TEMELLER

Rabia EKŞİ

23.02.2025

İçindekiler

GİRİŞ

Siber güvenlik, günümüzde dijital dünyanın hızla büyümesiyle birlikte daha da önemli hale gelmiştir. Teknolojinin gelişmesi, siber tehditlerin çeşitlenmesini ve karmaşıklığını artırmıştır. Bu tehditlerle başa çıkabilmek için güvenlik operasyonları merkezleri (SOC), organizasyonların savunmalarını yönetmek ve siber saldırılara karşı hızlı tepki verebilmek için kritik bir rol oynamaktadır. SOC analistleri, bu merkezlerde tehditleri tespit etmek, analiz etmek, ve saldırılara karşı etkili yanıtlar geliştirmek için uzmanlaşmış profesyonellerdir. Bu yazı, SOC analistlerinin rolü, sorumlulukları, kullandıkları güvenlik ürünleri ve ağ temelleri ile saldırılara karşı savunma yöntemleri hakkında derinlemesine bir inceleme sunacaktır. Aynı zamanda, Cyber Kill Chain ve ağ temellerinin saldırılara nasıl etki ettiği üzerine kapsamlı bilgiler verilecektir.

SOC FUNDAMENTALS

SOC Analisti

Bir **SOC (Security Operations Center) Analisti**, siber güvenlikte önemli bir rol oynayan ve bir kuruluşun Güvenlik Operasyon Merkezi (SOC) ekibinde görev alan uzmandır. Siber tehditleri sürekli olarak izleyerek güvenlik açıklarını belirler ve olası güvenlik olaylarına hızla müdahale eder. SOC analistleri, kuruluşların dijital ortamlarını güvende tutmak için ilk savunma hattı olarak görev yapar.

SOC Analistinin Temel Sorumlulukları

SOC analistleri, kuruluşların dijital varlıklarını korumak için birçok farklı görev üstlenir. SOC analistlerinin günlük olarak yürüttüğü temel görevler:

- **Security Monitoring**: SOC analistleri, ağ trafiğini, sistem günlüklerini ve diğer güvenlik araçlarını sürekli olarak takip ederek olağan dışı veya şüpheli etkinlikleri tespit eder. Bu sayede potansiyel ihlallere veya güvenlik açıklarına erken müdahale edebilirler.
- **Incident Detection**: Siber tehditleri belirleyerek kötü amaçlı yazılım bulaşmaları, veri ihlalleri ve içeriden gelen tehditler gibi güvenlik olaylarını sınıflandırır ve bunlara hızlı bir şekilde yanıt verilmesini sağlarlar.
- **Incident Response**: Bir güvenlik ihlali gerçekleştiğinde, SOC analistleri tehditleri analiz ederek hızlı bir şekilde etkisini sınırlar ve zararı en aza indirir. Bu süreç; etkilenen sistemlerin izole edilmesini, kötü amaçlı yazılımın kaldırılmasını ve diğer ekiplerle koordineli çalışmayı içerebilir.
- **Alarm Değerlendirme**: Güvenlik araçları tarafından üretilen uyarıları inceleyerek hangi olayların daha kritik olduğunu belirlerler. Böylece en önemli tehditlere öncelikli olarak müdahale edilir.
- **Threat Intelligence**: SOC analistleri, en güncel siber tehditler, güvenlik açıkları ve saldırı teknikleri hakkında bilgi sahibi olmalıdır. Yeni tehditlere karşı daha etkili savunmalar geliştirmek için tehdit istihbaratını sürekli olarak izler ve analiz ederler.
- **Log Analizi**: Güvenlik duvarları, saldırı tespit ve önleme sistemleri (IDS/IPS) ve antivirüs yazılımlarından gelen log kayıtlarını inceleyerek anormal aktiviteleri tespit ederler.

- Security Tool Management: SOC analistleri, **SIEM (Security Information and Event Management)**, **IDS/IPS (Intrusion Detection/Prevention Systems)** ve uç nokta güvenliği çözümleri gibi güvenlik teknolojilerini yönetir ve bunların etkin şekilde çalışmasını sağlar.

  Sonuç olarak SOC analistleri, siber güvenlik dünyasında kuruluşları tehditlerden koruyan kritik uzmanlardır. Güvenlik izleme, olay tespiti ve müdahale gibi görevleri yerine getirerek şirketlerin sistemlerini güvende tutarlar. Tehdit istihbaratı, güvenlik araçlarının yönetimi ve uyumluluk gibi konularda sürekli çalışarak siber saldırılara karşı güçlü bir savunma oluştururlar.

Bir SOC Analistinin Sahip Olması Gereken Temel Beceriler

Bir SOC analisti olarak başarılı olmak için teknik bilgi ile esnek becerilerin dengeli bir şekilde harmanlanması gerekir. SOC analistlerinin başarılı olmasını sağlayan en önemli yetkinlikler:

- Bilgi teknolojileri konusunda sağlam bir temel bilgiye sahip olmak kritik öneme sahiptir. Özellikle **işletim sistemleri, ağ protokolleri ve güvenlik araçları** hakkında güçlü bir anlayışa sahip olmak, siber tehditlere karşı her zaman bir adım önde olmayı sağlar.
- SOC analistleri, **SIEM (Security Information and Event Management) sistemleri, IDS/IPS (Intrusion Detection/Prevention Systems), güvenlik duvarları (firewall), antivirüs yazılımları ve uç nokta tespit sistemleri (EDR/XDR)** gibi araçlarla sürekli olarak çalışır. Bu araçları etkin bir şekilde kullanmak, tehditleri hızlı bir şekilde tespit edip yönetmek açısından kritik öneme sahiptir.
- **Python, PowerShell** gibi programlama dillerine hakim olmak büyük bir avantajdır. SOC analistleri, tekrar eden görevleri otomatikleştirmek, özel betikler (scriptler) oluşturmak ve hatta güvenlik analizlerini daha verimli hale getirmek için kendi araçlarını geliştirebilir.
- Bir güvenlik olayını araştırırken, **kanıtları koruma, veri kurtarma ve dijital izleri analiz etme** gibi adli bilişim temel prensiplerini bilmek önemlidir.
- Sistem günlükleri (log'lar), birçok değerli bilgiyi içerir. SOC analistleri, güvenlik duvarları, IDS/IPS ve diğer güvenlik araçlarından gelen log kayıtlarını inceleyerek anormallikleri ve tehditleri tespit eder.
- Bir güvenlik ihlali gerçekleştiğinde, **hızlı ve etkili bir müdahale süreci yürütmek** gerekir. SOC analistleri, tehditleri **izole etmek, ortadan kaldırmak ve sistemleri kurtarmak** için olay müdahale ekipleriyle koordineli bir şekilde çalışır.
- Siber saldırganların **MITRE ATT&CK gibi çerçevelerde tanımlanan saldırı zincirlerini ve tekniklerini** nasıl kullandığını bilmek, tehditleri öngörmek ve önlem almak için büyük bir avantaj sağlar.
- Siber güvenlik dünyası sürekli değişmektedir. SOC analistleri, **yeni tehditleri, güvenlik açıklarını ve saldırı tekniklerini takip ederek** sistemleri koruma konusunda güncel kalmalıdır.
- SOC analistleri, tespit ettikleri güvenlik olaylarını diğer ekiplerle paylaşmalı ve alınması gereken önlemleri açık bir şekilde anlatabilmelidir. **Net ve anlaşılır bir iletişim**, güvenlik operasyonlarının verimli yürütülmesini sağlar.

- SOC analistleri, olay müdahale ekipleri, tehdit avcıları (threat hunters) ve güvenlik mühendisleri ile birlikte çalışarak tehditlere karşı kolektif bir savunma oluşturur. **İş birliği içinde çalışabilme yeteneği**, bu rolde başarının anahtarıdır.

  Sonuç olarak bir SOC analisti, teknik bilgi, analitik düşünme ve takım çalışması gibi yetkinlikleri bir araya getirerek kuruluşun siber güvenlik savunmasını güçlendirir. **Saldırıları tespit etmek, olaylara müdahale etmek ve güvenliği sürekli iyileştirmek**, başarılı bir SOC analistinin temel görevleri arasındadır. Gelişen tehditlere karşı etkili bir savunma oluşturmak için güncel kalmak ve sürekli öğrenmeye açık olmak büyük önem taşır.

SOC Analistinin Rolleri

Güvenlik Operasyon Merkezi (SOC), analistlerini farklı seviyelere (tier) ayırarak siber güvenlik operasyonlarını daha verimli bir şekilde yönetir.

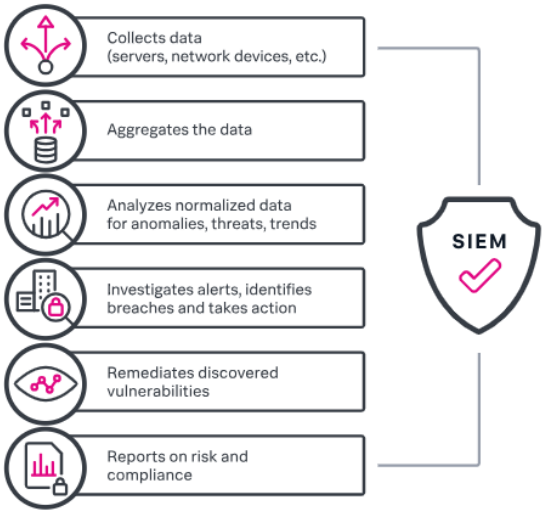
- **Tier 1 SOC Analisti:** Bu seviyedeki güvenlik analistleri, günlük güvenlik olaylarını izlemekten ve güvenlik uyarılarını değerlendirmekten sorumludur. **SIEM (Security Information and Event Management) sistemleri tarafından üretilen alarmları** inceleyerek, olayların önem derecesini ve aciliyetini belirlerler.
- **Tier 2 SOC Analisti:** Tier 2 analistleri, **Tier 1 analistlerinden gelen olayları daha derinlemesine analiz eder ve en uygun müdahale yöntemini belirler**. Bir saldırının ne kadar geniş çaplı olduğunu değerlendirerek, gerekli kurtarma prosedürlerini başlatırlar.
- **Tier 3 SOC Analisti:** Bu seviye, **tehdit avcılığı (threat hunting) ve proaktif güvenlik önlemleri** üzerine yoğunlaşır. Tier 3 analistleri, yeni saldırı tekniklerini araştırır, güvenlik açıklarını keşfeder ve gelişmekte olan tehditlere karşı yenilikçi çözümler üretir.
- **SOC Yöneticisi (SOC Manager):** SOC yöneticileri, güvenlik olaylarının nasıl ele alınacağına karar verir ve müdahale süreçlerini koordine eder. **Ciddi güvenlik olaylarında organizasyon içi ve dışı paydaşlara gerekli bilgileri aktarmakla da sorumludurlar**.

Kullanılan Güvenlik Ürünleri

Herhangi bir güvenlik analizi yapabilmek için öncelikle ilgili bilgilere ulaşmak gereklidir. **Loglar**, ağınızda gerçekleşen çeşitli aktiviteler hakkında en iyi bilgi kaynağıdır. Ancak, ağ boyunca birçok cihaz tarafından her gün milyonlarca log üretilmektedir. Bunları manuel olarak incelemek, etkisiz ya da neredeyse imkansızdır. **Bir log yönetim aracı**, log toplama, çözümleme ve analiz sürecini otomatikleştirebilir. Bu tür araçlar genellikle bir **SIEM** çözümünün parçası olarak kullanılır.

- Güvenlik Bilgisi ve Olay Yönetimi (SIEM)

SOC'nin temel yapı taşlarından biri olan **SIEM aracı**, organizasyonun ağındaki logların toplanmasını sağlar ve bu verileri anormal davranışları tespit etmek için analiz eder. **SIEM platformu**, heterojen kaynaklardan toplanan log verilerini bir araya getirir, analiz eder ve bir tehdit tespit edilirse hızlıca alarm verir.



Şekil 1 SIEM kullanım amacı

Güvenlikle ilgili bilgiler, SOC ekibine **interaktif bir kontrol panelinde grafiksel raporlar** şeklinde sunulur. Bu raporlar sayesinde SOC ekibi, tehditleri ve saldırı desenlerini hızlıca inceleyebilir ve log trendlerinden çeşitli içgörüler elde edebilir. Bir güvenlik olayı meydana geldiğinde ise, SOC ekibi **log adli analizini** kullanarak ihlalin kök nedenini bulabilir. Log verilerine derinlemesine inerek herhangi bir güvenlik olayını daha ayrıntılı bir şekilde inceleyebilirler.

- Endpoint Tespiti ve Yanıt (EDR)

EDR teknolojisi, genellikle uç noktalara (endpoint) ya da hostlara yönelik tehditleri araştırmaya odaklanan araçlar olarak tanımlanır. **EDR araçları**, SOC ekibine, **perimeter savunmalarını kolayca aşabilecek tehditlere karşı ön savunma** işlevi görerek yardımcı olur.

EDR araçlarının temel işlevleri şunlardır:

- Güvenlik tehditlerini tespit etmek
- Tehditleri uç noktada sınırlamak
- Tehditleri araştırmak
- Tehdit yayılmadan önce önlemek

EDR araçları, farklı uç noktaları sürekli izler, bu uç noktalardan veri toplar ve bu verileri şüpheli aktiviteler ve saldırı desenlerini analiz etmek için kullanır. Bir tehdit tespit edildiğinde, EDR aracı tehditleri sınırlayacak ve güvenlik ekibini hemen uyaracaktır. Ayrıca, EDR araçları **siber tehdit istihbaratı**, **tehdit avcılığı** ve **davranış analizleri** ile entegre edilebilir, böylece kötü niyetli aktivitelerin daha hızlı tespit edilmesi sağlanır.

- SOAR (Security Orchestration, Automation, and Response)

SOAR, güvenlik operasyonlarının hızla ve verimli bir şekilde yönetilmesine yardımcı olan bir platformdur. **Güvenlik Orkestrasyonu**, **Otomasyonu** ve **Yanıtı** içerir. Bu araç, SOC ekiplerinin **güvenlik olaylarına müdahale etme sürecini hızlandırarak**, **insan hatasını azaltır** ve **yanıt süresini kısaltır**. SOAR çözümleri, farklı güvenlik araçlarını entegre eder, olayları analiz eder ve otomatikleştirilen yanıtları tetikler.

Özellikleri ve Kullanım Alanları:

- **Otomatik Yanıt:** SOAR, güvenlik olaylarına otomatik yanıtlar vererek, tekrarlanan manuel görevlerin yerine geçer. Bu, SOC ekiplerinin önemli tehditlere odaklanmasını sağlar.
- **Orkestrasyon:** Farklı güvenlik araçları arasında iletişimi sağlar, böylece farklı sistemler arasında bilgi akışı hızlanır ve uyumluluk artar.
- **Hızlı Müdahale:** SOAR platformu, güvenlik ihlallerine hızla yanıt verilmesini sağlayarak, potansiyel zararları minimuma indirir.
- **İşlem İzleme:** Tüm güvenlik olayları ve yanıtları kaydeder, böylece geçmişteki olaylar analiz edilebilir ve sürekli iyileştirme sağlanabilir.

SOAR, güvenlik süreçlerini modernize eder ve organizasyonları daha **proaktif hale getirir**, böylece gelişen tehditlere karşı daha hızlı ve etkili bir şekilde savunma yapılabilir.

- IDS (Intrusion Detection System)

IDS, bir ağda veya sistemdeki potansiyel tehditleri tespit etmeye yönelik bir güvenlik teknolojisidir. **Saldırı Tespit Sistemi**, ağdaki ve sistemdeki anormal aktiviteleri izler ve potansiyel güvenlik ihlalleri hakkında uyarılar gönderir.

Özellikleri ve Kullanım Alanları:

- **Anomali Tespiti:** IDS, ağ trafiğinde veya sistemdeki olağan dışı aktiviteleri algılar. Örneğin, şüpheli bir IP adresinden gelen yüksek trafik gibi.
- **İhlal Bildirimleri:** Tespit edilen tehditler hakkında anında uyarılar oluşturur. Bu uyarılar, güvenlik ekibinin müdahale etmesi için kritik bilgi sağlar.
- **Veri Yükü Tespiti:** IDS, zararlı yazılımlar veya kötü amaçlı yazılımlar gibi tehditlerin ağda yayılmasını tespit edebilir.

IDS, sadece bir **gözlem aracıdır**; tehditleri tespit eder fakat müdahale etmez. Bu nedenle, genellikle **IPS** (Intrusion Prevention System) veya diğer güvenlik önlemleri ile birlikte kullanılır.

- IPS (Intrusion Prevention System)

IPS, saldırıları **engelleyen** bir güvenlik teknolojisidir. **Saldırı Önleme Sistemi**, IDS'nin aksine, tespit edilen tehditlere karşı **aktif bir yanıt verir** ve saldırıları **engeller**. IPS, ağdaki veya sistemdeki şüpheli aktiviteleri izler ve doğrudan müdahale ederek zararın önlenmesini sağlar.

Özellikleri ve Kullanım Alanları:

- **Saldırı Engelleme:** IPS, tespit edilen tehditlere karşı doğrudan müdahale ederek, saldırıları engeller. Örneğin, kötü niyetli trafik akışını kesebilir.
- **Proaktif Savunma:** IPS, ağda bulunan potansiyel tehditleri önceden tespit ederek, saldırıların başarılı olmasını engeller.

- **Etkili Güvenlik:** IPS, anında tepki vererek ağdaki zararlı aktivitelerin yayılmasını engeller ve **ağ performansını korur**.

IPS, genellikle **IDS ile birlikte** kullanılır ve daha **aktif bir güvenlik katmanı** sağlar. Bu sayede potansiyel tehditler yalnızca tespit edilmekle kalmaz, aynı zamanda anında engellenir.

Bu araçlar, güvenlik operasyonlarının temel bileşenleri olup, SOC analistleri için kritik öneme sahiptir. Her birinin kendi işlevi vardır ve birlikte çalışarak daha güçlü ve etkili bir siber güvenlik savunma sistemi oluştururlar.

CYBER KILL CHAIN

Cyber Kill Chain, saldırı sürecini sistematik bir şekilde analiz etmek ve tehditlere karşı önlem almak için kullanılan güçlü bir çerçevedir. İlk kez Lockheed Martin tarafından geliştirilen bu model, bir siber saldırının adım adım nasıl gerçekleştirildiğini ortaya koyarak güvenlik uzmanlarına tehditleri daha iyi anlama ve yanıt verme imkânı sunar. Cyber Kill Chain modeli, bir saldırının yedi temel aşamadan oluştuğunu varsayar: Reconnaissance (Keşif), Weaponization (Silahlandırma), Delivery (Teslimat), Exploitation (Kötüye Kullanım), Installation (Kurulum), Command and Control (Komuta ve Kontrol), ve Actions on Objectives (Hedefteki Eylemler). Bu aşamalar, saldırganın hedefi belirlemesinden nihai amacına ulaşmasına kadar olan tüm süreci kapsamaktadır. Modelin temel amacı, her aşamada saldırıyı durdurabilecek noktaları tespit etmek ve savunma mekanizmalarını bu doğrultuda geliştirmektir. Cyber Kill Chain'in sunduğu en önemli avantajlardan biri, saldırganın hareketlerini ve motivasyonlarını anlamaya yardımcı olmasıdır. Bu anlayış, güvenlik ekiplerinin sadece mevcut tehditlere karşı değil, aynı zamanda gelecekteki potansiyel tehditlere karşı da hazırlıklı olmalarını sağlar. Örneğin, bir saldırgan Recon aşamasında hedef ağ hakkında bilgi toplarken bu faaliyetleri tespit etmek, saldırının diğer aşamalara ilerlemesini engelleyebilir.

Tablo 1 Cyber Kill Chain

Aşama	Açıklama
Reconnaissance	Saldırganların hedef sistem hakkında bilgi topladığı aşamadır. Hedef ağın yapısı, açık portlar, servisler ve zafiyetler analiz edilir.
Weaponization	Saldırganların, hedef sistem üzerinde kullanılacak zararlı yükleri oluşturduğu aşamadır. Genellikle exploit kitleri, zararlı yazılım ve araçlar hazırlanır.
Delivery	Zararlı yükün hedef sisteme ulaştırıldığı aşamadır. Bu genellikle phishing e-postaları, ağ üzerinden dosya transferi veya kötüye kullanılan açıklarla yapılır.
Exploitation	Saldırganların, zararlı yükü hedef sistemde çalıştırarak sistem üzerindeki açıkları kullandığı aşamadır.
Installation	Zararlı yazılımın sisteme kurulduğu ve kalıcılık sağlamak için yöntemlerin kullanıldığı aşamadır.
Command & Control	Saldırganların hedef sistemle iletişim kurduğu ve kontrolü sağladığı aşamadır. Bu genellikle C2 (Command & Control) sunucuları ile gerçekleştirilir.
Actions on Objectives	Saldırının nihai hedefinin gerçekleştirildiği aşamadır. Dosya şifreleme, veri çalma, hizmet kesintisi yaratma gibi sonuçlar içerir.

Cyber Kill Chain Örnek Saldırı Senaryosu

Bu senaryoda tehdit aktörleri, MSSQL sunucusunun “sa” (System Administrator) hesabını brute-force saldırısıyla ele geçirmiş ve sistemde yerleşik bir özellik olan “xp_cmdshell”'i etkinleştirmiştir. Bu özellik, sysadmin yetkisine sahip kullanıcıların sunucuda komut satırı komutları çalıştırmasına izin verir. Saldırganlar bu özelliği kullanarak ilk olarak bir PowerShell komutu çalıştırmış ve Base64 ile kodlanmış bu komut sayesinde Cobalt Strike Komuta ve Kontrol (C2) sunucusuna bir bağlantı kurmuştur.

Bağlantının kurulmasının ardından, winlogon gibi meşru bir sürece enjeksiyon gerçekleştirilmiş ve bu süreç üzerinden PowerShell ve cmd çalıştırılarak ağdaki diğer sistemlere yönelik SMB taramaları yapılmıştır. Aynı zamanda, Tor2Mine madencilik yazılımını bir stager sunucusundan indiren PowerShell komutları yürütülmüştür. Bu komutlar, AV çözümlerinin devre dışı bırakılmasını, sistemde bir Monero madencisi olan Tor2Mine’ın yüklenmesini ve saldırının kalıcılığını sağlamak amacıyla görev zamanlayıcıları ve servisler oluşturulmasını sağlamıştır.

Saldırının ilk 30 dakikası içinde, tehdit aktörleri yan ağlara ve etki alanı denetleyicilerine doğru yatay hareket yapmış, benzer PowerShell komutlarıyla Tor2Mine zararlısını bu sistemlere de yaymıştır. Yaklaşık 32 dakika sonra, BlueSky fidye yazılımı tüm ağda dağıtılarak cihazların şifrelenmesi sağlanmıştır. Bu hızlı ve koordineli saldırı, MSSQL sunucularının yeterli güvenlik önlemleri olmadan internete açık bırakılmasının ne denli ciddi sonuçlar doğurabileceğini göstermektedir.

Reconnaissance (Keşif)

Bu aşamada saldırganlar, hedef sistem hakkında bilgi toplamak için genel tarama ve keşif işlemleri gerçekleştirdi. DCE/RPC çağrıları, ağ profilini anlamak için kullanıldı. Ayrıca, port 445 üzerinden SMB protokolü aracılığıyla iletişim denemeleri yapıldı.

Ağ profilini belirlemek için PowerShell tabanlı Invoke-SMBExec komutları kullanıldı. Bu komutlar, ağdaki SMB protokolü üzerinden çeşitli uç noktalara DCE/RPC çağrıları yaptı. Saldırganların ana hedefi, ağ haritasını çıkararak potansiyel hedef makineleri belirlemekti.

MSSQL sunucularına beklenmedik bir şekilde 1433/TCP portundan yoğun trafik tespit edilirse IDS uyarısı tetiklenmeli.

Weaponization (Silahlandırma)

Saldırganlar, özel hazırlanmış zararlı PowerShell betikleri ve yürütülebilir dosyalar (örn. java.exe, vmware.exe) oluşturdu. Bu dosyalar, çeşitli savunma mekanizmalarını atlatmak ve hedef sistemde kalıcılığı sağlamak üzere tasarlandı.

Zararlı dosyalar PowerShell üzerinden indirilip çalıştırıldı. java.exe, WinRing0x64.sys gibi sürücüler, AV atlatma ve sistem araçlarını devre dışı bırakma işlemlerinde kullanıldı.

Delivery (Dağıtım)

Zararlı yazılımlar ve betikler hedef sistemlere indirildi. Bu işlem sırasında HTTP tabanlı indirme komutları ve Base64 şifrelenmiş PowerShell betikleri kullanıldı.

Zararlı yazılımlar hxxp://83.97.20.81 gibi komuta kontrol sunucularından indirildi. PowerShell komutları, zararlı yazılımları indirip çalıştırmak için Invoke-Expression ve DownloadString yöntemlerini kullandı.

Exploitation (İstismar)

Hedef sistemlerde AV koruma mekanizmaları devre dışı bırakıldı. Sistem hizmetlerine kod enjeksiyonu yapılarak zararlı yazılım yürütüldü.

Set-MpPreference komutları ve kayıt defteri değişiklikleriyle AV koruması etkisiz hale getirildi. Ardından, CreateRemoteThread API'si kullanılarak süreçlere zararlı kod enjekte edildi.

Installation (Kurulum)

Zararlı yazılımlar ve sürücüler hedef sistemlere kalıcı olarak kuruldu. WinRing0 sürücüsü, madencilik işlemlerinde kullanıldı.

WinRing0x64.sys sürücüsü, CPU madenciliği için yüklendi. schtasks komutlarıyla sistemde yeni görevler tanımlandı.

Command & Control (Komuta ve Kontrol)

Sistem, saldırganın kontrolündeki C2 sunucularına bağlandı ve komutlar aldı. HTTPS üzerinden şifrelenmiş trafik kullanıldı.

C2 sunucularından (örn. 83.97.20.81, 5.188.86.237) zararlı dosyalar ve komutlar alındı. Trafik genellikle Base64 şifrelenmiş PowerShell komutları içeriyordu.

Actions on Objectives (Hedeflerdeki Faaliyetler)

Saldırgan, sistemdeki verileri şifreledi ve fidye notları bıraktı. BlueSky adlı fidye yazılımı kullanıldı.

vmware.exe adlı zararlı yazılım kullanılarak veriler şifrelenip .bluesky uzantılı hale getirildi. Sisteme fidye notları bırakılarak talimatlar verildi.

AĞ TEMELLERİ VE SALDIRILARI

Günümüzde ağ güvenliği, bir organizasyonun dijital varlıklarını korumak için kritik bir alan olmuştur. Ağın işleyişini ve potansiyel tehditlerini anlamak, hem ağ yöneticileri hem de

güvenlik uzmanları için büyük önem taşır. Ağ temelleri, ağ topolojileri, IP adresleme, TCP/IP protokollerinin işleyişi, OSI modelinin katmanları ve ağ tabanlı saldırılar hakkında bilinçli olmak, etkili bir güvenlik stratejisi oluşturmanın ilk adımlarındandır.

Ağ Topolojileri ve Yapıları

Ağ topolojileri, ağdaki cihazların birbirleriyle nasıl bağlandığını ve birbirleriyle nasıl iletişim kurduğunu belirleyen yapılandırmalardır. Ağ topolojisinin doğru bir şekilde tasarlanması, ağın verimli çalışmasını ve olası bir saldırıya karşı dayanıklılığını doğrudan etkiler. En yaygın ağ topolojileri şunlardır:

- **Yıldız Topolojisi:** Cihazlar merkezi bir anahtar ya da yönlendiriciye bağlanır. Bu topoloji genellikle ev ve ofis ağlarında kullanılır.
- **Halka Topolojisi:** Cihazlar birbirlerine sırayla bağlanır ve her cihaz veri paketini bir sonraki cihaza ileterek döngü oluşturur.
- **Ağaç Topolojisi:** Yıldız ve halka topolojilerinin birleşimi olup, büyük ağlar için uygundur.

Doğru ağ topolojisinin seçilmesi, ağın güvenliğini doğrudan etkileyebilir. Örneğin, yıldız topolojisi, merkezi bir cihazın hedef alınması durumunda ağın tamamının etkilenmesine yol açarken, ağaç topolojisi daha esnek bir yapıya sahiptir.

IP Adresleme, Subnetting ve CIDR

IP adresleme, her ağ cihazına benzersiz bir kimlik atanmasını sağlar ve ağlar arasında veri iletimini mümkün kılar. IP adresleri iki temel kategoride sınıflandırılır: **IPv4** ve **IPv6**. IPv4, daha yaygın olarak kullanılan ve sınırlı sayıda adresi barındıran 32 bitlik bir adresleme sistemine sahiptir. IPv6 ise daha büyük bir adres alanı sağlayan 128 bitlik bir sistemdir.

Ağlarda daha verimli IP adresi kullanımı sağlamak amacıyla **alt ağ oluşturma** (subnetting) yapılır. Alt ağ oluşturma, büyük bir ağın daha küçük ağlara bölünmesini sağlar. Böylece ağ trafiği daha yönetilebilir hale gelir ve ağ güvenliği artırılır. **CIDR** (Classless Inter-Domain Routing) ise, IP adreslerinin esnek bir şekilde gruplandırılmasını sağlayan bir yöntemdir. CIDR, IP adres bloğunun boyutunu belirlerken sınıf tabanlı ağ adresleme yerine daha verimli bir adresleme sağlar.

TCP/IP Protokol Ailesi ve Temel Protokoller

TCP/IP (Transmission Control Protocol/Internet Protocol), internet üzerindeki cihazlar arasındaki iletişimi yöneten temel protokoller bütünüdür. Bu protokol ailesi, ağ iletişimi için kritik olan birçok temel bileşenden oluşur. Bazı önemli protokoller şunlardır:

- **HTTP (HyperText Transfer Protocol):** Web sayfalarının istemci ve sunucu arasında iletilmesini sağlayan bir protokoldür.
- **HTTPS (HyperText Transfer Protocol Secure):** HTTP'nin güvenli versiyonudur ve verilerin şifreli bir şekilde iletilmesini sağlar.

- **DNS (Domain Name System):** Alan adı sisteminin bir parçasıdır ve IP adreslerini alan adlarına dönüştürerek kullanıcıların internet üzerinde doğru kaynaklara ulaşmasını sağlar.
- **ARP (Address Resolution Protocol):** IP adreslerini MAC adreslerine çevirerek, cihazlar arasındaki veri iletimini sağlamak için kullanılır.
- **ICMP (Internet Control Message Protocol):** Ağdaki cihazlar arasındaki iletişimi denetleyen ve hata mesajları ileten bir protokoldür.

Bu protokoller ağdaki cihazların birbiriyle doğru ve güvenli bir şekilde iletişim kurmasını sağlar. Ancak, bazı saldırılar bu protokoller üzerinden gerçekleştirilebilir. Örneğin, ARP spoofing saldırıları, ARP protokolünün yanlışlıkla kötü niyetli bir şekilde kullanılmasıyla yapılır.

OSI Modeli ve Katmanları

Ağ iletişimi, **OSI (Open Systems Interconnection) modeli** aracılığıyla tanımlanır. OSI modeli, ağdaki iletişimi 7 katmana ayırır ve her katman farklı işlevleri yerine getirir. Bu katmanlar sırasıyla:

- **Fiziksel Katman:** Fiziksel cihazlar ve bağlantıları içerir (kablolar, donanımlar vb.).
- **Veri Bağlantı Katmanı:** Veri iletiminin güvenli ve hatasız olmasını sağlar (Ethernet).
- **Ağ Katmanı:** Paketlerin yönlendirilmesi ve IP adreslemesi gibi görevleri üstlenir.
- **Transport Katmanı:** Verinin güvenli bir şekilde taşınmasını sağlar (TCP, UDP).
- **Oturum Katmanı:** Uygulamalar arasında oturumlar açar ve yönetir.
- **Sunum Katmanı:** Veri biçimlerinin uyumlu olmasını sağlar (şifreleme, sıkıştırma).
- **Uygulama Katmanı:** Kullanıcılarla etkileşime giren uygulamalar ve servisler (HTTP, FTP).

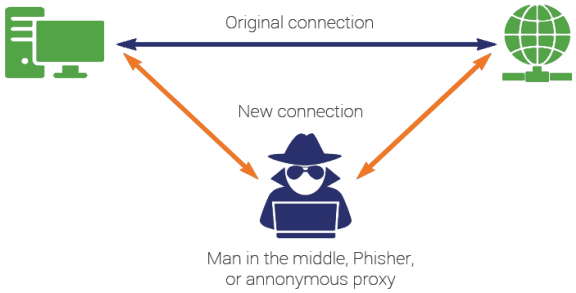
OSI modeli, ağ iletişiminin her bir yönünü anlamamıza yardımcı olur ve ağ tabanlı saldırıların hangi katmanda gerçekleşebileceğini analiz etmemizi sağlar.

Ağ Tabanlı Saldırılar

Ağ tabanlı saldırılar, ağ üzerinde gerçekleştirilen ve sistemleri hedef alan tehditlerdir. En yaygın ağ tabanlı saldırılar şunlardır:

- **DoS (Denial of Service) ve DDoS (Distributed Denial of Service):** Bu saldırılar, hedef sistemi aşırı trafik ile zorlayarak hizmeti kesintiye uğratmayı amaçlar.
- **ARP Spoofing:** ARP protokolünün kötüye kullanılmasıyla, ağdaki cihazlar arasında yanlış veri iletimi sağlanarak veri trafiği yönlendirilebilir veya kesilebilir.

- **MITM (Man-in-the-Middle):** Saldırgan, iki cihaz arasındaki iletişime müdahale ederek verileri çalabilir veya değiştirebilir.



Şekil 2 MITM Saldırısı

Savunma Yöntemleri

Ağ tabanlı saldırılara karşı savunma yöntemleri, saldırının türüne ve hedef alınan sisteme göre değişiklik gösterebilir. Ancak, genel savunma stratejileri şunlardır:

- **Firewalls (Güvenlik Duvarları):** İçeriye ve dışarıya çıkan veri trafiğini denetleyerek kötü niyetli bağlantıları engeller.
- **IDS/IPS (Intrusion Detection/Prevention Systems):** Ağ trafiğini izleyerek olağandışı davranışları tespit eder ve saldırıları engeller.
- **DDoS Koruma:** DDoS saldırılarını engellemek için trafik filtreleme ve yönlendirme teknikleri kullanılır.
- **Eğitim ve Farkındalık:** Ağ kullanıcıları için düzenli güvenlik eğitimleri, insan faktörünü minimize ederek iç tehditleri engeller.

Ağ güvenliği, teknoloji ve internetin hayatımızda giderek daha fazla yer edinmesiyle daha da önemli hale gelmiştir. Ağ yapılarının doğru bir şekilde tasarlanması, ağ protokollerinin iyi anlaşılması ve potansiyel ağ tabanlı saldırılara karşı etkili savunma stratejilerinin uygulanması, dijital güvenliği sağlamak için temel adımlardır. Bu bağlamda, ağ temellerini anlamak ve güvenlik açıklarını minimize etmek, bir organizasyonun dijital varlıklarını korumanın ilk adımıdır.

SONUÇ

SOC analistleri, siber güvenlik alanında organizasyonların ilk savunma hattını oluşturur. Bu uzmanlar, potansiyel tehditleri erkenden tespit etmek ve müdahale etmek için derin teknik bilgi ve becerilerle donanmış olmalıdır. Ağ temellerinin, protokollerinin ve savunma stratejilerinin anlaşılması, ağ üzerindeki tehditleri etkili bir şekilde yönetmek için büyük bir öneme sahiptir. Cyber Kill Chain gibi saldırı zincirlerinin her aşamasına hakim olmak, güvenlik analistlerinin tehditleri önceden görmelerini ve hızlıca çözüm üretmelerini sağlar. Her ne kadar saldırılar giderek daha sofistike hale gelse de, güçlü güvenlik ürünleri, stratejiler ve uzman bir SOC ekibiyle, organizasyonlar siber tehditlerle başa çıkabilir ve dijital güvenliklerini koruyabilirler. Bu yazıda ele alınan konular, SOC analistlerinin daha etkili ve bilinçli bir şekilde görev yapabilmeleri için önemli bilgiler sunmaktadır.

KAYNAKÇA

[1] https://www.manageengine.com

[2] https://www.splunk.com

[3] https://sprinto.com

[4] https://chatgpt.com/?oai-dm=1

[5] https://medium.com

[6] https://www.offsec.com