BAB III

PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Selama menjalani program magang, penulis menempati posisi sebagai OT (*Operational Technology) Module Adoption Intern.* Penulis berada di bawah supervisi langsung Bapak Hedi Santoso selaku *Head of Design Firms* dalam melaksanakan tugas. Seluruh proses kerja magang, mulai dari perencanaan hingga implementasi dilakukan melalui koordinasi dan pengawasan beliau. Struktur alur kerja serta mekanisme koordinasi selama magang dapat dilihat pada gambar berikut.

Supervisor memberikan dokumen modul *cybersecurity* yang masih dalam versi Eropa dan juga alat simulasi yang akan digunakan untuk pelatihan. Kemudian, *supervisor* memberi pekerjaan penulis untuk mempelajari dokumen tersebut agar dapat memahami dan mengerti apa yang harus dilakukan. Penulis mempelajari dokumen tersebut dan mempelajari cara mengadaptasinya ke versi lokal. Selain dokumen, simulasi secara langsung juga dilakukan untuk memahami lebih baik operasi alat yang digunakan. Penulis memberikan laporan kepada *supervisor* secara rutin untuk perbaikan dan juga perkembangan. Selama proses magang, penulis juga terhubung dengan karyawan lain di bidang bidang yang memerlukan *expert* seperti penggunaan aplikasi dan juga *firewall* yang berbeda dengan dokumen yang diberikan.

3.2 Tugas dan Uraian Kerja Magang

3.3.1. Tugas Kerja Magang

Selama menjalani program magang, penulis bertanggung jawab untuk mengadopsi modul pelatihan *Operational Technology (OT) Cybersecurity* ke dalam versi Indonesia. Proses adaptasi tidak hanya mencakup penerjemahan materi, tetapi juga pemahaman teknis terhadap komponen-komponen yang digunakan dalam modul, seperti PLC, HMI, *firewall, managed switch, variable speed drive,* motor, serta perangkat BME NOC 0321 untuk

segmentasi jaringan. Penulis juga mempelajari cara konfigurasi dan koneksi antar perangkat serta integrasi dengan PC, guna memastikan simulasi berjalan sesuai dengan skenario pelatihan. Modul ini dirancang untuk memberikan pemahaman praktis mengenai kemanan siber di lingkungan OT, khususnya dalam konteks industri yang menggunakan sistem otomasi. Penulis juga menyoroti potensi vektor serangan yang umum terjadi di lingkungan OT, seperti akses jaringan tamu (*guest wifi*) yang memungkinkan pengguna melakukan pemindaian jaringan untuk menemukan IP *address* perangkat kritis, penggunaan media fisik seperti USB yang berpotensi membawa *malware* atau virus ke sistem kontrol, serta ruangan *server* atau kontrol yang tidak diawasi sehingga dapat dimanfaatkan pelaku untuk memasang perangkat berbahaya atau mengakses langsung ke sistem.

Salah satu bagian penting dari tugas saya adalah melakukan simulasi serangan siber terhadap sistem OT yang telah dikonfigurasi. Penulis berhasil menunjukkan bagaimana sebuah serangan yang berhasil menembus jaringan dapat menyebabkan motor industri berputar secara acak tanpa perintah operator. Skenario ini menggambarkan potensi ancaman nyata terhadap sistem otomasi jika tidak dilindungi dengan baik. Simulasi ini menjadi sorotan utama dalam laporan penulis karena menunjukan dampak langsung dari kelemahan keamanan jaringan OT, sekaligus memperkuat urgensi penerapan praktik keamanan siber yang tepat dalam lingkungan industri.

3.3.2. Uraian Kerja Magang

3.3.2.1. Pendahuluan OT *Cybersecurity*

Cybersecurity merupakan disiplin yang mempelajari dan menerapkan mekanisme untuk menjaga keandalan dan kepercayaan dalam sistem digital. Secara konseptual, *cybersecurity* berfungsi sebagai upaya perlindungan terhadap penyalahgunaan, pengambilalihan, manipulasi, maupun gangguan yang dapat menghambat fungsi normal suatu sistem. Disiplin ini muncul dari kebutuhan dasar untuk memastikan bahwa interaksi, pemrosesan informasi, dan pengambilan keputusan berbasis teknologi berlangsung secara aman.

Cybersecurity dipahami sebagai proses pengelolaan risiko baik yang berasal dari kesalahan manusia, kegagalan sistem, maupun ancaman eksternal dengan tujuan menjaga stabilitas dan keandalan proses digital. Hal ini membuat *cybersecurity* tidak hanya berfokus pada penggunaan teknologi pertahanan, tetapi juga melibatkan pendekatan strategis, kebijakan, serta praktik operasional yang dirancang untuk mempertahankan ketahanan sistem terhadap berbagai bentuk ancaman.

Operational Technology (OT) adalah sistem dan perangkat keras yang digunakan untuk memantau, mengontrol, dan mengotomasi proses fisik dalam lingkungan industri.[3] OT mencakup berbagai komponen seperti *Programmable Logic Controller* (PLC), *Human Machine Interface* (HMI), sensor, aktuator, motor dan perangkat lainnya yang berfungsi untuk menjalankan proses produksi secara efisien dan aman. Sistem OT bekerja secara langsung dengan peralatan fisik dan sering kali beroperasi secara *real-time* untuk memastikan kelancaran proses industri seperti bahan pengolahan, pengemasan, dan pengendalian mesin.

Berbeda dengan *Information Technology* (IT) yang berfokus pada pengelolaan data dan komunikasi digital, *Operational Technology* (OT) lebih menekankan pada keandalan dan kontinuitas proses fisik. OT digunakan di berbagai sektor seperti manufaktur, energi, transportasi, dan utilitas. Peranan OT krusial dalam menjaga operasional industri sehingga sistem OT harus dirancang dengan tingkat kestabilan dan keamanan yang tinggi, terutama dalam menghadapi tantangan masa kini seperti integrasi dengan jaringan IT dan potensi ancaman siber.

Tabel 3.1 Perbedaan IT & OT

Aspek	***Operational Technology* (OT)**	***Information Technology* (IT)**
Fokus	Ketersediaan & Keamanan	Kerahasiaan & Integritas
Lingkungan Kerja	Industri (Pabrik, Lapangan)	Korporat (Kantor, *Data Center*)
Perangkat	PLC, Sensor, Aktuator	*Server*, Laptop, *Router*

Resiko	Kerusakan Fisik, Bahaya Keamanan	Pelanggaran terhadap Data, Kerugian Finansial

Gambar 3.1 Tingkat Prioritas antara IT dan OT berdasarkan CIA Triad

Tabel 1 dan gambar 1 menunjukkan perbedaan IT dan OT dalam berbagai aspek serta tingkat prioritasnya. Sistem OT memprioritaskan keamanan dan ketersediaan sedangkan IT memprioritaskan kerahasiaan. Ketersediaan dan keamanan penting karena jika sistem industri tidak berjalan dengan baik maka perusahaan akan mengalami kerugian dan keamanan dari pekerja pabrik juga terancam.

Seiring meningkatnya konektivitas antara jaringan IT dan sistem kontrol industri, risiko serangan siber dalam lingkungan OT juga semakin meningkat. OT *cybersecurity* berfokus pada perlindungan perangkat yang mengendalikan proses fisik dari ancaman digital yang dapat mengganggu operasi, merusak perangkat, atau membahayakan keselamatan.

Purdue Enterprise Reference Architecture (PERA) atau Purdue Model menjadi acuan penting dalam memahami arsitektur sistem OT. Model ini membagi sistem industri ke berbagai level:

- Level 0 dan 1 mencakup sensor, aktuator, serta PLC yang menjalankan kontrol langsung terhadap proses fisik.
- Level 2 berisi sistem SCADA dan HMI yang memantau operasi secara *real time.*
- Level 3 mencakup sistem menajemen operasi seperti *Manufacturing Execution Systems* (MES)

- Level 3.5 yaitu zona DMZ (*Demilitarized Zone*) yang merupakan zona jaringan perantara yang memisahkan IT dan OT untuk mencegah akses langsung. Area ini menjadi tempat server perantara sehingga serangan dari IT tidak bisa langsung mencapai sistem kontrol industri.
- Level 4 merupakan domain OT yang berupa ERP dan aplikasi IT lainnya. Seiring meningkatnya konektivitas antara sistem OT dan jaringan IT, ancaman terhadap keamanan sistem otomasi industri juga semakin kompleks.

Berdasarkan analisis Purdue Model, titik serangan yang paling rentan berada di dua lokasi utama. Pertama, zona level 3.5 atau DMZ yang menjadi perbatasan antara jaringan bisnis dan jaringan operasi. Zona ini sering menjadi pintu masuk karena adanya pertukaran data, *remote access* dan layanan *bridging* lainnya. Kedua, kerentanan signifikan berada di level 1 dan 2, yaitu sistem kontrol supevisi seperti PLC, SCADA dan HMI. Banyak perangkat ini masih menggunakan protokol industri tanpa enkripsi atau autentikasi yang kuat.

Serangan terhadap OT biasanya berfokus pada manipulasi proses fisik, bukan pencurian data. Serangan umum meliputi : manipulasi parameter proses, *denial of service,* penyusupan melalui protokol industri yang tidak aman, *Man in the Middle* dan *remote access* berbahaya melalui koneksi IT-OT.[4] Vektor serangan terhadap OT dapat dikategorikan sebagai :

1. Manusia : Vektor serangan yang paling sering terjadi dengan cara mengeksploitasi atau menargetkan individu. Contoh vektor ini adalah email *phising.*
2. Perangkat Lunak : Vektor yang biasanya memanfaatkan kerentanan dalam perangkat lunak, yang bisa ditemukan di berbagai level: perangkat lunak dasar, sistem operasi, bahkan *firmware.*
3. Jaringan : Vektor yang menargetkan protokol komunikasi dalam jaringan dan/atau mengeksploitasi konfigurasi jaringan. Salah satunya yang dapat terjadi adalah celah pada *firewall*.

4. Fisik : Vektor serangan yang dilakukan dari sisi fisik sistem. Contohnya adalah serangan dengan memasukkan USB secara fisik ke dalam mesin.

Serangan terhadap sistem OT dapat menyebabkan kerusakan fisik, gangguan operasional, bahkan membahayakan keselamatan manusia. Contoh nyata dari ancaman ini adalah kasus Stuxnet, *malware* yang berhasil merusak *centrifuge* di fasilitas nuklir Iran dengan memanipulasi kontrol PLC secara tersembunyi. Selain itu, terdapat juga serangan Triton yang menargetkan sistem pengaman industri. Kasus-kasus ini menunjukkan pentingnya penerapan OT *cybersecurity* untuk melindungi sistem kontrol industri yang semakin kompleks dan berbahaya.

Melihat berbagai kasus nyata serangan siber terhadap sistem industri, semakin jelas bahwa perlindungan terhadap *Operational Technology* bukan lagi pilihan, melainkan kebutuhan mendesak. OT *Cybersecurity* memiliki standar yang menjadi acuan utama dalam pengembangan dan penerapan keamanan siber di lingkungan industri. Standar yang digunakan adalah IEC 62443 yang memberikan kerangka kerja yang komprehensif untuk mengidentifikasi risiko, menetapkan kebijakan keamanan, dan menerapkan kontrol teknis yang sesuai. Standar ini mencakup berbagai aspek mulai dari arsitektur sistem, pengelolaan aset, hingga pengujian dan pemantauan keamanan. Salah satu aspek dalam IEC 62443 adalah *Security Level* (SL).

Tabel 3.2 *Security Level*

Level	Target	Kemampuan	Motivasi	Tujuan	Sumber Daya
4	Negara	Spesifik ke ICS	Tinggi	Canggih secara Strategi	Tim multidisiplin yang luas
3	Haktivis, Teroris	Spesifik ke ICS	Sedang	Canggih secara serangan	Sedang (Kelompok peretas)
2	Kejahatan Siber, *Hacker*	Generik	Rendah	Sederhana	Rendah (Individu yang terisolasi)
1	Pelanggaran Kebetulan atau Tidak Disengaja	Tidak ada Kemampuan	Kecelakaan	Tidak Disengaja	Individu

Konsep *defense in depth* juga menjadi aspek dalam penerapan kontrol keamanan di lingkungan OT. Prinsip ini menkankan bahwa keamanan tidak boleh bertumpu pada satu mekanisme pertahanan saja, tetapi harus dibangun berlapis lapis agar kegagalan di satu lapisan tidak langsung membuka celah bagi penyerang. Salah satu penerapan kunci dari *defense in depth* adalah *network segmentation,* yaitu pemisahan jaringan berdasarkan fungsi dan tingkat kritikalitas sehingga serangan ke satu segmen tidak menyebar ke seluruh sistem. Segmentasi ini umumnya dilakukan pada arsitektur berlapis seperti Purdue Model, penggunaan *firewall* industri, serta pembatasan akses antar zona.

Semua pendekatan diatas sejalan dengan tiga pilar utama *cybersecurity* yaitu manusia, proses dan teknologi. Manusia yang mengoperasikan OT harus mendapatkan pelatihan keamanan, budaya kepatuhan dan kesadaran terhadap ancaman. Proses mengacu pada kebijakan, prosedur operasional, standar, serta tata Kelola yang mengatur bagaimana keamanan diterapkan. Terakhir, teknologi mencakup seluruh perangkat keras, perangkat lunak dan mekanisme teknis yang digunakan untuk melindungi sistem dari ancaman siber.

3.3.2.2.Modul OT *Cybersecurity*

Modul ini dirancang untuk mensimulasikan arsitektur jaringan industri yang aman, serta mendemonstrasikan potensi serangan dan mekanisme perlindungan.

Gambar 3.2 Modul *Cybersecurity*

Modul ini memiliki komponen utama sebagai berikut :

- **PLC M580 (Schneider Electric)** : Sebagai pusat kontrol logika dalam sistem otomasi industri. PLC ini menjadi target utama dalam simulasi serangan dan proteksi. Unit ini mendukung enkripsi komunikasi dan pengaturan akses (FTP, HTTP, IP) serta dapat diintegrasikan dengan *firewall.*

- **HMI (*Human Machine Interface)*** : Menyediakan antarmuka visual bagi operator untuk memantau dan mengontrol proses. HMI dapat menjadi titik masuk serangan jika tidak diamankan, terutama melalui Web Gate atau *remote access*

- **BME NOC 0321** : Memisahkan jaringan antara PLC dan PC serta mengatur *routing* antar *subnet.* Unit ini dapat digunakan untuk segmentasi jaringan dan pengaturan jalur komunikasi yang aman antara VLAN.
- **Komunikasi CANopen** : Protokol komunikasi *fieldbus* untuk perangkat seperti VSD dan sensor.

- **VSD Altivar 320** : Mengatur kecepatan dan torsi motor sinkron berdasarkan sinyal dari PLC. VSD ini menjadi target serangan yang dapat menyebabkan gangguan fisik pada proses industri

- **Motor Sinkron** : Berfungsi sebagai aktuator fisik yang dikendalikan oleh VSD. Motor ini menunjukkan dampak nyata dari serangan siber terhadap perangkat fisik.

- **Managed Switch** : Mengelola lalu lintas jaringan dan mendukung VLAN untuk segmentasi. Unit ini memungkinkan pemisahan jaringan antara *engineering*, operasi, dan manajemen, serta pengaturan akses.

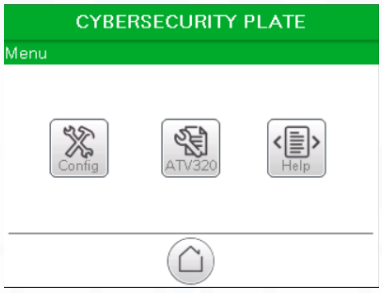
- ***Firewall* Fortinet FGR-60F** : Melindungi jaringan dari akses tidak sah dan serangan eksternal. Unit ini berfungsi untuk menyaring lalu lintas jaringan berdasarkan IP, *port,* dan protokol. *Firewall* digunakan untuk mendemonstrasikan pemblokiran serangan dan pembatasan akses ke PLC.

Modul ini mensimulasikan serangan siber seperti *sniffing*, *unauthorized access*, dan *injection.* Efektivitas segmentasi jaringan dan *firewall* dalam melindungi sistem OT juga ditunjukkan melalui modul ini. Tujuan modul ini adalah memberikan pemahaman praktis tentang arsitektur jaringan industri yang aman.

3.3.2.3. Cara Modul Bekerja pada Kondisi Normal

- Tampilan *speed drive control*

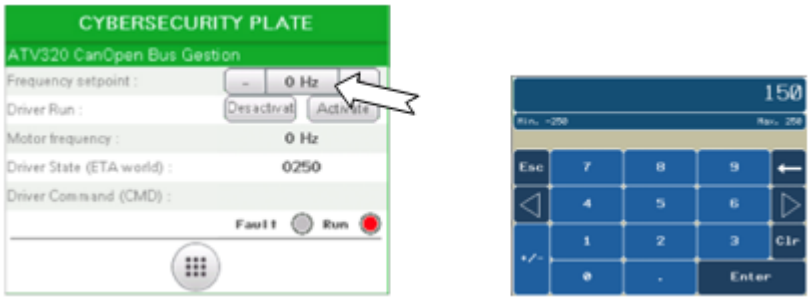
Gambar 3.3 Tampilan Awal HMI



Gambar 3.4 Tampilan Menu HMI

Gambar 3.5 Menu Pengaturan Kecepatan

- Ubah *setpoint* kecepatan



Gambar 3.6 Perubahan *Setpoint* Kecepatan

- Mulai motor dengan menekan tombol "*Activate"* dan pastikan motor berputar.

Gambar 3.7 Kondisi Motor Menyala

- Ubah nilai *setpoint* kecepatan dan periksa apakah kecepatan motor sesuai dengan *setpoint* tersebut. Motor dapat dihentikan dengan menekan tombol "*Deactivate",* lalu periksa apakah motor benar benar berhenti.

3.3.2.4. Simulasi Penyerangan terhadap Motor

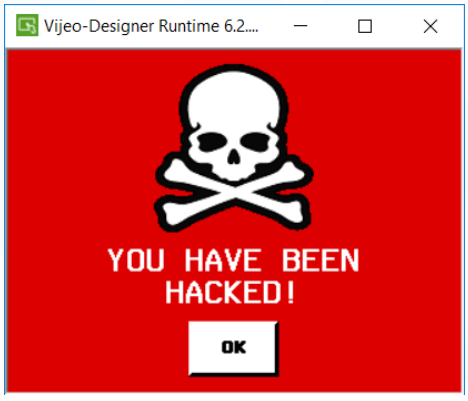
Simulasi yang dilakukan dalam laporan ini adalah simulasi pengiriman instruksi perubahan kecepatan motor ke PLC M580 melalui *firewall* yang termasuk ke dalam serangan dari vektor jaringan dan perangkat lunak. Hal ini dikarenakan serangan mendapatkan akses masuk melewati firewall dan juga menyalahgunakan fungsi logika PLC untuk menjalankan instruksi manipulatif.

Skenario serangan siber dilakukan terhadap sistem kontrol motor sinkron yang terhubung melalui VSD Altivar 320 dan dikendalikan oleh PLC M580. Tujuan dari simulasi adalah menunjukkan dampak nyata dari gangguan komunikasi akibat akses tidak sah ke sistem kontrol. Tahapan serangan dalam simulasi adalah sebagai berikut :

- Inisiasi akses : perangkat eksternal mencoba mengakses jaringan yang terhubung dengan PLC melalui *firewall*
- *Firewall* mengizinkan lalu lintas : karena tidak ada filter khusus, koneksi diizinkan masuk
- Pengiriman instruksi : perintah perubahan kecepatan motor dikirim ke PLC M580
- Eksekusi PLC : PLC menjalankan perintah tersebut tanpa autentikasi tambahan
- Perubahan fisik : kecepatan motor berubah secara tidak sah selama 30 detik yang menggambarkan manipulasi proses industri. Penyerang juga mengubah layar tampilan HMI menjadi "**YOU HAVE BEEN HACKED**"

```
C:\>python random_speed.py
Automate IP address ? (Default: 192.168.0.1)

Modbus Port ? (Default: 502)


[+] Connecting to 192.168.0.1:502...
[+] Connected to 192.168.0.1:502.
[+] Setting speed to 50...
[+] Speed set to 50.
[+] Setting screen to 100...
[+] Screen set to 100.
[+] Setting screen to 404...
[+] Screen set to 404.
[+] Starting speed controller...
[+] Speed controller started.
[+] Setting speed to 199...
[+] Speed set to 199.
[+] Setting speed to 27...
[+] Speed set to 27.
[+] Setting speed to 185...
[+] Speed set to 185.
[+] Setting speed to 64...
[+] Speed set to 64.
[+] Setting speed to 198...
[+] Speed set to 198.
[+] Setting speed to 47...
[+] Speed set to 47.
[+] Setting speed to 12...
[+] Speed set to 12.
[+] Setting speed to 180...
[+] Speed set to 180.
[+] Setting speed to 63...
[+] Speed set to 63.
[+] Setting speed to 8...
[+] Speed set to 8.
[+] Stopping speed controller...
[+] Speed controller stopped.
[+] Setting screen to 100...
[+] Screen set to 100.
[+] Closed connection to 192.168.0.1:502.
```

Gambar 3.8 Program Python Penyerang



Gambar 3.9 Tampilan HMI yang diserang

Simulasi ini menunjukkan dampak nyata dari serangan siber terhadap perangkat fisik di lingkungan OT dan pentingnya proteksi jaringan seperti segmentasi dan *firewall.*

3.3.2.5. Proteksi terhadap Sistem OT

Setelah simulasi penyerangan yang menyebabkan motor bergerak dengan *setpoint* acak selama 30 detik, terlihat jelas bahwa sistem kontrol industri sangat rentan jika tidak dilindungi dengan baik. Pencegahan akses tidak sah dan manipulasi data kontrol dapat dilakukan dengan penerapan proteksi jaringan menggunakan *firewall* dan segmentasi. Proteksi ini bertujuan untuk membatasi jalur komunikasi hanya untuk perangkat yang terotorisasi, baik berdasarkan IP *address,* MAC *address*, maupun protokol komunikasi seperti Modbus TCP.

Segementasi jaringan adalah teknik penting dalam OT *cybersecurity* yang berfungsi untuk memisahkan jalur komunikasi antar perangkat agar tidak semua perangkat bisa saling berkomunikasi secara bebas. Dalam proteksi ini, segmentasi dilakukan dengan menggunakan BME NOC 0321, yaitu *Network Option Card* dari Schneider Electric yang dipasang pada PLC M580. BME NOC 0321 menyediakan *port* terpisah untuk komunikasi antara jaringan industri dan jaringan administrasi. Dalam simulasi ini, jaringan dibagi menjadi beberapa segmen yaitu jaringan industri (172.16.12.0/24) dan jaringan administrasi (172.16.112.0/24).

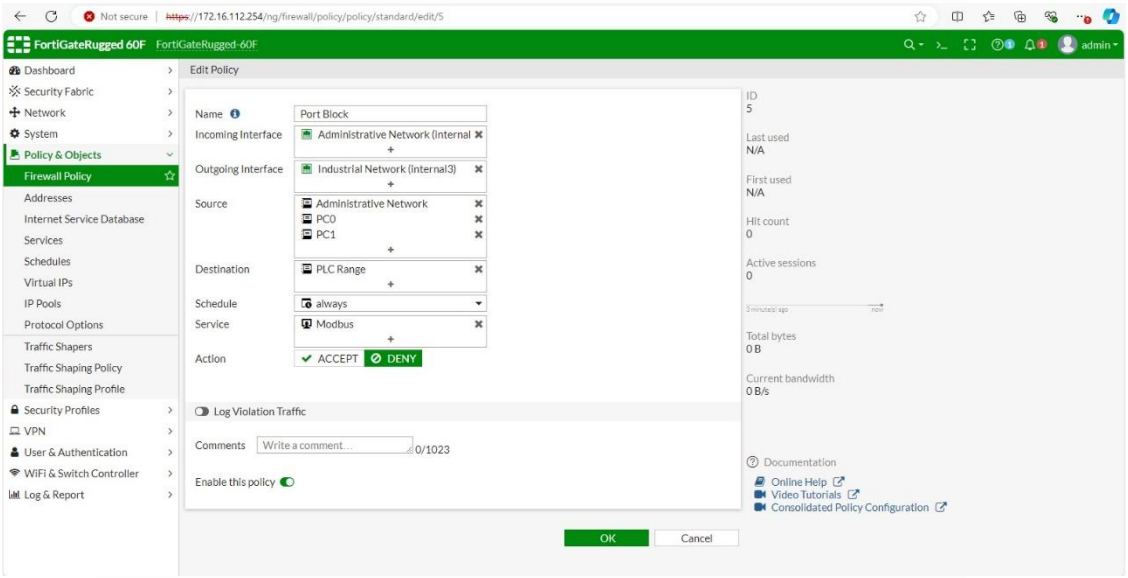
Setelah jaringan berhasil disegmentasi menggunakan BME NOC 0321, proteksi terhadap serangan sebelumnya dilakukan. Proteksi dilakukan dengan mengatur *firewall* Fortinet FGR-60F untuk memblokir akses tidak sah melalui tiga level, yaitu *port* 502, IP *address* dan MAC *address.*

Tabel 3.3 Lapisan Jaringan

Layanan	Manajemen Jaringan	Sinkronisasi Waktu	Konfigurasi			*Web Server*	E-mail	Pesan	Pemindaian I/O
Aplikasi	SNMP	NTP	DHCP	TFTP	FTP	HTTP	SMTP	Modbus / UMAS	
Transport	UDP				TCP				
Jaringan	IP								
Link	*Ethernet*								

- **Proteksi Aplikasi: Modbus / UMAS**

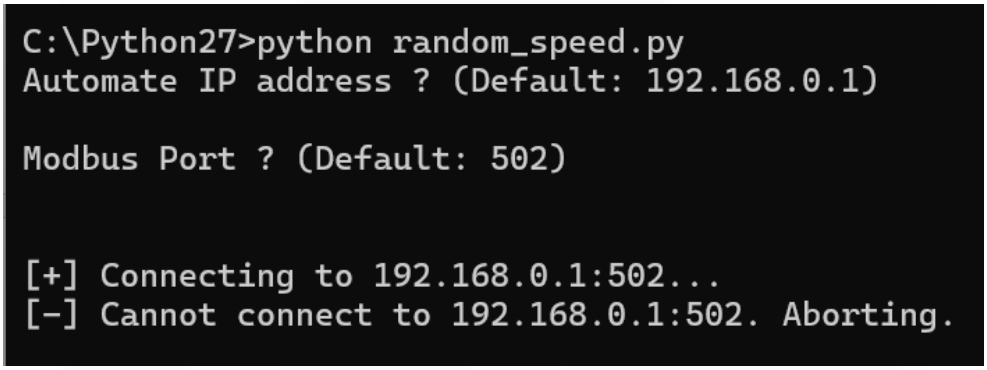
  Perlindungan Aplikasi pada protokol Modbus/UMAS dilakukan pada lapisan Aplikasi. Salah satu bentuk perlindungan tingkat aplikasi yang dapat dilakukan adalah dengan menonaktifkan sepenuhnya protokol Modbus/UMAS di jaringan. Berikut ini adalah pengaturan *firewall* untuk penolakan Modbus.



Gambar 3.10 Pemblokiran *Port* 502

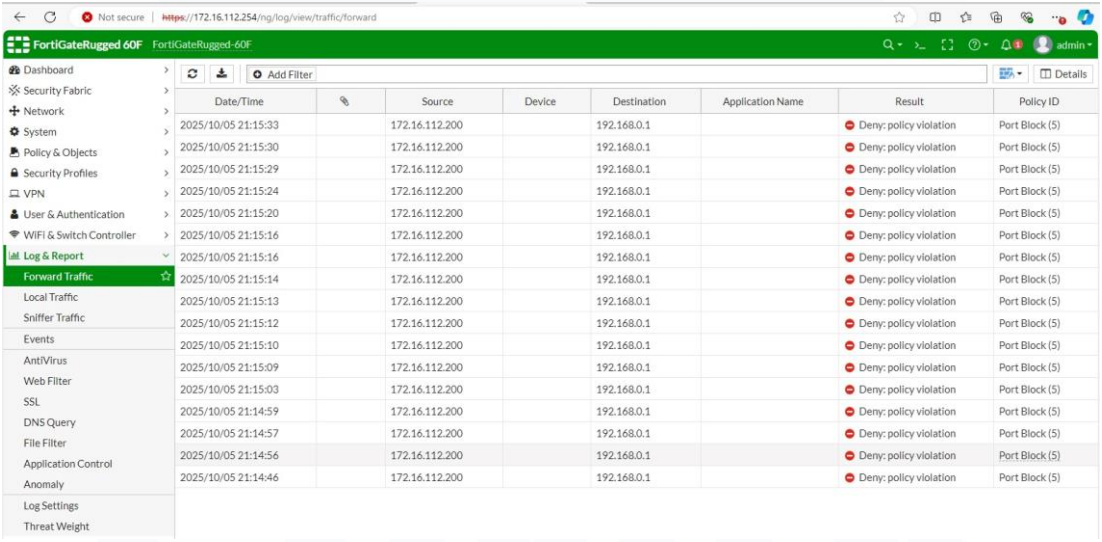
Policy ini akan memblokir *port* 502 sehingga PLC tidak bisa diakses. Kemudian, pada *command prompt*, jalankan skrip serangan yang dibahas

sebelumnya. Setelah beberapa saat, hasil yang ditunjukkan sama dengan yang terlihat di bawah.



Gambar 3.11 Hasil Serangan Gagal

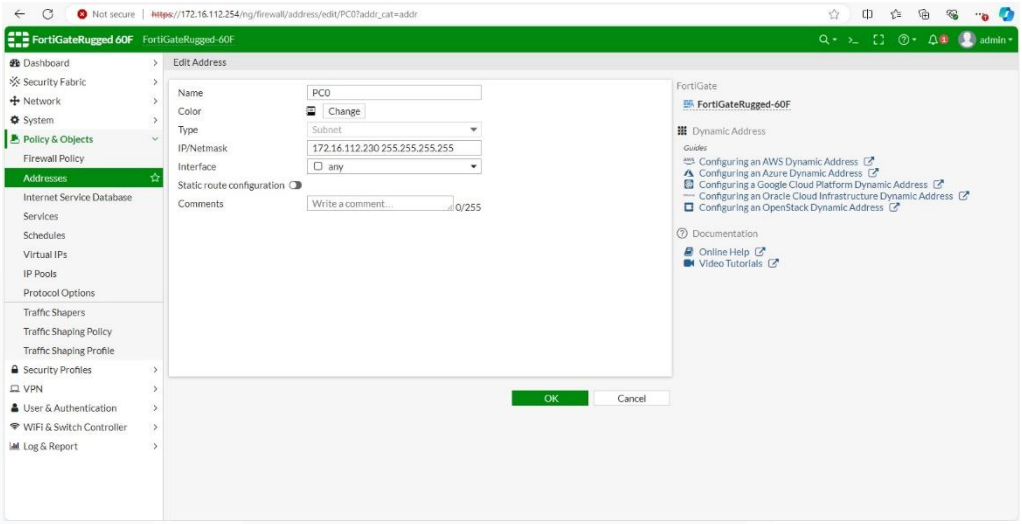
Serangan gagal karena paket tidak terkirim dan kontroler masih beroperasi secara normal. Kita juga dapat melihat dari *dashboard* FGR-60F bahwa paket yang diblokir tersebut tercatat.



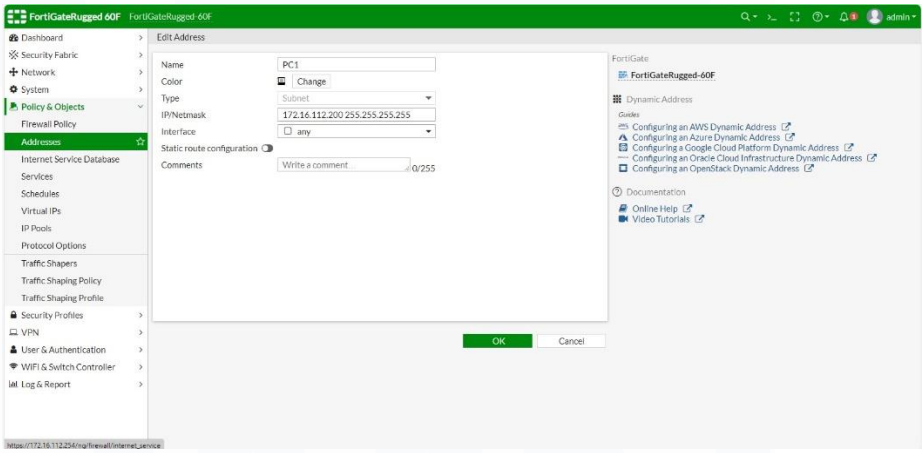
Gambar 3.12 *Log* lalu lintas melalui *port* 502

- **Proteksi Jaringan : *Filtering IP***

  Perlindungan dengan *filtering* IP tersedia pada tingkat jaringan dalam protokol IP. Untuk melakukan *filtering* berdasarkan IP *address*, kita perlu membuat *address* untuk IP yang diizinkan masuk dan IP yang diblokir. Pada contoh ini dibuat 2 *address* yaitu PC0 dengan IP *address* 172.16.112.200 dan PC1 dengan IP *address* 172.16.112.230.

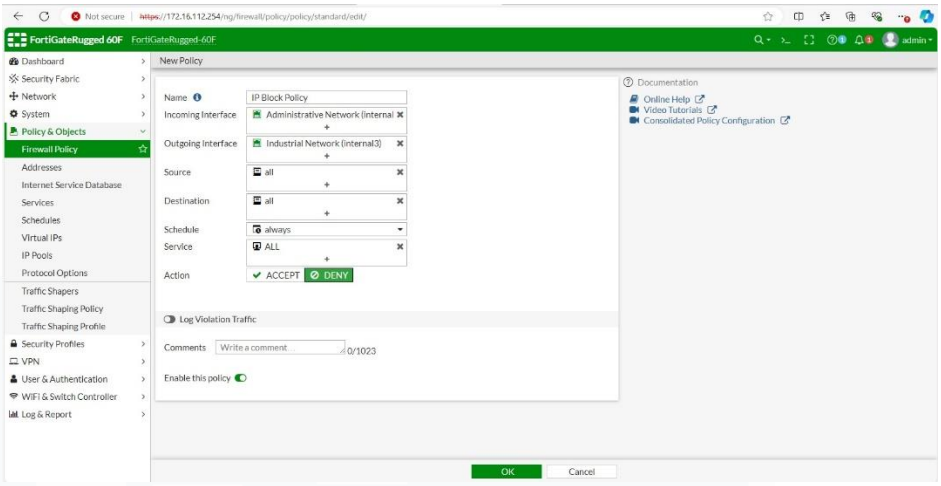


Gambar 3.13 *Address* IP PC0



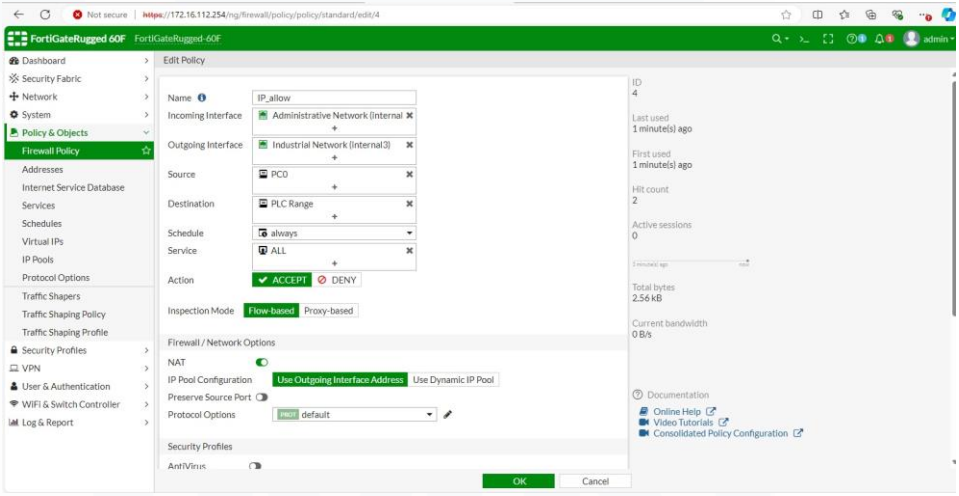
Gambar 3.14 *Address* IP PC1

Kemudian, sebuah *policy* untuk memblokir semua lalu lintas dibuat.



Gambar 3.15 *Policy* IP *Block*

PC0 dianggap sebagai PC yang sah untuk mengakses PLC, sehingga *address* ini diberi akses untuk masuk ke PLC.



Gambar 3.16 *Policy* IP *Allow*

Percobaan dilakukan dengan menggunakan Vijeo Designer yang menunjukkan bahwa PC masih memiliki akses ke PLC.

Gambar 3.17 Vijeo Designer dengan IP yang di izinkan

Ubah konfigurasi IP ke IP selain 172.16.112.230

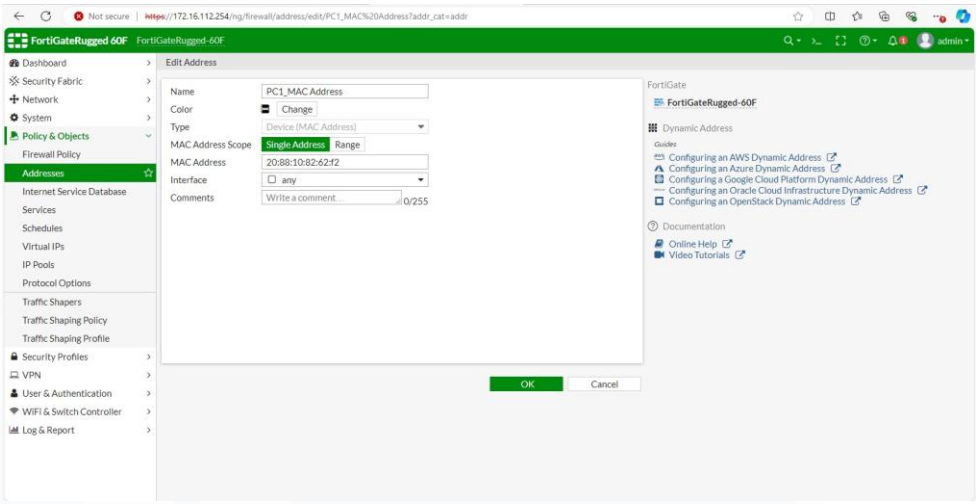
Mulai sekarang, jika skrip serangan dijalankan, komunikasi ke perangkat akan diblokir.

```
C:\Python27>python random_speed.py
Automate IP address ? (Default: 192.168.0.1)

Modbus Port ? (Default: 502)


[+] Connecting to 192.168.0.1:502...
[-] Cannot connect to 192.168.0.1:502. Aborting.
```

Gambar 3.18 Serangan Gagal ke IP Berbeda

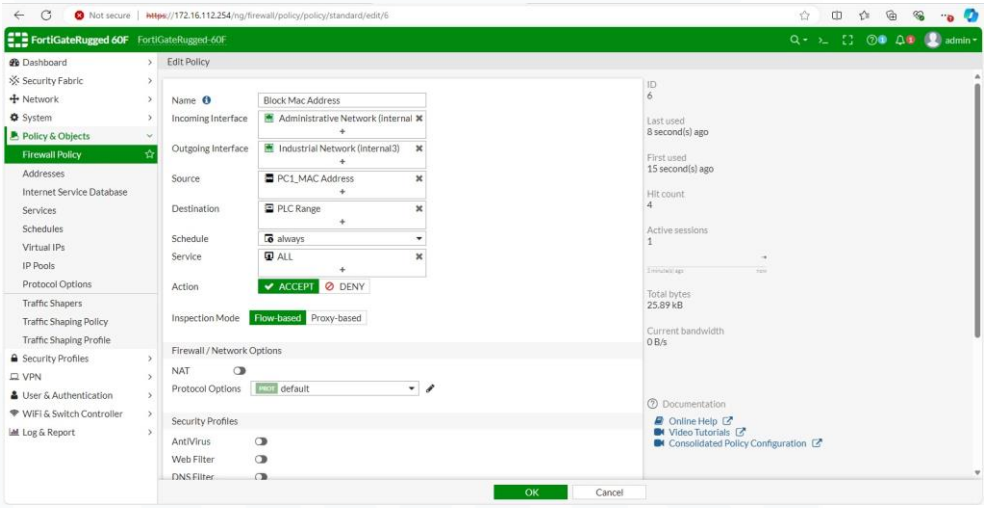
- **Perlindungan *Link: Filtering* MAC *address***

  Perlindungan MAC *address* disediakan pada tingkat *Link*, pada protokol Ethernet. Proteksi ini hanya mengizinkan MAC *address* tertentu untuk masuk ke perangkat. Kita perlu membuat *address* yang berisi MAC *address* yang diizinkan untuk masuk ke perangkat.



Gambar 3.19 MAC *Address* PC

Kemudian, buat sebuah *policy* untuk mengatur MAC *address* agar dapat mengakses perangkat.

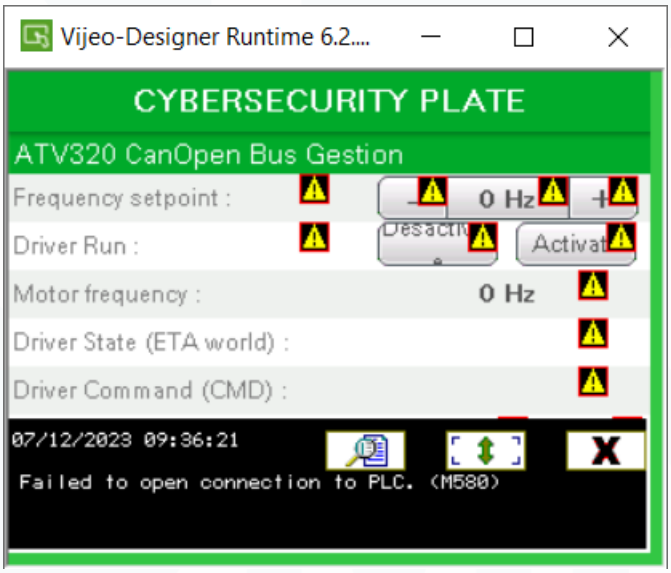


Gambar 3.20 *Policy Block* MAC *Address*

Periksa apakah koneksi ke kontroler bekerja dengan benar menggunakan Vijeo Designer.

Gambar 3.21 Tampilan Vijeo Designer MAC *Allow*

Saat *policy* diubah menjadi "DENY", akses ke perangkat akan ditolak. Hal ini ditunjukkan oleh tampilan Vijeo Designer yang *error*.



Gambar 3.22 Tampilan Vijeo Designer MAC Berbeda

Meskipun firewall dapat memblokir akses berdasarkan IP *address* dan MAC *address*, kenyataannya kedua identitas ini sangat mudah dimanipulasi. Seorang penyerang dengan pengetahuan teknis yang cukup dapat dengan mudah mengubah IP atau MAC perangkatnya, sehingga dapat melewati proteksi dasar tersebut. Bahkan, penyerang yang lebih mahir mampu membentuk paket data secara manual

dan mengatur setiap bit di dalamnya sesuai kebutuhan. Jenis serangan ini, yang menyamar sebagai perangkat lain dengan mencuri IP, MAC, atau informasi identifikasi lainnya, dikenal sebagai ***spoofing***. Oleh karena itu, sangat penting untuk menerapkan keamanan secara menyeluruh di semua lapisan jaringan. Untungnya, terdapat berbagai strategi untuk mencegah serangan *spoofing*, dan beberapa di antaranya sudah tersedia sebagai fitur bawaan dalam *firewall* modern.

3.3 Kendala yang Ditemukan

Kendala yang ditemukan selama proses magang adalah kurangnya pengetahuan terkait cara menggunakan perangkat lunak atau produk yang terkait. Hal ini menghambat penulis dalam pekerjaan sehingga membutuhkan waktu yang lebih lama. Alat yang digunakan berbeda dengan modul yang tersedia sehingga cara penggunaannya juga berbeda. Selain itu, di dalam proses adopsi terdapat juga beberapa bagian yang berbeda dengan tipe *firewall* yang sudah tersedia di modul versi luar. Contoh bagian yang berbeda adalah fitur *pass all* dan *block all* serta juga terdapat IPS Signature.

3.4 Solusi atas Kendala yang Ditemukan

Solusi bagi kendala terkait pemahaman penulis yang kurang terkait perangkat lunak dan produk adalah dengan bertanya kepada partner kerja dari divisi yang merupakan *expert* di bidang yang ingin dipahami. Sebagai contoh, penulis bertanya kepada *expert* di bidang Control Expert, PLC M580 dan *firewall* yang digunakan. Pada masalah terkait bagian yang berbeda, penulis mencari Solusi dengan mempelajari cara kerja dengan menggunakan *firewall* versi Indonesia dan menyusun ulang cara kerja sesuai modul terkait.