BAB 5
KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Dari hasil penelitian yang dilakukan dengan pemindaian menggunakan Nmap dan Nessus, berikut ini kesimpulan dari data yang telah dihasilkan.

1. Hasil pemindaian pada *website e-learning* FKES UNJAYA menunjukkan hanya ada satu kategori yaitu *Info*. Kategori ini mengindikasikan risiko minimal dengan tidak ada kerentanan yang memiliki dampak signifikan pada *website* tersebut dan sekedar memberikan informasi dari pemindaian yang dilakukan. Sehingga, secara keseluruhan *website e-learning* tersebut aman.
2. Hasil pemindaian tersebut terbagi menjadi 8 kelompok dengan total 21 hasil pemindaian. Semua hasil pemindaian termasuk dalam kategori *Info* dengan *score* 100%. Dari 8 kategori *output* yang ditemukan berdasarkan pemindaian, terdapat 2 jenis kerentanan dengan beberapa masalah (*multiple issues*) yaitu HTTP (Web *Servers*) dan HTTP (CGI *abuses*).
3. Dari semua data hasil pemindaian hanya ada 4 jenis *output* yang diberikan saran rekomendasi solusi oleh Nessus, diantaranya:
    a. HSTS *Missing from* HTTPS Server.
    b. *Missing or Permissive Content-Security-Policy frame-ancestors* HTTP *Response Header*.
    c. *Missing or Permissive X-Frame-Options* HTTP *Response Header*.
    d. Adanya *port* yang terbuka (Nessus SYN *scanner*).

5.2 SARAN

Berikut adalah saran yang dapat diberikan kepada pengelola Pusat Sistem Informasi FKES Universitas Jenderal Achmad Yani Yogyakarta berdasarkan penelitian yang telah dilakukan:

1. Implementasikan Rekomendasi Solusi: Dari hasil rekomendasi solusi yang telah disusun, sangat diharapkan agar dapat diimplementasikan. Tujuannya

adalah untuk mencegah tindakan penyerangan dari pihak yang tidak bertanggung jawab dengan memperbaiki kerentanan yang ada sekecil apapun dampaknya.

2. Rutin Memperbarui Keamanan *Website*: Selalu perbarui keamanan *website* dengan melakukan pengujian kerentanan secara rutin. Setiap kali ada pembaharuan pada *website*, pastikan untuk menguji kembali keamanan agar tetap terjaga dan terhindar dari potensi risiko.
3. Pada penelitian selanjutnya diharapkan dapat melakukan analisis lebih dalam terkait resiko *Downgrade Attacks, SSL Stripping Man in The Middle Attacks, Cookie Hijacking, Cross Site Scripting* (XSS), dan *Clickjacking*. Serta melakukan *Penetration Testing* dari hasil identifikasi pada penelitian ini.

Semoga saran-saran ini membantu dalam meningkatkan keamanan sistem informasi di Fakultas Kesehatan Universitas Jenderal Achmad Yani Yogyakarta.

.