**TUGAS BESAR MID**



**OLEH**

**NAMA : MUHAMMAD FAJRIN**

**NIM : 105841108223**

**KELAS : 5A**

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH MAKASSAR**

**2025**

# **1. Pendahuluan**

Penetration testing (pentest) merupakan proses sistematis untuk mengidentifikasi kerentanan dalam sistem dengan melakukan simulasi serangan yang terkontrol. Dalam laporan ini, pengujian dilakukan terhadap perusahaan fiksi **PT. SecureCorp** dengan fokus pada dua tahap utama:

1. **Passive Reconnaissance** – pengumpulan informasi publik (OSINT) tanpa berinteraksi dengan server.
2. **Active Reconnaissance** – interaksi langsung dengan target menggunakan teknik scanning dan enumerasi.

Tujuan utama dari pengujian ini adalah menemukan potensi titik serang (*attack vectors*) dan mengusulkan langkah mitigasi yang sesuai.

# **2. Passive Reconnaissance (Pengintaian Pasif)**

Passive Recon dilakukan tanpa mengirim request ke target. Semua informasi diperoleh dari sumber terbuka seperti DNS records, OSINT, GitHub, Google Dorks, dan footprinting teknologi.

## **2.1 Pencarian Domain dan Sub-domain**

### **Domain Utama**

* **securecorp.com**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Sub-domain** | **Sumber** | **Relevansi Keamanan** |
| **1** | **mail.securecorp.com** | **DNSDumpster** | **Server email → potensi MX spoofing** |
| **2** | **dev.securecorp.com** | **CRT.sh** | **Lingkungan dev paling rawan bocor** |
| **3** | **vpn.securecorp.com** | **Google Dorks** | **Akses remote → potensi brute-force** |
| **4** | **api.securecorp.com** | **Subfinder** | **Endpoint API internal** |
| **5** | **portal.securecorp.com** | **Shodan** | **Panel login internal** |

## **2.2 Informasi Email dan Karyawan**

### **Format Email**

* **nama.belakang@securecorp.com**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Nama** | **Jabatan** | **Sumber** | **Relevansi** |
| 1 | Ardiansyah Pratama | System Administrator | LinkedIn | Target rekayasa sosial |
| 2 | Ratna Dewi | IT Support | LinkedIn & Google | Akses SSO berpotensi lemah |
| 3 | Johann Putra | Backend Developer | GitHub | Risiko API key bocor |

## **2.3 Teknologi yang Digunakan**

Teridentifikasi melalui BuiltWith dan Wappalyzer:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Teknologi** | **Versi** | **Kategori** | **risiko** |
| 1 | Apache HTTP Server | 2.4.x | Web Server | Banyak CVE lama |
| 2 | WordPress CMS | 6.x | CMS | Sering diserang plugin |
| 3 | Google Analytics | — | Analytics | Risiko JS injection |

## 

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Temuan** | **Sumber** | **Dampak** |
| 1 | config.php mengandung kredensial | Google Dorks | Kebocoran akses database |
| 2 | API key dalam GitHub commit | GitHub | Penyalahgunaan API |
| 3 | error.log terindeks Google | Cache Google | Membocorkan jalur internal server |

## 

# **3. Active Reconnaissance (Pengintaian Aktif)**

Active Recon dilakukan hanya pada target yang diberikan:

🎯 **IP Target: 10.10.10.50**

Metode menggunakan Nmap untuk scanning port, enumerasi layanan, dan OS fingerprinting.

## **3.1 Host Discovery & Port Scanning**

### **SYN Scan (TCP)**

nmap -sS 10.10.10.50

### **UDP Scan**

nmap -sU 10.10.10.50

## **3.2 Hasil Pemindaian Port**

### **TCP Ports**

|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **Status** | **Service** | **Versi** |
| 22 | open | SSH | OpenSSH 8.2 |
| 80 | open | HTTP | Apache 2.4.54 |
| 443 | open | HTTPS | OpenSSL TLS1.3 |
| 3306 | filtered | MySQL | Unknown |
| 8080 | open | Reverse Proxy | Nginx Proxy |

### **Analisis:** versi Apache 2.4.54 memiliki beberapa potensi CVE 2023 meski lebih aman dari versi lama.

### **UDP Ports**

|  |  |  |
| --- | --- | --- |
| **Port** | **Status** | **Service** |
| 53 | open | DNS Resolver |
| 161 | filtered | SNMP |

### 

## 

## 

## **3.3 Service & Version Detection**

nmap -sV 10.10.10.50

### **Temuan:**

* Apache 2.4.54 → lebih baru tapi tetap rawan exploit tertentu
* Nginx Proxy 1.22 → potensi misconfig
* SSH 8.2 → relatif aman

## **3.4 OS Fingerprinting**

nmap -O 10.10.10.50

### **Hasil:**

* OS: **Linux Kernel 5.x**
* Distribusi: **Ubuntu Server 20.04 / 22.04**

Ini versi modern dengan patch lebih baik dibanding kernel 4.x.

## **3.5 Analisis Paket (Wireshark)**

Temuan:

* Paket **TCP SYN/SYN-ACK** normal
* Aktivitas HTTP GET tanpa enkripsi di port 80 → mudah disadap
* Server mendukung TLS1.3 untuk port 443 (aman)

# 

# 

# **4. Analisis Kerentanan**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Temuan** | **Risiko** | **Dampak** |
| 1 | Port 80 terbuka tanpa HTTPS mandatory | Sniffing | Data dapat diintersep |
| 2 | MySQL port 3306 filtered tapi tetap terlihat | Enumerasi | Potensi serangan koneksi brute |
| 3 | Subdomain dev terbuka | Misconfig | Kebocoran file dev |
| 4 | API key bocor (OSINT) | Impersonation | Eksploitasi API |
| 5 | Log error terindeks | Informasi sensitif | Mapping server lebih mudah |

# **5. Kesimpulan**

Hasil pengujian menunjukkan bahwa PT. SecureCorp memiliki beberapa kelemahan, terutama pada:

* paparan informasi sensitif dari OSINT
* port penting terbuka
* layanan tanpa enkripsi
* konfigurasi server yang tidak optimal
* risiko brute-force pada service tertentu

Langkah perbaikan mendesak perlu dilakukan sebelum sistem digunakan dalam lingkungan produksi.

# **6. Rekomendasi Perbaikan**

1. Terapkan HTTPS-only pada port 80 (HTTP redirect).
2. Tutup port MySQL dari akses publik.
3. Audit konfigurasi Apache dan Nginx.
4. Implementasi IDS/IPS seperti Suricata.
5. Rotasi API key yang bocor.
6. Audit GitHub developer secara rutin.
7. Terapkan VPN dengan MFA untuk seluruh akses internal.

# **7. Dokumentasi Tools**

* Nmap
* Wireshark
* DNSDumpster
* CRT.sh
* Subfinder
* Google Dorks
* Wappalyzer
* BuiltWith
* GitHub OSINT
* LinkedIn Enumeration