BAB V
PENUTUP

5.4. Kesimpulan

Project Monitoring Bandwidth dan Malware pada Network Perusahaan yang dilakukan penulis selama masa PKL ini menerapkan pengimplementasian alat pemantauan dan sistem keamanan yang dapat mendeteksi dan mencegah serangan *malware* dan *virus* secara *real-time.* Media untuk melakukan implementasi pemantauan berupa website milik Perusahaan yang berisi fitur-fitur untuk melakukan manajemen dan memantau Network di Perusahaan.

Fitur-fitur yang ada pada website mendukung pemantauan jaringan secara *real-time* untuk mengawasi kinerja dan kondisi jaringan. Salah satu fitur yang sangat berguna untuk melakukan monitoring yaitu *Local Report*. Kita dapat melihat beberapa dokumen dan isi di dalam dokumen tersebut merupakan rincian dari Bandwidth dan Malware di tanggal tersebut. Dengan adanya informasi rinci tersebut dapat segera mendeteksi dan menanggulangi masalah yang muncul.

Selain itu dengan adanya fitur Log Details juga membantu kita untuk melakukan analisis mendalam mengenai virus-virus yang menyerang jaringan. Karena di fitur tersebut kita bisa melihat detail dari virus-virus pada Network. Salah satunya informasi detail mengenai Level virus. Kita bisa mengetahui level virus dan kategori bahaya dari Virus. Sehingga kita bisa melakukan langkah selanjutnya untuk melakukan penanganan terhadap virus yang memiliki kategori berbahaya yang menyerang Network.

5.5. Saran

Beberapa saran ini mungkin bisa meningkatkan pengembangan Website yang digunakan untuk Monitoring Bandwidth dan Malware di Network Perusahaan dan strategi untuk menangani adanya serangan, yaitu:

1. Peningkatan Keamanan Login:
   Menambahkan fitur pemantauan aktivitas login untuk mendeteksi dan menginformasikan pengguna tentang upaya login yang mencurigakan atau tidak sah dengan memiliki tanda tertentu untuk mengidentifikasi jika ada user yang tidak sah sedang mengakses Website.
2. Optimasi Dashboard dan User Experience:
   Memastikan dashboard memiliki desain yang responsif dan intuitif, sehingga pengguna dapat dengan mudah mengakses dan mudah memahami informasi penting mengenai kinerja jaringan. Memberikan akses ke fitur-fitur tertentu berdasarkan peran pengguna untuk menghindari akses yang tidak perlu dan meningkatkan keamanan.
3. Strategi Mitigasi Serangan Malware dan Virus:
   Memastikan sistem antivirus selalu diperbarui dengan definisi virus terbaru untuk memberikan perlindungan maksimal terhadap ancaman baru.
4. Edukasi dan Pelatihan: Menyediakan edukasi dan pelatihan rutin bagi karyawan mengenai praktik keamanan siber terbaik, termasuk cara mengidentifikasi dan menghindari phishing dan serangan malware.

Berikut merupakan saran yang mungkin berguna untuk meningkatkan Monitoring Bandwidth dan Malware di Network Perusahaan agar bisa lebih waspada lagi dan mempersiapkan plan lain apabila ada permasalahan yang lebih buruk nantinya.