İSTANBUL TİCARET ÜNİVERSİTESİ
FEN BİLİMLERİ DERGİSİ

İstanbul Commerce University Journal of Science

http://dergipark.org.tr/ticaretfbd

Araştırma Makalesi /Research Article

LİNUX PLATFORMUNDA MITRE ATT&CK MATRİSİ KULLANARAK SALDIRI PLANLAMA VE UYGULAMA*

ATTACK PLANNING AND IMPLEMENTATION USING MITRE ATT&CK MATRIX ON LINUX PLATFORM

Suat TOKSÖZ[1] **Metin TURAN**[2]

https://doi.org/10.55071/ticaretfbd.1572294

Sorumlu Yazar
(Corresponding Author)
suat.toksoz@istanbulticaret.edu.tr

Geliş Tarihi
(Received)
23.10.2024

Revizyon Tarihi
(Revised)
26.12.2024

Kabul Tarihi
(Accepted)
26.12.2024

Öz

Bu makale, Linux platformunda MITRE ATT&CK matrisine dayalı saldırıların planlanması ve uygulanması süreci ele alınmaktadır. MITRE ATT&CK matrisi, siber tehditlere karşı savunma mekanizmalarının güçlendirilmesi amacıyla geliştirilmiş bir çerçeve olarak tanımlanmakta olup, saldırganların teknikleri, taktikleri ve prosedürleri sistematik bir şekilde sınıflandırılmaktadır. Çalışmada, Linux tabanlı sistemlerde bu matris kullanılarak çeşitli saldırı senaryoları oluşturulmakta ve bu senaryoların uygulanabilirliği test edilmektedir. Ayrıca, bu saldırıların tespiti ve önlenmesi için kullanılabilecek yöntemler ve araçlar tartışılmaktadır. Çalışmada, Balküpü üzerinden gelen saldırılara ait loglar toplanmakta, analiz edilmekte ve değerlendirilmektedir. Elde edilen sonuçlar, siber güvenlik uzmanlarının Linux platformlarında karşılaşabilecekleri tehditleri daha iyi anlamalarına ve bu tehditlere karşı etkili savunma stratejileri geliştirmelerine katkı sağlamak amacıyla sunulmaktadır.

Anahtar Kelimeler: Mitre Att&ck, siber güvenlik, saldırı planlama, saldırı tespiti, savunma stratejileri.

Abstract

This paper discusses the process of planning and executing attacks based on the MITRE ATT&CK matrix on the Linux platform. The MITRE ATT&CK matrix is defined as a framework developed to strengthen defense mechanisms against cyber threats and systematically classifies attackers' techniques, tactics and procedures. In this study, various attack scenarios are created using this matrix on Linux-based systems and the applicability of these scenarios is tested. Furthermore, methods and tools that can be used to detect and prevent these attacks are discussed. The study collects, analyzes and evaluates the logs of the attacks received through Balküpü. The results are presented in order to help cybersecurity experts better understand the threats they may face on Linux platforms and develop effective defense strategies against these threats.

Keywords: Mitre Att&ck, cybersecurity, attack planning, attack detection, defense strategies.

* *Bu yayın Suat Toksöz isimli öğrencinin İstanbul Ticaret Üniversitesi Lisansüstü Eğitim Enstitüsü, Siber Güvenlik Programındaki Yüksek Lisans tezinden üretilmiştir.*

[1] İstanbul Ticaret Üniversitesi, Lisansüstü Eğitim Enstitüsü, Siber Güvenlik Yüksek Lisans Programı, İstanbul, Türkiye. suat.toksoz@istanbulticaret.edu.tr, Orcid.org/0000-0002-3074-5455.

[2] İstanbul Ticaret Üniversitesi, Yazılım Mühendisliği Anabilim Dalı, İstanbul, Türkiye. mturan@ticaret.edu.tr, Orcid.org/0000-0002-1941-6693

1. GİRİŞ

Günümüzde dijital dönüşüm ve internetin yaygın kullanımıyla birlikte, siber güvenlik kritik bir öneme sahip hale getirilmiştir. Bilgi teknolojileri altyapılarının korunması ve hassas verilerin güvenliği sağlanarak toplumların güvenliği temin edilmeye çalışılmaktadır. Özellikle Linux tabanlı sistemler, sunucular ve diğer cihazlar, yaygın bir tercih haline gelmiş olduğundan, siber saldırganlar tarafından hedef alınmaktadır.

Linux platformunda MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) matrisine yönelik saldırı planlama ve uygulama konusuyla ilgili temel sorun, Linux platformlarının karmaşıklığı ve çeşitliliği nedeniyle ortaya çıkmaktadır. Bu platformda kullanılan farklı dağıtımlar, çekirdek versiyonları ve uygulama yelpazesi, saldırganların hedef sistemlerdeki zafiyet çeşidini ve sayısını arttırmaktadır (Liao vd. 2023). Ayrıca, linux'un açık kaynak doğası ve topluluk tarafından sürekli güncellenen yapısı, savunma ve saldırı stratejilerinin sürekli değişen bir ortamda tutulmasına neden olmaktadır.

Bu bağlamda, Linux platformunda MITRE matrisine yönelik saldırı planlama ve uygulama süreçlerindeki sorunlar, güvenlik uzmanlarının karşılaştıkları zorlukları anlamalarını ve etkili savunma tedbirlerinin geliştirilmesini gerektirmektedir. Siber suçlular, yanlış yapılandırılmış veya kötü yönetilen sistemlerden yararlanılarak fidye yazılımı ve kripto para madenciliği saldırıları (cryptojacking) için Linux platformları giderek daha fazla hedef alınmaktadır. VMware'in siber güvenlik araştırmacıları, hibrit çalışma ortamlarında bulut hizmetlerinin benimsenmesiyle daha da kötüleşen Linux tabanlı sistemleri hedef alan sofistike kötü amaçlı yazılımlarda bir artış olduğuna vurgu yapılmaktadır. Linux sunuculara yönelik saldırılar, yaygın ağ tehlikesine, fidye taleplerine ve veri hırsızlığına yol açabileceğinden ve olay müdahale çabalarının zorlaştırılmasından dolayı bu eğilim önemli riskler oluşturmaktadır (Palmer, 2024).

Siber suçluların Linux platformlara yönelik artan tehdidi ve bu saldırıların işletmeler üzerindeki potansiyel etkileri günümüzde önemli bir problem olarak önümüze çıkmaktadır. Firmaların çoğunluğunun fidye yazılımı saldırılarına karşı savunmasız oldukları ve bu tür saldırılar sonrasında önemli miktarda fidye ödedikleri tahmin edilmektedir.

Bilgi güvenliğinden sorumlu yöneticilerin (Chief Information Security Officer) %90'ı, kurumlarının 2023 yılında en az bir yıkıcı saldırıya maruz kaldığını ve %83'ü, bir fidye yazılımı saldırısının ardından saldırganlara ödeme yapıldığını belirtmiştir. Yarıdan fazlası ise fidye olarak en az $100.000 ödendiğini ifade etmiştir (Kovar ve Paine, 2024).

Siber saldırılara yönelik erken tespit ve erken önlem alınması, saldırıların etkisinin ve maliyetinin düşürülmesini sağlamaktadır. Tek bir kullanıcının tehdidi tanıyabilmesi durumunda, siber güvenlik olaylarının %80'inin önüne geçilebileceği ve ikinci olarak, tüm sistemlerin zamanında güncellenmesi ve uygun şekilde yapılandırılması da son derece önemli görülmektedir (Yousaf ve Zhou 2024).

T-Pot balküpü (honeypot), farklı etkileşim seviyelerine sahip geniş bir balküpü koleksiyonu sunarak, güvenlik uzmanlarının ağlara yönelik çeşitli saldırı türlerini izlemeleri ve saldırgan davranışlarını analiz etmeleri sağlanmaktadır. Düşük etkileşimli

balküpleri (MedPot, Honeyd, Dionaea gibi) temel saldırı bilgilerini toplarken, orta etkileşimli balküpleri (HoneyTrap, Snare, Glutton gibi) daha derinlemesine analiz yapılmasını sağlamakta ve yüksek etkileşimli balküpleri (Cowrie, Hellpot, Redishoneypot gibi) gerçekçi saldırı ortamları sunarak ayrıntılı veriler sağlanmaktadır. Bu çeşitlilik, T-Pot'in ağ güvenliğini güçlendirmek ve siber tehditleri etkin bir şekilde tespit etmek için güçlü bir araç olarak kullanılmaktadır (Rawat 2024).

T-Pot balküpü teknolojisi ve Wazuh gibi güvenlik çözümleri, Linux platformunda MITRE ATT&CK matrisinde bulunan teknik, taktik ve prosedürlerine (Tactics, Techniques and Procedures/TTP) yönelik saldırıların simüle edilmesiyle etkili bir çözüm sağlanmaktadır. T-Pot, gerçek saldırılar taklit edilerek savunma mekanizmalarının test edilmesine olanak tanınmakta ve saldırganların dikkatleri çekilerek izlenmeleri ve tespit edilmeleri mümkün kılınmaktadır. Balküpleri, erken tehdit tespiti yapılmasını sağlamakta, saldırganların taktiklerinin anlaşılmasına olanak tanımakta, dikkatlerinin kritik sistemlerden uzaklaştırılması sağlanmakta ve ağ adli bilişimi için faydalı veriler sağlanmaktadır (Koutsikos 2024). Wazuh, log yönetimi, tehdit algılama ve log analiz özellikleriyle Linux platformlarında saldırılar için önleyici ve tespit edici bir rol üstlenmektedir. Bu çözümler, Linux platformunda MITRE ATT&CK matrisi çerçevesinde saldırıların nasıl etkin bir şekilde planlanıp uygulanabileceğini göstermek, saldırı planlama ve uygulama süreçlerinin daha iyi anlaşılmasını sağlamakta ve güvenlik ekiplerine gerçek dünya senaryolarında pratik deneyim kazandırmakta katkı sağlamaktadır. Ayrıca, savunma stratejilerinin geliştirilmesine de katkı sağlanmaktadır.

Bu çalışmanın amacı, Linux platformunda MITRE ATT&CK matrisine yönelik saldırıların planlanması ve uygulanması süreci detaylı bir şekilde incelenmektedir. Araştırmada, öncelikle siber güvenliğin önemi ve günümüzdeki tehdit manzarası üzerine çalışmalar yapılmış ve MITRE ATT&CK matrisinin yapısı ve işlevi hakkında bilgi verilmiştir. Daha sonra, Linux tabanlı sistemlere yönelik kullanılabilecek çeşitli saldırılar belirlenmiş ve bu saldırıların log analizleri yapılarak MITRE ATT&CK matrisine adreslenmesi sağlanmıştır. Çalışmanın sonuçları, siber güvenlik uzmanlarının Linux platformlarında karşılaşabilecekleri tehditleri daha iyi anlamalarına ve bu tehditlere karşı etkili savunma stratejileri geliştirmelerine katkı sağlamayı hedeflemektedir.

Bu araştırmanın literatüre ana katkısı, siber saldırılara karşı bir savunma aracı olarak kabul gören T-Pot balküpü kullanımının, diğer araçlarla entegre edildiğinde verimli bir şekilde nasıl kullanılacağına ilişkin bir çerçeve sunması ve bunun deneysel olarak uygulanmış sonuçlarını paylaşarak potansiyelini ortaya koymasıdır. Bu araştırma ile, MITRE ATT&CK matrisine uygun şekilde sınıflandırılma ve Wazuh ile entegrasyonu sayesinde güvenlik olaylarının etkin bir şekilde yönetilmesi süreçlerine ilişkin önemli bulgular elde edilmiştir. T-Pot'tan elde edilen veriler, MITRE ATT&CK matrisine entegre edilerek, saldırıların teknik aşamaları ve saldırganların kullandığı yöntemler doğru bir şekilde sınıflandırılmıştır. Bu sayede, saldırıların gelişim aşamaları daha net bir şekilde tanımlanmış ve siber güvenlik uzmanlarına savunma stratejilerini güçlendirme fırsatı sağlanmıştır. Wazuh'un, bu sürece dahil edilmesiyle birlikte, gerçek zamanlı güvenlik olaylarının izlenmesi ve analiz edilmesi sağlanmış, potansiyel tehditler hızlı bir şekilde tespit edilmiştir. Wazuh'un sağladığı tehdit istihbaratı ve alarm mekanizmaları, saldırılara karşı hızlı yanıt verilmesini mümkün kılmıştır. Bu

çerçeve ile, sadece saldırıların tespit edilmesi değil, aynı zamanda siber savunma stratejilerinin geliştirilmesi de mümkün olmuştur. Elde edilen sonuçlar, siber güvenlik alanında savunma stratejilerinin iyileştirilmesi ve saldırı tespit sistemlerinin geliştirilmesi için önemli bir referans oluşturmaktadır.

2. LİTERATÜR ARAŞTIRMASI

"An Adversarial Approach: Comparing Windows and Linux Security Hardness Using Mitre ATT&CK Framework for Offensive Security" isimli makale, MITRE ATT&CK çerçevesi kullanılarak gerçek dünya saldırıları simüle edilmektedir. Bu testler, gelişmiş kalıcı tehditlere (APT'ler) ve diğer saldırı vektörlerine karşı güvenlik değerlendirmesi yapılmak amacıyla Windows (7, 8, 10 ve Windows Server 2012) ve Linux (16.04, 18.04 ve 20.04) sürümlerinde gerçekleştirilmektedir (Sikandar vd. 2022).

Hobert ve arkadaşları, makalelerinde, Linux sistemlere yönelik saldırıların MITRE ATT&CK matrisi çerçevesinde etkin bir şekilde planlanmasının birkaç önemli strateji ile gerçekleştirildiğini belirtmişlerdir. Ayrıca, otomatik benzerlik hesaplaması ile 793 ön işlenmiş komut seti analiz edilerek sekiz farklı saldırgan grubunun belirlendiği ifade edilmiştir. Son olarak, saldırılar MITRE ATT&CK çerçevesine göre kategorize edilerek, her bir saldırının aşamaları ve kullanılan tekniklerin belirlendiği aktarılmıştır. Bu yöntemler, saldırganların davranışlarının anlaşılması ve daha etkili savunma mekanizmalarının geliştirilmesi açısından kritik öneme sahiptir (Hobert, Lim, ve Budiarto 2023).

Shrivastava ve arkadaşları, makalelerinde, Linux sistemlere yönelik saldırıların etkin bir şekilde planlanabilmesi için MITRE ATT&CK matrisi çerçevesinde çeşitli adımlar ve stratejilerin uygulandığını belirtmişlerdir. Özellikle Cowrie balküpü kullanılarak saldırıların tespiti ve analizi yapılmakta, bu sayede saldırganların davranışları hakkında derinlemesine bilgiler elde edilmektedir. Saldırılar altı farklı kategoriye ayrılmaktadır: kötü niyetli yük, SSH saldırısı, XOR DDoS, casusluk, şüpheli ve temiz. Cowrie balküpü, saldırganların etkileşimlerini kaydederek veri toplamakta ve bu veriler, güvenlik duvarı ve saldırı tespit sistemleri (IDS) gibi savunma mekanizmalarının güçlendirilmesine katkı sağlanmaktadır. (Shrivastava, Bashir ve Hota 2019).

Weapon, MITRE ATT&CK matrisinden yararlanılarak fidye yazılımlarının erken aşamalarında tespit edilmesi için tasarlanmış bir araçtır. Weapon, kritik fidye yazılımı özelliklerini çıkarmak için dinamik analiz kullanılmakta ve ayrıca, anlamsal özellikleri bu temel niteliklerle eşleştirmek için Android geliştirici belgelerinden türetilen bir anlamsal veri tabanı kullanılmaktadır. Bu bilgiler, MITRE saldırı verileriyle ilişkilendirilerek fidye yazılımları ilk aşamalarında verimli bir şekilde tanımlanmaktadır. Yaklaşım, gerçek dünya senaryolarında gözlemlenen düşman taktiklerini ve tekniklerini detaylandıran MITRE ATT&CK matrisinden elde edilen saldırı verileri kullanılarak bir model oluşturulmaktadır. Yapılan testlerde, Weapon, sırasıyla 2.794 fidye yazılımı örneğinden 2.568'ini ve 5.875 fidye yazılımı örneğinden 5.286'sını operasyonel aşamaya ulaşmadan önce başarıyla tespit etmiştir. Bu araç, fidye yazılımı tespitinde %99,21 gibi etkileyici bir doğruluk oranına ulaşmaktadır. Genel olarak, Weapon, gelişmiş özellik çıkarma teknikleri kullanılarak ve MITRE

ATT&CK matrisindeki kapsamlı saldırı verilerinden yararlanarak erken aşama fidye yazılımı tespiti için etkili bir yöntemi temsil etmektedir (Singh ve Tripathy 2024).

Araştırmacılar, balküpü modeli kullanılarak, saldırganların sistemle daha derinlemesine etkileşimde bulunması sağlanmış ve siber güvenlik araştırmaları ile tehdit tespiti açısından daha zengin veriler elde edilmiştir. Yüksek etkileşimli bir balküpü kullanılarak, saldırganların gerçek sistemlerde gerçekleştirdiği hareketler ve komutlar daha ayrıntılı bir şekilde izlenebilmiştir. MITRE ATT&CK matrisi kullanılarak, balküpleri tasarlanmış ve denetlenmiştir. Bu taksonomi, siber saldırılar belirli teknikler ve taktikler çerçevesinde sınıflandırılarak, tehdit analizinin daha sistematik hale getirilmesine yardımcı olmuştur. Araştırmacılar, balküpü uygulanması sırasında, on yedi günlük süre boyunca çeşitli saldırgan profilleri ve saldırı yöntemlerini gözlemlemişlerdir. Toplanan veriler, daha önce belgelenmemiş Tehdit Göstergeleri içermekte olup, bu da siber güvenlik topluluğuna yeni bilgiler sağlanmasını olanaklı kılmıştır. Yeni bir balküpü modelinin ve tasarımının etkinliği gösterilmiş, saldırganların davranışlarını daha iyi anlamak ve yeni tehdit göstergeleri keşfetmek için yüksek etkileşimli balküplerinin potansiyeli ortaya konmuştur. Bu çalışma, siber güvenlik uzmanlarına saldırıları tespit etme ve önleme konusunda daha etkili stratejiler geliştirmeleri için değerli bilgiler sunmaktadır (Abbas-Escribano ve Debar 2023).

Saldırganlar balküpü ile etkileşime girdikçe, balküpü yazılımı tarafından komutlar ve aktiviteler dikkatlice kaydedilmekte, bu da saldırganların davranışları ve taktikleri hakkında değerli bilgiler sağlanmaktadır. Bir sonraki adımda, bu kaydedilen komutlar toplanarak analiz edilmekte ve saldırganlar tarafından kullanılan desenler, eğilimler ve yaygın teknikler belirlenmektedir. Bu veriler, Linux komutlarının MITRE ATT&CK taktik ve teknikleri ile eşleştirilmesi için temel oluşturmaktadır. Eşleştirilen sonuçların doğruluğu ve etkinliği, bazı metrikler kullanılarak değerlendirilmekte ve modelin performansı bu şekilde ölçülmektedir. Bu değerlendirme, sürecin Linux komutlarını MITRE ATT&CK taktik ve teknikleri ile ne kadar iyi ilişkilendirdiğini belirlemeye yardımcı olmaktadır. Elde edilen içgörüler, siber güvenlik uzmanlarına saldırganların Linux platformları ile etkileşime geçerken kullandıkları taktik ve teknikler hakkında daha derin bir anlayış sağlamaktadır. Balküpü kullanılarak saldırgan davranışları yakalanmakta ve analiz edilmekte, NLP teknikleri uygulanarak Linux komutları MITRE ATT&CK ile eşleştirilmektedir. Bu sayede, siber güvenlik uzmanları tehdit tespiti, olay müdahalesi ve genel siber güvenlik savunmalarını önemli ölçüde iyileştirebilmektedirler (Andrew, Lim, ve Budiarto 2022).

Yang ve arkadaşlarının yaptığı çalışmada, ağ tehditlerinin yönetilmesi için son derece etkileşimli bir balküpü tabanlı yaklaşımın nasıl kullanılabileceği incelenmektedir. Balküpü, saldırganları çekmek amacıyla tasarlanmış simüle edilmiş sistemler olup, güvenlik ekiplerinin saldırıların faaliyetlerini izlemesine ve analiz etmesine olanak tanımaktadır. Bu yeni yaklaşım, geleneksel bal peteği işlevselliği geliştirilerek sistemlerin daha tepkisel ve etkileşimli hale getirilmesi sağlanmaktadır. Bu sayede, potansiyel tehditler hakkında daha detaylı bilgi toplanabilmektedir. Yazarlar, bu yaklaşımın ağ güvenliğini iyileştirme konusundaki faydalarını tartışmakta ve siber tehditlerin tanımlanması ve azaltılmasında etkin bir rol oynandığı vurgulanmaktadır (Yang vd. 2023).

Bu kapsamda, siber saldırılara karşı etkili bir savunma stratejisi geliştirmek için doğru araçlara ve yöntemlere sahip olunması hayati önem taşımaktadır. Bu noktada, MITRE ATT&CK matrisi, siber tehditlerin daha iyi anlaşılması ve savunma mekanizmalarının güçlendirilmesi için önemli bir araç olarak öne çıkmaktadır. MITRE ATT&CK matrisi, saldırganların kullandığı TTP'ler kapsamlı bir şekilde belgelenerek, savunma mekanizmalarını güçlendirmek isteyen kuruluşlara rehberlik edilmektedir.

Xiong ve arkadaşları, kurumsal sistemler için Meta Saldırı Dili (MAL) çerçevesine dayanan ve MITRE Enterprise ATT&CK Matrisi ile entegre olan enterpriseLang adlı bir tehdit modelleme dili kapsamında bir çalışma yapmışlardır. Bu dil, kurumsal sistemlerin siber saldırılara karşı dayanıklılığını değerlendirmek için sistem varlıklarının, saldırı adımlarının, savunmaların ve varlık ilişkilerinin tanımlanmasına olanak tanımaktadır. Paydaşlar, enterpriseLang kullanarak bilinen saldırı teknikleriyle ilgili zayıflıkları analiz edebilir, sistem modelleri üzerinde siber saldırılar simüle edebilir ve güvenliği artırmak için hafifletme önerileri alabilmektedir. Bu dil, kurumsal sistemlerde tehdit modellemesi için yapılandırılmış bir yaklaşım sunarak paydaşların güvenlik sorunlarını proaktif bir şekilde ele almalarını ve sistemlerinin güvenlik duruşunu güçlendirmek için bilinçli kararlar vermelerini sağlamaktadır. Makale, genel olarak kapsamlı tehdit analizi ve azaltma stratejileri için MITRE ATT&CK matrisi tarafından sağlanan bilgi tabanından yararlanarak siber tehditlerin etkili bir şekilde modellenmesi ve simüle edilmesi için enterpriseLang gibi alana özgü bir dil kullanmanın önemini vurgulamaktadır (Xiong vd. 2022).

Wazuh, IIoT (Industrial Internet of Things) ortamlarının güvenliğini sağlamak için sağlam bir mimari sunulmaktadır. Bu mimarinin merkezinde, izlenen cihazlara yerleştirilen, güvenlik verilerini toplayan ve bunları merkezi bir Wazuh sunucusuna ileten aracılar bulunmaktadır. Bu sunucu, verileri önceden tanımlanmış kurallara göre analiz etmekte, şüpheli faaliyetler için uyarıları tetiklemekte ve uzak aracılar ağı yönetilmektedir. Güvenlik duvarları ve yönlendiriciler gibi aracısız cihazlar, syslog, SSH veya uygulama programlama arayüzleri (API'ler) aracılığıyla veri göndererek katılabilmektedir. Bu esneklik, Wazuh'un çeşitli veri formatlarını işleme becerisiyle birleştiğinde, onu kapsamlı IIoT güvenlik izleme ve analizi için değerli bir araç olarak konumlandırmaktadır (Afenu, Asiri, ve Saxena 2024).

Andrew ve arkadaşlarının çalışmalarında, Linux komutlarının MITRE ATT&CK teknikleri ve alt tekniklerine, ayrıca ATT&CK taktiklerine eşleştirilmesi için Doğal Dil İşleme (NLP) teknikleri kullanılmıştır. Kullanılan yöntemler arasında Bag of Words (BoW), Term Frekansı-Ters Doküman Frekansı (TF-IDF) ve önceden eğitilmiş Kelime Gömmeleri (Word Embeddings) bulunmaktadır. Benzerlik skoru hesaplamak için kosinüs benzerliği kullanılmıştır. Elde edilen sonuçlar, MITRE ATT&CK teknikleri ve alt teknikleri için en yüksek recall-10 skoru: Unigram ve Bigram ile TF-IDF ve Snowball Stemmer kullanılarak 0,45575 olarak elde edilmiştir. MITRE ATT&CK taktikleri için en yüksek recall-10 skoru: Unigram ve Bigram ile TF-IDF ve Snowball Stemmer kullanılarak 0,75397 olarak elde edilmiştir. Ayrıca, önceden eğitilmiş Kelime Gömme modellerinin performansı, TF-IDF ve BoW modellerine kıyasla daha düşük bulunmuş ve bunun metinlerin bağlamlarının farklı olmasından kaynaklandığı belirtilmiştir. Çalışma, gelecekte siber güvenlik bağlamına özgü bir kelime gömme modeli oluşturulması ve farklı vektörizasyon ve tokenizasyon tekniklerinin denenmesi planlanmaktadır (Andrew, Lim, ve Budiarto 2022).

“Performance Analysis of Network Intrusion Detection Using T-Pot Honeypots” isimli makalede, T-Pot'un gerçek sistemleri taklit ederek saldırganları cezbettiği, etkileşimlerin kaydedildiği ve bu verilerin analiz edildiği belirtilmiştir. Ağ saldırıları, brute force denemeleri ve DDoS saldırıları gibi tehditler tespit edilmiştir. Ayrıca, Elasticsearch, Kibana ve Debian Linux gibi araçların, saldırı desenlerini anlamak, erken tespit yapmak ve tehdit istihbaratı sağlamak amacıyla kullanıldığı vurgulanmıştır. Yapılan araştırmalar, T-Pot’un bu saldırıları başarılı bir şekilde tespit ettiği, ancak daha karmaşık saldırıları işleyebilme kapasitesinin geliştirilmesi gerektiği ve veri işleme gücüne dayalı sınırlamaların bulunduğu ortaya konmuştur (Mohd Fuzi vd. 2024).

“Honeypot in a box: A distributed cluster network for honeypot deployment” isimli makalede, Kubernetes (K3s dağıtımı) ve WireGuard VPN kullanılarak dağıtık bir balküpü sistemi geliştirilmesi ve uygulanmasına odaklanılmaktadır. Artan internet bağlantısı ve sofistike siber saldırılarla birlikte siber güvenliğin öneminin giderek arttığı vurgulanmıştır. Geleneksel balküplerinin sınırlı olmasına rağmen, farklı coğrafi konumlarda saldırı desenlerini tespit etme yeteneklerinin yetersiz olduğu belirtilmiş ve bu sınırlamanın aşılması amacıyla farklı bölgelerde balküplerinin dağıtılarak daha kapsamlı bir saldırı analizi yapılabileceği savunulmuştur. Kubernetes’in ölçeklenebilirliği ve bulut sağlayıcılarıyla entegrasyon kolaylığı nedeniyle Docker Compose ve Docker Swarm yerine tercih edilmiştir; K3s’in ise düşük kaynak gereksinimleri ve kolay dağıtım özelliği nedeniyle seçildiği ifade edilmiştir. Güvenli iletişim için WireGuard VPN kullanılmış ve ağ gecikmesi ile bant genişliği performansının üstün olduğu belirtilmiştir. Yapılan performans testleri, sistemin balküpleri’nin dağıtırken kabul edilebilir performans seviyelerinin korunduğunu göstermiştir. Sonuç olarak, tezdeki hedeflerin başarıyla elde edildiği ve gelecekte daha fazla balküpü görüntüsünün eklenmesi, kümeler arasındaki güvenli bağlantıların sağlanması ve veri sınıflandırma gibi ek çalışmalara yer verileceği ifade edilmiştir (Candidate ve Ayala 2024).

“Enhancing Cybersecurity Resilience: Integrating IDS with Advanced Honeypot Environments for Proactive Threat Detection” isimli araştırma makalesinde, T-Pot'un bir ağ izinsiz giriş tespit sistemi olarak, ağlara yönelik çeşitli saldırı stratejilerini tanımlama etkinliğine odaklanılmaktadır. T-Pot'un kaba kuvvet (brute force), hizmet reddi (DoS) ve ağ haritalama saldırıları gibi çeşitli saldırı türlerine karşı performansı değerlendirilmiştir. Makalede, T-Pot’un siber saldırıları tespit etme ve engelleme konusundaki avantajları incelenmiş ve bu balküpünün potansiyel güvenlik tehditlerini nasıl etkili bir şekilde hafifletebileceği tartışılmıştır. Araştırma, T-Pot üzerinde gerçekleştirilen çeşitli deneylerden toplanan verileri analiz ederek, ağ izinsiz giriş tehditlerini tanımlama ve hafifletme konusundaki yetenekleri keşfetmiştir. Bu çalışmanın sonuçları, T-Pot’un ağ güvenliğini artırmada ve siber saldırılara karşı koruma sağlamada sağlam ve güvenilir bir çözüm sunduğunu göstermektedir (Raghul vd. 2024).

“Enhancing False Positive Detection in IDS/IPS Using Honeypots: A Case Study with CSE-CIC-2018 Dataset” araştırma makalesinde, T-Pot’un bir ağ izinsiz giriş tespit sistemi olarak, ağlara yönelik çeşitli saldırı stratejilerini tanımlamadaki etkinliğine odaklanılmaktadır. Bu balküpünün kaba kuvvet (brute force), hizmet reddi (DoS) ve ağ haritalama gibi çeşitli saldırı türlerine karşı performansı değerlendirilmiştir. Makale

ayrıca, T-Pot'un siber saldırıları tespit etme ve engelleme konusundaki avantajları incelenmiş ve bu balküpünün potansiyel güvenlik tehditlerini etkili bir şekilde nasıl hafifletebileceği tartışılmıştır. Araştırma, T-Pot üzerinde gerçekleştirilen çeşitli deneylerden toplanan verileri analiz ederek, ağ izinsiz giriş tehditlerini tanımlama ve hafifletme yetenekleri keşfedilmiştir. Çalışmanın sonuçları, T-Pot'un ağ güvenliğini artırma ve siber saldırılara karşı koruma sağlama konusunda güçlü ve güvenilir bir çözüm sunduğunu göstermektedir (Rawat 2024).

"Faking smart industry: exploring cyber-threat landscape deploying cloud-based honeypot" makalesinde, akıllı sanayilerdeki siber tehdit manzarasını anlamak amacıyla balküplerinin, özellikle de T-Pot balküpünün kullanımına odaklanılmaktadır. T-Pot, Amazon Elastic Compute Cloud (AWS EC2) üzerinde altı farklı bölgede, endüstriyel kontrol sistemlerini (ICS) simüle eden çeşitli cihaz ve protokollerle dağıtılarak kullanılmıştır. Bu yaklaşım, T-Pot'un geniş hizmet yelpazesi, kolay kurulum ve kullanım özellikleri ile kullanıcı dostu analiz panosundan dolayı tercih edilmiştir. Çalışma, sanayilerdeki siber saldırıların hızla arttığı ve Endüstri 4.0'ın sanayi ile bilgi ve iletişim teknolojilerinin entegrasyonunu hızlandırarak kritik sistemlerin saldırı yüzeyini genişlettiği bir dönemde yapılmıştır. Balküplerinden toplanan veriler, saldırı kaynakları, kullanılan teknikler ve hedeflenen cihazlar hakkında değerli bilgiler sunmuş, saldırıların çoğunlukla bulut hizmetlerinden geldiği ve IPMI cihazları, Siemens PLC'leri ve akıllı sayaçlar gibi cihazları hedef aldığı gözlemlenmiştir. Yaygın saldırı yöntemleri arasında kaba kuvvet (brute force) kimlik doğrulama, bilinen güvenlik açıklarının istismarı ve veri sızdırma gibi sonrasındaki eylemler yer almakta, zararlı yazılım örneklerinde ise fidye yazılımları ve Truva atı (Trojan) yaygın olarak gözlemlenmiştir. Bulgular, ICS güvenliği için yamanmamış güvenlik açıklarının ve eski hizmetlerin ciddi riskler oluşturduğunu, internet üzerinden erişilebilen ICS cihazlarının aktif bir şekilde hedef alındığını ve bu verilerin, saldırı tespit sistemlerini geliştirmek, tehdit istihbaratını güçlendirmek ve akıllı sanayiler için siber güvenlik savunmalarını güçlendirmek amacıyla kullanılabileceğini vurgulamaktadır. Makale, akıllı sanayilerde uygun güvenlik önlemlerinin uygulanmasının önemine dikkat çekmekte ve balküpü dağıtımlarından elde edilen bilgilerin, gelişen tehdit manzarasını anlamak ve sağlam bir siber savunma sistemi kurmak için kritik bir rol oynayabileceğini belirtmektedir (Rashid vd. 2024).

"Learning Models to Detect Personality Traits of Cyber Attackers: A Combined Approach Using Honeypot and Surveys" isimli araştırmada, gerçek dünyadaki siber saldırıları çekmek ve analiz etmek amacıyla kurulan bir balküpü sisteminin nasıl kullanıldığı detaylı bir şekilde açıklanmaktadır. Araştırma, toplanan verilerle saldırı tespiti ve önlenmesi için makine öğrenmesi modellerinin eğitilmesi hedeflenmiş, aynı zamanda saldırganların kişilik özelliklerinin incelenmesi, motivasyonlarının ve davranışlarının anlaşılmaya çalışıldığı belirtilmiştir. T-Pot balküpü, ESPOCH (Escuela Superior Politécnica del Chimborazo) altyapısında, çeşitli hizmetleri ve işletim sistemlerini taklit eden çok yönlü bir sistem olarak kurulmuştur. Saldırganları çekmek için balküpü'nün IP adresi hacker forumlarında yayımlanmış ve sunucu, yaygın güvenlik açıklarıyla yapılandırılarak saldırganları cezbetmek amacıyla standart portlarda hizmet vermeye başlamıştır (José ve Santander 2024).

Bu yaklaşım, saldırganların davranışlarını anlamak için çok yönlü bir veri toplama sürecini başlatmakta, aynı zamanda bu veriler kullanılarak makine öğrenmesi

algoritmaları aracılığıyla saldırganların kişilik özellikleri ve motivasyonlarına dair çıkarımlar yapılmaktadır. Araştırmada, saldırıların detayları ve saldırganların kullandığı teknikler, MITRE ATT&CK matrisine yerleştirilerek daha sistematik bir analiz yapılmaktadır. Bu yaklaşım, saldırganların kullandığı taktik ve tekniklerin etkili bir şekilde izlenmesini ve anlaşılmasını sağlamaktadır. Bu tür çalışmalar, yalnızca saldırı tespiti ve savunma stratejileri geliştirme açısından önemli katkılar sağlamakla kalmaz, aynı zamanda saldırganların davranışlarını daha derinlemesine anlamaya yardımcı olarak, onları etkili bir şekilde tahmin etme ve önleme kapasitesini de artırmaktadır. Altı ay süresince toplanan veriler, DoS (Denial of Service) saldırılarının en yaygın saldırı türü olduğunu, bunları SQL enjeksiyonu ve siteler arası komut dosyası çalıştırma (XSS) saldırılarının izlediğini ortaya koymuştur. Bu tür veriler, saldırı desenlerinin analizine yardımcı olarak savunma sistemlerini güçlendirebilmektedir. Ayrıca, bu veriler, makine öğrenmesi algoritmalarıyla birleştirilerek, saldırı türlerini sınıflandırmak ve evrilen saldırı desenlerine karşı daha akıllı güvenlik sistemleri geliştirmek amacıyla kullanılmaktadır. Makine öğrenmesi, saldırıları otomatik olarak tespit etme ve sınıflandırma konusunda büyük bir avantaj sağlamaktadır (José ve Santander 2024).

"Investigating Threats to ICS and SCADA Systems Via Honeypot Data Analysis and SIEM" başlıklı makale, SCADA (Denetim ve Veri Toplama) ve ICS (Endüstriyel Kontrol Sistemleri) sistemlerine yönelik tehditlerin incelenmesi amacıyla balküpü verisi analizi ve SIEM (Güvenlik Bilgisi ve Olay Yönetimi) sistemlerinin kullanımı ele alınmaktadır. Araştırma, Conpot adlı açık kaynaklı bir balküpü aracı kullanılarak SCADA sistemlerinin simüle edilmesi sağlanmış ve bu sistem, bulut ortamında bir konteyner içinde internete açılarak gerçek dünya tehdit verisi toplanmıştır. Bu veriler, ICS ve SCADA sistemlerinin savunmasını güçlendirebilecek önemli bilgileri içermektedir. Toplanan balküpü günlükleri, Wazuh adlı açık kaynaklı bir SIEM çözümüne entegre edilmiştir. Wazuh, tehditlerin zamanında analiz edilmesini sağlayarak saldırı tespiti ve yanıt süreçlerini optimize etmiştir. Wazuh tarafından üretilen uyarılar, TheHive adlı bir güvenlik orkestrasyonu, otomasyon ve yanıt (SOAR) platformuna yönlendirilmiş ve otomatik yanıt eylemleri için çalışma kitapları oluşturulmuştur. Örneğin, bu yanıt eylemleri arasında kötü amaçlı IP adreslerinin engellenmesi yer almaktadır. Bu tür otomatik yanıt süreçleri, siber tehditlere karşı daha hızlı ve etkili bir savunma sağlamaktadır. Araştırma, kaba kuvvet giriş denemeleri, keşif ve zafiyet taramaları, kimlik doğrulama limitlerini aşmaya yönelik saldırılar gibi çeşitli saldırı türlerinin tespit edilmesini sağlamıştır. Ayrıca, bu saldırıların çoğunun ABD, ardından Çin, Birleşik Krallık ve diğer ülkelerden geldiği tespit edilmiştir. Saldırıların çoğunun HTTP protokolünü hedef aldığı ve özellikle web tabanlı zafiyetler nedeniyle bu protokolün saldırganlar için daha cazip olduğu belirtilmiştir. Bu bulgular, SCADA ve ICS sistemlerinin internet üzerinden erişilebilirliğinin, saldırganlar için geniş bir saldırı yüzeyi sunduğunu göstermektedir (Muhammad ve Hafee y.y.).

"Developing Proactive Cyber Threat Defense Systems on Server Computers Using Honeypot Techniques" isimli makale, sunucu bilgisayarlarında siber tehditlere karşı proaktif bir savunma stratejisinin geliştirilmesine odaklanılmaktadır. Araştırmacılar, Brute Force saldırılarını engellemek için, sahte bir sunucu ortamı kullanarak kötü niyetli erişim girişimlerinin tespit edilmesi amacıyla bir balküpü sistemi kurulmuştur. AWS Cloud Services üzerinde kurulan balküpü, kamuya açık ağlardan erişilebilir hale getirilmiş ve sistem günlük verilerini toplamak için bir ajan yerleştirilmiştir. 16 Mart

2024 ile 15 Nisan 2024 tarihleri arasında toplanan 35.968 günlük veri analiz edilmiştir ve bu verilerin çoğu, "Root" kullanıcı adıyla yapılan SSH erişim girişimlerinden oluşan kaba kuvvet (Brute Force) saldırılarını göstermektedir. Veriler, Wazuh adlı açık kaynaklı bir SIEM (Güvenlik Bilgisi ve Olay Yönetimi) sistemi ile analiz edilmiştir ve MITRE ATT&CK çerçevesine dayalı yeni bir kural oluşturulmuştur. Bu yeni kural, belirli olayların 10 dakika içinde dört kez gerçekleşmesi durumunda tetiklenmiştir. Araştırma, sistemin gerçek dünyada nasıl çalıştığının test edilmesi için Nmap aracı kullanılarak yapılan simülasyonlarla başarıyla doğrulanmıştır. Yeni kural, kaba kuvvet saldırısı tespit edildiğinde, saldırganın IP adresini 30 dakika süreyle engellemiş ve bu süreç SIEM tarafından kaydedilmiştir. Araştırma, balküplerinin potansiyel saldırganlar ve teknikleri hakkında bilgi toplamada ne kadar etkili olduğu, ayrıca SIEM sistemlerinin bu verileri analiz etme ve otomatik önlemler alma konusundaki önemi vurgulanmıştır. Bu çalışma, siber saldırılara karşı proaktif bir savunma stratejisinin geliştirilmesinde balküpleri ve SIEM sistemlerinin entegrasyonunun büyük bir potansiyele sahip olduğunu göstermektedir (Mungsing ve Sringendee y.y.).

3. MITRE ATT&CK MATRİSİNİN YAPISI VE İŞLEVİ

MITRE ATT&CK matrisi, siber tehditlerin anlaşılmasını ve savunma stratejilerinin geliştirilmesini desteklemek amacıyla tasarlanmış bir çerçeve olarak kullanılmaktadır. Bu matris, saldırganların kullanabileceği çeşitli taktikleri, teknikleri ve prosedürleri kapsamaktadır.

Siber güvenlik alanında tehditlerin modellenmesi ve tehditlere yönelik savunma stratejilerinin belirlenmesi kapsamında MITRE ATT&CK matrisi önemli bir rol oynamaktadır. Gerçek dünya gözlemlerine dayanan kapsamlı bir TTP (Taktikler, Teknikler ve Prosedürler) deposu sunulmaktadır. MITRE ATT&CK matrisi, düşman davranış kalıplarının ve saldırı metodolojilerinin ayrıntılı bir şekilde anlaşılmasını sağlamaktadır. Bu bilgi, potansiyel siber tehditleri öngörebilen ve bunlara karşı koyabilen etkili tehdit modellerinin oluşturulması için gereklidir (Al-Sada, Sadighian, ve Oligeri 2024).

MITRE ATT&CK matrisi, platform geliştirme ve güvenlik operasyonlarını bilgilendirebilecek değerli bilgiler sunmaktadır. Platform geliştiricileri, düşmanlar tarafından kullanılan taktik ve teknikler anlaşılmakta, özellikle bu saldırı yöntemlerini hedef alan araçlar geliştirilebilmektedir. Ayrıca, güvenlik platformları, tehditleri önceliklendirmek için MITRE ATT&CK çerçevesinden yararlanılabilmektedir. Platform uyarıları, ATT&CK teknikleriyle uyumlu hale getirilerek, güvenlik ekiplerinin kuruluşlarının risk profiline dayalı olarak en kritik tehditlere odaklanmasına olanak tanınmaktadır. Bunun yanı sıra, MITRE ATT&CK matrisi verileri, platformlardaki güvenlik farkındalığı eğitim modüllerine entegre edilebilmektedir. Kullanıcılar, gerçek dünya saldırı tekniklerine maruz bırakılmakta, şüpheli faaliyetleri belirleme ve bildirme yetenekleri geliştirilmekte ve böylece kuruluşların siber güvenlik duruşu güçlendirilmektedir (Georgiadou, Mouzakitis, ve Askounis 2021).

Bilinen saldırı modelleri analiz edilerek ve bunlar toplanan verilerle ilişkilendirilerek, kuruluşların savunma stratejileri güçlendirilebilmektedir. MITRE ATT&CK, güvenlik açıklarının ve potansiyel saldırı vektörlerinin belirlenmesine yardımcı olarak, proaktif

savunma önlemlerinin alınmasını sağlamaktadır. Bu bilgi tabanı, saldırı olasılıkları ve başarı oranları hesaplanarak risk değerlendirme metodolojilerinde kullanılabilmektedir. MITRE ATT&CK ile saldırı grafiklerinin birleştirilerek, kuruluşların siber güvenlik duruşları değerlendirilebilmekte ve saldırıları azaltma çabalarına öncelik verilebilmektedir. Ayrıca, MITRE ATT&CK matrisi, siber saldırıların tespit edilmesine, tahmin edilmesine, önlenmesine ve azaltılmasına yardımcı olmaktadır. Mobil kötü amaçlı yazılımlar sınıflandırılarak ve MITRE ATT&CK matrislerine dayalı benzerlikler hesaplanarak, kuruluşların yanlış pozitifleri (false positive) azaltılmakta ve güvenlik uyarılarının doğruluğu artırılabilmektedir (Al-Sada, Sadighian, ve Oligeri 2024).

3.1. Mitre Att&Ck Matrisinin Genel Yapısı

MITRE ATT&CK matrisi, birçok farklı siber saldırı tekniğini kapsayan bir dizi taktik ve teknikten oluşmaktadır. Matris, taktikleri geniş bir kategori altında gruplandırmakta ve her taktik altında çeşitli saldırı teknikleri listelenmektedir. Her teknik, belirli bir saldırı yöntemini veya aşamayı temsil etmekte olup, bu teknikler, saldırganların ağları ele geçirme, gizlenme, hareket etme ve hasar verme gibi amaçlarına ulaşmak için kullandıkları araçlar olarak belirlenmektedir.

Çalışma kapsamında, balküpleri üzerinden gelen saldırılar MITRE ATT&CK Linux platformunda tespit edilenler ile ilişkilendirilmiş ve aşağıdaki Tablo 1'de gösterilmiştir.

Tablo 1. Tespit Edilen MITRE ATT&CK Saldırıları

Saldırı Türü (Attack Type)
Kalıcılık (Persistence)
Savunma Kaçırma (Defense Evasion)
Ayrıcalık Yükseltme (Privilege Escalation)
İlk Erişim (Initial Access)
Keşif (Discovery)
Sızma (Exfiltration)
Komuta ve Kontrol (Command and Control)
Koleksiyon (Collection)
Etki (Impact)
Yürütme (Execution)
Kimlik Bilgileri Erişimi (Credential Access)
Yanal Hareket (Lateral Movement)

Kalıcılık (Persistence), saldırganların sisteme uzun süreli erişim elde etmelerini sağlamak için kullanılan teknikleri kapsar. Bu teknikler, bir defa giriş sağlandıktan sonra, saldırganların sistemden çıkarılmadan veya fark edilmeden bir süre boyunca erişimlerini sürdürebilmelerini mümkün kılar. Çoğunlukla, kötü amaçlı yazılımlar veya sistemde yapılan değişiklikler aracılığıyla sağlanır.

Savunma Kaçırma (Defense Evasion), saldırganların savunma mekanizmalarından (antivirüs yazılımları, güvenlik duvarları vb.) kaçmak için kullandıkları yöntemleri ifade eder. Bu teknikler, tespit edilmeden sistemi manipüle etmek veya kontrol altına almak amacıyla tercih edilir.

Ayrıcalık Yükseltme (Privilege Escalation), saldırganların sahip oldukları erişim seviyesini artırmalarına olanak tanır. Kullanıcı seviyesindeki izinlerle sınırlı kalmak yerine, daha yüksek yönetici (admin) seviyelerine çıkarak sistem üzerinde tam kontrol elde edilir. Bu genellikle sistemin zayıflıklarından yararlanılarak yapılır.

İlk Erişim (Initial Access), saldırganların hedef sisteme ilk defa girmelerini sağlayan yöntemleri kapsar. Genellikle kimlik avı, zararlı yazılım yükleme veya ağ zafiyetlerinden yararlanılarak gerçekleştirilir. Saldırgan, sistemin güvenlik önlemlerini aşarak ilk adımda erişim sağlar.

Keşif (Discovery), saldırganların sistemde bilgi toplamak amacıyla kullandığı teknikleri ifade eder. Bu süreçte, saldırganlar ağdaki cihazları, kullanıcıları ve diğer sistem bileşenlerini belirlemek için çeşitli araçlar kullanır. Keşif, sonraki adımlar için yol gösterici olur.

Sızma (Exfiltration), hassas verilerin sistemden dışarıya çıkarılması sürecidir. Bu, saldırganın hedefe dair önemli verileri ele geçirmesinin ardından yapılır. Veriler çoğunlukla şifrelenir ve güvenli yollarla dışarıya aktarılır.

Komuta ve Kontrol (Command and Control), saldırganların hedef sistem üzerinde kontrol sağlamak ve eylemlerini yönlendirmek için kullandıkları tekniklerdir. Genellikle dışarıdan bağlanan bir sunucu aracılığıyla, saldırganlar sisteme emirler gönderir ve veri alırlar. Bu iletişim, çoğu zaman şifrelenmiş olur.

Koleksiyon (Collection), saldırganların hedef sistemdeki önemli bilgileri toplama sürecidir. Bu bilgiler, kullanıcı verileri, sistem yapılandırmaları veya ağ trafiği gibi unsurları içerebilir. Bu teknik, genellikle keşif ve sızma aşamalarından sonra yapılır.

Etki (Impact), saldırganların hedef sisteme zarar vermek amacıyla uyguladıkları teknikleri ifade eder. Bu, verilerin silinmesi, sistemin çalışamaz hale getirilmesi veya kritik hizmetlerin engellenmesi gibi durumları kapsar. Amaç, hedefin işleyişini bozmak veya kullanılmaz hale getirmektir.

Yürütme (Execution), saldırganların kötü amaçlı kodlarını veya komutlarını hedef sistemde çalıştırdıkları aşamadır. Bu teknik, zararlı yazılımların, komut dosyalarının veya araçların hedefte çalıştırılmasını içerir. Yürütme, genellikle saldırganın sistemi kontrol etmek için gerçekleştirdiği ilk eylem olabilir.

Kimlik Bilgileri Erişimi (Credential Access), saldırganların sistemdeki kullanıcı adı ve şifre gibi kimlik bilgilerine ulaşmalarını sağlayan teknikleri kapsar. Bu teknik, genellikle kimlik avı saldırıları veya zayıf parola kullanımından yararlanarak gerçekleştirilir.

Yanal Hareket (Lateral Movement), saldırganların ağdaki diğer sistemlere geçiş yaparak erişim sağladıkları süreçtir. Bu, genellikle bir ağda daha fazla yetki elde etmek veya daha fazla hedefe ulaşmak için yapılır. Saldırgan, bir bilgisayarın kontrolünü ele geçirdikten sonra, ağdaki diğer makinelerde de erişim sağlamayı hedefler.

3.2. Taktikler, Teknikler ve Prosedürler (TTP'ler)

MITRE ATT&CK matris veri tabanı, siber güvenlik alanında tehdit tanımlama, risk değerlendirmesi, savunma stratejileri geliştirme, tespit ve önleme yeteneklerini artırma ve bilgi paylaşımı gibi konularda önemli bir kaynak sunulmaktadır. Gerçek dünya saldırılarına dayalı olarak düşman taktiklerini, tekniklerini ve prosedürlerini kapsayan kapsamlı bir bilgi tabanı sağlanarak, siber saldırganların kullandığı yöntemleri tanımlamaya ve anlamaya yardımcı olunmaktadır. Araştırmacılar ve uzmanlar, bu çerçeveden yararlanarak çeşitli siber tehditlerle ilişkili riskleri değerlendirebilir, potansiyel saldırı vektörlerini yapılandırılmış bir analizle inceleyebilir ve savunma önlemlerini önceliklendirebilirler (Al-Sada, Sadighian, ve Oligeri 2024).

Tablo 2'de MITRE ATT&CK Linux matrisi, Linux işletim sistemi hedef alınarak gerçekleştirilen siber saldırılarda kullanılan taktikler ve teknikler sistematik bir şekilde sınıflandırılmaktadır. Her bir taktik, saldırı sırasında gerçekleştirilmesi amaçlanan belirli bir adımı temsil etmektedir, örneğin başlangıç erişimi sağlanması, yetki artırılması ya da savunmanın kaçırılması gibi. Her taktiğe karşılık gelen teknikler, bu hedeflere ulaşmak için kullanılan özel yöntemleri içermektedir. Örneğin, başlangıç erişimi sağlamak için SSH kaba kuvvet saldırıları ya da bir yetki artırma tekniği olarak sudo caching kullanılması gibi. Bu matris kullanılarak, güvenlik uzmanları ve ağ yöneticileri, Linux tabanlı sistemlerin daha etkili bir şekilde korunması ve saldırıların erken tespit edilmesi sağlanabilir (Mitre Att&Ck 2023).

Tablo 2. MITRE ATT&CK Taktik ve Teknikler

Taktikler	Teknikler
Başlangıç Erişimi (Initial Access)	Kimlik Bilgisi Phishing (Spearphishing), Web Shell, Saldırgan Tarafından Yönlendirilen Zararlı Web Sitesi (Drive-by Compromise)
Çalıştırma (Execution)	Komut ve Betik Yorumlayıcı, PowerShell, Planlanmış Görevler/İşler (Scheduled Task/Job)
Kalıcılık (Persistence)	Başlangıç veya Oturum Açılış Otomatik Başlatmaları (Boot or Logon Autostart), Kayıt Defteri Çalıştırma Anahtarları/ Başlangıç Klasörleri (Registry Run Keys/Startup Folder), Planlanmış Görevler/İşler (Scheduled Task/Job)
Yetki Artırma (Privilege Escalation)	Açıklar Aracılığıyla Sömürme (Exploitation of Vulnerability), Sudo Önbelleklemesi (Sudo Caching), Erişim Tokeni Manipülasyonu (Access Token Manipulation)

Savunma Kaçırma (Defense Evasion)	Şifreli Dosyalar veya Bilgiler (Obfuscated Files or Information), Zaman Damgası Manipülasyonu (Timestomp), Dosya ve Dizin İzinlerinin Değiştirilmesi (File and Directory Permissions Modification)
Kimlik Bilgisi Erişimi (Credential Access)	Kaba Kuvvet Saldırısı (Brute Force), Kimlik Bilgisi Dökümü (Credential Dumping), Girdi Yakalama (Input Capture)
Keşif (Discovery)	Sistem Bilgisi Keşfi (System Information Discovery), Ağ Paylaşımı Keşfi (Network Share Discovery), Uzak Sistem Keşfi (Remote System Discovery)
Yatay Hareket (Lateral Movement)	Uzak Masaüstü Protokolü (Remote Desktop Protocol), SMB/Windows Yönetici Paylaşımları (Windows Admin Shares), Windows Uzak Yönetimi (Windows Remote Management)
Toplama (Collection)	Yerel Sistemden Veri Toplama (Data from Local System), Ekran Görüntüsü Yakalama (Screen Capture), Pano Verisi (Clipboard Data)
Veri Sızdırma (Exfiltration)	Komut ve Kontrol Kanalı Üzerinden Veri Sızdırma (Exfiltration Over Command and Control Channel), Web Servisi Üzerinden Veri Sızdırma (Exfiltration Over Web Service), Diğer Ağ Ortamları Üzerinden Veri Sızdırma (Exfiltration Over Other Network Medium)
Etkileşim (Impact)	Veri Yok Etme (Data Destruction), Servis Durdurma (Service Stop), Kaynak Kaçırma (Resource Hijacking)

MITRE ATT&CK her TTP için koruma stratejileri sunarak, kritik altyapıları korumaya yönelik çözümler sağlanmaktadır. Taktik ve teknikleri inceleyen siber güvenlik uzmanları, etkili savunma stratejileri geliştirerek, siber tehditleri önlemek ve hafifletmek için harekete geçebilirler. Belgelenen saldırı teknikleri anlaşılmakta ve organizasyonlar, tespit ve önleme yeteneklerini artırarak, bilinen saldırı kalıplarına uyumlu savunma önlemleri alarak potansiyel tehditlere karşı proaktif bir şekilde savunma sağlamaktadırlar. MITRE ATT&CK ayrıca tehdit istihbaratı verilerini ve bilgilerini paylaşma platformu olarak hizmet verilmekte olup, siber güvenlik profesyonellerinin yeni bilgileri bilgi tabanına entegre etmelerine olanak tanınmakta ve tehdit profilleri, taktikler ve tekniklerle güncellenmektedir (Al-Sada, Sadighian, ve Oligeri 2024).

Sonuç olarak, MITRE ATT&CK matrisi, siber güvenlikte tehdit modelleme ve savunma stratejileri için değerli bir kaynak olarak sunulmakta olup, siber tehditlerin anlaşılması, analiz edilmesi ve hafifletilmesi konularında yapılandırılmış bir çerçeve sağlanmaktadır.

3.3. Matrisin Siber Güvenlikteki Önemi

MITRE ATT&CK matrisi, siber güvenlik alanında çok önemli bir araç olarak kabul edilmektedir. MITRE tarafından geliştirilen bu matris, saldırganların kullanabileceği taktik ve teknikleri sistemlerin savunmasını güçlendirmek amacıyla tanımlar. Bu

matris, savunma ekiplerine saldırıların nasıl gerçekleşebileceği konusunda kapsamlı bir rehber sunmakta ve bu sayede savunma stratejilerinin oluşturulması ve güçlendirilmesinde yardımcı olunmaktadır.

MITRE ATT&CK matrisi, saldırganların kullanabileceği taktikleri ve bu taktiklerin gerçekleştirilmesi için kullanılabilecek teknikleri detaylı olarak listelemektedir. Bu, güvenlik ekiplerine saldırıların nasıl ilerleyebileceği konusunda bir anlayış kazandırmakta ve bu taktik ve tekniklerin izlerini sürmelerine yardımcı olmaktadır. MITRE ATT&CK matrisi aynı zamanda, güvenlik olaylarını inceleme ve analiz etme sürecinde de önemli bir kılavuz olarak hizmet etmektedir. Saldırıların izleri sürülerek, saldırıların detayları anlaşılmakta ve sistemdeki zayıf noktalar tespit edilmektedir. Bu sayede, olaylara hızlı bir şekilde yanıt verilmesi ve sistemin daha güvenli hale getirilmesi sağlanmaktadır.

MITRE ATT&CK matrisi, siber güvenlik alanında kritik bir araç olarak kabul edilmektedir çünkü savunma stratejilerinin oluşturulması, güçlendirilmesi ve güvenlik olaylarının analiz edilmesi süreçlerinde güvenlik ekiplerine büyük ölçüde yardımcı olunmaktadır. Bu matris, güvenlik uzmanlarına saldırıların anlaşılması ve etkili bir şekilde savunulması için gerekli olan bilgileri ve yönergeleri sunmaktadır.

4. KULLANILAN ARAÇLAR VE TEKNOLOJİLER

Linux tabanlı sistemlerin güvenliği için bir dizi araç kullanılmaktadır. Bu araçlar, güvenlik izleme, saldırgan davranışlarının analizi, güvenlik denetimi, olay izleme ve saldırı simülasyonları gibi çeşitli amaçlarla tercih edilmektedir. Bu bölümde, Wazuh, T-Pot Balküpü, Auditd (The Linux Audit Daemon) ve Atomic Red Team gibi Linux platformunda kullanılan bazı güvenlik araçları incelenmektedir.

Bu makalede, Linux platformlarına yönelik yapılan siber saldırılar, balküpü sistemleri aracılığıyla toplanmış ve bu saldırılar, MITRE ATT&CK matrisine dayalı olarak analiz edilmiştir. Saldırılara ait log verileri, Wazuh platformunda işlenmiş ve bu verilerle saldırılara yönelik kod çözücüler ve kurallar oluşturulmuştur. Literatürde, Linux tabanlı sistemler üzerinde balküpü kullanılarak yapılan saldırıların bu şekilde MITRE ATT&CK çerçevesi ile adreslenmesi ve Wazuh platformunda analiz edilmesi konusunda daha önce benzer bir çalışma yapılmamıştır. Bu nedenle, yapılan bu çalışma, Linux tabanlı balküpleri ve Wazuh platformu ile saldırıların tespiti ve analiz edilmesi bakımından özgün bir katkı sunmaktadır.

Wazuh ve T-Pot gibi araçlar, bu çalışmada stratejik olarak seçilmiştir. Wazuh, açık kaynaklı bir SIEM (Güvenlik Bilgisi ve Olay Yönetimi) çözümü olarak, log verilerinin toplanması, saldırı tespiti ve güvenlik yönetimi konularında güçlü özellikler sunmaktadır. Linux platformları üzerinde gerçekleştirilen saldırıların etkin bir şekilde tespit edilmesi ve analiz edilmesi için Wazuh tercih edilmiştir. T-Pot ise, balküpü teknolojisinin geniş bir yelpazede saldırıları simüle etmesi ve çok sayıda saldırı tipi ile etkileşimde bulunabilmesi nedeniyle kullanılmıştır. T-Pot, Elasticsearch ve Kibana gibi araçlarla güçlü bir entegrasyon sağlayarak, saldırılara dair derinlemesine veriler elde edilmesini sağlamaktadır. Bu araçların, Linux tabanlı sistemlerdeki siber tehditlere dair

analizler yapılırken bir arada kullanılması, literatürde bu tür bir kombinasyonun daha önce denenmemiş olması açısından önemli bir yenilik taşımaktadır.
Wazuh, açık kaynaklı bir güvenlik izleme ve yönetim platformu olarak kullanılmaktadır. Sistemlerin güvenliği sağlanmak amacıyla log toplama, anomali tespiti, dosya bütünlüğü denetimi, zararlı yazılım analizi ve güvenlik yapılandırması denetimi gibi özellikler sunulmaktadır. Wazuh, aynı zamanda gerçek zamanlı saldırı tespiti sağlanarak saldırıların kaydı tutulmakta ve olaylar merkezi bir sunucuda toplanmaktadır.

T-Pot balküpü, hazır paket çözüm sunması, çok protokollü destek, merkezi izleme ve analiz imkanı, ve gerçek zamanlı saldırı tespiti gibi avantajlarla geleneksel balküplerine kıyasla daha kapsamlı ve etkili bir yaklaşım sağlamaktadır (Mohd Fuzi vd. 2024). T-Pot, birden fazla balküpü içeren bir Linux güvenlik aracı olarak kullanılmaktadır. Balküpleri, saldırganların davranışlarını izlemek ve analiz etmek amacıyla kullanılmaktadır. T-Pot, siber saldırganların ağ üzerinde gerçekleştirdiği faaliyetleri izlemek ve bu verilerle güvenlik açıklarını belirlemek için kullanılmıştır. Balküpü, saldırı türlerinin çeşitliliği ve saldırganların yöntemleri hakkında detaylı bilgiler elde edilmesini sağlamaktadır.

Balküpleri, siber güvenlikte hem erken tehdit tespiti sağlayarak gerçek sistemlere yönelik saldırıların engellenmesine yardımcı olunur, hem de saldırganların davranışları izlenerek güvenlik uzmanlarının onların kullandığı yöntemler ve stratejiler daha iyi anlaşılmaktadır. Bu sayede sıfırıncı gün saldırıları gibi karmaşık tehditler düşük yanlış alarm oranlarıyla tespit edilebilir ve aynı zamanda araştırmacılara, yeni güvenlik araçlarının geliştirilmesi için değerli veriler sunularak genel güvenlik duruşu güçlendirilmektedir (Javadpour vd. 2024).

Auditd, Linux sistemlerinde güvenlik olaylarını izlemek ve kaydetmek için kullanılan bir araç olarak kullanılmaktadır. Sistem üzerinde gerçekleşen tüm önemli olaylar, örneğin kullanıcı işlemleri, dosya erişimleri ve ağ bağlantıları kaydedilmektedir. Bu veriler, saldırı tespitinde ve sistemdeki olağan dışı aktivitelerin belirlenmesinde faydalı olmaktadır. Ayrıca, sistem yöneticilerine yasal uyumluluk ve denetim amaçları için gerekli veriler sağlanmaktadır.

Atomic Red Team, güvenlik testi ve saldırı simülasyonu yapmak için kullanılan açık kaynaklı bir araç olarak kullanılmaktadır. Linux sistemlerinde saldırganların yöntemlerini simüle etmek ve sistemin savunma yeteneklerini test etmek amacıyla kullanılmaktadır. Atomic Red Team, önceden tanımlanmış saldırı tekniklerine dayalı testler sağlamakta, sistemdeki zayıf noktaların tespit edilmesini ve savunmaların güçlendirilmesini sağlamaktadır.

Bu araçlar, Linux tabanlı sistemlerin güvenliğinin sağlanması, saldırıların tespit edilmesi ve önlenmesi için kritik öneme sahiptir. Her biri, farklı güvenlik seviyelerinde ve ihtiyaçlarda çeşitli özellikler sunarak Linux tabanlı altyapıların savunmalarını güçlendirmeye yardımcı olmaktadır.

4.1. Wazuh: Güvenlik İzleme ve Log Yönetimi

Wazuh, günlük veri analizi, bir BT altyapısındaki varlıkların faaliyetleri hakkında bilgi edinmek için farklı kaynaklardan oluşturulan günlüklerin incelenmesini içermektedir. Wazuh, açık kaynak kodlu bir SIEM (Security Information and Event Management) çözümü olarak kullanılmaktadır ve mimarisi çoğunlukla izlenen ana makinalarda çalışan ajanlara dayanır; bu ajanlar, güvenlik bilgilerini merkezi SIEM sunucusuna gönderir (Zahid vd. 2023).SIEM sunucusu, ayrı işlevleri tek bir ajan ve platform mimarisi içinde birleştirerek uç nokta güvenliği, tehdit istihbaratı, detaylı güvenlik operasyonları ve bulut güvenliği sağlamaktadır.

Tehdit tespiti ve müdahalesi, düzenlemelere uygunluğun sağlanması ve sistem performansı sorunlarının belirlenmesi için izlenen varlıklardan günlüklerin gerçek zamanlı olarak toplanması ve işlenmesi sağlanmıştır. Wazuh, bulut, şirket içi, sanallaştırılmış ve konteynerli ortamlardaki güvenlik tehditlerine karşı koruma sağlanmaktadır.

Wazuh, kendisine ajanları üzerinden ve syslog olarak gönderilen günlükleri analiz etmek için önceden tanımlanmış kod çözücülere (decoder) ve kurallara (rules) sahiptir. Bu kod çözücüler ve kurallar, farklı tehdit modellerini işlemek ve tespit etmek için PCRE (Perl Compatible Regular Expressions) desteği ile düzenli ifadeler kullanmaktadır. Wazuh, toplanan günlüklerden ilgili alanları çıkarmak için kod çözücüleri kullanmaktadır. Bu alanlar, IP adresleri, bilgisayar adları, zaman damgaları, kullanıcı adları, bağlantı noktaları, MAC adresleri ve diğer ilgili veri alanlarını içermektedir. Wazuh, toplanan günlüklerin kodunu çözdükten sonra, bunları kullanıma hazır kurallarıyla karşılaştırmaktadır. Bir kural, kod çözülmüş bir günlükle eşleştiğinde, Wazuh kontrol panelinde uyarılar tetiklenmektedir. Bu araştırma kapsamında, balküpleri üzerinden gelen günlükler için özel kod çözücü ve kurallar tanımlanmıştır.

Wazuh aracıları, sistem günlükleri, uygulama günlükleri ve ağ günlükleri gibi çeşitli kaynaklardan günlük verilerini toplamak amacıyla sunucular, iş istasyonları ve IoT cihazları gibi uç noktalara dağıtılmaktadır. Toplanan günlük verileri, SIEM sistemiyle tutarlılığını ve uyumluluğunu sağlamak için Wazuh aracıları tarafından normalleştirilmektedir. Bu süreç, daha kolay analiz için günlük formatlarının standartlaştırılmasını içermektedir (Hussein ve Hamza 2022).

Wazuh, günlük toplama ve analiz yeteneklerinin geliştirilmesi için SIEM çözümleriyle entegre edilebilen açık kaynaklı bir güvenlik izleme platformu olarak kullanılmaktadır. Toplanan günlük verileri, SIEM sistemiyle tutarlılık ve uyumluluk sağlanması için Wazuh aracıları tarafından normalleştirilmektedir. Bu süreç, daha kolay analiz için günlük formatlarının standartlaştırılmasını içermektedir. Normalleştirilen günlük verileri, daha sonra ağdaki birden fazla aracıdan günlüklerin toplanması ve işlenmesi için merkezi bir sunucu görevi gören Wazuh yöneticisine iletilmektedir. Wazuh yöneticisi, güvenlik olaylarının, anormalliklerin ve potansiyel tehditlerin belirlenmesi için önceden tanımlanmış kurallar ve korelasyon mekanizmaları kullanılarak günlük verilerini gerçek zamanlı olarak analiz etmektedir. Bir güvenlik olayı tespit edildiğinde, Wazuh, güvenlik ekiplerine veya yöneticilere potansiyel güvenlik sorunu hakkında uyarmak için uyarılar ve bildirimler oluşturmaktadır. Wazuh, kapsamlı bir güvenlik

izleme ve olay müdahale yeteneği sağlanması için ELK Stack (Elasticsearch, Logstash, Kibana) gibi popüler SIEM çözümleriyle veya diğer ticari SIEM ürünleriyle entegre edilebilmektedir (Hussein ve Hamza 2022).

4.2. T-pot Balküpü: Saldırgan Davranışlarının Analizi

Güvenlik uzmanları, balküpü etkileşimlerinden toplanan verilerin günlüğe kaydedilmesi ve analiz edilmesiyle, saldırganların taktikleri ve stratejileri hakkında değerli bilgiler edinilebilmektedir. Bu etkileşimler, yeni saldırı eğilimleri, güvenlik açıkları ve kötü amaçlı yazılım örnekleri gibi tehdit istihbaratını toplamak için önemli bir kaynak teşkil etmektedir. Elde edilen bilgiler, kuruluşların güvenlik duruşlarını iyileştirmelerine ve ortaya çıkan tehditlere karşı etkili karşı önlemler geliştirmelerine yardımcı olabilmektedir. Araştırmacılar, balküpü sistemlerinin kullanılmasıyla parmak izi alma ve tanımlama tekniklerini incelemekte ve geliştirmektedirler. Bu sayede, güvenlik uzmanları, saldırganların balküpleri nasıl tespit etmeye çalıştıklarını anlayarak, aldatma tekniklerini geliştirebilmekte ve balküpü dağıtımlarının etkinliği artırılabilmektedir. Balküpleri, düşmanların nasıl çalıştığı ve düşündüğü hakkında değerli bilgiler sağlamakta hizmet etmektedir. Ayrıca, güvenlik uzmanları bu etkileşimler kullanılarak, saldırgan davranışları incelenebilmekte, güvenlik savunmaları test edilebilmekte ve siber güvenlik tehditleri ile savunmalar üzerine araştırmalar yapılabilmektedir (Srinivasa, Pedersen, ve Vasilomanolakis 2023).

T-Pot balküpü, çeşitli balküpü teknolojilerinin tek bir platformda birleştirilmesiyle saldırgan davranışlarının analiz edilmesine olanak tanınmaktadır. Balküpleri, saldırganları çekmek ve davranışlarını gözlemlemek için oluşturulmuş sunucu veya sistemler olarak kullanılmaktadır. T-Pot, Linux platformlarına yapılan saldırıların tespit edilmesi ve analiz edilmesi için tasarlanmış açık kaynaklı bir balküpü platformu olarak tanımlanmaktadır. Güvenlik araştırmacıları, sızma test uzmanları ve olaya müdahale edenler, saldırganlar tarafından kullanılan TTP (Taktikler, Teknikler ve Prosedürler) yöntemlerini anlamak için bu platformu güçlü bir araç olarak kullanmaktadırlar. Balküpü, yetkisiz erişimi veya kötü niyetli etkinlikleri çekmek ve tespit etmek amacıyla kasıtlı olarak savunmasız bırakılan bir yem sistemi veya ağ kaynağı olarak tasarlanmaktadır. Bu sistemler, saldırganlar, yöntemleri ve motivasyonları hakkında bilgi toplamak için kullanılmaktadır.

T-Pot, çok sayıda protokole ve saldırı türüne karşı hassasiyet göstermekte ve ağ güvenliği ekiplerinin saldırganların taktiklerini daha iyi anlamalarına ve savunma stratejilerini geliştirmelerine yardımcı olmaktadır. Saldırganların kullandığı tekniklerin tespit edilmesi ve analiz edilmesi, savunmaların güçlendirilmesine olanak tanımakta ve güvenlik uzmanlarına değerli bilgiler sunmaktadır. T-Pot gibi balküpü platformları, saldırganların davranışlarını gözlemlemek, yeni saldırı tekniklerini keşfetmek ve güvenlik açıklarını belirlemek için önemli bir kaynak oluşturmaktadır.

4.3. Auditd: Güvenlik Denetimi ve Olay İzleme

Auditd, Linux platformlarında güvenlik denetimi ve olay izleme amacıyla kullanılan önemli bir araç olarak tanımlanmaktadır. Auditd, sistem çağrılarını izleyerek şüpheli etkinlikleri tespit etmekte ve bu etkinlikleri günlük dosyalarına kaydetmektedir. Bu sayede, sistem yöneticileri ve güvenlik uzmanları, potansiyel saldırı girişimlerini hızlı

bir şekilde tespit edebilmekte ve bu verileri analiz ederek gerekli önlemleri alabilmektedirler. Auditd aracılığıyla, sistem üzerinde gerçekleşen tüm kritik olaylar, örneğin kullanıcı işlemleri, dosya erişimleri, ağ bağlantıları ve diğer güvenlik açısından önemli aktiviteler kaydedilmektedir. Bu günlükler, sistemdeki olağan dışı hareketleri belirlemek, izinsiz erişimi engellemek ve genel güvenlik durumunu iyileştirmek için kullanılabilmektedir. Auditd, aynı zamanda yasal uyumluluk ve denetim amaçları için de önemli bir kaynak sağlamakta, böylece kuruluşlar düzenlemelere uygunluklarını denetleyebilmektedirler.

4.4. Atomic Red Team: Saldırı Simülasyonları

Atomic Red Team, MITRE ATT&CK matrisine dayalı olarak gerçek dünya saldırılarını simüle etmek için kullanılan bir test çerçevesi olarak tanımlanmaktadır. Bu araç, saldırganların TTP'lerini (Taktikler, Teknikler ve Prosedürler) taklit ederek, savunma mekanizmalarının etkinliğini test etmeye yardımcı olmaktadır. Atomic Red Team, savunma ekiplerinin mevcut güvenlik önlemlerinin zayıf noktalarını belirlemelerine ve bu önlemleri güçlendirmelerine olanak tanımaktadır. Saldırı simülasyonları, ekiplerin gerçek dünyada karşılaşabilecekleri tehditlere karşı daha hazırlıklı olmalarını sağlamakta ve savunma stratejilerinin geliştirilmesinde önemli bir rol oynamaktadır. Bu sayede, savunma ekipleri, daha etkili müdahale planları oluşturabilmekte ve güvenlik altyapılarını iyileştirerek olası saldırılara karşı daha dirençli hale gelebilmektedirler.

5. SALDIRI PLANLAMA

5.1. Test Ortamının Hazırlanması

Bu çalışmada, T-Pot Balküpü platformu kullanılarak, siber saldırı senaryoları simüle edilmiştir ve bu saldırılar, Wazuh SIEM sistemiyle izlenip analiz edilmiştir. T-Pot, çeşitli balküpü uygulamalarını bir araya getirerek merkezi bir yönetim konsolunda izleme olanağı sunan entegre bir çözüm olarak tanımlanmıştır. T-Pot, sanal bir makine üzerine yüklenmiş ve gerekli bağımlılıklar ile yapılandırma işlemleri tamamlanmıştır. Balküpü sisteminin güvenlik etkinliklerinin izlenmesi amacıyla, T-Pot üzerine Wazuh ajanı kurulumu yapılmıştır. Bu ajan, balküplerinde bulunan tüm aktiviteleri toplayarak merkezi Wazuh sunucusuna iletmiştir. Wazuh, bu logları merkezi sunucusunda çözümleyerek anlamlı hale getirmiş ve saldırıların detaylı analizi için özel olarak oluşturulmuş kurallar kullanılarak değerlendirilmiştir. Elde edilen veriler, MITRE ATT&CK matrisine göre kategorize edilerek hangi saldırı tekniklerinin ve taktiklerinin kullanıldığı belirlenmiş ve raporlanmıştır.

Saldırı senaryolarının kapsamı genişletilmek amacıyla, iki adet son kullanıcı Linux makinesi üzerinde izleme ve saldırı simülasyonları gerçekleştirilmiştir. Bu makineler, kullanıcı aktivitelerini ve simüle edilen saldırıları izlemek üzere yapılandırılmıştır. Çalışmada, her iki makineye de Wazuh ajan kurulumu yapılmış ve ajan, makinelerdeki tüm etkinlikleri ve güvenlik olaylarını merkezi Wazuh sunucusuna iletmiştir. Kullanıcı aktiviteleri, dosya erişimleri, komut çalıştırmaları ve ağ bağlantıları gibi kritik işlemler sürekli olarak izlenmiş ve kaydedilmiştir.

Atomic Red Team araçları kullanılarak, MITRE ATT&CK matrisine dayanan çeşitli saldırı teknikleri simüle edilmiştir. Bu simülasyonlar, gerçek saldırı senaryolarını taklit ederek güvenlik önlemlerinin etkinliğini test etmek amacıyla gerçekleştirilmiştir. Simülasyonlar sırasında üretilen loglar, Wazuh ajanı tarafından toplanmış ve merkezi Wazuh sunucusuna iletilmiştir. Bu loglar, Wazuh sunucusunda çözümlenmiş ve anlamlı hale getirilmiştir. Çözümlenen loglar, MITRE ATT&CK matrisine göre haritalanarak kullanılan saldırı teknikleri ve bu tekniklerin nasıl tespit edildiği belirlenmiştir.

Elde edilen sonuçlar, detaylı raporlar halinde güvenlik ekiplerine iletilmiş ve siber güvenlik duruşu değerlendirilmiştir. Bu süreç, balküpü ve son kullanıcı makineleri üzerinde gerçekleştirilen saldırı simülasyonlarının etkin bir şekilde izlenmesini ve analiz edilmesini sağlamış, böylece kuruluşun savunma yetenekleri güçlendirilmiş ve siber güvenlik stratejilerinin etkinliği arttırılmıştır.

5.2. Senaryo Belirleme ve Hedefleme

MITRE ATT&CK, siber saldırganların ağlar üzerinde hedeflerine ulaşmak için kullandıkları taktik ve tekniklerin ayrıntılı bir şekilde tanımlandığı kapsamlı bir bilgi tabanı olarak kullanılmaktadır. Bu matris, her bir taktiğin ve bu taktiğe yönelik saldırı tekniklerinin sistematik bir şekilde sınıflandırılması sağlanmakta, böylece güvenlik uzmanlarının, belirli bir saldırı türünün nasıl gerçekleştirildiği ve bu saldırının nasıl tespit edilebileceği anlaşılabilmektedir.

Balküpleri, saldırganların ağlara sızma girişimlerinin simüle edilmesi için kullanılan özel sistemler olarak tanımlanmaktadır. Balküpleri, saldırganların cezbedilmesi ve onların saldırı yöntemlerinin gözlemlenmesi için kasıtlı olarak savunmasız bırakılmış sistemler olarak yerleştirilmektedir. Bu tür sistemler, saldırganların faaliyetlerinin izlenmesi ve analiz edilmesi için önemli bir araç olarak kullanılmaktadır.

Balküpü üzerinden alınan saldırgan aktiviteleri, MITRE ATT&CK matrisine dayalı olarak sınıflandırılabilmektedir. Örneğin, bir saldırgan, bir balküpüne erişmeye çalışırken belirli araçlar veya teknikler kullanabilmektedir. Bu teknikler, MITRE ATT&CK matrisindeki belirli saldırı teknikleriyle eşleştirilebilmektedir. Böylece, balküpü üzerindeki aktiviteler, kullanılan saldırı taktikleri ve teknikleri ile bağlantılı olarak izlenebilmekte ve analiz edilebilmektedir.

Örneğin, bir saldırgan, “Initial Access” taktiği altında, bir balküpüne sızmaya çalışırken kimlik avı veya kamusal yüzeydeki uygulama zafiyetlerinin kullanılması gibi teknikler kullanabilmektedir. Bu aktiviteler, MITRE ATT&CK matrisinde belirtilen teknikler ile ilişkilendirilerek daha derinlemesine analiz edilebilmektedir. Balküpü üzerinden elde edilen bu tür veriler, güvenlik uzmanlarının saldırganların ağlara yönelik niyetlerini ve yeteneklerini anlamalarına yardımcı olmakta ve bu sayede savunma stratejilerinin güçlendirilmesine olanak tanımaktadır.

Sonuç olarak, balküpü üzerinden toplanan veriler, MITRE ATT&CK matrisine dayalı olarak sınıflandırıldığında, saldırıların tespiti ve analizi daha etkin hale getirilmektedir. Bu, saldırganların ağlara yönelik davranışlarının daha iyi anlaşılmasını sağlamakta ve bunlara karşı savunma önlemlerinin geliştirilmesi için önemli bir kaynak sunmaktadır.

5.3. Saldırı Tekniklerinin Seçimi

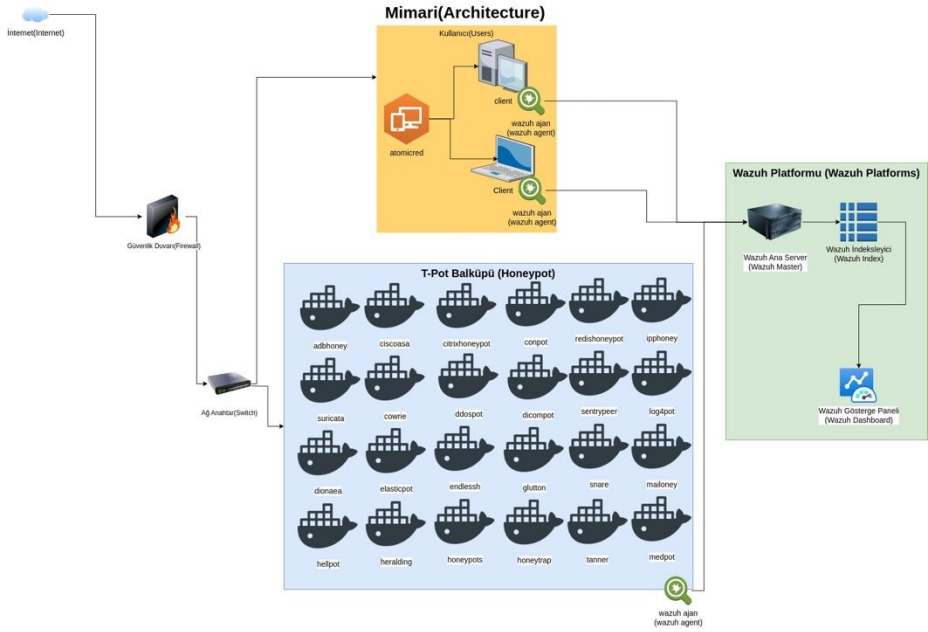
MITRE ATT&CK matrisi, siber güvenlikte saldırganların ağlar üzerindeki hedeflerine ulaşmak için başvurdukları taktik ve tekniklerin ayrıntılı bir şekilde tanımlandığı kapsamlı bir bilgi tabanı olarak kullanılmaktadır. Bu matris, saldırganların ağlara sızma girişimlerinin ve kullandıkları yöntemlerin anlaşılmasına yardımcı olacak önemli bir kaynak sağlamakta, aynı zamanda bu tür aktivitelerin belirli taktikler ve tekniklerle ilişkilendirilebilmesini sağlamaktadır. Örneğin, bir saldırganın bir balküpünde erişim sağlamaya çalışırken kullandığı belirli araçlar veya taktikler, MITRE ATT&CK matrisinde tanımlanan saldırı teknikleriyle eşleştirilebilmektedir. Bu sayede, balküpü üzerinden yapılan saldırılar tespit edilip analiz edilerek, saldırganların ağlara yönelik niyetleri ve yetenekleri daha iyi anlaşılmaktadır.

Siber saldırı süreci, genellikle bir dizi aşamadan oluşmakta olup, her bir aşama, saldırganın hedeflerine ulaşmak için izlediği belirli bir stratejiyi temsil etmektedir. İlk Erişim aşamasında, hedef sisteme ilk kez sızılmakta, Çalıştırma aşamasında ise hedef sistem üzerinde zararlı yazılım veya komutlar çalıştırılmakta, Süreklilik aşamasında, saldırganlar sistemde kalıcı olabilmek için gerekli önlemleri almaktadır. Yetki Yükseltme aşaması, saldırganların daha yüksek erişim hakları elde etmek amacıyla gerçekleştirdiği faaliyetleri kapsamaktadır. Savunmadan Kaçınma aşamasında, güvenlik önlemleri atlatılmakta, Kimlik Bilgisi Erişimi aşamasında, saldırganlar sistemdeki kullanıcı bilgilerini ele geçirmeye hedeflemekte, Keşif aşamasında ise sistem ve ağ hakkında bilgi toplama faaliyetleri gerçekleştirilmektedir. Yanal Hareket aşamasında, ağda yayılma işlemleri başlatılmakta, Toplama aşamasında, hedef sistemdeki hassas veriler toplanmaktadır. Komanda ve Kontrol aşamasında, uzaktan erişim sağlanarak sistem kontrol altına alınmakta, Veri Sızdırma aşamasında ise elde edilen veriler dışarıya çıkarılmaktadır. Son olarak, Etkileme aşamasında, hedef sistem üzerinde zarar verici eylemler gerçekleştirilmektedir.

Bu taktikler, siber güvenlik uzmanlarının saldırıların aşamalarını daha iyi anlamalarını sağlamakta ve etkili savunma stratejilerinin geliştirilmesi kolaylaştırılmaktadır. MITRE ATT&CK matrisine dayalı olarak yapılan analizler, saldırganların hangi teknikleri kullandığının belirlenmesini sağlamakta ve bu tekniklerin nasıl tespit edilebileceği konusunda yol gösterici olmaktadır. Bu sayede, savunma ekipleri, ağlarını daha güvenli hale getirebilmek için her aşama için uygun tespit ve önleme yöntemlerinin belirlenmesine olanak tanımakta ve saldırılara karşı etkin bir savunma stratejisi geliştirilmesi sağlanmaktadır (Mitre Att&Ck 2023).

6. SALDIRI UYGULANMASI

Saldırı senaryolarının planlanması aşamasından sonra, bu bölümde belirlenen senaryoların gerçekleştirilmesi ve saldırıların uygulanması adımlarının ele alınacağı belirtilmiştir. Bu süreçte, Wazuh, T-pot Balküpü, Auditd ve Atomic Red Team gibi çeşitli araçların kullanılması ifade edilmiştir. Çalışma için oluşturulan simülasyon mimarisinin Şekil 1'de görüleceği belirtilmiştir.



Şekil 1. Çalışma için Oluşturulan Simülasyon Mimarisi

6.1. Wazuh ile İzleme ve Tespit

Wazuh, güvenlik izleme ve log yönetimi için kullanılan bir platform olarak tanıtılmaktadır. Bu bölümde, Wazuh'un nasıl kurulacağı ve yapılandırılacağı incelenmiş olacak, ardından saldırıların izlenmesi ve tespit edilmesi süreci detaylı olarak ele alınacaktır.

Wazuh, açık kaynaklı bir güvenlik bilgi ve olay yönetimi çözümü olarak açıklanmaktadır. Wazuh, merkezi bir izleme ve yönetim platformu sağlayarak güvenlik olaylarının tespit edilmesine, analiz edilmesine ve yanıtlanmasına yardımcı olmaktadır. Wazuh'un temel bileşenlerinden biri olan kod çözücü ve kural yapısı, güvenlik olaylarını anlamak ve uygun aksiyonları almak için kritik öneme sahip olduğu belirtilmektedir. Kod çözücüler, Wazuh'un farklı formatlardaki günlük kayıtlarını anlayıp standart bir formata çevirmesini sağlamaktadır. Herhangi bir log kaynağından gelen veriler, önce kod çözücü tarafından işlenmektedir. Kod çözücüler, belirli bir format veya düzeni tanıyarak log verilerini yapılandırılmış bir forma dönüştürmektedir. Kod çözücüler, logun hangi log kaynağından geldiğini belirlemektedir. Log verileri, yapılandırılmış ve anlaşılabilir bir formata dönüştürülmektedir. Eşleşen kurallara göre alarmlar oluşturulmakta ve tanımlı aksiyonlar (örneğin, e-posta gönderme, komut çalıştırma) gerçekleştirilmektedir. Wazuh'un kod çözücü ve kural yapısı, log verilerini anlamlandırma ve güvenlik olaylarına uygun yanıt verme sürecinin temel bileşenleri olarak vurgulanmaktadır. Kod çözücüler log verilerini belirli bir formata dönüştürürken, kurallar bu verileri analiz etmekte ve güvenlik olaylarını yönetmektedir. Bu yapı, güvenlik operasyonlarının daha etkili ve verimli hale getirilmesini sağlamaktadır.

6.2. T-pot Balküpü ile Saldırgan Davranışlarının Kaydedilmesi

Ağ güvenliğinde bal noktaları kullanmanın temel amacı, saldırganların TTP'ler hakkında bilgi toplamak için onlarla etkileşime geçmek ve kandırılmak olarak belirtilmektedir. Bal noktaları, meşru hedefler gibi görünen ancak aslında izole edilmiş ve izlenen ortamlar olan tuzak sistemler olarak kasıtlı olarak konuşlandırılmaktadır. Güvenlik uzmanları, saldırganların bal noktalarıyla etkileşime girmeye ikna edilerek davranışlarının gözlemlenip analiz edilmesini sağlayabilmekte, saldırı yöntemlerinin anlaşılması ve genel ağ güvenliğinin artırılması için değerli istihbarat toplanabilmektedir. Bal noktaları, istenmeyen e-postalar, kimlik avı, kimlik hırsızlığı, hizmet reddi saldırıları ve hatta fidye yazılımı faaliyetleri gibi çeşitli siber suçların tespit edilmesine ve incelenmesine yardımcı olabilmektedir. Ek olarak, balküpleri, saldırgan davranışının tanımlanması, saldırı eğilimlerinin bulunması ve toplanan içgörülere dayanarak güvenlik önlemlerinin iyileştirilmesi için kullanılabilmektedir (Amal ve Venkadesh 2023).

6.3. Auditd ile Sistem Çağrılarının İzlenmesi

Siber saldırı senaryolarının planlanması kapsamında, son kullanıcı Linux makinelerine auditd (Linux Audit Daemon) yüklenmiş ve bu uygulama ile özel auditd kuralları tanımlanmıştır. Auditd, Linux platformlarında çeşitli güvenlik olaylarını izlemek ve kaydetmek için kullanılan güçlü bir araç olarak açıklanmıştır. Bu çalışma, son kullanıcı makinelerinde kullanıcıların ve/veya dışarıdan erişim sağlayan saldırganların komut satırı üzerinden gerçekleştirdikleri işlemleri denetlemek amacıyla yapılmıştır.

İlk olarak, her iki linux makinesine auditd kurulumu yapılmıştır. Auditd kurulduktan sonra, kullanıcı ve saldırgan aktivitelerini izlemek için özel auditd kuralları tanımlanmıştır. Auditd'nin yapılandırılması tamamlandıktan sonra, sistemde gerçekleştirilen tüm komut satırı işlemleri kontrol edilmiş ve detaylı loglar oluşturulmuştur. Bu loglar, her komut çalıştırma işleminin zamanını, hangi kullanıcı tarafından gerçekleştirildiğini ve hangi komutların çalıştırıldığını içermektedir. Bu loglar, Wazuh ajanları aracılığıyla merkezi Wazuh sunucusuna iletilmektedir. Wazuh ajanı, Linux makinesinde sürekli çalışarak auditd tarafından oluşturulan logları toplamakta ve Wazuh sunucusuna göndermektedir. Wazuh sunucusunda, bu loglar çeşitli çözümleyici ve kurallar kullanılarak anlamlı hale getirilmektedir. Bu kod çözücü ile edinilen veriler, MITRE ATT&CK matrisi göre haritalanmaktadır. MITRE ATT&CK matrisi, siber saldırganların saldırı amaçlı kullandıkları teknik ve taktikleri içeren kapsamlı bir çerçeve olarak tanımlanmaktadır. Wazuh, bu verileri MITRE ATT&CK tekniklerine göre sınıflandırmakta ve hangi saldırı tekniklerinin kullanıldığını belirlemektedir. Sonuç olarak, toplanan ve çözümlenen loglar MITRE ATT&CK matrisine göre haritalandırılmakta ve raporlanmaktadır. Bu raporlar, hangi saldırı tekniklerinin kullanıldığını ve bu tekniklerin nasıl tespit edildiğini göstermektedir. Raporlar, güvenlik ekiplerine iletilerek güvenlik açıklarının belirlenmesi ve giderilmesi için kullanılmaktadır. Bu süreç, son kullanıcı makineleri üzerinde gerçekleştirilen saldırı simülasyonlarının etkin bir şekilde izlenmesini ve analiz edilmesini sağlamaktadır. Bu sayede, kuruluşların siber güvenlik duruşu değerlendirilmekte ve iyileştirilmektedir.

Atomic Red Team, kuruluşların siber güvenlik seviyelerinin ölçülmesi, değerlendirilmesi ve iyileştirilmesi amacıyla kullanılan bir açık kaynaklı saldırı simülasyon uygulaması olarak tanımlanmaktadır. Bu uygulama, MITRE ATT&CK matrisine dayanan çeşitli saldırı tekniklerinin ve taktiklerinin simüle edilmesine olanak tanımaktadır. Atomic Red Team, güvenlik ekiplerinin olası saldırılara karşı hazırlıklı olmalarını sağlarken, mevcut güvenlik kontrollerinin etkinliğinin de test edilmesini sağlamaktadır. Her bir atomik test, belirli bir saldırı tekniğini hedef almakta ve bu tekniklerin güvenlik kontrolleri üzerindeki etkisi değerlendirilmek üzere tasarlanmaktadır. Böylece, güvenlik açıkları tespit edilip giderilerek kuruluşun siber güvenlik durumu sürekli olarak iyileştirilebilmektedir.

Atomic Red Team'in kullanımı, kuruluşların tehdit avlama ve olay müdahale kapasitelerinin geliştirilmesine önemli katkılar sunmaktadır. Testlerin düzenli olarak uygulanması, güvenlik ekiplerine gerçek saldırı senaryoları üzerinde çalışma imkânı sağlamakta ve güvenlik önlemlerinin etkinliğinin ölçülmesine olanak tanımaktadır. Ayrıca, bu simülasyonlar sayesinde güvenlik açığı yönetimi süreçleri daha etkin hale getirilmekte ve personelin bilgi birikimi artırılmaktadır. Atomic Red Team'in sağladığı yapılandırılmış ve tekrarlanabilir testler, kuruluşların siber tehditlere karşı daha dirençli olmalarını sağlamakta ve güvenlik olgunluğunun artırılmasına yardımcı olmaktadır. Bu bağlamda, Atomic Red Team, sürekli değişen tehdit ortamında kuruluşların proaktif bir güvenlik stratejisi geliştirmelerine ve uygulamalarına önemli bir destek sağlamakta bulunmaktadır.

7. SALDIRI SONUÇLARININ ANALİZİ

7.1. İzleme ve Analiz Sonuçları

Saldırıların tespit edilmesi ve analiz edilmesi sürecinden elde edilen veriler, izleme ve analiz sonuçları olarak adlandırılmaktadır. Bu veriler, saldırıların tespit edilmesi, incelenmesi ve analiz edilmesi için kullanılmaktadır. Bu bölümde, izleme ve analiz sonuçlarının nasıl değerlendirileceği ve kullanılacağı üzerinde durulmaktadır.

Tablo 3. Ttp Sayıları

TTP Kodları	Hit Sayıları
T1078 (Geçerli Hesaplar)	86.794
T1133 (Dış Uzaktan Servisler)	75.525
T1082 (Sistem Bilgisi Keşfi)	56.182
T1119 (Otomatik Veri Toplama)	56.182
T1030 (Veri Aktarım Boyut Sınırlamaları)	50.348
T1043 (Yaygın Olarak Kullanılan Portlar)	50.348
T1071 (Uygulama Katmanı Protokolü)	44.175
T1018 (Uzaktan Sistem Keşfi)	35.442
T1036 (Gizlenme)	28,520

T1041 (Komut ve Kontrol Kanalı Üzerinden Veri Sızıntısı)	28.520
T1053 (Planlanmış Görev)	28.520
T1102 (Web Servisi)	28.520
T1485 (Veri Yok Etme)	28.520
T1003 (İşletim Sistemi Kimlik Bilgisi Toplama)	27.662
T1048 (Alternatif Protokol Üzerinden Veri Sızıntısı)	6.615
T1110.001 (Kaba Kuvvet)	212
T1021.004 (Uzaktan Servisler: SSH)	116
T1020 (Otomatik Veri Sızıntısı)	99
T1529 (İşletim Sistemi Kimlik Bilgisi Toplama)	97
T1040 (Ağ Dinleme)	24
T1107 (Dosya ve Dizin İzinlerini Değiştirme)	24
T1565.001 (Depolanan Verilerin Manipülasyonu)	23
T1027 (Karmaşıklaştırma)	21
T1110 (Kaba Kuvvet)	20
T1059 (Komut ve Betik Yorumlayıcıları)	18
T1526 (Ağ Servisinde Hizmet Reddi)	6

T-pot üzerinde toplanan saldırılar, Wazuh platformu aracılığıyla MITRE ATT&CK matrisi çerçevesindeki TTP'ler ile detaylı bir şekilde ilişkilendirilmiştir. Bu süreçte, saldırganların kullandığı belirli tekniklerin toplam hit sayıları analiz edilerek, hangi TTP'lerin daha yaygın olarak tercih edildiği ortaya konulmuştur. Bu analizler, güvenlik ekiplerinin saldırıların doğasını daha iyi anlamalarına ve hangi alanlarda daha fazla güvenlik önlemi alınması gerektiğini belirlemelerine yardımcı olmaktadır. Her bir TTP'nin hit sayısının izlenmesi, saldırıların zaman içindeki trendlerini değerlendirmek ve potansiyel zayıflıkları tespit etmek açısından büyük önem taşımaktadır. Böylece, toplanan veriler üzerinden stratejik kararlar alınmakta, güvenlik politikaları güncellenmekte ve sistemlerin dayanıklılığı artırılmaktadır.

Tablo 3'de belirtilen MITRE ATT&CK matris TTP'lerinin Balküpü test çalışmasında elde edilen toplam 184.750 olay analiz edilmiştir. Bu olayların her biri, siber saldırıların farklı yönlerini yansıtmakta olup, bazen birden fazla MITRE ATT&CK TTP'si (Taktik, Teknik ve Prosedür) ile eşleştirilmiştir. Bu durum, saldırganların karmaşık ve çok katmanlı yöntemler kullanarak sistemlere sızma ve veri elde etme stratejilerinin bir göstergesi olarak değerlendirilmiştir. Örneğin, T1078 (Geçerli Kullanıcı Hesapları) 86.794 kez gibi teknikler, saldırganların yetkili hesapları kullanarak daha fazla olayın tetiklenmesine neden olmakta iken, T1119 (Otomatik Veri Toplama) 56.182 kez teknikleri de veri toplama süreçlerinde sıklıkla bir arada kullanılmaktadır. Bu çoklu eşleşmeler, saldırıların karmaşıklığını ve tespit edilen olayların birbirleriyle olan ilişkilerini anlamada kritik bir rol oynamaktadır.

Analiz sonuçları, her bir TTP'nin siber güvenlik tehditleri ile olan bağlantısını ve hangi tekniklerin daha yaygın olarak kullanıldığını göstermektedir. Örneğin, T1133 (Dış Uzaktan Servisler) 75.525 kez ve T1043 (Yaygın Olarak Kullanılan Portlar) 50.348 kez gibi teknikler, saldırganların sistemlere erişim sağlamak için yaygın olarak

kullandıkları yolları temsil etmektedir. Bu bağlamda, bir olayın birden fazla TTP ile eşleşmesi, sistemin çeşitli zafiyetlerine yönelik saldırıların gerçekleştirildiğini göstermekte ve siber güvenlik alanında alınacak önlemlerin kapsamını genişletmektedir.

Tablo 4. Ttp Sayıları

Ttp Grubu	Hit Sayısı
T1030 (Veri Aktarım Boyut Sınırlandırma) T1043 (Yaygın Olarak Kullanılan Portlar) T1078 (Geçerli Hesaplar) T1133 (Dış Uzaktan Servisler) T1036 (Gizlenme) T1041 (Komut ve Kontrol Kanalı Üzerinden Veri Sızıntısı) T1053 (Planlanmış Görev) T1082 (Sistem Bilgisi Keşfi) T1102 (Web Servisi) T1119 (Otomatik Veri Toplama) T1485 (Veri Yok Etme)	50.348
T1003 (İşletim Sistemi Kimlik Bilgisi Toplama) T1078 (Geçerli Hesaplar) T1082 (Sistem Bilgisi Keşfi) T1119 (Otomatik Veri Toplama)	27.662

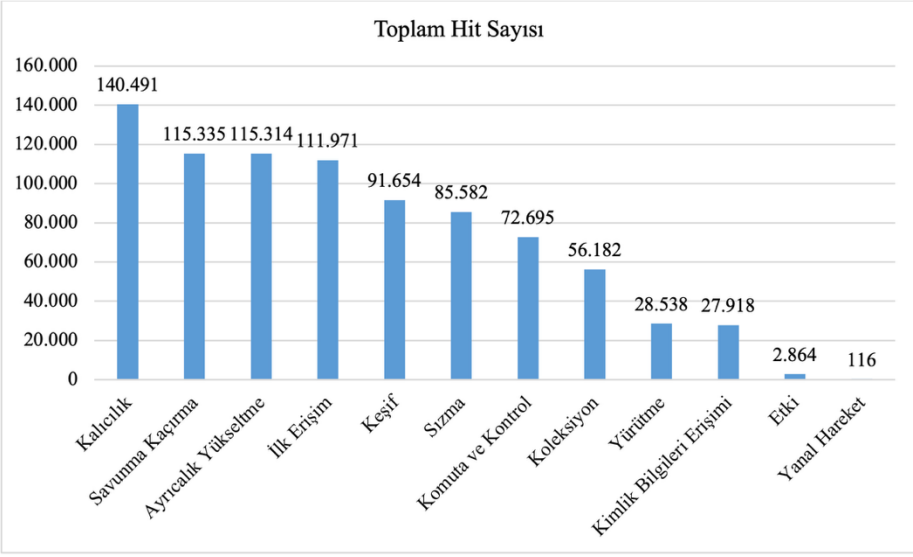
Tablo 4'te verilen MITRE TTP değerleri, Wazuh analizinde etiketlenmiş saldırı tekniklerinin etkinliği ve yaygınlığı gösterilmektedir. İlk grupta, T1030 (Veri Aktarım Boyut Sınırlamaları), T1043 (Yaygın Olarak Kullanılan Portlar), T1078 (Geçerli Kullanıcı Hesapları) ve T1133 (Dış Uzaktan Servisler) toplam 50.348 hit almıştır. Bu durum, sistemlere erişim sağlamak için saldırganların kimlik doğrulama ve ağ yönetim protokollerini hedef alma eğiliminde olduklarını ortaya koymaktadır. Bu tekniklerin yüksek hit sayısı, güvenlik ekiplerinin kimlik bilgilerini koruma ve ağ yönetim stratejilerini güçlendirme gerekliliğini vurgulamaktadır.

İkinci grupta ise, T1036 (Gizlenme), T1041 (Komut ve Kontrol Kanalı Üzerinden Veri Sızıntısı), T1053 (Zamanlayıcı Görevler), T1082 (Sistem Bilgisi Keşfi), T1102 (Web Servisi) ve T1119 (Otomatik Veri Toplama) toplam 28.520 hit almıştır. Bu gruptaki teknikler, daha karmaşık ve çok katmanlı saldırı stratejilerinin benimsendiğini göstermektedir. Özellikle, sistem bilgilerini toplama ve kötü niyetli yazılım yerleştirme gibi faaliyetler, siber tehditlerin daha karmaşık hale geldiğini ortaya koymaktadır.

Son olarak, T1003 (İşletim Sistemi Kimlik Bilgisi Toplama), T1078 (Geçerli Kullanıcı Hesapları), T1082 (Sistem Bilgisi Keşfi) ve T1119 (Otomatik Veri Toplama) teknikleri toplam 27.662 hit almıştır. Bu veri, kimlik bilgileri çalma ve kötü amaçlı yazılımlar kullanarak sistemlere sızma girişimlerinin odak noktası haline geldiğini göstermektedir. Genel olarak, bu analiz, saldırıların hangi alanlarda yoğunlaştığını ve hangi tekniklerin daha fazla dikkat ve önlem gerektirdiğini belirlemek açısından değerli bir kaynak sunmaktadır. Güvenlik ekipleri, bu verileri kullanarak savunma stratejilerini güncelleyebilir ve önceliklendirebilir.

Savunma stratejileri geliştirirken, bu tekniklerin birbirleriyle olan ilişkileri göz önünde bulundurularak, saldırı tespit ve önleme süreçlerinde daha etkili olunması sağlanmaktadır. Genel olarak, bu analiz saldırganların daha sık tercih ettiği teknikleri ve saldırı vektörlerini ortaya koyarak, savunma stratejilerinin hangi alanlara odaklanması gerektiğine dair önemli ipuçları sunmaktadır. Savunma stratejilerinin güçlendirilmesi ve olası saldırıların önlenmesi için bir dizi çözüm önerisi ve aksiyonlar bulunmaktadır. Öncelikle, T1078 (Geçerli Kullanıcı Hesapları) ve T1082 (Sistem Bilgisi Keşfi) tekniklerinin sıkça kullanıldığı göz önünde bulundurularak, güçlü kimlik doğrulama yöntemlerinin uygulanması ve çok faktörlü kimlik doğrulamanın (MFA) zorunlu hale getirilmesi kritik bir önem taşımaktadır. Kullanıcı hesaplarının düzenli olarak denetlenmesi ve şüpheli etkinliklerin izlenmesi de gereklidir.

Ayrıca, T1030 (Veri Aktarım Boyut Sınırlamaları) ve T1041 (Komut ve Kontrol Kanalı Üzerinden Veri Sızıntısı) tekniklerine karşı, veri transferlerinin izlenmesi ve anormal büyük veri hareketlerinin tespit edilmesi için gelişmiş veri kaybı önleme (DLP) çözümleri kullanılmalıdır. Ağ trafiğinin sıkça kullanılan portlar, T1043 (Yaygın Olarak Kullanılan Portlar) üzerinden izlenmesi ve analiz edilmesi, potansiyel gizlenmiş saldırıların tespit edilmesine yardımcı olabilmektedir. T1036 (Gizlenme) ve diğer gizlenme tekniklerine karşı, davranış tabanlı izleme ve analiz araçlarının kullanılması, meşru süreçlerin taklit edilmesini zorlaştırmaktadır. Ayrıca, T1133 (Dış Uzaktan Servisler) ve T1018 (Uzaktan Sistem Keşfi) tekniklerine karşı, dış ağ bağlantılarının sıkı denetimi ve sadece gerekli erişimlerin izin verilmesi, ağ üzerindeki keşif ve erişim saldırılarını azaltmaktadır. Düzenli siber güvenlik eğitimleri ve farkındalık programları ile çalışanların bu tür saldırı tekniklerine karşı bilinçlendirilmesi, insan hatasından kaynaklanan zafiyetlerin azalmasına katkı sağlamaktadır. Bu çözüm önerileri ve aksiyonlar, genel savunma hattının güçlendirilmesine ve olası saldırıların başarı şansının önemli ölçüde düşürülmesine yardımcı olmaktadır.



Şekil 2. Mitre Taktik Sayıları

Araştırma bulguları, sistemlerde kalıcılığın sağlanması, güvenlik önlemlerinin atlatılması ve yetki yükseltme gibi saldırıların en yaygın olduğu göstermektedir. Şekil 2'de detaylandırıldığı üzere, T-Pot üzerinden tespit edilen 184.750 adet olayın MITRE taktiklere eşleştirilmesi sonucunda bir tablo oluşturulmuştur. Bir olay, birden fazla MITRE taktik ile eşleştirilebilmektedir. Kalıcılık kategorisinde, 140.491 saldırı sayısıyla en yüksek değer elde edilmiştir, bu da saldırganların sistemde kalıcı olma çabalarının belirgin olduğu gösterilmektedir. Ayrıcalık Yükseltme ve Savunma Kaçırma, her biri 115.335 saldırı ile dikkat çekmekte ve bu, saldırganların daha fazla yetki elde etme ve güvenlik önlemlerini atlatma çabalarının önemli olduğu gösterilmektedir. İlk Erişim 11.197 ve Sızma 8.558 olayları da oldukça yüksek olup, saldırganların sisteme giriş yapma ve daha fazla yayılma konusundaki başarılarının yansıması olarak görülmektedir. Keşif 91.654 ve Koleksiyon 56.182 saldırıları, saldırganların sistem hakkında bilgi toplama ve veri çalma çabalarının önemli bir kısmını oluşturduğu gösterilmektedir. Kimlik Bilgileri Erişimi 27.918 ve Komuta ve Kontrol 72.695 saldırıları, kimlik bilgilerini elde etme ve sistemle sürekli iletişim kurma çabalarının yaygın olduğu gösterilmektedir. Etki 28.640 ve Yürütme 28.640 saldırıları, saldırganların sistem üzerinde zararlı işlemler gerçekleştirme çabalarını göstermekteyken, Yanal Hareket 116 saldırıları en düşük kategoriyi oluşturmuş ve saldırganların sistem içinde yatay hareketlerinin nispeten daha az olduğu ortaya konmuştur. Bu veriler, savunma stratejilerinin kalıcılığın engellenmesi, güvenlik önlemlerinin güçlendirilmesi ve Ayrıcalık Yükseltme girişimlerinin tespit edilmesi konularına odaklanması gerektiğini göstermektedir.

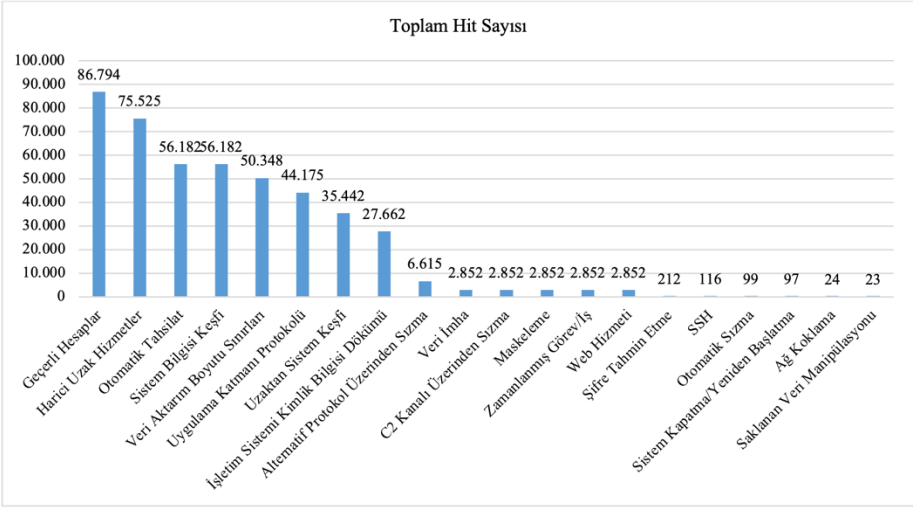
Saldırganlar, bir sisteme ilk erişimi sağladıktan sonra kalıcılığı sürdürmek için çeşitli yöntemler kullanmaktadır. Benzer şekilde, Ayrıcalık Yükseltme ve Savunma Kaçırma teknikleri de sıklıkla birlikte kullanılabilmektedir; saldırganlar, ayrıcalıklarını yükselterek daha fazla yetki elde eder ve savunma mekanizmalarını atlatmak için çeşitli stratejiler geliştirmektedirler.

İlk Erişim ve Ayrıcalık Yükseltme saldırılarının önlenmesi için, güçlü kimlik doğrulama yöntemleri ve çok faktörlü kimlik doğrulama (MFA) kullanılmasının önemi vurgulanmaktadır. Kullanıcı hesaplarının düzenli olarak denetlenmesi ve şüpheli etkinliklerin izlenmesi de saldırıların önlenmesinde kritik rol oynamaktadır. Kalıcılık ve Savunma Kaçırma tekniklerine karşı, davranış tabanlı izleme ve analiz araçlarının kullanılması gerekmektedir. Bu araçlar, anormal etkinliklerin tespit edilmesine ve hızlı müdahale edilmesine olanak tanımakta, böylece saldırganların sistemde kalıcı hale gelmesi zorlaştırılmaktadır.

Ağ segmentasyonu ve mikro-segmentasyon stratejilerinin, yanal hareketi sınırlayarak saldırganların ağ içinde yayılmasını zorlaştırabileceği belirtilmektedir. Ayrıca, keşif aşamasında anormal ağ trafiğini tespit edebilecek gelişmiş ağ izleme araçlarının kullanılması önem arz etmektedir. Koleksiyon ve Komuta ve Kontrol tekniklerine karşı, gelişmiş veri kaybı önleme (DLP) çözümleri ve ağ trafiği analiz araçları kullanılarak, verilerin dışarıya sızdırılmasının engellenebileceği ifade edilmektedir. Anormal veri transferlerinin izlenmesi ve engellenmesi gereklidir.

Çalışanların siber güvenlik farkındalığını artırmak için düzenli eğitim programlarının düzenlenmesi gerektiği önerilmektedir. Bu programlar, insan hatasından kaynaklanan zafiyetlerin azaltılmasına yönelik olmalı ve çalışanlar, kimlik avı saldırıları ve sosyal

mühendislik gibi tehditler konusunda bilinçlendirilmelidir. Bu aksiyonlar ve önlemler, saldırganların başarılı olma şansını azaltarak genel savunma hattının güçlenmesine katkı sağlayacak ve kuruluşun siber güvenlik duruşunun önemli ölçüde iyileştirilmesini sağlayacaktır.



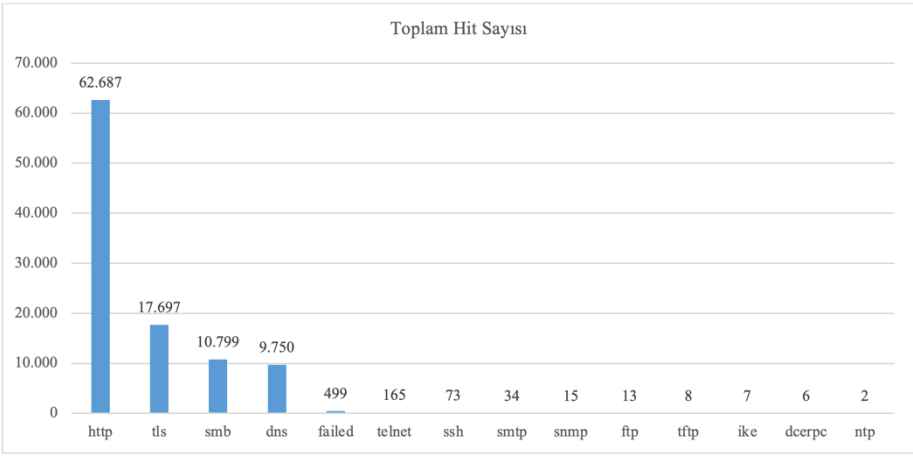
Şekil 3. Ttp Toplam Rakamları

Şekil 3'deki araştırma bulgularına göre, çeşitli MITRE ATT&CK TTP'lerinin yaygın olarak kullanıldığı görülmüştür. Geçerli Hesaplar (T1078), 86.794 saldırı ile en yüksek değeri almış olup, bu, saldırganların mevcut hesapları kullanarak sistemlere erişim sağlama çabalarının yoğun olduğunu göstermektedir. Sistem Bilgisi Keşfi (T1082) ve Otomatik Veri Toplama (T1119) teknikleri de her biri 56.182 saldırı ile oldukça yüksek bir oranda kullanılmıştır. Bu da, saldırganların sistem hakkında bilgi toplama ve veri toplama çabalarının yaygın olduğunu göstermektedir.

Veri Aktarım Boyutu Sınırları (T1030), 50.348 saldırı ile saldırganların büyük veri setlerini gizlice aktarma çabalarının yoğun olduğunu göstermektedir. Harici Uzak Hizmetler (T1133), 75.525 saldırı ile saldırganların yaygın kullanılan ağ noktalarını hedef alma eğiliminde olduğunu ortaya koymaktadır. Zamanlanmış Görev/İş (T1053) ve Komut ve Kontrol Kanalı Üzerinden Sızma (T1041), her biri 28.520 saldırı ile saldırganların kalıcılık sağlama ve komuta ve kontrol kanalları üzerinden veri sızdırma çabalarını vurgulamaktadır. Maskeleme (T1036) ve Uygulama Katmanı Protokolü (T1071), 28.520 ve 44.175 saldırı ile saldırganların varlıklarını gizleme ve veri iletişimini sürdürme stratejilerini göstermektedir.

SSH (Secure Shell) (T1071) ve Şifre Tahmin Etme (T1110), her biri 116 ve 212 saldırı ile, daha az yaygın olmakla birlikte önemli tehditler olarak tespit edilmiştir. Web Hizmeti (T1102) ve İşletim Sistemi Kimlik Bilgisi Dökümü (T1003), sırasıyla 28.520 ve 27.662 saldırı ile saldırganların web tabanlı uygulamaları ve işletim sistemi kimlik bilgilerini hedef alma eğiliminde olduklarını göstermektedir.

Bu veriler, güvenlik stratejilerinin, geçerli hesapların korunması, sistem bilgisi keşfi ve otomatik veri tahsilatı gibi yüksek riskli alanlara odaklanması gerektiğini ortaya koymaktadır.



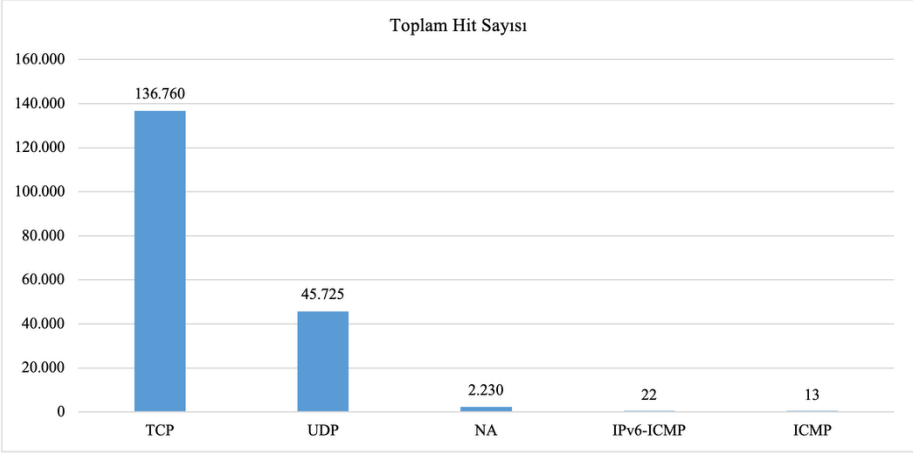
Şekil 4. Uygulama Protokol Sayıları

Alınan saldırıların analizi sonucunda elde edilen verilere göre, saldırıların uygulama protokollerine göre dağılımı Şekil 4'de gösterilmiştir. En fazla saldırıya maruz kalan protokol, 62.687 işlemle HTTP (Hypertext Transfer Protocol) olmuştur. Bu durum, HTTP protokolünün yaygın kullanımından ve güvenlik açıklarının sıkça hedef alınmasından kaynaklanmıştır. İkinci sırada ise TLS (Transport Layer Security) protokolü yer almakta olup, toplamda 17.697 işlem kaydedilmiştir. TLS, güvenli iletişim sağlamak için yaygın olarak kullanıldığından, saldırganlar bu protokolü hedef alarak güvenlik açıklarını sömürmeye çalışmıştır.

Üçüncü sırada SMB (Server Message Block) protokolü yer almakta olup, toplamda 10.799 işlem kaydedilmiştir. SMB, özellikle dosya paylaşımı ve ağ iletişimi için kullanılan bir protokol olduğundan, saldırganların ilgisini çekmiştir. DNS (Domain Name System) protokolü üzerinden 9.750 işlem gerçekleştirilmiştir. DNS saldırıları, internet trafiğinin yönlendirilmesinde kritik bir rol oynayan DNS sunucularını hedef alarak, kullanıcıların yanlış yönlendirilmesi veya servis kesintilerine yol açılmasını amaçlamaktadır.

Analiz sırasında belirlenen 499 işlem, hangi protokol kullanılarak yapıldığı tespit edilemediği için "failed" olarak sınıflandırılmıştır. Bu işlemler, saldırıların karmaşıklığını ve bazı durumlarda kullanılan araçların tespit edilememesini göstermektedir. Diğer protokoller ise daha az saldırıya maruz kalmıştır: Telnet üzerinden 165, SSH üzerinden 73, SMTP (Simple Mail Transfer Protocol) üzerinden 34, SNMP (Simple Network Management Protocol) üzerinden 15, FTP (File Transfer Protocol) üzerinden 13, TFTP (Trivial File Transfer Protocol) üzerinden 8, IKE (Internet Key Exchange) üzerinden 7, DCERPC (Distributed Computing Environment Remote Procedure Call) üzerinden 6 ve NTP (Network Time Protocol) üzerinden 2 işlem kaydedilmiştir.

Bu protokoller, nispeten daha az kullanılmakta veya daha iyi korunmuş olduklarından, saldırganlar tarafından daha az hedef alınmıştır. Analiz, saldırganların genellikle yaygın ve kritik protokolleri hedef aldığını ortaya koymuştur. Özellikle HTTP ve TLS protokollerine yönelik saldırıların yüksek sayıda olması, bu protokollerin güvenliğinin sağlanmasının önemini vurgulamaktadır. Daha az saldırıya maruz kalan protokoller bile dikkate alınmalı ve güvenlik önlemleri sürekli olarak güncellenmelidir.



Şekil 5. Protokol Özeti

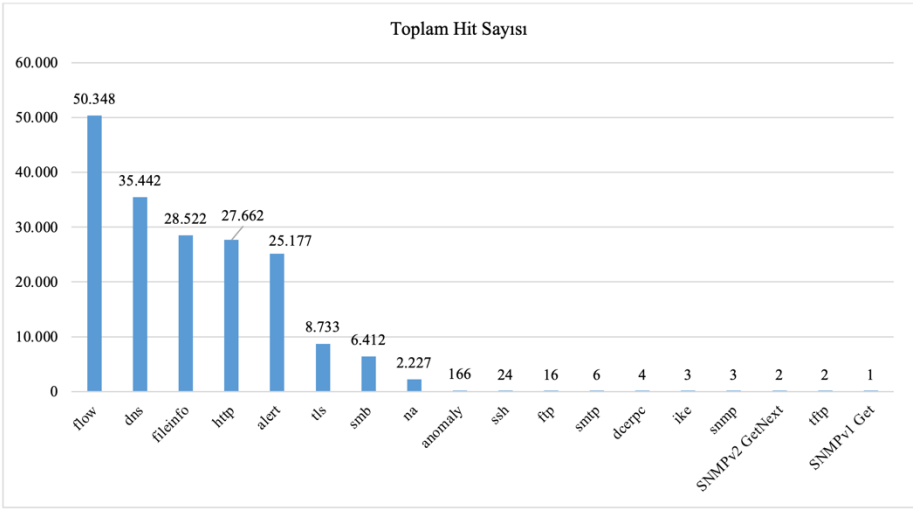
Şekil 5'de detaylandırıldığı üzere, ağ protokollerine göre dağılımın belirgin farklılıklar gösterdiği ortaya konulmuştur. T-Pot üzerinden toplanan ve analiz edilen 184.750 olayın protokol bazında kırılımının tespit edilmiş olduğu görülmüştür. Bu analiz, TCP (Transmission Control Protocol) ve UDP (User Datagram Protocol) protokollerinin saldırıların büyük bir kısmını oluşturduğunu göstermektedir. En fazla saldırıya maruz kalan protokol TCP olup, toplamda 136.760 işlem kaydedilmiştir. TCP, internetin temel iletişim protokollerinden biri olup, birçok uygulamanın veri iletimi için kullandığı bir protokol olduğundan, saldırganlar tarafından sıklıkla hedef alınmaktadır. TCP üzerinden gerçekleştirilen saldırıların, genellikle hizmet engelleme DoS (Denial of Service) saldırıları, oturum kaçırma veya kötü amaçlı yazılım yayma gibi amaçlarla yapılmış olduğu görülmüştür.

İkinci sırada, toplamda 45.725 işlemle UDP protokolü yer almaktadır. UDP, TCP'ye göre daha az güvenli kabul edilmekle birlikte, hızlı veri iletimi sağladığı için birçok uygulama tarafından tercih edilmektedir. UDP üzerinden gerçekleştirilen saldırıların, genellikle DNS (Domain Name System) yansıma (reflection) saldırıları, DDoS (Distributed Denial of Service) saldırıları veya ağ hizmetlerinin zayıflıklarını hedef alan diğer saldırılar olabileceği görülmüştür.

Daha az sayıda saldırıya maruz kalan protokoller arasında IPv6-ICMP (Internet Control Message Protocol) ve ICMP bulunmaktadır. IPv6-ICMP protokolü üzerinden 22 işlem, ICMP protokolü üzerinden ise 13 işlem kaydedilmiştir. ICMP protokolleri, genellikle ağ teşhis ve hata mesajları için kullanılmaktadır. Bu nedenle, saldırganlar tarafından diğer protokoller kadar sık hedef alınmamaktadır. Ancak, ICMP protokolleri üzerinden

yapılan saldırıların, ağ altyapısına zarar vermek veya ağ haritalaması (network mapping) gibi amaçlarla kullanılabileceği görülmüştür.

Bu analiz, saldırganların genellikle yaygın ve kritik iletişim protokollerini hedef aldığını göstermektedir. TCP ve UDP protokollerine yönelik saldırıların sayısının yüksek olması, bu protokollerin güvenliğinin sağlanmasının ne kadar önemli olduğunu vurgulamaktadır. Daha az saldırıya maruz kalan ICMP ve IPv6-ICMP protokollerinin bile dikkate alınması ve bu protokoller üzerinden yapılabilecek olası saldırılara karşı önlemler alınması gerektiği sonucuna varılmaktadır.



Şekil 6. Olay Türü Bazında

Şekil 6'da alınan saldırıların çeşitli olay türleri bazında incelenmiş olduğu görülmüştür. T-Pot sistemi üzerinden toplanan 184.750 olayın analizi ve etiketlenmesi sonucunda çeşitli event türleri tespit edilmiştir. En yüksek hit sayısına sahip olan HTTP olayları, 27.662 kez kaydedilmiş olup, bu da web tabanlı saldırıların ve etkileşimlerin yaygınlığını göstermektedir. DNS olayları ise 35.442 kez kaydedilmiş olup, ağ tabanlı iletişimin önemli rolünü vurgulamaktadır.

Bunun yanı sıra, dosya bilgilerine dair olaylar 28.522 kez rapor edilmiş olmuştur, bu da saldırganların dosya manipülasyonu ve bilgi toplama faaliyetlerine odaklanmış olduklarını göstermektedir. TLS ve alert olayları, sırasıyla 8.733 ve 25.177 hit alarak, güvenlik tehditlerinin ve şifreli iletişimin izlenmesinin önemini ortaya koymuştur. Bu olay türlerinin analizi, saldırganların hangi alanlarda daha yoğun faaliyet gösterdiğini ve güvenlik stratejilerinin hangi olay türlerine daha fazla odaklanması gerektiğini ortaya koymuştur.

Ayrıca, akış verileri (flow) 50.348 hit ile dikkat çekmiş olup, bu da ağ trafiğinin analizinin ve yönetiminin kritik bir unsur olduğunu göstermektedir. SMB olayları 6.412 kez kaydedilmişken, anomali durumları ise yalnızca 166 defa tespit edilmiştir, bu da anormal durumların nadir olduğunu göstermektedir. Diğer olay türleri, örneğin

IKE, SNMP ve SMTP olayları, toplamda daha düşük hit sayıları ile kaydedilmiş olmuştur, bu da belirli protokollerin kullanımının sınırlı olduğunu ortaya koymaktadır.

Bu bulgular, siber güvenlik alanında proaktif önlemler almak ve saldırıların doğasını daha iyi anlamak için değerli bilgiler sunmuş olmaktadır. Saldırıların çeşitli protokoller ve hedefler üzerinde odaklandığı gösterilmiştir. Özellikle HTTP ve DNS gibi yaygın olarak kullanılan servislerin saldırıya maruz kalmış olmaları dikkat çekicidir. Dosya bilgisi ve TLS ile ilgili olaylar da muhtemelen sistemlere erişim veya hassas verilere erişim girişimlerini yansıtmaktadır. Uyarılar ise genellikle potansiyel tehditler veya ihlaller konusunda uyarı veren sistemler tarafından oluşturulmuş olup dikkatle incelenmelidir.

Ancak, çok düşük sayıda gerçekleşen anormallikler ve diğer nadir olaylar, genel olarak düşük risk taşısa da göz ardı edilmemelidir; çünkü bunlar da potansiyel olarak yeni ve gelişen tehditlerin göstergesi olabilir.

HTTP ve DNS saldırılarına karşı daha güçlü koruma önlemleri uygulanmış olmalıdır; bu, Web Uygulama Güvenlik Duvarları (WAF) ve DNS güvenlik çözümleriyle desteklenmiş olmalıdır. Dosya bilgisi ve TLS erişimlerinde güvenlik kontrolleri sıkılaştırılmalı, hassas verilere erişim için katı kimlik doğrulama ve yetkilendirme politikaları benimsenmiş olmalıdır. Uyarılar derhal incelenmiş olmalı ve etkili tepki planları oluşturulmuş olmalıdır. Ağ akışı ve SMB protokolü üzerindeki güvenlik zafiyetleri azaltılmalı, yeni veya gelişen tehditler için tehdit algılama sistemleriyle sürekli izleme sağlanmalıdır. Personel güvenlik farkındalığı eğitimleri almalı ve sosyal mühendislik saldırılarına karşı bilinçlendirilmiş olmalıdır.

Güvenlik önlemleri sürekli olarak gözden geçirilmiş ve iyileştirilmiş olmalı, yeni tehditlere karşı proaktif önlemler alınmış olmalıdır.

8. SONUÇLAR VE GELECEK ÇALIŞMALAR

Bu çalışmanın temel amacı, Linux platformunda MITRE ATT&CK matrisi çerçevesinde saldırıların nasıl etkin bir şekilde planlanıp uygulanabileceği gösterilmiş olmuştur. MITRE ATT&CK matrisi, saldırganların kullandığı Taktikler, Teknikler ve Prosedürler (TTP'ler) kapsamlı bir şekilde belgelenmiş ve savunma mekanizmalarını güçlendirmek isteyen kuruluşlara rehberlik edilmiştir. T-Pot Balküpü, Wazuh, auditd ve Atomic Red Team gibi araçlar kullanılarak gerçekleştirilen bu saldırılar, MITRE ATT&CK matrisindeki farklı taktikler üzerinden değerlendirilmiş olmuştur.

Tespit edilen saldırı sayıları ve bu taktiklerin sıklığı, sistemlerin hangi alanlarda daha fazla savunmasız olduğu açıkça ortaya konmuş olmuştur. Balküpü tabanlı bu yaklaşım, saldırıları gerçekleştiren aktörlerin taktik ve tekniklerini daha iyi anlamamıza olanak tanımış ve aynı zamanda savunma stratejilerinin geliştirilmesine katkı sağlanmış olmuştur. Bu yöntemlerin belirlenmesi ve raporlanması, ağ güvenliği uzmanlarına saldırıları önceden tespit etme ve etkili bir şekilde karşılama konusunda kritik bir rol oynamış olmuştur.

Bu çalışma, bal peteği kullanımının artan etkisinin ve bu teknolojinin siber güvenlik pratiğine nasıl entegre edilebileceğinin gösterildiği bir araştırma olmuştur. MITRE ATT&CK matrisi çerçevesinde yapılan bu çalışma, siber güvenlikteki yeni yaklaşımların ve savunma stratejilerinin geliştirilmesine ilham verilmesine katkı sağlanmış olmuştur. Bu araştırma, siber güvenlik alanındaki bilgi ve uygulamaların derinleştirilmesine olanak tanırken, aynı zamanda savunma ekiplerinin saldırılara karşı nasıl daha etkin bir şekilde hazırlanmaları gerektiğine dair önemli bilgiler sunmuş olmuştur.

Saldırganların sistem içinde yatay geçiş yaparak diğer makineler üzerinde kontrol elde etme çabaları belirli ölçüde tespit edilmiş olmuştur. Kullanıcı kimlik bilgilerine erişim denemelerinin yüksek sayıda olması, kimlik doğrulama mekanizmalarının güçlendirilmesi gerektiğini ortaya koymuş olmuştur. Saldırganların zararlı kod çalıştırma girişimleri, güvenlik açıklarının ciddi bir tehdit oluşturduğunu göstermiştir. Ayrıca, saldırganların uzaktan komut çalıştırma yeteneklerinin, sistemlerin kontrolünü ele geçirme riski taşıdığı görülmüş olmuştur.

Hassas verilerin toplanmasına yönelik saldırılar, veri güvenliğinin öncelikli bir konu olduğunu işaret etmiştir. Yapılan çalışma ve saldırı senaryosu kapsamında, sistemin zayıf noktalarını keşfetme çabalarının yoğunluğu, saldırganların detaylı bilgi toplama girişimlerinde bulunduğunu göstermiş olmuştur. Saldırı sonuçları incelendiğinde, sisteme izinsiz giriş denemelerinin yüksek sayıda olması, dışarıdan gelen tehditlere karşı daha güçlü bir koruma gerektiğini ortaya koymuş olmuştur.

Bu saldırı simülasyonu kapsamında, ilk erişim denemelerinin fazlalığı, saldırıların başlangıç noktalarının güvenliğinin yetersiz olduğunu göstermiştir. Saldırganların savunma mekanizmalarını atlatma ve sistemdeki ayrıcalıklarını artırma girişimleri, mevcut güvenlik önlemlerinin güçlendirilmesi gerekliliğini ortaya koymuş olmuştur. Bu çalışmanın bir sonucu olarak, saldırganların sistemde kalıcı olarak yerleşme çabalarının yüksek sayıda olmasının, uzun vadeli tehditlerin varlığına işaret ettiği şeklinde yorumlanmış olmalıdır.

Tablo 5'de görüldüğü üzere literatürde bulunan çalışmalar genel olarak, balküpü kullanarak siber güvenliği geliştirmeye yönelik çeşitli araştırmalara bir bakış sunmaktadır. Bizim çalışmamız, diğer araştırmalarla benzer şekilde, Linux sistemlerine yönelik siber saldırıların tespiti ve analizine odaklanmakta olup, balküpü tabanlı bir yaklaşım kullanılmaktadır. Bu çalışmalardaki ortak tema, saldırı tekniklerini sınıflandırmak ve anlamak için MITRE ATT&CK çerçevesinin kullanılmasında yatmaktadır. Ayrıca, bu makalelerin çoğu, çeşitli saldırı türlerini test etme amacını gütmektedir. Ancak, bizim çalışmamız, kullanılan araçlar açısından bildiğimiz kadarıyla benzersizdir; saldırı simülasyonuna verilen önem ve siber güvenlik uzmanlarına yardımcı olmayı hedefleyen yaklaşımı ile öne çıkmaktadır.

Tablo 5. Literatür Çalışmaların Karşılaştırması

Makale	Kullanılan Metod	Sonuçlar	Kullanılan Teknoloji	Kullanılan Balküpü Çeşitleri	T-Pot Kullanımı	Test Edilen Saldırı Türleri	Wazuh Kullanımı
A Highly Interactive Honeypot-Based Approach to Network	Yüksek etkileşimli bir balküpü tehdit yönetim sistemi için modüler tasarım aşağıdaki modüllere ayrılmıştır.Glastopf, savunmasız web sunucularını simüle etmek için düşük etkileşimli bir balküpü olarak kullanılmaktadır.	65 saldırı verisi kaydı belirli bir süre boyunca toplanmıştır. Merkezi düğüm, sürekli saldırılara rağmen güvenli tutulmuştur. Bu yöntem, geleneksel ağ tehdit yönetim yöntemlerine kıyasla önemli avantajlar sunmaktadır. Sistem, mevcut ağ ortamında güvenlik sağlamakta etkili olduğu kanıtlanmıştır.	Glastopf, MongoDB	Yüksek etkileşimli: Shadow Daemon, Ehoney Düşük etkileşimli: Glastopf	Geçerli değildir (Not Applicable)	Genel saldırı davranışı, belirli türler açıkça belirtilmemiştir, ancak kaynak SQL enjeksiyonu gibi güvenlik açıklarına odaklanmıştır.	Hayır
An Improved Honeypot Model for Attack Detection and Analysis	Sistemin bütünlüğü korunurken saldırganlarla daha yüksek etkileşim sağlanması amacıyla yeni bir balküpü modelinin tasarımı yapılmıştır.	17 gün boyunca 1.5 milyon olay toplanmıştır. Daha önce belgelenmemiş Kompromize Göstergeleri (IOC'ler) tespit edilmiştir. Bu sonuçlar, literatürdeki benzer dağıtımlar ile karşılaştırılabilir niteliktedir.	Wazuh, Elasticsearch-Logstash-Kibana (ELK), IPTables	Yüksek etkileşimli: Özel balküpleri (detaylar sağlanmamıştır)	Geçerli değildir (Not Applicable)	RDP brute-force denemeleri, SSH brute-force denemeleri, Apache Web Sunucusu ve Apache Druid'teki güvenlik açıklarını istismar etme girişimleri.	Hayır
An Adversarial Approach Comparing Windows and Linux Security Hardness Using Mitre ATT&CK Framework for Offensive Security	Statik ve dinamik analizlerin kötü amaçlı yazılım tespiti üzerindeki etkinliği incelenmektedir.	Verilen alıntı, herhangi bir spesifik sonucu belirtmemektedir. Bu alıntı, siber güvenlikle ilgili çeşitli mevcut çalışmaları özetlemeye odaklanmaktadır, bunlar arasında kötü amaçlı yazılım tespiti teknikleri de bulunmaktadır.	Belirtilmemiştir (Not specified)	Belirtilmemiştir (Not specified)	Geçerli değildir (Not Applicable)	Phishing, süreklilik ve yatay hareketle ilgili zafiyetlerin istismarı, belirli saldırı türleri metinde ayrıntılı olarak belirtilmemiştir.	Hayır

Makale	Kullanılan Metod	Sonuçlar	Kullanılan Teknoloji	Kullanılan Balküpü Çeşitleri	T-Pot Kullanımı	Test Edilen Saldırı Türleri	Wazuh Kullanımı
Cyber security threat modeling based on the MITRE Enterprise ATT&CK	MITRE Enterprise ATT&CK Matrisi'ne dayalı olarak, kurumsal güvenlik için 'enterpriseLang' adı verilen bir tehdit modelleme dili önerilmektedir. Saldırı simülasyonları kullanılarak güvenlik ayarları ve mimari değişiklikler incelenmektedir.	Saldırı simülasyonları yapmak, paydaşların kurumlarına yönelik bilinen tehditleri, potansiyel azaltma önlemleri, en kısa saldırı yolları ve düşmanların sistemi tehlikeye atmak için gereken süreyi değerlendirmelerine olanak tanımıştır.	Belirtilmemiştir (Not specified)	Geçerli değildir(Not Applicable) Tehdit modelleme, balküpü dağıtımı değil	Geçerli değildir (Not Applicable)	Geçerli değildir (MITRE ATT&CK çerçevesi kullanılarak saldırı senaryolarının modellenmesine odaklanılmakta, belirli saldırı türlerine odaklanılmamaktadır).	Hayır
Developing Proactive Cyber Threat Defense Systems on Server Computers Using Honeypot	Brute Force saldırıları karşısında sunucu bilgisayarları üzerindeki olay yanıtı analiz teknikleri kullanılmaktadır. SIEM sistemi, saldırıları MITRE ATT&CK çerçevesi ile karşılaştırarak saldırı tekniklerini tanımlamaktadır.	Bir saldırı gerçekleştiğinde, SIEM saldırıyı "Parola Tahmini", bir SSH Brute Force Saldırısı olarak kaydeder ve tanımlar.	SIEM	Belirtilmemiştir (Not specified)	Geçerli değildir (Not Applicable)	SSH brute-force saldırıları (özellikle Şifre Tahmin Etme)	Hayır

Makale	Kullanılan Metod	Sonuçlar	Kullanılan Teknoloji	Kullanılan Balküpü Çeşitleri	T-Pot Kullanımı	Test Edilen Saldırı Türleri	Wazuh Kullanımı
Enhancing False Positive Detection in IDS-IPS Using Honeypots: A Case Study with CSE-CIC-2018 Dataset	Balküpü verilerini IDS/IPS çıktılarıyla entegre eden hibrit bir yaklaşım geliştirilmiştir. Bu yaklaşımın etkinliği, CSE-CIC-2018 veri seti kullanılarak değerlendirilmiştir.	Yanlış pozitif oranları, doğru pozitif oranları, doğruluk ve ilgili metriklerin nicel ölçümleri, mimarinin etkinliğini değerlendirmiştir. Sonuçlar, yanlış pozitiflerin azaldığını göstermiştir. Verilerin analizi, saldırgan davranışları hakkında içgörüler sunmuştur.	Honeyd, Collapsar, Snort, TPOT CE Honeynet	Düşük etkileşim: Honeyd Orta etkileşim: TPOT CE'nin SentryPeer, DICOMPot, HoneyTrap, Glutton Snare ve Tanner gibi orta etkileşimli balküpleri	Cowrie, Dionaea, Snare, Tanner, Citrix Honeypot	SQL Injection, Cross-Site Scripting (XSS), Nmap taramaları, sızma saldırıları (geniş bir kategori olup, sızma içindeki belirli teknikler ayrıntılı olarak belirtilmemiştir), çeşitli protokollere yönelik saldırılar (FTP, HTTP, HTTPS, SSH), ve CSE-CIC-2018 veri setinde bulunan saldırılar (çok çeşitli saldırı türlerini içermekte olup, hepsi metinde açıkça listelenmemiştir; ancak kaynak, brute force, DoS, heartbleed, botnet, sızma ve DDoS gibi örnekleri belirtmektedir) kullanılarak yapılan saldırılar tanımlanmıştır.	Hayır

Makale	Kullanılan Metod	Sonuçlar	Kullanılan Teknoloji	Kullanılan Balküpü Çeşitleri	T-Pot Kullanımı	Test Edilen Saldırı Türleri	Wazuh Kullanımı
Faking smart industry_ exploring cyber-threat landscape deploying cloud-based honeypot	Bulut tabanlı balküpü dağıtımı, akıllı endüstrilerde siber tehdit manzarasını keşfetmek için kullanılmıştır. İzleme için T-Pot balküpü ve Cockpit kullanılmıştır.	SHODAN ve SHODAN dışı tabanlı eşler arasındaki etkileşimler ve korelasyonlar belirlenmiştir. Araştırma, aşağıdaki veriler toplanmıştır: Saldırgan kullanıcı adları, İstismar sonrası kullanılan komutlar, İstismar edilen CVE'ler, Kötü amaçlı yazılım imzaları.	T-Pot, Cockpit, Conpot, Cowrie, Dicompot, Heralding, Honeysap, Honeytrap, Medpot, Rdpy Honeypot, Cyberchef, ELK, Fatt, Elasticsearch Head, Ews-poster, Nginx, Spiderfoot, P0f, Suricata	Düşük etkileşim: Conpot, Dionaea, Heralding, Medpot; Orta etkileşim: Cowrie, Honeytrap kullanılarak etkileşimler sağlanmaktadır.	Conpot, Cowrie, Dionaea, Heralding, Honeysap, Honeytrap, Medpot	Çeşitli protokoller (SSH, FTP, Telnet, HTTP, HTTPS, IMAP, IMAPS, POP3, POP3S, SMTP, VNC, Socket5, PostgreSQL) karşısında brute-force kimlik doğrulama saldırıları, Çeşitli CVE'leri (belirli CVE'ler alıntıda belirtilmemiştir) kullanarak yapılan istismar girişimleri, Belirli endüstriyel kontrol sistemlerini hedef alan saldırılar (Guardian AST, Siemens S7-200, Akıllı Sayaç)	Hayır
Honeypot in a box_ A Distributed cluster network for honeypot deployment	Orkestrasyon için Kubernetes kullanılan dağıtılmış bir balküpü altyapısı kurulmuştur. Altyapının performansını ve etkinliğini değerlendirmek için karşılaştırmalı testler (benchmarking) yapılmıştır.	Ortalama bir ağ gecikmesi 17ms ve bant genişliği 95 Mbit/s olarak elde edilmiştir. Bu yaklaşım, balküpleri farklı konumlara başarıyla dağıtılmıştır.	Kubernetes, Cowrie	Not specified.	Cowrie	Brute-force attacks	Hayır

Makale	Kullanılan Metod	Sonuçlar	Kullanılan Teknoloji	Kullanılan Balküpü Çeşitleri	T-Pot Kullanımı	Test Edilen Saldırı Türleri	Wazuh Kullanımı
Industrial Control Systems Security Validation Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework	Endüstriyel Kontrol Sistemlerinde güvenlik doğrulaması için Snort IDS ve T-Pot balküpü gibi açık kaynaklı araçlar kullanılmıştır. Saldırıları analiz etmek için MITRE ATT&CK çerçevesi kullanılmıştır.	Çeşitli saldırı senaryoları için IOC'ler belirlenmiştir. Araştırma, açık kaynak araçlarının ICS ortamlarında tehditlerin tespit edilmesi ve hafifletilmesindeki etkinliği incelenmiştir.	Snort IDS, T-Pot	Belirtilmemiştir, ancak T-Pot'un yeteneklerine dayalı olarak düşük, orta ve yüksek etkileşimli balküplerinin bir kombinasyonu kullanılır.	Belirtilmemiştir, ancak T-Pot'un kullanımı göz önünde bulundurularak, farklı saldırı türleri için çeşitli honeypotlar içerildiği tahmin edilmektedir.	Sağlanan alıntıda belirli saldırı türleri ayrıntılı olarak belirtilmemiştir, ancak odak noktası Endüstriyel Kontrol Sistemleri güvenliği üzerinedir.	Hayır
Investigating Threats to ICS and SCADA Systems Via Honeypot Data Analysis and SIEM	Conpot balküpü, Wazuh SIEM ve The Hive kullanarak tehdit istihbaratı paylaşımı yapan gerçek zamanlı bir tehdit analiz sistemi geliştirilmiştir. Bu araştırma, ICS (Endüstriyel Kontrol Sistemleri) ve SCADA (Denetleyici ve Veri Toplama) ortamlarında saldırı eğilimlerini tanımlamaya ve proaktif tehdit azaltma sağlamaya odaklanmaktadır.	ICS/SCADA sistemlerinde proaktif tehdit azaltma için balküpü verilerinin gerçek zamanlı analizi yapılmış ve tehdit istihbaratı çıkarılmıştır. Balküpleri tarafından tespit edilen kötü niyetli IP'ler başarıyla engellenmiştir.	Conpot, Wazuh SIEM, The Hive	Düşük etkileşim: Conpot	Geçerli değildir (Not Applicable)	HTTP, SNMP ve Modbus protokollerini hedef alan saldırılar, Gözlemlenen belirli taktikler ve teknikler, MITRE ATT&CK çerçevesi kullanılarak kategorize edilmiştir.	Evet

Makale	Kullanılan Metod	Sonuçlar	Kullanılan Teknoloji	Kullanılan Balküpü Çeşitleri	T-Pot Kullanımı	Test Edilen Saldırı Türleri	Wazuh Kullanımı
It's too late if exfiltrate _ Early stage Android ransomware detection	MITRE ATT&CK bilgi tabanını kullanarak fidye yazılımlarını erken aşamada tespit etmek için 'Weapon' adı verilen yeni bir çerçeve geliştirilmiştir. Bu çerçeve, dinamik analiz kullanarak özellikler çıkarır ve bunları MITRE saldırı verileriyle ilişkilendirir.	Fidye yazılımlarını erken aşamalarda tespit etmede yüksek doğruluk elde edilmiştir. Bu, aşağıdaki yöntemlerin bir kombinasyonu kullanılarak başarmıştır: - Dinamik analiz - Semantik özellik eşlemesi - MITRE ATT&CK çerçevesi Önerilen Weapon yöntemi, tespit doğruluğu açısından diğer son teknoloji yaklaşımları geride bırakmıştır.	Belirtilmemiştir (Not specified)	Geçerli değildir (fidye yazılımı tespit çerçevesi, balküpü dağıtımı değil).	Geçerli değildir (Not Applicable)	Fidye yazılımı saldırıları, özellikle aşağıdaki tekniklerle ilgili odaklanılmaktadır: Süreklilik (Persistence) Ayrıcalık Yükseltme (Privilege Escalation) Komut ve Kontrol (Command and Control) Keşif (Discovery) Toplama (Collection)	Hayır

Makale	Kullanılan Metod	Sonuçlar	Kullanılan Teknoloji	Kullanılan Balküpü Çeşitleri	T-Pot Kullanımı	Test Edilen Saldırı Türleri	Wazuh Kullanımı
Mapping Linux Shell Commands to MITRE ATT&CK using NLP-Based Approach	Doğal dil işleme (NLP) yaklaşımı, Linux kabuk komutlarını MITRE ATT&CK tekniklerine ve taktiklerine eşlemek için kullanılmaktadır.	Linux komutlarını hem MITRE ATT&CK tekniklerine/alt tekniklerine hem de taktiklere eşlemek için makul geri çağırma (recall) değerleri elde edilmiştir. En iyi performans gösteren model, şu geri çağırma değerlerini elde etmiştir: Taktiklere eşleme için Recall-10: 0.75397 Tekniklere/alt tekniklere eşleme için Recall-10: 0.45575 Bu araştırma, doğal dil işlemenin (NLP) bu görev için uygulanabilirliğini göstermektedir.	Cowrie	Geçerli değildir(Not Applicable)	Odak noktası, shell komutlarının MITRE ATT&CK'e haritalanmasına yöneliktir, belirli saldırı türlerinin test edilmesine değil. Kaynak, curl komutunu bir örnek olarak kullanır.	Hayır	Hayır

Makale	Kullanılan Metod	Sonuçlar	Kullanılan Teknoloji	Kullanılan Balküpü Çeşitleri	T-Pot Kullanımı	Test Edilen Saldırı Türleri	Wazuh Kullanımı
Performance analysis of network intrusion detection using T-Pot honeypots	T-Pot balküpü dağıtımı ve ağ izinsiz giriş tespiti için performans analizi amacıyla ELK yığını (stack) kullanılmıştır. Etkinlik değerlendirmesi için Nmap, Hydra ve DDoS saldırıları kullanılarak deneyler yapılmıştır.	Balküpleri, port taramaları, brute-force saldırıları ve DDoS saldırıları da dahil olmak üzere izinsiz giriş girişimlerini başarılı bir şekilde tespit etmiş ve kaydetmiştir. Sonuçlar, T-Pot balküpü'nün çeşitli ağ saldırılarını tespit etmede etkili olduğunu göstermektedir. Toplanan verilerin analizi: Saldırgan davranışları hakkında içgörüler sunmaktadır. Potansiyel güvenlik açıklarını tanımlamaya yardımcı olmaktadır.	T-Pot, ELK stack	Belirtilmemiştir, ancak T-Pot'un kullanımı göz önünde bulundurularak, farklı saldırı türleri için çeşitli balküplerinin içerildiği tahmin edilmektedir.	Belirtilmemiştir, ancak araştırmada açıkça şunlar kullanılır: Port taraması için Nmap, brute-force saldırıları için Hydra, DDoS saldırıları.	Hayır	Hayır

Makale	Kullanılan Metod	Sonuçlar	Kullanılan Teknoloji	Kullanılan Balküpü Çeşitleri	T-Pot Kullanımı	Test Edilen Saldırı Türleri	Wazuh Kullanımı
Attack detection and forensics using honeypot in IoT environment	Çeşitli makine öğrenimi algoritmaları, saldırıları sınıflandırmak için uygulanmıştır.	Weka'dan elde edilen bir bilgi grafiği, kullanılan tüm yaklaşımların karşılaştırılmasını sağlamıştır. SVM (Support Vector Machine) ve Random Forest, daha iyi doğruluk ve ROC eğrisi sunmuştur. Balküpü adli incelemeleri, bir saldırının nasıl çalıştığına dair derin içgörüler sağlamıştır. Balküpü verilerinin analizi, güvenlik duvarı kurallarını güçlendirmek için kullanılmaktadır.	Cowrie honeypot, Naive Bayes, J48 decision tree, Random Forest, SVM	Orta etkileşim: Cowrie kullanılır.	Geçerli değildir (Not Applicable)	SSH ve Telnet hedef alan saldırılar, Kötü niyetli yük teslimi, XOR DDoS saldırıları, Casusluk olarak sınıflandırılan saldırılar	Hayır
Bizim Çalışmamız	Linux sistemlerini hedef alan siber saldırıları tespit etmek ve analiz etmek için bir bal peteği tabanlı yaklaşım kullanılmıştır.	Çalışma, Linux platformlarındaki saldırıların MITRE ATT&CK matrisi kullanılarak nasıl etkili bir şekilde planlanabileceğini ve yürütülebileceğini göstermiştir. Sonuçlar, siber güvenlik uzmanlarının Linux platformlarında karşılaşabilecekleri tehditleri daha iyi anlamalarına ve bu tehditlere karşı etkili savunma stratejileri geliştirmelerine yardımcı olmuştur.	T-Pot Balküpü-Wazuh-auditd-Atomic Red Team	Düşük etkileşimli bal petekleri (MedPot, Honeyd, Dionaea) Orta etkileşimli bal petekleri (HoneyTrap, Snare, Glutton) Yüksek etkileşimli bal petekleri (Cowrie, Hellpot, Redishoneypot)	Evet	Kaba kuvvet girişimleri, Hizmet reddi (DoS) saldırıları, Ağ haritalama saldırıları, SQL enjeksiyon saldırıları, Siteler arası komut dosyası çalıştırma (XSS) saldırıları, Bilinen güvenlik açıklarının istismarı, Veri sızdırma	Evet

Araştırmalarda balküpü platformu olan T-Pot'un kullanımı vurgulanırken, bizim çalışmamız daha kapsamlı bir yaklaşım benimsemektedir. T-Pot'un yanı sıra, bir güvenlik bilgi ve olay yönetimi (SIEM) sistemi olan Wazuh, Linux sistem denetimi için auditd ve saldırı simülasyonu için Atomic Red Team kullanılmaktadır. Bu araçlar birleşimi, saldırıların ve bunların Linux sistemi üzerindeki etkilerinin daha derinlemesine analiz edilmesini sağlamaktadır.

Bizim çalışmamızı diğer çalışmalarla ayıran bir başka faktör, MITRE ATT&CK matrisinin sadece saldırı desenlerini anlamak için değil, aynı zamanda kontrollü bir ortamda saldırıları planlayıp gerçekleştirmek için kullanılmasına odaklanılmasıdır. Bu proaktif yaklaşım, araştırmacıların olası saldırı vektörlerini önceden tahmin etmelerini ve sağlam savunma stratejileri geliştirmelerini mümkün kılmaktadır. Bu tür bir saldırı simülasyonuna vurgu, daha çok gözlemlenen saldırıların reaktif analizine odaklanan diğer araştırmalarda pek belirgin değildir. Ayrıca, hedef kitlesi açıkça belirtilmiştir. Çalışma, siber güvenlik profesyonellerine Linux platformlarını hedef alan tehditlere karşı daha iyi bir anlayış kazandırmayı ve etkili savunma stratejileri oluşturmalarına yardımcı olmayı amaçlamaktadır. Uygulamalı yaklaşıma ve siber güvenlik uzmanlarına yönelik yardım amacına açıkça odaklanılması, bazı diğer araştırmalardan ayıran bir özelliktir; çünkü diğer çalışmalar genellikle daha geniş bir kapsamdadır.

Bu çalışmada sunulan yenilikçi unsur, Linux platformlarına yönelik yapılan siber saldırıların balküpü sistemleri aracılığıyla toplanarak MITRE ATT&CK matrisine dayalı olarak ele alınması ve bu saldırılara ait log verilerinin Wazuh platformunda analiz edilerek yeni kod çözücülerin (decoder) ve kuralların (rules) oluşturulmasıdır. Literatürde, genellikle Windows tabanlı sistemler veya genel saldırı türleri üzerine yapılan çalışmalarda, Linux tabanlı sistemlerin balküpü ortamında bu kadar derinlemesine analiz edilmediği ve saldırıların MITRE ATT&CK çerçevesi üzerinden detaylı şekilde ele alınmadığı görülmektedir. Özellikle, Linux platformları üzerinde balküpü kullanılarak saldırıların tespit edilmesi ve bu verilerin zamanında analiz edilmesi konusunda sınırlı sayıda araştırma yapılmıştır.

Bu çalışma, Linux tabanlı sistemlerinde çeşitli siber saldırı türlerini tespit etmek amacıyla MITRE ATT&CK matrisinin kullanılmasıyla, farklı saldırı tekniklerinin ve prosedürlerinin analiz edilmesi hedeflenmiştir. Saldırılar, SSH kaba kuvvet saldırıları gibi yaygın tehditlerden web tabanlı zafiyetlerin istismarına kadar geniş bir yelpazeyi kapsayacak şekilde ele alınmıştır. Bu tür saldırılardan toplanan log verileri, Wazuh SIEM platformunda analiz edilmiş ve bu saldırı türlerine yönelik özel kod çözücüler (decoder) ve kurallar (rules) geliştirilmiştir. Özellikle, saldırganların kullandığı yöntemlerin ve saldırı tekniklerinin MITRE ATT&CK matrisine dayalı olarak modellenmesi, bu araştırmanın en önemli yeniliklerinden biri olarak belirlenmiştir.

Wazuh ve T-Pot araçlarının seçilme gerekçeleri, literatürdeki güvenlik ihtiyaçları ve bu araçların sunduğu avantajlarla ilişkilidir. Wazuh, güvenlik bilgi ve olay yönetimi (SIEM) alanında kullanılan açık kaynaklı bir araç olarak tanımlanır ve ağ güvenliği ile tehdit tespiti açısından kritik bir rol üstlenir. Literatürde, Wazuh'un gelişmiş olay izleme, güvenlik açığı tespiti ve anomali analizi işlevlerinin ağlardaki tehditleri hızlı ve etkili şekilde tespit ettiği belirtilir. Bu araç, ayrıca merkezi log yönetimi sağlayarak, saldırıların kaydını tutar ve gerçek zamanlı izleme imkânı sunar.

T-Pot ise, saldırganları cezbetmek ve kullandıkları teknikleri anlamak amacıyla kullanılan bir balküpü çözümüdür. Balküpü teknolojilerinin ağ üzerindeki saldırıları gözlemlemek ve detaylarını kaydetmek için faydalı olduğu literatürde vurgulanır. T-Pot, farklı balküpleri araçlarını entegre ederek, çeşitli saldırı türlerini (DDoS, SQL injection, brute force vb.) tespit etmek ve analiz etmek için kapsamlı bir çözüm sunar.

Wazuh ve T-Pot'un birlikte kullanılması, ağ güvenliği ve saldırı tespiti konusunda güçlü bir kombinasyon oluşturur. Wazuh, sistemleri izleyerek tehditleri erken aşamalarda tespit ederken, T-Pot, saldırıların teknik detaylarını analiz etme fırsatı sağlar. Bu sayede, sistemdeki güvenlik açıkları ve saldırganların taktikleri daha iyi anlaşılır, böylece savunma stratejileri geliştirilir.

Wazuh platformu, saldırıların tespiti ve analizinin kolaylaştırılması amacıyla kullanılmış, log verileri bu sistemde detaylı bir şekilde incelenmiş ve yeni kurallar geliştirilmiştir. Bu kurallar, belirli saldırı tekniklerini tanımlamak için MITRE ATT&CK çerçevesine dayalı olarak tasarlanmış ve Linux tabanlı sistemlere özgü saldırılara dair daha kapsamlı bir analiz sağlanmıştır. Ayrıca, bu çalışma ile elde edilen veriler, Wazuh platformunun Linux sistemlerine yönelik tehditleri tanıma ve analiz etme kapasitesinin güçlendirilmesini sağlamıştır.

Literatürdeki mevcut çalışmalar genellikle belirli saldırı türlerinin tespit edilmesine veya savunma stratejilerinin geliştirilmesine odaklanmıştır. Ancak, günümüz siber tehdit ortamının hızla evrimleşmesi ve saldırganların daha sofistike teknikler kullanması nedeniyle, literatürdeki mevcut yaklaşımların bazen yeni tehditleri ve gelişen saldırı tekniklerini yeterince kapsamlı bir şekilde ele almadığı görülmüştür. Bu nedenle, bu çalışma, mevcut literatürdeki eksikliklerin giderilmesi ve daha dinamik bir tehdit tespiti sürecinin sunulması amacıyla ortaya konmuştur. Wazuh ve T-Pot gibi araçların birlikte kullanılması, yalnızca geleneksel saldırı tespit yöntemlerinin değil, aynı zamanda saldırganların taktiklerinin ve yöntemlerinin derinlemesine incelenmesine olanak tanımaktadır. Literatürdeki çoğu çalışmanın, yalnızca tek bir araç ya da yöntemi kullanarak saldırıların tespit edilmesine odaklandığı, bu çalışmada ise çoklu araçların entegrasyonu sağlanarak her iki aracın da güçlü yönlerinden faydalanılmıştır. Wazuh, ağ ve sistem güvenliğini izlerken, T-Pot saldırganların kullandığı teknikleri simüle etmekte ve bu sayede saldırıların gerçek zamanlı olarak izlenmesi mümkün olmaktadır. Bu şekilde hem savunma hem de saldırı analizi açısından daha derinlemesine ve etkili bir bakış açısı elde edilmektedir. Bu çalışma, siber güvenlik alanında daha proaktif bir yaklaşım geliştirilmesine katkı sağlamak amacıyla yapılmıştır. Bu tür bir yaklaşım, literatüre önemli bir katkı sunmakta ve siber güvenlik araştırmalarında daha bütünsel ve dinamik bir güvenlik modelinin oluşturulmasına zemin hazırlamaktadır.

Bu yenilikçi yaklaşım, özellikle Linux tabanlı sistemlerde güvenlik açıklarının tespit edilmesi, analiz edilmesi ve buna yönelik otomatik karşı önlemler geliştirilmesi konusunda önemli bir katkı sağlamaktadır.

8.1. Savunma Önlemleri

Siber güvenlik alanında, Linux tabanlı sistemlere yönelik saldırılara karşı çeşitli savunma önlemleri uygulanmış olmuştur. Brute Force saldırılarına karşı alınan

önlemler arasında, şifre politikalarının güçlendirilmesi ve SSH erişimi için genel anahtar yetkilendirmesi (public key authentication) yönteminin zorunlu kılınması yer almıştır. Ayrıca, Fail2ban gibi araçlar kullanılarak, başarısız giriş denemeleri sayısına göre IP adreslerinin engellenmesi sağlanmış olmuştur. Sistem üzerindeki tüm şüpheli girişler takip edilmiş, zayıf şifreler engellenmiş ve root erişimi için yapılan kötü niyetli giriş denemeleri başarıyla tespit edilmiştir. Port yönlendirme ve gizleme yöntemleri ile, yalnızca güvenli IP adreslerinden erişim sağlanması mümkün kılınmıştır.

DDoS saldırıları gibi yüksek trafikle yapılan saldırılara karşı savunma önlemleri de önemli bir yer tutmuş olmuştur. Bu tür saldırılar için, trafik analizi ve rate limiting gibi teknikler uygulanmış olmuştur. Yük dengeleme (load balancing) yöntemleri ile, anormal trafik birden fazla sunucuya yönlendirilerek, tek bir sunucunun aşırı yüklenmesi engellenmiş olmuştur. Ayrıca, Cloudflare gibi bulut tabanlı hizmetler ile gelen trafik önceden filtrelenmiş ve asıl hedef sistemlere ulaşmadan zararlı trafik engellenmiş olmuştur. Bu önlemler sayesinde, sistemlere yapılan DDoS saldırıları etkin bir şekilde tespit edilmiş ve gerekli aksiyonlar alınmıştır.

Web tabanlı saldırılar, özellikle SQL enjeksiyonu ve XSS gibi tehditlere karşı alınan önlemler de hayati öneme sahip olmuştur. Web Application Firewall (WAF) kullanılarak, web uygulamalarına gelen zararlı istekler tespit edilmiş ve engellenmiş olmuştur. Ayrıca, kullanıcıdan alınan tüm girişler sanitize edilmiş ve prepared statements kullanılarak, SQL enjeksiyonuna karşı güvenlik sağlanmış olmuştur. Bu yöntemler ile, web uygulamaları üzerindeki güvenlik açıkları minimize edilmiş ve siber saldırılara karşı dayanıklılık artırılmış olmuştur. Güvenli kod yazma ve sistem güncellemeleri gibi genel güvenlik önlemleri, Linux tabanlı sistemlerin sürekli olarak güvenli kalmasını sağlamıştır.

Tespit edilen saldırılara karşı alınabilecek savunma önlemleri, saldırı türlerine ve kullanılan araçlara bağlı olarak farklı stratejiler içermektedir. Wazuh ve T-Pot gibi araçlar, bu saldırıları tespit etmek için etkin bir şekilde kullanılmakta ve bu tespitler üzerine uygun savunma önlemleri geliştirilmesi sağlanmaktadır. DDoS (Dağıtık Hizmet Engelleme) saldırıları, ağ üzerindeki kaynakları hedef alarak hizmetin kesintiye uğratılmasına yol açmaktadır. Bu tür saldırılara karşı, ağ trafiği izlenmekte ve anormal trafik artışları tespit edilerek, IP kara listeleri ve trafik sınırlama gibi yöntemlerle savunma önlemleri alınmaktadır. Kaba kuvvet saldırıları, zayıf şifrelerin kırılması amacıyla gerçekleştirilmektedir. Bu tür saldırılara karşı, güçlü şifre politikaları uygulanmakta, hesaplar belirli sayıda hatalı denemeden sonra kilitlenmekte ve çift faktörlü kimlik doğrulama yöntemleri devreye sokulmaktadır. SQL enjeksiyon saldırıları, veri tabanlarına yetkisiz erişim sağlamayı hedeflemektedir. Bu saldırılara karşı, hazırlanan SQL sorguları için hazırlanmış ifadeler kullanılmakta, kullanıcı girdileri doğrulanmakta ve web uygulama güvenlik duvarları (WAF) ile ek bir koruma sağlanmaktadır.

Zafiyet tabanlı saldırılar ise sistemdeki açıkları hedef almaktadır. Bu saldırılar için, sistemlerin düzenli olarak güncellenmesi, güvenlik yamalarının uygulanması ve sistem sertleştirme yöntemleri kullanılmaktadır. Kimlik avı ve sosyal mühendislik saldırıları, kullanıcıları kandırarak kişisel bilgilerini ele geçirmeyi amaçlamaktadır. Bu tür saldırılara karşı, kullanıcılar eğitimle bilinçlendirilmekte, e-posta sistemlerinde gelişmiş spam filtreleme teknikleri kullanılmakta ve kimlik doğrulama protokolleri

devreye sokulmaktadır. Son olarak, fidye yazılımı saldırıları, verilerin şifrelenip fidye talep edilmesiyle gerçekleşmektedir. Bu tür saldırılara karşı, düzenli yedekleme yapılmakta, antivirüs yazılımları kullanılmakta ve erişim denetimleri ile kritik verilere yalnızca yetkili kullanıcıların erişmesi sağlanmaktadır. Bu savunma önlemleri, tespit edilen saldırılara karşı etkili bir koruma sağlamakta ve sistem güvenliği artırılmaktadır.

9. ÖNERİ VE TAVSİYELER

Balküpü tabanlı yaklaşım, siber uzay güvenliğinin artırılmasına ve potansiyel risklerin azaltılmasına katkıda bulunmuş olmuştur. Balküplerinin, saldırganları kendilerine çekerek, güvenlik uzmanlarının potansiyel tehditleri gerçek ağı etkilemeden önce proaktif olarak tespit ve analiz etmelerine olanak tanıdığı gözlemlenmiş olmuştur. Bu sayede tehditlerin erken azaltılması mümkün kılınmış olmuştur. Balküpleri, saldırgan davranışı, taktikleri ve teknikleri hakkında ayrıntılı bilgi sağlayarak güvenlik ekiplerinin potansiyel tehditleri daha kapsamlı bir şekilde anlamasını ve analiz etmesini sağlamış olmuştur. Balküplerinin kullanımı sayesinde kuruluşlar, sistem ve uygulamalarındaki güvenlik açıkları hakkında içgörü kazanmış ve bu zayıflıkları gerçek saldırganlar tarafından istismar edilmeden önce ele alıp yamalamışlardır.

Genel anlamda yapılması gereken güvenlik önlemleri söz konusu olmuştur. Örneğin, MFA kullanılarak kimlik bilgileri erişim girişimlerinin önüne geçilmesi sağlanmış olmalıdır. Sistemlerin ve uygulamaların düzenli olarak güncellenmesi ve güvenlik yamalarının uygulanması sağlanmış olmalıdır. Yanal hareketlerin önlenmesi için ağ segmentasyonu yapılmış ve kritik sistemler izole edilmiştir. Ayrıca, güvenlik olaylarının ve logların düzenli olarak incelenmesi, anormal aktivitelerin tespitini hızlandırmış olmalıdır. Hassas verilerin şifrelenmesi, yetkisiz erişimlerin etkisini en aza indirmiş olmalıdır. Kullanıcılara yönelik düzenli siber güvenlik eğitimleri verilmiş ve farkındalık artırılmış olmalıdır. Ağ cihazları ve yazılımları düzenli olarak güncellenmiş ve güvenlik açıkları kapatılmış olmalıdır. Ağ trafiği sürekli izlenmiş ve anormallikleri tespit etmek için analiz araçları kullanılmış olmalıdır. Çalışanlara ağ güvenliği konusunda eğitim verilmiş ve farkındalık artırılmış olmalı ve kritik verilerin düzenli olarak yedeklenmesi sağlanmış olmalıdır. Felaket kurtarma planları oluşturulmuş ve uygulanabilir hale getirilmiş olmalıdır.

Olası bir siber saldırı durumunda hızlı ve etkili müdahale için olay müdahale planlarının hazırlanmış ve test edilmiş olması gerekmektedir. Kullanıcı ve sistem ayrıcalıkları minimum yetki prensibine göre yönetilmiş ve düzenli olarak gözden geçirilmiş olmalıdır. Güvenlik duvarları ve IDS/IPS (Intrusion Detection System/Intrusion Prevention System) kullanılarak ağ trafiği izlenmiş ve kontrol altında tutulmuş olmalıdır. Bu sistemler, anormal trafik davranışlarını tespit ederek saldırıları engellemiş olabilmektedir. DDoS saldırılarına karşı bulut tabanlı koruma hizmetlerinin kullanılması sağlanmış ve ağ segmentasyonu yapılarak saldırıların yayılması önlenmiş olmalıdır. UDP protokolüne yönelik olarak DNS güvenliği sağlanmış, oran sınırlama (rate limiting) uygulanmış ve gelen UDP paketleri doğrulanarak yalnızca meşru trafik kabul edilmiş olmalıdır. ICMP ve IPv6-ICMP trafiğinde gereksiz paketler filtrelenmiş ve ağ haritalaması saldırılarına karşı önlemler alınmış olmalıdır.

Genel güvenlik önlemleri kapsamında, ağ cihazları ve yazılımları düzenli olarak güncellenmiş ve güvenlik açıkları kapatılmış olmalıdır. Ağ trafiği sürekli izlenmiş ve anormallikleri tespit etmek için analiz araçları kullanılmış olmalıdır. Çalışanlara ağ güvenliği konusunda eğitim verilerek farkındalık artırılmış ve kritik verilerin düzenli olarak yedeklenmesi sağlanmış olmalıdır. Felaket kurtarma planları oluşturulmuş ve uygulanabilir hale getirilmiş olmalıdır.

Bu önlemler, Linux platformlarında MITRE ATT&CK matrisine yönelik saldırıların etkili bir şekilde tespit edilmesi ve önlenmesi için kritik öneme sahip olmuştur. Bu önlemler, sistemlerin güvenlik seviyesini yükseltmiş ve olası siber tehditlere karşı daha dirençli hale getirilmiş olmuştur.

Araştırmamız, Linux platformunda MITRE ATT&CK matrisinin saldırıların planlanması ve uygulanması sürecindeki rolünün ortaya koyulmuş olduğu kabul edilmiştir. Bundan sonra yapılacak çalışmalar, mevcut araştırmanın bulgularına dayanarak derinlemesine analizlerin sunulmuş olabileceği düşünülmektedir. Özellikle, farklı Linux dağıtımları üzerinde MITRE ATT&CK matrisi temelli daha karmaşık ve gerçekçi saldırı senaryolarının simülasyonlarına odaklanılmış olabileceği öngörülmektedir. Bu senaryoların, güvenlik sistemlerinin tepki süreçlerini ve saldırı tespit mekanizmalarını nasıl etkilediğini anlamak için daha geniş kapsamlı bir veri setinin kullanılmış olabileceği tahmin edilmektedir. Ayrıca, makalemizde belirtilen savunma stratejilerinin, gerçek dünya koşullarında nasıl uygulanabileceği ve iyileştirilebileceği üzerine uygulamalı çalışmalar yapılmış olabileceği ifade edilmektedir. Bu çalışmalar, Linux tabanlı sistemlerde siber güvenlik önlemlerinin güçlendirilmesine yönelik yeni yaklaşımların geliştirilmesine katkı sağlanmış olabilecektir.

Gelecekteki araştırmalar, Linux sistemlerinde siber güvenliğin artırılması için yeni teknoloji ve araçların entegrasyonu hedeflenmiş olmalıdır. Örneğin, yapay zekâ (AI) ve makine öğrenimi (ML) tabanlı tehdit analiz araçlarının kullanımı, MITRE ATT&CK matrisinde belgelenen saldırı taktiklerinin daha hızlı ve etkin bir şekilde tespit edilmesi için önemli bir potansiyele sahip olmuştur. Bu teknolojiler, büyük veri kümelerinin analiz edilerek anormal davranışların belirlenmesi ve saldırıların olası hedeflerinin öngörülmesi sağlanmış olabilir. Ayrıca, otomatik yanıt mekanizmalarının geliştirilmesi ve bu teknolojilerle entegrasyonu, saldırılara karşı daha hızlı tepki verilmesini sağlamış olabilir. Bu bağlamda, Linux platformunda AI ve ML teknolojilerinin güvenlik operasyonlarına nasıl uygulanacağı ve mevcut savunma stratejilerinin nasıl iyileştirileceği üzerine uygulamalı çalışmalar yapılmış olmalıdır. Bu çalışmalar, siber tehditlere karşı savunma kapasitelerinin artırılması için önemli bir adım olarak kabul edilmiş olabilir.

Yazarların Katkısı

Bu çalışmada 1. yazar fikir, araştırma, veri toplama, analiz, bilgisayar ortamının sağlanması, kaynak taraması ve makalenin yazımı konusunda katkıda bulunmuştur. 2. yazar düzeltme, gözden geçirme, analiz ve yorum konusunda katkı sağlamıştır.

Çıkar Çatışması Beyanı

Yazarlar arasında herhangi bir çıkar çatışması bulunmamaktadır.

Araştırma ve Yayın Etiği Beyanı
Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

KAYNAKÇA

Abbas-Escribano, M., & Hervé D. (2023). An Improved Honeypot Model for Attack Detection and Analysis. *ACM International Conference Proceeding Series*, doi:10.1145/3600160.3604993.

Afenu, D. S., Asiri, M. & Saxena, N. (2024). Industrial Control Systems Security Validation Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework. *Electronics (Switzerland)* 13(5). doi:10.3390/electronics13050917.

Al-Sada, B., Sadighian, A. & Oligeri, G. (2024). Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database. *IEEE Access* 12. doi:10.1109/ACCESS.2023.3344680.

Amal, M. R., & P. Venkadesh. (2023). H-DOCTOR: Honeypot based firewall tuning for attack prevention. *Measurement: Sensors* 25. doi:10.1016/j.measen.2022.100664.

Andrew, Y, Lim, C. & Budiarto, E. (2022). Mapping Linux Shell Commands to MITRE ATT&CK using NLP-Based Approach. *Proceedings of the International Conference on Electrical Engineering and Informatics*, doi:10.1109/ICELTICs56128.2022.9932097.

Candidate, A., & Ayala, G. (2024). *POLITECNICO DI TORINO Master's Degree in ICT FOR SMART SOCIETIES Honeypot in a box: A distributed cluster network for honeypot deployment Supervisors Prof. Marco MELLIA Prof. Idilio DRAGO*.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors* 21(9). doi:10.3390/s21093267.

Hobert, K,. Lim, C. & Budiarto, E. (2023). Enhancing Cyber Attribution through Behavior Similarity Detection on Linux Shell Honeypots with ATT&CK Framework. *Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICoCICs 2023*, doi:10.1109/ICoCICs58778.2023.10276639.

Hussein, M.A., & Hamza, E.K. (2022). Secure Mechanism Applied to Big Data for IIoT by Using Security Event and Information Management System (SIEM). *International Journal of Intelligent Engineering and Systems* 15(6). doi:10.22266/ijies2022.1231.59.

Javadpour, A., Ja'fari, F., Taleb, T., Shojafar, M., & Benzaïd, C. (2024). A comprehensive survey on cyber deception techniques to improve honeypot performance. *Computers and Security* 140. doi:10.1016/j.cose.2024.103792.

José, C. & Santander, M. (2024). Learning Models to Detect Personality Traits of Cyber Attackers: A Combined Approach Using Honeypot and Surveys. doi:10.1007/978-3.

Kovar, R. & Paine, K. (2024). The CISO Report. *https://www.splunk.com/en_us/pdfs/gated/ebooks/the-ciso-report.pdf* adresinden 16 Kasım 2024 tarihinde alınmıştır.

Koutsikos, I. (2024). *Improving Infrastructure Security using Deceptive Technologies*.

Liao, M.L., Yu, C.L., Lai, Y.C., Chiu, S.P. & Chen, J.L. (2023). An Intelligent Cyber Threat Classification System. *International Conference on Advanced Communication Technology, ICACT*, doi:10.23919/ICACT56868.2023.10079405.

Mitre Att&Ck. (2023). Techniques - Enterprise | MITRE ATT&CK®. *Techniques*.

Mohd Fuzi, M. F., Mazlan, M.F., Jamaluddin, M.N.F. & Halim, I.H.A. (2024). Performance analysis of network intrusion detection using T-Pot honeypots. *Journal of Computing Research and Innovation* 9: 348–60. https://ir.uitm.edu.my/id/eprint/103968 adresinden 16 Kasım 2024 tarihinde alınmıştır.

Muhammad, S. & Hafee, A.U. (2024) *Investigating Threats to ICS and SCADA Systems Via Honeypot Data Analysis and SIEM*. https://www.researchgate.net/publication/382398394 adresinden 16 Kasım 2024 tarihinde alınmıştır.

Mungsing, S. & Sringendee, K. (2024) *Developing Proactive Cyber Threat Defense Systems on Server Computers Using Honeypot Techniques*. http://www.ijert.org.

Palmer, D. (2024). Linux malware attacks are on the rise, and businesses aren't ready for it. *https://www.zdnet.com/article/linux-malware-attacks-are-on-the-rise-and-businesses-arent-ready-for-it/* adresinden 16 Kasım 2024 tarihinde alınmıştır.

Raghul, S. A., Gayathri, G., Bhatt, R. & Varun Kumar, K. A. (2024). Enhancing Cybersecurity Resilience: Integrating IDS with Advanced Honeypot Environments for Proactive Threat Detection. *Proceedings of the 3rd International Conference on Applied Artificial Intelligence and Computing, ICAAIC 2024*, Institute of Electrical and Electronics Engineers Inc., 1363–68. doi:10.1109/ICAAIC60222.2024.10575865.

Rashid, S.M.Z.U, Haq, A., Hasan, S.T., Furhad, M.H., Ahmed, M. & Ullah, A.B. (2024). Faking smart industry: exploring cyber-threat landscape deploying cloud-based honeypot. *Wireless Networks* 30(5). doi:10.1007/s11276-022-03057-y.

Rawat, S. (2024). *Enhancing False Positive Detection in IDS/IPS Using Honeypots: A Case Study with CSE-CIC-2018 Dataset*.

Shrivastava, R.K., Bashir, B. & Hota, C. (2019). Attack detection and forensics using honeypot in IoT environment. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, doi:10.1007/978-3-030-05366-6_33.

Sikandar, H.S., Sikander, U., Anjum, A. & Khan, M.A. (2022). An Adversarial Approach: Comparing Windows and Linux Security Hardness Using Mitre ATT&CK Framework for Offensive Security. *IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI, HONET 2022*, doi:10.1109/HONET56683.2022.10018981.

Singh, N. & Tripathy, S. (2024). It's too late if exfiltrate: Early stage Android ransomware detection. *Computers and Security* 141. doi:10.1016/j.cose.2024.103819.

Srinivasa, S., Pedersen, L.M. & Vasilomanolakis, E. (2023). Gotta Catch 'em All: A Multistage Framework for Honeypot Fingerprinting. *Digital Threats: Research and Practice* 4(3). doi:10.1145/3584976.

Xiong, W., Legrand, E., Åberg, O. & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling* 21(1): 157–77. doi:10.1007/s10270-021-00898-7.

Yang, X., Yuan, J., Yang, H., Kong, Y., Zhang, H. & Zhao, J. (2023). A Highly Interactive Honeypot-Based Approach to Network Threat Management. *Future Internet* 15(4). doi:10.3390/fi15040127.

Yousaf, A. & Zhou, J. (2024). From sinking to saving: MITRE ATT &CK and D3FEND frameworks for maritime cybersecurity. *International Journal of Information Security*. doi:10.1007/s10207-024-00812-4.

Zahid, H., Hina, S., Hayat, M.F. & Shah, G.A. (2023). Agentless Approach for Security Information and Event Management in Industrial IoT. *Electronics (Switzerland)* 12(8). doi:10.3390/electronics12081831.