



```
root@ahbyte:~# ./aegis_init
```

Aegis Terminal

El Escudo de la Seguridad Digital: Suite Avanzada
de Pentesting

 Desarrollado por: AHByte

 Versión: 1.6 Stable



Introducción y Filosofía

```
// AegisTerminal Core Concept  
  
class AegisTerminal {  
    vision = "Centralized Automation";  
    goal = "Strategic Focus";  
}
```

_AegisTerminal centraliza las herramientas más potentes en una interfaz modular.

_Filosofía: "Automatizar lo repetitivo para centrarse en lo estratégico".

_Inspiración: Basado en la eficiencia de suites clásicas como Iscript, con un enfoque moderno.



Reconocimiento de Red

- 🔒 Gestión de Identidad: MAC & IP Anonymity
- 🔍 Nmap Avanzado: Stealth & Version Detection
- 🎯 Análisis Agresivo: OS & Service Fingerprinting

```
root@aegis:~# nmap -sS -sV -T4 192.168.1.1
Starting Nmap 7.92...
Nmap scan report for target (192.168.1.1)
PORT STATE SERVICE VERSION
80/tcp open  http Apache 2.4.41
```



Auditoría Inalámbrica (WiFi)

Capacidades de la Suite

- > Gestión de interfaces en modo monitor con **airmon-ng**.
- > Escaneo de redes en tiempo real con **airodump-ng**.
- > Captura automatizada de handshakes WPA/WPA2.
- > Evaluación de seguridad en infraestructuras inalámbricas.

```
CH 11 ][ Elapsed: 12 s ][ 2025-12-30 14:00
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
AA:BB:CC:DD:EE:FF -42 12 45 0 11 54e WPA2 CCMP PSK Target_WiFi

BSSID STATION PWR Rate Lost Frames Probe
AA:BB:CC:DD:EE:FF 11:22:33:44:55:66 -50 0 - 1 0 12

[+] WPA HANDSHAKE CAPTURED!
```

Escaneo Web Estratégico



Nikto

Análisis exhaustivo de servidores web en busca de configuraciones inseguras, archivos peligrosos y CGI's obsoletos.



WPScan

Auditoría especializada para ecosistemas WordPress. Detección de plugins, temas y versiones del core vulnerables.

[!] Identificación temprana de vectores de ataque.



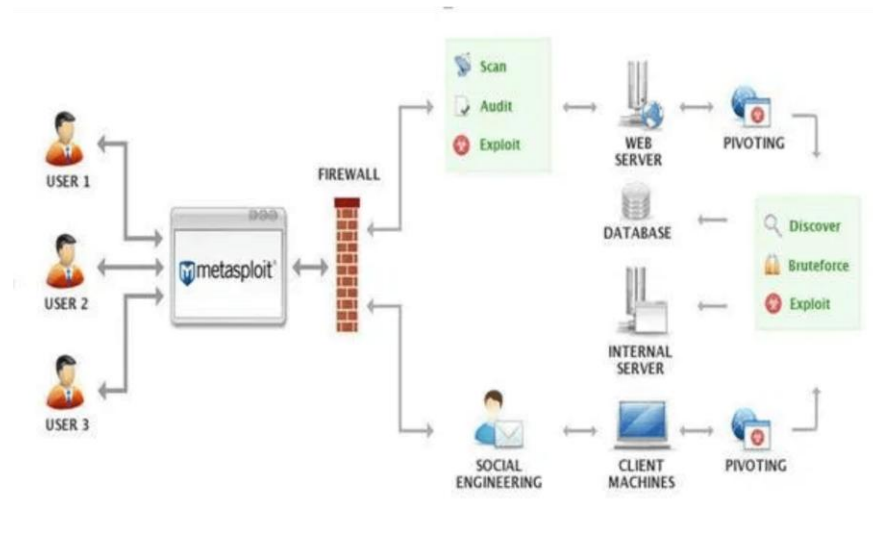
Fuerza Bruta y Explotación

Hydra: Brute Force

Ataques automatizados contra servicios críticos (**SSH, FTP**).
Soporte para wordlists personalizadas y multithreading para máxima eficiencia.




Metasploit Framework

Generación de payloads con **msfvenom** y configuración de listeners con **msfconsole**. Demostración de impacto real mediante la obtención de acceso.



Ingeniería Social (SET)

Integración de la suite líder **Social-Engineer Toolkit** para evaluar el factor humano en la seguridad.

-  Clonación de sitios web para simulaciones de phishing ético y recolección de credenciales.
-  Vectores de ataque basados en email (Spear-Phishing) y medios extraíbles infectados.
-  Herramienta clave para programas de concienciación y evaluación de resiliencia organizacional.

Social Engineering Tactics to Watch For

Knowing the red flags can help you avoid becoming a victim.



Your 'friend' sends you a strange message.



Your emotions are heightened.



The request is urgent.



The offer feels too good to be true.



You're receiving help you didn't ask for.



The sender can't prove their identity.

Auditoría Móvil (Android/iOS)

Análisis Básico

Extracción de metadatos críticos, permisos y versiones de SDK utilizando **aapt**.

```
$ aapt dump badging app.apk  
package: name='com.target.app'  
sdkVersion:'21'  
targetSdkVersion:'30'
```

Análisis Profundo

Descompilación completa de archivos APK en código Smali y recursos con **apktool**.

```
$ apktool d app.apk  
I: Using Apktool 2.6.1  
I: Loading resource table...  
I: Decompiling code...
```


Instalación y Escalabilidad

Instalador Inteligente

Gestión automatizada de dependencias en Kali Linux y sistemas Debian.

```
# sudo ./setup.sh
```

Arquitectura Modular

Estructura de directorios diseñada para la fácil integración de nuevos módulos y herramientas.

Enfoque Comunitario

Código abierto bajo licencia GPL-3.0, fomentando la colaboración y mejora continua.



Conclusión

AegisTerminal es la solución integral para el profesional de seguridad moderno, cubriendo todas las fases del ciclo de vida del pentesting.

[!] ADVERTENCIA: Esta herramienta es exclusivamente para fines educativos y auditorías autorizadas. El uso indebido es ilegal.

```
root@aegis:~# exit
Logout... [OK]
```

