**Writeup LycoReco**

**Final Gemastik XV - Institut Teknologi Bandung**



**Anggota tim:**

**Muhammad Garebaldhie**

**Frederik Imanuel Louis**

**Rachel Gabriela Chen**

# **Daftar Isi**

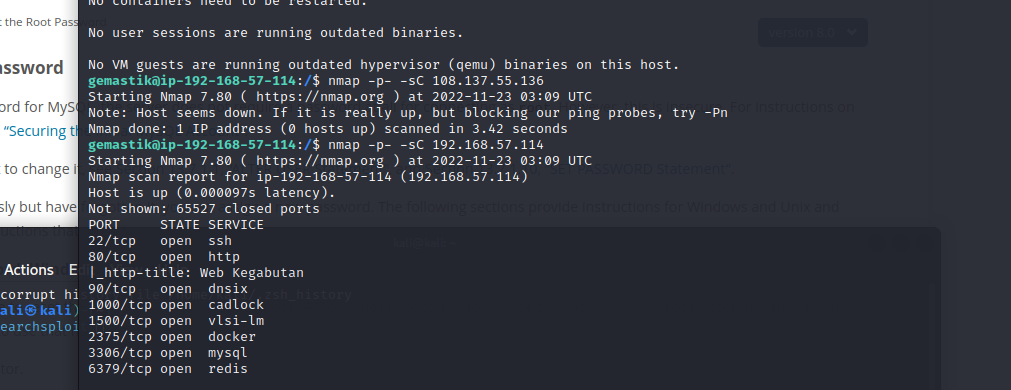
[**Daftar Isi**](#_jtobumv3ewy0) **2**

[**Hardening**](#_dx0lkflrke9q) **3**

[**Attacking**](#_bb8dp4b4v6we) **10**

# Hardening

Pada fase awal hardening kami melakukan scanning dengan `nmap` untuk mencari service service yang berjalan pada machine

****

Terdapat 7 service pada machine masing masing pada port 80, 90, 1000, 1500, 2375, 3306 dan 6379

| No | Port | Service | Vulnerablity |
| --- | --- | --- | --- |
| 1 | 80 | Web kegabutan | 1. LFI pada parameter page= 2. SQLi pada parameter name= |
| 2 | 90 | Sandbox php | PHP unsafe eval |
| 3 | 1000 | Number | Python2 input vulnerability |
| 4 | 1500 | Kalkulator Web App | Jinja2/Flask SSTI |
| 5 | 2375 | Docker | Tidak menemukan |
| 6 | 3306 | Mysql | No auth pada mysql sehingga dapat melakukan arbitrary code excecution |
| 7 | 6379 | Redis | No auth pada redis bisa melakukan RCE |

### 

**Patching pada service**

| No | Item | Penjelasan |
| --- | --- | --- |
| 1 | Jenis Celah Keamanan/Kesalahan Konfigurasi | Not password-protected gemastik & ubuntu |
| Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi | Login user dan root |
| Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi | Akses shell memberikan attacker kontrol pada VM |
| Mitigasi/Solusi yang telah dilakukan. | Memasang password pada gemastik & ubuntu   1. Gunakan `sudo su ubuntu` ataupun `sudo su gemastik` untuk berpindah user 2. Execute command `sudo -i passwd` untuk merubah password 3. Digunakan strong password seperti 22526e7fefe7d180457ba96708e440f22b0170f2 untuk pencegahan brute force |
| 2 | Jenis Celah Keamanan/Kesalahan Konfigurasi | Not password-protected MySQL |
| Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi | Mysql shell |
| Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi | Dapat dilakukan brute force pada password user yang insecure |
| Mitigasi/Solusi yang telah dilakukan. | 1. Masuk ke mysql dengan cara `sudo mysql -u root` 2. Lihat database yang ada pada mysql dengan cara `show databases`; 3. Pilih databse mysql 4. Execute query `select user from users` untuk mengambil list user pada mysql 5. Setelah itu ganti password semua user dengan cara **`ALTER USER username@'localhost' IDENTIFIED BY 'veryverystrongpassword'**; lalu **FLUSH PRIVILEGES;** |
| 3 | Jenis Celah Keamanan/Kesalahan Konfigurasi | Not password-protected Redis |
| Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi | /etc/redis/redis.conf |
| Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi | Dapat dilakukan brute force pada password user yang insecure |
| Mitigasi/Solusi yang telah dilakukan. | 1. **Lakukan sudo nano /etc/redis/redis.conf** 2. **Search # require pass** 3. **Uncomment line tersebut lalu isi dengan password yang kuat** |
| 4 | Jenis Celah Keamanan/Kesalahan Konfigurasi | Php eval |
| Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi | /var/sandbox/index.php |
| Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi | RCE, command injection |
| Mitigasi/Solusi yang telah dilakukan. | 1. Lakukan nano /var/sandbox/index.php 2. “Potong” / “Slice” param pada query code agar input terbatas 3. Gunakan substr dengan penjang maksimum 13 char. |
| 5 | Jenis Celah Keamanan/Kesalahan Konfigurasi | Malicious user input in “nama” query |
| Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi | /var/www/html/index.php |
| Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi | RCE, command injection |
| Mitigasi/Solusi yang telah dilakukan. | 1. Escaping $\_GET[‘name’] dengan mysqli\_real\_escape\_string 2. Melakukan prepare query (tidak langsung mengquery) |
| Screenshot |  |
| 6 | Jenis Celah Keamanan/Kesalahan Konfigurasi | Execute arbitrary command in python2 |
| Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi | /var/www/number/app.py |
| Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi | Pada python2, input() memiliki vulnerability dimana semua input akan dieval sebagai code |
| Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step | 1. Buka file /var/www/number/app.py 2. Rubah shebang line pada line pertama yang awalnya `#!/usr/bin/python2` menjadi `#!/usr/bin/python3` |
| Screenshot |  |
| 7 | Jenis Celah Keamanan/Kesalahan Konfigurasi | Konfigurasi php.ini yang tidak aman |
| Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi | php.ini |
| Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi | Pengguna dapat melakukan RCE dari shell karena tidak ada disabled functoin |
| Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step | 1. Buka file php.ini 2. Tambahikan function berikut pada disabled function: pcntl\_alarm,pcntl\_fork,pcntl\_waitpid,pcntl\_wait,pcntl\_wifexited,pcntl\_wifstopped,pcntl\_wifsignaled,pcntl\_wifcontinued,pcntl\_wexitstatus,pcntl\_wtermsig,pcntl\_wstopsig,pcntl\_signal,pcntl\_signal\_dispatch,pcntl\_get\_last\_error,pcntl\_strerror,pcntl\_sigprocmask,pcntl\_sigwaitinfo,pcntl\_sigtimedwait,pcntl\_exec,pcntl\_getpriority,pcntl\_setpriority,exec,passthru,shell\_exec,system,proc\_open,popen,curl\_exec,curl\_multi\_exec,parse\_ini\_file,show\_source,fwrite,file |

# Attacking

| No | Item | Penjelasan |
| --- | --- | --- |
| 1 | IP Address Mesin Target | IP semua peserta lain |
| Jenis Celah Keamanan/Kesalahan Konfigurasi | SQL Injection |
| Lokasi Potensi Celah Keamanan/Konfigurasi | Escaping query string yang kurang tepat pada service |
| Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada | 1. Gunakan SQLMap untuk mengotomasi SQL Injection dan diisikan dengan argument –os-shell untuk mendapatkan shell. 2. Setelah itu dilakukan curl untuk mendapatkan flag 3. Jika curl tidak bisa dilakukan, gunakan printf “GET /\n\n” | nc 192.168.56.150 4444 |
|  | Screenshot |  |

### 