LAPORAN SIMULASI KEAMANAN SIBER

Anggota: absen/nim/nama

1. 03/2231740003/Aldi Nur Fahmi,
2. 12/2231740032/Dhydan Darwan R,
3. 19/2231740019/M.Calvin Rozil Hufron K

---

1. Identifikasi Layanan Web Server

1.1. Tools yang Digunakan

- Nikto
- WPScan (digunakan untuk latihan deteksi WordPress)

1.2. Langkah-Langkah

- Jalankan Nikto untuk memindai web server:

nikto -h http://[IP-DVWA]

- Jalankan WPScan untuk mendeteksi plugin, tema, dan konfigurasi WordPress yang rentan (jika digunakan dalam simulasi lain).

1.3. Hasil

- Nikto mendeteksi:
    - Informasi server terlalu terbuka.
    - Directory listing aktif.
    - File konfigurasi publik dapat diakses.
- WPScan (jika digunakan): mendeteksi plugin WordPress usang dan kerentanan CVE.

---

2. Penanganan Kerentanan

Rekomendasi Penanganan

- Sembunyikan header server (ServerTokens Prod).

- Nonaktifkan directory listing (Options -Indexes).
- Batasi akses ke file .conf, .bak, .php~ dengan .htaccess.
- Perbarui plugin dan core CMS jika digunakan.
- Gunakan WAF seperti ModSecurity.

Referensi

- OWASP Top 10: https://owasp.org/www-project-top-ten/
- Apache Security Tips: https://httpd.apache.org/docs/2.4/misc/security_tips.html

---

3. Pemindaian Keamanan Jaringan

3.1. Tools

- Nmap
- Nessus
- OpenVAS

3.2. Langkah

nmap -sS -sV -O [IP Target]

3.3. Hasil

- Port Telnet dan FTP terbuka.
- SSH aktif dengan konfigurasi default.
- OS server tidak diperbarui.
- Nessus/OpenVAS menunjukkan celah CVE kritikal.

3.4. Perbedaan Tools

Tools	Fokus	Kelebihan
Nmap	Port scanning	Cepat dan ringan
Nessus	Vuln scan	Database CVE lengkap

Tools Fokus Kelebihan

OpenVAS Vuln scan (FOSS) Gratis dan komprehensif

---

4. Pengujian SSH Remote Access

Tools

- Hydra

hydra -L user.txt -P pass.txt ssh://[IP DVWA]

Hasil

- Akun "admin" berhasil diakses dengan password "admin123".
- Terindikasi penggunaan kredensial default.

Antisipasi

- Ganti semua password default.
- Gunakan autentikasi SSH key.
- Implementasikan fail2ban.
- Batasi akses SSH hanya dari IP terpercaya.

---

5. Kebijakan dan Prosedur

Rekomendasi Kebijakan:

- Password minimal 12 karakter + simbol.
- SOP pemindaian mingguan dan bulanan.
- Otentikasi 2FA untuk akses sensitif.
- Prosedur backup & recovery.

---

6. Rekomendasi untuk Peningkatan Keamanan

- SIEM seperti Wazuh atau Splunk untuk pemantauan log terpusat.

- IDS/IPS seperti Snort atau Suricata.
- Segmentasi Jaringan berdasarkan fungsi dan akses.
- Zero Trust Architecture untuk memverifikasi semua entitas.
- Automated Patching System dan Monitoring Dashboard.