**Metasploit Framework Nedir?**

**Metasploit Framework**, siber güvenlik uzmanları ve etik hackerlar tarafından yaygın olarak kullanılan, güçlü ve açık kaynaklı bir **sızma testi (penetration testing)** platformudur. Ruby diliyle geliştirilmiş olan bu araç, sistemlerdeki açıklıkları tespit etme, istismar etme (exploit), arka kapı yerleştirme (payload) ve saldırı sonrası işlemleri gerçekleştirme yeteneklerine sahiptir.

İlk olarak HD Moore tarafından geliştirilen Metasploit, daha sonra Rapid7 tarafından satın alınmış ve aktif olarak geliştirilmeye devam edilmiştir. Metasploit, güvenlik açıklarını hızlı bir şekilde test etmeyi ve sistem zafiyetlerini gerçek saldırı senaryolarına benzer şekilde analiz etmeyi mümkün kılar.

**Metasploit Ne İşe Yarar**

* **Exploit (İstismar) gerçekleştirme:** Bilinen güvenlik açıklarını kullanarak sistemlere sızma.
* **Payload (Yük) gönderme:** Hedef sisteme erişim sağlamak için zararlı kod çalıştırma.
* **Post-Exploitation:** Erişim sağlanan sistemde bilgi toplama, kullanıcı hakları yükseltme vb.
* **Auxiliary modüller:** Tarama, brute-force, servis tanıma gibi işlemler için kullanılır.
* **Encoder:** Payload’ları güvenlik yazılımlarından gizlemek için kodlama.
* **Nops:** İstismar sırasında boş talimatlar (no operation) ile istikrar sağlama.

**Metasploit Nasıl Kurulur?**

Kali Linux gibi sızma testi dağıtımlarında Metasploit ön yüklü gelir. Diğer sistemler için manuel kurulum gerekebilir.

**Kali'de başlatmak için:**

**metin, ekran görüntüsü içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**Meterpreter Nedir?**

**Meterpreter**, Metasploit’in gelişmiş payload’larından biridir. Hafızada çalışır, diske yazılmaz, tespit edilmesi zordur. Özellikleri:

* Dosya sistemi kontrolü
* Kamera ve mikrofon erişimi
* Anahtar kaydedici (keylogger)
* Ekran görüntüsü alma
* Ters bağlantı (reverse shell)

**Avantajları**

* Geniş açık veritabanı (exploit-db tabanlı)
* Otomasyon ile hızlı test imkânı
* Modüler yapı (kendi exploit ya da payload’ını yazma)
* Aktif topluluk ve geniş belge desteği
* Gelişmiş post-exploitation araçları (özellikle meterpreter)

**Dezavantajları**

* Öğrenme eğrisi yüksektir (özellikle CLI kullanımı).
* Ağ güvenlik duvarları tarafından tespit edilebilir.
* Gelişmiş hedeflerde başarısız olabilir (yeni güncellemelerle patchlenmiş sistemler).

**Gelin kullanımına beraber göz atalım:**

**metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**