# ESCANEO BÁSICO DE VULNERABILIDADES

## CVES Y EXPLOITS PÚBLICOS

OpenWebinars

# CVE & EXPLOITS

- Exploits & CVEs
- Fuentes de malware
- Análisis de explotaciones

# ¿QUÉ ES UN EXPLOIT?

- Un exploit es un fragmento de software, un conjunto de datos o una secuencia de comandos que aprovecha una vulnerabilidad en software para causar comportamientos no previstos, como la obtención de control sobre un sistema

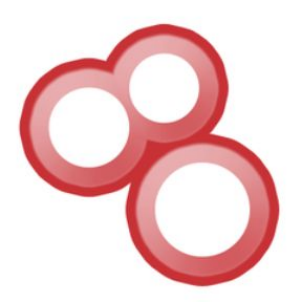
# ¿QUÉ ES UN CVE?

- Un CVE es un identificador estándar para una vulnerabilidad de seguridad conocida
- El sistema CVE proporciona una referencia de seguridad pública para cada vulnerabilidad conocida

# ¿QUÉ ES UN CVE?

- El formato para las entradas CVE es: **`CVE-YYYY-NNNN`**
    - (YYYY indica el año y NNNN el número de vulnerabilidad)
        - Desde enero de 2014 este identificador puede contener, si es necesario, más de cuatro dígitos

# FUENTES PÚBLICAS DE EXPLOITS



Shodan Exploits


Exploit-DB

Sploitus


CVE Database

# RECONOCIMIENTO DE EXPLOTABILIDADES

- **Fuentes publicas: cvedetails.com**
- **EXPLOIT-DB (API - searchsploit)**
  - `searchsploit apache 2.4`

# RECONOCIMIENTO DE EXPLOTABILIDADES

```
kali@kali:~$ searchsploit wordpress mail list
------------------------------------------------------------------------------ --
 Exploit Title                                                                |
------------------------------------------------------------------------------ --
WordPress Plugin Mailing List - Arbitrary File Download                       | p
WordPress Plugin Mailing List 1.3.2 - Remote File Inclusion                   | p
WordPress Plugin WP-phpList 2.10.2 - 'unsubscribeemail' Cross-Site Scripting  | p
------------------------------------------------------------------------------ --
Shellcodes: No Results
kali@kali:~$
kali@kali:~$ searchsploit wordpress mail list | grep "Mailing List 1.3.2"
kali@kali:~$
kali@kali:~$ searchsploit wordpress mail list --colour | grep "Mailing List 1.3.2
WordPress Plugin Mailing List 1.3.2 - Remote File Inclusion                   | p
kali@kali:~$
```

# ANÁLISIS DE EXPLOTACIONES

**Sploitus**:

- Ejemplo de Uso: Navegar a sploitus.com y buscar por la tecnología o el tipo de vulnerabilidad. Ej. ”remote code execution”

**Acceso a CVE Database**:

- Ejemplo de Uso: Navegar a cvedetails.com y buscar información detallada de CVEs específicos, tecnologías asociadas, incluso pruebas de concepto públicas

# AUTOMATIZACIONES

- El almacenaje de exploits y CVEs es crucial para comprensión de los mismos y la mejora en cuanto a seguridad informática
- Herramientas y recursos proporcionados son esenciales para mantenerse informado y protegido

# AUTOMATIZACIONES

**Llamado a la acción:**

- Continuar aprendiendo y utilizando recursos de seguridad ofensiva en entornos controlados, ayuda y nutre al pentester para mejorar la seguridad personal y empresarial en los ámbitos en los que la aplica.