Modul 5: Vulnerability Assessment & Basic Penetration Testing

Memahami cara menemukan kelemahan keamanan secara sistematis, legal, dan bertanggung jawab — fondasi utama setiap praktisi keamanan siber.

EDY SUSANTO — FOUNDER C-SIX SECURITY

Peta Pembelajaran

Apa yang Akan Kita Pelajari?

Modul ini dirancang untuk membawa peserta dari pemahaman konseptual hingga praktik langsung di lingkungan lab yang aman. Berikut adalah peta perjalanan belajar kita hari ini.

01

Konsep Dasar

Vulnerability Assessment, perbedaan scanning vs exploitation, dan common vulnerabilities

02

Framework & Standar

OWASP Top 10, password security, dan kesalahan konfigurasi umum

03

Praktik Lab

Network scanning, service enumeration, dan vulnerability discovery di lab simulasi

04

Pelaporan

Mendokumentasikan temuan secara profesional dan bertanggung jawab

Apa Itu Vulnerability Assessment?

Vulnerability Assessment (VA) adalah proses sistematis untuk mengidentifikasi, mengklasifikasikan, dan memprioritaskan kelemahan keamanan pada suatu sistem, jaringan, atau aplikasi — *sebelum* penyerang menemukannya lebih dulu.

Tujuan Utama VA

- Menemukan celah keamanan secara proaktif
- Menilai tingkat risiko setiap kelemahan
- Memberikan rekomendasi perbaikan

Siapa yang Melakukannya?

- Tim keamanan internal perusahaan
- Konsultan keamanan siber eksternal
- Auditor IT bersertifikat

Scanning vs Exploitation: Apa Bedanya?

Ini adalah salah satu perbedaan paling krusial yang wajib dipahami setiap praktisi keamanan siber. Keduanya adalah bagian dari proses, tetapi memiliki batasan hukum dan etika yang sangat berbeda.

🔍 Scanning (VA)

Tujuan: Menemukan dan mengidentifikasi kelemahan tanpa mengeksploitasinya.

Contoh: Menggunakan Nmap untuk mendeteksi port terbuka dan versi layanan yang berjalan.

Status: Legal bila dilakukan pada sistem yang Anda miliki atau mendapat izin tertulis.

⚡ Exploitation (Pen Test)

Tujuan: Membuktikan bahwa kelemahan dapat dimanfaatkan untuk mendapatkan akses tidak sah.

Contoh: Menggunakan Metasploit untuk menembus sistem melalui celah yang ditemukan.

Status: Hanya legal dengan kontrak dan scope yang jelas dan ditandatangani.

⚠ Melakukan scanning atau exploitation pada sistem tanpa izin adalah tindakan ilegal dan dapat dikenai sanksi pidana berdasarkan UU ITE.

Ancaman Nyata

Common Vulnerabilities yang Sering Ditemukan

Default Credentials

Username dan password bawaan perangkat (admin/admin) yang tidak pernah diganti oleh administrator sistem.

Unpatched Software

Perangkat lunak yang tidak diperbarui mengandung celah keamanan yang sudah diketahui publik dan tercatat di database CVE.

Open Ports Tidak Perlu

Port layanan yang terbuka tanpa kebutuhan bisnis memperluas attack surface dan memberi akses masuk bagi penyerang.

Misconfiguration

Konfigurasi yang salah pada server, firewall, atau aplikasi web membuka celah yang mudah dieksploitasi.

Standar Industri

OWASP Top 10: Kelemahan Aplikasi Web Paling Kritis

OWASP (Open Web Application Security Project) menerbitkan daftar 10 risiko keamanan aplikasi web paling berbahaya yang diperbarui secara berkala. Ini adalah referensi wajib bagi setiap praktisi keamanan.

1

Broken Access Control

Pengguna dapat mengakses resource di luar hak aksesnya.

2

Cryptographic Failures

Data sensitif tidak dienkripsi dengan benar saat disimpan atau dikirim.

3

Injection

Input berbahaya seperti SQL Injection diproses sebagai perintah oleh sistem.

4

Security Misconfiguration

Konfigurasi default yang tidak aman, fitur tidak diperlukan yang diaktifkan, atau pesan error yang terlalu detail.

Empat entri teratas ini secara konsisten menjadi penyebab mayoritas insiden keamanan aplikasi web di seluruh dunia.

Password Security: Garis Pertahanan Pertama

Mengapa Password Masih Jadi Masalah?

Meskipun teknologi terus berkembang, password lemah tetap menjadi vektor serangan nomor satu. Banyak sistem berhasil dibobol bukan karena kecanggihan serangan, melainkan karena password yang mudah ditebak.

Serangan Brute Force

Mencoba semua kombinasi karakter secara otomatis menggunakan tools seperti Hydra atau Hashcat.

Dictionary Attack

Menggunakan daftar kata-kata umum, nama, dan password yang sering digunakan oleh pengguna.

Credential Stuffing

Menggunakan kombinasi username/password yang bocor dari data breach sebelumnya.

Praktik Password yang Aman

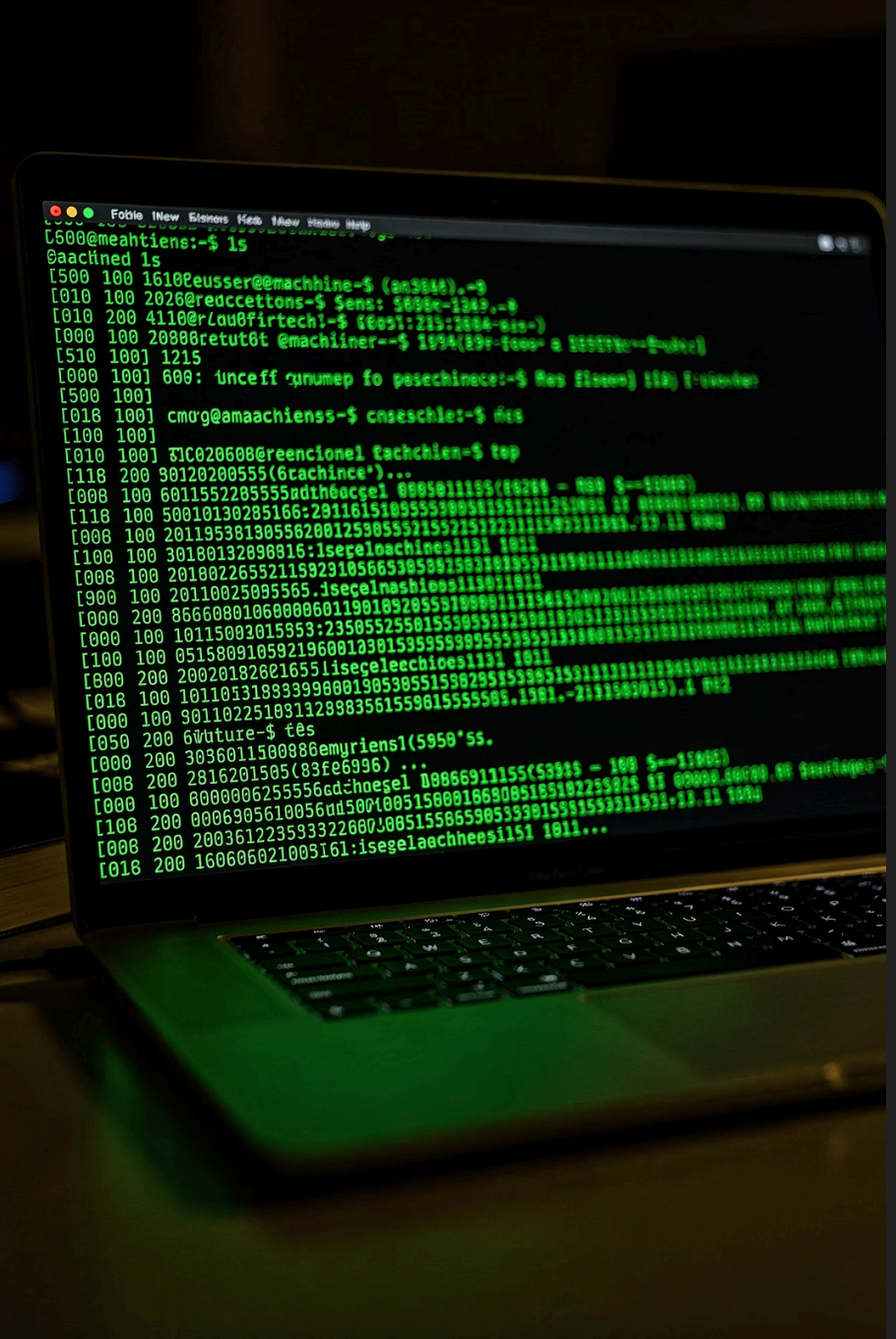
- Minimal 12 karakter dengan kombinasi huruf, angka, dan simbol
- Gunakan password unik untuk setiap akun
- Aktifkan Multi-Factor Authentication (MFA)
- Gunakan password manager terpercaya
- Hindari informasi pribadi yang mudah ditebak

Sumber Risiko Tersembunyi

Misconfiguration: Celah yang Sering Diabaikan

Kesalahan konfigurasi adalah salah satu penyebab pelanggaran keamanan yang paling umum — dan paling bisa dihindari. Sistem yang secara teknis aman pun bisa menjadi rentan akibat konfigurasi yang ceroboh.

ⓘ Checklist konfigurasi yang dijalankan secara rutin — misalnya menggunakan CIS Benchmarks — dapat secara drastis mengurangi risiko akibat misconfiguration.



Lab Praktik

Network Scanning dengan Nmap

Nmap (Network Mapper) adalah tool open-source paling populer untuk network discovery dan security auditing. Dengan Nmap, kita dapat mendeteksi host aktif, port terbuka, layanan yang berjalan, dan sistem operasi target.

Ping Scan

Menemukan host yang aktif di jaringan

```
nmap -sn 192.168.1.0/24
```

Port Scan

Mendeteksi port terbuka pada target

```
nmap -sV 192.168.1.1
```

OS Detection

Mengidentifikasi sistem operasi target

```
nmap -O 192.168.1.1
```

Lab Praktik

Service Enumeration & Web Scanning

Service Enumeration

Setelah port terbuka ditemukan, langkah berikutnya adalah **enumerasi layanan** — mengidentifikasi versi software yang berjalan untuk mencocokkan dengan database kerentanan yang diketahui.

- Deteksi versi layanan (`nmap -sV`)
- Banner grabbing menggunakan Netcat
- Identifikasi layanan tersembunyi di port non-standar

Web Scanning dengan Nikto

Nikto adalah scanner web server open-source yang secara otomatis mencari lebih dari 6.700 potensi masalah keamanan, termasuk file berbahaya, konfigurasi keliru, dan software usang.

- Scan header HTTP yang tidak aman
- Deteksi direktori dan file sensitif
- Identifikasi versi web server yang rentan

```
nikto -h http://192.168.1.1
```

Lab Praktik

Vulnerability Discovery dengan OpenVAS

OpenVAS (Open Vulnerability Assessment System) adalah platform pemindai kerentanan komprehensif yang digunakan secara luas oleh profesional keamanan. Ini adalah versi komunitas dari Greenbone Vulnerability Manager.

1

1. Setup Target

Tentukan host atau range IP yang akan dipindai dalam lingkungan lab simulasi

2

2. Pilih Scan Config

Pilih profil pemindaian: Full and Fast untuk coverage lengkap atau Discovery untuk pengenalan awal

3

3. Jalankan Scan

Eksekusi pemindaian dan monitor progres melalui dashboard web OpenVAS secara real-time

4

4. Analisis Hasil

Review temuan berdasarkan severity (Critical, High, Medium, Low) dan baca detail setiap kerentanan

Memahami Hasil: CVSS Score

Setiap kerentanan yang ditemukan memiliki skor risiko yang disebut **CVSS (Common Vulnerability Scoring System)**. Memahami skor ini penting untuk memprioritaskan tindakan remediasi secara efektif.

Critical (9.0–10.0)

Harus segera ditangani. Eksploitasi mudah dilakukan dan dampaknya sangat besar.

High (7.0–8.9)

Prioritas tinggi. Dapat menyebabkan kompromi sistem secara signifikan.

Medium (4.0–6.9)

Perlu ditangani dalam jangka menengah. Risiko terbatas pada kondisi tertentu.

Low (0.1–3.9)

Risiko minimal namun tetap perlu didokumentasikan dan dijadwalkan untuk diperbaiki.

Langkah Akhir yang Krusial

Reporting Findings: Mendokumentasikan Temuan

Sebuah vulnerability assessment baru benar-benar selesai ketika temuannya terdokumentasi dengan baik. Laporan yang buruk membuat temuan teknis terbaik sekalipun menjadi tidak berguna bagi tim manajemen dan pengembang.

Struktur Laporan VA yang Baik

1 Executive Summary

Ringkasan non-teknis untuk manajemen: total temuan, tingkat risiko keseluruhan, dan rekomendasi utama.

2 Detail Temuan

Deskripsi teknis lengkap setiap kerentanan: CVSS score, bukti (screenshot/log), dampak, dan langkah reproduksi.

3 Rekomendasi Remediasi

Langkah konkret dan terukur untuk memperbaiki setiap kelemahan, disertai referensi patch atau panduan konfigurasi.

Tips Laporan Profesional

- Gunakan bahasa yang jelas dan tidak ambigu
- Sertakan bukti visual (screenshot) untuk setiap temuan
- Prioritaskan temuan berdasarkan risiko bisnis, bukan hanya skor teknis
- Hindari jargon teknis berlebihan di bagian eksekutif
- Sertakan tanggal dan versi tools yang digunakan

Rangkuman Modul 5

Key Takeaways & Outcome Pembelajaran

✅ Vulnerability Assessment

Proses sistematis menemukan kelemahan *sebelum* penyerang menemukannya — selalu dengan izin dan dalam scope yang jelas.

✅ Tools Utama

Nmap untuk network scanning, **Nikto** untuk web scanning, dan **OpenVAS** untuk pemindaian kerentanan komprehensif.

✅ Standar Referensi

OWASP Top 10 dan CVSS Score adalah dua referensi wajib untuk mengklasifikasikan dan memprioritaskan kerentanan.

✅ Etika & Legalitas

Semua aktivitas security testing harus dilakukan secara legal, beretika, dan bertanggung jawab — selalu gunakan lab simulasi untuk latihan.

Edy Susanto — Founder C-SIX Security · Modul 5 selesai. Lanjut ke sesi praktik lab!