

### Worksheet 3.1

Instructions:

- Explore one of testing techniques in performance, security, and usability testing. See the main reference for more detailed information.
- Answer the questions by filling the blank cell.

Full Name	Taufan Ali
NIM	2215016135
Nama Teknik Pengujian yang dipilih	Penetration Test

#### What is it?

Deskripsikan teknik pengujian yang telah Anda pilih secara singkat dan jelas. Jelaskan pengertian dan konsep dasar dari teknik ini.

Contoh: Load testing adalah teknik pengujian performa yang bertujuan untuk mengevaluasi bagaimana sistem beroperasi di bawah beban kerja yang meningkat.

Penetration test (pentest) adalah sebuah teknik pengujian keamanan yang bertujuan untuk mengidentifikasi vulnerability (kerentanan) dalam aplikasi, sistem, atau jaringan. Pentest mensimulasikan serangan seperti yang mungkin dilakukan oleh hacker, baik dari luar maupun dari dalam, untuk mengeksploitasi kelemahan keamanan.

#### Apa tujuan dari pengujian ini?

Jelaskan tujuan utama dari teknik pengujian ini. Apa yang ingin Anda capai atau uji dalam perangkat lunak dengan menggunakan teknik ini?

Contoh: Tujuan dari load testing adalah untuk memastikan bahwa sistem dapat menangani sejumlah besar pengguna secara bersamaan tanpa mengalami penurunan kinerja.

Tujuan utama dari penetration testing (pentest) adalah untuk mengidentifikasi kerentanan dalam aplikasi, sistem, atau jaringan dengan mensimulasikan serangan yang mungkin dilakukan oleh hacker. Pengujian ini membantu mengevaluasi efektivitas mekanisme keamanan yang ada, memberikan gambaran tentang bagaimana sistem dapat diserang, dan menawarkan rekomendasi untuk memperbaiki kelemahan yang ditemukan. Dengan demikian, pentest bertujuan untuk memitigasi risiko keamanan dan mencegah potensi serangan sebelum celah tersebut dapat dieksploitasi oleh pihak yang tidak berwenang.

**Apa saja metrik yang digunakan?**

Identifikasi dan jelaskan metrik-metrik yang akan diukur dalam teknik pengujian ini. Apa indikator kinerja yang akan dipantau?

Contoh: Metrik dalam load testing dapat berupa response time, throughput, error rate, dan resource utilization.

1. **Severity Level (Tingkat Keparahan):** Mengukur tingkat keparahan kerentanan (Low, Medium, High, Critical), membantu menentukan prioritas perbaikan berdasarkan risiko yang ditimbulkan.
2. **Exploitability:** Menilai apakah kerentanan bisa dieksploitasi dan seberapa mudah hal itu dilakukan. Ini penting untuk mengetahui ancaman nyata yang bisa dieksploitasi oleh hacker.
3. **Post-Exploitation Impact:** Mengukur dampak setelah kerentanan dieksploitasi, seperti akses ke data sensitif atau kemampuan untuk mengontrol sistem, yang menunjukkan potensi kerugian jika kerentanan tidak diperbaiki.
4. **Time to Remediation:** Waktu yang dibutuhkan untuk memperbaiki kerentanan. Metrik ini menunjukkan seberapa cepat organisasi merespons dan menutup celah keamanan setelah terdeteksi.

**Bagaimana cara mengumpulkan data?**

Jelaskan bagaimana data akan dikumpulkan selama pengujian. Apakah menggunakan tool otomatis, pemantauan manual, atau metode lain?

Contoh: Data dalam load testing dikumpulkan menggunakan tool seperti JMeter yang dapat mencatat waktu respon dan jumlah request yang diproses oleh server.

1. **Tool Otomatis:** Menggunakan alat seperti Nmap, Burp Suite, dan Metasploit untuk pemindaian kerentanan dan eksploitasi otomatis.
2. **Pengujian Manual:** Pentester melakukan eksploitasi manual pada kerentanan yang lebih kompleks atau yang tidak terdeteksi oleh alat otomatis.
3. **Pemantauan Sistem dan Jaringan:** Alat seperti Wireshark digunakan untuk menganalisis lalu lintas jaringan dan aktivitas serangan.
4. **Log Analysis:** Log dari server dan aplikasi dianalisis untuk melacak jejak serangan dan respons sistem.

**Bagaimana cara analisis data?**

Deskripsikan metode atau teknik analisis data yang akan digunakan setelah pengujian selesai. Bagaimana data ini akan diolah untuk mendapatkan kesimpulan?

Contoh: Hasil load testing dianalisis dengan membandingkan metrik kinerja dengan baseline atau standar yang diharapkan untuk menentukan apakah sistem berfungsi sesuai harapan.

**Klasifikasi Kerentanan:** Mengkategorikan kerentanan berdasarkan tingkat keparahan (low, medium, high, critical).

**Analisis Dampak:** Menilai dampak eksploitasinya terhadap sistem dan data.

### **Bagaimana cara analisis data?**

Deskripsikan metode atau teknik analisis data yang akan digunakan setelah pengujian selesai. Bagaimana data ini akan diolah untuk mendapatkan kesimpulan?

Contoh: Hasil load testing dianalisis dengan membandingkan metrik kinerja dengan baseline atau standar yang diharapkan untuk menentukan apakah sistem berfungsi sesuai harapan.

1. Perbandingan dengan Baseline Keamanan: Membandingkan hasil dengan standar keamanan yang ditetapkan.
2. Rekomendasi Perbaikan: Menyusun rekomendasi prioritas berdasarkan tingkat keparahan dan dampak.
3. Klasifikasi Kerentanan: Mengkategorikan kerentanan berdasarkan tingkat keparahan (low, medium, high, critical).
4. Analisis Dampak: Menilai dampak eksploitasinya terhadap sistem dan data.
5. Perbandingan dengan Baseline Keamanan: Membandingkan hasil dengan standar keamanan yang ditetapkan.
6. Rekomendasi Perbaikan: Menyusun rekomendasi prioritas berdasarkan tingkat keparahan dan dampak.

### **Tools yang dapat digunakan**

Sebutkan tools yang mendukung pelaksanaan teknik pengujian ini. Jelaskan fitur utama dari tools yang relevan dengan pengujian.

Contoh: Tools untuk load testing meliputi Apache JMeter, LoadRunner, dan Gatling yang mendukung simulasi pengguna virtual untuk menguji beban pada aplikasi.

1. Nmap: Pemindaian port dan deteksi layanan untuk memetakan jaringan dan menemukan port terbuka.
2. Metasploit: Kerangka kerja eksploitasi untuk menguji kerentanan dan menjalankan exploit terhadap target yang rentan.
3. Burp Suite: Alat pengujian keamanan aplikasi web, termasuk pemindaian kerentanan dan manipulasi request.
4. Wireshark: Analisis paket jaringan untuk memantau lalu lintas dan mendeteksi aktivitas mencurigakan.

### **Cara Melaporkan Hasil Pengujian**

Jelaskan format laporan yang Anda usulkan untuk menyajikan hasil pengujian. Apa saja komponen yang harus disertakan dalam laporan?

Contoh: Laporan load testing meliputi ringkasan tujuan pengujian, metode, hasil metrik (grafik response time, throughput, dll), analisis, serta kesimpulan dan rekomendasi.

1. Ringkasan Eksekutif : Gambaran umum tujuan, lingkup, hasil utama pengujian.
2. Temuan dan Kerentanan : Daftar kerentanan yang ditemukan, termasuk deskripsi, tingkat keparahan, dan rekomendasi perbaikan.
3. Analisis Dampak : Penjelasan potensi risiko dari setiap kerentanan yang

**Cara Melaporkan Hasil Pengujian**

Jelaskan format laporan yang Anda usulkan untuk menyajikan hasil pengujian. Apa saja komponen yang harus disertakan dalam laporan?

Contoh: Laporan load testing meliputi ringkasan tujuan pengujian, metode, hasil metrik (grafik response time, throughput, dll), analisis, serta kesimpulan dan rekomendasi.

ditemukan.

4. Kesimpulan dan Rekomendasi : Kesimpulan tentang kesehatan keamanan sistem dan langkah-langkah yang perlu diambil.