Implementasi *Snort* pada Simulator GRFICSv2 sebagai Sarana Pembelajaran di Poltek SSN

Marcella Risky Avianti[1)], Rahmat Purwoko[2)]

1) Program Studi Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, marcella.risky@student.poltekssn.ac.id

2) *Program Studi Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, rahmat.purwoko@poltekssn.ac.id*

Abstrak

Pada beberapa tahun terakhir kasus kejahatan siber semakin meningkat serta target serangan semakin beragam. Industrial Control System (ICS) sebagai infrastruktur kritis juga menjadi target serangan siber. Politeknik Siber dan Sandi Negara (Poltek SSN) memiliki program studi Rekayasa Keamanan Siber (RKS) yang bertujuan mencetak praktisi keamanan siber nasional. Untuk meningkatkan keterampilan taruna Poltek SSN dapat dilakukan pembelajaran yang mampu memberikan simulasi terkait proses fisik ICS. Pembatasan masalah pada penelitian ini adalah penggunaan lingkungan mesin virtual menggunakan simulator Graphical Realism Framework for Industrial Control Simulation versi 2 (GRFICSv2) untuk memberikan gambaran mengenai proses fisik ICS dengan penambahan aspek keamanan berupa Intrusion Detection System (IDS) Snort dan simulasi serangan berupa Injecting Malicious Modbus Command dan Uploading Malicious PLC Program. Serangan tersebut dilakukan dengan menargetkan simulator yang dilengkapi IDS Snort sehingga memberikan informasi atau alert. Pengujian pemahaman diberikan kepada taruna Poltek SSN berupa pre-test dan post-test, untuk mengetahui pemahaman terhadap proses fisik dan keamanannya. Hasil pengujian yang didapatkan diolah menggunakan uji-t berpasangan untuk mengetahui perbedaan nilai rata-rata sebelum dan sesudah adanya simulator.

Kata kunci: ICS, Poltek SSN, Simulator, Uji-t berpasangan

Abstract

In recent years, cybercrime cases have increased and the targets of attacks have become more diverse. The Industrial Control System (ICS) as critical infrastructure is also the target of cyber attacks. The National Cyber and Crypto Polytechnic (Poltek SSN) has a Cyber Security Engineering (RKS) study program which aims to produce national cyber security practitioners. To improve the skills of SSN Polytechnic cadets, learning can be carried out which is able to provide simulations related to ICS physical processes. The limitation of the problem in this research is the use of a virtual machine environment using the Graphical Realism Framework for Industrial Control Simulation version 2 (GRFICSv2) simulator to provide an overview of the physical processes of ICS with the addition of security aspects in the form of Intrusion Detection System (IDS) Snort and attack simulations in the form of Injecting Malicious Modbus Command and Uploading Malicious PLC Program. The attack was carried out by targeting simulators equipped with IDS Snort to provide information or alerts. Understanding testing is given to SSN Polytechnic cadets in the form of pre-test and post-test, to determine understanding of physical processes and safety. The test results obtained were processed using a paired t-test to determine the difference in average values before and after the simulator.

Keywords: ICS, Paired t-test, Polytechnic SSN, Simulator

1. PENDAHULUAN

Penggunaan internet yang banyak digunakan membuat munculnya pihak-pihak lain yang memiliki tujuan untuk menyerang atau memanfaatkan celah yang ada pada untuk mengambil data atau informasi berharga dari pengguna. Hal ini akan terus meningkat jika tidak segera ditangani. Menurut laporan Badan Siber dan Sandi Negara (BSSN) [1] pada tahun 2021 telah terjadi 1.637.973.022 anomali lalu lintas jaringan di Indonesia dimana 1cenari ini terjadi karena adanya serangan yang masuk ke dalam wilayah Indonesia.

Menurut V. Gkioulos and N. Chowdhury dalam penelitiannya [2], pada era saat ini, keamanan siber menjadi perhatian utama dengan kasus serangan siber menjadi berita utama di berbagai media. Banyak 1cenar yang menjadi target serangan siber. Infrastruktur kritis dan 1cenario menjadi salah satu target utama serangan siber dalam beberapa tahun terakhir di berbagai wilayah di dunia. Infrastruktur kritis memiliki peran yang sangat penting dan perlu dipastikan berjalan sesuai dengan yang seharusnya. Jika terjadi insiden sekecil apapun pada infrastruktur kritis akan memengaruhi sistem yang lain atau akan menjadi risiko yang lebih besar [3].

Sebagai infrastruktur besar, cukup sulit untuk mempelajari cara kerja suatu *Industrial Control System* (ICS) tanpa melihat bagaimana cara kerjanya. ICS memiliki komponen dengan jumlah yang cukup banyak, seperti PLC, HMI, *testbed*, dan lainnya. Ketika peneliti ingin bekerja dengan lingkungan nyata dari ICS, solusi yang paling tepat adalah dengan membangun *testbed*. Hal ini dikarenakan *testbed* dapat merepresentasikan 1cenario nyata dari ICS [4]. Menurut *Teixeira et al*. [5] *testbed* dikembangkan untuk memberikan pemahaman lebih baik mengenai proses fisik, serangan, dan dampak yang ditimbulkan pada sistem *Supervisory Control and Data Acquisition* (SCADA). Oleh karena itu, pemilihan

testbed berperan penting untuk menentukan keefektifan dari penelitian yang dilakukan. Pada penelitian ini *testbed* yang digunakan adalah *virtual testbed. Virtual testbed* merupakan *testbed* yang menggunakan bantuan *software* untuk membangun lingkungan penelitian. *Virtual testbed* dipilih karena memiliki keunggulan dalam sektor biaya dan waktu pembangunan lingkungan penelitian.

Politeknik Siber dan Sandi Negara atau Poltek SSN memiliki program studi Rekayasa Keamanan Siber yang memiliki visi menjadi program studi di bidang keamanan siber yang berkualitas dan menghasilkan aparatur keamanan siber yang unggul, serta berkontribusi dalam keamanan nasional pada 2030 [6] tentunya harus menyiapkan lulusan yang memahami konsep serangan dan pertahanan pada jaringan, contohnya pada ICS. Pembelajaran mengenai ICS saat ini masih dilakukan secara teoritis. Taruna Poltek SSN tidak dapat melihat langsung mengenai cara kerja atau proses fisik dari ICS. Penggunaan simulator untuk memudahkan taruna Poltek SSN dapat dicoba untuk diterapkan, guna mengetahui cara kerja atau proses fisik yang terjadi pada ICS serta memberikan gambaran mengenai dampak yang ditimbulkan jika terjadi serangan yang menargetkan ICS sebagai target serangan.

Penelitian ini mengunakan bantuan simulator *Graphical Realism Framework Industrial Control Simulation version* 2 (GRFICSv2) untuk mempermudah pembelajaran mengenai ICS. GRFICSv2 merupakan suatu *tools* yang bersifat *open-source* yang dapat menampilkan simulasi keadaan ICS. Dengan adanya simulator, maka akan lebih tergambar bagaimana keadaan ICS jika menerima serangan. GRFICSv2 *framework* menggunakan 3D *game engine* untuk menampilkan visualisasi keadaan sebenarnya dengan lebih menarik [7]. Penggunaan simulator GRFICSv2 pada penelitian ini akan diintegrasikan dengan *Intrusion Detection System* (IDS) *Snort* untuk meningkatkan aspek keamanan pada simulator ICS.

Snort merupakan sistem *Intrusion Detection System/Intrusion Prevention System* (IDS/IPS) yang bersifat *open source* dan mampu melakukan analisis lalu lintas jaringan dan *packet sniffing* [8]. *Snort* mampu mendeteksi berbagai jenis serangan seperti *buffer overflow*, CGI *attack, stealth port scan*, dan lainnya [9]. *Snort* akan mengambil data secara *realtime* dari internet yang selanjutnya paket yang sudah di-*capture* akan dicocokkan dengan *predefined signature* atau *rules* yang telah dibuat sebelumnya dan memberikan *alert* jika terdapat hal yang tidak sesuai. Menurut penelitian yang dilakukan oleh *Bada et al*. [10], *Snort* memiliki persentase dalam mengirimkan *true-positive* yang lebih baik dibandingkan dengan dua IDS lainnya, yaitu Suricata dan Bro IDS.

Simulator GRFICSv2 yang dibangun pada lingkungan virtualiasi proxmox dan diuji coba dengan menjalankan dua jenis serangan. Setelah dilakukan penambahan keamanan berupa IDS *Snort*, dilakukan pengujian kembali dengan serangan yang sama. Penelitian ini bertujuan untuk mengetahui apakah IDS *Snort* dapat memberikan *alert* jika terjadi serangan yang menargetkan simulator dan untuk mengetahui apakah dengan adanya simulatordapat meningkatkan pemahaman taruna Poltek SSN mengenai materi ICS.

2. TELAAH KEPUSTAKAAN

2.1 GRFICSv2

Graphical Realism Framework for Industrial Control Simulations (GRFICS) melakukan virtualisasi terhadap keseluruhan jaringan ICS mulai dari antarmuka operator hingga simulasi dari proses yang dilakukan ICS [7]. GRFICSv2 diciptakan secara modular untuk memudahkan dilakukan pengembangan atau bahkan kustomisasi sesuai dengan kebutuhan. Selain itu, proses fisik yang dilakukan oleh ICS divisualisasikan menggunakan visualisasi 3D *game engine*, Unity.

2.2 SCADA

SCADA merupakan sistem yang digunakan untuk melakukan kontrol terhadap aset yang tersebar menggunakan kontrol pengawasan [11]. SCADA menyediakan otomatisasi proses pengumpulan data secara *real time*, melakukan kontrol proses industri, dan memantau peralatan fisik industri yang tersebar [12]. Jaringan SCADA biasanya mencakup *server* kontrol pada pusat kontrol, tautan komunikasi, dan situs lapangan. SCADA akan mengirimkan sinyal ke perangkat lapangan seperti *Programmable Logic Controller* (PLC), *Remote Terminal Unit* (RTU) atau *Intelligent Electronic Device* (IED). Melalui tautan komunikasi, terjadi transfer informasi antara perangkat kontrol lapangan dengan pusat kontrol. Pusat kontrol akan menyimpan informasi status di data historian dan menampilkannya di HMI (*Human Machine Interface*) yang menyediakan pemantauan informasi status digital dan kontrol sistem secara terpusat [13].

2.3 PLC

PLC merupakan salah satu komponen penting dalam ICS khususnya dalam SCADA [14]. PLC berfungsi untuk mengelola dan mengontrol komponen fisik seperti motor, sensor, dan lainnya. PLC biasanya memiliki tiga komponen utama yaitu *embedded operating system*, *control system software*, dan *analog and digital inputs/outputs.*

2.4 Snort

Snort merupakan sistem IDS/IPS yang bersifat *open source* dan mampu melakukan analisis lalu lintas jaringan jaringan dan *packet sniffing* [8]. *Snort* mampu mendeteksi berbagai jenis serangan seperti *buffer overflow*, CGI *attack, stealth port scan*, dan lainnya. Untuk melakukan deteksi terhadap intrusi pada jaringan perlu dilakukan konfigurasi *rules* pada

Snort. *Rules* pada *Snort* dapat dikonfigurasikan sesuai kebutuhan pengguna. Menurut penelitian yang dilakukan oleh *Bada et al*. [10], dalam rentang waktu yang sama dengan dua IDS lainnya, yaitu Suricata dan Bro IDS, *Snort* memiliki persentase yang lebih baik dalam mengirimkan data yang bernilai *true-positive*.

2.5 Modbus *Protocol*

Modbus *protocol* merupakan protokol yang paling umum digunakan pada SCADA. Modbus melakukan transmisi informasi menggunakan jalur serial antar perangkat elektronik. Biasanya Modbus digunakan untuk menghubungkan *supervisory computer* dengan *Remote Terminal Unit* (RTU) [15]. Namun, berdasarkan penelitian yang dilakukan oleh Evangelia [15], Parian *et al.* [16], serta Philips *et al.* [17] menjelaskan bahwa protokol Modbus tidak memiliki sistem keamanan seperti otentikasi atau otorisasi, serta tidak ada verifikasi integritas data. Semua data yang dikirimkan oleh Modbus berupa data tanpa enkripsi atau secara *plaintext* [17].

2.6 Metode Pembelajaran Praktikum

Terdapat beberapa model pembelajaran yang dapat digunakan seperti penyampaian materi secara teoritis atau menggunakan metode praktis yang melibatkan siswa untuk berperan dalam pembelajaran yang dilakukan. Metode praktis atau bisa disebut sebagai metode percontohan memungkinkan siswa untuk melakukan pengumpulan data berdasarkan penelitian yang dilakukan. Metode percontohan yang terorganisir dengan baik berpotensi untuk meningkatkan kualitas penelitian yang dilakukan [18].

Berdasarkan penelitian yang dilakukan oleh Ukwandu [20] dijelaskan bahwa melakukan latihan dalam lingkungan yang sudah dibangun sesuai dengan kondisi nyata akan mempermudah dan mempercepat siswa untuk memahami tentang konsekuensi terhadap aksi yang dilakukan. Saat ini perkembangan teknologi berpengaruh dalam proses pendidikan. Penggunaan teknik interaktif dalam dunia pendidikan dapat meningkatkan efektivitas pendidikan dan menumbuhkan minat belajar siswa [21].

2.7 Uji-t Berpasangan

Metode untuk melakukan pengujian hipotesis yang digunakan adalah dengan melakukan uji-t. Berdasarkan jumlah sampel yang digunakan, terdapat pengujian dengan satu sampel (*one sample t-test*) dan uji-t berpasangan. Pada uji-t berpasangan, satu objek penelitian akan menerima dua perlakuan berbeda. Selanjutnya akan dilihat perbandingan nilai rata-rata objek saat sebelum mendapat perlakuan dan setelah mendapatkan perlakuan. Untuk melakukan uji-t, langkah awal yang perlu dilakukan adalah dengan merumuskan hipotesis awal, menentukan besaran nilai alfa, melakukan perhitungan uji-t, pengambilan keputusan, hingga kemudian penarikan kesimpulan [22]. Berikut ini merupakan formula yang digunakan untuk perhitungan uji-t.

$$t_{hit} = \frac{\overline{x_1} - \overline{x_2}}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2} - 2r\left(\frac{s_1}{\sqrt{n_1}}\right)\left(\frac{s_2}{\sqrt{n_2}}\right)}}$$

Keterangan:
t_{hit} = t hitung
$\overline{x_1}$ = nilai rata-rata sampel 1
$\overline{x_2}$ = nilai rata-rata sampel 2
r = korelasi antara 2 sampel
s_1 = simpangan baku sampel 1
s_2 = simpangan baku sampel 2
s_1^2 = variansi sampel 1
s_2^2 = variansi sampel 2
n_1 = jumlah sampel sebelum perlakuan
n_2 = jumlah sampel setelah perlakuan

Setelah dilakukan perhitungan uji-t dan didapatkan besaran nilai t hitung, hal yang perlu dilakukan selanjutnya adalah membandingkan nilai t hitung yang didapatkan dengan besaran nilai t tabel. Besaran nilai t tabel dapat diketahui mencari pada t tabel berdasarkan dengan besaran derajat bebas dan nilai alfa yang digunakan. Pada Gambar 1 ditunjukkan kurva daerah penerimaan dan penolakan H_0.

Gambar 1. Daerah penerimaan H_0

Berdasar Gambar 1 diketahui terdapat daerah penolakan H_0 dan daerah penerimaan H_0. Daerah penolakan atau disebut daerah kritis adalah interval nilai dimana hitungan suatu statistik uji yang berada dalam interval tersebut akan ditolak hipotesis nolnya. Untuk mengetahui apakah H_0 diterima atau ditolak ada dua bentuk pengujian hipotesis yaitu:

1. Hipotesis Direksional, merupakan rumusan hipotesis yang arahnya sudah jelas (kanan atau kiri) atau disebut hipotesis langsung.
   a. Uji pihak kiri, pada pengujian pihak kiri H_0 diterima jika nilai $t_{hitung} \geq -t_{tabel}$
   b. Uji pihak kanan, pada pengujian pihak kanan H_0 diterima jika nilai $t_{hitung} \leq t_{tabel}$
2. Hipotesis Nondireksional, merupakan rumusan hipotesis yang dilakukan secara dua pihak. Uji dua pihak dilakukan jika H_0 bernilai "sama dengan" (=) dan H_a bernilai "tidak sama dengan" (≠). Pada pengujian dua pihak, H_0 diterima jika nilai $-t_{tabel} \leq t_{hitung} \leq t_{tabel}$

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan simulator ICS berupa GRFICSv2 yang tersedia secara *open source* di situs Github. Objek penelitian ini berupa integrasi *Snort* sebagai IDS/IPS yang diharapkan dapat memberikan notifikasi berupa *alert* jika terjadi serangan yang ditujukan kepada simulator ICS sebagai targetnya. Penambahan *Snort* pada GRFICSv2 diharapkan mampu meningkatkan aspek keamanan pada simulator ICS dengan memberikan notifikasi atau *alert* ketika terjadi serangan yang ditujukan ke simulator ICS.

Jenis penelitian yang digunakan yaitu campuran, dimana pada tahap awal dilakukan penelitian rancang bangun dengan membangun lingkungan uji dan setelah dilakukan penelitian dilakukan pengambilan data dengan pendekatan kuantitatif.

Tahapan penelitian beserta metode atau prosedur yang dilakukan sebagai berikut:

a. Analisis Kebutuhan dan Ketersediaan Perangkat
   Pada tahap analisis kebutuhan dan ketersediaan perangkat, peneliti harus mengetahui kebutuhan perangkat atau kebutuhan pendukung lain yang diperlukan dalam pembangunan sarana penelitian. Peneliti juga perlu mengetahui spesifikasi perangkat yang diperlukan untuk membangun sarana penelitian. Oleh karena itu, penting bagi peneliti untuk melakukan identifikasi kebutuhan dan perancangan lingkungan simulasi sebelum membangun sarana simulasi.
b. Pembangunan Sarana Simulasi
   Pada tahap ini peneliti akan membangun mesin virtual dengan lingkungan virtual proxmox sesuai dengan GRFICSv2 seperti HMI, PLC, Workstation, Pfsense, dan Simulator. Mesin penyerang berupa Kali Linux yang dibangun pada perangkat lain yang disiapkan untuk melakukan simulasi serangan dengan koneksi OpenVPN.
c. Pengujian Simulasi Serangan Sebelum Ditambahkan *Snort*
   Simulasi serangan akan dilakukan dua kali pengujian. Pengujian pertama adalah pengujian saat simulator ICS berjalan tanpa adanya penambahan Intrusion Detection System (IDS). Jenis serangan yang dilakukan pada pengujian pertama adalah *Injecting Malicious* Modbus *Command* dan *Uploading Malicious* PLC Program.
d. Penambahan IDS *Snort* pada Pfsense
   Untuk menambahkan keamanan pada simulator GRFICSv2 yang dibangun, ditambahkan mekanisme keamanan berupa IDS *Snort* pada pfsense dengan *rules* yang dibuat sesuai dengan protokol modbus.
e. Pengujian Simulasi Serangan Setelah Ditambahkan *Snort*
   Pengujian dilakukan kembali dengan menggunakan dua jenis serangan yang sama seperti pengujian yang pertama dan dilakukan analisis apakah dengan adanya penambahan IDS pada router dapat memberikan *alert* atau peringatan saat dilakukan serangan yang ditujukan kepada simulator.
f. Pengujian Pemahaman
   Sebelum tahap proses pembelajaran dilakukan ujian pra-pembelajaran (*pre-test*). Pre-test dilakukan untuk mengetahui sejauh mana taruna memahami materi mengenai ICS. Setelah dilakukan *pre-test* peneliti akan melanjutkan proses pembelajaran. Proses pembelajaran akan dilakukan secara teori dan praktik. Pada pembelajaran teori peneliti akan menjelaskan dasar-dasar pengetahuan ICS dan jenis serangan yang dapat dilakukan pada ICS. Proses pembelajaran praktik dilakukan dengan menggunakan sarana simulasi yang telah dibangun sebelumnya. Pada proses praktik akan dilakukan pengujian terhadap simulator GRFICSv2.
   Pengujian pada penelitian ini dilakukan dengan mencoba simulasi serangan yang ditujukan kepada simulator ICS. Jenis serangan yang akan dilakukan yaitu *Malicious Modbus Command Injection* dan *Uploading Malicious PLC Program*. Setelah proses pembelajaran secara teori dan praktik dilakukan, peneliti akan melakukan ujian pasca pembelajaran atau *post-test*. *Post-test* dilakukan untuk mengetahui apakah terjadi peningkatan pemahaman materi mengenai ICS oleh taruna yang sebelumnya telah diberikan pembelajaran.
g. Uji-t Berpasangan
   Data hasil yang didapat dari responden akan dihitung menggunakan uji-t statistik untuk mengetahui apakah terjadi peningkatan pemahaman taruna terhadap materi ICS berdasarkan nilai hasil dari pertanyaan *pre-test* dan *post-test* yang telah diisi responden. Uji-t berpasangan digunakan untuk mengetahui perbedaan rata-rata nilai dari saat *pre-test* dan *post-test*. Populasi yang ingin diteliti yaitu taruna tingkat IV Poltek SSN. Hal ini dilakukan karena taruna Poltek SSN baru menerima materi mengenai ICS pada semester tujuh dan delapan. Setelah dilakukan pengujian *pre-test* dan *post-test* akan dilakukan pengujian uji-t berpasangan untuk mengetahui perbedaan nilai rata-rata sebelum dan sesudah adanya proses pembelajaran.

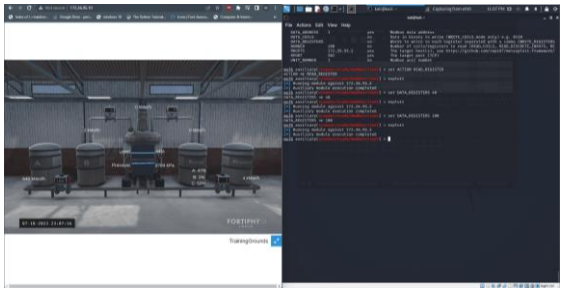
4. HASIL PENELITIAN

Setelah lingkungan uji berhasil terbangun, selanjutnya melakukan pengujian simulasi serangan. Serangan yang akan diujikan adalah *Injecting*

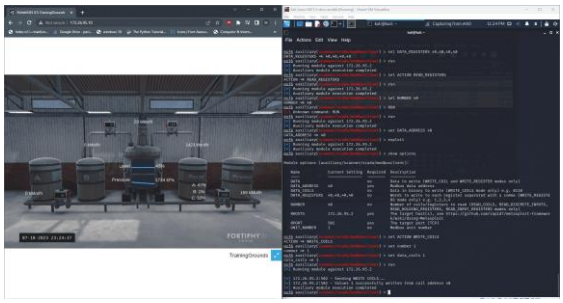
Malicious Modbus Command dan *Uploading Malicious PLC Program*.

4.1 *Injecting Malicious* Modbus *Command*

Serangan *Injection Malicious* Modbus *Command* merupakan serangan yang dilakukan dengan mencoba memasukkan perintah modbus yang bersifat *malicious*. Pada penyerangan ini, *tools* yang diperlukan dalam proses injeksi perintah *malicious* adalah metasploit. Metasploit dapat dijalankan melalui terminal Kali Linux dengan menggunakan perintah *msfconsole*. Gambar 2 sebelah kiri memperlihatkan kondisi normal simulator, selanjutnya dilakukan penyerangan terhadap simulator PLC dengan melakukan penulisan parameter koil dari nilai 0 menjadi nilai 1 seperti yang terlihat pada Gambar 3. Hasil dari penyerangan tersebut adalah penurunan tekanan (*pressure*) yang cukup signifikan.



Gambar 2. Kondisi normal simulator

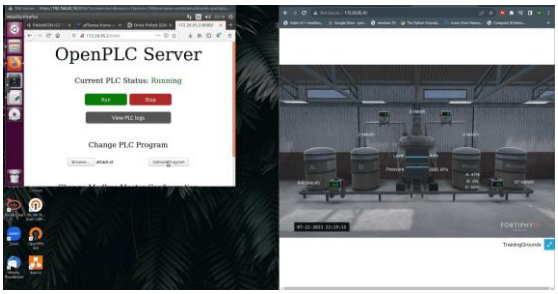


Gambar 3. Kondisi simulator setelah serangan

4.2 *Uploading Malicious* PLC *Program*

Serangan *uploading malicious* PLC *program* merupakan serangan yang dilakukan menggunakan *tools* OpenPLC Editor untuk membuat kode PLC. Kode PLC akan dibuat destruktif atau bersifat merusak. Pada mesin virtual *Workstation*, buka OpenPLC Editor dan buka fungsi *initialize_sp* untuk mengetahui konfigurasi PLC yang diterapkan. Pada serangan yang akan dilakukan, nilai *press_sp_c* akan dimodifikasi menjadi lebih tinggi agar tekanan selalu bertambah melebihi kapasitas yang dimiliki. Dengan demikian, nantinya ICS akan rusak karena tidak mampu menahan nilai tekanan yang melebihi batas maksimal. Serangan ini dilakukan dengan mengubah kode PLC pada variabel *press_sp_c* melebihi nilai yang sebelumnya tercantum pada kode PLC asli. Kode PLC yang sudah dimodifikasi akan diunggah sebagai *attack script* yang nantinya akan merusak ICS.

Konfigurasi mesin PLC simulator dilakukan menggunakan web GUI. Penyerangan dilakukan dengan mengunggah *attack script* melalui *browser*. Gambar 4 memperlihatkan tampilan web GUI mesin PLC saat dilakukan pengunggahan *attack script*, sedangkan Gambar 5 memperlihatkan kondisi simulator saat mesin PLC menjalankan kode PLC yang telah dimodifikasi sehingga mengakibatkan kenaikan tekanan yang drastis dan kerusakan pada *boiler*.



Gambar 4. Pengunggahan *attack script*

Gambar 5. Kondisi simulator setelah serangan

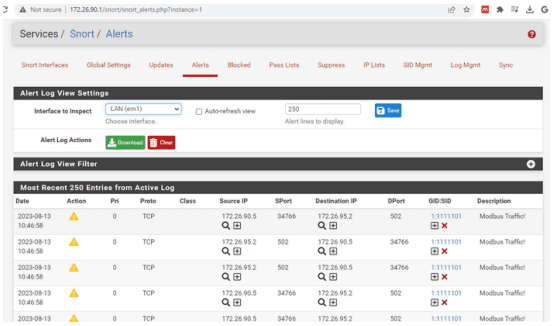
4.3 Hasil Deteksi IDS Snort pada Simulator

Setelah dilakukan pengujian serangan awal sebelum adanya IDS, tahap berikutnya adalah menambahkan IDS *Snort* pada pfsense dan membuat *Snort rules* untuk mendeteksi serangan pada protokol modbus dengan *port* yang digunakan adalah 502. Berikut ini merupakan konfigurasi *Snort rules* yang digunakan.

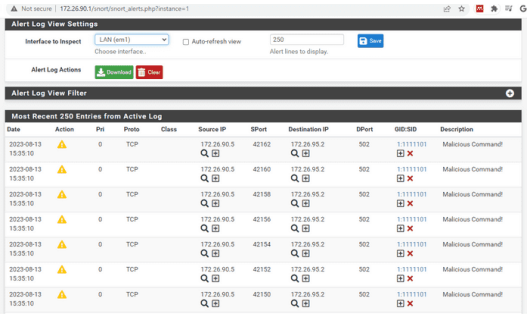
```
alert tcp any any -> any 502 (msg:"Malicious Command!";sid:1111101;)
```

Gambar 6. Konfigurasi snort *rule*

Tahap selanjutnya adalah pengujian simulasi kedua yaitu pengujian serangan sama dengan sebelumnya dengan penambahan IDS *Snort rules* deteksi modbus diaktifkan. Gambar 6 dan 7 memperlihatkan tampilan web GUI pfsense terkait *alert* IDS snort saat mendeteksi serangan pada protokol modbus.



Gambar 7 Tampilan *alert* saat terjadi serangan



Gambar *8* Tampilan *alert* setelah serangan

4.4 Pengujian Pemahaman Taruna

Setelah pengujian dengan adanya *Snort* dilakukan, langkah selanjutnya adalah melakukan pengujian pemahaman. berupa *pre-test* dan *post-test. Pre-test* diberikan kepada responden untuk mengetahui sejauh mana pemahaman responden mengenai ICS. Setelah responden mengerjakan soal *pre-test* maka peneliti akan rekapitulasi nilai yang didapatkan oleh responden. Setelah dilakukan *pre-test* peneliti akan melakukan proses pembelajaran kepada responden. Nilai *pre-test* yang didapatkan responden akan dihitung rata-ratanya dan dilakukan pengujian dengan uji-t berpasangan dengan rata-rata nilai *post-test.*

Uji-t berpasangan merupakan pengujian yang dilakukan untuk mengetahui perbedaan dua rata-rata dalam satu sampel pengujian yang sama. Pada penelitian ini diharapkan terjadi peningkatan pemahaman, sehingga hipotesis awal disusun sebagai berikut.

H_0= Tidak terdapat perbedaan signifikan terhadap nilai rata-rata *pre-test* dan *post-test.*

H_a= Terdapat perbedaan signifikan terhadap nilai rata-rata *pre-test* dan *post-test.*

Penelitian ini menggunakan populasi taruna tingkat IV Poltek SSN dengan sampel yang diteliti adalah 40 orang taruna tingkat IV Poltek SSN. Responden nanti nya akan melakukan *pre-test* untuk menguji pemahaman mengenai materi ICS sebelum diberikan proses pembelajaran. Setelah dilakukan *pre-test*, peneliti akan memberikan pembelajaran mengenai materi ICS secara teori dan praktik. Responden akan mencoba melakukan praktikum menggunakan simulator yang telah dibangun. Setelah itu, responden akan diminta untuk melakukan *post-test* dengan soal yang sama seperti *pre-test.* Kemudian jika *pre-test* dan *post-test* sudah didapatkan nilainya maka akan dilakukan uji-t berpasangan untuk mengetahui perbedaan nilai rata-rata sebelum dan sesudah dilakukan pembelajaran. Perbandingan hasil nilai *pre-test* dan *post-test* yang didapat oleh responden dapat dilihat pada Tabel 1.

Untuk terjadi peningkatan pemahaman, nilai rata-rata *post-test* seharusnya lebih tinggi dibanding dengan nilai rata-rata *pre-test.* Dari berpasangan nilai $\mu_1 - \mu_2 \neq 0$ maka diambil pengujian sisi kiri $\mu_1 - \mu_2 < 0$ sehingga $\mu_1 < \mu_2$. Pada Gambar 10 terlihat bahwa nilai t hitung bernilai -31,085, dimana nilai ini lebih kecil dibanding dengan nilai t tabel dengan df 39 dan α 0,05 (1.685). Berdasarkan hasil perhitungan nilai t hitung, nilai t hitung < t tabel maka H_0 ditolak dan H_a diterima. Sehingga dapat ditarik kesimpulan bahwa terdapat perbedaan signifikan terhadap nilai rata-rata *pre-test* dan *post-test* pada pengujian dengan taraf nyata sebesar 5%.

5. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa kesimpulan untuk menjawab rumusan masalah dalam penelitian ini:

a. IDS *Snort* dapat diintegrasikan dengan simulator ICS untuk melakukan deteksi serangan dan memberikan peringatan (*alert*) terhadap serangan yang ditujukan ke simulator. Pada penelitian ini IDS *Snort* berhasil memberikan *alert* terhadap serangan berupa *Injecting Malicious* Modbus *Command* dan *Uploading Malicious PLC Program.* Integrasi IDS dilakukan pada sisi router dikarenakan semua *traffic* jaringan akan melewati router. IDS *Snort* dapat menerima *alert* ketika terjadi serangan karena telah dilakukan konfigurasi *rules* pada *Snort.*
b. Berdasarkan hasil penilaian *pre-test* dan *post-test* taruna terhadap materi ICS dapat diketahui bahwa terdapat peningkatan pemahaman taruna Poltek SSN terhadap materi ICS.

Tabel 1. Hasil uji-t berpasangan

	Paired Differences					t	df	Sig (2-tailed)
	Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
				Lower	Upper			
Pair 1 Sebelum pembelajaran – Setelah pembelajaran	-63.50000	12.91987	2.04281	-67.63198	-59.36802	-31.085	39	.000

REFERENSI

[1] Direktorat Operasi Keamanan Siber BSSN, "Laporan Tahunan Monitoring Keamanan Siber 2021".

[2] V. Gkioulos And N. Chowdhury, "Cyber Security Training For Critical Infrastructure Protection: A Literature Review," *Computer Science Review*, Vol. 40. Elsevier Ireland Ltd, May 01, 2021. DOI: 10.1016/J.Cosrev.2021.100361.

[3] K. S. Robbani, A. H. Reksoprodjo, and B. Bastari, "PERLINDUNGAN INFRASTRUKTUR INFORMASI KRITIKAL NASIONAL SEKTOR KETENAGALISTRIKAN DARI ANCAMAN SIBER", PA, vol. 6, no. 1, Feb. 2020.

[4] M. Conti, D. Donadel, And F. Turrin, "A Survey On Industrial Control System Testbeds And Datasets For Security Research," Feb. 2021, DOI: 10.1109/Comst.2021.3094360.

[5] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, And M. Samaka, "Scada System Testbed For Cybersecurity Research Using Machine Learning Approach," *Future Internet*, Vol. 10, No. 8, Aug. 2018, DOI: 10.3390/Fi10080076.

[6] "Keamanan Siber – Politeknik Siber Dan Sandi Negara." https://poltekssn.ac.id/rks/ (Accessed Oct. 22, 2022).

[7] D. Formby, M. Rad, And R. Beyah, "Lowering The Barriers To Industrial Control System Security With GRFICS," 2018.

[8] G. Samrat Krishna, T. Srinivasa Ravi Kiran, And A. Srisaila, "Testing Performance Of Raspberrypi As Ids Using Snort," *Mater Today Proc*, Feb. 2021, DOI: 10.1016/J.Matpr.2021.01.607.

[9] "What Is Snort?" Https://Www.Snort.Org/Faq/What-Is-Snort (Accessed Oct. 22, 2022).

[10] G. K. Bada, W. K. Nabare, And D. K. K. Quansah, "Comparative Analysis Of The Performance Of Network Intrusion Detection Systems: Snort, Suricata And Bro Intrusion Detection Systems In Perspective," *Int J Comput Appl*, Vol. 176, No. 40, Pp. 39–44, Jul. 2020, DOI: 10.5120/Ijca2020920513.

[11] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, And A. Hahn, "Guide To Industrial Control Systems (ICS) Security," Gaithersburg, Md, Jun. 2015. DOI: 10.6028/Nist.Sp.800-82r2.

[12] A. Abou El Kalam, "Securing Scada And Critical Industrial Systems: From Needs To Security Mechanisms," *International Journal Of Critical Infrastructure Protection*, Vol. 32, Mar. 2021, DOI: 10.1016/J.Ijcip.2020.100394.

[13] D. Upadhyay And S. Sampalli, "Scada (Supervisory Control And Data Acquisition) Systems: Vulnerability Assessment And Security Recommendations," *Comput Secur*, Vol. 89, Feb. 2020, DOI: 10.1016/J.Cose.2019.101666.

[14] A. Ghaleb, S. Zhioua, And A. Almulhem, "On PLC Network Security," *International Journal Of Critical Infrastructure Protection*, Vol. 22, Pp. 62–69, Sep. 2018, DOI: 10.1016/J.Ijcip.2018.05.004.

[15] E. I. Evangelia, "Vulnerabilities Of The Modbus Protocol," 2018.

[16] C. Parian, T. Guldimann, And S. Bhatia, "Fooling The Master: Exploiting Weaknesses In The Modbus Protocol," In *Procedia Computer Science*, Elsevier B.V., 2020, Pp. 2453–2458. DOI: 10.1016/J.Procs.2020.04.265.

[17] B. Phillips, E. Gamess, And S. Krishnaprasad, "An Evaluation Of Machine Learning-Based Anomaly Detection In A Scada System Using The Modbus Protocol," In *Acmse 2020 - Proceedings Of The 2020 Acm Southeast Conference*, Association For Computing Machinery, Inc, Apr. 2020, Pp. 188–196. DOI: 10.1145/3374135.3385282.

[18] N. F. Ilxomovna, "Increasing the Effectiveness of Education and the Role of Interactive Medodes in Teaching the Subject of Batanics," Iqro Jurnali, vol. 2, no. 1, 2023, [Online]. Available: https://wordlyknowledge.uz/index.php/iqro/article/view/274

[20] E. Ukwandu *Et Al.*, "A Review Of Cyber-Ranges And Test-Beds: Current And Future Trends," *Sensors (Switzerland)*, Vol. 20, No. 24. Mdpi Ag, Pp. 1–36, Dec. 02, 2020. DOI: 10.3390/S20247148.

[21] N. R. Riyadi, "Pengujian Usability Untuk Meningkatkan Antarmuka Aplikasi Mobile Myumm Students," *Jurnal Sistemasi*, Vol. 8, Pp. 226–232, 2019.

[22] M. Nurmalasari, "Uji Beda Dua Rata-Rata Berpasangan (Uji T-Dependent)," in MODUL STATISTIK INFERENS (MIK 411), Jakarta, 2018, pp. 1–16. [Online]. Available: https://lms-paralel.esaunggul.ac.id/pluginfile.php?file=/44909/mod_resource/content/2/Modul2 MIK411 Uji T-Dependen.pdf