KAJIAN KEAMANAN CCTV BERBASIS INTERNET OF THINGS "MENGIDENTIFIKASI MASALAH DAN SOLUSI PERLINDUNGAN"

Michael Keyva Valiant[-1], Ninuk Wiliani [-2],
Universitas Pancasila, Teknik Informatika, Indonesia [-1]
Universitas Pancasila, Teknik Informatika, Indonesia [-2]
email : keyvavaliant@gmail.com [-1] ninukwiliani15@gmail.com [-2]

[1]***Abstract—*** Perkembangan teknologi khususnya pada Internet of Things (IoT) yang menjadi awal adopsi perangkat seperti CCTV IoT dalam sistem keamanan rumah. Tetapi perangkat tersebut rentan terhadap ancaman siber seperti Man-in-the-Middle, Denial of Serivices, dan Brute force. Dari lemahnya autentikasi, enkripsi data yang kurang baik, serta penggunaan kredensial default. Penelitian bertujuan mengidentifikasi potensi kerentanan dan mengeksploitasi nya dengan metode serangan pada perangkat CCTV IoT dan memberikan solusi pendekatan ekperimental. Pengujian ini dilakukan pada dua perangkat CCTV IoT yang dipasang pada ruang lingkup rumah, dengan menggunakan beberapa tools open-sources seperti Nmap, Bettercap, dan Metasploit pada sistem operasi ubuntu linux. Hasil dari pengujian ini menunjukkan perangkat memiliki kerentanan keamanan pada konfigurasi jaringan dan autentikasi, serta rentan terkena serangan DoS dan Sniffing data. Solusi yang bisa diberikan, penggunaan firewall, sistem deteksi intrusi, dan pembaruan firmware, serta penguatan kredensial.

Kata Kunci : IoT, Man in The Middle, CCTV, ubuntu, Metasploit

1. PENDAHULUAN

IoT atau *Internet of Things* mengacu pada jaringan perangkat fisik yang dilengkapi dengan sensor, perangkat lunak, dan teknologi lainnya yang memungkinkan mereka terhubung dan bertukar data melalui internet atau jaringan komunikasi lainnya[1]. IoT mencakup pada berbagai bidang dan produk, diantaranya elektronik, komunikasi, dan rekayasa ilmu komputer[2]. Tak hanya itu, bentuk serangan siber pada perangkat berbasis IoT juga banyak terjadi pada bulan Oktober 2019 dan bulan Desember 2019. Perkembangan IoT cukup pesat pada beberapa tahun ini dikarenakan adanya teknologi Radio Frequency Identification dan Wireless Sensor Network.

RFID merupakan teknologi yang menggunakan komunikasi gelombang elektromagnetik yang dapat merubah data antara terminal dengan suatu objek seperti produk barang, hewan, ataupun manusia[2].

Dengan *demand* penggunaan yang tinggi membuat IoT tidak luput dari celah keamanan akibat kurangnya protocol enkripsi, autentikasi yang kurang baik, dan kata sandi default yang mudah ditebak. Masalah ini pernah terjadi pada kasus serangan terhadap *smart home* pada tahun 2020. Pada kejadiannya, peretas menargetkan berbagai fitur *smart home* seperti *smart lock*, *smart thermostat*, dan *smart assistants* (Alexa & Google Home). Peretas melakukan pembobolan pada *smart lock* dengan intrusi ke sistem suara untuk mengaktifkan AI seperti Alexa atau Google Assistant, yang kemudian dapat diinstruksikan untuk melakukan pembelian barang.

Dilansir dari *Cyberthreat.id, hacker* tidak dikenal meretas sistem kamera keamanan di Penjara Lang Suan, Provinsi Chumphon, Thailand. Peretasan kamera keamanan tersebut berhasil memperlihatkan lingkungan internal penjara yang dibocorkan melalui internet.

Hal ini dikarenakan kamera merk HiChip yang diproduksi di China ditemukan celah keamanannya, serta berhasil dieksploitasi peretas dengan mengakses protokol iLnkP2P yang digunakan kamera tersebut.

Solusi yang dapat diberikan merupakan peningkatan keamanan perangkat CCTV yang berbasis IoT[3]. Ada beberapa Solusi yang dapat digunakan, pertama menggunakan enkripsi end-to-end seperti TLS (Transport Layer Security) yang dapat melindungi komunikasi antara perangkat CCTV dan server cloud penyedia jasa[4]. Yang kedua untuk mendeteksi ancaman pengguna dapat menggunakan IDS (Intrusion Detection System) dan firewall untuk membantu memantau serta dapat memblokir aktivitas yang mencurigakan pada perangkat CCTV[5].

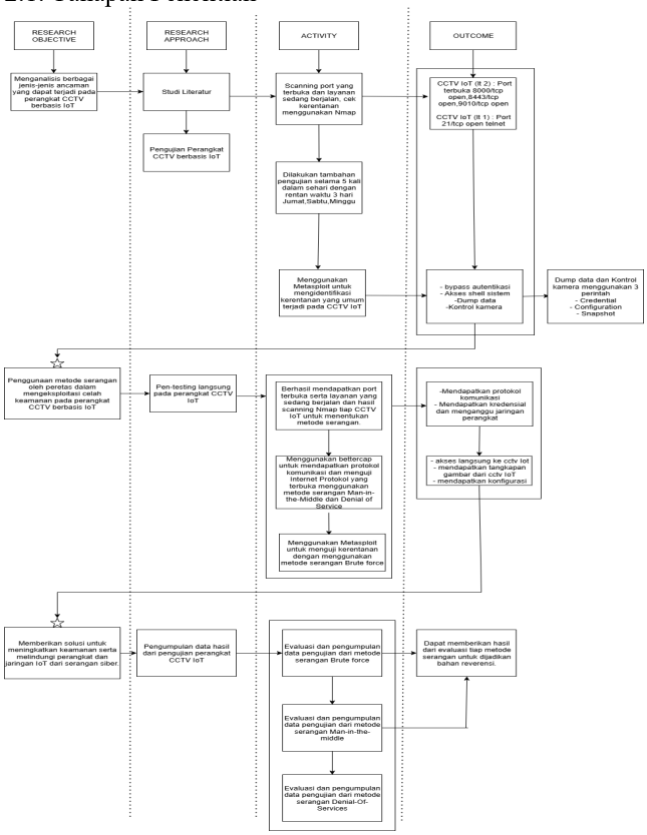
1

Penelitian ini bertujuan untuk melakukan pengujian pada CCTV IoT yang sudah ada tanpa harus membuatnya[6]. kerentanan keamanan dan memberikan Solusi pada CCTV yang berbasis IoT dengan skala kecil pada ruang lingkup rumah saja. Berbeda dengan penelitian ini, bahwa penelitian ini membuat CCTV yang berbasis IoT untuk memonitoring keamanan yang dapat diakses melalui website yang memerluka skala besar.

2. METODE PENELITIAN

Penelitian ini bertujuan untuk mengidentifikasi ancaman, metode serangan dan mengevaluasi tingkat keamanan pada perangkat CCTV IoT (Internet Of Things) pada lingkungan rumah apakah sudah menggunakan keamanan yang baik[7]. Fokus nya pada pengujian terhadap kerentanan sistem keamanan, yang termasuk enkripsi data, autentikasi pengguna, dan protokol jaringan yang digunakan pada perangkat CCTV IoT[8]. Penelitian ini dilakukan secara nyata dengan pendekatan eksperimental, dengan menggunakan bermacam tools open source seperti Ubuntu Linux, Nmap, Bettercap, dan Metasploit. Penelitian ini juga melakukan pen-testing atau penetration testing pada perangkat CCTV IoT dengan menyimulasikan beberapa metode serangan siber seperti Man-in-the-Middle (MITM), Brute Force, dan Denial Of Service (DoS). Dan dapat memberikan solusi teknis seperti penarapan IDS (INTRUSION DETECTION SYSTEM), Firewall, dan update perangkat keamanan untuk menjaga perlindungan terhadap ancaman siber[9].

2.1. Tahapan Penelitian



Gambar 1 Kerangka Pemikiran

Tahapan penelitian ini dirancang untuk menganalisis, menguji, dan dapat memberikan solusi terkait potensi ancaman keamanan pada perangkat CCTV berbasis Internet of Things(IoT)[10].

Penelitian mencakup pembahasan jenis-jenis ancaman, Teknik serangan yang umum dapat digunakan oleh penyerang pada perangkat CCTV berbasis IoT, dan metode apa yang dapat digunakan untuk pengujian yang relevan. Tahap selanjutnya merupakan pengujian awal perangkat CCTV IoT yang menggunakan Nmap untuk melakukan pemindaian port terbuka dan layanan yang sedang berjalanan.

Dari hasil scanning port tersebut terdapat beberapa port terbuka, termasuk protocol Telnet yang memiliki Tingkat keamanan rendah. Setelah port dan layanan terbuka teridentifikasi, tahap berikutnya melalukan eksploitasi kerentanan menggunakan Metasploit.

Proses dimulai dengan memilih modul eksploit yang sesuai, dan konfigurasi Alamat IP target,port layanan, serta metode serangan. Tools Metasploit digunakan untuk melakukan serangan Brute force pada layanan login yang ditemukan saat pemindaian[11].

Pengujian ini juga menggunakan tools Bettercap untuk mensimulasikan serangan yang berbasis jaringan. Bettercap dikonfigurasi untuk melakukan serangan Man-in-the-Middle (MITM) dengan Teknik ARP Spoofing pada target. Bettercap juga digunakan untuk melakukan serangan Denial of Services (DoS) dengan menganggu aliran jaringan antara perangkat CCTV dan gateway[12].

2.2. Kebutuhan Instalasi

Pada tahap penelitian ini, dibutuhkan instalasi alat serta perangkat lunak dan perangkat keras apa saja yang digunakan untuk melakukan pengujian.

Tabel 1 Perangkat Keras

NO	KOMPONEN	SPESIFIKASI
1	Laptop	Acer Predator Triton 300, Intel Core i7 gen 9, RAM 8, SSD + HDD 512GB
2	CCTV IoT 1	Merek Shenzhen, terpasang diruang tamu/keluarga
3	CCTV IoT 2	Merek Ezviz, terpasang di balkon lantai 2
4	Router	Router 1 (Lt 1) : Indihome Router 2 (Lt 2) : Bnefit
5	Jaringan Lokal (WI-FI)	Digunakan untuk menghubungkan CCTV berbasis IoT ke laptop pengujian

Tabel 2 Perangkat Lunak

NO	KOMPONEN	SPESIFIKASI
1	Ubuntu Linux 22.04 LTS	Sistem operasi yang digunakan untuk mempermudah menggunakan berbagai tools
2	Nmap	Digunakan untuk mengidentifikasi port terbuka, layanan yang aktif, dan kerentanan umum.
3	Bettercap	Digunakan untuk sniffing lalu lintas jaringan, Man-in-the-Middle dan Denial of Service attack
4	Metasploit Frame Work	Digunakan untuk eksploitasi langsung terhadap CCTV IoT dan firmware yang rawan
5	Browser Web	Mengakses antarmuka web dari perangkat CCTV IoT

2.3 Analisis Celah keamanan

Pada tahap analisis celah keamanan, ada beberapa pengujian yang dilakukan pada CCTV berbasis IoT ini. pertama akan dilakukan pengujian scanning port yang terbuka menggunakan tools *Nmap* untuk mengidentifikasi port mana saja yang terbuka dan layanan yang sedang berjalanan pada perangkat. Tujuan nya untuk mengidentifikasi celah atau pintu masuk yang dapat dimanfaatkan untuk mengeksploitasi perangkat.

Kedua akan dilakukan identifikasi celah autentikasi dalam hal penggunaan kredensial default (username dan password bawaan pabrik) yang sangat rentan di eksploitasi, pengujian Man-in-the-Middle dan Denial of Service menggunakan bettercap[13].

Ketiga dilakukan pengujian terhadap system enkripsi yang digunakan perangkat CCTV berbasis IoT, untuk mengevaluasi apakah ada data yang perangkat CCTV berbasis IoT, untuk mengevaluasi apakah ada data yang dikirimkan melalui jaringan yang tidak dilindungi dengan protocol enkripsi yang baik[7]. Jika enkripsi lemah maka data video dan informasi yang dikirimkan perangkat dapat disadap atau dimanipulasi oleh penyerang.

2.4. Data

Data yang digunakan pada penelitian ini merupakan data primer yang bersifat privet karena berasal dari hasil pengujian langsung pada kedua CCTV berbasis Internet of Things (IoT) yang terpasang dilingkungan rumah peneliti. Oleh karena itu data ini merupakan privasi pengguna, Kedua perangkat tersebut adalah CCTV dengan merek Ezviz yang terhubung ke WI-FI Bnefit dan Shengzhen yang terhubung ke WI-FI Indihome. Data yang diperoleh melalui uji coba keamanan menggunakan beberapa tools seperti Nmap, Bettercap, dan Metasploit pada system operasi Ubuntu Linux.

Proses pengumpulan data ini dimulai dengan pemindaian port dan layanan yang sedang berjalan menggunakan Nmap untuk mengidentifikasi jalur komunikasi terbuka yang dimana berhasil mendapatkan port 8000 http dan port 8443 https pada perangkat Ezviz dan Port 23 telnet pada perangkat Shengzhen.

Selanjutnya menggunakan tools Bettercap yang digunakan untuk menangkap paket lalu lintas jaringan, dengan melakukan serangan Man-in-The-Middle (MITM), yang berhasil mendapatkan informasi berupa Alamat IP Ezviz 192.168.1.2, Shengzhen 192.168.1.3 dan pengujian serangan Denial of Services (DoS) yang berhasil memutus jaringan lalu lintas perangkat Ezviz dan Shengzhen.

Tools terakhir merupakan Metasploit untuk melakukan uji auntentikasi dengan metode brute force dengan perbedaan serangan, untuk Ezviz metode brute force dapat dilakukan dengan mereset password dari perangkat, sedangkan untuk perangkat Shengzhen dapat dilakukan dengan menebak tiap krendesial login karena menggunakan layanan Telnet yang. mengeksploitasi layanan yang rentan, memperoleh akses shell dan data konfigurasi perangkat.

2.5. Gambar

Nmap: Gambar 2 merupakan tools untuk memindai jaringan yang berbasis open-source dengan kegunaan menemukan dan memetakan perangkat yang terhubung dalam jaringan kompurer. Nmap dapat memungkinkan pengguna untuk melakukan proses pemindaian secara efisien dan baik terhadap satu perangkat maupun jaringan.



Gambar 2. Tools Nmap

Bettercap: Gambar 3 merupakan alat jaringan dan keamanan siber yang berbasis command-line untuk melakukan serangan pengintaian, Man-in-the-Middle, dan Denial of Services. Bettercap sangat mudah digunakan karena mendukung

 E-ISSN : 2722-0346

berbagai protocol jaringan seperti HTTP,HTTPS,TCP,UDP,ARP,DNS.



Gambar 3. Tools Bettercap

Metasploit: Gambar 4 merupakan framework untuk melakukan penetration testing atau uji coba keamanan sistem secara menyeluruh. Tools ini menyediakan kumpulan modul eksploitasi yang dapat digunakan pengguna untuk melakukan serangan terhadap kerentanan yang diketahui dalam system target yang termasuk CCTV IoT.



Gambar 4. Tools Metasploit

Ubuntu Linux: Gambar 5 merupakan sistem operasi berbasis Linux yang bersifat open- source. Sistem operasi ini digunakan untuk pada lingkungan server, cloud computingm dan pengujian keamanan siber karena kompatibel dengan banyak alat open source.



Gambar 5. Tools Ubuntu Linux

Gambar 6 merupakan table hasil pengujian menggunakan Nmap pada dua perangkat CCTV berbasis IoT, yaitu EZVIZ dan Shengzhen, berhasil memporoleh temuan penting. Pada perangkat Ezviz, port 8000 terdeteksi aktif dan layananan HTTP berjalan dengan baik. Tidak ditemukan kerentanan serius yang dapat dimanfaatkan dan tidak dapat mengambil informasi lebih dalam dari perangkat. Hasil pengujian juga konsisten pada hari pertama dan kedua, menunjukkan kondisi port dan layanan yang sama.

Sedangkan untuk perangkat Shengzhen, hanya terdeteksi port 23 yang terbuka dengan layanan yang sedang berjalanan telnet. Sama halnya dengan perangkat Ezviz, tidak ditemukan kerentanan parah serta tidak dapat memungkinkan untuk mengambil informasi sensitive dari perangkat. Pada perangkat Ezviz juga ditemukan port 8443 dengan layanan HTTPS yang berjalan, tetapi tanpa kerentanan yang signifikan.

PERANGKAT	EZVIZ		SHENGZHEN	Metode Serangan	LAYER
PORT	8000	8443	23		Network
IP ADDRES	192.168.1.2	192.168.1.2	192.168.1.3		Network
MAC ADDRESS	a0:ff:0c:83:43:2d	a0:ff:0c:83:43:2d	bc:fd:0c:d9:d2:86		Data Link
	PENGUJIAN				
NMAP Hari ke 1 ezviz: 21.59WIB 22.08WIB 22.33WIB 23.02WIB 23.31WIB Hari ke 1 Shengzhen: 0.09WIB 0.24WIB 0.40WIB 0.52WIB 1.05WIB	-Berhasil mendeteksi port 8000 dan layanan HTTP berjalan -Tidak terdeteksi kerentanan yang parah -Tidak dapat mengambil informasi perangkat	-Berhasil mendeteksi port 8443 dan layanan HTTPS berjalan -Tidak terdeteksi kerentanan yang parah -Tidak dapat mengambil informasi perangkat	-Mendeteksi port 23 dengan layanan Telnet -Tidak terdeteksi kerentanan yang parah -Tidak dapat mengambil informasi perangkat		Network
NMAP Hari ke 2 ezviz: 22.46WIB 23.01WIB 23.08WIB 23.15WIB 23.33WIB Hari ke 2 Shengzhen: 21.04WIB 21.17WIB 21.29WIB 21.48WIB 22.04WIB	-Berhasil mendeteksi port 8000 dan layanan HTTP berjalan -Tidak terdeteksi kerentanan yang parah -Tidak dapat mengambil informasi perangkat	-Berhasil mendeteksi port 8443 dan layanan HTTPS berjalan -Tidak terdeteksi kerentanan yang parah -Tidak dapat mengambil informasi perangkat	-Mendeteksi port 23 dengan layanan Telnet -Tidak terdeteksi kerentanan yang parah -Tidak dapat mengambil informasi perangkat		Network
NMAP	-Berhasil	-Berhasil	-Mendeteksi port 23		Network

Gambar 6. hasil penelitian

Pada Gambar 7 merupakan pengujian menggunakan Bettercap terhadap perangkat Ezviz dan Shengzhen, yang berhasil mengidentifikasi beberapa hal terkait serangan Man-in-the-Middle dan Denial Of Services. Pada pengujian MITM, perangkat Ezviz terbukti rentan dan berhasil mendapatkan informasi berupa kredensial, IP hostname, dan Mac address target.

Sama halnya dengan perangkat Shengzhen, pengujian ini menunjukkan hasil yang serupa, keberhasilan memperoleh kredensial, alamat IP, hostname, dan Mac address perangkat. Pengujian dengan menggunakan metode serangan DoS pada kedua perangkat Ezviz dan Shengzhen, sama-sama terbukti rentan dan serangan berhasil memutus koneksi lalu lintas perangkat ke gateway dan mengganggu akses perangkat. Pengujian tambahan pada perangkat Shengzhen juga memperlihatkan hasil serupa selama 3 hari tanpa ada perubahan yang signifikan.

PERANGKAT	EZVIZ		SHENGZHEN	Metode Serangan	LAYER
Hari ke 3 ezviz: 0.11WIB 15.06WIB 15.12WIB 15.22WIB 15.32WIB Hari ke 3 Shengzhen: 20.07WIB 20.18WIB 20.28WIB 20.39WIB 20.48WIB	mendeteksi port 8000 dan layanan HTTP berjalan -Tidak terdeteksi kerentanan yang parah -Tidak dapat mengambil informasi perangkat	mendeteksi port 8443 dan layanan HTTPS berjalan -Tidak terdeteksi kerentanan yang parah -Tidak dapat mengambil informasi perangkat	dengan layanan Telnet -Tidak terdeteksi kerentanan yang parah -Tidak dapat mengambil informasi perangkat -Mendeteksi port baru yang terbuka pada hari ke 3 pengujian tambahan yaitu RTSP 8554 dan 8699 VNYX		
BETTERCAP Hari ke 1 ezviz: 21.33WIB 22.18WIB 22.54WIB 23.19WIB 23.40WIB Hari ke 1 Shengzhen: 23.54WIB 00.18WIB 00.32WIB 00.45WIB 00.55WIB	-Tidak berhasil mendapatkan informasi kredensial -mendapatkan IP,hostname dan mac address (MITM): a0:ff:0c:83:43:2d	-Tidak berhasil mendapatkan informasi kredensial -mendapatkan IP,hostname dan mac address (MITM): a0:ff:0c:83:43:2d	-Tidak berhasil mendapatkan informasi kredensial -Berhasil mendapatkan Mac addres dan IP addres (MITM): bc:fd:0c:d9:d2:86 -Penambahan uji coba selama 3 hari tidak ada perubahan (Mac addres, hostname, IP) yang sama dengan pengujian pertama.	Man-in-the-Middle	Network
BETTERCAP Hari ke 1 ezviz: 21.33WIB 22.18WIB 22.54WIB 23.19WIB 23.40WIB Hari ke 1	-berhasil memutus serangan ke gateway (DoS)	-berhasil memutus serangan ke gateway (DoS)	-Berhasil memutus serangan ke gateway (DoS) -Penambahan uji coba selama 3 hari tidak ada perubahan (tetap	Denial of Services	Network

Gambar 7. hasil penelitian

Gambar 8 merupakan hasil pengujian lanjutan menggunakan tools Bettercap, yang dilakukan pada hari ke 2. Serangan Man-in-the-Middle menujukkan bahwa perangkat Ezviz tidak berhasil memberikan informasi kredensial, tetap dapat memberikan data seperti IP address, hostname, dan Mac Addres. Sedangkan pada perangkat Shengzhen, serangan MITM tetap sama mendapatkan alamat IP address, Mac address. Penyerang juga dapat mempertahankan hasil peroleh data tersebut selama 3 hari tanpa adanya perubahan.

PERANGKAT	EZVIZ		SHENGZHEN	Metode Serangan	LAYER
Shengzhen: 23.54WIB 00.18WIB 00.32WIB 00.45WIB 00.55WIB			berhasil DoS) yang sama dengan pengujian pertama.		
BETTERCAP Hari ke 2 ezviz: 22.42WIB 22.58WIB 23.06WIB 23.13WIB 23.31WIB Hari ke 2 Shengzhen: 20.56WIB 21.09WIB 21.21WIB 21.40WIB 21.56WIB	-Tidak berhasil mendapatkan informasi kredensial -mendapatkan IP,hostname dan mac address (MITM)	-Tidak berhasil mendapatkan informasi kredensial -mendapatkan IP,hostname dan mac address (MITM)	-Tidak berhasil mendapatkan informasi kredensial -Berhasil mendapatkan Mac addres dan IP addres (MITM) -Penambahan uji coba selama 3 hari tidak ada perubahan (Mac addres, hostname, IP) yang sama dengan pengujian pertama.	Man-in-the-Midlle	Network
BETTERCAP Hari ke 2 ezviz: 22.42WIB 22.58WIB 23.06WIB 23.13WIB 23.31WIB Hari ke 2 Shengzhen: 20.56WIB 21.09WIB 21.21WIB 21.40WIB 21.56WIB	-berhasil memutus serangan ke gateway (DoS)	-berhasil memutus serangan ke gateway (DoS)	-Berhasil memutus serangan ke gateway (DoS) -Penambahan uji coba selama 3 hari tidak ada perubahan (tetap berhasil DoS) yang sama dengan pengujian pertama..	Denial of Services	Network
BETTERCAP	-Tidak berhasil	-Tidak berhasil	-Tidak berhasil	Man-in-the-Middle	Network

Gambar 8. hasil penelitian

Gambar 9 hasil pengujian hari ke 3 menggunakan tools Bettercap pada perangkat CCTV Ezviz dan Shengzhen menunjukkan hasil yang konsisten dengan pengujian pada hari ke 2. Pada serangan Man-in-the-Middle yang menggunakan Bettercap, kedua perangkat tersebut tidak berhasil memberikan informasi kredensial baru, namun data dasar yang berupa IP address, hostname, dan Mac Addres tetap dapat diperoleh sehingga menandakan perangkat masih memiliki kerentanan meskipun tidak parah.

Serangan dengan metode Denial of Services pada perangkat Evziz dan Shengzhen terbukti Kembali perangkat rentan karena serangan berhasil memutus koneksi gateway dan membuat perangkat tidak dapat diakses. Dapat disimpulkan bahwa dari hari ke 2 dan ke 3 yang Dimana kondisi keamanan kedua perangkat tidak mengalami perbaikan dan tetap rentan terhadap serangan DoS. Hasil ini dapat memungkinkan pengambilan informasi dasar perangkat melalui serangan Man-in-the-Middle.

PERANGKAT	EZVIZ		SHENGZHEN	Metode Serangan	LAYER
Hari ke 3 ezviz: 00.08WIB 15.03WIB 15.09WIB Hari ke 3 Shengzhen: 19.59WIB 20.12WIB 20.22WIB 20.32WIB 20.42WIB	mendapatkan informasi kredensial -mendapatkan IP,hostname dan mac address (MITM)	mendapatkan informasi kredensial -mendapatkan IP,hostname dan mac address (MITM)	mendapatkan informasi kredensial -Berhasil mendapatkan Mac addres dan IP addres (MITM) -Penambahan uji coba selama 3 hari tidak ada perubahan perubahan (Mac addres, hostname, IP) yang sama dengan pengujian pertama.		
BETTERCAP Hari ke 3 ezviz: 00.08WIB 15.03WIB 15.09WIB Hari ke 3 Shengzhen: 19.59WIB 20.12WIB 20.22WIB 20.32WIB 20.42WIB	-berhasil memutus serangan ke gateway (Dos)	-berhasil memutus serangan ke gateway (DoS)	-Berhasil memutus serangan ke gateway (DoS) -Penambahan uji coba selama 3 hari tidak ada perubahan (tetap berhasil DoS) yang sama dengan pengujian pertama.	Denial of Services	Network

Gambar 9. hasil penelitian

Gambar 10 merupakan hasil pengujian dengan menggunakan tools Metasploit pada perangkat CCTV IoT dengan merek Ezviz dan Shengzhen, kedua perangkat masih relative aman terhadap serangan berbasis aplikasi. Pada perangkat Ezviz upaya bypass autentikasi tidak berhasil, reset kredensial juga tidak berhasil.

Akses shell sama halnya tidak berhasil dijalankan karena perangkat tidak memberikan respons apapun, dikarenakan adanya system pengamanan internal yang memblokir permintaan dari Metasploit. Percobaan pada dump data dan snapshot melalui port 8000 juga gagal, sehingga tidak dapat memungkinkan untuk mengambil informasi kredensial, data perangkat, maupun tampilan layer CCTV IoT.

Untuk perangka Shenzhen menunjukkan hasil yang mirip. Percobaan bypass autentikasi dan akses shell tidak berhasil dijalankan karena ada kecocokan kredensial maupun respons dari perangkat.

Untuk dump data dan control kamera juga sama gagal, meskipun perangkat rentan menerima permintaan eksploitasi, tetapi modul yang digunakan dalam Metasploit tidak cocok dengan system target sehingga serangan tidak memberikan hasil yang diharapkan. Faktor penggunaan protocol HTTPS/SSL pada Ezviz dan ketidak cocokan modul eksploitasi pada Shengzhen menjadi alasan mengapa serangan tidak membuahkan hasil.

PERANGKAT	EZVIZ		SHENGZHEN	Metode Serangan	LAYER
METASPLOIT Hari ke 1 ezviz: 21.48WIB 22.26WIB 22.57WIB 23.26WIB 23.41WIB Hari ke 1 Shengzhen: 00.00WIB 00.19WIB 00.33WIB 00.45WIB 00.56WIB	-Bypass autentikasi: Tidak berhasil mereset kredensial perangkat -Akses shell: Tidak berhasil mengakses, tidak ada respon dari target karena diblokir oleh perangkat CCTV IoT Ezviz - Dump data dan Snapshot: pada IP 192.168.1.2: 8000 tidak berhasil untuk mengambil informasi kredensial, informasi perangkat, dan Tangkapan layar CCTV IoT Ezviz - Tidak terdeteksi SSL karena menggunakan HTTP	-Bypass autentikasi: Tidak berhasil mereset kredensial perangkat -Akses shell: Tidak berhasil mengakses, tidak ada respon dari target. - Dump data dan Snapshot: Tidak berhasil. - Terdeteksi SSL karena menggunakan HTTPS.	-Bypass autentikasi: Tidak berhasil menemukan kecocokan kredensial dengan menggunakan teknik brute force -Akses Shell: tidak dijalankan karena bypass tidak berhasil -Dump data dan Kontrol Kamera Target rentan dan menerima eksploitasi, tetapi karena modul yang tidak cocok dengan target sehingga tidak ada hasil nya. -Uji coba yang dilakukan selama 3 hari tidak ada identifikasi kerentanan terbaru.	Brute Force	Application

Gambar 10. hasil penelitian

Gambar 11 merupakan hasil pengujian hari ke 2 dengan menggunakan tools Metasploit, pada perangkat Ezviz dan Shenzhen. Hasil pengujian tersebut kembali menunjukkan pola yang konsisten dengan hasil pada hari pertama. Pada perangkat CCTV IoT Ezviz, serangan bypass autentikasi tidak berhasil, begitu juga dengan upaya reset kredensial.

Percobaan pada akses shell juga tidak dapat dilakukan karena perangkat tidak memberikan respon apapun, karena adanya mekanisme keamanan internal seperti Intrusi deteksi sistem (IDS), firewall. Selain itu, percobaan pada dump data dan snapshot yang melalui port 8000 juga gagal sehingga tidak dapat memungkinkan untuk mengambil informasi kredensial maupun data perangkat CCTV berbasis IoT.

Hal ini dapat diperkuat dengan terdeteksinya penggunaan SSL/HTTPS pada Ezviz, yang menjadi lapisan perlindungan tambahan.

Pada perangkat Shengzhen, hasil dari pengujiannya sama. Serangan brute force tidak berhasil menemukan kecocokan kredensial, sehingga bypass autentikasi tidak berhasil

dilakukan. Percobaan akses shell juga tidak dapat dijalankan karena modul yang digunakan tidak sama. Untuk dump data dan kontrol kamera gagal juga meski target sebenarnya rentan dan menerima permintaan eksploitasi.

Kegagalan ini dapat disebabkan oleh ketidak sesuaian modul eksploitasi yang digunakan pada Metasploit dengan sistem perangkat target. Dari uji coba tambahan yang dilakukan selama dua hari tetap tidak ditemukan adanya identifikasi kerentanan baru pada perangkat Shengzhen.

PERANGKAT	EZVIZ		SHENGZHEN	Metode Serangan	LAYER
Hari ke 2 ezviz: 22.43WIB 22.59WIB 23.07WIB 23.13WIB 23.31WIB **Hari ke 2 Shengzhen:** 20.58WIB 21.10WIB 21.22WIB 21.41WIB 21.57WIB	-Bypass autentikasi: Tidak berhasil mereset kredensial perangkat -Akses shell: Tidak berhasil mengakses, tidak ada respon dari target karena diblokir oleh perangkat CCTV IoT Ezviz - Dump data dan Snapshot: pada IP 192.168.1.2: 8000 tidak berhasil untuk mengambil informasi kredensial, informasi perangkat, dan Tangkapan layar CCTV IoT Ezviz - Tidak terdeteksi SSL karena menggunakan HTTP	-Bypass autentikasi: Tidak berhasil mereset kredensial perangkat -Akses shell: Tidak berhasil mengakses, tidak ada respon dari target. - Dump data dan Snapshot: Tidak berhasil. - Terdeteksi SSL karena menggunakan HTTPS.	-Bypass autentikasi: Tidak berhasil menemukan kecocokan kredensial dengan menggunakan teknik brute force -Akses Shell: tidak dijalankan karena bypass tidak berhasil -Dump data dan Snapshot Target rentan dan menerima eksploitasi, tetapi karena modul yang tidak cocok dengan target sehingga tidak ada hasil nya. -Uji coba yang dilakukan selama 3 hari tidak ada identifikasi kerentanan terbaru.	Brute Force	Application

Gambar 11. hasil penelitian

Gambar 12 merupakan hasil pengujian hari ke 3 yang menggunakan tools Metasploit. Perangkat CCTV berbasis IoT dengan merek Ezviz dan Shenzhen kembali munjukkan hasil yang sama dengan hari-hari sebelumnya. Pada perangkat EZVIZ, upaya bypass autentikasi tidak berhasil dilakukan, begitu pula dengan percobaan reset kredensial.

Usaha untuk mendapatkan akses shell juga gagal karena perangkat tidak memberikan respons, kemungkinan besar karena adanya sistem proteksi dari perangkat CCTV IoT EZVIZ.

Percobaan dump data dan snapshot melalui port 8000 pun tidak berhasil, sehingga informasi penting seperti kredensial, data perangkat, maupun tampilan layar CCTV tidak dapat diambil. Selain itu, perangkat EZVIZ terdeteksi menggunakan SSL/HTTPS, yang memberikan tambahan lapisan keamanan terhadap eksploitasi.

Pada perangkat Shengzhen, hasil dari pengujiannya sama. Serangan brute force tidak berhasil menemukan kecocokan kredensial, sehingga bypass autentikasi tidak berhasil dilakukan.

Percobaan akses shell juga tidak dapat dijalankan karena modul yang digunakan tidak sama. Untuk dump data dan kontrol kamera gagal juga meski target sebenarnya rentan dan menerima permintaan eksploitasi.

Kegagalan ini dapat disebabkan oleh ketidak sesuaian modul eksploitasi yang digunakan pada Metasploit dengan sistem perangkat target.
Hasil dari pengujian hari ke 3 dapat mempertegas bahwa pada lapisan aplikasi, baik dari Perangkat Ezviz dan Perangkat Shenzhen masih cukup aman dari eksploitasi langsung menggunakan metasploit. Upaya untuk bypass autentikasi, brute force, reset kredensial, dan akses shell konsisten gagal dilakukan, sehingga perangkat tidak dapat ditembus melalui metode kerentanan dan serangan ini.

PERANGKAT	EZVIZ		SHENGZHEN	Metode Serangan	LAYER
METASPLOIT **Hari ke 3 ezviz:** 00.09WIB 15.04WIB 15.10WIB 15.21WIB 15.31WIB **Hari ke 3 Shengzhen:** 20.02WIB 20.12WIB 20.22WIB 20.33WIB 20.43WIB	-Bypass autentikasi: Tidak berhasil mereset kredensial perangkat -Akses shell: Tidak berhasil mengakses, tidak ada respon dari target karena diblokir oleh perangkat CCTV IoT Ezviz - Dump data dan Snapshot: pada IP 192.168.1.2: 8000 tidak berhasil untuk mengambil informasi kredensial, informasi perangkat, dan Tangkapan layar CCTV IoT Ezviz - Tidak terdeteksi SSL karena menggunakan HTTP	-Bypass autentikasi: Tidak berhasil mereset kredensial perangkat -Akses shell: Tidak berhasil mengakses, tidak ada respon dari target. - Dump data dan Snapshot: Tidak berhasil. - Terdeteksi SSL karena menggunakan HTTPS.	-Bypass autentikasi: Tidak berhasil menemukan kecocokan kredensial dengan menggunakan teknik brute force -Akses Shell: tidak dijalankan karena bypass tidak berhasil -Dump data dan Snapshot Target rentan dan menerima eksploitasi, tetapi karena modul yang tidak cocok dengan target sehingga tidak ada hasil nya. -Uji coba yang dilakukan selama 3 hari tidak ada identifikasi kerentanan terbaru.	Brute Force	Application

Gambar 12. hasil penelitian

3. HASIL DAN PEMBAHASAN

Pengujian ini dilakukan terhadap dua perangkat CCTV Berbasis IoT dengan merek Ezviz dan Shengzhen dengan menggunakan beberapa skenario serangan seperti: brute force untuk mengambil kredensial pada perangkat dan mencoba mereset kredensial perangkat, Man in the Middle (MITM) untuk mendapatkan informasi kredensial, Alamat IP, Mac Address, dan Denial of Services untuk memutus lalu lintas jaringan antara perangkat CCTV berbasis IoT ke gateway.

Tabel 3. Hasil Pengujian dua perangkat

Jenis Pengujian	CCTV Ezviz	CCTV Shengzhen	Keterangan
Brute Force	Tidak Berhasil	Berhasil	Ezviz sudah memiliki pertahanan login yang baik, dan shengzhen tidak memiliki pertahanan login sehingga bisa dilakuakan serangan brute force
MITM	Berhasil	Berhasil	Berhasil menyadap informasi berupa alamat IP 192.168.1.2 Ezviz dan Shengzhen 912.168.1.3, Mac Address bc:fd:0c:d9:d2:86 Shengzhen, a0:ff:0c:83:43:2d Ezviz dan hostname hanya ezviz yang berhasil diidentifikasi
DoS	Berhasil	Berhasil	Berhasil melakukan DoS dengan memutus jaringan dari perangkat ke gateway

Hasil dari pengujian yang disajikan pada tabel menunjukkan bahwa CCTV Shengzhen lebih rentan terhadap serangan dibandingkan dengan CCTV Ezviz. pengujian brute force dan DoS pada perangkat Shengzhen tidak memiliki mekanisme perlindungan yang cukup memadai, sehingga akses dapat diperoleh penyerang dan layanan terganggu pada penelitian ini jika kredensial berhasil ditebak penyerang dapat menggunakan perangkat untuk memantau CCTV dari jarak jauh.

Untuk Ezviz hanya pada brute force saja yang tidak berhasil dijalankan karena sudah memiliki proteksi keamanan login. Sama dengan perangkat Shengzhen, perangkat Ezviz juga terkena serangan Denial of Services yang berhasil memutus lalu lintas jaringan dari perangkat ke gateway sehingga mengganggu kinerja perangkat tersebut.

Serangan Man-in-the-Middle berhasil dijalankan yang mendapatkan beberapa informasi penting pada perangkat Ezviz dan Shengzhen, seperti Alamat IP 192.168.1.3 Shengzhen, Ezviz 192.168.1.2, Mac Address bc:fd:0c:d9:d2:86 Shengzhen, a0:ff:0c:83:43:2d Ezviz. Hostname hanya ezviz yang berhasil diiendentifikasi.

Pada temuan ini dapat memperkuat penelitian sebelumnnya yang menyebutkan bahwa perangkat IoT dengan keamanan rendah lebih rentan terhadap serangan autentikasi dan gangguan layanan jaringan.

Kontribusi penelitian ini ada pada mengungkap adanya celah keamanan pada CCTV IoT yang masih digunakan, khususnya pada perangkat CCTV IoT dengan merek Shengzhen yang tidak dilengkapi mekanisme pertahanan standar.

Menambahkan pertahanan tambahan seperti Intrusi Sistem Deteksi (IDS) pada dua perangkat CCTV IoT dengan IP 192.168.1.3 (Port 23 Telnet) Shengzhen bc:fd:0c:d9:d2:86 dan 192.168.1.2 (Port 8000 HTTP & Port 8443 HTTPS) Ezviz a0:ff:0c:83:43:2d, dengan merk Suricata karena mampu mendeteksi pola trafik secara real time, untuk menghindari serangan Denial of Services.

Penambahan firewall dengan merk pfSense yang dapat memblocking IP tertentu, rate limit untuk menghindari serangan Man-In-the-Middle pada perangkat CCTV IoT dengan IP 192.168.1.3 (Port 23 Telnet) Shengzhen bc:fd:0c:d9:d2:86 dan 192.168.1.2 (Port 8000 HTTP & Port 8443 HTTPS) Ezviz a0:ff:0c83:43:2d.

Pada port 8000 HTTP diganti dengan port 8443 HTTPS karena sudah menggunakan sertifikat keamanan enkripsi. Karena HTTPS sudah masuk standar keamanan.

Karena layer ini termasuk Application, maka metode Brute force digunakan dan berhasil dijalankan. Untuk mengatasi masalah tersebut sebaiknya menerapakan CAPTHA login untuk mencegah Brute force dan menguatkan kredensial pada IP 192.168.1.3 dengan port 23 Telnet.

Mengganti layanan Telnet ke HTTPS untuk mencegah metode Brute force dengan kerentanan bypass autentikasi, karena Telnet merupakan layanan tertua yang tidak dienkripsi dan termasuk ke Application layer

Menambahkan pertahanan tambahan seperti Intrusi Sistem Deteksi (IDS)[14] pada layer Network untuk kedua perangkat CCTV IoT dengan IP 192.168.1.3 Shengzhen dan 192.168.1.2

Ezviz, dengan merk Suricata karena mampu mendeteksi pola trafik secara real time, untuk menghindari serangan Denial of Services

Pada layer network ini menambahankan firewall dengan merk pfSense yang dapat memblocking IP tertentu, rate limit untuk menghindari serangan Man-In-the-Middle pada perangkat CCTV IoT Ezviz 192.168.1.2 dan Shengzhen 192.168.1.3

Port terbaru yang diidentifikasi pada hari ke 3 yaitu RTSP 8554 dan 8699 VNYX, sebaiknya penggunaan port 8554 dan 8699 dibatasi dan bisa menggunakan Firewall dengan merk pfSense untuk membatasi akses IP tertentu untuk mengakses kedua port tersebut.

5. SIMPULAN

Berdasarkan rumusan masalah dan hasil dari penelitian yang telah dilakukan pada perangkat CCTV berbasis IoT bahwa dapat disimpulkan perangkat tersebut memiliki berbagai potensi ancaman keamanan yang cukup serius.

Beberapa ancaman dapat teridentifikasi seperti Man-in-the-Middle untuk menangkap data login dan informasi penting seperti Alamat MAC bc:fd:0c:d9:d2:86 Shengzhen, a0:ff:0c:83:43:2d Ezviz, IP address Alamat IP 192.168.1.3 Shengzhen, Ezviz 192.168.1.2, dan hostname.

Eksploitasi kerentanan menggunakan Metasploit untuk melakukan bypass autentikasi, akses shell, dump data, dan control kamera.

Metode serangan yang berhasil diimplementasikan meliputi brute force menggunakan modul Metasploit, pada perangkat Shengzhen dapat digunakan untuk menebak kredensial yang masih menggunakan pengaturan default.

Serangan Man-in-the-Middle juga berhasil dilakukan pada kedua perangkat tersebut, yang dimana berhasil mendapatkan informasi sensitif seperti IP addres, hostname, dan Alamat MAC dapat disadap.

Metode serangan berupa Denial of Services terbukti mampu memutus koneksi lalu lintas dari perangkat CCTV ke gateway, akibatnya layanan tidak dapat diakses sesaat.

Solusi Perlindungan Keamanan yang diharapkan diantaranya adalah Menambahkan pertahanan tambahan seperti Intrusi Sistem Deteksi (IDS) pada dua perangkat CCTV IoT dengan merk Suricata karena mampu mendeteksi pola trafik secara real time, Penambahan firewall pada dua perangkat CCTV IoT dengan merk pfSense versi 24.11 yang dapat memblocking IP tertentu, rate limit, dan Khusus untuk CCTV IoT Shengzhen menerapkan Captha dan mengganti layanan Telnet menjadi HTTPS yang bersertifikat.

DAFTAR PUSTAKA

[1] R. P. Simanjuntak, R. Parlindungan Simanjuntak, R. Rikson, M. Sijabat, and E. P. Korespondensi, “Dike : Jurnal Ilmu Multidisiplin Meningkatkan Keamanan Siber dalam Lingkungan Internet of Things (IoT) dengan Menggunakan Sistem Deteksi Intrusi Berbasis Pembelajaran Mesin,” 2024.

[2] K. M. Alamsyah, P. Ulung, A. D. Fattah, M. Hanif Muzakky, and D. Pratama5, “JURNAL REIN (REKAYASA INFORMATIKA) Analisis Implementasi Internet of Things di Berbagai Bidang.”

[3] F. Majedi, A. Choirul Arifin, D. N. Fauzi, D. A. Wicaksono, M. Shafwallah, and A. Aziz, “Aplikasi Monitoring Keamanan (Majedi, dkk.) | 330 Nanggroe,” *Nanggroe: Jurnal Pengabdian Cendikia*, vol. 3, no. 6, pp. 330–333, 2024, doi: 10.5281/zenodo.13864617.

[4] Shafwan Iman Ramadhani, Ratu Farah Humainah, Aditio Nugroho, and Didik Aribowo, “Penerapan Komunikasi Data Pada Osi Layer PC to PC Menggunakan Cisco Packet Tracer,” *Jurnal Penelitian Rumpun Ilmu Teknik*, vol. 3, no. 2, pp. 66–76, May 2024, doi: 10.55606/juprit.v3i2.3791.

[5] A. Kurniawan, “SEJARAH, CARA KERJA DAN MANFAAT INTERNET OF THINGS.”

[6] E. Mutiha, P. Siagian, J. Siregar, and R. H. Siahaan, “ANALISIS KEAMANAN PADA SISTEM INTERNET OF THINGS UNTUK PENGENDALIAN PERANGKAT ELEKTRONIK RUMAH TANGGA,” *Jurnal Teknologi Informasi dan Industri*, vol. 4, no. 1, 2023.

[7] M. S. Asang and I. Sembiring, “Keamanan Data Pada Perangkat Internet Of Things Menggunakan Metode Public-Key Cryptography.”

[8] “jm_informatika,+31208-66912-1-ED+(3)”.

[9] Y. Efendi, “INTERNET OF THINGS (IOT) SISTEM PENGENDALIAN LAMPU MENGGUNAKAN RASPBERRY PI BERBASIS MOBILE,” *Jurnal Ilmiah Ilmu Komputer*, vol. 4, no. 1, 2018, [Online]. Available: http://ejournal.fikom-unasman.ac.id

[10] W. Setiawan, I. Made, and S. Ardana, “OKTAL : Jurnal Ilmu Komputer dan Science Implementasi Internet of Things Pada Sistem Kendali Lampu Rumah Menggunakan Telegram Messenger Bot Dan Board ESP”.

[11] W. Najib, T. Ancaman dan Solusi Keamanan, S. Sulistyo, and K. Kunci, “Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things (Review on Security Threat and Solution of Internet of Things Technology),” 2020.

[12] F. Antony and R. Gustriansyah, “Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata,” *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 1, pp. 43–52, Nov. 2021, doi: 10.30812/matrik.v21i1.1078.

[13] “IMPLEMENTASI IOT PADA SISTEM KEAMANAN CCTV BERBASIS NODEMCU Hendri Maruli Tua *Saniman**, Deski Helsa Pane*** *

Sistem Komputer, STMIK Triguna Dharma ** Sistem Komputer, STMIK Triguna Dharma ***Sistem Informasi, STMIK Triguna Dharma," 2020, [Online]. Available: https://ojs.trigunadharma.ac.id/

[14] Adi Ahmad, R. Maulana, and K. Akmal, "Data Privacy and Security in the Age of IoT A Comprehensive Study on Information System Vulnerabilities," *Journal Informatic, Education and Management (JIEM)*, vol. 6, no. 2, pp. 1–7, Jun. 2024, doi: 10.61992/jiem.v6i2.78.