LAPORAN UAS

Oleh:

Danis Asfa Ramadhan	(2231740030)
Martasari Dwi Ningtias	(2231740007)
Nur Manda Devi Puspita Wangi	(2231740011)

Dosen Pengajar:

Vipkas Al Hadid Firdaus, S.T, M.T.

PROGRAM STUDI D3 TEKNOLGI INFORMASI

POLITEKNIK NEGERI MALANG PSDKU LUMAJANG

TAHUN 2025

SKENARIO SIMULASI KEAMANAN CYBER

1. **Identifikasi Layanan Web Server**

   Tools yang digunakan:

   a. Nikto (untuk layanan A: e-commerce berbasis PHP)

   b. WPScan (untuk layanan B: dashboard internal berbasis WordPress)

   Langkah-langkah:

Nikto	WPScan
1. Menentukan target IP/domain layanan A. 2. Menjalankan perintah: nikto -h http://ip_layanan_A 3. Menyimpan hasil scan untuk analisis.	1. Mengidentifikasi URL dashboard WordPress (layanan B). 2. Menjalankan perintah: wpscan --url http://ip_layanan_B --enumerate p 3. Jika menggunakan API Token dari WPScan, bisa juga mengecek kerentanan plugin secara detail.

   c. Hasil:

   Layanan A (Nikto):

   - Header server terlalu terbuka (Apache/2.4.41 (Ubuntu))
   - File .git, phpinfo.php, dan backup.zip dapat diakses public

   Layanan B (WPScan):

   - WordPress versi lawas terdeteksi (v4.x)
   - Plugin Contact Form 7 dan Slider Revolution belum diperbarui, ditemukan kerentanan eksploitasi (CVEs tertentu)

2. **Penanganan Kerentanan**

a. Tindakan Pengamanan:

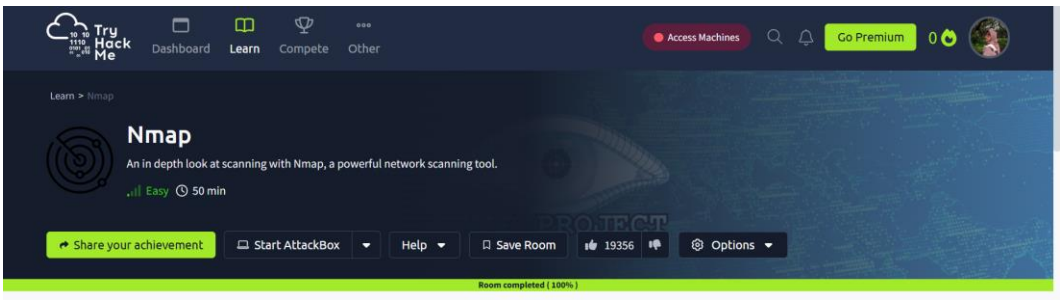
Layanan A	Layanan B
Konfigurasi .htaccess untuk memblokir akses ke file sensitif	Update WordPress ke versi terbaru
Konfigurasi .htaccess untuk memblokir akses ke file sensitif	Update plugin dan hapus yang tidak digunakan
Menghapus file konfigurasi atau backup dari direktori publik	Pasang Web Application Firewall (WAF) seperti Sucuri atau ModSecurity
Menyembunyikan versi server di header: • ServerTokens Prod • ServerSignature Off	

b. Referensi Perbaikan:

- OWASP Secure Configuration Guide
- WPScan Vulnerability Database
- Apache Hardening Documentation

3. **Pemindaian Keamanan Jaringan**

a. Tools yang digunakan: Nmap



b. Langkah-Langkah:

1. Tentukan IP range internal, punya kami 192.168.1.0/24
2. Jalankan perintah:

   nmap -sS -sV -O 192.168.1.0/24
3. Catat port dan OS yang terdeteksi.

c. Hasil:

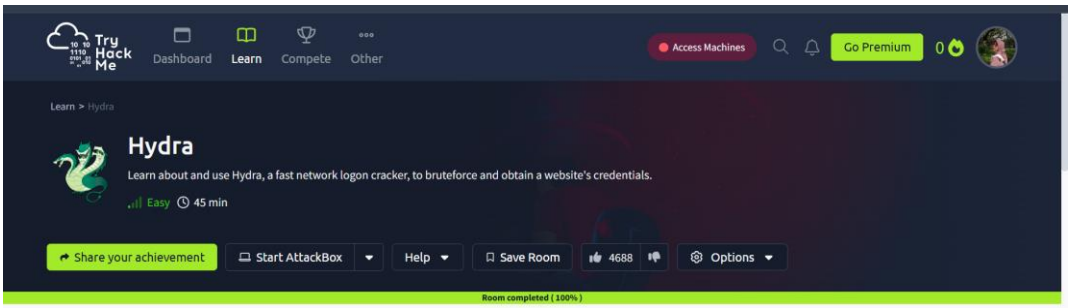
- Server dengan port Telnet (23) terbuka
- Server produksi memiliki port FTP (21) tanpa enkripsi
- Beberapa sistem masih menjalankan OS lama (Windows 7, Ubuntu 16.04)

d. Fitur Pembeda Tools:

Tools	Fokus	Kelebihan
Nikto	Web Server	Deteksi direktori/file sensitif, misconfig
WPScan	WordPress	Fokus eksploitasi plugin/tema WP
NMap	Jaringan	Deteksi port, OS, dan service fingerprinting

4. Pengujian SSH Remote Access

a. Tools yang digunakan: Hydra



b. Langkah-Langkah

1. Siapkan wordlist pengguna dan password (user.txt, pass.txt)
2. Jalankan Hydra:

   hydra -L user.txt -P pass.txt ssh://192.168.1.10

c. Hasil:

- Berhasil login ke akun admin dengan password admin123
- Akun marketing dengan password marketing1 juga berhasi

d. Antisipasi

- Ganti semua password default
- Terapkan password policy (kombinasi kuat dan masa berlaku)
- Gunakan SSH key-based authentication

- Batasi akses dengan AllowUsers di SSH config dan iptables/firewall

5. **Kebijakan dan Prosedur**
   a. Evaluasi dan Masukan:
      - Belum ada SOP untuk pemindaian berkala atau mitigasi kerentanan.
      - Password policy tidak diterapkan secara menyeluruh.
   b. Rekomendasi Kebijakan Baru:
      - Pemindaian berkala menggunakan Nikto/WPScan/Nmap minimal 1 bulan sekali
      - SOP pembaruan sistem dan plugin setiap minggu
      - Implementasi security baseline (minimal OS hardening dan patch)
      - Pelatihan pegawai untuk phishing awareness dan password hygiene
      - Audit akses SSH secara rutin

6. **Rekomendasi untuk Peningkatan Keamanan**
   a. Teknologi & Tools:
      - IDS/IPS: Suricata atau Snort (untuk deteksi dan blokir serangan real-time)
      - SIEM: ELK Stack (Elasticsearch, Logstash, Kibana), atau Wazuh untuk log analisis dan deteksi ancaman
      - Patch Management: WSUS (Windows), Ansible (Linux automation), atau Landscape (Ubuntu)
      - Zero Trust Architecture:
        - Validasi identitas pengguna terus-menerus
        - Segmentasi jaringan (VLAN, firewall mikro)
   b. Arsitektur Tambahan:
      - Reverse proxy + WAF (Contoh: Nginx + ModSecurity)
      - VPN internal untuk akses dashboard atau SSH
      - Backup otomatis harian untuk konten kritis