## Firecrack Nedir, Neden Kullanılır?

Firecrack, basit ama etkili bir **parola kırma (brute-force)** aracıdır. Özellikle HTTP Basic Authentication, FTP, SSH ve benzeri hizmetlerde kullanılan zayıf veya tahmin edilebilir parolaları denemek için kullanılır. Python ile yazılmış olan bu araç, hız ve sadelik ön planda tutularak geliştirilmiştir. Hem dosya tabanlı parola listeleriyle çalışabilir hem de doğrudan terminalden veri girilerek işlem yapılabilir.

Firecrack’in temel amacı, hizmetlere karşı kaba kuvvet (brute-force) saldırısı uygulayarak erişim sağlamaya çalışmaktır. Penetrasyon testlerinde hedef sistemin kimlik doğrulama mekanizmalarının sağlamlığını test etmek amacıyla sıkça tercih edilir. Özellikle zayıf parola politikaları olan sistemlerde etkili sonuçlar verir.

Aracın sade yapısı sayesinde, kullanıcıdan karmaşık bir kurulum veya yapılandırma beklemez. Doğrudan hedef sistem, kullanıcı adı ve parola listesi verilerek çalıştırılabilir.

## Kurulum

Firecrack genellikle bağımlılığı olmayan, taşınabilir bir Python betiği olarak dağıtılır. GitHub üzerinden indirilip doğrudan kullanılabilir.

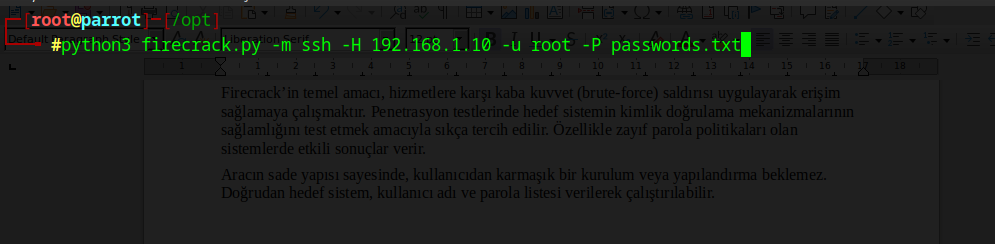
Kurulum için terminalde aşağıdaki adımlar izlenebilir:

* git clone https://github.com/Rajchowdhury420/Firecrack
* cd Firecrack
* python3 firecrack.py –help

Firecrack’in çalışabilmesi için requests, socket veya paramiko gibi bazı temel Python kütüphaneleri gerekebilir. Bu durumda requirements.txt varsa aşağıdaki komutla yükleme yapılabilir:

* pip3 install -r requirements.txt

**Kullanım Örneği:**



Bu örnekte:

* -m ile brute-force yöntemi seçilir (ssh, ftp, http, telnet vb.)
* -H ile hedef IP belirtilir
* -u ile kullanıcı adı girilir
* -P ile parola listesinin bulunduğu dosya belirtilir

## Elde Edilebilecek Bilgilerden ve Etkilerden Örnekler

Başarılı bir brute-force işlemi sonucunda aşağıdaki verilere ulaşılabilir:

* Hedef sistemde geçerli kullanıcı adı ve şifresi
* Yönetici (root/admin) düzeyinde erişim imkânı
* SSH veya FTP üzerinden sistem dosyalarına doğrudan erişim
* Web uygulamalarında kimlik doğrulama atlanarak erişim sağlama
* Zayıf parola politikalarının tespiti

Bu bilgiler ışığında, saldırgan sistemde daha ileri erişim sağlayabilir, veri sızıntısı yapabilir veya sistemi kalıcı şekilde manipüle edebilir. Test senaryolarında bu tür risklerin önceden görülmesi, güvenlik politikalarının güncellenmesi açısından çok değerlidir.

## Kullanılabilecek Parametreler ve Özellikler

Firecrack, sade bir terminal arayüzü üzerinden aşağıdaki parametreleri destekler:

* -m: Kullanılacak modül (ssh, ftp, http-basic, telnet vs.)
* -H: Hedef IP adresi veya domain
* -u: Kullanıcı adı
* -U: Kullanıcı adı listesi (birden fazla kullanıcı için)
* -p: Tek bir parola (liste yerine doğrudan girilmek istenirse)
* -P: Parola listesi dosyası
* --port: Özel port belirtmek istenirse (varsayılan portlar dışı durumlar için)
* --timeout: Her deneme için maksimum bekleme süresi
* --verbose: Deneme sonuçlarını daha ayrıntılı görmek için kullanılabilir

Bu parametrelerle farklı hedeflere yönelik özelleştirilmiş brute-force senaryoları üretilebilir.

Firecrack, basitliği ve etkinliğiyle dikkat çeken bir brute-force aracıdır. Eğitim, test veya denetim senaryolarında güvenlik duvarı arkasındaki servislerin ne kadar güvenli olduğunu anlamak için güçlü bir yardımcıdır. Zayıf parolaların sistemlerde yaratabileceği riskleri ortaya koymak açısından önemlidir. Özellikle parola politikası denetimi yapılacak ağlarda Firecrack, ilk başvurulacak araçlardan biridir.