDLC (Network Development Life Cycle) Pada BPU Bagas Raya Lubuk Linggau. *Jurnal Ilmiah Betrik*, *7*(01), 50–59. https://doi.org/10.36050/betrik.v7i01.12

Moldovan, A. N., & Ghergulescu, I. (2020). Leveraging Virtual Labs for Personalised Group-based Assessment in a Postgraduate Network Security and Penetration Testing Module. *SMAP 2020 - 15th International Workshop on Semantic and Social Media Adaptation and Personalization*. https://doi.org/10.1109/SMAP49528.2020.9248457

Muhajarah, K., & Sulthon, M. (2020). Pengembangan Laboratorium Virtual sebagai Media Pembelajaran: Peluang dan Tantangan. *Justek : Jurnal Sains Dan Teknologi*, *3*(2), 77. https://doi.org/10.31764/justek.v3i2.3553

Robles-Gómez, A., Tobarra, L., Pastor-Vargas, R., Hernández, R., & Cano, J. (2020). Emulating and evaluating virtual remote laboratories for cybersecurity. *Sensors (Switzerland)*, *20*(11), 1–22. https://doi.org/10.3390/s20113011

Semarang, P. N. (2014). *Implementasi Virtualisasi dan Server Cloud*.

Setiawan, F. M. B. (2019). Analisis Cybersecurity pada Bukalapak dan Tokopedia terhadap keamanan bertransaksi. *UNPAR Institutional Repository*, *1789*. http://repository.unpar.ac.id/bitstream/handle/123456789/7903/Bab5 - Daftar Pustaka - 1314014sc-p.pdf?sequence=3&isAllowed=y

Uramová, J., Segeč, P., Papán, J., Brídová, I., Ilmu, F., & Zilina, U. (2021). *Manajemen Insiden Keamanan Siber di Lab Virtual*. 3–12.

## RIWAYAT HIDUP

Miskatur Rahman dilahirkan di Banda Aceh Provinsi Aceh pada tanggal 26 Agustus 2000, anak ketiga dari tujuh bersaudara pasangan dari Syamsul Rizal dan Afniar. Penulis menyelesaikan Pendidikan di sekolah Dasar di MIN TELADAN Banda Aceh dengan lulus pada tahun 2012, kemudian melanjutkan pendidikan di jenjang Sekolah Menengah Pertama di SMP Islam YPUI Banda Aceh yaitu di Darul 'ulum dengan lulus pada tahun 2015. Kemudian melanjutkan Pendidikan di MAN 2 Banda Aceh dengan lulus pada tahun 2018. Pada tahun 2018 penulis melanjutkan Strata-1 (S1) di perguruan Tinggi Negeri, tepatnya di Universitas Islam Negeri Ar-Raniry Fakultas Sains dan Teknologi pada Program Studi Teknologi Informasi.