

# BAB I

## PENDAHULUAN

### A. Latar Belakang Masalah

Pada era internet saat ini, informasi sangat mudah diperoleh dan disebarluaskan. Oleh karena itu, informasi menjadi aset yang sangat berharga baik bagi perseorangan, pemerintah maupun swasta. Informasi memiliki nilai dan harus dilindungi, sehingga menjadi penting bagi individu untuk melakukan perlindungan terhadap informasi. Informasi sangat berharga karena jika suatu informasi tersebut berada di tangan pihak yang tidak berhak bisa disalahgunakan. Kemudahan layanan informasi dan kemajuan teknologi menjadi faktor utama terciptanya koneksi komunikasi antar umat manusia di segala penjuru bumi. Di satu sisi, informasi akan gampang mengalir dan didapatkan, baik itu informasi yang faktual maupun hoaks. Konsekuensinya, manusia dituntut untuk menjadi lebih bijak dalam koneksi didirikan baik dalam urusan pribadi, karena jika kurang berhati-hati dalam berkomunikasi dapat membahayakan kerahasiaan dan keamanan informasi pribadi.

Sniffing adalah tindak kejahatan penyadapan yang dilakukan menggunakan jaringan internet dengan tujuan utama untuk mengambil data dan informasi sensitive secara illegal. Cara kerja sniffing adalah ketika terhubung ke jaringan yang bersifat *public*, saat melakukan proses transfer data dari client server dan sebaliknya. Karena data yang mengalir pada client dan server yang bersifat bolak-balik, sniffing ini akan menangkap paket-paket yang dikirimkan dengan cara illegal menggunakan tools pembantu.

Universitas Muhammadiyah Purwokerto memiliki beberapa web server yang

bertujuan untuk mendukung penyelenggaraan pendidikan, sehingga dapat tersedia layanan informasi yang lebih baik dan efektif, baik didalam maupun diluar perguruan tinggi melalui internet. Berbagai kebutuhan dalam bidang pendidikan maupun peraturan yang melingkupinya sedemikian tinggi, sehingga pengelolaan akademik dalam suatu lembaga pendidikan menjadi pekerjaan yang sangat menguras waktu, tenaga dan pikiran. Sistem Informasi Akademik dan Onclass merupakan web server yang sangat membantu dalam kegiatan perkuliahan serta memberikan informasi terutama pada situasi saat ini yang mengharuskan perkuliahan secara online. Dalam situasi saat ini dimana perkuliahan dilakukan secara online dan segala aktivitas hanya dapat dilakukan dari rumah, onclass menjadi media yang disediakan oleh Universitas Muhammadiyah Purwokerto untuk menunjang perkuliahan secara daring. Sementara Sistem Informasi Akademik sangat membantu mahasiswa untuk mendapat informasi mengenai perkuliahan secara lebih mudah yang dapat diakses dimana saja. Untuk mengakses web server Universitas Muhammadiyah Purwokerto, mahasiswa diharuskan melakukan login dengan cara memasukkan username berupa nomor induk mahasiswa dan password. Ketika proses pengiriman data dari client ke server dan sebaliknya, disinilah yang paling rawan terjadi tindak kejahatan sniffing. Jadi saat melakukan login pada web server perlu selalu waspada, apakah ada *sniffer* yang mencoba mencuri data username dan password atau tidak.

Penelitian ini mengacu pada penelitian yang berjudul “Analisis Keamanan Website terhadap Sniffing Process pada Jaringan Nirkabel Menggunakan Aplikasi Wireshark (Studi Kasus : Simak Unismuh)”, membahas tentang gambaran umum tentang keamanan website Simak Unismuh terhadap proses sniffing pada jaringan nirkabel, serta

gambaran umum tentang kemungkinan metode serangan yang dapat terjadi pada website Simak Unismuh. Penelitian ini juga memberikan solusi kepada pengguna internet dan web developer untuk mencegah serangan dari kerentanan yang ditemukan. Dalam penelitian ini dilakukan dua tahap, yang pertama yaitu mengidentifikasi tingkat keamanan website Simak Unismuh menggunakan aplikasi Wireshark dan yang kedua yaitu membandingkan tingkat keamanan website Simak Unismuh dengan Google Account untuk mengetahui kelemahannya. Hasil dari penelitian ini adalah dengan penyerangan packet sniffing pada website Simak Unismuh, dapat merekam dan menampilkan informasi sensitif seperti username dan password dengan menggunakan aplikasi wireshark. Selain itu website Simak Unismuh rentan terhadap serangan MITM (man in the middle), karena belum menggunakan sertifikat SSL.

Berdasarkan uraian di atas maka perlu dilakukan penelitian untuk mempelajari keamanan web server Universitas Muhammadiyah Purwokerto terhadap sniffing. Oleh karena itu, diambillah bahan mengenai keamanan web server untuk judul skripsi “Analisis Keamanan Web Server Universitas Muhammadiyah Purwokerto Terhadap Packet Sniffing Menggunakan Wireshark”.

## **B. Perumusan Masalah**

Perumusan masalah pada penelitian ini adalah :

1. Apakah web server Universitas Muhammadiyah Purwokerto aman terhadap proses sniffing *passive* pada jaringan nirkabel?
2. Bagaimana cara menganalisa keamanan web server Universitas Muhammadiyah Purwokerto terhadap sniffing *passive*?

### **C. Batasan Masalah**

Untuk menghindari pembahasan yang meluas maka penulis akan membatasi masalah yang akan dianalisis yaitu :

1. Dilakukan analisis keamanan web server sistem informasi akademik Universitas Muhammadiyah Purwokerto dan onclass Universitas Muhammadiyah Purwokerto pada jaringan nirkabel.
2. Penggunaan aplikasi Wireshark untuk menganalisa keamanan web server Universitas Muhammadiyah Purwokerto terhadap tindakan sniffing *passive* pada jaringan nirkabel.

### **D. Tujuan Penelitian**

Adapun tujuan yang ingin dicapai dari penelitian ini yaitu untuk mengetahui keamanan web server Universitas Muhammadiyah Purwokerto terhadap proses sniffing pada jaringan nirkabel menggunakan wireshark.

### **E. Manfaat Penelitian**

Manfaat yang diperoleh dari penelitian ini adalah sebagai berikut :

1. Sebagai data yang bisa diberikan dan digunakan oleh pihak IT Universitas Muhammadiyah Purwokerto guna menjadi bahan pertimbangan dan masukan dalam upaya meningkatkan keamanan web server yang lebih baik.
2. Meningkatkan pemahaman bagi pengguna yang awam terhadap bahaya keamanan informasi yang bersifat pribadi