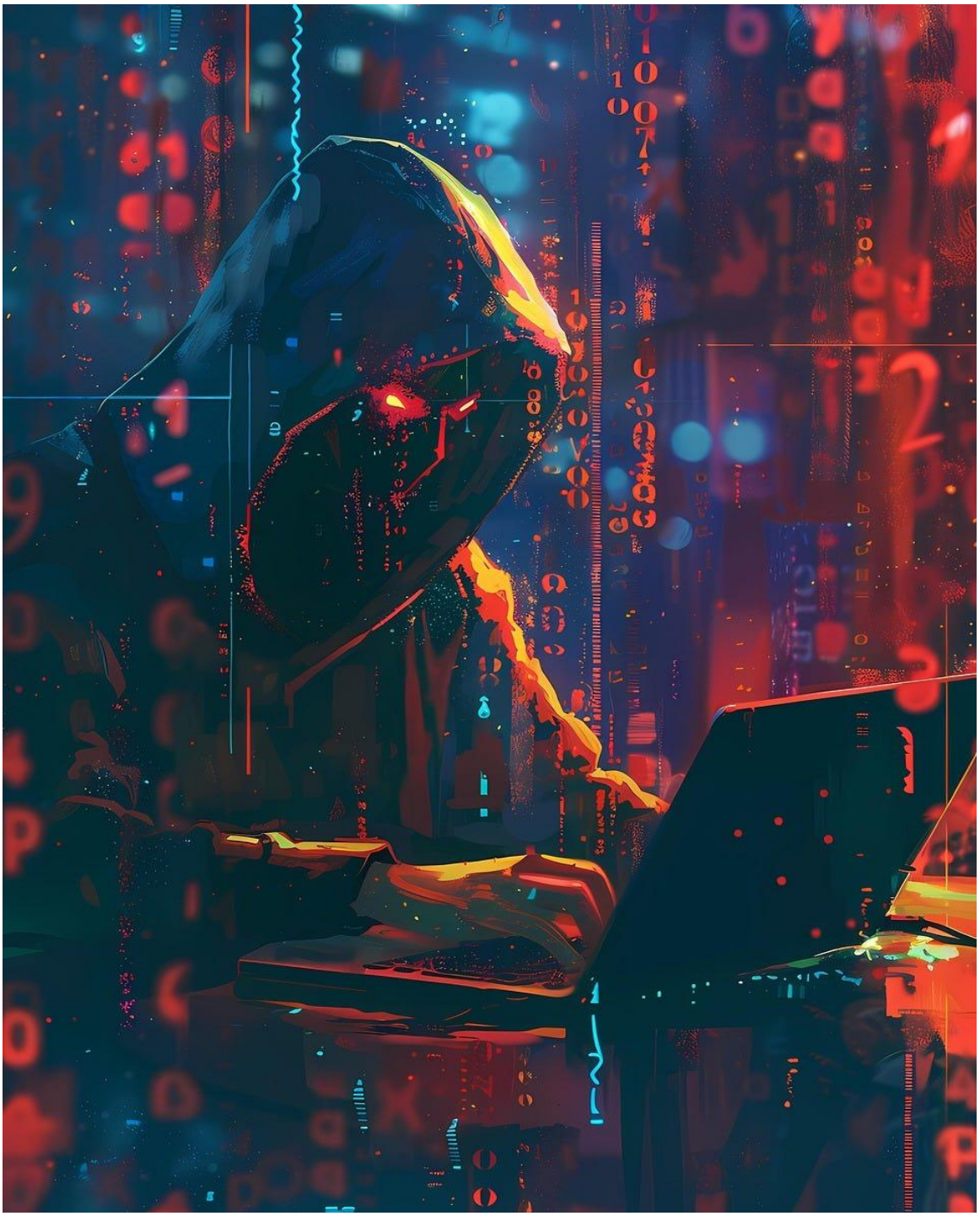
KIRMIZI TAKIM



İÇERİKLER

1- Kırmızı Takım Nedir?

Kurumun, işyerinin hizmet sunduğu sisteme bir black hack gibi düşünerek belirli zamanlarda sistemin açıklarını bulmak ,bunu yetkili kişilere raporlamak ve açıkların kapatılması için aksiyon alınan bir testi gerçekleştiren takıma kırmızı takım diyoruz.

2- Kırmızı Takımın Amacı

Kurumun , işyerinin sadece açıklarını kapatmak değil aynı zamanda , herhangi bir meydana gelecek siber saldırı ve siber savaşa karşı korumakla sorumlu olan ekiptir.

3- Kırmızı ,Mavi ve Mor Takımlar

a)Mavi Takım: Mavi takım, bir kuruluşun güvenlik ekibidir. Siber güvenlik testleri sırasında kuruluşu simüle edilmiş saldırılara karşı korumaktan sorumludur.

b)Kırmızı Takım: bu saldırıları gerçekleştiren saldırı tarafıdır. Kırmızı takımın amacı, bir kuruluşun karşılaşabileceği gerçek dünya tehditlerini doğru bir şekilde simüle etmek ve kuruluşun bunlara karşı savunmasını test etmektir.

c)Mor Takım: Bir kuruluşun güvenlik sistemlerini test etmek ve iyileştirmek için kırmızı takımları ve mavi takımları ile iş birliği yapılır.

Bu iş birliği ile , sürekli bir geri bildirim döngüsü, bilgi aktarımı ve gelişmiş siber saldırı simülasyonları aracılığıyla bir kuruluşun güvenlik sistemini güçlendirmeyi amaçlar.

4- Kırmızı Takım Süreci

Kırmızı takım çalışması :

1. Kırmızı takım alacağı rolü tanımlamak.
2. Hedef üzerinde bilgi toplayıp keşif yapmak.
3. Saldırı yöntemlerini belirlemek.
4. Saldırıya yönelik bir plan oluşturulması.
5. Zafiyet taraması ve sosyal mühendislik gibi yöntemler kullanılarak hedefe yönelik bir dizi kontrollü saldırının gerçekleştirilmesi.

Saldırıların sonucunu BT güvenliğini iyileştirmek için önerilerde bulunmak.

5- Kırmızı Takım Araçları

- Metasploit Framework
- Nmap (Ağ tarama)
- Burp Suite (Web uygulama testi)
- Kali Linux (Pentest işletim sistemi)
- Wireshark ve John the Ripper gibi diğer çeşitli penetrasyon araçlarıdır.

6- Kırmızı Takım Egzersiz Adımları

- Planlama (tatbikatın hedefleri ve bir saldırı durumunda uygulanacak angajman kuralları, test edilecek sistemlerin ve simüle edilecek saldırı türlerinin tanımlanması)
- Keşif (Ağ mimarisi, çalışan bilgileri ve kamuya açık bilgiler . Kırmızı Takım tarafından simüle edilmiş saldırılar için kullanılabilecek zayıf noktaları bulmaya çalışmak içindir.)
- İstismar (Toplanan bilgilerle, kimlik avı, kötü amaçlı yazılım dağıtımı ve hatta ağ sızması gibi çeşitli tekniklerle bulunan güvenlik açığından yararlanmaya çalışır. Sistemlere yetkisiz erişimde bulunur.)
- İstismar Sonrası (Erişim sağlandıktan sonra ekip, ağda yatay hareket, ayrıcalık yükseltme ve veri sızdırma gibi neler başarabileceğini belirler. Bu adım, gerçek bir saldırganın verebileceği hasarı simüle eder ve tam bir görünüm sunar.)
- Raporlama ve Analiz (Tespit edilen zafiyetler, istismar edilen zayıflıklar ve iyileştirme önerileri de dahil olmak üzere ayrıntılı raporlar hazırlanır. Elde edilen bilgilerin somut eylem adımlarına dönüştürülmesini sağlamalıdır.)

7- Kırmızı Takım Tatbikatının Amaçları

1)Güvenlik açıklarını belirleme

2)Olay yanıtını test edin

3)Güvenlik önlemlerini iyileştirin

4) Farkındalığı artırın

5) Uyumluluk ve Denetim

8- Kırmızı Takım İçin Sertifika/Eğitim

a) Temel Seviye Sertifikalar

- CompTIA Security+
- (ISC)2
- SSCP (Systems Security Certified Practitioner)

b) Orta Seviye ve Uzmanlaşma Sertifikaları

- OSCP (Offensive Security Certified Professional)

- CRTP (Certified Red Team Professional)
- CRTE (Certified Red Team Expert)
- eWPT (eLearnSecurity Web Application Penetration Tester)
- PNPT (Practical Network Penetration Tester)

c) İleri Seviye ve Özel Alan Sertifikaları

- OSEP (Offensive Security Experienced Penetration Tester)
- OSWE (Offensive Security Web Expert)
- CEH (Certified Ethical Hacker)
- CFR (CyberSec First Responder)
- GPEN (GIAC Penetration Tester)

9- Kırmızı Takım için Ek Eğitim Alanları ve Beceriler

- Programlama Dilleri
- İşletim Sistemleri Derinlemesine Bilgisi
- Ağ Protokolleri
- Bulut Güvenliği
- Sosyal Mühendislik
- Raporlama ve İletişim

10- Nereden Başlamalıyım Diyorsan

Bu aşağıdakilerden ingilizce bilgisiyle beraber aşağıdaki yolu izlemenizi tavsiye ediyorum.

- Yeni Başlıyanlar: CompTIA Security+, (ISC)2 SSCP.
- Pratik Sızma Testi: OSCP (mutlaka!), eWPT, PNPT.
- Active Directory Uzmanlığı: CRTP, CRTE
- Gelişmiş Saldırı Teknikleri: OSEP, OSWE.

11- SON

- https://www.ibm.com/think/topics/red-teaming
- https://www.securefors.com/read-team-blue-team-nedir-farklari-nelerdir/
- https://www.vaadata.com/blog/what-is-red-teaming-methodology-and-scope-of-a-red-team-operation/
- https://inventiv.com.tr/tr/blog/siber-guvenlikte-kirmizi-ve-mavi-takim-yaklasimlari
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/red-team-careers-skills-jobs/
- https://www.sentinelone.com/cybersecurity-101/services/red-team-exercise-in-cybersecurity/
- https://www.checkpoint.com/cyber-hub/cyber-security/what-is-a-blue-team/
- https://www.picussecurity.com/resource/glossary/what-is-purple-team