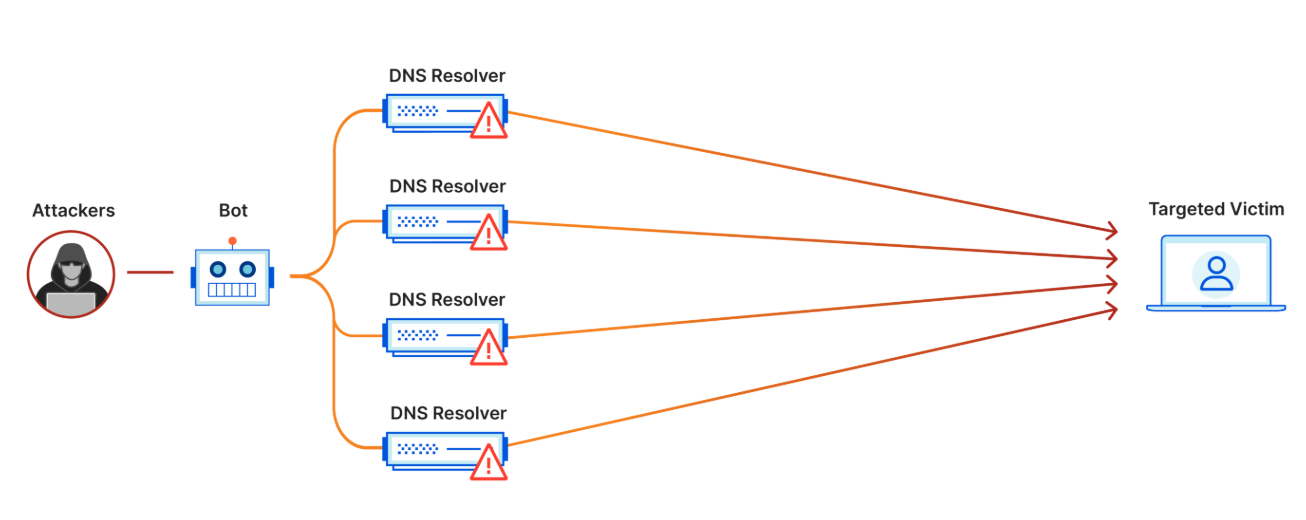
**IP Attack Nedir?**

IP Attack, yani IP tabanlı saldırılar, bilgisayar ağlarında IP (Internet Protocol) üzerinden hedef sistemlere zarar vermek, erişimi engellemek veya bilgileri çalmak amacıyla yapılan saldırı türleridir.

Bu saldırılar genellikle hedef sistemin IP adresi üzerinden gerçekleştirilir ve çok çeşitli yöntemlerle yapılabilir.

**IP Saldırı Türleri**

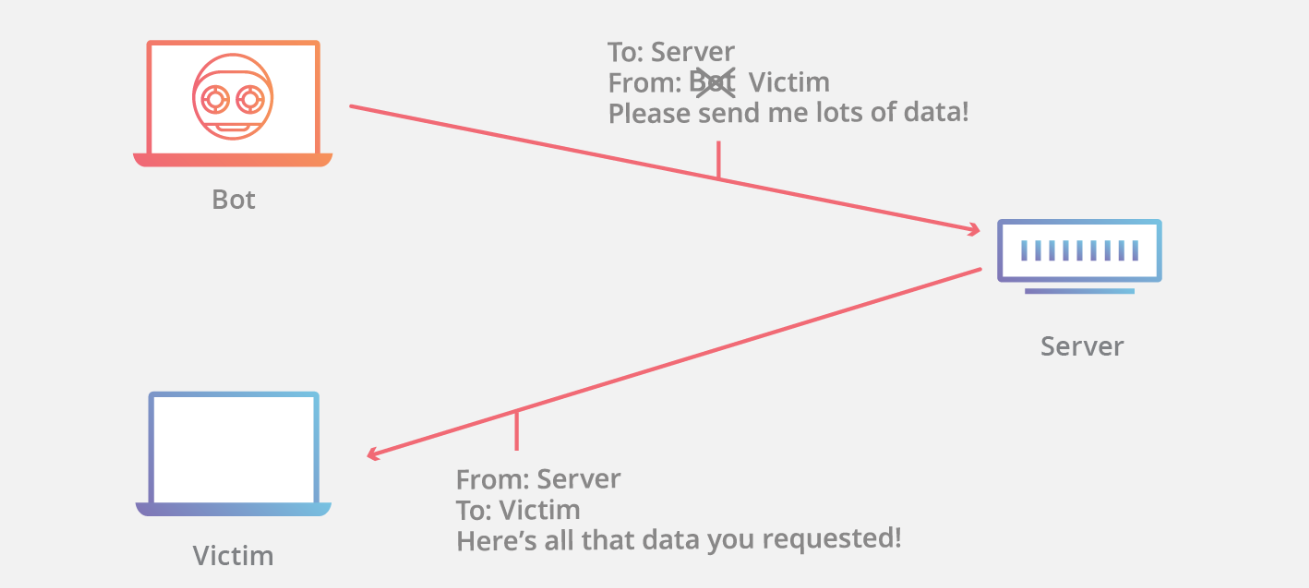
1. **DoS (Denial of Service) ve DDoS (Distributed Denial of Service) Saldırıları**

****

* **DoS**: Tek bir kaynaktan gelen aşırı trafikle hedef sistemin hizmet vermesi engellenir.
* **DDoS**: Birden fazla farklı kaynaktan eş zamanlı gelen trafikle sistem çökertilir.

**Örnek: Ping Flood saldırısı**  
Saldırgan, hedefe çok sayıda ICMP Echo Request (ping) paketi göndererek sistemi meşgul eder.

1. **IP Spoofing (IP Sahteciliği)**

****

Saldırgan, kaynak IP adresini değiştirilerek, hedefe sahte IP ile saldırır. Böylece saldırının kaynağı gizlenir veya hedefte yanlış yönlendirme yapılır.

1. **Smurf Attack**

Özel bir tür DoS saldırısıdır. Saldırgan, hedefin IP adresini kaynak IP olarak kullanarak, broadcast adreslerine ping gönderir. Ağdaki tüm cihazlar hedefe yanıt verir ve hedef aşırı trafikle çökebilir.

**4. Man-in-the-Middle (MitM) Saldırıları**

IP tabanlı iletişimleri keserek veya araya girerek veri çalma, değiştirme saldırılarıdır.

**IP Attack Araçları**

**a) Hping3**

Hping3, ağ paketleri oluşturup göndermeye yarayan güçlü bir araçtır. DoS saldırıları, port tarama, traceroute ve IP spoofing gibi işlemler için kullanılır.

Temel kullanım örneği: ***sudo hping3 -S -p 80 --flood 192.168.1.10***

* -S : SYN paketi gönderir (TCP bağlantı isteği)
* -p 80 : Hedef port 80 (HTTP)
* --flood : Paketleri mümkün olduğunca hızlı gönderir.

**b) Nmap**

Nmap, ağ keşfi ve güvenlik taraması için kullanılır. Açık portlar ve servisler tespit edilir. Saldırı öncesi bilgi toplamak için çok faydalıdır.

**c)Scapy**

Python tabanlı, paket oluşturma ve manipülasyon kütüphanesi. Özel IP paketleri oluşturmak için kullanılır.

**Pratik Örnek: Hping3 ile Basit SYN Flood**

Komut: ***sudo hping3 -S -p 80 --flood 192.168.1.10***

Bu komutla hedef sistemin 80 numaralı portuna, çok sayıda SYN paketi gönderilir. Sistem cevap veremeyince hizmette yavaşlama ya da çökme yaşanabilir.

**IP Attack Önleme Yöntemleri**

* **Firewall Kullanımı**: Şüpheli trafik filtrelenir.
* **Anti-DDoS Çözümleri**: Trafik analizi ve saldırı engelleme araçları.
* **Güçlü Ağ İzleme**: Anormal trafik tespiti.
* **IP Spoofing Önlemleri**: Router ve firewall ayarlarında paket kaynağının doğrulanması.

IP tabanlı saldırılar, ağ güvenliğini tehdit eden önemli saldırı türlerindendir. Bu saldırıların anlaşılması ve önlenmesi, siber güvenlikte temel bilgi alanlarındandır. Hping3 ve benzeri araçlarla yapılan testlerle ağınızın dayanıklılığı ölçülebilir.