ANALISIS KEAMANAN JARINGAN PADA *SMART KWH METER* BERBASIS *INTERNET OF THINGS (IOT)*

NETWORK SECURITY ANALYSIS OF SMART KWH METER BASED ON INTERNET OF THINGS

Muhammad Farhan Fadhlulloh[1], Dr. Ir. Basuki Rahmat, M.T.[2], Arif Indra Irawan, S.T, M.T.[3]

[123]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

[1]fadhullohfarhan@gmail.com, [2]basukir@telkomuniversity.ac.id,
[3]arifirawan@telkomuniversity.ac.id

Abstrak

***IoT* atau *Internet of Things* merupakan jaringan yang dapat menghubungkan bermacam objek yang memiliki identitas pengenal serta alamat *IP*, sehingga dapat saling berkomunkasi dan bertukar informasi. Dalam simulasi rancangan keamanan jaringan listrik pintar ini penerapan *Smart KWH Meter* memanfaatkan koneksi jaringan internet dan menghubungkannya dengan *device* berupa *android* untuk menampilkan data daya yang dikonsumsi. Namun proses pengiriman informasi dengan memanfaatkan jaringan internet ke *device android* melalui *server firebase* tersebut terkadang tidak selalu berjalan dengan baik.**

Untuk menghindari serangan yang dapat menyebabkan kegagalan dalam pengiriman data tersebut. Dengan menggunakan perintah hping3 pada simulasi penyerangan *DOS attack* dan *Sniffing attack* menggunakan tools *Etttercap.*

Dari hasil penelitian dan analisis yang telah dilakukan dapat disimpulkan bahwa dengan menggunakan *IP tables* yang telah dikonfigurasi kemudian dilakukan pengujian dengan simulasi serangan *DOS attack* dan *Sniffing attack* dapat melindungi jaringan atau koneksi *Smart KWH Meter* pada saat proses pengiriman data menggunakan jaringan internet.

Kata Kunci: ***Internet of Things, Android, Firebase, Cyber Security, DOS Attack, Sniffing Attack,***

Abstract

IoT or the Internet of Things is a network that can link various objects that have identity identities and IP addresses, so they can connect to each other and exchange information. In this simulation of security design of smart electricity network, the implementation of Smart KWH Meter utilizes Internet connection and connect it with Android device to display the power data consumed. But the process of sending information by utilizing the Internet network to an Android device through the Firebase server is sometimes not always going well..

At the end of this task is implemented a network security system for the process of sending power usage data on Smart KWH meters. To avoid attacks that can cause failures in the transmission of such data. Using the hping3 command on the attack simulation DOS attack and Sniffing attack using Etttercap tools.

From the results of research and analysis that has been done it can be concluded that by using IP tables that have been configured and then tested with a DOS attack simulation and Sniffing attack can protect the network or Smart KWH Meter connection when sending data using the internet network.

Keywords: Internet of Things, Android, Firebase, Cyber Security, DOS Attack, Sniffing Attack.

1. Pendahuluan

Menyalurkan listrik dari pembangkit sampai dengan ke pelanggan banyak terjadi penyusutan daya. Pada saat pengiriman energi dari pembangkit listrik, lalu mengirimkannya melalui media transmisi daya dan sampai ke Gardu Induk (GI) PT. PLN (Persero.) Sudah dapat diketahui angka penyusutan daya, karena pengukuran dan pemantauan berjalan dengan baik. Namun pada saat distribusi dari GI sampai ke pelanggan rugi tidak dapat diketahui. Ditemukan kejadian penambahan daya listrik ilegal disekitar wilayah Jakarta dalam kejadian tersebut terjadi perbedaan kapasitas listrik seperti yang terdapat di daerah Johar Baru, dalam kapasitas resmi yang seharusnya tertera 450 *Voltampere(VA)* tetapi kenyataannya saat petugas PT. PLN(Persero) melakukan inspeksi dadakan, pemilik rumah menambahkan kapasitas daya menjadi 2200 VA tanpa sepengetahuan pihak PT. PLN(Persero) [7].

Kemajuan teknologi dibidang telekomunikasi khususnya internet oleh masyarakat sangat meningkat dan hampir dibutuhkan setiap saat. Sekarang banyak perangkat teknologi yang dapat terkoneksi dengan internet [6]. Menurut paper yang diterbitkan oleh *Electrical Engineering Department, UND, USA.* Meskipun *smart grid* mengatasi beberapa masalah jaringan tradisional, *smart grid* dapat menghadapi sejumlah tantangan dalam keamanan jaringan. Dikarenakan komunikasi telah dimasukan kedalam daya listrik dengan kelemahan bawaannya, sehingga memiliki banyak risiko [3]. Dalam tugas akhir ini dirancang suatu keamanan dan pertahanan jaringan pada sistem yang akan bekerja pada jaringan tenaga listrik pintar dirumah. Implementasi ini diharapkan dapat dijadikan sebuah solusi untuk melindungi server dari serangan *DOS attack* (*smurfing attack*) dan *Sniffing attack.*

Tinjauan Pustaka

2.1 Smart Grid

Perpindahan ke jaringan listrik pintar *(Smart Grid)* untuk mengubah seluruh model bisnis industri yang berhubungan dengan semua pemangku kepentingan, agar memengaruhi utilitas, regulator, penyedia layanan energi, vendor teknologi, dan, otomasi. Jaringan listrik pintar *(Smart Grid)* memungkinkan transformasi ini dengan membawa filosofi, konsep, dan teknologi yang memungkinkan jaringan listrik pintar *(Smart Grid)* dapat dihubungkan dengan internet [4].

Gambar 2. 1 Arsitektur Smart Grid

.

1.1 NodeMCU

NodeMCU merupakan papan rangkain elektronik yang didalamnya tersusun beberapa komponen utama, salah satunya *chip* mikrokontroler yang dikembangkan dengan berbasiskan modul *ESP8266*. Pada *NodeMCU* sudah terdapat pin - pin yang berfungsi layaknya sebuah mikrokontroller diantaranya pin *GPIO (General Purpose Input Output), PWM (Pulse Width Modulation), IIC, 1- Wire, ADC (Analog to Digital Converter* dan sudah terdapat modul *wireless* yang terintegrasi dengan *board NodeMCU* [8].

1.2 Internet Of Things (IOT)

Pada zaman sekarang *Internet of things (IoT)* terdapat di berbagai bidang. Pengertian Internet of Things pada akhirnya semakin banyak berkembang pada zaman sekarang. Belum ada artian secara sah yang membentuk konsep *Internet of Things (IoT)*. Pada dasarnya kata "*Things*" dalam artian *Internet of Things* adalah sesuatu objek. Objek tersebut dikembangkan dan ditelusuri potensinya untuk dihubungkan dengan internet sehingga dapat bermanfaat bagi aktivitas manusia. Sebuah konsep dimana objek memiliki kemampuan untuk mentransfer data melalui jaringan tanpa memerlukan interaksi manusia ke manusia atau manusia ke komputer disebut dengan Internet of Things. *IoT* telah berkembang dari konvergensi teknologi *nirkabel, micro-electromechanical systems (MEMS)*, dan Internet.

1.3 Cloud Computing

Cloud computing merupakan sebuah perpaduan dari pemanfaatan teknologi komputasi dan teknologi berbasis internet. Untuk dapat mengakses layanan yang terdapat di dalam cloud computing pengguna dapat menggunakan internet.

1.4 Firebase

Firebase adalah *Backend as a Service (BaaS)* yang sekarang dimiliki oleh google [1]. Salah satu penawaran dari google untuk menjadi solusi agar mempermudah developer yaitu *Firebase* merupakan salah satu yang ditawarkan dnegan solusi yang tersedia aplikasi dapat dibuat tanpa harus memikirkan pemrograman sisi *server* sehingga pembuatan aplikasi mejadi lebih mudah terselesaikan.

1.5 Hypertext Transfer Protocol Secure

Hypertext Transfer Protocol Secure memiliki pengertian yang sama dengan http hanya saja https memiliki kelebihan fungsi di bidang keamanan (secure). Dengan menggunakan Secure Socket Layer (SSL) atau Transport Layer Security (TLS) sebagai sublayer di bawah http aplikasi layer yang biasa. Teknologi https protokol mencegah kemungkinan "dicurinya" informasi penting yang dikirimkan selama proses komunikasi berlangsung antara user dengan web server atau sebaliknya.

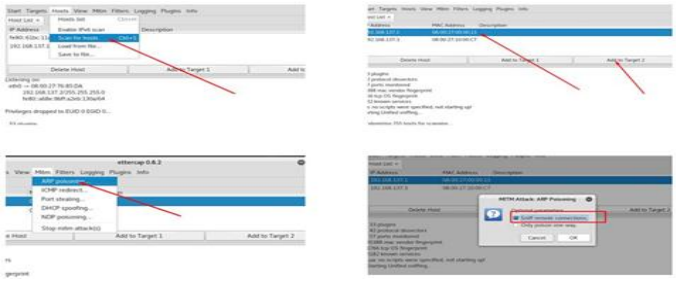
1.6 Keamanan Jaringan

Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang yang tidak bertanggung jawab. Segi-segi keamanan didefinisikan dari kelima pon ini [5].

a. Confidentiality Mensyaratkan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.
b. Integrity Mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang.
c. Availability Mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.
d. Authentication Mensyaratkan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.
e. Nonrepudiation Mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

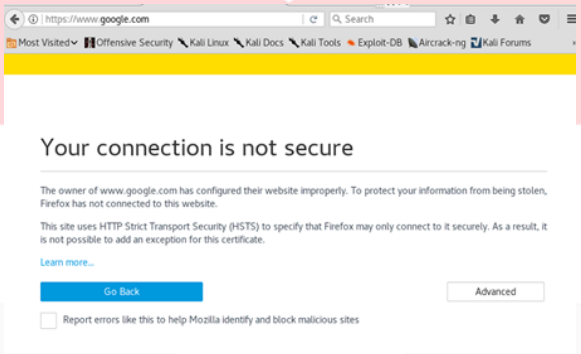
Sniifing Atttack

Sniffing attack adalah sebuah serangan pada keamanan jaringan dengan tujuan penyadapan yang memanfaatkan *mode premicious* pada port *Ethernet* jaringan komputer. Salah satu software yang biasa digunakan dalam proses sniffing yaitu menggunakan software ettercap. Ettercap merupakan sebuah tools packet sniffer yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan.



Gambar 2. 2 Sniffing Tools Ettercap

Gambar 2.4 Sniffing Tools Ettercap merupakan proses simulasi sniffing di ettercap. Dimulai dari pemilihan target dengan mengklik tab hosts dan lakukan *scan for host*. Setelah didapatkan address target kemudian dilakukan *sniffing* di ettercap menggunakan perintah ARP Poisonning.

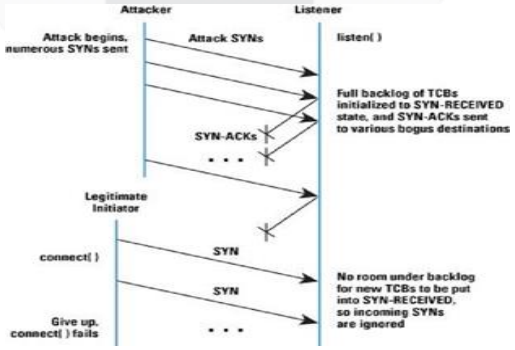


Gambar 2. 3 Hasil Sniffing di Web Browser

Gambar 2.5 Hasil Sniffing di Web Browser merupakan tampilan *web browser* yang terdeteksi tidak aman dikarenakan sniffing yang dilakukan pada tools ettercap sebelumnya. Jaringan yang tidak aman rentan akan peretasan dan sabotase dari pihak yang tidak memiliki wewenang. Peretasan dan sabotase tersebut dapat menyebabkan data-data penting yang dikirimkan hilang atau disabotase oleh pihak lain.

Denial Of Service

Denial of Service (DoS) merupakan serangan dimana suatu pihak mengekploitasi aspek dari suite Internet Protocol untuk menghalangi akses pihak yang berhak atas informasi atau sistem yang diserang. Contoh dari serangan ini salah satunya adalah TCP SYN.



Gambar 2. 4 Proses SYN FLOOD

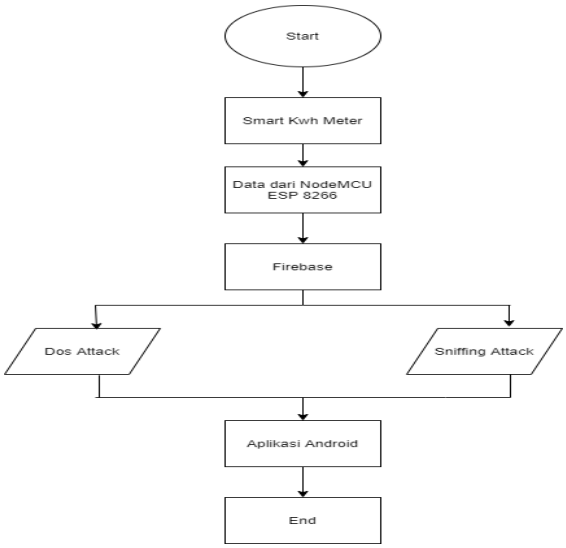
3. Perancangan Sistem

31 Desain Sistem

Peralatan elektronik yang memiliki alamat *IP* tersendiri akan sangat rawan terjadi gangguan keamanan. *Smart* KWH meter memiliki alamat IP, yang salah satunya berasal dari *Node MCU ESP 8266*. Maka dari itu diperlukan cara untuk melindungi smart KWH Meter agar tidak mudah diretas oleh pihak yang tidak memiliki wewenang. Pada *Smart* KWH meter yang akan dibuat dilakukan desain keamanan jaringan yang diuji dengan menggunakan teknik penyerangan *DOS attack* dan *Sniffing attack*.

3.2 Blok Diagram

Berikut merupakan diagram blok sistem Analisis Keamanan Jaringan Pada Smart Kwh Meter Berbasis Internet Of Things.

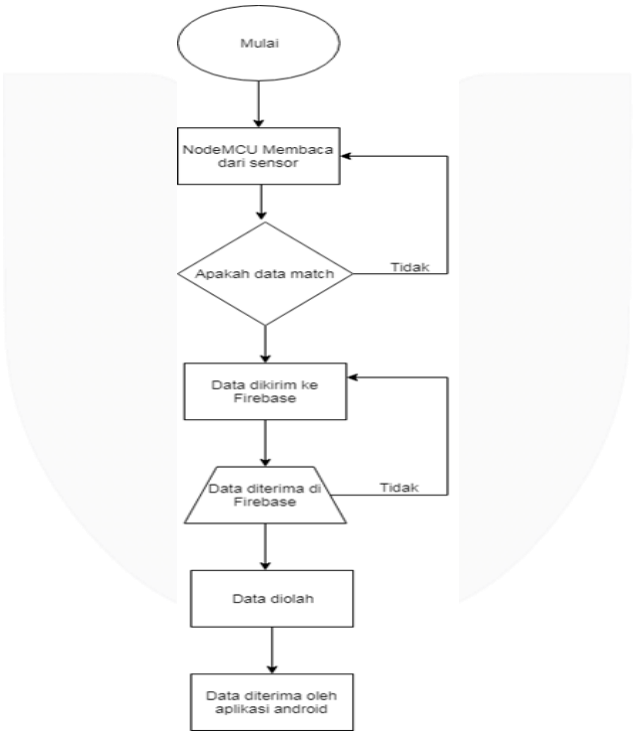


Gambar 3. 2 Diagram blok system

Secara Garis besar pada **Gambar 3.2** Data berupa daya kemudian dikirimkan ke perangkat android dengan memanfaatkan jaringan sistem IoT. Data berupa hasil daya tersebut kemudian disimpan dalam sebuah *cloud storage* dengan menggunakan *firebase* yang disediakan oleh penyedia layanan *search engine* yaitu google.

Pada proses percobaan *DOS Attack* menggunakan Hping 3 dimana proses tersebut merupakan sebuah peritah pengiriman data dalam jumlah yang banyak sehingga menyebabkan aktifitas *traffic* menjadi padat, hal tersebut membuat *DOS Attack* dapat dilakukan.

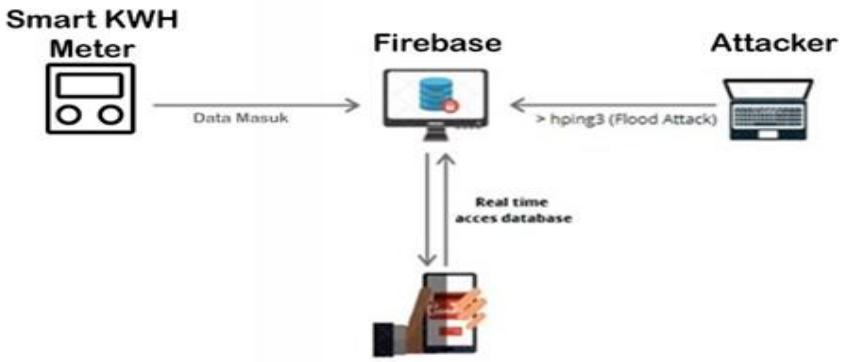
3.3 Diagram Alir Sistem



.

3.4 Skenario Pengujian Sistem

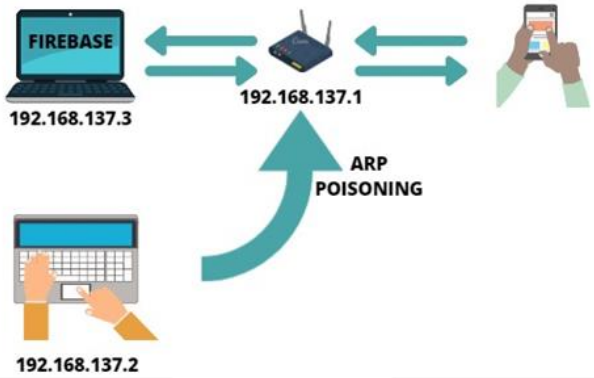
A. Skenario Pengujian



Gambar 3. 1 Skenario Pengujian

Gambar 3.3 Skenario Pengujian menjelaskan skema pengujian secara keseluruhan. Data yang didapatkan oleh *smart* Kwh akan dikirimkan ke Firebase. Firebase kemudian akan diserang oleh PC 2 (*attacker*) menggunakan serangan hping3 (flood attack). Perintah hping3 merupakan sebuah perintah untuk mengirimkan data dalam jumlah yang banyak sehingga menyebabkan aktifitas traffic menjadi padat dan membuat *user* tidak bisa memiliki akses kedalam *firebase*.

B. Skema Pengujian *Sniffing* di *Ettercap*



Gambar 3. 2 Skema Pengujian Sniffing

Gambar 3.4 menjelaskan skema pengujian *sniffing* menggunakan ettercap. Firebase dengan IP 192.168.137.3 yang terhubung dengan perangkat router (192.168.137.1) akan disadap oleh PC yang telah terpasang tools ettercap (192.168.137.2) dengan *command* ARP Poisoning di ettercap akan membuat router yang terhubung dengan firebase tidak dapat diakses secara aman oleh firebase tersebut. Sehingga menyebabkan device android atau smartphone mengalami kesulitan dalam mengakses firebase dikarenakan koneksi yang dibuat terdeteksi tidak aman oleh device android tersebut.

4. Hasil dan Analisis

4.1 Hasil Pengujian Jaringan Sebelum Menggunakan Rules IP Tables

Pada skema ini PC 1 yang berfungsi sebagai firebase tidak memiliki sistem keamanan jaringan. Hal ini ditunjukkan dari PC 1 yang tidak memiliki *rule* pada iptables. Tabel 4.1 dan Gambar 4.1 menjelaskan presentase penggunaan CPU 1 saat di *DOS attack* oleh PC 2 dalam keadaan tidak menggunakan *rules* pada IP Tables

Tabel 4. 1 Presentase Without Ip Tables

Without IP Tables Rules						
Time(s)	No Attack	100 packets	1000 packets	10000 packets	100000 packets	1000000 packets
0	0,30%	7,30%	7,50%	6,50%	5,80%	4,80%
5	0,20%	4,70%	4,70%	3,70%	4,00%	3,90%
10	0,50%	5,80%	6,70%	3,50%	6,70%	3,80%
15	0,53%	4,90%	6,40%	14,30%	3,90%	3,90%
20	0,43%	7,90%	5,80%	5,70%	6,00%	8,30%
25	0,73%	6,60%	7,50%	4,80%	3,80%	5,80%
30	0,33%	6,70%	4,80%	5,60%	5,40%	5,50%
35	0,93%	4,30%	4,80%	7,30%	4,90%	4,80%
40	0,03%	4,30%	4,80%	3,90%	4,80%	4,40%
45	0,13%	7,30%	6,80%	5,50%	6,70%	4,00%
55	0,23%	5,30%	5,80%	7,90%	8,60%	3,60%
60	0,33%	6,30%	4,80%	6,30%	10,50%	3,20%

Saat PC 1 di *DOS attack* oleh PC 2 dalam waktu sampling selama 1 menit dan di *capture* setiap interval 5 detik, didapatkan hasil berupa peningkatan penggunaan CPU PC 1. Pada skema pengujian pengiriman ICMP paket

sebanyak 100-1.000.000 packets, penggunaan CPU 1 mengalami peningkatan hingga 7,90%, 7,50%, 14,30, 10,50%, 8,30%.

4.2 Hasil Pengujian Jaringan Setelah Menggunakan Rulus IP Table

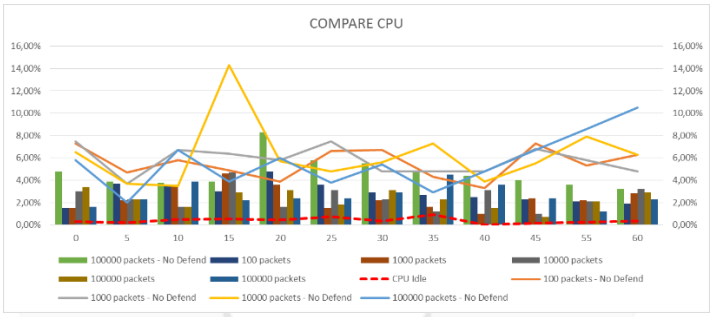
Tabel 4. 2 Presentase Penggunaan CPU 1

WITH RULE IN IPTABLES						
Time(s)	No Attack	100 packets	1000 packets	10000 packets	100000 packets	100000 packets
0	0,30%	1,50%	1,50%	3,00%	3,40%	1,60%
5	0,20%	3,70%	2,20%	2,30%	2,30%	2,30%
10	0,50%	3,60%	3,60%	1,60%	1,60%	3,90%
15	0,53%	3,00%	4,60%	4,70%	2,90%	2,20%
20	0,43%	4,80%	3,60%	1,60%	3,10%	2,40%
25	0,73%	3,60%	1,50%	3,10%	1,80%	2,40%
30	0,33%	2,90%	2,20%	2,30%	3,10%	2,90%
35	0,93%	2,70%	1,60%	1,20%	2,30%	4,50%
40	0,03%	2,50%	1,00%	3,10%	1,50%	3,60%
45	0,13%	2,30%	2,40%	1,00%	0,70%	2,40%
55	0,23%	2,10%	2,20%	2,10%	2,10%	1,20%
60	0,33%	1,90%	2,80%	3,20%	2,90%	2,30%

Pada skema ini PC 1 yang berfungsi sebagai firebase sudah memiliki sistem keamanan jaringan. Penggunaan IP Tables pada sistem jaringan bertujuan melindungi jaringan dari *address* yang tidak diinginkan. Tabel 4.2 dan Gambar 4.2 menjelaskan presentase penggunaan CPU 1 saat di *DOS attack* oleh PC 2 dalam keadaan menggunakan *rules* pada IP Tables.

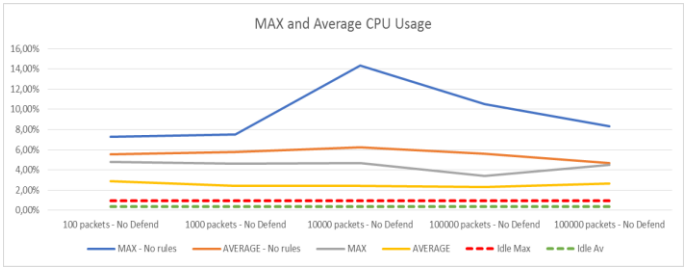
PC 1 yang sudah menggunakan IP Tables di *DOS attack* oleh PC 2 dalam waktu sampling selama 1 menit dan di *capture* setiap interval 5 detik, didapatkan hasil berupa penggunaan CPU PC 1. Pada skema pengujian pengiriman ICMP paket sebanyak 100-1.000.000 packets, penggunaan CPU 1 menjadi sebesar 4,80%, 4,60%, 4,70%, 3,40%, 4,50%.

4.3 Perbandingan Sebelum dan Setelah Menggunakan IP Tables



Gambar 4. 1 Penggunaan CPU Sebelum dan Setelah IP Tables

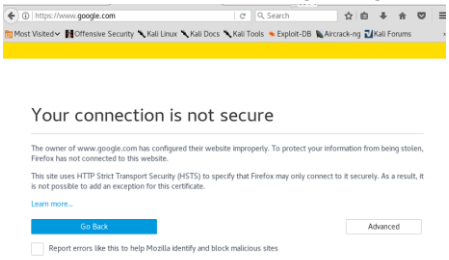
Gambar 4.3 menjelaskan perbandingan penggunaan CPU 1 saat diserang oleh PC 2 dalam keadaan sebelum dan sesudah menggunakan IP Tables. Terlihat adanya penurunan penggunaan CPU 1 yang signifikan saat pengiriman 100 ICMP packets di detik 20. CPU 1 mengalami penurunan yang awalnya sebesar 7,90% menjadi 4,80%. Terbukti dari Gambar 4.4 nilai maksimum dan rata-rata sesudah menggunakan IP Tables mengalami penurunan. Dapat disimpulkan bahwa penggunaan IP Tables pada sistem keamanan jaringan dapat melindungi jaringan *smart KWH* meter dari serangan DOS oleh IP address yang tidak dikenal



Gambar 4. 3 Nilai Maximum dan Rata rata

4.4 Hasil Pengujian Serangan Man in The Middle (ARP Posisoning) Menggunakan Tools Ettercap

Pada pengujian ini sudut yang dihasilkan adalah berdasarkan perhitungan trigonometri. Pengujian dilakukan dengan mengabaikan ukuran panjang dy. Pengujian dilakukan dengan mengggunakan lampu ukuran 50watt yang dipasang pada penyangga dengan tinggi penyangga 2m. Pada pengujian ini lampu digerakan setengah lingkaran.

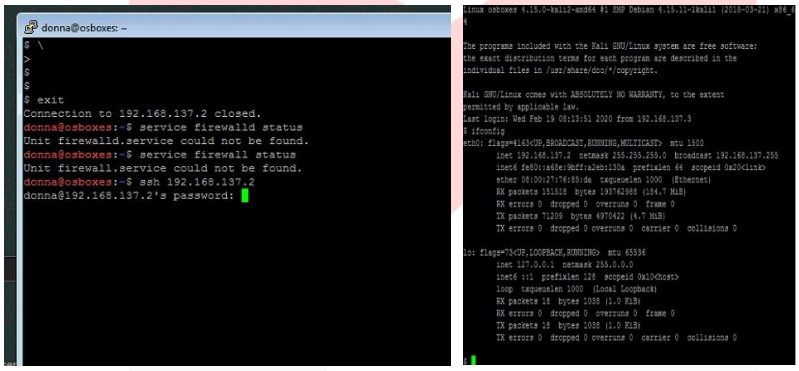


Gambar 4. 4 Firebase tidak dapat diakses

Gambar 4.5 merupakan tampilan *web browser* saat adanya serangan *man in the middle (sniffing)*. Serangan ini menyerang *gateway* sehingga pengguna tidak dapat mengakses server firebase yang terdapat di PC 1. Adanya serangan ini juga menyebabkan tidak adanya pertukaran informasi dikarenakan firebase tidak dapat menerima informasi yang dikirimkan oleh pengguna aplikasi.

4.5 Hasil Pengujian Serangan *Man In The Middle*

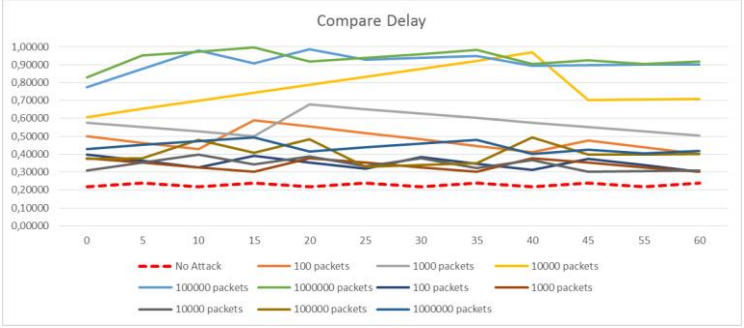
Pada pengujian ini dilakukan skema serangan *man in the middle* di antara koneksi PC 1 dan PC 2. Gambar 4.6 merupakan proses *sniffing* yang terjadi pada koneksi PC 1 dan PC 2.



Gambar 4. 2 Proses SSH di PC 2 dan Masuk Ke PC 1

Gambar 4. 3 Paket yang Terenkripsi Menggunakan SSH

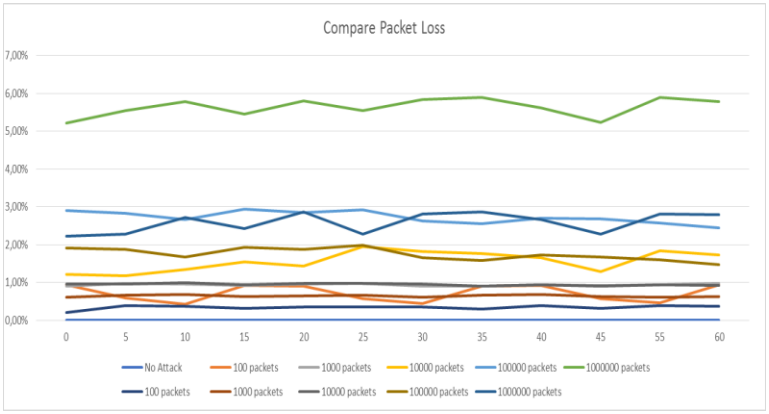
4.6 Hasil Pengujian Delay Jaringan



Gambar 4. 6 Perbandingan Delay Sebelum dan Setelah Menggunakan IP Tables

Berdasarkan Gambar 4.6 setelah sistem menggunakan rules IP Tables terjadi penurunan delay yang awalnya sebesar 0.47, 0.573,0.76,0.91,0.93 (s) menjadi 0.35, 0.33,0.34,0.40,0.44 (s). Walaupun dalam keadaan diserang dengan metode DOS, IP Tables dapat dijadikan sebuah solusi yang dapat melindungi jaringan dari penetrasi.

Hasil Pengujian Packet Loss Jaringan



Perbandingan *Packet Loss* Sebelum dan Setelah Menggunakan IP Tables

Berdasarkan Gambar 4.7 setelah sistem tidak menggunakan rules IP Tables terjadi penurunan delay yang awalnya sebesar 0.47, 0.573,0.76,0.91,0.93 (s) menjadi 0.35, 0.33,0.34,0.40,0.44 (s). Walaupun dalam keadaan diserang dengan metode DOS, IP Tables dapat dijadikan sebuah solusi yang dapat melindungi jaringan dari penetrasi.

5. Kesimpulan

Berdasarkan hasil pengujian dan analisa dapat di simpulkan sebagai berikut:

1. IP Tables dapat dijadikan sebuah solusi untuk melindungi sistem keamanan jaringan *smart kwh* meter.
2. Penggunaan IP Tables berhasil meredam serangan DOS, terbukti terjadi penurunan penggunaan CPU 1 yang signifikan saat pengiriman 100 ICMP packets di detik 20. Penggunaan CPU 1 mengalami penurunan yang awalnya sebesar 7,90% menjadi 4,80%.
3. Berdasarkan skema pengujian dengan mengirimkan 1000 ICMP packets didapatkan hasil berupa penurunan penggunaan CPU 1 di detik 25 yang awalnya sebesar 7,50% menjadi sebesar 1,50%.
4. Berdasarkan skema pengujian dengan mengirimkan 10000 ICMP packets didapatkan hasil berupa penurunan CPU 1 di detik 15 yang awalnya sebesar 14,30% menjadi sebesar 4,70%.
5. Didapatkan rata-rata penurunan penggunaan CPU 1 menggunakan semua skema sebesar 3,03%.
6. ARP Poisoning dapat dijadikan tools untuk skema penyerangan Man In The Middle. Hal ini dibuktikan dengan web browser yang tidak dapat diakses oleh pengguna aplikasi maupun firebase.

Daftar Pustaka

[1] K. M. Kumar, K. Akhi, S. K. Gunti and M. P. Reddy, "Implementing Smart Home Using Firebase," *International Journal of Research in Engineering and Applied Sciences (IJREAS)*, vol. 6, no. 10, pp. 193-198, 2016.

[2] Elmrabet Z, Electrical Engineering Department, UND, USA *Cyber-Security in Smart Grid: Survey and Challenges*

[3] Magnus Almgren, Davide Balzarotti, Marina Papatriantafilou and Valentin Tudor: Cyber Security in Smart Grid

[4] The Smart Grid: An introduction prepared for the U.S. Department of Energy by Litos Strategic Communication under contract No. DE-AC26-04NT41817, Subtask 560.01.04

[5] Robby C.," Jaringan Komunikasi Lanjut ", Gunadarma

[6] Ambarita Jurnaldo, Rancang Bangun Prototipe Smarthome Berbasis Internet Of Things cz (Iot) Menggunakan Aplikasi Blynk Dengan Modul ESP 8266, 2019

[7] Eko Pebrianto, "PLN Buru Rumah yang Tambah Daya Listrik Ilegal," Liputan 6,25 Maret, 2015.https://www.liputan6.com/bisnis/read/2196625/pln-buru-rumah-yang-tambahdaya-listrik-ilegal. [Diakses 26 September 2019 2015, 21:40 WIB].

[8] NodeMCU Data Sheet