CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 4, No. 2, November 2021, hlm. 87-95

UJI KERENTANAN SMART HOME MENGGUNAKAN METODE SQUARE UNTUK MENDUKUNG SMART CAMPUS

Arini[1], Nurul Faizah Rozy[2], Iik Muhamad Malik Matin[3]

[1,2,3]Teknik Informatika, Fakultas Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta

E-mail: [1]arini@uinjkt.ac.id, [2]nurulfaizah@uinjkt.ac.id,[3]iikmuhamadmalikmatin@gmail.com

Abstrak

Kampus sebagai penyelenggara pendidikan tinggi dituntut dapat bertransformasi untuk meningkatkan kualitas pendidikan dengan pendekatan teknologi. *Smart campus* merupakan teknologi yang dapat mengintegrasikan proses bisnis organisasi seperti pembelajaran, manajemen perpustakaan, dan manajemen kampus lainnya. *Smart campus* dapat diintegrasikan dengan *smart home*. Perangkat-perangkat *smart home* seperti *gadget, laptop, speaker* yang dapat dikontrol secara otomatis dapat menunjang kegiatan akademik. Namun keamanan menjadi hal yang krusial. Kampus sebagai penyedia layanan akademik harus menjamin keamanan informasi demi keberlangsungan kegiatan akademik. Untuk itu diperlukan suatu uji kerentanan pada *smarthome* untuk mendukung *smart campus* untuk menjamin keamanan proses bisnis organisasi. Penelitian ini kami melakukan pengujian kerentanan pada *smarthome* menggunakan metode SQUARE. Pengujian menargetkan pada teknologi *teleconference* dan *e-learning.* Hasil penelitian ini menunjukan terdapat kerentanan yang dapat diekploitasi enggunakan tenik *DoS, Man in the middle attack*, *port scanning,* dan *brute force*. Selain itu kami menentapkan rekomendasi yaitu melakukan penerapan protokol yang memiliki mekanisme enkripsi, penerapan IP dan MAC a*ddress filtering*, penerapan *firewall*, penerapan perangkat keamanan, dan mengubah password secara berkala.

Kata kunci: *Smart home, Smart campus, SQUARE.*

SMART HOME VULNERABILITY TEST USING THE SQUARE METHOD TO SUPPORT SMART CAMPUS

Abstract

Campuses as providers of higher education are required to be able to transform to improve the quality of education with a technological approach. Smart campus is a technology that can integrate organizational business processes such as learning, library management, and other campus management. Smart campus can be integrated with smart home. Smart home devices such as gadgets, laptops, speakers that can be controlled automatically can support academic activities. But security is crucial. Campuses as academic service providers must ensure information security for the continuity of academic activities. For that we need a vulnerability test on smarthomes to support smart campuses to ensure the security of the organization's business processes. In this study, we conducted vulnerability testing on smarthomes using the SQUARE method. The test targets teleconference and e-learning technology. The results of this study indicate that there are vulnerabilities that can be exploited using DoS techniques, Man in the middle attack, port scanning, and brute force. In addition, we make recommendations, namely implementing protocols that have encryption mechanisms, implementing IP and MAC address filtering, implementing firewalls, implementing security devices, and changing passwords regularly..

Keywords: *Smart home, Smart campus, SQUARE*

1. PENDAHULUAN

Pada tahun 2021 APJII merilis peningkatan yang siginifikan terhadap penetrasi internet setiap tahunnya di Indonesia. Hal ini dipengaruhi beberapa faktor seperti kebutuhan akan layanan pendidikan yang berbasis online juga pekerjaan atau aktivitas lain secara virtual, layanan medis, *e-commerce* dan lain-lain ((APJII), 2021).

Secara infrastruktur hal tersebut dipicu juga oleh perkembangan *Internet of Thing* (IoT) yang mampu mengkoneksikan perangkat-perangkat secara *smart* (pintar) ke layanan internet. *Smart Campus* (Kampus cerdas/pintar) menerapkan dan memadukan sistem pembelajaran dalam proses untuk kepentingan urusan manajemen kampus, perpustakaan dan lain sebagainya menggunakan

teknologi informasi secara terintegrasi. Dalam kondisi *physical distancing* sekarang ini maka kehadiran *Smart Campus* sangat diperlukan sekali terutama dalam penyediaan *e-learning* misalnya dari para dosen juga hal lain pada penerapan *Information Communication Technology* (ICT) dalam menjalankannya kegiatan-kegiatan akademik. Smart lainnya, ada pada *smart home* (rumah cerdas/pintar). *Smart home* yang menyediakan pengaturan rumah yang nyaman dengan peralatan/perangkat dapat dikontrol secara otomatis menggunakan misal telepon pintar, *tablet, laptop*, atau konsol *game* dari jarak jauh dan dari mana saja dalam koneksi *internet* dengan menggunakan perangkat seluler atau perangkat jaringan lainnya. Perangkat di *smart home* yang saling terhubung tersebut, memungkinkan pengguna untuk mengontrol fungsi seperti akses keamanan ke rumah/kunci rumah, suhu, pencahayaan, pengaturan jadwal waktu pemakaian, pengaturan untuk mampu mengenali atau mempelajari para pemiliknya, menyelaraskan jadwal keseharian pemilik/kebutuhan pemilik, memberitahukan hal-hal yang mencurigakan yang terjadi secara otomatis.

Kelebihan *smarthome* ini yaitu sangat dibutuhkan oleh orang-orang dengan kondisi wabah covid-19 dalam menyelesaikan pekerjaan dalam hal ini misal untuk pekerjaan sebagai dosen, yang mana *user* baik dosen maupun banyak melakukan aktivitas di rumah dan atau untuk orang yang isoman maka akan sangat membantu sekali memantau kondisi *user* oleh dinas Covid.

Kondisi *home* yang aman tentu menjadi hal yang sangat penting, hal ini tentunya akan membantu terbentuknya *smart campus*. Adanya perkembangan tersebut maka hal-hal yang berkaitan dengan sarana dan prasarananya menjadi hal utama yang harus dikaji dan dipersiapkan agar proses komunikasi/informasi tetap terjaga dengan baik dan aman (*secure*). Sistem keamanan *smart home* ini dapat menggunakan kombinasi beberapa metode seperti pengaman *biometric fingerprint* dan *password* dan lain-lain dengan menggunakan beberapa perangkat diantaranya seperti *Arduino Mega, modul fingerprint, keypad, LCD, power supply unit (PSU), magnetic switch, solenoid door lock* dan *buzzer*. Kondisi ini yang terimplementasi secara riil tentu saja jika akan ada perubahan dan atau lainnya maka akan berpengaruh terhadap kondisi *smart home* yang ada tersebut. Sehingga untuk menjaga keamanan *smart home* ini maka perlu adanya upaya untuk melakukan terobosan secara simulasi sehingga biaya dan lainnya dapat dihemat. Salah satu metode yang dapat digunakan untuk melakukan uji atas simulasi kerentanan pada *smart home* ini dapat menggunakan metode SQUARE (*Security Quality Requirements Engineering*) yang menyediakan identifikasi dan analisis kebutuhan dengan pendekatan masalah non-fungsional ke fungsional dan memberikan hasil keluaran berupa kategori dan prioritas keamanan

Beberapa penelitian telah dilakukan oleh Isa Shemsi (Shemsi, 2018) yang menerapkan Infrastruktur dan Arsitektur *Smarthome* IoT menggunakan *Cisco Packet Tracer Simulator*, Andrea Finardi (Finardi & Jääskeläinen, 2018) yang menerapkan Infrastruktur dan Arsitektur IoT menggunakan *Cisco Packet Tracer Simulator*, Zainab Alansari et al (Alansari et al., 2018) mengkaji infrastruktur, arsitektur, keamanan dan privasi, Ernita Dwi Meutia (E. D. Meutia, J. Teknik, E. Universitas, 2015) yang mengkaji keamanan dan privasi IoT. Elyas et al (Palantei et al., 2019) melakukan penerapan *smart card* untuk mendukung *smart campus*, Aprilia Sulistyowati (Sulistyohati et al., 2017) yang mengkaji penggunaan *green IT Readiness* dalam *Smart campus. Tianping Bi et al* (Bi, 2017) mengimplementasikan *smart* kampus menggunakan BIM dan 3DGIS, dan Ghizlane Ikrissi (Ikrissi & Mazri, 2020) yang mengkaji serangan yang dapat mempengaruhi data dan informasi.

Berdasarkan masalah yang telah disebutkan, maka 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* yang mampu mendukung *Smart Campus* dengan menggunakan metode SQUARE (*Security Quality Requirements Engineering*).

2. TINJAUAN PUSTAKA

2.A Smart Home

Smarthome yang merupakan salah satu penerapan teknologi *Internet of Things* (IoT) dalam bidang *home automation* yang menyediakan kenyamanan, keamanan, efisiensi energi dan kontrol terhadap perangkat rumah. Ada berbagai jenis area aplikasi *smart home* seperti *Smart home* untuk keamanan, *smart home* untuk orang tua, *smart home* untuk perawatan kesehatan, *smart home* untuk penitipan anak, *smart home* untuk efisiensi energi, dan *smart home* untuk hiburan, music dan lain-lain (De Silva et al., 2012). Selain itu *smart home* juga dapat digunakan sebagai media pembelajaran salah satunya menggunakan *smarthome* berbasis audio (Ronen et al., 2018). Smart home saat ini rentan dengan serangan keamanan yang meliputi:

1. *Interruption:* merusak suatu perangkat sistem sehingga tidak lagi tersedia. Serangan ini mengancam kepada ketersediaan *(availabilit*y) sistem. Contoh serangan adalah "*denial of service attack*".
2. *Interception:* asset atau informasi dapat diakses oleh pihak yang tidak memiliki wewenang. Contoh dari serangan ini adalah penyadapan/ *Data Sniffing, MAC Address Spoofing,* dan *Rogue Access Point*.
3. *Modification:* Selain mendapatkan akses, pihak tidak berwenang ini juga dapat mengubah

(tamper) aset. Contoh dari serangan ini yaitu memodifikasi isi dari web site dengan pesan-pesan yang merugikan pemilik *web site*.

4. Serangan pada lingkungan *smarthome* dapat dimungkinkan dengan beberapa teknik yang terdiri dari (Mantoro et al., 2014):
5. *Denial of Service*, serangan yang yang dapat menyebabkan suatu sistem tidak dapat melayani pihak yang sah.
6. Merusak secara fisik objek-objek dalam jaringan
7. *Eavesdropping*/*Data Sniffing*, serangan pasif yang menargetkan berbagai kanal komunikasi dengan tujuan mengekstrak data dari aliran informasi.
8. *Hijacking*, penyerang mengekstrak informasi dari node maupun dari infrastruktur lain yang memiliki kemampuan penyimpanan data.

2.B Metode SQUARE

SQUARE (*Security Quality Requirements Engineering*) merupakan framework untuk memunculkan, mengkategorikan persyaratan keamanan yang diprioritaskan untuk sarana dan prasarana teknologi informasi dan aplikasi. SQUARE membantu analis keamanan dan organisasi mempertimbangkan masalah keamanan pada tahap awal siklus hidup pengembangan sistem yang mengarah pada pengembangan sistem yang lebih aman dan dapat bertahan dengan biaya yang lebih hemat (Suleiman & Svetinovic, 2013). Tujuan jangka panjang dari metode SQUARE (*Security Quality Requirements Engineer*) adalah untuk mengintegrasikan pertimbangan keamanan pada tahap awal siklus pengembangan. Berikut adalah tahapan metode SQUARE yang akan dilakukan pada metodologi SQUARE (Mead & Stehney, 2005):

1. *Agree on Definition*
2. *Identify Security Goals*
3. *Develop Artifacts*
4. *Perform Risk Assesment*
5. *Select Elicitation Technique*
6. *Elicit Security Requirements*
7. *Categorize Requirement*
8. *Prioritize Requirements*
9. *Requirements Inspection*

2.C Anonymous Doser

Anonymous doser merupakan sebuah perangkat yang sering digunakan untuk melakukan serangan DoS. Anonymous doser dikembangkan dengan bahasa C. Anonymous doser dapat bekerja pada platform windows sehingga sangat mudah digunakan.

2.D Wireshark

Wireshark merupakan perangkat analisis protokol jaringan yang dapat untuk menangkap dan menelusuri lalu lintas yang berjalan di jaringan komputer secara interaktif. Wireshark dapat berjalan di berbagai sistem operasi termasuk Windows, macOS, Linux, dan UNIX. Profesional jaringan, pakar keamanan, pengembang, dan pendidik menggunakannya secara teratur. Wireshark dapat diakses secara bebas sebagai open source, dan dirilis di bawah versi GNU General Public License (Wireshark.org, 2022).

2.E Hydra

Hydra merupakan perangkat pemecah kata sandi menggunakan brute force yang mendukung banyak protokol untuk menyerang secara cepat dan fleksibel dengan modul baru mudah ditambahkan. Alat ini memungkinkan mendapatkan akses tidak sah ke sistem dari jarak jauh. perangkat ini dapat menddukung banyak protokol seperti Cisco auth, FTP, HTTP(S)IMAP, MySQL, POP3, PostgreSQL, SMTP, SSH (v1 and v2), SSHKEY, dan lain-lain. (CyberPunk, n.d.).

2.F Nmap

Nmap merupakan perangkat audit keamanan sumber terbuka. paket IP digunakan nmap untuk menentukan informasi pentig seperti host, layanan yang terbuka, sistem operasi yang digunakan, jenis filter paket/firewall yang digunakan, dan karakteristik lainnya. Nmap bekerja dengan memindai jaringan besar dengan cepat, dan bekerja dengan baik pada host tunggal. Nmap dapat digunakan berbagai operasi komputer seperti Linux, Windows, dan Mac OS X. Selain dapat dieksekusi pada baris perintah klasik Nmap, suite Nmap menyertakan GUI dan penampil hasil (Zenmap), transfer data yang mudah, dan alat debugging (Ncat), sebuah perangkat untuk membandingkan hasil scan (Ndiff), dan generasi paket dan alat analisis respon (Nping) (Lyon, 2008).

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan *Security Quality Requirements Engineering* (SQUARE) (Mead & Stehney, 2005). Pendekatan *Security Quality Requirements Engineering* (SQUARE) terdiri dari tahapan yang meliputi *identify security goals, develop artifacts, perform risk assesment, select elicitation technique, elicit security requirements, categorize requirement, prioritize requirements* dan *requirements inspection*.

1. Agree on Definition

Mendefinisikan kebutuhan yang akan dijalankan. Kandidat definisi tersebut dapat diambil dari standar IEEE dan standar lainnya. Peran yang terlibat dalam penentuan definisi yakni *stakeholders* dan *requirement team* hingga ditemukan kesepakatan definisi yang digunakan. Dalam penelitian ini kami menentukan definisi kebutuhan berdasarkan beberapa studi literatur sejenis.

2. Identify Security Goal

Mengidentifikasi tujuan keamanan yakni menyetujui serangkaian prioritas keamanan yang akan diterapkan, hal tersebut menjadi tanggung

jawab sebagai relevansi persyaratan keamanan yang akan dihasilkan. Dalam penelitian ini kami menentukan tujuan prioritas tujuan keamanan sistem yang diterapkan berdasarkan studi literatur sejenis. Pada penelitian ini ditentukan tujuan keamanan (*security goal*) yaitu *privacy*, *integrity*, *authentication*, *access control* dan *non-repudiation*.

3. Develop Artifact

Tim *engineering* dan *stakeholder* dapat menghasilkan seperangkat persyaratan keamanan, tim harus mengumpulkan satu set lengkap artefak. Beberapa artefak yang dikumpulkan pada penelitian ini terdiri dari:

a. Diagram Arsitektur
b. Diagram *Usecase*
c. Diagram *Misusecase*

4. Perform Risk Assessment

Pada tahapan ini, kami melakukan penilaian risiko untuk menentukan persyaratan yang tepat digunakan pada keamanan *smarthome*. Pada penelitian ini kami melakukan *risk assessment* yang terdiri dari:

a. Penentuan metodologi yang akan digunakan dalam melakukan *risk assessment*
b. Kami melakukan simulasi serangan terhadap arsitektur *smarthome* yang telah didefinisikan. Serangan yang dilakukan terdiri dari *Man in the Middle attack*, *Port Scan*, *Denial of Service*, dan *Brute Force*. Perangkat yang kami gunakan untuk melakukan serangan ditunjukan pada tabel 1.

Tabel 1. perangkat yang digunakan

No.	Jenis Serangan	perangkat
1	*Man in the Middle attack*	Wireshark
2	*Port Scan*	Nmap
3	*Denial of Service*	Anonymous Doser
4	*Brute Force*	THC Hydra

5. Select Elicitaion Techniques

Tahapan ini digunakan untuk menentukan teknik elisitasi yang cocok untuk melakukan penanganan terhadap pekerjaan yang dilakukan. Dengan membandingkan teknik yang tersedia. Pada metodologi SQUARE terdapat 9 kriteria teknik elisitasi yaitu *adaptability*, *case tool*, *client acceptance*, *complexity*, *graphical output*, *implementation duration*, *learning curve*, dan *scalability*. Setiap teknik dipetakan berdasarkan 9 kategori yaitu *misusecases*, SSM, QFD, CORE, IBIS, JAD, FODA, CDA, ARM. Langkah selanjutnya yaitu diberi penilaian dengan skala 1 sampai 3 dimana nilai tertinggi merupakan nilai yang sangat baik.

6. Elicit Security Requirement

Elisitasi persyaratan keamanan untuk menyediakan pedoman rinci bagaimana melakukan elisitasi keamanan yang baik. Pada tahap ini kami menentukan elisitasi persyaratan keamanan sebagai langkah-langkah mitigasi yang diperlukan.

7. Categorize Requirement

Pada tahapan ini, kami melakukan klasifikasi persyaratan keamanan awal sistem yang dibagi ke dalam beberapa kelompok dengan kode pada setiap kelompoknya. Adapun kelompok tersebut dibagi terdiri dari *Privacy*, *Access Control & Authentication*, *Integrity*, dan *availability*. Setiap kelompok berisi persyaratan keamanan yang dikategorikan oleh nama kelompok tersebut.

8. Prioritize Requirement

Pada tahapan ini, kami memprioritaskan persyaratan keamanan yang berkaitan dengan isu yang diteliti berdasarkan misusecase yang telah ditentukan sebelumnya. Prioritas persyaratan keamanan dilakukan dengan membuat tabel prioritas kemanan dari serangan (*misusecase*) yang mungkin terjadi dengan risiko bahaya yang lebih tinggi.

9. Inspection Requirement

Terakhir, kami mengembangkan persyaratan keamanan yang akurat dan dapat diverifikasi dengan mengembangkan *review log* dengan tingkat penilaian masalah yang terjadi pada sistem. Tahapan ini bertujuan untuk melakukan penilaian terhadap perencanaan yang telah dilakukan. Pemeriksaan dapat dilakukan pada berbagai tingkat formalitas, Tujuan dari setiap *review log* adalah untuk menemukan kelemahan pada sistem.

4. HASIL DAN PEMBAHASAN

4.A Agree on Definition

Persetujuan pada definisi ditentukan menggunakan metode studi literatur yang dikorelasikan sesuai dengan studi kasus yang sedang dianalisis. Kami telah mendefinisikan istilah dan definisi serta kebutuhan sistem.

4.B Identify Security Goals

Pada tahapan kedua, kami mendefinisikan kebutuhan sistem pada *smarthome*. Kebutuhan sistem dibagi menjadi dua tujuan yang terdiri dari tujuan bisnis dan tujuan keamanan *smarthome*. Tujuan bisnis diidentifikasi berdasarkan manfaat yang didapat dari adanya jaringan *smarthome* dalam rangka menunjang kegiatan pembelajaran. Tabel 1 menunjukan tujuan bisnis yang dicapai.

Tabel 2. Tujuan bisnis

No.	Tujuan Bisnis
1	Jaringan *smarthome* dibangun untuk keperluan penghuni rumah untuk memudahkan akses kegiatan dengan menggunakan peralatan rumah untuk menunjang kegiatan pembelajaran
2	Jaringan *smarthome* dibangun untuk mengintegrasikan seluruh peralatan, dan perangkat lainnya dengan tujuan meningkatkan kualitas pembelajaran
3	Jaringan *smarthome* dibangun untuk membantu

No.	Tujuan Bisnis
	kenyamanan, kemudahan penghuni rumah dalam menjangkau fasilitas kampus selama pembelajaran

Kemudian kami menentukan tujuan keamanan. ditunjukan pada tabel 3.

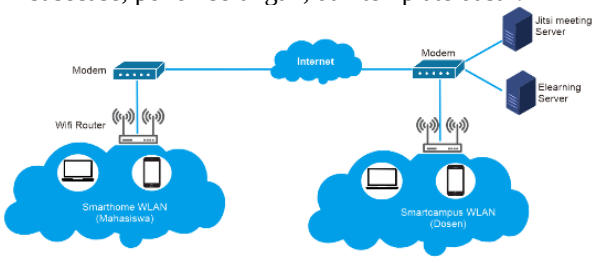
Tabel 3 Tujuan keamanan

ID	Aspek Kemanan	Tujuan Keamanan
G-1	*Confidentiality*	Kerahasiaan data dan informasi harus terjaga dari akses akses tidak sah pihak luar.
G-2	*Integrity*	Keaslian data dan informasi user harus terjaga dari akses akses tidak sah pihak luar.
G-3	*Authentication*	Kebenaran data dan informasi yang melakukan akses suatu data, informasi atau layanan dari sistem.
G-4	*Availability*	Ketersediaan data, informasi, dan layanan sistem ketika diakses dan digunakan oleh user.
G-5	*Access Control*	Klasifikasi pengguna dan pengaturan kontrol akses terhadap user dan komponen sistem sesuai dengan haknya dan wewenangnya. Pengguna yang berwenang melakukan penambahan, pengubahan, atau penghapusan user dan akses pada sistem adalah administrator.
G-6	*Non Repudiation*	Pencatatan user terhadap aktifitas akses data, informasi dan layanan yang tersedia dari sistem.

Tabel 3 menunjukan tujuan-tujuan keamanan berdasarkan pada aspek-aspek keamanan yang harus dipenuhi. Tujuan keamanan ini juga digunakan untuk memetakan persyaratan teknis elisitasi berdasarkan ID yang ditentukan.

4.C Develop Artifact

Tahap ketiga dikembangkan serangkaian artefak. Artefak yang dikembangkan meliputi diagram arsitektur, diagram *usecase*, diagram misusecase, pohon serangan, dan template dasar.



Gambar 1. Diagram Arsitektur

1. Diagram Arsitektur

Proses perencanaan artefak membutuhkan suatu arsitektur yang dapat menggambarkan gambaran sistem yang sedang berjalan. Pada kasus ini kami memvisualisasikan gambaran sistem atau proses bisnis yang ditampilkan

2. Diagram Usecase

Diagram usecase digunakan untuk menggambarkan aktivitas sistem yang berjalan.

3. Misusecase

Mis*usecase* menjabarkan aktivitas serangan apa saja yang dapat terjadi pada sistem jaringan. Aktivitas serangan pada jaringan dilakukan oleh penyerang secara ilegal untuk mengakses sistem. berikut ini misusecase yang teridentifikasi pada penelitian ini.

4. Dos (Denial of Service)

Membanjiri sistem dengan mengirim paket dalam jumlah yang besar sehingga server tidak dapat melayani *client*

5. Man-in-the-Middle-Attack (MITM)

Mencuri informasi akses masuk sistem dengan menyadap lalu lintas jaringan

6. Port Scan

Mendeteksi port yang terbuka dan mendapatkan informasi penting *pada suatu jaringan atau host untuk kemudian diteruskan ke serangan lebih lanjut*

7. Brute force

Menebak *username* dan password dengan cara mencoba berbagai kombinasi *username* dan password sebanyak mungkin.

4.D Agree on Definition

Kami menentukan metodologi penilaian risiko yang tepat untuk elisitasi persyaratan keamanan. Dari metodologi yang ada kemudian dilakukan penilaian risiko berdasarkan kriteria yaitu *Small Organization* [C1], *Short Time Frame* [C2], *Additional Data Collection Required* [C3], *Requirement* [C4]. Tabel 4 menunjukan penilaian pada setiap metodologi.

Tabel 4. Penilaian Metodologi

Risk Assessment	***C1***	***C2***	***C3***	***C4***	***average***
GAO	2	4	2	2	2.50
NIST	**2**	**2**	**1**	**1**	**1.50**
NSA/IAM	3	3	2	2	2.50
SAEM	4	4	4	4	4.00
V-RATE	3	4	4	4	3.75
Haimes	**2**	**2**	**2**	**2**	**2.00**
SSA	2	2	2	4	2.50
DDP/Feather	3	4	2	4	3.25

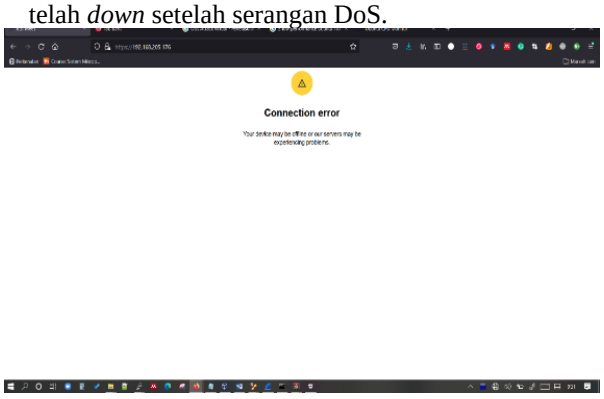
Dalam pemilihan metodologi *risk assessment*, nilai terkecil merupakan nilai yang paling tepat untuk menentukan metodologi yang sesuai. Pada tabel 3 diketahui metodologi NIST dan Haimes memiliki nilai paling kecil. Untuk itu, pada penelitian ini kami menentukan metodologi NIST dan Haimes sebagai metodologi *risk assessment.*

Pada tahap ini juga dilakukan simulasi pengujian keamanan terhadap sistem *smarthome*. Simulasi menggunakan teknik yang telah ditentukan pada tahapan *misusecase*.

1. *Simulasi* DoS

Kami mencoba melakukan serangan DoS attack dengan mengirimkan paket pada server *Jitssi Meeting*. Pada simulasi ini penyerang mencoba mengirim paket dengan ukuran besar pada *server jitsi meeting*. Serangan ini bertujuan agar *server* tidak dapat lagi melayani *client*.

Simulasi ini terdiri dari 100, 1.000, dan 100.000 paket ping. Hasilnya, pada paket 100 layanan server masih dapat memberikan layanan pada *client*. Pada paket 1.000, server masih dapat diakses namun *client* memerlukan waktu lebih ama untk memuat request. Terakhir, pada 100.000 paket server sudah tidak dapat diakses lagi. Gambar 2 menunjukan server jitsi meeting yang telah *down* setelah serangan DoS.



Gambar 2. Server Jitsi yang telah *down*

2. *Simulasi* MITM

serangan Man in the Middle Attack dilakukan pada server elearning. Tujuan dari simulasi ini adalah untuk mengidentifikasi kerentanan yang terdapat pada server elearning. Teknik serangan Man in the Middle Attack dapat melakukan penangkapan paket-paket pada jaringan yang ditransmisikan baik menggunakan wifi maupun menggunakan kabel koneksi.

```
username=test&password=test2HTTP/1.1 303 See Other
Date: Wed, 10 Nov 2021 08:18:48 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: http://192.168.175.218/moodle/login/index.php
Content-Language: en
Content-Length: 443
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

Gambar 3. tangkapan pada *wireshark*

Dalam simulasi ini, diskenariokan *client* mengakses elearning kemudian mengisikan username dan password. Kemudian attacker memantau tranmisi jaringan menggunakan apliaksi wireshark. Hasilnya, username dan password dapat ditangkap dengan menganalisis TCP stream pada IP elearning. Gambar 3 menunjukan username dan password yang tertangkap ada aplikasi wireshark

3. Simulasi *Port Scan*

Port scanning merupakan teknik pencarian vulnerability. Scanning dilakukan untuk mengidentifikasi port mana yang terbuka. Informasi ini berguna untuk menentukan teknik serangan apa yang tepat selanjutnya digunakan. Pada simulasi ini, kami melakukan port scanning pada server elearning dan server *Jitssi Meeting*.

Pada server elearning, serangan dilakukan dengan menginputkan sintak *nmap –sS 192.168.85.218* dimana IP 192.168.85.218 merupakan IP server elearning. Hasilnya port yang terbuka dapat teridentifikasi. yaitu port 21,22, dan 80 dengan layanan masing-masing pada ftp, ssh dan http. Gambar 4 menunjukan port yang terbuka pada elearning

```
┌──(root💀kali)-[~]
└─# nmap -sS 192.168.85.218
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 01:54 EST
Nmap scan report for 192.168.85.218
Host is up (0.00010s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:C5:F6:F0 (Oracle VirtualBox virtual NIC)
```

Gambar 4. port yang terbuka

Serangan juga dilakukan pada server *Jitssi Meeting*. Serangan dilakukan dengan menginputkan sintak *nmap –sS 192.168.85.176* dimana IP 192.168.85.176 merupakan IP server elearning. Hasilnya port yang terbuka dapat teridentifikasi yaitu port 22, 80, dan 443 dengan layanan masing-masing pada ssh, http dan https. Gambar 5 menunjukan port yang terbuka.

```
┌──(root💀kali)-[~]
└─# nmap -sS 192.168.85.176
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 10:54 EST
Nmap scan report for 192.168.85.176
Host is up (0.00037s latency).
Not shown: 996 filtered ports
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
443/tcp   open   https
10000/tcp closed snet-sensor-mgmt
```

Gambar 5. *port* yang terbuka pada jitsi

4. Simulasi *Brute* force

Pada simulasi ini, kami melakukan teknik serangan brute force pada server menggunakan hydra. Simulasi ini, attacker mencoba menyerang layanan ssh dengan port 22. Username dan password ditebak dengan menggunakan wordlist yang telah disiapkan. kami memberikan input sintak pada terminal kali linux sebagai berikut:

hydra -L /usr/share/wordlists/userlist.txt -P /usr/share/wordlists/passlist.txt 192.168.55.176 ssh dimana;

- hydra digunakan untuk memanggil aplikasi yang digunakan.
- –L merupakan input file wordlist untuk mengidentifikasi login username.

- Pada */usr/share/wordlists/userlist.txt* merupakan direktori worlist username.
- –P merupakan perintah input wordlist password. Pada */usr/share/wordlists/passlist.txt* merupakan direktori wordlist password.
- 192.168.55.176 merupakan IP target
- Sintak ssh merupakan jenis layanan yang dijadikan target serangan.

Gambar 6 menunjukan hasil serangan brute force beserta username dan password yang valid.

Gambar 6. Serangan brute force pada ssh

4.E Select Elicitaion Technique

Tahap kelima adalah memilih teknik elisitasi. Teknik elisitasi diambil berdasarkan literature yang terdiri dari *Misuse Case*, *SSM*, *QFD*, *CORE*, *IBIS*, *JAD*, *FODA*, *CDA*, dan *ARM*. Setiap teknik elisitasi dinilai berdasarkan 9 kriteria yang terdiri dari *Adaptability* (D1), CASE *Tool*, *Client Acceptance* (D2), *Complexity*, *Graphical Output* (D2), *Implementation Duration* (D3), *Learning Curve* (D4), *Maturity* (D5), dan *Scalability* (D6). Tabel 4 menunjukan penilaian teknik elisitasi.

Dari hasil penilaian yang ditunjukan pada tabel 5 dapat dilihat rata-rata pada kriteria Misusecase, SSM, IBIS, JAD, dan ARM memiliki nilai paling baik. Namun pada teknik elisitas misusecase memiliki kompleksitas, implementasi, dan pendekatan yang lebih baik dan lebih tepat diterapkan pada penelitian ini dibandingkan dengan teknik elisitas yang lain. Untuk itu, pada penelitian ini penulis memilih *misusecase* utnuk melakukan analisis keamanan

Tabel 5. Penilaian Teknik Elisitasi

Criteria	*MC*	*SSM*	*QFD*	*CORE*	*IBIS*	*JAD*	*FODA*	*CDA*	*ARM*
D1	3	1	3	2	2	3	2	1	2
D2	1	2	1	1	3	2	1	1	1
D3	2	2	2	2	3	2	1	3	3
D4	2	2	1	2	3	2	1	1	2
D5	2	2	1	1	2	1	2	2	3
D6	2	2	1	1	2	1	2	2	3
D7	3	1	2	1	3	2	1	1	1
D8	2	3	3	3	2	3	2	2	1
D9	1	3	3	3	2	3	2	1	2

4.F Elicite Security Requirement

Skenario dari *misusecase* yang telah disimulasikan kemudian dinilai berdasarkan kategori tingkat risikonya. Tingkatan kategori risiko terdiri dari high, medium dan low. Tabel 6 menunjukan kategori ancaman dengan level ancamannya

Tabel 6. Kategorisasi Ancaman

No.	Kategori ancaman	Kategori
1	*Port scanning*	***Medium***
2	*Data Sniffing/ MITM*	***High***
3	*Denial of Service* (DoS)	***High***
4	*Brute force*	***High***

Selanjutnya didefinisikan elisitasi persyaratan keamanan dengan teknik *misusecase*. Tabel 7 menunjukan pendefinisian persyaratan keamanan.

Tabel 7. Penilaian Teknik Elisitasi

ID	Persyaratan keamanan	tujuan
R-01	Sistem ini diperlukan untuk melakukan mekanisme pemblokiran terhadap IP yang mencurigakan. pemblokiran dilakukan dengan cara menerapkan firewall untuk unutk menghalau IP yang mencoba mengidentifikasi *port* yang terbuka .	G-1 G-3 G-5 G-6
R-02	Sistem ini diperlukan untuk melakukan mekanisme untuk mencegah kemungkinan bocornya informasi username dan password pada paket yang ditransmisikan dengan cara mengubah protokol yang tidak terlindungi engan enkripsi seperti http dengan protokol yang lebih terlindungi seperti https dan mengubah *port* akses dari 80 ke *port* 443.	G-1 G-2 G-3 G-5 G-6
R-03	Sistem ini diperlukan untuk menghalau request mencurigakan dengan menerapkan firewall dan menyediakan load balancer. Perangkat keamanan lainnya seperti IDS juga dapat dipertimbangkan.	G-2 G-4 G-6
R-04	Sistem ini diperlukan untuk melakukan mekanisme pembatasan *login*, penguatan *password*, menerapkan *captcha* dan *two factor authentication*, dan mengubah *port default* pada layanan ssh	G-3 G-5 G-6

4.G Categorize Requirement

Pada tahapn ini persyaratan keamanan yang telah didefinisikan pada tahapan sebelumnya dikategorisasikan berdasarkan kriteria keamanan. Kategori keamanan meliputi *Privacy*, *Access Control & Authentication*, *Integrity*, dan *Availability*. Tabel 8 menunjukan kategorisasi persyaratan keamanan.

Tabel 8. pengelompokan persyaratan keamanan

Group A: *Privacy*	**Group B: *Authentication***
Setiap pengguna yang mengakses *elearning* maupun jitsi pada jaringan *smarthome* harus menjaga kerahasiaan data dan informasi dari akses pengguna secara illegal.	1. penggunaan protokol-protokol yang memiiliki mekanisme enkripsi data seperti pada penggunaan protokol https. 2. adanya pengamanan akses login seperti penggunaan kombinasi *username* dan *password* yang rumit, penerapan *captcha* dan mekanisme pembatasan *login*
Group C: *Integrity*	**Group D: *Availability***
Melakukan evaluasi secara berkala pada semua perangkat, konfigurasi serta setiap hak akses setiap user.	Penerapan menerapkan perangkat sistem keamanan seperti IDS, maupun *firewall* pada jalur akses jaringan paling luar.

4.H Prioritize Requirement

Pada tahapan ini dilakukan pemilihan prioritas persyaratan yang berkaitan dengan sistem keamanan *smarthome* berdasarkan mis*usecase* sebelumnya. Prioritas persyaratan keamanan dihasilkan untuk memenuhi tujuan keamanan yang ditetapkan. prioritas persyaratan keamanan. Tabel 9 menunjukan kategori priotitas persyaratan keamanan.

Tabel 9. Kategori prioritas persyaratan keamanan

Aspek	Prioritas
Tujuan	*Privacy, Authentication, Availability*
Kebutuhan	• Keamanan sistem login. • Keamanan pada IP address. • Keamanan data pengguna.
Kategori	• *Privacy* • *Authentication* • *DoS*
Rekomendasi	• Penerapan protokol yang memiliki mekanisme enkripsi. • Penerapan IP dan *MAC Address filtering*. • Penerapan Firewall. • penerapan perangkat keamanan • mengubah *password* secara berkala.

4.I Prioritize Requirement

Pada tahapan ini dilakukan pemilihan prioritas persyaratan yang berkaitan dengan sistem keamanan *smarthome* berdasarkan mis*usecase* sebelumnya. Prioritas persyaratan keamanan dihasilkan untuk memenuhi tujuan keamanan yang ditetapkan. prioritas persyaratan keamanan. Tabel 8 menunjukan kategori priotitas persyaratan keamanan.

5. KESIMPULAN

Kerentanan pada jaringan smarthome dapat diidentifikasi. Kerentanan dapat dieksploitasi dengan menggunakan teknik serangan DoS untuk melumpuhkan layanan *server*, *man in the middle attack* sebagai sniffing data dan informasi pada paket yang ditransmisikan, dan *port scanning* untuk menemukan *port* server yang terbuka sebagai jalan untuk metode ekploitasi lainnya

Serangan dianalisis menggunakan metode SQUARE untuk menentukan kategorisasi persayaratan berdasarkan pada misusecase yang ada. Serangan dipetakan sesuai dengan tingkat risiko keamanannya. Kemudian menentukan persyaratan yang diperlukan sebagai mitigasi dari risiko yang telah disimulasikan.

DAFTAR PUSTAKA

(APJII), A. P. J. I. I. (2021). Peluang Penetrasi Internet dan Tantangan Regulasi Daerah. *Buletin APJII*, 15.

Alansari, Z., Anuar, B. A., Kamsin, A., Belgaum, M. R., Alasher, J., Soomro, S., & Miraz, H. M. (2018). Internet of Things: Infrastructure, Architecture, Security and Privacy. *International Conference on Computing, Electronics & Communications Engineering (ICCECE)*, 150–155. https://doi.org/10.5772/intechopen.96669

Bi, T. (2017). The Design and Implementation of Smart Campus System. *Journal of Computers*, *12*(6), 527–533. https://doi.org/10.17706/jcp.12.6.527-533

CyberPunk. (n.d.). *Password Cracker THC Hydra*. Retrieved September 22, 2022, from https://www.cyberpunk.rs/password-cracker-thc-hydra

De Silva, L. C., Morikawa, C., & Petra, I. M. (2012). State of the art of smart homes. *Engineering Applications of Artificial Intelligence*, *25*(7), 1313–1321. https://doi.org/10.1016/j.engappai.2012.05.002

E. D. Meutia, J. Teknik, E. Universitas, and S. K. (2015). Interet of Things – Keamanan dan Privasi. *Semin. Nas. Dan Expo Tek. Elektro*, 85–89.

Finardi, A., & Jääskeläinen, V. (2018). IoT Simulations with Cisco Packet Tracer. *Information Technology*, *Master of*(June), 89 pages + 3 appendices.

Ikrissi, G., & Mazri, T. (2020). A study of smart campus environment and its security attacks. *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives*, *44*(4/W3), 255–261. https://doi.org/10.5194/isprs-archives-XLIV-4-W3-2020-255-2020

Lyon, G. F. (2008). *Nmap: Discover your network*. Nmap Software LLC. https://nmap.org/

Mantoro, T., Ayu, M. A., & Binti Mahmod, S. M. (2014). Securing the authentication and message integrity for Smart Home using smart phone. *International Conference on Multimedia Computing and Systems - Proceedings*, 985–989. https://doi.org/10.1109/ICMCS.2014.6911150

Mead, N. R., & Stehney, T. (2005). Security quality requirements engineering (SQUARE) methodology. *SESS 2005 - Proceedings of the 2005 Workshop on Software Engineering for Secure Systems - Building Trustworthy Applications*, 1–7. https://doi.org/10.1145/1083200.1083214

Palantei, E., Suyuti, A., Areni, I. S., Baharuddin, M., & Samman, F. A. (2019). Pengembangan dan Implementasi Smart Campus Berbasis Smart Card. *TEPAT Jurnal Teknologi Terapan Untuk Pengabdian Masyarakat*, *2*.

Ronen, R., Radu, M., Yom-Tov, E., & Ahmadi, M. (2018). *Microsoft Malware Classification Challenge*. 183–194. https://doi.org/10.1145/2857705.2857713

Shemsi, I. (2018). Implementing Smart Home Using Cisco Packet Tracer Simulator. *International Journal of Engineering Science Invention*

Research & Development, *IV*(Vii), 261–269.

Suleiman, H., & Svetinovic, D. (2013). Evaluating the effectiveness of the security quality requirements engineering (SQUARE) method: A case study using smart grid advanced metering infrastructure. *Requirements Engineering*, *18*(3), 251–279. https://doi.org/10.1007/s00766-012-0153-4

Sulistyohati, A., Kusumawardani, S. S., & Santosa, P. I. (2017). Kajian Indikator Pengukuran Kesiapan Pada Green Smart Campus Menggunakan Kerangka Kerja Green It Readiness. *Prosiding Semnastek*, *November*, 1–2. https://jurnal.umj.ac.id/index.php/semnastek/article/view/1923

Wireshark.org. (2022). *What is Wireshark*. https://www.wireshark.org/faq.html#_what_is_wireshark