🛡️ ThreatChaser DDoS Simülasyon Testi: Gerçekçi Senaryolarla Güvenlik Testi

Günümüzün dijital dünyasında, işletmelerin çevrimiçi varlıkları operasyonlarının bel kemiğini oluşturmaktadır. Dağıtık Hizmet Engelleme (DDoS) saldırıları, bu kritik hizmetleri hedef alarak, finansal kayıplardan itibar zedelenmesine kadar uzanan ciddi sonuçlar doğurabilir. ThreatChaser DDoS Simülasyon Testi, sisteminizin zayıf noktalarını gerçek bir saldırı yaşanmadan önce tespit etmeniz için tasarlanmış kapsamlı bir çözümdür.

Neden DDoS Simülasyon Testi?

DDoS saldırıları, beklenmedik anlarda ortaya çıkarak iş sürekliliğini ciddi şekilde tehdit eder. Bu tür saldırıların etkilerini azaltmanın en etkili yolu, proaktif bir yaklaşımla sistemlerinizi test etmek ve olası zafiyetleri gidermektir. Kontrollü simülasyon testleri sayesinde, altyapınızın gerçek saldırılar karşısında nasıl performans göstereceğini önceden görebilirsiniz.

ThreatChaser DDoS Simülasyon Testi, kurumların kendi altyapılarını çeşitli saldırı senaryolarıyla test ederek, dayanıklılık seviyelerini bilimsel verilerle ölçmelerine yardımcı olur. Bu sayede, güvenlik açıklarınızı kapatmak ve hizmet kesintilerini önlemek için gerekli iyileştirmeleri zamanında yapabilirsiniz.

Öne Çıkan Özellikler

✅ Gerçekçi Senaryolar

UDP flood, SYN flood, HTTP flood ve daha birçok güncel saldırı tipi, sisteminizin gerçek dünya tehditlerine karşı dayanıklılığını ölçmek için simüle edilir.

✅ Ölçeklenebilir Testler

Küçük ölçekli denemelerden, kurumsal seviyede yoğun saldırılara kadar farklı yük seviyelerinde testler gerçekleştirilebilir.

✅ Risk Analizi

Testler sırasında hizmet kesintisi yaşanan noktalar ve performans düşüşleri detaylı bir şekilde raporlanır.

✅ Performans Ölçümü

Ağ altyapınızın, güvenlik duvarlarınızın (firewall) ve yük dengeleyicilerinizin (load balancer) saldırılara karşı dayanıklılığı somut verilerle ölçülür.

✅ Detaylı Raporlama

Tespit edilen zayıf noktalar ve bunlara yönelik çözüm önerileriyle birlikte kapsamlı, anlaşılır raporlar sunulur.

✅ Önleyici Stratejiler

Altyapınızı güçlendirmek ve gelecekteki saldırılara karşı daha dirençli olmanızı sağlamak için uygulanabilir tavsiyeler sunulur.

Kimler İçin İdeal?

🌐 Kurumsal Firmalar: Online hizmetlerini kesintisiz sürdürmek isteyen tüm kurumlar.

🛒 E-Ticaret Siteleri: Satışların durmasını engellemek ve müşteri memnuniyetini korumak isteyen platformlar.

💳 Bankacılık ve Finans Sektörü: Kritik finansal hizmetlerin kesintisiz ve güvenli bir şekilde sunulmasını sağlamak isteyen kuruluşlar.

📡 Telekom ve İnternet Servis Sağlayıcıları: Ağ altyapılarının güvenliğini ve sürekliliğini maksimum düzeyde tutmak isteyen operatörler.

🏥 Sağlık Kuruluşları: Hasta verilerine kesintisiz erişim sağlamak ve kritik sağlık hizmetlerinin devamlılığını garantilemek isteyen kurumlar.

🎓 Üniversiteler ve Eğitim Kurumları: Online ders platformlarının ve eğitim sistemlerinin sürekliliğini garanti altına almak isteyen kurumlar.

🛡️ Siber Güvenlik Ekipleri: Kendi altyapılarını proaktif güvenlik testleriyle sürekli olarak güçlendirmek isteyen profesyoneller.