BiltekCyber

Bilgi Toplama 101

BiltekCyber

İçerik

BiltekCyber

Bilgi Toplamanın Önemi

Bilgi toplama, siber güvenlik uzmanları için stratejik bir öneme sahiptir. Bu süreç, potansiyel tehditleri belirlemek, zafiyetleri tespit etmek, güvenlik önlemlerini güçlendirmek ve saldırıları önceden tahmin edip engellemek için kullanılır.

BiltekCyber

Neden Bilgi Toplanır?

- **Zafiyet Tespiti**: Bilgi toplama, sistemlerdeki güvenlik açıklarını ve zafiyetleri belirlemek için kullanılır. Bu sayede savunmasız noktaları tespit ederek düzeltme işlemleri yapılabilir.

- **Tehdit İzleme ve Analizi**: Uzmanlar, sürekli olarak ağları ve sistemleri izleyerek potansiyel tehditleri tespit ederler. Bu tehditlerin doğasını anlamak, uygun savunma stratejileri geliştirmek için önemlidir.

- **Güvenlik Stratejisi Oluşturma**: Bilgi toplama, etkili bir güvenlik stratejisinin oluşturulmasına rehberlik eder. Hangi tehditlere karşı hangi önlemlerin alınması gerektiği gibi konularda bilgi toplama süreci kritik bir rol oynar.

BiltekCyber

Bilgi Toplama Yolları

Ağ Taramaları ve Analizleri: Ağ tarama araçları kullanarak sistemlerdeki açık portları, hizmetleri ve potansiyel zafiyetleri tararlar. Bu sayede saldırılara karşı korumasız alanlar tespit edilir.

Zafiyet Taramaları: Otomatik zafiyet tarama araçlarıyla, sistemlerdeki güvenlik açıkları ve zafiyetler taranır. Bu, saldırganların istismar edebileceği zayıf noktaların belirlenmesini sağlar.

BiltekCyber

Bilgi Toplama Yolları

Açık Kaynak İstihbarat (OSINT): Kamuya açık kaynaklardan elde edilen bilgilerle, hedefler ve saldırganlar hakkında bilgi toplanır. Sosyal medya, haber kaynakları ve forumlar gibi yerlerden istihbarat elde edilir.

Sosyal Mühendislik Simülasyonları: Saldırganların kullanabileceği sosyal mühendislik yöntemlerini test etmek amacıyla sahte e-postalar veya telefon aramaları gibi yöntemler kullanılır.

BiltekCyber

Bilgi Toplama Yolları

Kara Liste İncelemeleri: Bilinen kötü amaçlı IP adresleri, alan adları veya dosya hash değerleri gibi kara liste verileri incelenir.

Log ve Günlük Analizleri: Sistem ve ağ günlükleri incelenerek anormal aktiviteler veya potansiyel saldırı göstergeleri araştırılır. Bu, saldırıları önceden tespit etmeye yardımcı olur.

Penetrasyon Testleri: Kontrollü saldırılar düzenleyerek sistemlerin ve ağların zafiyetleri tespit edilir. Bu testler, gerçek dünya saldırı senaryolarını simüle etmeye yardımcı olur.

BiltekCyber

Bilgi Toplama Yolları

Güvenlik Bültenleri ve Raporlarının İzlenmesi: Güvenlik firmalarının yayınladığı güvenlik bültenleri ve raporları takip edilerek yeni tehditler ve zafiyetler hakkında bilgi edinilir.

İçerik Analizleri: Web siteleri ve dosyalar üzerinde yapılan analizlerle zararlı içerik veya kötü amaçlı kodlar tespit edilir.

Eğitim ve Sertifikasyon Programları: Uzmanlar, güncel bilgileri edinmek ve becerilerini geliştirmek için siber güvenlik eğitimleri ve sertifikasyon programlarına katılabilirler.

BiltekCyber

Bilgi Toplama Aşamaları

1

Hedef Belirleme: Uzmanlar, hangi sistemleri, ağları veya organizasyonları inceleyeceklerini belirler. Bu aşamada, hedefin özellikleri ve potansiyel tehlikeleri hakkında fikir sahibi olurlar.

2

Toplama Planı Oluşturma: Bilgi toplama sürecini organize etmek için bir plan oluştururlar. Hangi araçları kullanacakları, hangi yöntemleri izleyecekleri ve ne tür verileri toplayacakları bu aşamada belirlenir.

BiltekCyber

Bilgi Toplama Aşamaları

3 **Veri Toplama**: Uygulama aşamasıdır. Hedef sistemler ve ağlar üzerinde ağ taraması, zafiyet taraması, OSINT araştırmaları ve diğer tekniklerle verileri toplarlar.

4 **Veri Analizi**: Toplanan verileri analiz ederler. Bu aşamada elde edilen bilgileri sınıflandırarak anlamlı bilgileri çıkarmaya çalışırlar.

5 **Tehdit Değerlendirmesi**: Toplanan verileri kullanarak potansiyel tehditleri ve zafiyetleri değerlendirirler. Hangi tehditlerin öncelikli olduğunu ve hangi zafiyetlerin acil müdahale gerektirdiğini belirlerler.

BiltekCyber

Bilgi Toplama Aşamaları

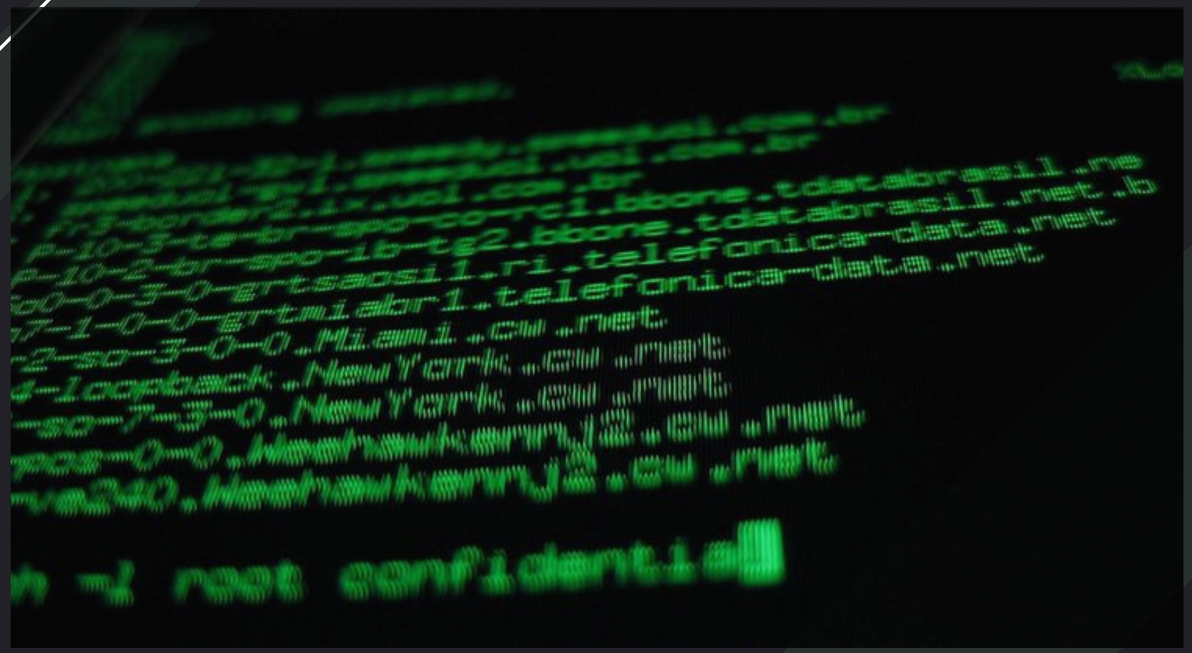
6 **Raporlama**: Analiz sonuçlarını ve bulguları içeren bir rapor hazırlarlar. Bu rapor, organizasyonun yönetimine veya ilgili paydaşlara sunularak alınması gereken önlemleri belirlemelerine yardımcı olur.

7 **Eyleme Geçme**: Raporda önerilen önlemleri uygulamak veya zafiyetleri kapatmak için gerekli adımları atarlar. Bu aşama, organizasyonun güvenliğini artırmak ve potansiyel saldırılara karşı savunmayı güçlendirmek amacıyla gerçekleştirilir.

BiltekCyber

Aktif Bilgi Toplama

BiltekCyber



Aktif Bilgi Toplama Nedir?

Siber güvenlik uzmanları, aktif bilgi toplama işlemi sırasında hedef sistemlere veya ağlara doğrudan etkileşimde bulunarak veri toplarlar. Bu süreç, potansiyel olarak sistemi etkileyebilir ve hedefte tespit edilme riskini artırabilir.

.

BiltekCyber

Aktif Bilgi Toplama Teknikleri

- **Ağ Taraması:** Ağda bulunan cihazları ve açık portları tespit etmek için kullanılır. Bu, hedef ağın topografyasını çıkarmaya yardımcı olur.

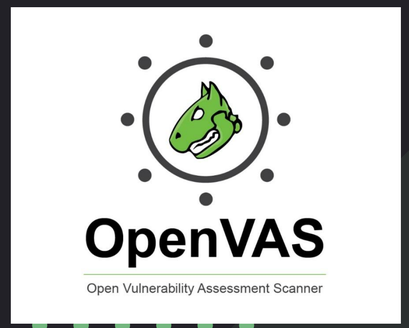
- **Zafiyet Taraması:** Hedef sistemlerdeki güvenlik açıklarını tespit etmek için kullanılır. Bu taramalar, zafiyetleri belirleyerek savunma önlemlerinin güçlendirilmesine yardımcı olur.

- **Penetrasyon Testleri (Pen Test):** Hedef sistemlere saldırı senaryolarını simüle ederek zafiyetleri tespit etmeye çalışır. Bu, zafiyetlerin gerçek dünya saldırılarına karşı nasıl kullanılabileceğini anlamak amacıyla yapılır.

BiltekCyber

Aktif Bilgi Toplama Toolları

Nmap: Ağ taraması ve port taraması yapmak için kullanılır. Hedef ağdaki cihazları ve açık portları tespit etmek amacıyla kullanılır.



OpenVAS: Zafiyet taraması yaparak güvenlik açıklarını tespit etmek için kullanılır.

BiltekCyber

Aktif Bilgi Toplama Toolları

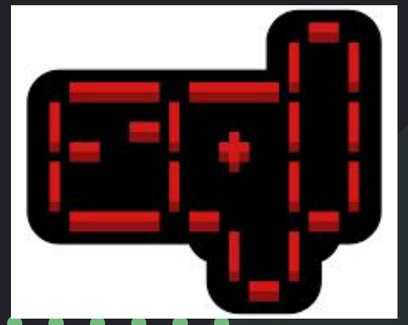
Metasploit: Penetrasyon testleri ve saldırı senaryoları oluşturmak amacıyla kullanılır.

Burp Suite: Web uygulamalarını analiz ederek güvenlik açıkları tespit etmek için kullanılır.

BiltekCyber

Aktif Bilgi Toplama Toolları

Wireshark: Ağ trafiğini izlemek ve analiz etmek için kullanılır.



SQLMap: SQL enjeksiyon zafiyetlerini tespit etmek ve istismar etmek için kullanılır.

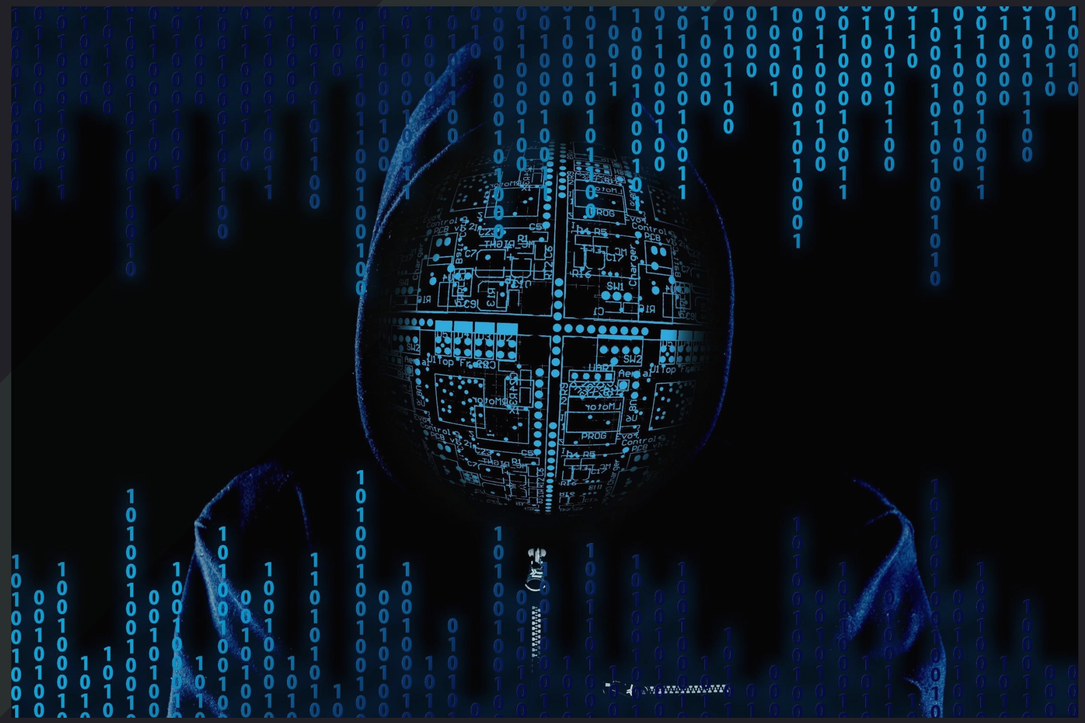
BiltekCyber

Pasif Bilgi Toplama

BiltekCyber

Pasif Bilgi Toplama Nedir?

Pasif bilgi toplama işlemi, aktif bilgi toplama tekniğinin aksine, sırasında hedef sistemlere veya ağlara doğrudan müdahalede bulunmadan veri toplarlar. Böylelikle, hedefte tespit edilme riskini minimize eder.



BiltekCyber

Pasif Bilgi Toplama Teknikleri

- **Açık Kaynak İstihbarat (OSINT):** Kamuya açık kaynaklardan veri toplamak için kullanılır. İnternet üzerindeki sosyal medya profilleri, web siteleri, haber kaynakları gibi bilgiler OSINT aracılığıyla elde edilir.

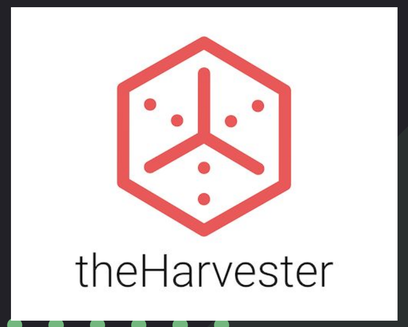
- **Ağ Trafiği İzleme:** Hedef ağın trafiğini izlemek ve analiz etmek amacıyla kullanılır. Bu sayede ağdaki etkinlikler ve iletişimler hakkında bilgi elde edilebilir.

- **Veritabanı Sorgulamaları:** Kamuya açık veritabanlarını sorgulayarak hedefle ilgili bilgiler toplamak için kullanılır.

BiltekCyber

Pasif Bilgi Toplama Toolları

Maltego: OSINT aracı olarak kullanılır. Kamuya açık kaynaklardan bilgi toplamak ve verileri görselleştirmek amacıyla kullanılır.



theHarvester: OSINT aracıdır ve kamuya açık alan adları ve e-postaları toplamak için kullanılır.

BiltekCyber

Pasif Bilgi Toplama Toolları

Shodan: Kamuya açık cihazların ve sistemlerin bilgilerini tarayarak toplamak için kullanılır.

Censys: İnternet üzerindeki cihaz ve sistemlerin bilgilerini toplamak için kullanılır.

BiltekCyber

Bilgi Toplama Çeşitleri

Aktif Bilgi Toplama	Pasif Bilgi Toplama
Doğrudan hedef sistemlere veya ağlara etkileşimde bulunmayı gerektiren bir süreçtir.	Hedef sistemlere veya ağlara doğrudan müdahalede bulunmadan veri toplama sürecidir.
Tarama araçları veya penetrasyon testleri ile gerçekleştirilir.	Açık kaynak istihbarat (OSINT) ve ağ trafiği izleme gibi yöntemlerle gerçekleştirilir.
Hedef sistemlere yönelik potansiyel saldırı girişimleri içerebilir, bu nedenle etik ve yasal sınırlamalara dikkat edilmelidir.	Hedef sistemlere herhangi bir talepte bulunulmaz, dolayısıyla tespit edilme riski daha düşüktür.
Ağ taraması veya zafiyet taraması yapmak bu kategoriye örnek olarak verilebilir.	Kamuya açık veri tabanları veya sosyal medya profilleri üzerinden bilgi toplamak bu kategoriye örnek olarak verilebilir.

BiltekCyber

Kaynakça

1-https://www.cert.org/
2-https://csrc.nist.gov/
3-https://www.sans.org/
4-https://nmap.org/
5-https://www.openvas.org/
6-https://www.metasploit.com/
7-https://portswigger.net/burp
8-https://www.wireshark.org/
9-https://github.com/sqlmapproject/sqlmap
10-https://www.maltego.com/
11-https://github.com/laramies/theHarvester
12-https://www.shodan.io/
13-https://censys.io/

BiltekCyber

Hazırlayan

Adı: Yahya
Soyadı: Çakıcı
Fakülte: Mühendislik ve Doğa Bilimleri Fakültesi
Departman: Yazılım Mühendisliği 2.Sınıf

Linkedin: https://www.linkedin.com/in/yahya-çakıcı-584004256/