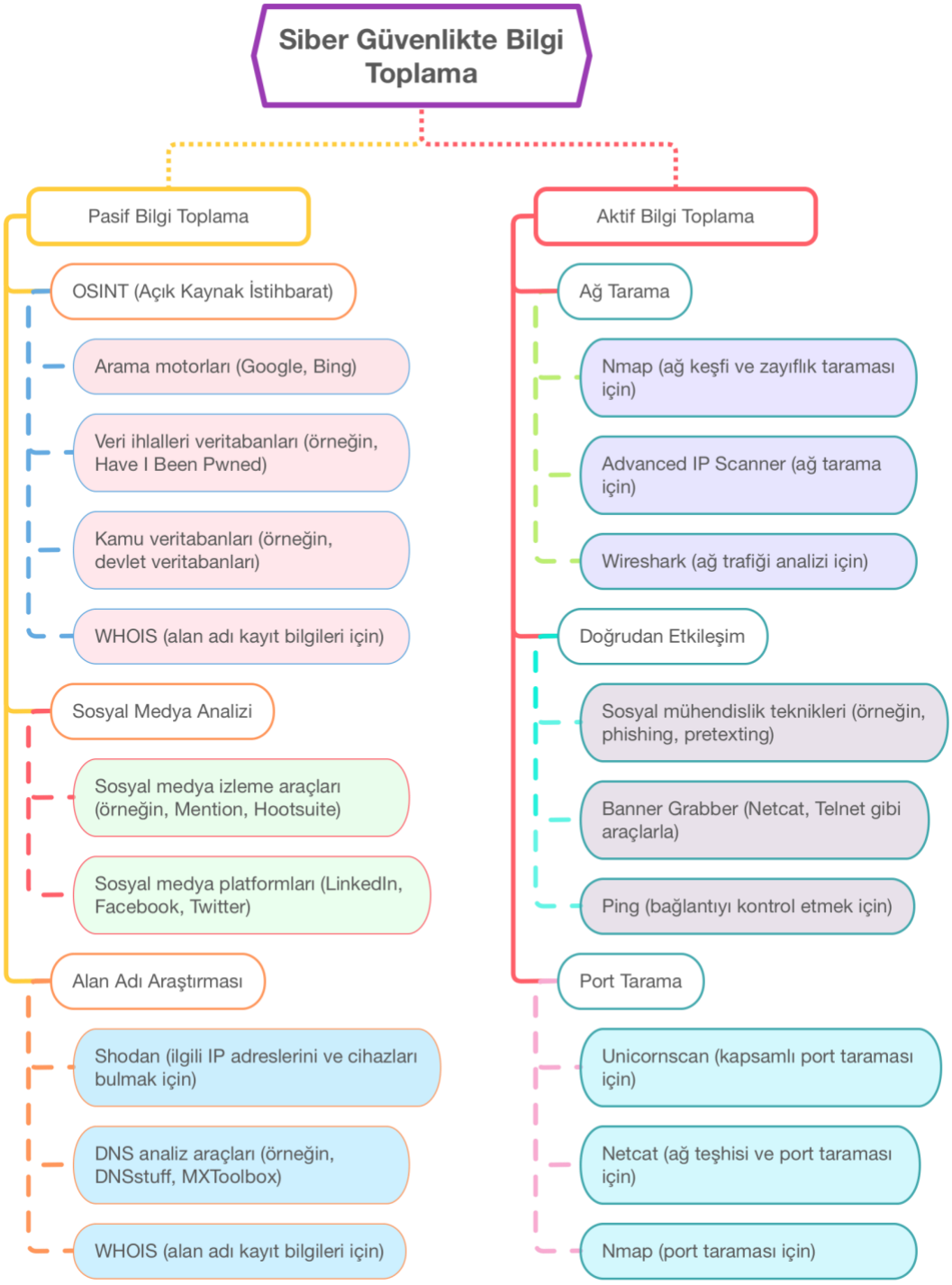
Siber Güvenlikte Bilgi Toplama

Ahsen Beyza Özkul

ahsenbeyza@securedebug.com

CONTENTS

SIBER GÜVENLIKTE BILGI TOPLAMA ZIHIN HARITASI 3
SIBER GÜVENLIKTE BILGI TOPLAMA 4
NEDEN ÖNEMLIDIR? 4
BILGI TOPLAMANIN TÜRLERI 4
TEKNIKLER VE ARAÇLAR 5
ZORLUKLAR VE SINIRLAMALAR 6
VAKA ÇALIŞMALARI / GERÇEK DÜNYA ÖRNEKLERI 6
KAYNAKLAR 7



Siber Güvenlikte Bilgi Toplama Zihin Haritası

Siber Güvenlikte Bilgi Toplama

Siber güvenlikte bilgi toplama, bir hedef hakkında veri toplama ve analiz etme sürecidir. Bu hedef bir bilgisayar ağı, bir web sitesi veya hatta bir birey olabilir. Bu adım, potansiyel zayıflıkları belirlemek ve bu zayıflıkları siber saldırılar için kullanmak ya da güvenlik önlemlerini güçlendirmek için kritik öneme sahiptir. Hem saldırganlar hem de savunucular için temeldir.

Neden Önemlidir?

Bilgi toplamanın önemi, hedef çevresinin net bir şekilde görülmesini sağlamasında yatar. Saldırganlar için zayıf noktaları bulmakla ilgilidir. Savunucular için ise, saldırıların nerelerde gerçekleşebileceğini öngörmek ve bu alanları güçlendirmekle ilgilidir.

1) Proaktif Savunma: Güvenlik ekipleri, toplanan bilgileri potansiyel tehditleri öngörmek ve saldırılar meydana gelmeden önce korumalar kurmak için kullanabilirler.
2) Tehditleri Anlama: Verileri analiz ederek, organizasyonlar karşılaşabilecekleri tehditleri ve bunların sistemleri nasıl etkileyebileceğini daha iyi anlayabilirler.
3) Stratejik Planlama: Hem saldırganlar hem de savunucular bu bilgileri bir sonraki adımlarını planlamak için kullanır. Saldırganlar en kolay giriş yolunu ararken, savunucular boşlukları kapatmaya çalışır.
4) Erken Tespit: Bilgi toplamanın nasıl yapıldığını bilmek, organizasyonların saldırıların erken belirtilerini tespit etmelerine yardımcı olabilir, böylece hızlıca harekete geçerek hasarı minimize edebilirler.

Bilgi Toplamanın Türleri

1) Pasif Bilgi Toplama Pasif bilgi toplama, hedefle doğrudan etkileşime girmeden veri toplamayı ifade eder. Amaç, hedefi uyandırmadan mümkün olduğunca fazla bilgi toplamaktır. Bazı yaygın teknikler şunlardır:

- OSINT (Açık Kaynak İstihbarat): Web siteleri, haber makaleleri, devlet veritabanları ve diğer kaynaklardan halka açık bilgileri toplamak.

- Sosyal Medya Analizi: Sosyal medya profillerini inceleyerek bireyler veya organizasyonlar hakkında bilgi edinmek, çalışanlar, operasyonlar veya güvenlik uygulamaları hakkında bilgi almak.

- Alan Araştırması: Hedefle ilişkili alan adlarını araştırarak, IP adresleri ve alt alan adları gibi altyapı bilgilerini öğrenmek için WHOIS ve DNS sorgulamaları gibi araçları kullanmak.

2) Aktif Bilgi Toplama Aktif bilgi toplama, hedef sistemle doğrudan etkileşime girerek veri toplamayı içerir. Bu yaklaşım daha ayrıntılı bilgi sağlayabilir ancak daha yüksek bir tespit riski taşır. Bazı yaygın yöntemler şunlardır:

- Ağ Tarama: Hedefin ağını taramak için araçlar kullanmak, açık portlar, hizmetler ve zayıflıkları bulmak, bu da saldırganların ağın yapısını ve zayıf noktalarını anlamalarına yardımcı olur.

- Port Tarama: Ağ taramanın özel bir türü olan port tarama, açık portları belirler ve hangi hizmetlerin çalıştığını ve potansiyel olarak saldırılara açık olanları ortaya çıkarır.

- Doğrudan Etkileşim: Ping gönderme, sistem banner'larını çekme veya sosyal mühendislik taktikleri kullanma gibi eylemleri içerir. Bu, ayrıntılı bilgi sağlayabilir ancak hedef tarafından fark edilme olasılığı daha yüksektir.

Teknikler ve Araçlar

1) Keşif Araçları

Keşif araçları, hedef hakkında başlangıç verileri toplamak için önemlidir. Bazı örnekler şunlardır:

- WHOIS: Alan adlarının veya IP adreslerinin kayıtlı kullanıcıları hakkında bilgi sorgulamak için kullanılan bir araç.
- Shodan: İnternete bağlı belirli türdeki cihazları (web kameraları, yönlendiriciler, sunucular gibi) bulmak için kullanılan bir arama motoru.
- Arama Motorları: Google gibi araçlar, hedef hakkında teknik detaylar ve organizasyon bilgileri dahil olmak üzere kamuya açık bilgileri bulmak için yaygın olarak kullanılır.

2) Tarama Araçları

Tarama araçları, aktif bilgi toplama için kullanılır ve hedef sistemdeki zayıflıkları keşfetmeye odaklanır. Örnekler şunlardır:

- Nmap: Bilgisayar ağında ev sahiplerini ve hizmetleri keşfetmeye yardımcı olan bir ağ tarama aracı.
- Nessus: Hedef sistemdeki zayıflıkları, açık portları ve yapılandırma hatalarını belirleyen bir zayıflık tarama aracı.

3) Sosyal Mühendislik

Sosyal mühendislik, insanları gizli bilgileri ifşa etmeye ikna etme yöntemlerini içerir. Bazı teknikler şunlardır:

- Phishing: Güvenilir kaynaklardan geliyormuş gibi görünen sahte e-postalar göndererek kişileri hassas bilgileri ifşa etmeye kandırma.
- Pretexting: Birini bilgi vermeye veya bir eylem gerçekleştirmeye ikna etmek için sahte bir senaryo oluşturma.
- Baiting: Hedefi sistemlerini tehlikeye atmak için fiziksel veya dijital bir yem (örneğin, bir USB bellek) bırakma.

Sosyal mühendislik, insan davranışını teknik kusurlardan daha iyi kullanabildiği için genellikle çok etkili olur. Ancak, bu taktikleri tanıma ve bunlara karşı eğitim arttıkça daha zor hale gelmektedir.

Zorluklar ve Sınırlamalar

Bilgi toplama süreci zorluklarla doludur:

1) Veri Doğruluğu: Toplanan bilgi her zaman doğru veya güncel olmayabilir, bu da tehditlerin değerlendirilmesinde veya savunma stratejilerinin oluşturulmasında hatalara neden olabilir.

2) Gizlilik Endişeleri: Özellikle sosyal medya analizi gibi pasif yöntemlerle bilgi toplamak, hedefin bilgisi veya rızası olmadan veri toplama gibi ciddi gizlilik sorunlarına yol açabilir.

3) Tespit Riskleri: Aktif bilgi toplama sürecinde, tespit edilme riski büyük bir endişedir. Hedef, gözlemlendiğini fark ederse, sistemlerini güvence altına almak veya hatta karşı saldırıya geçmek için önlemler alabilir.

Vaka Çalışmaları / Gerçek Dünya Örnekleri

1) Target Şirketi İhlali (2013): Saldırganlar, Target'ın ağı ve tedarikçileri hakkında bilgi toplamak için keşif yaptı. Bu bilgiyi, Target'ın satış noktası sistemini ihlal etmek için kullandılar ve milyonlarca müşterinin kredi kartı bilgilerini ortaya çıkardılar.
2) Stuxnet Solucanı (2010): İran'ın nükleer programına yönelik bu siber saldırıda, saldırganlar hedefin endüstriyel kontrol sistemleri hakkında kapsamlı bilgi topladılar. Bu bilgi, Uranyum zenginleştirme süreçlerini yıllarca tespit edilmeden hedef alıp bozan bir solucanı tasarlamada kritik rol oynadı.
3) Equifax Veri İhlali (2017): Saldırganlar, Equifax'ın web uygulamasında bilinen bir zayıflığı istismar etti. Bilgi toplama, bu zayıflığı belirlemede ve hassas müşteri verilerine erişimde kritik rol oynadı ve milyonlarca kişiyi etkiledi.

KAYNAKLAR

1) Sagba, B. (2023, 27 Eylül). *Siber güvenlikte bilgi toplama araçları*. Medium. https://medium.com/@blessmartinsagba/information-gathering-tools-in-cybersecurity-e2c20c345e37
2) Bugraptors. (t.y.). *Siber güvenlik testi için bilgi toplama araçları*. Erişim adresi: https://www.bugraptors.com/blog/information-gathering-tools-in-cybersecurity-testing#:~:text=Information%20gathering%20is%20the%20process,%2C%20websites%2C%20or%20even%20individuals
3) Scaler. (t.y.). *Keşif ve bilgi toplama*. Erişim adresi: https://www.scaler.com/topics/cyber-security/reconnaisance-and-information-gathering/
4) Scaler. (2024, 21 Ocak). *Keşif ve bilgi toplama*. Erişim adresi: https://www.scaler.com/topics/cyber-security/reconnaisance-and-information-gathering/