Laporan Simulasi Keamanan Cyber

Nama : Aprintan Dwi Cahyani

NIM : 2231740021

Prodi : D3 Teknologi Informasi PSDKU Lumajang

1. Identifikasi Layanan Web Server

a. Layanan yang Diidentifikasi

Layanan	Deskripsi
A	Portal e-commerce (berbasis PHP), digunakan pelanggan untuk transaksi
B	Dashboard internal marketing (berbasis WordPress)

b. Tools yang Digunakan dan Langkah-Langkah

Layanan A (PHP): Menggunakan Nikto

Perintah: nikto -h http://target-ecommerce.com

Layanan B (WordPress): Menggunakan WPScan

Perintah: wpscan --url http://dashboard-marketing.com --enumerate p

c. Hasil Pemindaian

Tools	Hasil
Nikto	- Header server terlalu terbuka - File konfigurasi (phpinfo, .git) dapat diakses publik
WPScan	- WordPress versi lama - Plugin usang & rentan - Tema tidak di-update

2. Penanganan Kerentanan

Layanan A:

- Sembunyikan header informasi server (ServerTokens Prod, ServerSignature Off)

- Batasi akses ke file sensitif dengan konfigurasi .htaccess atau Nginx

- Update PHP ke versi terbaru

Layanan B:

- Update WordPress ke versi terbaru

- Hapus plugin tidak digunakan atau rentan

- Aktifkan Web Application Firewall (WAF)

- Gunakan plugin keamanan seperti Wordfence

3. Pemindaian Keamanan Jaringan

Tools: Nmap

Perintah: nmap -sS -sV -O 192.168.1.0/24

Hasil:

Temuan	Penjelasan
Port terbuka	Beberapa port seperti 23 (telnet), 21 (FTP) terbuka tanpa enkripsi
OS tidak di-update	Versi sistem operasi lawas ditemukan
Layanan di port non-standar	Layanan jalan di port tidak lazim, tanpa dokumentasi yang jelas

Fitur Pembeda Tools:

Tools	Fokus Pemindaian
Nikto	Web server & file konfigurasi
WPScan	WordPress (plugin, tema, versi)
Nmap	Jaringan (port, OS, service)

4. Pengujian SSH Remote Access

Tools: Hydra

Perintah: hydra -L user.txt -P pass.txt ssh://192.168.1.100

Hasil: Beberapa akun berhasil login (contoh: admin:admin123), menunjukkan kelemahan autentikasi.

Antisipasi:

- Ganti semua password default

- Terapkan login via SSH key

- Batasi akses hanya dari IP terpercaya dengan iptables atau firewall

5. Kebijakan dan Prosedur Keamanan

- Password Policy: Password minimal 12 karakter, kombinasi huruf besar/kecil, angka, simbol

- Update Policy: Penjadwalan update aplikasi & server setiap minggu/bulan

- Monitoring & Scanning Rutin: Gunakan tools (Nikto, WPScan, Nmap) secara berkala

- Pelatihan SDM: Edukasi karyawan tentang phishing, remote access, dan data handling

6. Rekomendasi Peningkatan Keamanan

Implementasi Teknologi:

- SIEM (Splunk, Graylog) – untuk log terpusat dan analisis insiden

- IDS/IPS (Snort, Suricata) – deteksi dan blok serangan

- WAF – proteksi aplikasi web

- Patch Management System – otomatisasi pembaruan sistem

Model Arsitektur:

- Zero Trust Security – verifikasi semua akses

- Network Segmentation – pisahkan jaringan penting dari umum