**Boofuzz**, sızma testlerinde hedef sistemlerin güvenliğini değerlendirmek için kullanılan açık kaynaklı bir **fuzzing (hatalı veri ile test)** aracıdır. Python tabanlıdır ve TCP/IP protokolleri, web sunucuları, cihaz yazılımları gibi çeşitli hedeflere karşı kullanılabilir. **Boofuzz**, eski Sulley framework’ünün devamı niteliğindedir ve daha kararlı, modüler bir yapı sunar.

**Bu aracın özellikleri nelerdir?**

**Fuzzing Testleri**: Hedef uygulamalara çeşitli girdiler göndererek beklenmeyen durumları (crash, timeout) gözlemler.

**Protokol Desteği**: FTP, HTTP, SNMP gibi birçok protokolde kullanılabilir.

**Session Yönetimi**: Oturumların kontrolünü sağlar, testleri duraklatıp devam ettirebilir.

**Kapsamlı Raporlama**: Hangi veri girdisinin hangi sonucu doğurduğunu detaylı şekilde raporlar.

**Python API**: Kütüphane olarak kullanılabilir, özelleştirilebilir testler yazılabilir.

**Açık Kaynak ve Aktif Geliştirici Desteği**: GitHub üzerinden sürekli güncellenir.

**Bu aracı Kali Linux'a kurma ve kullanma adımları:**

**Adım 1: Python ve pip’in Kurulu Olduğundan Emin Olun**

Boofuzz, Python 3 tabanlı çalışır. Sisteminizde Python 3 ve pip 3 yüklü değilse aşağıdaki komutlarla yükleyin:

“sudo apt update

sudo apt install python3 python3-pip -y”

**Adım 2: Boofuzz Kurulumu**

pip ile doğrudan kurulum yapabiliriz

“pip3 install boofuzz”

Veya GitHub üzerinden manuel kurulum sağlayabilirsiniz

“git clone https://github.com/jtpereyda/boofuzz.git

cd boofuzz

python3 setup.py install”

**Adım 3: Basit Bir Fuzzing Senaryosu Oluşturma**

Kali üzerinde boofuzz\_test.py adında bir Python dosyası oluşturun. Aşağıda örnek bir python dosyası içeriği mevcut

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 4: Testi Başlatma**

Dosyayı çalıştırmak için terminalde bulunduğunuz dizinde şu komutu yazın:

“python3 boofuzz\_test.py”

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu