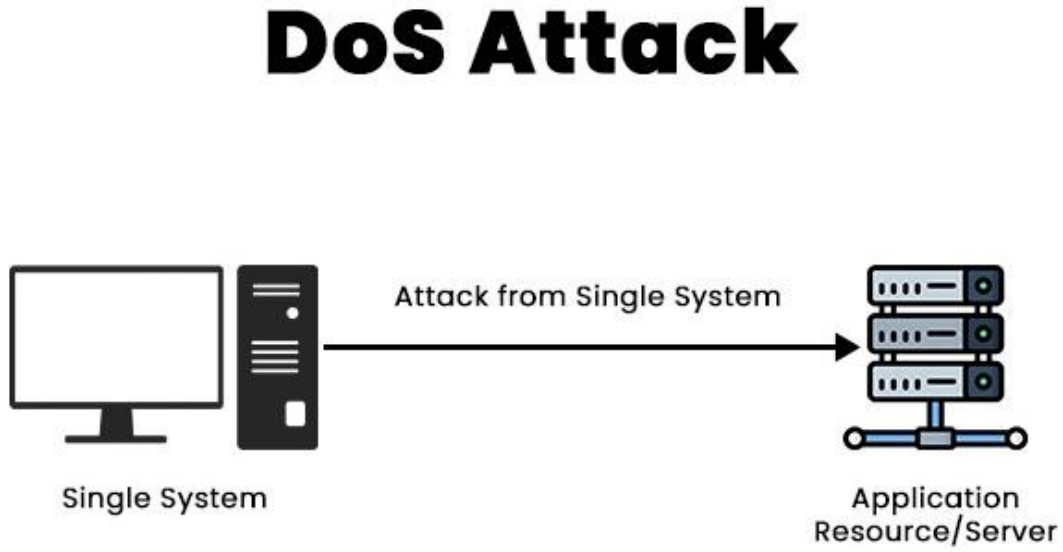
SİBER SALDIRILAR VE SALDIRI ÖNLEME YÖNTEMLERİ

DoS Saldırısı

DoS saldırısı, bilgisayar korsanının sistemi ve ağı tahrip edebilecek bazı farklı saldırı yöntemleri kullanarak hizmeti ele geçirmesi ve ayrıca CPU, ram, arabellek, ağ bant genişliği gibi bilgisayar kaynaklarını işgal edebilmesi nedeniyle normal kullanıcının hizmeti alamaması olarak tanımlanır.

DoS saldırganları, sistemdeki bir yazılım güvenlik açığından yararlanır ve sunucunun RAM veya CPU'sunu tüketmeye devam eder. Bir DoS saldırısının temel amacı, Şekil' de gösterildiği gibi ağ bağlantılı bir hizmeti aşırı yükleyerek kullanılamaz hale getirmektir. Servis sağlayıcıya gönderilen bu kadar çok sayıda kötü niyetli istek, sunucuyu bir noktadan sonra yanıt veremez duruma getirir.



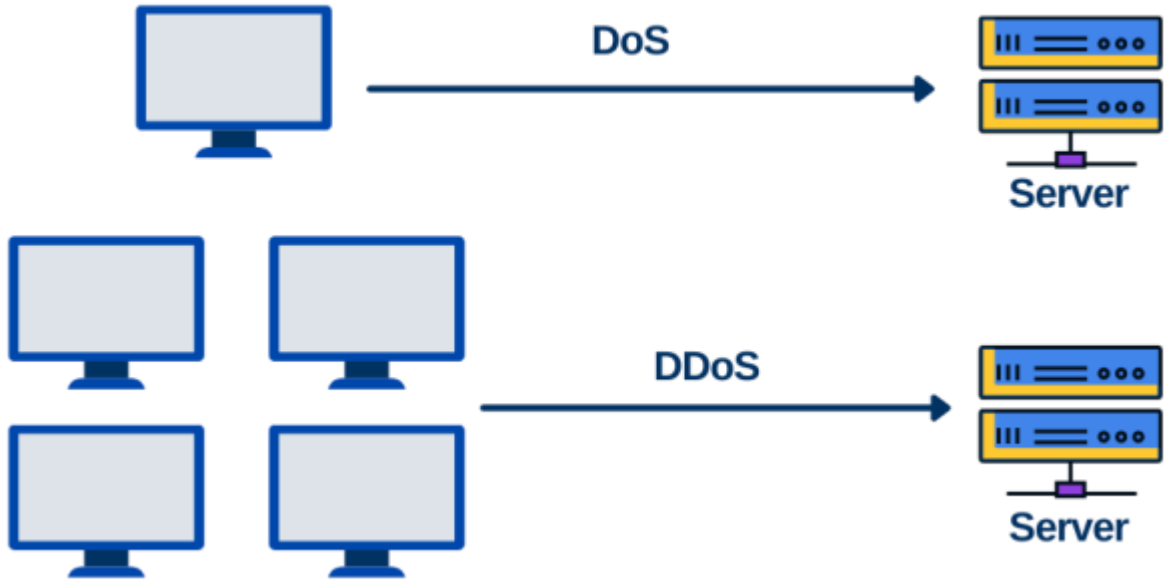
DDoS Saldırısı

DDoS saldırısı, en az bir hedefe karşı bir DoS saldırısı başlatmak amacıyla birçok bilgisayarın kullanıldığı koordineli bir DoS saldırısıdır. Saldırgan, birden fazla bilgisayarın farkında olmadan kaynaklarını kullanarak saldırı başlatır. İstemci/sunucu teknolojisi kullanılırsa saldırgan sayısı arttırılabilir.

- Saldırıyı başlatan gerçek saldırgan.
- Zombi bilgisayarları kontrol edebilen, güvenliği istismar edilmiş anabilgisayarlar.
- Zombi bilgisayarlar (Botnet).
- Hedef bilgisayar.

DDoS Saldırısı

Dağıtılmış Hizmet Reddi (DDoS) saldırısında, bir saldırgan, bir hedefe yönelik saldırıyı düzenlemek için birden çok kaynak kullanır. Bu kaynaklar, kötü amaçlı yazılım bulaşmış bilgisayarların, yönlendiricilerin, IoT cihazlarının ve diğer uç noktaların dağıtılmış gruplarını içerebilir. Şekil ’de, saldırıya katılan ve hedefi hizmet dışı bırakmak için bir paket akışı veya istek üreten güvenliği ihlal edilmiş bir ana bilgisayar ağını göstermektedir



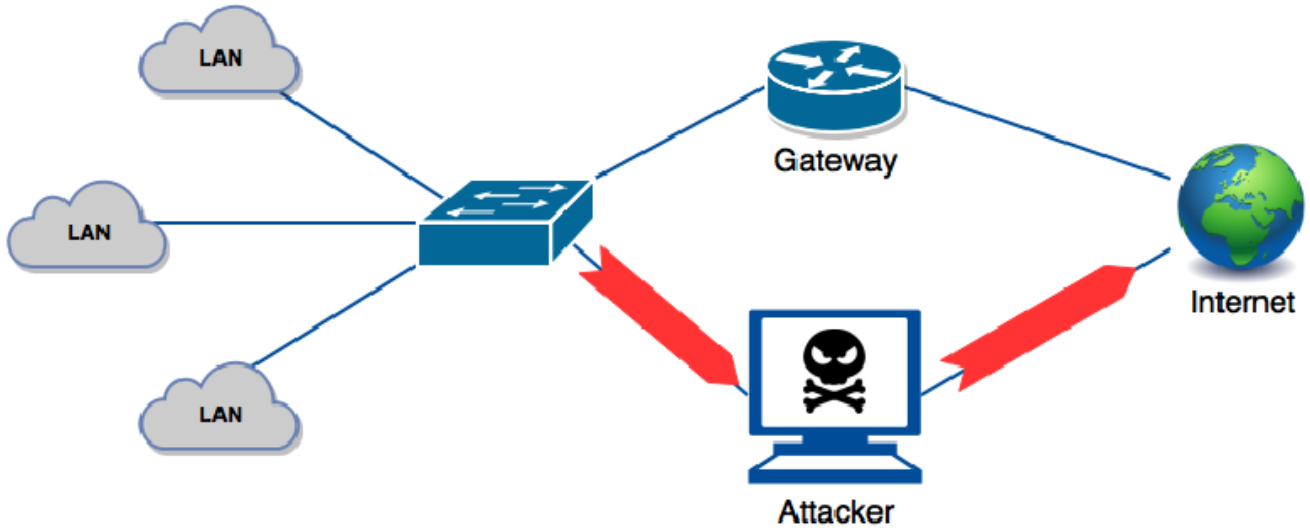
BruteForce (Kaba Kuvvet/Şifre) Saldırısı

Kaba kuvvet saldırısında saldırganlar, hedefledikleri kullanıcı hesaplarına sızmak ve hesapla bağlantılı bilgileri ele geçirmek için genellikle otomatik (amaca yönelik siber korsanlık yazılımları üzerinden) deneme-yanılma yöntemi uygulamaktadır. Bu yöntem, çeşitli güvenlik unsurları içeren karmaşık kombinasyona sahip (ya da kriptografik) şifrelerin kırılmasını mümkün kılmaktadır. Aynı kapsamdaki farklı bir yöntem de manuel olarak rastgele karakterler kullanılarak parola tahmini yapılmaya çalışılmasıdır.

```
NSE: [http-brute 127.0.0.1:80] Trying admin/<empty> against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/123456 against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/12345 against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/123456789 against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/password against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/iloveyou against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/princess against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/12345678 against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/1234567 against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/abc123 against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/nicole against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/daniel against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/monkey against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/babygirl against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/qwerty against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/lovely against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/654321 against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/michael against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/jessica against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/111111 against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/ashley against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/abril against 127.0.0.1:80
NSE: [http-brute 127.0.0.1:80] Trying admin/000000 against 127.0.0.1:80
```

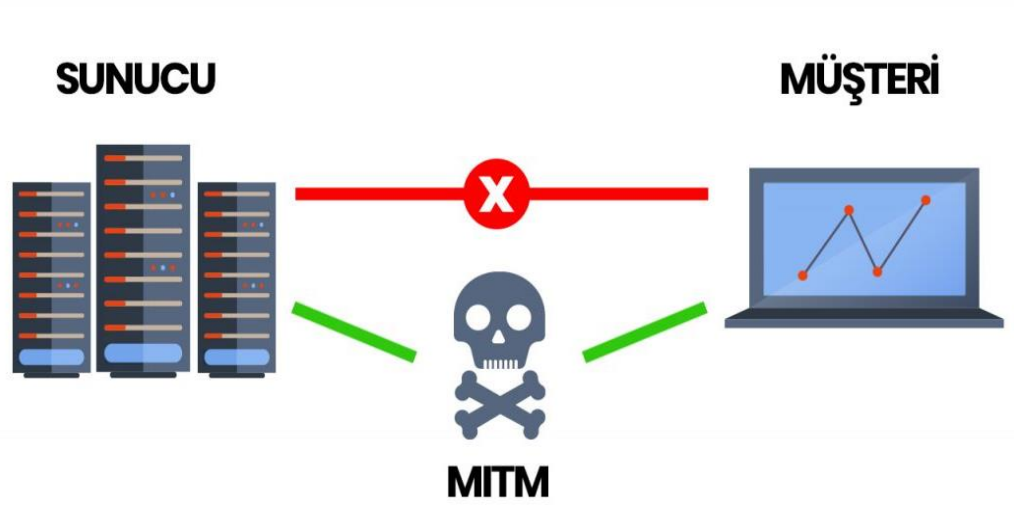
Dinleme Saldırısı

Bilgi güvenliği perspektifinden bakıldığında, paket dinleme (sniffing), trafiği yakalanabileceği, analiz edebileceği ve izlenebileceği bir hedefe yönlendirmek anlamına gelir. Ağ trafiğinin dinlenmesinde temel mantık, Şekil ’de görüldüğü üzere ağ geçidi cihazına gelen her paket kabul edildiği için iki bilgisayar arasındaki tüm verilerin yakalanarak saklanması olarak tanımlanabilir. Düz metin olarak bilgi içeren herhangi bir ağ paketi, saldırganlar tarafından ele geçirilebilir ve okunabilir. Bu bilgiler, kullanıcı adları, şifreler, gizli kodlar, bankacılık detayları veya saldırgan için değerli olan herhangi bir bilgi olabilir. Bilgisayarlar arasındaki bağlantıların şifreli olması bu saldırıya karşı alınabilecek en önemli önlemdir. Şifreli paketler yakalanabilse bile içeriği anlaşılmayacaktır. Şifreleme algoritmasının da saldırılara karşı dayanıklı ve uygun performans sağlayan yapıda olmalıdır.



Ortadaki Adam Saldırısı

Ortadaki adam (Man In The Middle - MITM) saldırısında, saldırgan iki hedef arasındaki iletişimi gizlice dinler ve ardından birbirleriyle doğrudan iletişim kurduklarına inanan iki taraf arasındaki mesajları gizlice aktarır veya değiştirir. Ortadaki adam saldırılarının bir örneği, saldırganın kurbanlarla bağımsız ilişkiler kurduğu ve kurbanların birbirleriyle özel bir ilişkisi üzerinden doğrudan konuştuklarına güvenmelerini sağlamak için aralarındaki mesajları aktardığı dinamik bir gizli dinlemedir. Tüm iletişim saldırgan tarafından kontrol edilir. Saldırgan, iki taraf arasında geçen her önemli mesajı engelleme ve yenilerini enjekte etme kapasitesine sahip olmalıdır. Bu, birçok koşulda doğrudandır; örneğin, şifrelenmemiş bir kablosuz erişim noktasının kapsamı içindeki bir saldırgan, kendisini ortadaki adam olarak ekleyebilir.



SQL Enjeksiyonu

SQLI olarak da bilinen SQL enjeksiyonu, görüntülenmesi amaçlanmayan bilgilere erişmek için veritabanına yönelik kötü amaçlı SQL kodu kullanan yaygın bir saldırı türüdür. Bu bilgiler, kişisel veriler, hassas şirket verileri, müşteri bilgileri veya kullanıcı listeleri dahil olmak üzere pek çok öğeyi içerebilir. SQL enjeksiyon, web uygulamalarından alınan kullanıcı girdileri ile oluşturulan SQL sorgularının manipülasyonu olarak da tanımlanabilir.

Bir SQL enjeksiyonun potansiyel maliyetini hesaplarken ve kredi kartı bilgileri, adresler, telefon numaraları, gibi kişisel bilgilerin çalınması durumunda yaşanacak kayıplar göz önünde bulundurmak önemlidir. SQL enjeksiyonu herhangi bir SQL veritabanına saldırmak için kullanılabilirken, en çok hedefler web siteleri olmaktadır.

SQL Enjeksiyonu