OWASP

Open Worldwide Application Security Project

- OWASP - Background
- OWASP - Amass

OWASP - Background

OWASP (Open Web Application Security Project) adalah organisasi nirlaba yang fokus pada peningkatan keamanan perangkat lunak. OWASP menyediakan berbagai sumber daya gratis, termasuk dokumentasi, alat, dan panduan praktik terbaik untuk membantu pengembang, peneliti keamanan, dan perusahaan dalam mengidentifikasi serta mengatasi kerentanan keamanan dalam aplikasi web.

Salah satu proyek paling terkenal dari OWASP adalah **OWASP Top 10**, yaitu daftar sepuluh ancaman keamanan aplikasi web yang paling kritis dan umum terjadi. Daftar ini diperbarui secara berkala untuk mencerminkan ancaman terbaru di dunia keamanan siber.

Selain itu, OWASP juga mengembangkan alat dan proyek lain seperti:

- **OWASP ZAP (Zed Attack Proxy):** Alat untuk pengujian penetrasi aplikasi web.
- **OWASP ASVS (Application Security Verification Standard):** Standar verifikasi keamanan aplikasi.
- **OWASP SAMM (Software Assurance Maturity Model):** Kerangka kerja untuk mengukur dan meningkatkan keamanan perangkat lunak.

OWASP sangat dihormati di industri keamanan siber dan sering dijadikan acuan untuk praktik terbaik dalam pengembangan aplikasi yang aman.

OWASP - Amass

AMASS adalah alat open-source yang sangat kuat untuk **enumerasi subdomain**, **pengintaian jaringan**, dan **pemetaan aset internet**. Alat ini sering digunakan oleh pentester dan profesional keamanan siber untuk:

- **Mencari Subdomain** dari suatu domain utama.
- **Melakukan Pengintaian Pasif** tanpa mengirimkan permintaan langsung ke target.
- **Menggunakan Sumber Data Publik** seperti DNS, API publik, sertifikat SSL, dan lainnya.
- **Melakukan Brute Force Subdomain** untuk menemukan subdomain yang tidak terindeks.
- **Pemetaan Jaringan** dengan mencari hubungan antara domain dan subdomain.
- **Pengintaian Organisasi** untuk mencari domain yang terkait dengan nama organisasi.

---

1. Instalasi Amass di Ubuntu

Jika belum terpasang, instal dengan perintah berikut :

```
sudo snap install amass -y
```

2. Memeriksa Versi Amass

Pastikan instalasi berhasil dengan memeriksa versi :

```
amass -version
```

3. Contoh Penggunaan Amass untuk `ilusidigital.com`

a. Enumerasi Subdomain Dasar

Enumerasi dasar untuk mencari subdomain publik :

```
amass enum -d ilusidigital.com
```

b. Menggunakan Mode Aktif untuk Pemindaian Langsung

Mode aktif melakukan pemindaian langsung ke DNS server target :

```
amass enum -active -d ilusidigital.com
```

c. Menampilkan Sumber Data yang Digunakan

Untuk melihat dari mana data subdomain diambil :

```
amass enum -src -d ilusidigital.com
```

d. Menyimpan Hasil ke File

Untuk menyimpan hasil ke dalam file teks :

```
amass enum -d ilusidigital.com -o /home/ilusi/hasil_ilusi.txt
```

4. Menggunakan `Amass Intel` untuk Investigasi Lebih Dalam

Amass Intel digunakan untuk menemukan domain terkait dengan organisasi :

```
amass intel -org "Ilusi Digital"
```

Menggunakan WHOIS untuk Investigasi Organisasi:

```
amass intel -org "Ilusi Digital" -whois
```

5. Menggunakan Brute Force untuk Pencarian Lebih Mendalam

Untuk mencoba menemukan subdomain dengan brute force :

```
amass enum -brute -d ilusidigital.com
```

Catatan: Gunakan wordlist untuk hasil yang lebih baik :

```
amass enum -brute -w /path/to/wordlist.txt -d ilusidigital.com
```

6. Mode Verbose untuk Debugging dan Logging

Gunakan verbose untuk melihat proses secara rinci :

```
amass enum -v -d ilusidigital.com
```

Atau simpan log untuk dianalisis :

```
amass enum -d ilusidigital.com -v -log amass_ilusi.log cat amass_ilusi.log
```

7. Pencarian Sertifikat SSL untuk Subdomain

Amass dapat mencari subdomain yang terdaftar di sertifikat SSL :

```
amass enum -passive -d ilusidigital.com
```

---

8. Contoh Kombinasi untuk Hasil Maksimal

Menggabungkan beberapa teknik untuk hasil yang lebih komprehensif :

```
amass enum -active -brute -src -d ilusidigital.com -o hasil_lengkap.txt
```

---

9. Menggunakan API Key untuk Sumber Data Tambahan

Amass dapat menggunakan API key untuk memperluas cakupan sumber data. Beberapa sumber yang didukung :

- VirusTotal
- SecurityTrails
- Shodan
- Censys
- Dan Lainnya

Cara Konfigurasi:

1. Daftar dan dapatkan API key dari situs terkait.
2. Buat atau edit file konfigurasi :

```
nano ~/.config/amass/config.ini
```

3. Tambahkan API key seperti ini :

```
[virustotal] apikey = "API_KEY_ANDA" [securitytrails] apikey = "API_KEY_ANDA"
```

4. Gunakan Amass dengan konfigurasi API :

```
amass enum -config ~/.config/amass/config.ini -d ilusidigital.com
```

10. Tips dan Praktik Terbaik

- Gunakan VPN saat melakukan pengintaian untuk menjaga privasi.
- Selalu pastikan Anda memiliki izin sebelum melakukan pengintaian terhadap domain yang bukan milik Anda.