Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 9, No. 11, November 2024

EVALUASI PENGUJIAN KEAMANAN ARSITEKTUR ZERO TRUST NETWORK PADA JARINGAN SMART HOME UNTUK MENGATASI SERANGAN DATA SNIFFING

Dwi Rizki Mugianto[1*], Rahmat Budiarto[2]
Universitas Mercu Buana, Jakarta, Indonesia[1,2]
Email: dwirizkimugianto62549@gmail.com[1], rahmat.budiarto@mercubuana.ac.id[2]

Abstrak

Keamanan jaringan Smart Home menjadi perhatian utama dalam menghadapi ancaman serangan data sniffing yang semakin meningkat. Penelitian ini bertujuan untuk mengevaluasi pengujian keamanan arsitektur Zero Trust Network pada jaringan Smart Home guna mengatasi risiko serangan data sniffing. Pendekatan Zero Trust Network diterapkan untuk meminimalkan potensi kerentanan sistem, dengan mendasarkan kepercayaan pada pengguna dan perangkat secara individual, bahkan dalam lingkungan internal. Metode penelitian melibatkan simulasi serangan data sniffing terhadap jaringan Smart Home yang diimplementasikan dengan arsitektur Zero Trust Network. Hasil penelitian ini diharapkan dapat memberikan wawasan mendalam tentang keamanan jaringan Smart Home dengan pendekatan Zero Trust Network, termasuk identifikasi potensi celah keamanan yang perlu diperbaiki. Penelitian ini memberikan kontribusi dalam pengembangan strategi keamanan yang lebih efektif untuk melindungi data sensitif di lingkungan Smart Home, menjadikannya lebih tahan terhadap serangan data sniffing, dan memberikan landasan untuk pengembangan lebih lanjut dalam mengamankan infrastruktur IoT di masa depan.

Kata Kunci: Data Sniffing, Metode Square, Internet of Things, Smart home, Zero trust network

Abstract

Smart Home network security is a major concern in facing the increasing threat of data sniffing attacks. This research aims to evaluate Zero Trust Network architecture security testing on Smart Home networks to overcome the risk of data sniffing attacks. The Zero Trust Network approach is implemented to minimize potential system vulnerabilities, by basing trust on individual users and devices, even within the internal environment. The research method involves simulating a data sniffing attack on a Smart Home network implemented with a Zero Trust Network architecture. It is hoped that the results of this research will provide in-depth insight into Smart Home network security using a Zero Trust Network approach, including identifying potential security gaps that need to be corrected. This research contributes to the development of more effective security strategies to protect sensitive data in Smart Home environments, making them more resilient to data sniffing attacks, and provides a foundation for further developments in securing IoT infrastructure in the future.

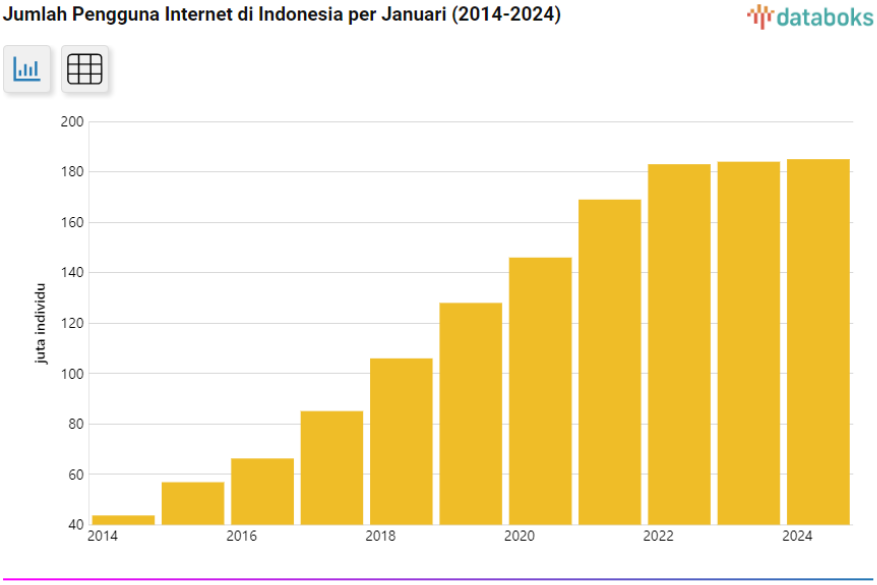
Keywords*: Data Sniffing, Square Method, Internet of Things, Smart home, Zero trust network*

Pendahuluan

Pertumbuhan jumlah pengguna internet di dunia saat ini terus bertambah. Meningkatnya jumlah pengguna internet di seluruhdunia menjadi tantangan bagi semua kalangan termasuk Indonesia, mengenai kebutuhan keamanan jaringan yang digunakan.

How to cite: Mugianto, D. R., & Budiarto, R. (2024). Evaluasi Pengujian Keamanan *Arsitektur Zero Trust Network* pada Jaringan *Smart Home* untuk Mengatasi Serangan Data Sniffing. *Syntax Literate. (9)11.* http://dx.doi.org/10.36418/syntax-literate.v9i11
E-ISSN: 2548-1398

Indonesia merupakan salah satu negara yang jumlah pengguna internetnya terus meningkat dan terus bertambah (Abu-Dabaseh & Alshammari, 2018; Amarudin, 2018; Deki & Fitri, 2018).



Gambar 1. Pengguna Internet di Indonesia (databoks)

Hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet (APJII) juga menunjukkan bahwa lebih dari separuh penduduk Indonesia kini sudah terkoneksi dengan internet. Pada Januari 2024 ada 185 juta individu pengguna internet di Indonesia, setara 66,5% dari total populasi nasional yang berjumlah 278,7 juta orang.

Produk *Internet of Things* yang paling terkenal adalah *smart city* dan *smart homes*. *Internet of Things* merupakan teknologi yang menghubungkan dunia nyata dan dunia maya, yang menjadikan teknologi tersebut menarik dalam membuat dunia menjadi lebih pintar (Esposito et al., 2018; Gunawan et al., 2021; He et al., 2022). Konsep *Internet of Things* adalah integrasi dari banyak teknologi yang berbeda. *Internet of Things* didukung oleh pengembangan *RFID*, sensor pintar, teknologi komunikasi, dan protokol Internet (Yudhanto & Azis, 2019).

Smarthome atau rumah pintar adalah sebuah konsep rumah yang menggunakan teknologi untuk mengontrol dan mengotomatisasi berbagai perangkat dan sistem di dalam rumah. Hal ini termasuk pencahayaan, sistem keamanan, termostat, peralatan rumah tangga, dan perangkat hiburan. Semua perangkat ini dapat diatur dan diawasi dari jarak jauh menggunakan smartphone, tablet, atau perangkat lainnya yang terhubung ke internet. Dalam evolusinya, Internet, *smartphone*, dan teknologi *machine-to-machine (M2M)* merupakan tahap pertama dari *Internet of Things* (Jaya, 2018; Kindervag et al., 2010; Rahmadhani & Widya Arum, 2022). Selanjutnya, *Internet of Things* diharapkan menjadi salah satu penghubung utama antara teknologi yang berbeda dengan menghubungkan objek fisik cerdas bersama-sama dan memungkinkan aplikasi yang berbeda untuk mendukung *smart decision making.* Teknologi perangkat elektronik saat ini yang biasa ditemui dan tergabung dalam *Internet of Things* adalah *smartphone*, tablet, komputer, *router*, dan *CCTV*, serta jenis perangkat elektronik berkemampuan jaringan lainnya yang dapat berkabel atau nirkabel untuk berbagi data atau *remote control* (Acar et al., 2020; Anagnostopoulos et al., 2020; Araya & Rifà-Pous, 2023).

Pertumbuhan pengguna internet di Indonesia meningkat berkat infrastruktur dan perangkat elektronik portabel, yang menguntungkan industri networking. Namun, peningkatan ini menimbulkan tantangan keamanan jaringan (Setayeshfar et al., 2022; Surahman et al., 2021). Kekhawatiran tentang privasi internet global juga meningkat. Di Indonesia, kekhawatiran serupa muncul setelah beberapa kasus peretasan, termasuk peretasan data Tiket.com yang merugikan Rp 1,9 miliar dan Telkomsel. Kasus ini menunjukkan pentingnya keamanan internet dan IoT.

Tujuan yang ingin dicapai dari penelitian ini adalah menemukan kerentanan, memberikan kategori dan prioritas keamanan dalam jaringan *Smarthome* baik di *Home Server* dan *Remote Server* dalam penerapan *Internet of Things (IoT).*

Metode Penelitian

Penelitian ini menggunakan pendekatan experimental research. Experimental research adalah penelitian yang bersifat sistematis, teliti, dan logis untuk melakukan kendali terhadap suatu kondisi. Peneliti memanipulasi stimuli, keadaan / kondisi eksperimental, serta mengobservasi pengaruh akibat perlakuan. Secara garis besar tujuan penelitian ini; pertama menguji hipotesis yang diajukan; kedua memprediksi kejadian dalam eksperimental; ketiga menarik generalisasi hubungan antarvariabel (Akbar et al., 2023). Penelitian ini menggunakan aplikasi Cisco Packet Tracer untuk membuat simulasi perangkat IoT smarthome ditambah instalasi Cisco Identity Service Engine untuk implementasi arsitektur ZTN. Beberapa perangkat smarthome yang disimulasikan antara lain lampu pintar, kamera keamanan, colokan pintar, dan smart door lock.

Metode SQUARE (Security Quality Requirements Engineering)

Analisis data juga mencakup hasil dari proses SQUARE yang digunakan untuk mengidentifikasi dan mengelaborasi kebutuhan keamanan jaringan Smart Home. Hasil analisis SQUARE mencakup:

a) Identifikasi Kebutuhan Keamanan: Berdasarkan proses Agree on Definition, Identify Security Goals, dan Develop Artifacts, telah diidentifikasi sejumlah kebutuhan keamanan yang spesifik, seperti perlindungan data pribadi dan perlindungan perangkat dari akses tidak sah.
b) Evaluasi Risiko: Melalui proses Perform Risk Assessment, risiko serangan Data Sniffing dievaluasi dan diberi prioritas untuk tindakan pengamanan yang sesuai.
c) Prioritisasi Kebutuhan: Proses Prioritize Requirement telah menghasilkan prioritas yang memandu implementasi kebutuhan keamanan sesuai tingkat risiko dan dampaknya.

Hasil dan Pembahasan

Dataset

Source IP,Destination IP,Source Port,Destination Port,Protocol,Packet Size
192.168.4.223,10.0.173.223,59289,15255,UDP,1489
192.168.108.113,10.0.50.83,28259,29774,TCP,1360
192.168.227.182,10.0.86.65,26920,28289,TCP,70
192.168.115.183,10.0.172.20,12092,55570,TCP,696
192.168.97.235,10.0.72.10,37709,24597,UDP,1094
192.168.191.6,10.0.221.8,15911,61114,UDP,1066
192.168.227.111,10.0.67.203,25304,8297,TCP,794
192.168.98.64,10.0.31.1,21938,54389,TCP,95

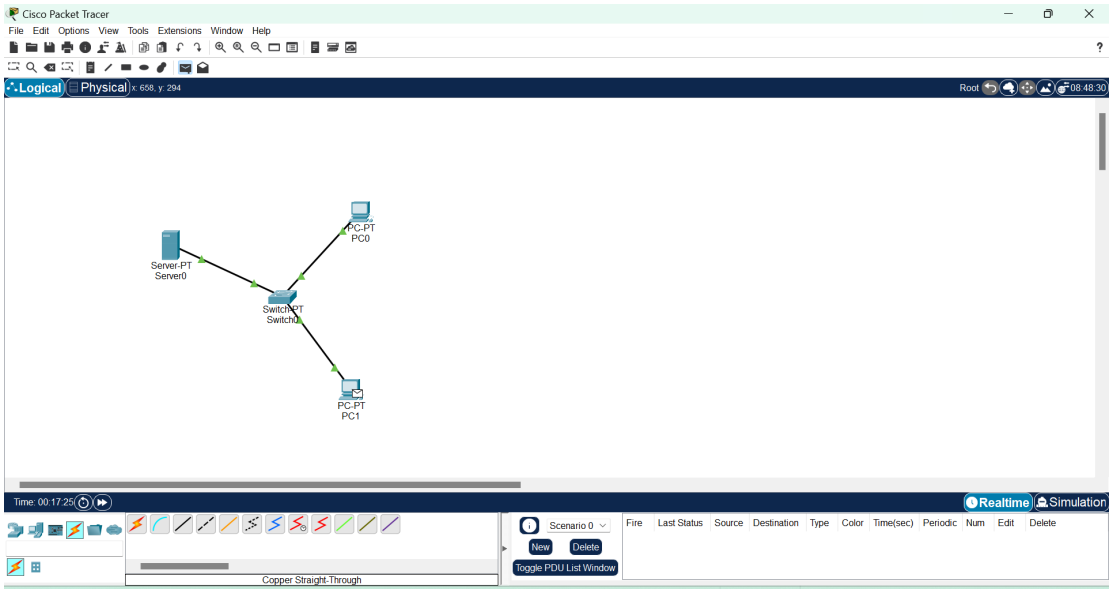
192.168.18.51,10.0.150.31,24381,55977,UDP,1064

Dataset ini terdiri dari 9 baris data yang masing-masing mewakili sebuah paket jaringan. Setiap baris memiliki enam atribut: Source IP, Destination IP, Source Port, Destination Port, Protocol, dan Packet Size. Source IP menunjukkan alamat IP pengirim paket, sementara Destination IP menunjukkan alamat IP penerima paket. Source Port dan Destination Port adalah nomor port yang digunakan oleh pengirim dan penerima, masing-masing. Protocol menunjukkan jenis protokol yang digunakan, seperti UDP atau TCP. Packet Size adalah ukuran paket dalam byte.

Pertama, paket pertama dikirim dari alamat IP 192.168.4.223 ke alamat IP 10.0.173.223 melalui UDP dengan ukuran 1489 byte. Paket kedua dikirim dari 192.168.108.113 ke 10.0.50.83 melalui TCP dengan ukuran 1360 byte. Paket ketiga dikirim dari 192.168.227.182 ke 10.0.86.65 melalui TCP dengan ukuran 70 byte. Paket keempat dikirim dari 192.168.115.183 ke 10.0.172.20 melalui TCP dengan ukuran 696 byte. Paket kelima dikirim dari 192.168.97.235 ke 10.0.72.10 melalui UDP dengan ukuran 1094 byte. Paket keenam dikirim dari 192.168.191.6 ke 10.0.221.8 melalui UDP dengan ukuran 1066 byte.

Selanjutnya, paket ketujuh dikirim dari 192.168.227.111 ke 10.0.67.203 melalui TCP dengan ukuran 794 byte. Paket kedelapan dikirim dari 192.168.98.64 ke 10.0.31.1 melalui TCP dengan ukuran 95 byte. Terakhir, paket kesembilan dikirim dari 192.168.18.51 ke 10.0.150.31 melalui UDP dengan ukuran 1064 byte. Dataset ini memberikan informasi tentang komunikasi jaringan antara berbagai host yang terlibat, termasuk alamat IP mereka, port yang digunakan, jenis protokol, dan ukuran paket yang dikirim.

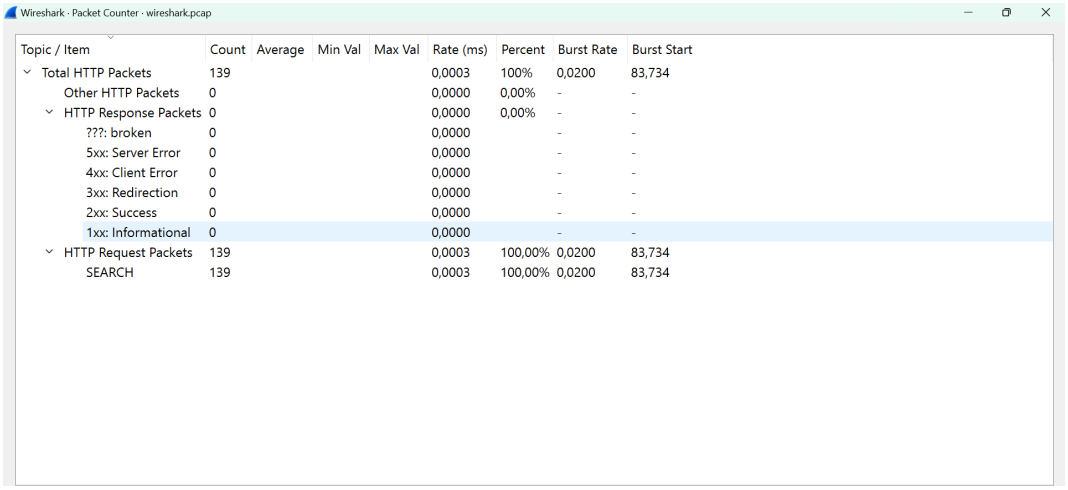
Cisco



Gambar 2. Cisco Paket Trace

Gambar di atas menunjukkan bahwa objek pintar tersebut adalah terkait dengan gateway rumah melalui media Nirkabel dan Kabel Ethernet untuk kendali lokal dan jarak jauh perangkat pintar. Portal beranda juga bertindak sebagai server yang memberikan IP alamat ke perangkat pintar apa pun yang terhubung.

Wireshark



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	139				0,0003	100%	0,0200	83,734
Other HTTP Packets	0				0,0000	0,00%	-	-
HTTP Response Packets	0				0,0000	0,00%	-	-
???: broken	0				0,0000		-	-
5xx: Server Error	0				0,0000		-	-
4xx: Client Error	0				0,0000		-	-
3xx: Redirection	0				0,0000		-	-
2xx: Success	0				0,0000		-	-
1xx: Informational	0				0,0000		-	-
HTTP Request Packets	139				0,0003	100,00%	0,0200	83,734
SEARCH	139				0,0003	100,00%	0,0200	83,734

Gambar 3. Wireshark

Arsitektur Zero Trust Network telah diuji dalam konteks jaringan smart home untuk mengatasi serangan data sniffing. Dalam skenario ketika perangkat diklasifikasikan sebagai aman, deteksi ancaman dilakukan terhadap IP Source tertentu yang mencurigakan.

Jumlah Serangan Selama 5 Menit

Jumlah serangan ada 40 serangan pada sistem yang terdeteksi dalam waktu 5 menit yang digunakan untuk melakukan capturing pada jaringan wireshark.Adapun data yang didapatkan selama capturing ialah sebagai berikut ini:

Serangan yang terdeteksi:
Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 51.11.192.49
Sumber Port: 53970
Tujuan Port: 443
Waktu: Jun 9, 2024 23:50:50.151735000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.1.25
Sumber Port: 53976
Tujuan Port: 7680
Waktu: Jun 9, 2024 23:51:41.744245000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.1.25
Sumber Port: 53976
Tujuan Port: 7680
Waktu: Jun 9, 2024 23:51:42.752725000 SE Asia Standard Time

Jenis Serangan: SYN Flood

Sumber IP: 192.168.100.237
Tujuan IP: 192.168.1.25
Sumber Port: 53976
Tujuan Port: 7680
Waktu: Jun 9, 2024 23:51:44.758991000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.1.25
Sumber Port: 53976
Tujuan Port: 7680
Waktu: Jun 9, 2024 23:51:48.771557000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.1.25
Sumber Port: 53976
Tujuan Port: 7680
Waktu: Jun 9, 2024 23:51:56.773714000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 53977
Tujuan Port: 53
Waktu: Jun 9, 2024 23:52:09.381043000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 53978
Tujuan Port: 53
Waktu: Jun 9, 2024 23:52:09.381195000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 53979
Tujuan Port: 53
Waktu: Jun 9, 2024 23:52:09.596951000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 53980
Tujuan Port: 53
Waktu: Jun 9, 2024 23:52:09.597480000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 53981
Tujuan Port: 53
Waktu: Jun 9, 2024 23:52:11.701699000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 53982
Tujuan Port: 53
Waktu: Jun 9, 2024 23:52:11.702125000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 53983
Tujuan Port: 53
Waktu: Jun 9, 2024 23:52:11.913504000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 53984
Tujuan Port: 53
Waktu: Jun 9, 2024 23:52:11.913819000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 35.186.224.24
Sumber Port: 53990
Tujuan Port: 443
Waktu: Jun 9, 2024 23:52:55.398530000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 45.121.219.184
Sumber Port: 53991
Tujuan Port: 443
Waktu: Jun 9, 2024 23:52:55.433809000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 20.189.172.33
Sumber Port: 53993
Tujuan Port: 443
Waktu: Jun 9, 2024 23:53:00.517189000 SE Asia Standard Time

Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.12.235
  Sumber Port: 53994
  Tujuan Port: 7680
  Waktu: Jun 9, 2024 23:53:01.764818000 SE Asia Standard Time
---
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.12.235
  Sumber Port: 53994
  Tujuan Port: 7680
  Waktu: Jun 9, 2024 23:53:02.777061000 SE Asia Standard Time
---
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.12.235
  Sumber Port: 53994
  Tujuan Port: 7680
  Waktu: Jun 9, 2024 23:53:04.783747000 SE Asia Standard Time
---
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.12.235
  Sumber Port: 53994
  Tujuan Port: 7680
  Waktu: Jun 9, 2024 23:53:08.790813000 SE Asia Standard Time
---
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.100.1
  Sumber Port: 53995
  Tujuan Port: 53
  Waktu: Jun 9, 2024 23:53:09.419137000 SE Asia Standard Time
---
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.100.1
  Sumber Port: 53996
  Tujuan Port: 53
  Waktu: Jun 9, 2024 23:53:09.419360000 SE Asia Standard Time
---
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.100.1
  Sumber Port: 53997
  Tujuan Port: 53

Waktu: Jun 9, 2024 23:53:09.632491000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 53998
Tujuan Port: 53
Waktu: Jun 9, 2024 23:53:09.632829000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 52.123.253.211
Sumber Port: 53999
Tujuan Port: 443
Waktu: Jun 9, 2024 23:53:11.049662000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 52.123.253.211
Sumber Port: 54000
Tujuan Port: 443
Waktu: Jun 9, 2024 23:53:11.342956000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.12.235
Sumber Port: 53994
Tujuan Port: 7680
Waktu: Jun 9, 2024 23:53:16.792686000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 54005
Tujuan Port: 53
Waktu: Jun 9, 2024 23:53:39.356533000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 54006
Tujuan Port: 53
Waktu: Jun 9, 2024 23:53:39.356790000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 54007

```
  Tujuan Port: 53
  Waktu: Jun  9, 2024 23:53:39.401679000 SE Asia Standard Time
----------
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.100.1
  Sumber Port: 54008
  Tujuan Port: 53
  Waktu: Jun  9, 2024 23:53:39.401951000 SE Asia Standard Time
----------
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.100.1
  Sumber Port: 54009
  Tujuan Port: 53
  Waktu: Jun  9, 2024 23:53:39.567186000 SE Asia Standard Time
----------
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.100.1
  Sumber Port: 54010
  Tujuan Port: 53
  Waktu: Jun  9, 2024 23:53:39.567491000 SE Asia Standard Time
----------
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.100.1
  Sumber Port: 54011
  Tujuan Port: 53
  Waktu: Jun  9, 2024 23:53:39.613025000 SE Asia Standard Time
----------
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.100.1
  Sumber Port: 54012
  Tujuan Port: 53
  Waktu: Jun  9, 2024 23:53:39.613344000 SE Asia Standard Time
----------
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.100.1
  Sumber Port: 54013
  Tujuan Port: 53
  Waktu: Jun  9, 2024 23:53:41.722647000 SE Asia Standard Time
----------
Jenis Serangan: SYN Flood
  Sumber IP: 192.168.100.237
  Tujuan IP: 192.168.100.1
```

Sumber Port: 54014
Tujuan Port: 53
Waktu: Jun 9, 2024 23:53:41.723025000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 54016
Tujuan Port: 53
Waktu: Jun 9, 2024 23:53:41.935840000 SE Asia Standard Time

Jenis Serangan: SYN Flood
Sumber IP: 192.168.100.237
Tujuan IP: 192.168.100.1
Sumber Port: 54017
Tujuan Port: 53
Waktu: Jun 9, 2024 23:53:41.936263000 SE Asia Standard Time

Hasil serangan yang terdeteksi menunjukkan berbagai insiden SYN flood dengan detail seperti jenis serangan, alamat IP sumber dan tujuan, port sumber dan tujuan, serta waktu serangan terjadi. Semua serangan yang terdeteksi adalah SYN flood yang merupakan jenis serangan DoS (Denial of Service) yang berusaha menghabiskan sumber daya server target dengan mengirimkan sejumlah besar paket SYN tanpa melanjutkan proses tiga langkah handshake TCP. Berikut adalah ringkasan hasil serangan yang terdeteksi:

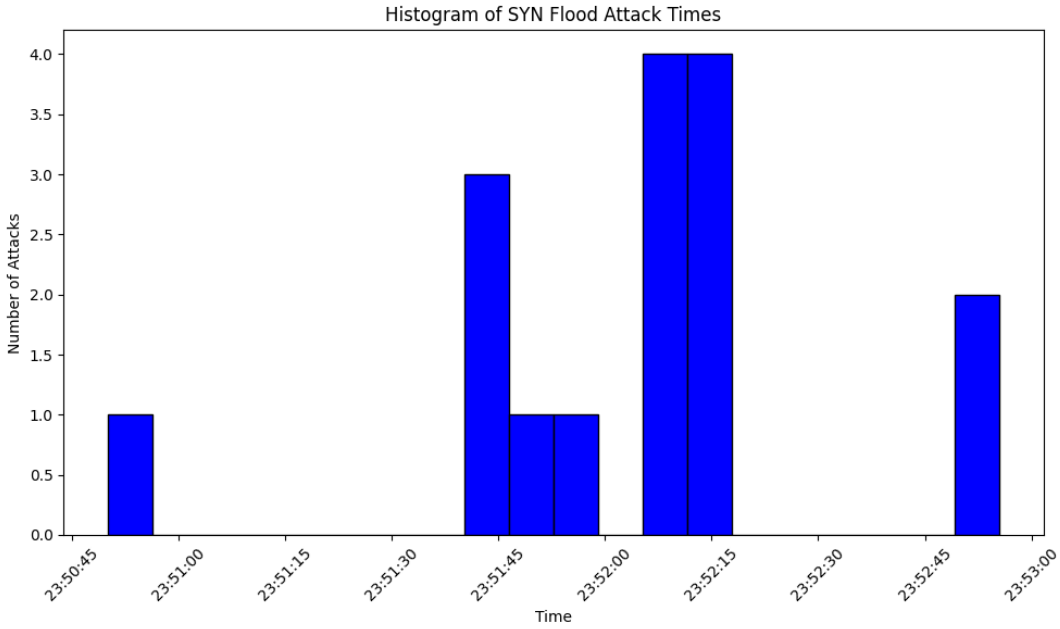
Serangan yang Terdeteksi:

1. **SYN Flood**
   - **Sumber IP**: 192.168.100.237
   - **Tujuan IP**: 51.11.192.49
   - **Sumber Port**: 53970
   - **Tujuan Port**: 443
   - **Waktu**: Jun 9, 2024 23:50:50.151735000 SE Asia Standard Time
2. **SYN Flood**
   - **Sumber IP**: 192.168.100.237
   - **Tujuan IP**: 192.168.1.25
   - **Sumber Port**: 53976
   - **Tujuan Port**: 7680
   - **Waktu**: Jun 9, 2024 23:51:41.744245000 SE Asia Standard Time
3. **SYN Flood**
   - **Sumber IP**: 192.168.100.237
   - **Tujuan IP**: 192.168.1.25
   - **Sumber Port**: 53976
   - **Tujuan Port**: 7680
   - **Waktu**: Jun 9, 2024 23:51:42.752725000 SE Asia Standard Time
4. **SYN Flood**
   - **Sumber IP**: 192.168.100.237
   - **Tujuan IP**: 192.168.1.25

- **Sumber Port**: 53976
- **Tujuan Port**: 7680
- **Waktu**: Jun 9, 2024 23:51:44.758991000 SE Asia Standard Time

5. **SYN Flood**
   - **Sumber IP**: 192.168.100.237
   - **Tujuan IP**: 192.168.1.25
   - **Sumber Port**: 53976
   - **Tujuan Port**: 7680
   - **Waktu**: Jun 9, 2024 23:51:48.771557000 SE Asia Standard Time
6. **SYN Flood**
   - **Sumber IP**: 192.168.100.237
   - **Tujuan IP**: 192.168.1.25
   - **Sumber Port**: 53976
   - **Tujuan Port**: 7680
   - **Waktu**: Jun 9, 2024 23:51:56.773714000 SE Asia Standard Time
7. **SYN Flood**
   - **Sumber IP**: 192.168.100.237
   - **Tujuan IP**: 192.168.100.1
   - **Sumber Port**: 53977
   - **Tujuan Port**: 53
   - **Waktu**: Jun 9, 2024 23:52:09.381043000 SE Asia Standard Time
8. **SYN Flood**
   - **Sumber IP**: 192.168.100.237
   - **Tujuan IP**: 192.168.100.1
   - **Sumber Port**: 53978
   - **Tujuan Port**: 53
   - **Waktu**: Jun 9, 2024 23:52:09.381195000 SE Asia Standard Time
9. **SYN Flood**
   - **Sumber IP**: 192.168.100.237
   - **Tujuan IP**: 192.168.100.1
   - **Sumber Port**: 53979
   - **Tujuan Port**: 53
   - **Waktu**: Jun 9, 2024 23:52:09.596951000 SE Asia Standard Time
10. **SYN Flood**
    - **Sumber IP**: 192.168.100.237
    - **Tujuan IP**: 192.168.100.1
    - **Sumber Port**: 53980
    - **Tujuan Port**: 53
    - **Waktu**: Jun 9, 2024 23:52:09.597480000 SE Asia Standard Time

Dan seterusnya, dengan pola serangan yang sama dari alamat IP sumber yang sama menuju berbagai alamat IP tujuan pada port yang bervariasi.



Gambar 4. Serangan Wireshark

```
if dst_port == 53706:
        threats.append({
            "issue": "Suspicious Destination Port",
            "src_ip": assets['src_ip'],
            "src_port": src_port,
            "dst_ip": assets['dst_ip'],
            "dst_port": dst_port,
            "length": length,
            "description": "Packet sent to a suspicious destination port"
        })
```

Metode SQUARE (Security Quality Requirements Engineering) adalah pendekatan yang sistematis untuk mengidentifikasi dan mengelola kebutuhan keamanan dalam suatu proyek. Dalam konteks analisis jaringan, penerapannya mencakup beberapa tahapan utama: identifikasi aset, identifikasi ancaman, analisis risiko, penentuan persyaratan keamanan, dan dokumentasi hasil. Dalam analisis file PCAP yang telah dilakukan, kita telah mengidentifikasi paket-paket yang mencurigakan berdasarkan port tujuan yang tidak biasa, yaitu port 53706. Setiap paket yang menuju ke port ini diidentifikasi sebagai potensi ancaman karena port tersebut dianggap tidak biasa atau mencurigakan.

Tahap pertama dalam metode SQUARE adalah identifikasi aset. Dalam analisis ini, aset utama yang diidentifikasi adalah alamat IP sumber dan tujuan dari paket-paket jaringan. Aset ini penting karena mereka merupakan titik awal dan tujuan komunikasi dalam jaringan, yang dapat mengindikasikan sumber dan target potensial dari suatu serangan. Pada kasus ini, aset yang diidentifikasi adalah IP sumber **74.125.24.102** dan IP tujuan **192.168.100.191**. Identifikasi aset ini membantu dalam memahami konteks di mana ancaman keamanan mungkin muncul.

Tahap kedua adalah identifikasi ancaman. Ancaman keamanan diidentifikasi berdasarkan pola lalu lintas yang mencurigakan. Dalam contoh ini, semua paket yang dikirim ke port tujuan 53706 dianggap sebagai ancaman. Hal ini didasarkan pada aturan

yang telah ditentukan bahwa penggunaan port tujuan tersebut tidak biasa dan mencurigakan. Dengan menggunakan metode SQUARE, kita dapat mendefinisikan aturan dan pola yang dapat digunakan untuk mengidentifikasi ancaman dalam lalu lintas jaringan. Setiap paket yang memenuhi kriteria ini dicatat sebagai potensi ancaman.

Tahap ketiga adalah analisis risiko. Dalam analisis risiko, setiap ancaman yang telah diidentifikasi dievaluasi untuk menentukan tingkat risiko yang dihadapinya. Faktor-faktor seperti frekuensi kemunculan ancaman dan potensi dampak pada aset yang dilindungi dipertimbangkan. Dalam hasil analisis ini, terdapat banyak entri yang menunjukkan paket yang menuju ke port 53706. Meski port ini mencurigakan, frekuensi kemunculan yang tinggi menunjukkan bahwa ancaman tersebut berulang kali muncul, menandakan adanya pola serangan atau aktivitas yang terus-menerus.

Tahap keempat adalah penentuan persyaratan keamanan. Berdasarkan analisis ancaman dan risiko, persyaratan keamanan dapat ditentukan untuk melindungi aset yang diidentifikasi. Dalam hal ini, salah satu persyaratan keamanan yang dapat disarankan adalah pemantauan dan pembatasan lalu lintas ke port tujuan yang mencurigakan seperti 53706. Firewall atau sistem deteksi intrusi dapat dikonfigurasi untuk memblokir atau memperingatkan administrator jaringan tentang paket-paket yang mencoba mengakses port ini. Dengan menentukan persyaratan ini, organisasi dapat mengimplementasikan langkah-langkah yang proaktif untuk mengurangi risiko.

Tahap terakhir adalah dokumentasi hasil. Hasil analisis yang mencakup identifikasi aset, ancaman, risiko, dan persyaratan keamanan harus didokumentasikan dengan baik. Dokumentasi ini penting untuk referensi di masa mendatang dan untuk memastikan bahwa semua pihak yang terkait memahami dan menyetujui langkah-langkah keamanan yang diambil. Dalam analisis ini, hasil-hasil yang telah disimpan ke dalam file JSON memberikan catatan yang jelas dan terstruktur tentang paket-paket yang mencurigakan.

Kesimpulan

Jaringan mengalami serangan SYN Flood yang berasal dari IP 192.168.100.237, menargetkan beberapa IP berbeda dalam kurun waktu 5 menit dengan total 40 serangan. Serangan ini berpotensi mengganggu konektivitas dan kinerja jaringan. Untuk mengatasinya, diterapkan arsitektur Zero Trust Network yang mendeteksi dan mengisolasi perangkat yang mencurigakan, serta menerapkan langkah-langkah keamanan yang tepat. Selain itu, dilakukan pemantauan lalu lintas ke port tujuan yang mencurigakan dan diterapkan aturan firewall untuk memperkuat keamanan. Upaya mitigasi ini didukung oleh analisis risiko dan dataset yang berisi informasi komunikasi jaringan antar host.

Penerapan arsitektur Zero Trust Network, pemantauan lalu lintas, dan aturan firewall terbukti efektif dalam memerangi serangan SYN Flood dan meningkatkan postur keamanan jaringan. Implementasi ini membantu melindungi jaringan dari serangan serupa di masa depan dan menjaga kelancaran operasi.

BIBLIOGRAFI

Abu-Dabaseh, F., & Alshammari, E. (2018). *Automated Penetration Testing : An Overview*. https://doi.org/10.5121/csit.2018.80610

Acar, A., Fereidooni, H., Abera, T., Sikder, A. K., Miettinen, M., Aksu, H., Conti, M., Sadeghi, A. R., & Uluagac, S. (2020). Peek-a-boo: I see your smart home activities, even encrypted! *WiSec 2020 - Proceedings of the 13th ACM Conference on*

Security and Privacy in Wireless and Mobile Networks. https://doi.org/10.1145/3395351.3399421

Akbar, R., Weriana, Siroj, R. A., & Afgani, M. W. (2023). Experimental Reseacrch Dalam Metodologi Pendidikan. *Jurnal Ilmiah Wahana Pendidikan, Januari*, *2023*(2), 465–474.

Amarudin, A. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal Teknoinfo*, *12*(2). https://doi.org/10.33365/jti.v12i2.121

Anagnostopoulos, M., Spathoulas, G., Viaño, B., & Augusto-Gonzalez, J. (2020). Tracing your smart-home devices conversations: A real world iot traffic data-set. *Sensors (Switzerland)*, *20*(22). https://doi.org/10.3390/s20226600

Araya, J. I. I., & Rifà-Pous, H. (2023). Anomaly-based cyberattacks detection for smart homes: A systematic literature review. In *Internet of Things (Netherlands)* (Vol. 22). https://doi.org/10.1016/j.iot.2023.100792

Deki, P., & Fitri, A. (2018). Pengaruh Penggunaan Simulasi Jaringan Komputer Cisco Packet Tracker Terhadap Kreativitas Belajar Siswa. *Jurnal Teknologi Pendidikan*, *3*.

Esposito, D., Rennhard, M., Ruf, L., & Wagner, A. (2018). Exploiting the potential of web application vulnerability scanning. *ICIMP 2018 the Thirteenth International Conference on Internet Monitoring and Protection, Barcelona, Spain, 22-26 July 2018*, *c*.

Gunawan, I. M. A. O., Indrawan, G., & Sariyasa, S. (2021). Pengembangan Sistem Informasi Kemajuan Akademik Menggunakan Model Incremental Berbasis Evaluasi Usability Dan White Box Testing. *SINTECH (Science and Information Technology) Journal*, *4*(1). https://doi.org/10.31598/sintechjournal.v4i1.661

He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing*, *2022*. https://doi.org/10.1155/2022/6476274

Jaya, T. S. (2018). Pengujian Aplikasi dengan Metode Blackbox Testing Boundary Value Analysis (Studi Kasus: Kantor Digital Politeknik Negeri Lampung). *Jurnal Informatika: Jurnal Pengembangan IT*, *3*(1). https://doi.org/10.30591/jpit.v3i1.647

Kindervag, J., Balaouras, S., & Coit, L. (2010). Build Security Into Your Network's DNA: The Zero Trust Network Architecture. *Security & Risk Professionals - Forrester Research*.

Rahmadhani, V., & Widya Arum. (2022). Literature Review Internet Of Think (Iot): Sensor, Konektifitas Dan QR Code. *Jurnal Manajemen Pendidikan Dan Ilmu Sosial*, *3*(2). https://doi.org/10.38035/jmpis.v3i2.1120

Setayeshfar, O., Subramani, K., Yuan, X., Dey, R., Hong, D., Kim, I. K., & Lee, K. H. (2022). Privacy invasion via smart-home hub in personal area networks. *Pervasive and Mobile Computing*, *85*. https://doi.org/10.1016/j.pmcj.2022.101675

Surahman, A., Aditama, B., Bakri, M., & Rasna, R. (2021). Sistem Pakan Ayam Otomatis Berbasis Internet Of Things. *Jurnal Teknologi Dan Sistem Tertanam*, *2*(1). https://doi.org/10.33365/jtst.v2i1.1025

Yudhanto, Y., & Azis, A. (2019). *Pengantar Teknologi Internet of Things (IoT)*. UNSPress.