Kelompok :

1. Dava Anugrah Illahi Putra (2231740036)
2. Fannisa Az Zahra (2231740037)

JAWABAN

1. Identifikasi Layanan Web Server

Tools yang Digunakan:
- Nmap (untuk scanning layanan dan port)
- Nikto (untuk web server vulnerability scanning)

Langkah-langkah yang Dilakukan:
1. Identifikasi IP target web server (misal: 192.168.1.10)
2. Gunakan Nmap untuk pemindaian port:
   nmap -sS -sV 192.168.1.10
3. Gunakan Nikto untuk scanning web server:
   nikto -h http://192.168.1.10

Hasil:
- Nmap: Port 80 dan 443 terbuka, Apache 2.4.29
- Nikto: Direktori /server-status terbuka, SSL misconfiguration, versi Apache rentan

2. Penanganan Kerentanan

Tindakan Pengamanan:
- Nonaktifkan akses /server-status
- Update versi Apache
- Konfigurasi ulang SSL/TLS

Referensi:
- OWASP Secure Configuration (https://owasp.org/www-project-top-ten/)
- Apache HTTP Server Hardening Guide (https://httpd.apache.org/docs/)

3. Pemindaian Keamanan Jaringan

Tools yang Digunakan:
- Nessus
- OpenVAS

Langkah-langkah:

1. Jalankan pemindaian Nessus terhadap IP jaringan
2. Validasi hasil dengan OpenVAS

Hasil:
- SMBv1 aktif, FTP dan Telnet terbuka
- OpenSSL versi lama

Perbedaan Tools:

Tool	Keunggulan	Kelemahan
Nmap	Cepat, ringan	Tidak mendalam
Nessus	Komprehensif, UI bagus	Berbayar
OpenVAS	Open-source, fleksibel	Setup kompleks

4. Pengujian SSH Remote Access

Tools yang Digunakan:
- Hydra

Langkah:
1. Gunakan Hydra:
   hydra -L users.txt -P passwords.txt ssh://192.168.1.10

Hasil:
- User 'admin' dengan password 'admin123' berhasil login

Antisipasi:
- Implementasi fail2ban
- Disable login root SSH
- Gunakan SSH Key-Based Authentication
- Ganti port default

5. Kebijakan dan Prosedur

Yang Perlu Diterapkan:
- Password Policy kuat
- Jadwal patching rutin
- Akses SSH terbatas
- Vulnerability scan berkala

Masukan SOP Tambahan:

- Validasi konfigurasi default sebelum deployment
- Terapkan security baseline tiap server

6. Rekomendasi untuk Peningkatan Keamanan

Rekomendasi Teknologi dan Tools:
- SIEM: Wazuh, ELK, atau Splunk
- Next-Gen Firewall
- VPN Access untuk Admin
- WAF seperti ModSecurity
- Asset Management Tools (GLPI)

Model Keamanan:
- Terapkan Zero Trust Architecture