# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Warnet Galeri Informatika terletak di dusun Karangasem, desa Bulurejo, Kecamatan Semin, Kabupaten Gunungkidul. Warnet ini memiliki sembilan komputer *client*. Tidak hanya melayani keperluan *browsing*, namun juga *game online*. Galeri Informatika adalah warnet kedelapan di kecamatan Semin, sekaligus menjadi yang terakhir berdiri hingga saat ini.

Menurut administrator jaringan, pengunjung terbanyak adalah usia anak-anak hingga remaja. Sedangkan penggunaan akses lebih banyak untuk keperluan *update game* daripada *browsing*.

Akses cepat untuk *download update game* adalah salah satu keunggulan Galeri Informatika dibandingkan Warnet lainnya dalam lingkup kecamatan Semin. Kecepatannya mencapai 60 hingga 70 mbps. Kemampuan tersebut cukup menguntungkan pihaknya. Namun bagi pihak tertentu, hal ini dapat dianggap sebagai ancaman dalam hal persaingan usaha.

Muncul usaha yang diduga sengaja dilakukan untuk merugikan Warnet Galeri Informatika dalam persaingan ini. Menurut pengakuan administrator, pernah ada percobaan *login* terhadap server proxy oleh orang yang tidak diketahui.

Mengetahui permasalahan berupa ancaman keamanan tersebut, penulis melakukan penelitian dengan objek server proxy Warnet Galeri Informatika. Dari penelitian ini, penulis ingin mengetahui kelemahan pada objek dan bagaimana cara menanggulanginya, kemudian memberikan rekomendasi kepada administrator jaringan di lokasi objek.

**1.2 Rumusan Masalah**

Rumusan masalah merupakan acuan atau arah penelitian yang dilakukan. Adapun perumusan masalahnya adalah sebagai berikut.

1. Bagaimana menganalisa keamanan server proxy di Warnet Galeri Informatika menggunakan metode testing penetrasi?
2. Bagaimana rekomendasi penanggulangan celah keamanan pada server proxy berdasarkan testing penetrasi yang telah dilakukan?

**1.3 Batasan Masalah**

Penelitian ini mencakup observasi dan pembuktian. Observasi akan berupa scanning untuk mencari *vulnerability* pada objek. Sedangkan pembuktian yang dimaksud adalah melakukan *testing attack* terhadap objek berdasarkan *vulnerability* yang telah ditemukan saat scanning.

Sesuai dengan judul yang dipilih dan untuk menghindari meluasnya permasalahan, maka skripsi ini membatasi masalah yang meliputi:

1. Melakukan analisa *vulnerability* dengan dengan Nessus.

2. Melakukan testing penetrasi pada server proxy Warnet Galeri Informatika menggunakan Metasploit. Dilakukan secara virtual menggunakan Oracle Virtual Box dan server proxy yang diteliti bersifat *cloning*.
3. Metode testing penetrasi mengacu pada standar *Penetration Testing Execution Standard* (PTES) yang dapat dilihat pada situs www.pentest-standard.org.
4. Skenario analisis dan serangan berada di LAN Warnet, bukan dari luar
5. Membahas langkah-langkah analisa dan *testing attack*. Kemudian penulis menyajikannya dalam bentuk *report* untuk diberikan kepada administrator jaringan. Skripsi ini tidak termasuk penerapan rekomendasi dari laporan akhir.

## 1.4 Tujuan Penelitian

Adapun tujuan dilakukannya penelitian adalah sebagai berikut.

1. Sebagai syarat untuk menyelesaikan pendidikan program Strata 1 (S1) di jurusan Teknik Informatika pada Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta.
2. Setelah menganalisa dan melakukan pembuktian, penulis ingin menyampaikan rekomendasi untuk menanggulangi celah keamanan pada server proxy Warnet Galeri informatika

## 1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut.

1. Setelah melakukan penelitian ini dan mendapatkan gelar sarjana strata 1 (S1), diharapkan dapat meningkatkan pengetahuan dan menambah pengalaman tentang keamanan jaringan yang nantinya bisa digunakan dalam dunia kerja secara langsung.
2. Rekomendasi yang diberikan oleh penulis kepada administrator jaringan Warnet Galeri Informatika dalam bentuk *report*, diharapkan dapat digunakan oleh administrator sebagai bahan pertimbangan mengamankan server proxy-nya di kemudian hari.

## 1.6 Metode Penelitian

Penyusunan laporan penelitian ini menggunakan metode-metode sebagai berikut.

1. Metode *Penetration Testing Execution Standard* (PTES)
    a. *Pre-engagement interactions*; aspek persetujuan dengan klien.
    b. *Intellegence gathering*; pengumpulan informasi tentang target.
    c. *Vulnerability analysis*; melakukan analisa kerentanan.
    d. *Threat modelling*; menyusun rencana pembuktian.
    e. *Exploitation*; implementasi rancangan pembuktian.
    f. *Post exploitation;* memanfaatkan kerentanan lebih lanjut.
    g. *Reporting;* menyampaikan laporan analisis dan pembuktian.

2. Metode Wawancara

   Wawancara terhadap administrator jaringan Warnet Galeri Informatika untuk mengetahui topologi jaringan, manajemen jaringan dan konfigurasi jaringan.

3. Metode Kepustakaan

   Mempelajari materi dari sumber buku yang valid dan jelas.

**1.7 Sistematika Penulisan**

BAB I PENDAHULUAN

Berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode pengumpulan data, sistematika penulisan dan rencana kegiatan.

BAB II LANDASAN TEORI

Berisi tinjauan pustaka serta uraian teori yang relevan dengan objek penelitian yang digunakan sebagai dasar untuk pembahasan. Dapat berupa definisi atau model lain yang langsung berkaitan dengan ilmu atau masalah yang diteliti.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Menjelaskan proses *intelligence gathering*, *vulnerability analysis* hingga *threat modelling*.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Menganalisa hasil *vulnerability analysis*, kemudian *exploitation*. Memberikan penjelasan tentang mengurangi resiko keamanan pada server proxy dalam bentuk *report*.

BAB V PENUTUP

Menguraikan tentang kesimpulan dari pelaksanaan seluruh kegiatan dan beberapa saran dari peneliti kepada pihak yang akan membuat skripsi dengan tema yang sama di masa yang akan datang.

DAFTAR PUSTAKA

Sumber pustaka yang menjadi acuan dan referensi ilmiah, digunakan peneliti sebagai teori yang valid untuk mendukung penelitian.

**1.8 Rencana Kegiatan**

**Tabel 1.1 Jadwal Kegiatan**

| No | Kegiatan | Deskripsi | Maret 2014 | | | | April 2014 | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 1. | Persiapan | - Perizinan dan legalitas kegiatan<br>- Wawancara dengan administrator jaringan mengenai kondisi dan konfigurasi objek | | | | | | | | |
| 2. | Observasi | - *Reconnaissance*<br>- *Scanning*<br>- *Gaining access*<br>- *Maintaining access*<br>- *Covering tracks*; | | | | | | | | |
| 3. | *Reporting* | Membuat *report* dengan standar tertentu. | | | | | | | | |
| 4. | Penulisan laporan skripsi | Menyusun laporan penelitian | | | | | | | | |