LAPORAN UAS - SIMULASI KEAMANAN CYBER
Nama: Indra Fajar Nurwahid | Fajar Sapto Mukti Raharjo
NIM: 2231740006 | 2231740018
Mata Kuliah: Keamanan Jaringan
Topik: Praktik Keamanan Web & Jaringan (DVWA - TryHackMe)

PENDAHULUAN

TryHackMe adalah platform belajar cybersecurity berbasis praktik. Salah satu lab yang digunakan adalah DVWA (Damn Vulnerable Web Application), aplikasi PHP/MySQL dengan berbagai celah keamanan yang sengaja dibuat untuk pembelajaran. Dalam laporan ini, saya melakukan simulasi sebagai seorang Junior Cyber Security sesuai dengan skenario dan soal yang diberikan.

Saya terhubung ke lab DVWA melalui OpenVPN dan melakukan berbagai analisis serta pengujian terhadap sistem dan jaringan seperti scanning, enumerasi, dan pengujian akses.

---

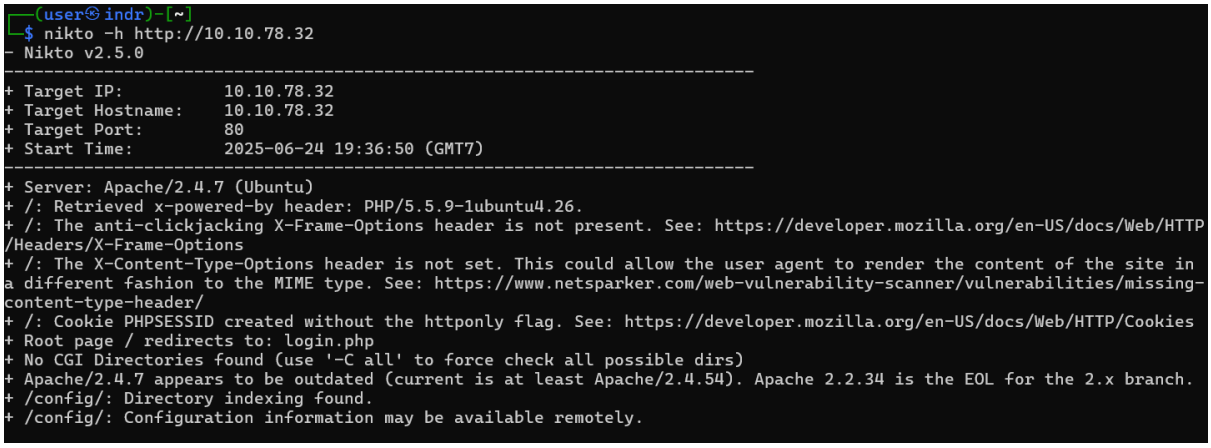
1. Identifikasi Layanan Web Server

Tools yang Digunakan:

- Nikto
- WhatWeb

Langkah-langkah:

1. Menghubungkan VPN ke TryHackMe:
   sudo openvpn --config tryhackme.ovpn
2. Menentukan IP target dari lab DVWA.
3. Menjalankan scanning dengan Nikto:
4. nikto -h http://10.10.78.32



5. Menjalankan enumerasi dengan WhatWeb:
6. whatweb http://10.10.78.32

Hasil:

- Nikto menunjukkan informasi server terbuka (Apache), file konfigurasi sensitif seperti phpinfo.php bisa diakses.
- WhatWeb mengidentifikasi layanan berjalan di atas PHP, Apache, dan MySQL.

---

2. Penanganan Kerentanan

Rekomendasi:

- Nonaktifkan informasi server header dengan ServerTokens Prod dan ServerSignature Off di Apache.
- Hapus file publik yang tidak perlu (phpinfo.php, test.php).
- Terapkan permission file yang aman.
- Gunakan HTTPS dan aktifkan firewall aplikasi web.

Referensi:

- OWASP Secure Headers
- Apache Hardening Guide

---

3. Pemindaian Keamanan Jaringan

Tools:

- Nmap

Langkah-langkah:

nmap -sS -sV -O 10.10.78.32

Hasil:

- Port terbuka: 22 (SSH), 80 (HTTP)
- OS terdeteksi sebagai Ubuntu
- Port 22 terbuka tanpa batasan IP

Perbandingan Tools:

- Nikto fokus pada vulnerability aplikasi web
- Nmap fokus pada scan jaringan, port, OS, dan versi service

---

4. Pengujian SSH Remote Access

Tools:

- Hydra

Langkah-langkah:

1. Siapkan wordlist (rockyou.txt)
2. Jalankan bruteforce:

hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://10.10.78.32

Hasil:

- Ditemukan akun dengan kombinasi user/password lemah seperti admin:admin

Rekomendasi:

- Ganti password default dan gunakan password policy ketat
- Gunakan otentikasi public key
- Batasi akses SSH berdasarkan IP
- Gunakan fail2ban untuk deteksi brute-force

---

5. Kebijakan dan Prosedur

Masukan Kebijakan:

- Password policy minimum 12 karakter, kompleksitas tinggi

- Update sistem dan aplikasi secara berkala
- Implementasi security baseline untuk server dan aplikasi
- Jadwal scan dan monitoring rutin
- Pelatihan keamanan dasar untuk seluruh user

---

6. Rekomendasi untuk Peningkatan Keamanan

Tools & Teknologi:

- **IDS/IPS** seperti Snort/Suricata
- **SIEM** seperti Wazuh/ELK untuk analisa log
- **Zero Trust Architecture** untuk membatasi akses hanya berdasarkan identitas dan otorisasi
- **Segmentasi jaringan** antara layanan publik dan internal

PENUTUP

Melalui simulasi di DVWA TryHackMe, saya mendapatkan pengalaman langsung dalam scanning, analisa kerentanan, serta melakukan pengujian keamanan dasar baik dari sisi aplikasi maupun jaringan. Langkah-langkah ini merupakan dasar penting dalam menjaga keamanan sistem informasi sebuah organisasi.

Lampiran (opsional):

- Screenshot hasil scan Nikto/Nmap/Hydra (jika diminta oleh dosen)
- Konfigurasi OpenVPN (dipersingkat jika perlu)
