

SKRIPSI
ANALISIS KEAMANAN OPERASI DAN PENGELOLAAN
DATA *SMART* CCTV IOT TERHADAP SERANGAN *DENIAL*
OF SERVICE

Diajukan sebagai salah satu syarat
untuk memperoleh gelar Sarjana Komputer

HANSEND CRISTOPER
NPM: 1932013



PROGRAM SARJANA TEKNOLOGI INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS INTERNASIONAL BATAM
2023

UNIVERSITAS INTERNASIONAL BATAM

Fakultas Ilmu Komputer
Program Sarjana Teknologi Informasi
Semester Ganjil 2022/2023

Analisis Keamanan Operasi dan Pengelolaan Data *Smart* CCTV IOT Terhadap Serangan *Denial of Service*

Hansend Cristoper
NPM: 1932013

ABSTRAK

Salah satu kebutuhan dasar manusia adalah menjalankan kehidupannya dengan rasa aman. Dengan bantuan teknologi yang digunakan dalam membantu proses kehidupan, dan dapat memperbaiki kualitas ekonomi, manusia juga bisa memanfaatkan teknologi untuk mendapatkan rasa aman. Salah satu teknologi yang dapat meningkatkan rasa aman pada manusia adalah CCTV. CCTV merupakan suatu perangkat yang dapat beroperasi dan memproses pengelolaan data video rekaman di media penyimpanan DVR berdasarkan hasil pantauan kamera yang terpasang pada CCTV. Selarasnya perkembangan teknologi dan internet, manusia saat ini masuk ke dalam dunia *Internet of Things*, di mana perangkat dapat terhubung ke internet dan dikelola menggunakan perangkat *Smartphone*. Salah satu perangkat yang bertransformasi akibat adanya IoT ini adalah CCTV menjadi *Smart* CCTV, di mana seseorang sekarang bisa mengoperasikan, memantau lingkungan sekitar dan pengelolaan data CCTV dari *Smartphone*. Penelitian ini akan menguji keamanan operasi dan keamanan pengelolaan data *Smart* CCTV yang terpasang langsung pada jaringan dengan serangan *Denial of Service*. Metode yang dilakukan dalam serangan ini adalah *Penetration Testing*, tahapan dimulai dari *footprinting* untuk mencari tau *IP Address* dan sistem operasi perangkat yang terhubung pada jaringan, dilanjutkan tahap *scanning* dan *enumeration* untuk memperdalam analisa pada perangkat yang telah ditemukan sebelumnya dengan tujuan mendapatkan target yang sesuai dan *port* yang terbuka sebagai jalan masuk serangan. Pada tahapan eksploitasi, *port* yang ditemukan akan diserang menggunakan *Denial of Service* untuk menguji ketahanan keamanan *Smart* CCTV. Dari hasil serangan *Denial of Service* pada *Smart* CCTV keamanan operasi dan keamanan pengelolaan data dapat dilumpuhkan secara langsung.

Kata kunci: *Keamanan Operasi, Keamanan Pengelolaan Data, DOS, Smart CCTV, IoT.*

DAFTAR ISI

LEMBAR PENGESAHAN KARYA ILMIAH SKRIPSI.....	ii
LEMBAR PERNYATAAN ORISINALITAS DAN HAK PUBLIKASI	iii
ABSTRAK	iv
ABSTRACT	v
KATA PENGANTAR	vi
UCAPAN TERIMAKASIH	vii
DAFTAR ISI	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
BAB I PENDAHULUAN	1
Latar Belakang	1
Rumusan Masalah	3
Batasan Masalah	3
Tujuan Penelitian	3
Manfaat Penelitian	3
Sistematika Penelitian	4
BAB II TINJAUAN PUSTAKA	5
Tinjauan Pustaka	5
Landasan Teori.....	6
<i>Internet of Things</i>	6
<i>Smarthome</i> atau Rumah pintar	6
<i>Cybersecurity</i>	7
CCTV	8
MITM atau <i>Man In The Middle</i>	8
<i>Networking</i>	9
Keamanan Jaringan	10
<i>Hacker</i>	10
<i>Penetration Test</i>	11
BAB III METODOLOGI PENELITIAN.....	12

Alur Penelitian	12
Rancangan Instrumen Penelitian.....	13
Kebutuhan Perangkat Keras.....	13
Kebutuhan Perangkat Lunak.....	13
BAB IV IMPLEMENTASI DAN PEMBAHASAN	14
Implementasi.....	14
<i>Perancangan Jaringan Simulasi</i>	14
<i>Footprinting</i>	17
<i>Scanning dan enumeration</i>	19
<i>Exploit</i>	21
BAB V KESIMPULAN DAN SARAN.....	24
Kesimpulan.....	24
Saran.....	24
DAFTAR PUSTAKA	25