BAB 1. PENDAHULUAN

1.1. Latar Belakang

Keamanan jaringan merupakan aspek penting dalam menjaga sebuah integritas, kerahasiaan, dan ketersediaan data dalam sebuah sistem. Pada era digital saat ini ancaman siber menjadi semakin kompleks, dengan berbagai celah keamanan yang dapat dimanfaat oleh pihak yang tidak bertanggung jawab untuk merusak sistem atau mencuri informasi (Ginanjar, 2022). Salah satu ancaman umum adalah eksploitasi kerentanan pada layanan jaringan, seperti File Transfer Protocol (FTP).

FTP sendiri merupakan protokol yang digunakan untuk mentransfer file dalam suatu jaringan. Banyak institusi, termasuk pemerintahan dan perusahaan, mengandalkan FTP untuk berbagi data antar sistem (Imam Rafi, 2022). Meskipun memiliki berbagai fitur yang mendukung pengelolaan file, beberapa versi ProFTPD memiliki celah keamanan. Salah satu versi yang rentan adalah ProFTPD 1.3.3c, yang memiliki kerentanan yang memungkinkan penyerang memperoleh akses tanpa autentikasi dan menjalankan perintah berbahaya pada sistem target .

ProFTPD (*Professional File Transfer Protocol Daemon*) adalah perangkat lunak yang digunakan sebagai layanan FTP Server. ProFTPD merupakan perangkat lunak *open source* yang sering digunakan pada lingkungan Linux dan Unix. Pada dasarnya ProFTPD berfungsi sebagai media transfer file antar komputer yang memiliki jarak cukup jauh, Dengan media ProFTPD dapat mempermudah pengguna saat melakukan transfer file tanpa harus melakukan kontak fisik secara langsung (M. Syawal Saputra, t.t.).

Badan Siber dan Sandi Negara (BSSN) adalah lembaga pemerintah yang bertugas untuk menjaga keamanan siber dan persandian nasional di Indonesia. BSSN berperan sebagai penyedia solusi keamanan berbasis teknologi informasi dalam menghadapi ancaman siber yang terus berkembang (Ginanjar, 2022). Dalam menjalankan tugasnya, BSSN melakukan monitoring terhadap berbagai layanan

jaringan yang digunakan oleh instansi pemerintahan dan infrastruktur kritis, termasuk layanan FTP. Layanan FTP seperti ProFTPD sering digunakan dalam berbagai sistem untuk pertukaran data, kelemahan dalam layanan ini dapat menjadi celah bagi serangan siber.

Jenis Serangan Eksploitasi pada ProFTPD Eksploitasi pada layanan FTP dapat terjadi melalui berbagai metode, seperti:

a Eksploitasi autentikasi – Menyerang kelemahan dalam mekanisme login untuk mendapatkan akses tanpa kredensial yang sah.
b Eksekusi kode jarak jauh (*Remote Code Execution* - RCE) – Memanfaatkan celah dalam layanan untuk menjalankan perintah berbahaya di sistem target.

Pada ProFTPD versi 1.3.3c, terdapat kerentanan yang memungkinkan penyerang mengeksekusi kode berbahaya dari jarak jauh tanpa autentikasi, sehingga memberikan akses penuh ke sistem target.

Dalam konteks pengujian ProFTPD dapat menggunakan berbagai alat dan teknik untuk mendeteksi serta mengevaluasi celah keamanan. Salah satu alat yang umum digunakan adalah Metasploit, sebuah alat yang banyak digunakan dalam dunia keamanan siber untuk simulasi serangan. Proses ini mencakup berbagai langkah, mulai dari pengumpulan informasi menggunakan network scanning, identifikasi layanan yang rentan, hingga eksploitasi terhadap kerentanan yang ditemukan (Tabassum, 2021).

Salah satu aktivitas pembelajaran selama kegiatan magang adalah pengujian keamanan jaringan dengan mengeksploitasi kerentanan layanan FTP. Aktivitas ini bertujuan untuk memahami proses pengujian keamanan jaringan secara praktis, khususnya pada layanan FTP ProFTPD versi 1.3.3c, yang memiliki celah keamanan signifikan.

Kegiatan ini bertujuan untuk melatih kemampuan menganalisis celah keamanan dan memahami cara kerja pelaku yang memanfaatkan kerentanan.

Dengan belajar ini, diharapkan pemahaman tentang pentingnya menjaga keamanan jaringan, terutama di lingkungan kerja, dapat meningkat.

1.2. Tujuan Magang

1.2.1 Tujuan Umum Magang

Tujuan Magang secara umum adalah :

a. Membantu mahasiswa mengembangkan keterampilan dan pengetahuan terkait aktivitas di perusahaan, industri, atau instansi tertentu;
b. Memberikan kesempatan kepada mahasiswa untuk mendapatkan pengalaman kerja langsung sehingga lebih memahami dinamika dunia kerja;
c. Melatih mahasiswa agar mampu bersikap kritis dan peka terhadap situasi di lingkungan kerja nyata;
d. Menghubungkan keterampilan yang telah dipelajari di kampus dengan praktik nyata melalui kegiatan magang;
e. Membuka peluang bagi mahasiswa untuk membangun jaringan profesional yang bermanfaat bagi karier di masa depan dan bertemu dengan para ahli di bidangnya.

1.2.2 Tujuan Khusus Magang

Tujuan Magang secara khusus adalah :

a. Mengembangkan aplikasi *web* Sistem Informasi sederhana untuk mendukung kebutuhan internal unit kerja di BSSN;
b. Memperoleh pemahaman dasar mengenai *penetration testing (pentest)*,dengan mencoba mengeksploitasi server atau perangkat lain yang berada dalam jaringan yang sama, menggunakan Kali Linux;
c. Mempelajari dasar *cybersecurity in depth* melalui sesi berbagi pengetahuan dengan para ahli di bidangnya;

d. Mempelajari dasar-dasar *Open Source Intelligence (OSINT)* dan penerapannya dalam mendukung upaya keamanan siber.

1.2.3 Manfaat Magang

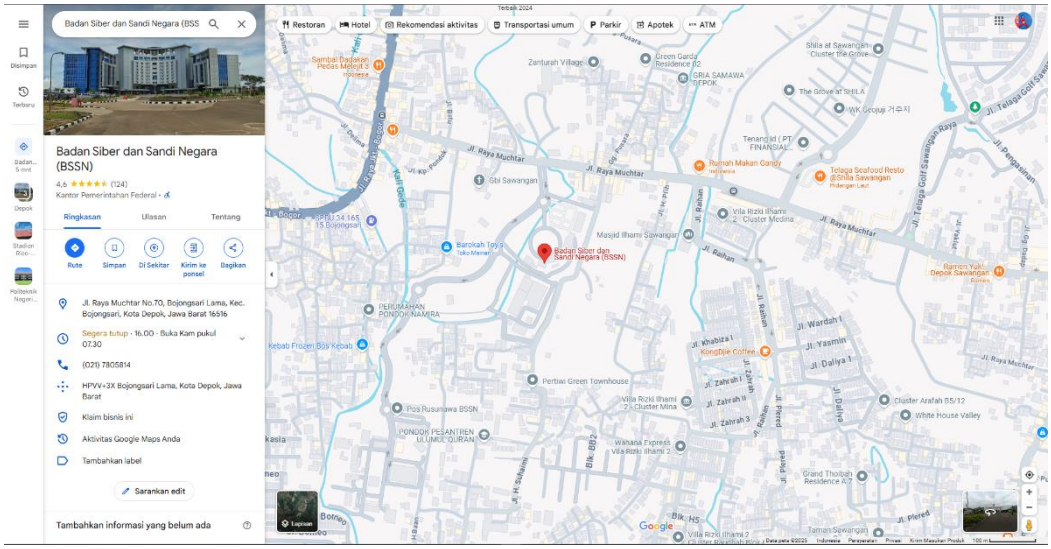
Manfaat Magang adalah sebagai berikut:

a. Memperdalam serta dapat mengembangkan keterampilan dan kreativitas tiap individu dalam sebuah lingkungan kerja yang berkaitan dengan program studi yang tengah diampu, menjadi lebih siap dengan tantangan di masa mendatang pada ranah profesional.
b. Memperoleh wawasan yang lebih luas mengenai aspek keamanan siber secara menyeluruh melalui pembelajaran dan diskusi dengan para praktisi.
c. Menambah keterampilan praktis dalam melakukan penetration testing dasar dan meningkatkan pemahaman mengenai cara kerja serangan siber pada sistem dan jaringan.

1.3. Lokasi dan Waktu

1.3.1 Lokasi

Lokasi magang berada di Badan Siber dan Sandi Negara (BSSN) yang terletak di Jl. Raya Muchtar No.70, Bojongsari Lama, Kec. Bojongsari, Kota Depok, Jawa Barat 16516. Berikut merupakan peta lokasi kantor BSSN Sawangan.



Gambar 1. 1 Denah Lokasi Magang

1.3.2 Waktu

Program magang ini yang telah dijadwalkan berlangsung selama empat bulan, yaitu dari tanggal 7 Oktober 2024 hingga 31 Januari 2025. Di Badan Siber dan Sandi Negara (BSSN), kegiatan magang dilakukan secara luring. Jam kerja dimulai pukul 07.30 hingga 16.00 WIB dari Senin sampai Kamis, sedangkan pada hari Jumat, jam kerja berlangsung dari pukul 07.30 hingga 16.30 WIB. Untuk memastikan kemajuan pekerjaan, setiap satu minggu sekali kami melaporkan perkembangan progres kepada pembimbing teknis yang bertugas memberikan arahan serta umpan balik terkait tugas yang sedang dikerjakan.

1.4. Metode Pelaksanaan

a. Dilakikan metode pembelajaran secara mandiri dan studi literatur untuk dapat menunjang aktivitas selama magang.
b. Rapat Mingguan, dilakukan pertemuan dengan pembimbing teknis untuk melaporkan hasil dari pengembangan dan perkembangannya. Laporan ini mencakup pada fitur yang telah berhasil diselesaikan, kendala teknis yang terjadi selama pengembangan, serta solusi terhadap kendala yang dihadapi selama proses pengembangan.
c. Melaksanakan pengembangan program berdasarkan pembagian tugas dari proyek magang. Aktivitas ini meliputi pengkodean, pengujian, serta integrasi fitur ke dalam sistem dengan kebutuhan dan arahan dari pembimbing teknis.