**🔍 1. Havoc Nedir?**

**Havoc**, modern güvenlik çözümlerini atlatmak için geliştirilmiş, modüler, hızlı ve esnek bir **C2 (Command & Control)** framework’tür.

* Açık kaynaklı, Go ve C++ ile yazılmıştır
* **Graphical User Interface (GUI)** arayüzüne sahiptir
* **Reflective DLL injection, fileless execution**, AMSI/ETW bypass gibi teknikleri destekler
* Cobalt Strike, Mythic gibi ticari çözümlere **özgür ve güçlü bir alternatif** sunar

**📦 2. Havoc Özellikleri**

| **Özellik** | **Açıklama** |
| --- | --- |
| 💻 GUI tabanlı kontrol | Ajan kontrolü grafiksel arayüz üzerinden yapılır |
| 🧩 Modüler tasarım | Komutlar, modüller ve payload’lar özelleştirilebilir |
| 🔒 AV/EDR atlatma | AMSI/ETW bypass, shellcode obfuscation, encrypted C2 |
| 🧠 Post-Exploitation | Sistem keşfi, credential dump, keylogger, pivoting |
| 📡 Çoklu listener desteği | HTTP, HTTPS, TCP listener yapılandırması |
| 🧬 Shellcode üretimi | Meterpreter veya özel loader ile uyumlu |

**⚙️ 3. Kali Linux Üzerinde Havoc Kurulumu**

**✅ Adım 1: Havoc’u klonla**

git clone https://github.com/HavocFramework/Havoc.git

cd Havoc

**✅ Adım 2: Bağımlılıkları yükle**

sudo apt install cmake mingw-w64 golang build-essential

**✅ Adım 3: Build işlemi**

./install.sh

Bu işlem sonunda hem Havoc Server hem Havoc GUI hazırlanır

**🖥️ 4. Havoc Başlatma**

**▶️ Server’ı başlat:**

cd Teamserver

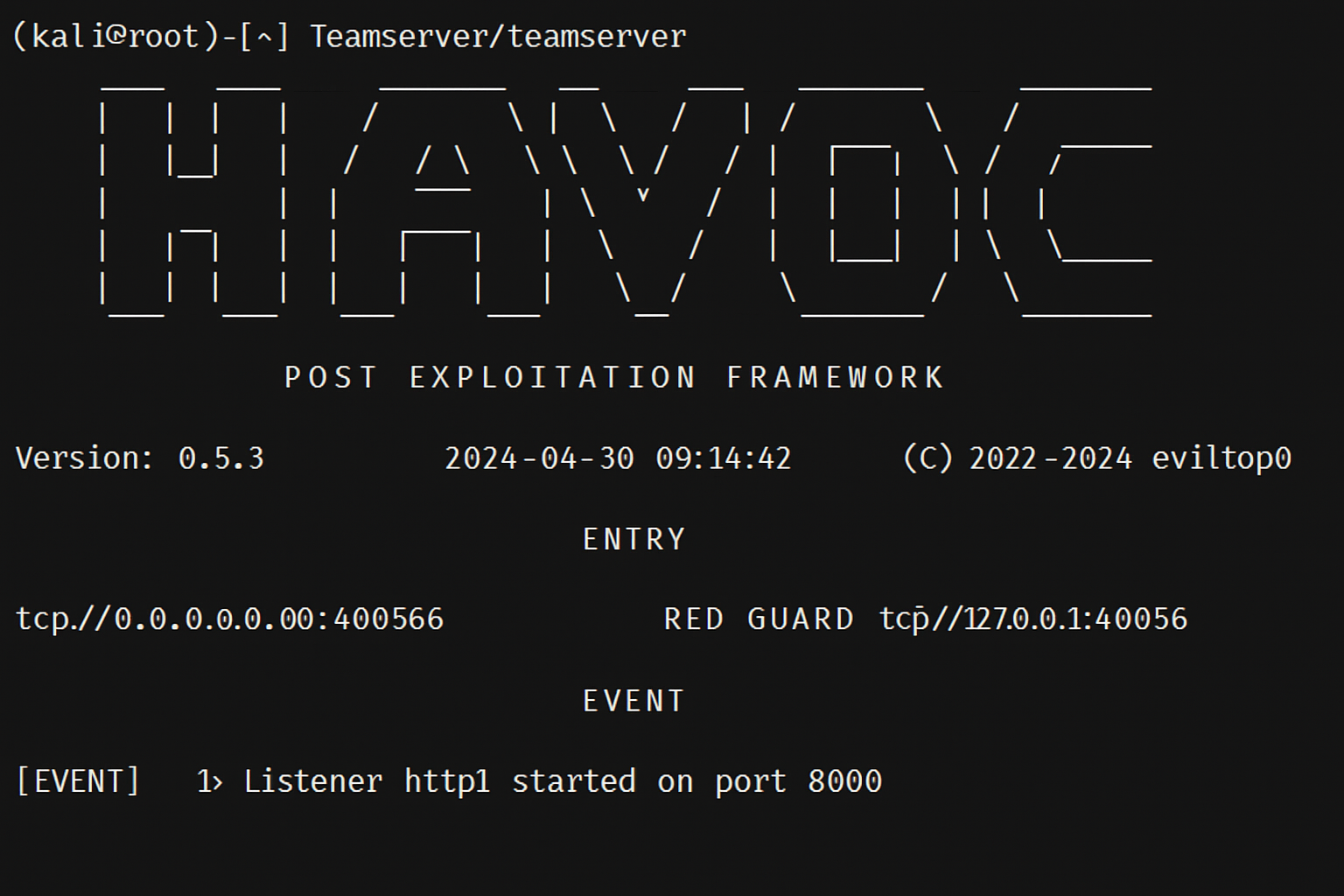
./teamserver

**▶️ GUI (Client) başlat:**

cd Client

./havoc

GUI açıldıktan sonra Teamserver’a IP ve port ile bağlanılır.



**🔧 5. Listener ve Payload Oluşturma**

**➕ Listener oluştur (örnek HTTP):**

* GUI → Listeners → Create
* Name: http1
* Type: HTTP
* Port: 8000

**🧬 Payload üret:**

* GUI → Payloads → Create
* Type: ELF, EXE, DLL, Shellcode
* Ajan adı: LinuxAgent
* Listener: http1
* Output: payload.exe ya da shellcode.bin

**🕵️ 6. Ajan (Beacon) Sisteme Yüklendikten Sonra**

Agent başarılı şekilde sisteme düştüğünde GUI'de aşağıdaki gibi görünür:

pgsql

KopyalaDüzenle

[+] New session from 192.168.1.23: Beacon Connected!

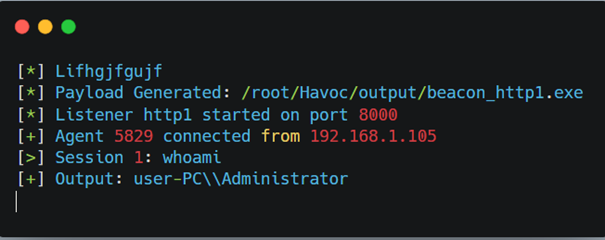
**➤ Ajanla Etkileşim:**

* CMD veya PowerShell komutu çalıştır
* Process, file, keylogger, credential dump işlemleri
* TCP pivot ile lateral movement

**🔥 7. Post-Exploitation Modülleri**

| **Komut / Modül** | **Açıklama** |
| --- | --- |
| shell | Komut satırı erişimi sağlar |
| screenshot | Ekran görüntüsü alır |
| keylogger | Tuş kayıtlarını başlatır |
| ls, cd, upload, download | Dosya sistemi işlemleri |
| credentials | LSASS üzerinden şifre bilgisi toplar |
| inject | Başka bir prosese shellcode enjekte eder |
| persistence | Kalıcılık oluşturur (registry/scheduled task) |

📷 8. Örnek Terminal/Görsel Çıktılar



**🎯 10. Öğrenim Çıktıları**

* Modern C2 framework mimarisini anlama
* Listener, payload, beacon ve komut akışını öğrenme
* AV/EDR atlatma taktikleri hakkında uygulamalı bilgi
* Post-exploitation evresinde sistem manipülasyonunu deneyimleme
* GUI kontrollü Red Team altyapısının nasıl yönetildiğini kavrama