**DNSChef**, sahte DNS yanıtları üreterek DNS trafiğini manipüle etmeye yarayan bir **DNS proxy/sniffer** aracıdır. Özellikle **MITM (Man-in-the-Middle)** saldırılarında, **phishing senaryolarında** ve **penetrasyon testlerinde** yaygın olarak kullanılır.

**Bu Aracın Özellikleri Nelerdir?**

* Belirli domain’ler için **yanlış IP döndürme**
* Tüm DNS trafiğini loglama ve yönlendirme
* Ters proxy ile sahte site barındırma testleri için ideal
* Tüm sorguları dinleyebilir veya sadece belirlenen domain’lere yanıt verebilir
* **Python ile yazılmıştır** ve oldukça hafiftir

**DNSChef Aracını Kali Linux’ta Kurma ve Kullanma Adımları**

**Adım 1: DNSChef Kurulu mu Kontrol Et / Yükle**

Kali’de genellikle yüklü gelir. Kontrol etmek için:

“dnschef -h”

Eğer kurulu değilse:

“sudo apt update

sudo apt install dnschef -y”

**Adım 2: Basit Bir DNS Spoofing Senaryosu Oluştur**

Örneğin, facebook.com gibi bir domain için sahte IP yönlendirmesi yapmak istiyoruz.

“sudo dnschef --fakeip 192.168.1.100 --fakedomains facebook.com”

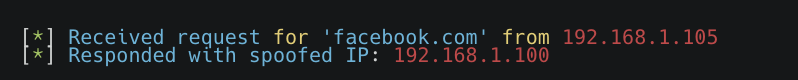


**Adım 3: Hedef Sistemde DNS Ayarlarını Kali IP’si Olarak Değiştir**

Bu işlem hedef sistemde yapılır. Kali makinesinin IP’si DNS sunucusu olarak tanımlanır. Örn: 192.168.1.103

**Adım 4: DNS Sorgularını Gerçek Zamanlı İzle**

DNSChef tüm gelen sorguları terminalde loglar:



**Adım 5: Diğer Kayıt Türlerini Spoof Et (Opsiyonel)**

“sudo dnschef --fakemx mail.fake.net --fakedomains example.com”