**C2 Frameworks Nedir?**

**C2 (Command and Control) Frameworks**, bir sızma testi (penetrasyon testi) ya da saldırı sırasında hedef sistem üzerinde **uzaktan kontrol sağlamak** için kullanılan altyapılardır. Bu frameworkler sayesinde saldırgan ya da Red Team üyesi:

* Hedef sisteme komut gönderebilir,
* Dosya transferi yapabilir,
* Erişim seviyesini yükseltebilir (privilege escalation),
* İletişimi şifreli bir şekilde sürdürebilir.

C2 Framework'ler saldırının “içerideki yönetim aşaması”nı temsil eder. Yani sisteme girdikten sonra orada nasıl hareket edileceğini, komutların nasıl verileceğini ve verilerin nasıl dışarı çıkarılacağını belirler.

Bu araçlar genellikle **Red Team operasyonlarında**, **APT analizlerinde** ve **gelişmiş sızma testlerinde** kullanılır.

## Frameworks Kapsamındaki Araçlar:

* Araç 1: **Brute Ratel**
* Araç 2: **Mythic**
* Araç 3: **Covenant**
* Araç 4: **Empire**
* Araç 5: **Havoc**

## Araç 1: Brute Ratel

### Nedir?

Brute Ratel, gelişmiş Red Team ve sızma testi operasyonları için geliştirilmiş bir C2 (Command and Control) framework’tür. Özellikle tespit edilmeden çalışabilmesiyle dikkat çeker. Antivirüs ve EDR sistemlerini atlatma konusunda oldukça başarılıdır.

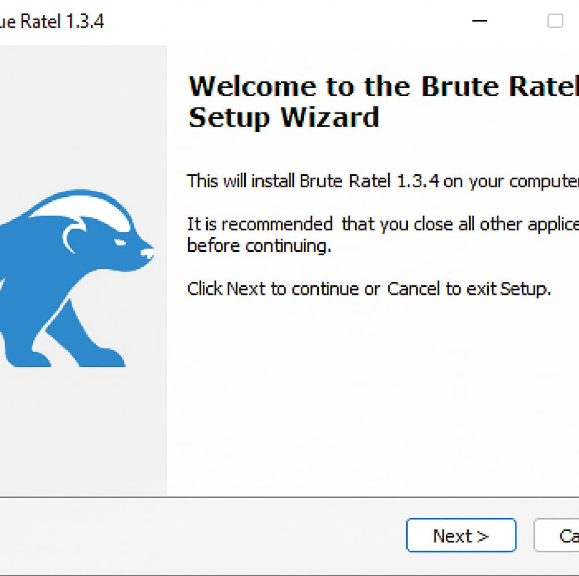
### Özellikleri:

* GUI (grafik arayüz) üzerinden kontrol imkânı sunar.
* AV ve EDR atlatma mekanizmalarına sahiptir.
* Modüler yapıdadır; farklı payload’lar üretilebilir.
* Beacon (istemci) ile iletişim şifreli olarak gerçekleşir.
* Windows sistemler üzerinde yoğunlaşmıştır.

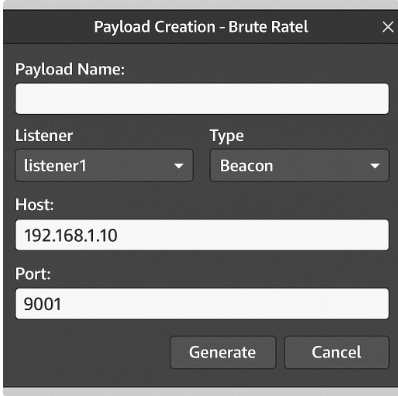
### Kullanım Alanları:

* Red Team operasyonları
* Sızma testleri (Pentest)
* Tespit edilmeden sistemde kalma (stealth persistence)
* EDR/AV karşılaştırma testleri

### Kurulum Aşamaları (Genel):

1. Brute Ratel'in resmi sitesinden lisanslı sürüm temin edilir. (Ücretlidir)
2. Sistem gereksinimleri kontrol edilir (genellikle Windows 10+)
3. Brute Ratel kurulumu yapılır ve kullanıcı arayüzü üzerinden yapılandırma yapılır. 

- Görsel: Brute Ratel kurulum sihirbazı ekranı. Kurulum sürecinde kullanıcı, bu arayüz üzerinden adımları takip ederek gerekli yapılandırmaları gerçekleştirir.

1. Payload oluşturulur ve hedef sisteme gönderilir. 

-Yukarıda örnek bir Brute Ratel payload oluşturma ekranı görülmektedir.

1. Beacon bağlantısı kurulduktan sonra kontrol paneli üzerinden yönetim sağlanır.

**Not:** Brute Ratel yasal olarak sadece lisanslı kullanıcılar tarafından kullanılabilir. Kötüye kullanımı yasa dışıdır.

### Dikkat Edilmesi Gerekenler:

* Ticari bir araçtır; ücretli lisansa ihtiyaç duyulur.
* Gerçek sistemlerde izinsiz kullanımı suçtur.
* AV/EDR atlatma gücü yüksek olduğu için dikkatli ve etik kullanılmalıdır.
* Kullanımı log kaydı bırakabilir, analiz yapılırken gizliliğe özen gösterilmelidir.

**ARAÇ 2: MYTHIC**

**Mythic Nedir:**

Mythic, modern ve modüler bir C2 (Command and Control) framework’üdür. Python ve Go dilleriyle geliştirilmiştir. Açık kaynaklıdır ve Docker desteği sayesinde hızlıca kurulup yönetilebilir. Kullanıcı dostu web arayüzüyle saldırı kampanyalarının planlanması ve izlenmesi kolaydır.

**Özellikleri:**

-Web tabanlı kullanıcı arayüzü

-REST API desteği

-Çoklu agent (Apollo, Poseidon vb.) desteği

-Otomasyon, görev yönetimi ve komut geçmişi

-Docker ile hızlı dağıtım

-Geliştirilebilir ve açık kaynak

**Kullanım Alanları:**

-Red Team operasyonları

-Saldırı simülasyonları

-Eğitim amaçlı senaryo testleri

-Komuta-kontrol iletişimi yönetimi

**Kurulum Aşamaları:**

**1. Sistem Gereksinimleri:**

-Linux veya Windows sistem

-Docker ve Git kurulu

-Python 3.8+ önerilir

**2. Depoyu İndirme: **

**3. Docker ile Kurulum: **

**4. Web Arayüzüne Erişim:**

Kurulum tamamlandıktan sonra tarayıcı üzerinden Mythic paneline şu adresten ulaşılır:

[http://localhost:7443]

**Dikkat Edilmesi Gerekenler:**

•Docker düzgün çalışmalı, yoksa kurulum tamamlanamaz.

•Antivirüs yazılımları bazı işlemleri engelleyebilir.

•Agent modülleri ayrı olarak indirilip yapılandırılmalıdır.

•Docker kurulumundan sonra sistemi yeniden başlatmak gerekebilir.

**ARAÇ 3: COVENANT**

**Covenant Nedir:**

Covenant, C# diliyle yazılmış, .NET tabanlı açık kaynaklı bir C2 (Command and Control) framework’üdür. Red Team aktivitelerinde gelişmiş kontrol ve izleme sunar. Web tabanlı kullanıcı arayüzüyle çalışır ve kullanıcı dostu yapısıyla öne çıkar.

**Özellikleri:**

✓.NET tabanlı, C# ile yazılmıştır

✓Web tabanlı arayüz

✓HTTPS iletişimi kullanır

✓Multi-user desteği (aynı anda birden fazla kullanıcı kontrolü)

✓Cross-platform istemci yönetimi

✓Gelişmiş görev ve modül kontrolü

**Kullanım Alanları:**

✓Red Team operasyonları

✓Sızma testleri

✓Ajan kontrol ve komut yönetimi

✓Gelişmiş hedef sistem etkileşimi

**Kurulum Aşamaları:**

**1. Sistem Gereksinimleri:**

•NET Core 3.1 yüklü olmalı

•Git ve PowerShell gereklidir

•Windows işletim sistemi önerilir

**2. Covenant’ın İndirilmesi: **

**3. Dotnet ile Derleme: **

**4. Covenant’ı Çalıştırma: **

**5. Web Arayüzüne Erişim:**

Tarayıcı üzerinden şu adrese gidilerek erişilir:

[https://localhost:7443]

**Dikkat Edilmesi Gerekenler:**

•NET Core 3.1 doğru şekilde yüklenmiş olmalı

•PowerShell script’leri engellenmemeli

•Varsayılan port olan 7443’ün sistemde açık olması gerekir

•Anti-virüs yazılımları Covenant dosyalarını tehdit olarak görebilir

**ARAÇ 4: EMPIRE**

**Empire Nedir:**

Empire, PowerShell ve Python tabanlı, post-exploitation (istismar sonrası) için kullanılan güçlü bir C2 (Command and Control) framework’tür. Özellikle hedef sistem üzerinde kalıcılık, veri toplama ve komut kontrolü için tercih edilir. Empire, kullanıcı dostu CLI (komut satırı arayüzü) ile çalışır ve geniş modül desteğine sahiptir.

**Özellikleri:**

-PowerShell ve Python tabanlı ajanlar

-CLI (komut satırı) üzerinden yönetim

-Modüler mimari

-Kalıcılık (persistence) ve yükseltilmiş ayrıcalık destekleri

-Saldırı sonrası veri toplama, oturum yönetimi, keylogger, ekran görüntüsü alma gibi yetenekler

-HTTP/HTTPS üzerinden iletişim

-RESTful API desteği

**Kullanım Alanları:**

✓Red Team faaliyetleri

✓Sızma testleri

✓Post-exploitation işlemleri (erişim elde ettikten sonra veri toplama, yayılma vs.)

✓Kalıcılık ve hedef sistem kontrolü

**Kurulum Aşamaları:**

**1. Sistem Gereksinimleri:**

•Linux tabanlı işletim sistemi önerilir (örneğin: Kali Linux)

•Python 3.6+

•Git ve pip kurulu olmalı

**2. Empire’ın İndirilmesi: **

**3. Kurulum Scriptini Çalıştırma: **

**4. Empire’ı Başlatma: **

**Dikkat Edilmesi Gerekenler:**

✓Python bağımlılıkları eksiksiz yüklenmeli

✓Kali gibi sistemlerde kurulumdan önce güncelleme yapılmalı

✓Bazı güvenlik yazılımları tarafından engellenebilir

✓Kurulum sonrası listeners ve agents yapılandırmaları yapılmalıdır

**ARAÇ 5: HAVOC**

**Havoc Nedir:**

Havoc, modern bir C2 (Command and Control) framework’tür. Rust diliyle geliştirilmiş, açık kaynaklı, gelişmiş Red Team operasyonlarında kullanılmak üzere tasarlanmıştır. Grafiksel arayüz desteği ve hızlı çalışan Rust ajanları ile dikkat çeker. Genellikle AV (antivirüs) ve EDR (endpoint detection & response) sistemlerinden kaçınmak için kullanılır.

**Özellikleri:**

✓Rust ile yazılmıştır (çok hızlı ve kararlı)

✓GUI (grafik kullanıcı arayüzü) destekli

✓Ajanlar düşük tespit oranına sahiptir

✓Modüler yapı: payload, listener, komut yönetimi ayrı ayrı tanımlanabilir

✓Cross-platform desteği (Linux/Windows)

✓HTTPS ile şifreli iletişim sağlar

**Kullanım Alanları:**

✓Red Team operasyonları

✓Sızma testlerinde gelişmiş kalıcılık ve kontrol sağlamak

✓Antivirüs ve EDR atlatma çalışmaları

✓Post-exploitation işlemleri

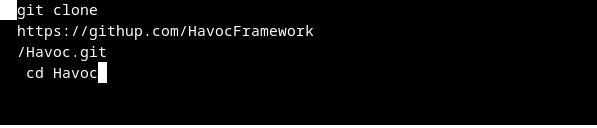
**Kurulum Aşamaları:**

**1. Sistem Gereksinimleri:**

•Rust ve Git yüklü olmalı

•Linux sistem önerilir (örneğin Kali veya Ubuntu)

•GCC ve make gibi derleyici araçlar kurulu olmalı

**2. Depoyu Klonlama: **

**3. Kurulum Scriptini Çalıştırma: **

**4. GUI Başlatma**: 

-Ardından, tarayıcı veya masaüstü arayüzü üzerinden Havoc paneli açılır.

**Dikkat Edilmesi Gerekenler:**

✓Rust derleyicisinin güncel olması gerekir

✓Derleme süreci sırasında eksik paketler hataya yol açabilir

✓İlk kullanımda bazı güvenlik duvarları engelleme yapabilir

✓Agent ve payload'lar özelleştirilmeden kullanılmamalıdır