BAB I
PENDAHULUAN

1.1. Latar Belakang

Jaringan yang saling terhubung dengan internet merupakan celah keamanan yang dapat dieksploitasi dan diserang, hal ini menjadi lebih beresiko jika didalamnya terdapat informasi atau data-data penting. Data-data penting yang berisi informasi tersebut merupakan hal yang sangat berharga, maka dari itu bermunculan beberapa pihak yang tidak bertanggungjawab, yang kemudian pihak tersebut berusaha atau berkeinginan mencuri maupun merusak dan mengubah data atau informasi. Banyak cara yang bisa digunakan untuk mendeteksi serangan maupun penyusupan, diantaranya *network, packet sniffing, monitoring* layanan dan *scanning*. Dengan cara-cara seperti itu kita bisa mengizinkan, memblokir maupun menyaring paket yang mencoba menyusup ke dalam sebuah jaringan atau ingin mengakses sumber daya maupun layanan tertentu (Firdaus & Hendrawan, 2019).

Mayoritas serangan saat ini adalah hasil dari eksploitasi melalui celah *port-port* yang terbuka. Berdasarkan laporan yang dikeluarkan oleh The European Union Agency for Network and Information Security (ENISA) salah satu dari masalah keamanan jaringan yang terjadi di bulan Mei 2017 adalah menyebarnya crypto-ransomwar yang memiliki banyak nama lain seperti WannaCry/WannaCrypt/ WannaCryptor/WCrypt/WCRY yang menyerang berbagai perusahaan dan organisasi. *WannaCry* menyebar dengan mengeksploitasi celah kerentanan yang terletak pada *port* 445. *Port* 445 sendiri adalah *port* yang dipakai oleh SMB *(Server Message Block).* Untuk membantu menjaga keamanan jaringan dan layananya dari serangan sejenis itu khususnya pada *server* SIPT, penelitian ini dilakukan untuk mencari tahu celah kerentanan yang terdapat pada *server* SIPT, melakukan *monitoring* pada *port server*, memaparkan serta merekomendasikan hal-hal yang bertujuan untuk pengamanan jaringan dan layananya pada *server* SIPT.

SIPT (Sistem Informasi Perguruan Tinggi) milik Universitas Buana Perjuangan Karawang (UBP Karawang), dimana didalamnya terdapat data-data penting yang perlu dilindungi dari ancaman pihak-pihak yang tidak bertangungjawab. Data - data penting yang terdapat di SIPT diantaranya adalah data *profile* mahasiswa UBP

Karawang dan data nilai mahasiswa. Didalam data *profile* mahasiswa terdapat data-data yang bersifat privasi seperti: No. KTP (Kartu Tanda Penduduk), alamat rumah, tempat dan tanggal lahir, data orang tua serta No. *handphone*. Data-data tersebut sangat mungkin untuk disalahgunakan, selain itu pada periode tertentu pihak UBP Karawang diwajibkan melaporkan data nilai ke PDDikti (Pangkalan Data Pendidikan Tinggi), jika sistem keamanan untuk melindungi data lemah dan terjadi perubahan data nilai oleh pihak yang tidak bertanggungjawab maka akan terjadinya ketidaksesuain data antara data di SIPT UBP Karawang dengan PDDikti. Oleh karena itu diperlukan sistem keamanan yang baik untuk perlindungan data-data tersebut. Untuk mengetahui tingkat keamanan yang sudah diterapkan oleh UBP Karawang maka perlu dilakukan sebuah analisis *vulnerability* (kerentanan) keamanan jaringan.

Teknik yang digunakan untuk menganalisis kemanan jaringan yaitu dengan menggunakan aplikasi nmap, nesssus dan owasp zap. Nmap merupakan sebuah *software* yang bisa digunakan untuk mencari informasi *port-port* yang terbuka serta dapat melihat *host* yang aktif pada jaringan. Nessus berfungsi sebagai audit kemanan suatu sistem yang kemudian menampilkan informasi celah kerentanan dari proses *scan host* target yang akan dianalisa (Masykur, Studi, Informatika, Teknik, & Ponorogo, 2015) sedangkan Owasp Zap adalah sebuah *tools scanner open source* yang dapat digunakan untuk pengujian penetrasi situs web. Serangan yang ditujukan kepada jaringan *server* SIPT di Universitas Buana Perjuangan Karawang dapat dilakukan oleh pihak luar maupun civitas akademik iternal. Serangan yang dilakukan oleh pihak luar bisa berupa melakukan *Denial of Service* (DOS) terhadap *server web* SIPT yang ada atau berusaha menembus masuk kedalam sistem informasi.

Adapun penelitian yang berkaitan dengan analisis keamanan jaringan diantaranya adalah penelitian yang dilakukan Rendro, Ngatono dan Aji pada tahun 2020 yang menganalisis *monitoring* sistem keamanan jaringan komputer menggunakan *software* Nmap (Studi kasus di SMK Negeri 1 Kota Serang) dari penelitian tersebut dilakukan proses *scanning* pada IP *host target* 192.168.105.254 jaringan LAN milik SMK Negeri 1 Kota Serang dan menghasilkan informasi beberapa *port* yang terbuka diantaranya adalah *port* 22 tcp ssh, *por*t 53 tcp domain,

port 80 tcp dan *port* 443 selain informasi *open port* didapatkan pula infomasi mengenai layanan dan versi layanan yang digunakan oleh *host target*. Selain IP *host target* proses *scanning* juga dilakukan pada *website* e-raport.smkn1serang.sch.id (Rendro, Ngatono, & Aji, 2020)

Selain itu, Ade Hendri Herawan pada tahun 2019 melaukan penelitian analisis keamanan *vulnerability* pada *server* absensi kehadiran laboratorium di program studi teknik informatika dengan menggunakan *tools* nmap dan nessus penelitian ini menghasilkan *monitoring* yakni beberapa *port* yang terbuka pada *server* absensi kehadiran laboratorium dantaranya *port* 53 dns, *port* 80 *web server*, *port* 21 ftp dan *port* 1723 *point-to-point tunelling,* selain itu didapatkan 4 kategori *vulnerablity* dari IP *host target* berupa 7 *vulnerability* kategori *info*, 12 kategori *medium*, 7 kategori *high* dan 2 untuk kategori *critical* (Kamilah & Hendri Hendrawan, 2019). Pada tahun 2019 Dicky Septian Firdaus juga melakukan penelitian analisis keamanan *vulnerability* pada sever Cloud Open Media Vault di fakultas teknik Ibn Khaldun Bogor. Penelitian ini menggunakan *software* nmap dan nessus, dari proses *scanning* pada IP *host target* ditemukan 6 *port* yang terbuka dan dari rekomendasi didapatkan solusi sebanyak 13 solusi yang disarankan untuk menyelesaikan masalah 17 *vulnerability*. 4 kategori *vulnerability* berupa 1% kategori critical, 1% kategori *high*, 5% kategori *medium* serta 10% untuk kategori *info* (Firdaus & Hendrawan, 2019).

Berdasarkan paparan tersebut, penulis terdorong untuk melakukan penelitian mengenai analisis *vulnerability* pada SIPT Universitas Buana Perjuangan Karawang , harapan hasil penelitian ini adalah dapat menemukan *vulnerability* pada *server* SIPT UBP Karawang serta memberikan solusi dari temuan yang ada.

1.2. Rumusan Masalah

Rumusan masalah pada penelitian ini adalah:

1. Bagaimana mendapatkan informasi *vulnerability* pada *server web* SIPT di Universitas Buana Perjuangan Karawang.
2. Bagaimana rekomendasi terhadap temuan keamanan *vulnerability* pada *server web* SIPT di Universitas Buana Perjuangan Karawang.

1.3. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mendapatkan hasil *monitoring* analisis kemanan *vulnerability* pada *server web* SIPT di Universitas Buana Perjuangan Karawang.
2. Mendapatkan rekomendasi dari temuan keamanan *vulnerability* pada *server* SIPT sebagai solusi dari hasil penelitian.

1.4. Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Mendapatkan data informasi celah keamanan yang dapat dimanfaatkan untuk keperluan penguatan *server web*.
2. Mencegah serangan dari pihak-pihak internal dan *external* dengan cara menutup temuan dari *vulnerability* yang sudah didapat mulai dari kategori *critical, high, medium* dan *info*.