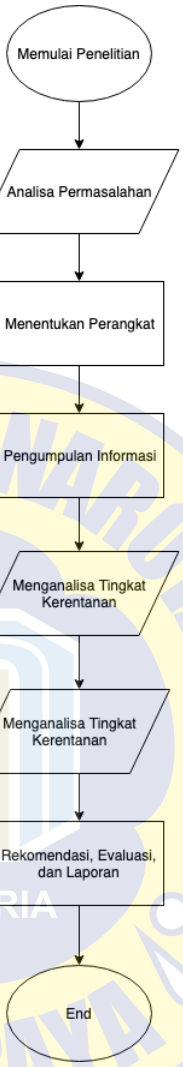
BAB III

METODE PENELITIAN

3.1 Alur Pembahasan Penelitian

Berdasarkan rumusan masalah dari penelitian ini diperlukan tahapan-tahan untuk menyelesaikan permasalahan tersebut dengan cara yang sistematis dan nantinya akan menjadi pedoman yang jelas dan mudah untuk diterapkan dalam menyelesaikan permasalahan pada peneletian ini. Tahapan tersebut akan digambarkan pada Gambar 3.1.



Gambar 3. 1 Diagram Alur Penelitian

3.2 Analisa Permasalahan

Perangkat-perangkat pendukung industri 4.0 yang lebih banyak memanfaatkan sensor-sensor yang saling terhubung dan perangkat utama seperti router, scada, ics, ip camera, dan nas server adalah salah satu contoh perangkat yang dikonfigurasi untuk terhubung ke internet dengan jaringan

ip public. Terhubungnya perangkat-perangkat tersebut membuat banyak sekali attacker memanfaatkan celah keamanan untuk melakukan *take over* ke suatu perusahaan melalui router mereka atau mengontrol segala bentuk aktifitas yang bisa mereka manfaatkan dari perangkat-perangkat yang terkoneksi ke internet dengan jaringan *ip public* tersebut. Maka dari itu diperlukannya kesadaran terhadap jenis serangan tersebut karena sering terjadi para engineer dari sebuah perusahaan hanya melakukan konfigurasi pernagkat-perangkat tersebut secara standar tanpa dilakukan konfigurasi khusus dan membatasi atau menghapus kredensial user yang tidak berhak untuk melakukan baca dan tulis pada perangkat-perangkat tersebut.

3.3 Menentukan Perangkat Yang Akan Diteliti

Dalam penelitian ini penulis telah membatasi perangkat-perangkat pendukung industri 4.0 yang akan dijadikan sampel untuk mengetahui celah kerentanan pada perangkat-perangkat tersebut dan nantinya akan dicari ID CVE dari perangkat yang sudah dikumpulkan informasinya. Berikut adalah daftar perangkat yang akan dijadikan sampel

Tabel 3. 1 Jenis dan Model Perangkat

Jenis	**Router**	**Scada**	**IP Cam**	**NAS**	**ICS**
Merek	Zte	AKCP	Speco	Western Digital	Modbus
	TP-Link	Schneider Electric	ACTi	Seagate	Omron
	Ubiquiti	CirCarLife Scada	HikVision	Synology	HART Ip

3.4 Pengumpulan Informasi

Pada tahap ini adalah untuk mengumpulkan informasi terkait port, ip, tipe dari perangkat-perangkat yang akan kita cari informasinya dan nantinya data-data tersebut akan diverifikasi kembali menggunakan nmap apakah data yang dikeluarkan shodan sudah valid. Setelah data-data tersebut dikatakan valid maka akan dilakukan proses selanjutnya yaitu mencari informasi terkait kerentanan pada perangkat-perangkat yang sudah dikumpulkan informasinya.

3.5 Melakukan Pengumpulan Data CVE

Setelah mengumpulkan informasi terkait perangkat-perangkat yang akan di uji, disini kita melakukan tahap pengumpulan informasi terkait CVE atau *Common Vulnerability and Exposure* yang berada di website https://cve.mitre.org dan mengumpulkan berapa banyak nomor CVE yang keluar untuk perangkat tersebut jika semakin banyak nomor CVE yang

keluar pada jenis perangkat tersebut dapat dipastikan perangkat tersebut menjadi focus para pelaku kejahatan siber.

3.6 Menganalisa Tingkat Kerentanan

Jika dalam tahap pengumpulan data CVE ada perangkat yang belum memiliki nomor CVE maka peneliti akan melakukan perhitungan secara manual dengan parameter sebagai berikut : Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality, Integrity, dan Availability. Setelah mendapatkan skor dari parameter-parameter tersebut baru dapat disimpulkan terkait kerentanan pada perangkat yang belum memiliki nomor CVE tersebut. Dan pada tahap ini juga peneliti menghitung terkait tingkat kerentanan yang terjadi pada perangkat-perangkat tersebut.

Tabel 3. 2 Tabel CVSS

No	Perangkat	Attack Vector	Attack Complexity	rivileges Require	User Interaction	Scope	onfidientalit	Integrity	Availability	Score
1	Mikrotik	Network(N)	Low(L)	None(N)	None(N)	Unchanged(U	None(N)	High(H)	None(N)	7.5
2	Zte	Network(N)	Low(L)	None(N)	None(N)	Unchanged(U	None(N)	Low(L)	None(N)	5.3
3	Scada	Network(N)	Low(L)	Low(L)	None(N)	Unchanged(U	None(N)	High(H)	None(N)	6.5

3.7 Menghitung Data CVE dan Tingkat Kerentanan

Pada tahap ini peneliti menghitung berapa banyak perangkat yang positif bisa dikenakan serangan siber dan berapa banyak jumlah CVE yang tercatat untuk perangkat tersebut sehingga peneliti dapat memberikan rekomendasi terkait perangkat-perangkat yang masih banyak menggunakan tipe lama dengan firmware yang masih memiliki kerentanan. Dan kurang lebih peneliti akan menuliskannya pada tabel seperti dibawah ini.

Tabel 3. 3 Tabel Penilaian Kerentanan

No	Perangkat	Tipe	CVE	Validasi Perangkat	Positif	Negatif
1	Mikrotik	RB750	14	On	✓	
2	Zte	HG5610	6	On	✓	
3	Scada	AKCP	3	On		✓

3.8 Rekomendasi, Evaluasi dan Laporan

Dalam tahap ini adalah untuk memberikan rekomendasi terkait celah kerentanan yang sering terjadi pada perangkat-perangkat pendukung industri 4.0 agar perangkat-perangkat yang mereka gunakan dapat terhindar dari tindak kejahatan siber. melakukan evaluasi dan penyusunan laporan penelitian.