BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Universitas Multimedia Nusantara atau yang biasa disingkat menjadi UMN adalah sebuah universitas yang berada di bawah naungan Yayasan Multimedia Nusantara dan didirikan oleh Kompas Gramedia pada tahun 2005. UMN terletak di daerah kabupaten Tangerang, tepatnya di daerah Gading Serpong. UMN sendiri memiliki visi menjadi perguruan tinggi unggulan di bidang ICT (*Information and Communication Technology*)[1]. Di era globalisasi saat ini, perkembangan teknologi informasi dan komunikasi (TIK) mengalami kemajuan yang sangat cepat, di mana kebutuhan teknologi informasi menjadi elemen yang dianggap sangat penting dalam kehidupan masyarakat. Salah satu teknologi yang sangat banyak digunakan pada saat ini adalah *website*.

Menurut Vermaat (2018), *website* adalah kumpulan halaman yang saling terhubung yang di dalamnya terdapat beberapa item seperti dokumen dan gambar yang tersimpan di dalam *web server* [2]. *Website* pun semakin hari memiliki banyak jenis dan kegunannya, mulai dari *website* untuk membaca berita, *website* menonton film, *website* organisasi / pemerintah, dan masih banyak lagi. Tentunya dengan semakin banyak *website* yang ada, data yang dimasukkan ke dalam *website* pun semakin banyak pula, karena sebagian besar dari *website* memerlukan kita untuk melakukan *register* / *login* untuk menggunakan fungsinya secara maksimal.

Untuk memenuhi visi UMN di bidang ICT, UMN menyiapkan berbagai *website* untuk mendukung kegiatan perkuliahan. Beberapa *website* yang dibuat secara mandiri oleh tim IT UMN adalah *gapura.umn.ac.id* yang berguna sebagai layanan pintu kegiatan non akademik dan juga *academic.umn.ac.id* yang berguna sebagai layanan skripsi mahasiswa. Berkaitan dengan perkembangan teknologi, maka keamanan informasi dalam sebuah *website* menjadi sesuatu yang penting. Salah satu indikator pentingnya keamanan informasi adalah dengan melihat pentingnya informasi yang tersimpan. Kedua *website* tersebut memiliki data penting yang berkaitan dengan aset UMN dan juga data pribadi milik mahasiswa dan data - data penting tersebut dapat terancam bocor jika terjadi serangan dunia maya. Oleh karena itu, kedua *website* tersebut dapat dijadikan sebagai subjek percobaan *penetration testing* dalam penelitian ini.

Di negara Indonesia, serangan dunia maya sangat sering terjadi. Data yang diperoleh dari Badan Siber dan Sandi Negara menyatakan bahwa serangan dunia maya di Indonesia pada tahun 2022 mencapai angka sembilan ratus tujuh puluh enam juta kasus dan jenis serangan dunia maya yang banyak ditemukan adalah serangan *malware* [3]. Selain itu menurut Mikalauskas (2021), beberapa serangan paling umum kepada *website* adalah *Distributed Denial of Service* (DDOS), *Cross-site Scripting* (XSS), *Web-based Malware*, *SQL Injection*, dan *PHP Vulnerabilities* [4].

Universitas Multimedia Nusantara (UMN) yang memanfaatkan berbagai situs untuk mewujudkan visinya pun pernah menjadi salah satu korban serangan dunia maya. Riwayat dari penyerangan tersebut dapat diketahui dari salah satu *website* arsip *defacement* yaitu http://zone-h.org/archive/filter=1/fulltext=1/domain=umn.ac.id. Dari keterangan diatas, dapat dilihat bahwa serangan paling baru yang terjadi pada *website* dengan *domain* umn.ac.id adalah serangan pada *ejournals.umn.ac.id*. *Website ejournal* milik UMN mengalami *redefacement*. *Defacement* adalah sebuah *attack* yang dimana *website* dimodifikasi oleh pihak yang tidak berwenang. Hal ini meliputi perubahan terhadap tampilan atau pun terhadap konten asli dari *website* tersebut [5].

Dalam menjaga keamanan data dan informasi, terdapat metode yang dapat dilakukan yaitu metode *penetration testing*. *Penetration testing* merupakan proses yang melibatkan proses analisis kepada sebuah *website* untuk mencari potensi celah keamanan seperti kesalahan konfigurasi, kesalahan pengembangan *software* maupun *hardware*, dan kelemahan dalam logika proses [6] . Dalam melakukan *penetration testing*, penulis akan menggabungkan dua metode *hacking* yaitu *zero entry hacking* (ZEH) dan juga *Open Web Application Security Project* (OWASP). *Zero entry hacking* akan digunakan sebagai acuan metode penelitian secara keseluruhan, sementara itu untuk *Open Web Application Security Project* (OWASP) akan digunakan ketika penelitian masuk ke tahap eksploitasi (*exploitation*). Metode *Open Web Application Security Project* (OWASP) dipilih karena berdasarkan penelitian sebelumnya, metode tersebut adalah yang paling cocok untuk melakukan *penetration testing* ke sebuah *website* [7].

Open Web Application Security Project (OWASP) merupakan aplikasi berbasis *web* pengujian keamanan non profit dari Amerika Serikat yang digunakan sebagai *framework* pengujian keamanan [8]. Penggunaan *framework* OWASP melakukan pendekatan sederhana untuk menghitung dan menilai risiko pada *web*. Dengan mengetahui risiko yang akan terjadi memudahkan untuk mengetahui

kerentanan *web* dan mengurangi risiko yang terjadi [9] .

Terjadinya serangan – serangan tersebut memperkuat argumen penulis untuk mengambil topik penelitian tentang keamanan sistem informasi dengan judul penelitian "Analisis Tingkat Keamanan *Website* Universitas Multimedia Nusantara dengan Metode *Penetration Testing*". Diharapkan dari penelitian ini dapat memberikan manfaat bagi UMN, dimulai dari pengujian kerentanan, pencarian celah kerentanan serta memberikan rekomendasi untuk menutupi celah yang ada sehingga ke depannya UMN dapat terhindar dari serangan dunia maya.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan, maka rumusan masalahnya adalah bagaimana tingkat keamanan dari *website gapura.umn.ac.id* dan *academic.umn.ac.id* menggunakan metode *penetration testing* dan penilaian menggunakan indikator CVSS v4.0?

1.3 Batasan Permasalahan

Berdasarkan rumusan masalah yang ada, maka batasan masalah pada penelitian ini adalah :

1. Terdapat dua *website* Universitas Multimedia Nusantara yang akan diuji tingkat keamanannya, yaitu *gapura.umn.ac.id* dan *academic.umn.ac.id*.
2. Penelitian ini menggunakan sistem operasi Kali Linux 2022.2 dengan menggunakan VMware Workstation 16 Player sebagai *virtual machine*.
3. *Penetration testing tools* yang digunakan pada penelitian ini adalah Nmap v7.92, Zmap, Masscan, Dnschecker.org, pentest-tools.com, Owasp Zap, Burp Suite, dan WireShark.
4. Penelitian ini menggunakan metode *Zero Entry Hacking* (ZEH) dan OWASP tanpa menggunakan *Social Engineering*, yang kemudian *vulnerability* yang ditemukan akan dianalisis menggunakan *Common Vulnerability Scoring System* (CVSS) v4.0.

1.4 Tujuan Penelitian

Berdasarkan latar belakang masalah yang telah dijelaskan, maka tujuan dari penelitian ini adalah :

1. Melakukan pengujian dan analisis terhadap *website* Universitas Multimedia Nusantara untuk mengetahui kondisi serta mengetahui tingkat kerentanan *website* menggunakan metode *penetration testing* dan penilaian menggunakan indikator CVSS v4.0.
2. Mendapatkan hasil *penetration testing* dan menjelaskan celah keamanan yang diperoleh dari *website* Universitas Multimedia Nusantara sehingga dapat membantu untuk memperbaiki kegagalan dalam mempertahankan keamanan *website* Universitas Multimedia Nusantara.

1.5 Manfaat Penelitian

Manfaat yang didapatkan dari analisis keamanan website Universitas Multimedia Nusantara adalah :

1. Bagi Peneliti
   (a) Untuk memenuhi salah satu syarat kelulusan di Universitas Multimedia Nusantara.
   (b) Menjadikan penelitian ini sebagai sebuah pengalaman langsung melakukan *penetration testing* kepada pihak di dunia nyata.
2. Bagi Instansi Terkait
   (a) Sebagai acuan untuk menjadi bahan evaluasi keamanan sistem informasi.
   (b) Untuk mengurangi kemungkinan terbobol nya sistem keamanan informasi oleh *attacker* luar.

1.6 Sistematika Penulisan

- Bab 1 PENDAHULUAN
  Bab pertama ini memberi penjelasan mengenai latar belakang pengambilan masalah, rumusan masalah, batasan masalah, tujuan dari penelitian, manfaat

penelitian, dan sistematika penulisan.

- Bab 2 LANDASAN TEORI
  Pada bab kedua akan dijelaskan mengenai teori-teori yang digunakan sebagai acuan dalam penelitian ini, mulai dari *vulnerability assesment, penetration testing, common vulnerability scoring system*, dan *zero entry hacking*.

- Bab 3 METODOLOGI PENELITIAN
  Pada bab ketiga akan dijelaskan mengenai metodologi yang digunakan dalam penelitian ini secara lebih detail, selain itu dilampirkan juga *tools* - *tools* apa saja yang akan digunakan.

- Bab 4 HASIL DAN DISKUSI
  Pada bab keempat akan dijelaskan mengenai hasil dari tahapan - tahapan metodologi yang telah dijelaskan pada bab sebelumnya, hasil dari *penetration testing* tersebut akan disimpulkan, dinilai, dan diberi solusinya.

- Bab 5 KESIMPULAN DAN SARAN
  Pada bab kelima akan dijelaskan mengenai kesimpulan dari penelitian yang telah dilakukan dan saran untuk penelitian kedepannya.