

LAPORAN PENETRATION TESTING: CHEMISTRY HTB

INFORMASI PROYEK

Nama Target: Chemistry HTB

Alamat IP: 10.10.11.38

Tipe Environment: Web Application + Linux System

Tingkat Kesulitan: Medium

Tanggal Testing: 11/30/2024

RINGKASAN EKSEKUTIF

Penetration testing terhadap lingkungan Chemistry HTB berhasil mengkompromi sistem secara penuh melalui serangkaian eksploitasi kerentanan aplikasi web, privilege escalation, dan local file inclusion. Testing dimulai dari eksploitasi template injection pada aplikasi web hingga mencapai akses root pada sistem target.

KERENTANAN YANG DIEKSPLOITASI

CVE-2024-23346: Arbitrary Code Execution di pymatgen

- **Attack Vector:** Local
- **CVSS Score:** 8.6
- **Dampak:** Confidentiality (High), Integrity (High), Availability (High)
- **Keterangan:** Eksekusi kode arbitrary melalui file template berbahaya

CVE-2024-23334: Local File Inclusion (LFI) di aiohttp

- **Attack Vector:** Network
- **CVSS Score:** 7.7
- **Dampak:** Confidentiality (High)
- **Keterangan:** Ekspos file sistem melalui kerentanan LFI

METODOLOGI PENGETESAN

1. **Reconnaissance** - Pemindaian jaringan dan enumerasi layanan
2. **Web Application Testing** - Identifikasi kerentanan template injection
3. **Initial Access** - Remote code execution melalui CVE-2024-23346
4. **Lateral Movement** - Credential discovery dan SSH access
5. **Privilege Escalation** - System enumeration dan service discovery
6. **Post-Exploitation** - LFI exploitation untuk root flag

TEMUAN DETAIL

1. Enumerasi Jaringan Awal

Tools: Nmap

Hasil: Teridentifikasi port terbuka termasuk SSH (22) dan web service (5000)

Layanan: Web application berjalan pada port 5000

2. Web Application Analysis

Akses: Browser web ke <http://10.10.11.38:5000>

Temuan: Aplikasi web chemistry dengan fitur upload template

Fitur Rentan: Template processing system tanpa validasi keamanan adequate

3. Template Injection Exploitation

Kerentanan: CVE-2024-23346 - Arbitrary Code Execution di pymatgen

Teknik: Modifikasi template file dengan malicious Python code

Payload: Reverse shell connection untuk remote access

Proses:

- Download template original dari aplikasi
- Inject malicious code pada akhir file template
- Upload modified template ke aplikasi
- Eksekusi template untuk trigger reverse shell

4. Initial Compromise

Result: Berhasil mendapatkan reverse shell connection

Akses: Web server user privileges

Discovery: Enumerasi user accounts dan credential discovery

5. Credential Discovery dan Lateral Movement

Temuan: File berisi hashed password user rosa

Hash Type: MD5

Cracking Result: Password "unicorniosrosados"

Akses: SSH access menggunakan credential yang ditemukan

6. Privilege Escalation Reconnaissance

Tools: linPEAS untuk system enumeration

Temuan: Local service berjalan pada 127.0.0.1:8080

Teknik: SSH tunneling untuk mengakses local service

Command:

```
ssh -L 7000:127.0.0.1:8080 rosa@10.10.11.38 -fn
```

7. Service Analysis dan LFI Exploitation

Service: aiohttp web server versi vulnerable

Kerentanan: CVE-2024-23334 - Local File Inclusion

Teknik: Curl exploitation untuk membaca file sistem

Eksplorasi:

- Identifikasi versi aiohttp vulnerable melalui curl
- LFI attack untuk membaca file sensitif
- Berhasil membaca root flag melalui LFI

TOOLS YANG DIGUNAKAN

- **Scanning:** Nmap
- **Web Testing:** Browser, Curl
- **Exploitation:** Custom Python templates, Reverse shell
- **Credential Cracking:** Online hash cracking tools
- **Privilege Escalation:** linPEAS
- **Remote Access:** SSH, SSH tunneling
- **Post-Exploitation:** Curl untuk LFI exploitation

SKILLS YANG DITUNJUKAN

Technical Skills

- Web application security testing
- CVE research dan exploitation
- Template injection attacks
- Reverse shell deployment
- Credential cracking dan reuse
- SSH tunneling techniques
- Local File Inclusion exploitation
- System enumeration dengan linPEAS

Analytical Skills

- Vulnerability chain analysis
- CVSS scoring comprehension
- Attack path development
- Service identification dan exploitation

REKOMENDASI KEAMANAN

1. Web Application Security

- Implementasi input validation untuk template processing
- Update pymatgen ke versi terbaru yang tidak vulnerable
- Sanitization user-supplied templates
- Implementasi sandbox untuk template execution

2. System Hardening

- Update aiohttp ke versi terbaru
- Restriksi akses file sistem melalui web services
- Implementasi least privilege untuk service accounts
- Regular vulnerability assessment





3. Credential Management

- Hindari penyimpanan password dalam format hash weak (MD5)
- Implementasi strong password policies
- Regular credential auditing

4. Network Security

- Restriksi unnecessary port exposure
- Implementasi network segmentation
- Monitoring untuk suspicious tunneling activities

PENCAPAIAN

-  **User Flag Captured** - Bukti user-level compromise
-  **Root Flag Captured** - Bukti full system compromise
-  **Multiple CVE Exploitation** - Demonstrasi real-world vulnerability exploitation
-  **Complete Attack Chain** - Web to root full compromise

KESIMPULAN

Penetration testing terhadap Chemistry HTB berhasil mendemonstrasikan eksploitasi multiple kerentanan termasuk arbitrary code execution melalui template injection dan local file inclusion.

Serangan dimulai dari layer aplikasi web dan berlanjut hingga mencapai akses root pada sistem melalui methodical enumeration dan exploitation.

Project ini menunjukkan kemampuan dalam mengidentifikasi, meneliti, dan mengeksploitasi kerentanan software specific (CVE-based attacks) serta melakukan comprehensive system penetration testing.