Journal of Computer Science
https://dergipark.org.tr/en/pub/bbd

ISSN,e-ISSN: 2548-1304
Volume:IDAP-2023, pp:24-30, 2023
https://doi.org/10.53070/bbd.1347019
Research Paper

Siber Güvenlikte T-Pot Honeypot Uygulanması: Kurumsal Ağ Üzerinde Örnek Durum Çalışması

Implementing T-Pot Honeypot in Cyber Security: A Case Study on an Enterprise Network

Çağatay Kılınç[1], Özgü Can[*2]

[1] Fen Bilimleri Enstitüsü, Ege Üniversitesi, Bornova-İzmir, Türkiye

[2]Bilgisayar Mühendisliği Bölümü, Ege Üniversitesi, Bornova-İzmir, Türkiye

(cagatay1klnc@gmail.com, ozgu.can@ege.edu.tr)

Received:Aug.30,2023 Accepted:Oct.16,2023 Published:Oct.18,2023

Özetçe— Honeypot (bal küpü), saldırganların ilgisini çekmek ve saldırıları analiz etmek amacıyla gerçek sunucuları taklit eden sanal sistemlerdir. Honeypot'lar siber tehdit aktörlerinin oluşturduğu tehditlerin, gerçek sistemler yerine önceden hazırlanmış ve büyük oranda gerçek sistemleri taklit eden tuzak sistemlere yöneltilmesini sağlayarak siber güvenliğe katkıda bulunur. Ayrıca, topolojide konumlandırıldığı yerle de ilişkili olarak tuttuğu loglar aracılığıyla iç ve/veya dış tehditlerin ortaya çıkarılmasında, atak vektörlerinin belirlenmesinde ve tehdit aktörlerinin teknik, taktik, prosedürlerinin analiz süreçlerinde birincil kaynak olarak kullanımıyla da ön plana çıkar. Honeypotların gelişimiyle beraber farklı alanlarda özelleşmiş honeypotlar da ortaya çıkmıştır. Örneğin IoT (Nesnelerin İnterneti), Endüstriyel Kontrol Sistemleri ve Bulut Bilişim gibi özelleşmiş alanlara yönelik açık kaynak ve lisanslı honeypotlar da mevcuttur. Bu kapsamda, birden fazla honeypotu bünyesinde barındıran ve sahip olduğu görselleştirme yeteneğiyle ön plana çıkan T-pot servisi kullanım kolaylığı ve çok yönlü platform özelliğiyle ön plana çıkmaktadır. Bu çalışmada, honeypotlar ve honeypot türleri açıklanmakta ve bir durum çalışması sunulmaktadır. Durum çalışması, bir kurumsal ağa yerleştirilmiş T-pot servisinin çıktılarını göstermektedir. Bu çalışmada ayrıca bu çıktıların güvenlik araçlarına nasıl kaynak olabileceği de sunulmaktadır.

Anahtar Kelimeler : *Honeypot, T-pot, Siber Güvenlik, Siber Saldırgan.*

Abstract— Honeypots are virtual systems that emulate real servers to attract attackers and analyze attacks. Honeypots contribute to cyber security by ensuring that threats posed by cyber threat actors are directed to decoy systems that are pre-made and largely mimic real systems, rather than authentic systems. Besides, it also comes to the forefront with its use as a primary source in the detection of internal and/or external threats, the determination of attack vectors and the analysis processes of the technical, tactical and procedures of threat actors through the logs it keeps in relation to its location in the topology. With the development of honeypots, honeypots specialized in different fields have also emerged. For example, open source and licensed honeypots are also available for specialized fields such as IoT (Internet of Things), Industrial Control Systems, and Cloud Computing. In this context, T-pot service, which includes more than one honeypot and stands out with its visualization ability, stands out with its ease of use and versatile platform feature. In this study, honeypot and types of honeypots are explained and a use case study is presented. The use case study shows the outputs of T-pot service placed in an enterprise network. The study also presents how these outputs can be a source of security instruments.

Keywords : *Honeypot, T-pot, Cyber Security, Cyber Attacker.*

1. Giriş

Giderek artan iletişim ihtiyacı doğrultusunda ortak ağların kullanımı giderek artmakta ve hemen hemen her sektörde bilgisayar ve İnternet teknolojileri kullanılmaktadır. Ancak artan bu kullanım, beraberinde birçok güvenlik tehdidini de getirmiştir. Bu noktadan yola çıkarak çözüm üretmeye çalışan güvenlik analistleri çeşitli güvenlik yaklaşımları geliştirmişlerdir. Honeypot teknolojileri ağları ve cihazları tehditlerden korumak, erken uyarı, istihbarat toplama gibi görevler için kullanılmaktadır. Zaman içerisinde çeşitlenen ve genişleyen tehdit algısı sebebiyle güvenlik çözümleri daha spesifik hale gelmiş, bu özelleşme süreci honeypot sistemlerine de yansımıştır. SSH honeypot, HTTP honeypot, veritabanı honeypot, e-mail honeypot, IoT honeypot gibi pek çok honeypot tipinin ortaya çıkması bu güvenlik ihtiyacının sonucudur. Bu noktada tuzak görevi gören ve saldırgana ve saldırıya özel

istatistik ve log tutan bu yapılardan alınan verilerin analiz edilmesi adına görselleştirilmesi, tek bir kaynak üzerinden istatistiklere dayalı veri elde edilmesi gibi konu başlıkları honeypotların gelişim sürecini yönlendirmiştir. Elde edilen logların bir istihbarat servisinde kullanılması ve güvenlik duvarı, saldırı tespit ve korunma sistemleri, güvenlik duvarları, siber istihbarat platformları gibi mevcut güvenlik enstrümanlarına giriş verisi olarak verilmesi süreçleri de tek kaynak çoğul platform anlayışına zemin hazırlamıştır. Özellikle güvenlik operasyonlarını yönetecek profesyonel personelin sayıca az olduğu organizasyonlarda tek bir yönetim arayüzü aracılığıyla müdahale ve kontrol sağlanan platformlar tercih sebebi olmaktadır. T-pot yapısında bulunan birden fazla honeypot servisi, ELK ve Kibana aracılığıyla sağladığı görsel ve istatiksel merkezi ve çok özellikli platform olarak ön plana çıkmaktadır. Bu çalışma, honeypot teknolojilerine, honeypot türlerine, ağa yerleştirilen T-pot servisinin çıktılarına ve bu çıktıların güvenlik enstrümanlarına nasıl kaynak olabileceğine odaklanmaktır.

Çalışmanın organizasyonu şu şekildedir: ikinci bölümde honeypot ve T-pot açıklanmakta, üçüncü bölümde çalışma kapsamında bir kurum ağı üzerinde yürütülen örnek durum çalışması sunulmakta, son olarak dördüncü bölümde öneriler verilmekte ve çalışmanın sonuçları değerlendirilmektedir.

2. Temel Kavramlar

Honeypot kelimesinin literatürde yer aldığı ilk akademik yayınlar 2000'li yılların başına kadar uzanmaktadır. Geniş çapta kabul gören tanım Spitzner tarafından sunulmuştur (Spitzner, 2003). Bu tanıma göre honeypot, sorgulanmak, saldırıya uğramak veya tehlikeye atılmak gibi özelliklere sahip olan bir sahte bilgisayar kaynağıdır. Bununla beraber, honeypot kavramı yeni değildir ve bilgi koruma ve ağ savunması alanında 1990'lı yıllarda kısmen kullanılmakla beraber farklı şekillerde adlandırılmıştır (Stoll, 1989; Cohen, 1998; Cheswick, 1991). Daha sonraki dönemlerde, birden çok honeypot birbirine bağlanarak honeynet adını almıştır. İlk kez bilinen bir tehdide odaklanan honeypotlardan biri, sub7 kötü amaçlı yazılımını analiz etmek için kullanılmıştır. Honeypot, birçok solucanın ardışık saldırılar için kullandığı 27374 numaralı bağlantı noktasına yanıt vererek sub7 trojanı tarafından enfekte edilmiş bir Windows sistemi taklit etmiştir. SANS Enstitüsü (SANS, 2023), W32/Leaves solucanını dakikalar içinde yakalamıştır. Günümüzde, honeypotlar zafiyetlere karşı etkili bir kavram olarak kabul edilmektedir. Bu amaçla hem saldırı hem de savunma amacı ile kullanılmaktadır. Karabay ve Eyüpoğlu (2023), honeypotların saldırı ve savunma amacı ile kullanımlarına ilişkin bir inceleme çalışması sunmaktadır.

2.1. Honeypot

Bir honeypot, kurban bir bilgisayar veya cihaza yetkisiz erişim ve erişim girişimleri hakkında veri toplayan bir bilgisayar güvenlik aracıdır (Campbell, Padayachee ve Masombuka, 2015). Bir honeypot, bir saldırganla etkileşime girerken meşru hizmetleri taklit ederek etkileşime girer. Bu etkileşimler daha sonra analiz edilmek üzere günlüğe kaydedilir ve güvenlik uyarıları için temel oluşturur. Honeypotlar amaçlarına ve etkileşim seviyelerine göre sınıflandırılabilir. Bu nedenle, honeypotlar Production Honeypot veya Research honeypot olarak sınıflandırabilirler (Zhang et al., 2003).

Production Honeypotlar, personele yetkisiz erişim girişimlerini bildirirken. Research Honeypotları, eğilimleri görmek için saldırganlardan olabildiğince fazla bilgi toplar ve iş dünyasında, devlette ve akademide kullanılır. Honeypotlar, düşük etkileşimli veya yüksek etkileşimli olabilir (Alata et al.,2006). Düşük etkileşimli bal küpleri, birkaç hizmeti taklit eder, temel yanıtlar sağlar, ancak gerçek bir sistemin yapacağı gibi daha karmaşık bir saldırıya yanıt veremez. Düşük etkileşimli honeypotların konuşlandırılması kolaydır ancak honeypot servisleri olarak kolayca belirlenebilir. Yüksek etkileşimli honeypotlar olabildiğince gerçek görünür ve hatta bir saldırganın etkileşime girmesi için bütün bir sanal sistemi içerebilir.

2.2. T-pot

T-pot (Telekom Security, 2023) bir honeypot dağıtım platformudur. T-pot, Debian 11 (Bullseye) Netinstaller'ı temel alır ve mümkün olduğu kadar çok aracı aynı anda çalıştırma ve böylece ana bilgisayarın donanımını maksimumda kullanma hedefine ulaşmak için docker ve docker-compose'u kullanır. T-Pot, aldatma aksiyonunu daha da geliştirmek için Elastic Stack, animasyonlu canlı saldırı haritaları ve çok sayıda güvenlik aracını kullanan 20'den fazla honeypot ve sayısız görselleştirme seçeneğini destekler.

Kullanıcılar birden çok şablon arasından seçim yapabilir. Örneğin, "tıbbi" şablonunda Dicompot (Keri, Lechthaler ve Ochse, t.y.) ve Medpot (Schmall, Vorbach ve Ochse, t.y.) gibi honeypotlar, sağlıkla ilgili protokollere yönelik saldırı yüzeyleri sağlamaktadır, Endüstriyel Kontrol Sistemleri şablonunda ise Conpot ve Cowrie bulunmaktadır. Şablonlar ayrıca Cockpit (Red Hat, 2023), Elastic Stack (Elastic Stack, 2023) ve Suricata (Open Information Security Foundation (OISF), 2023) gibi analiz ve gerçek zamanlı izleme araçları da içermektedir.

T-Pot, konteyner adı verilen örneklerde sanal işletim sistemlerinde yazılım çalıştırabilen bir program olan Docker'ı (Combe, Martin ve Di Pietro, 2016) kullanır. Bu konteynerlar, ana makinede kolayca yönetilebilir ve yapılandırılabilir ve tek bir makine birçok Docker kapsayıcısını çalıştırabilir. T-Pot'ta her bir honeypot ve araç

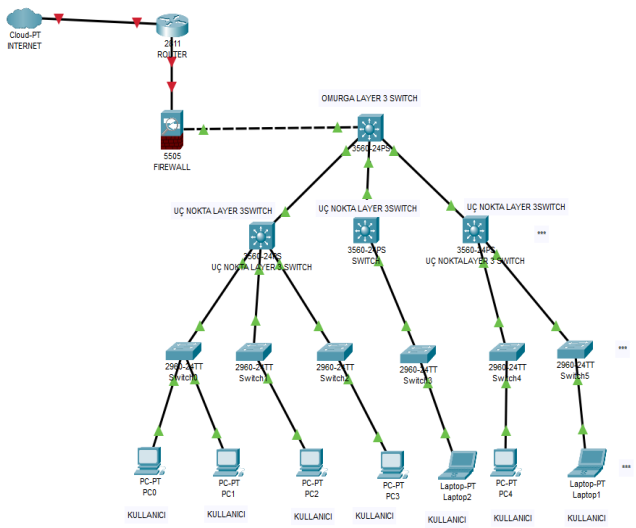
konteynerlaştırılmıştır ve ayrı Docker konteynerlarında çalışır; bu, modülerliğin yanı sıra yazılımı doğrudan makinede çalıştırmaya kıyasla daha iyi güvenlik sağlar.

Cockpit, Linux sunucuları için web tabanlı bir grafiksel kullanıcı arayüzüdür. T-Pot'un çalıştığı sistem üzerinde izleme ve yönetim işlemleri gerçekleştirir. İşlemci kullanımı, bellek ve disk 'I/O' gibi canlı grafikler gibi bazı bilgileri, DigitalOcean kontrol panelinde aktarır. Cockpit ayrıca çalışan Docker konteynerlerini, sistem hizmetlerini ve uygulamaları izler. Yazılım güncellemeleri yapabilir, yeni kullanıcı hesapları oluşturabilir ve web tabanlı bir terminal oturumu sağlayabilir. Genel olarak, Cockpit, yalnızca SSH ile kıyaslandığında T-pot kurulumunun daha kolay yönetimini sağlar.

Elastic Stack üç programdan oluşur: Elasticsearch, Logstash ve Kibana. Logstash, honeypot ve araç günlüklerinden gelen verileri Elasticsearch veritabanına gönderir. Elasticsearch, JavaScript Object Notation (JSON) kullanarak arama ve analiz yapar. Kibana, Elasticsearch veri tabanı için bir veri görselleştirme aracıdır. Kibana, önceden tanımlanmış panoları kullanarak kullanıcının tekil honeypotlardan, Suricata gibi bireysel araçlardan veya honeypotlar ve araçlarla ilgili genel bir "T-Pot Gösterge Paneli"nden verileri görüntülemesine olanak tanır. Suricata, hem bir sızma tespit sistemi (Intrusion Detection System, IDS) hem de sızma önleme sistemi (Intrusion Prevention System, IPS) olarak hareket edebilen bir tehdit tespit motorudur. T-pot içinde, Suricata yalnızca zararlı faaliyetleri tespit eder ve bunları ilişkili CVE (Common Vulnerabilities and Exposures) kodlarıyla birlikte günlüğe kaydeder. Suricata, saldırıların şiddeti, kategorisi ve imzası gibi ayrıntılarla gerçek zamanlı analiz sağlar. Suricata, honeypotların yakaladığından daha fazla paketi inceleyerek tüm alınan paketleri denetler. Örneğin, Suricata, SYN ve URG bayraklarının ayarlandığı ancak TCP 3-yönlü el sıkışmayı tamamlamayan ve HTTP yükü olmayan TCP (Transmission Control Protocol) paketlerini tespit eder, bu nedenle bunlar HTTP honeypotlarıyla etkileşime girmez. Suricata, bu paketleri endüstriyel kontrol sistemleri gibi cihazlarda kullanılan gerçek zamanlı bir işletim sistemi olan VxWorks'teki (Seri et al., 2019) önemli güvenlik açıklarıyla ilişkili olarak tanımlar. Bu ek veri noktaları aynı şekilde Elastic Stack'e aktarılır ve Kibana gösterge panelinde görüntülenebilir.

3. Kurum Ağı Üzerinde T-pot Servisinin Uygulanması

Şekil 1'de gösterilen topolojiye sahip kurum ağında T-pot servisi yönetici VLAN'indeki bir cihaza sanal makine üzerinde kurulmuştur. T-pot servisinin önerilen sistem gereksinimleri 8-16 GB RAM ve 128 GB boş disk alanı olarak belirtilse de kaynakların sınırlı olması nedeniyle minimum değerler olan 8GB RAM ve 70 GB boş disk alanı T-pot servisi için ayrılmıştır.

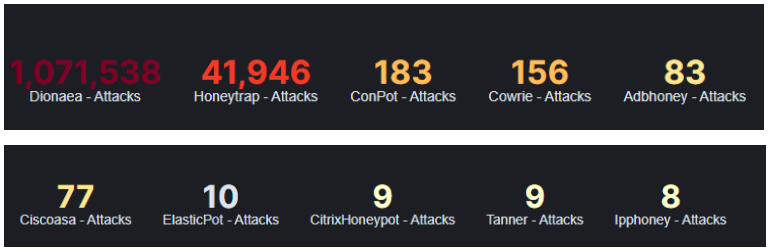


Şekil 1. Kurum topolojisi

Kurum topolojisinde, router aracılığıyla kurum ağı internet ile haberleşirken router'ın arkasında konumlandırılan yeni nesil güvenlik duvarı kurum iç ağını belirli kural setleri aracılığıyla dış ağdan korur. İçeride omurga katman 3 görevinde bulunan merkezi switch uç noktalardaki katman 3 switchler ile birlikte VLAN yapısını oluşturur ve kenar switchler aracılığıyla son kullanıcıya bağlantı sağlanır. Yönetici VLAN'inde ayağa kaldırılan servisin çalışma süresi 11 gündür. Bu süre zarfında çalışan T-pot servisi kurum iç ağında meydana gelen ve gelebilecek tehdit durumlarını ortaya çıkarmak için kullanılmıştır.

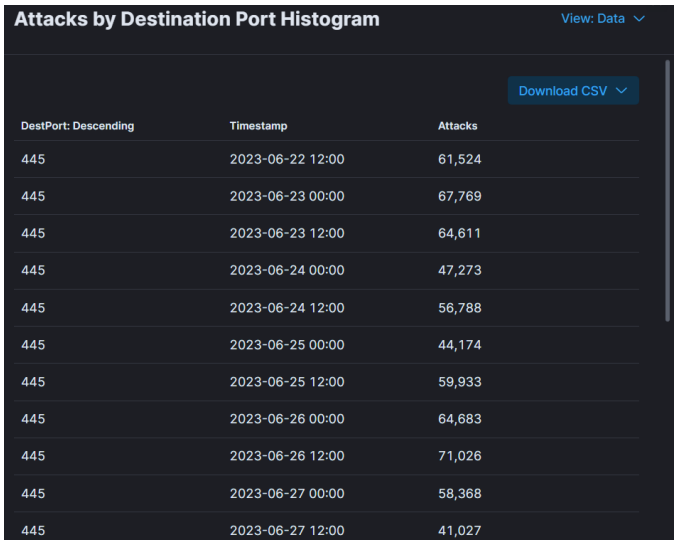
T-pot servisi üzerinde bulunan 20'den fazla honeypot servisinin 11 günlük süreçte aldığı saldırı sayısı Şekil 2'de gösterilmektedir. Kibana'nın arayüzünden alınan Şekil 2 de gösterildiği üzere Dionaea honeypot 11 günlük süreçte 1,701.538 saldırı sayısıyla ön plana çıkmaktadır. Dionaea honeypot, siber saldırganların davranışlarını ve saldırılarını analiz etmek için kullanılan bir tür honeypot yazılımıdır. Dionaea, saldırganların ve saldırganlar

tarafından zararlı bulaştırılmış yapıların zararlı faaliyetlerini taklit eden ve onları çekmek için kullanılan bir tuzak olarak tasarlanmıştır. Dionaea, birçok farklı protokol ve hizmeti emüle ederek saldırganların ilgisini çekmeyi hedefler. Bu protokoller arasında FTP, HTTP, SMB, Telnet ve daha fazlası bulunmaktadır.



Şekil 2. T-pot servisi üzerinde kurulu honeypotlara gelen toplam saldırı sayısı

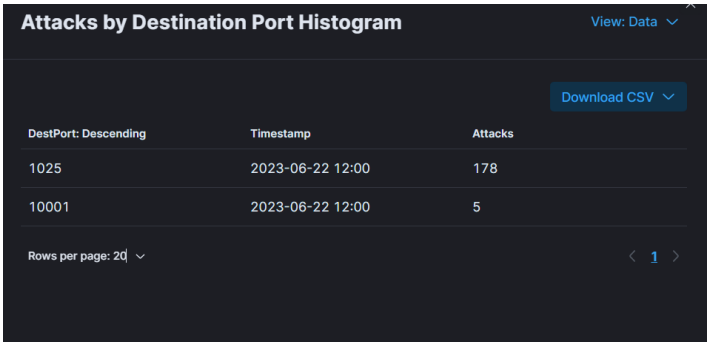
41.946 atak sayısıyla onu takip eden honeypot servisi olan Honeytrap TCP veya UDP servislerine yönelik saldırıları gözlemlemek için yazılmış ve daha çok ağ güvenliğine yönelik bir servis olarak ön plana çıkar. Daemon olarak çalışır ve istenen bağlantı noktalarında dinamik olarak sunucu işlemleri başlatır. Bir sunucu, yakalanan ağ trafiğini bağlı bir ana bilgisayara göndererek bir tanınmış servisi taklit eder. Şekil 3'te gösterildiği gibi servisin aktif olduğu 11 günlük süreç boyunca 445 portu hedef alınmıştır.



DestPort: Descending	Timestamp	Attacks
445	2023-06-22 12:00	61,524
445	2023-06-23 00:00	67,769
445	2023-06-23 12:00	64,611
445	2023-06-24 00:00	47,273
445	2023-06-24 12:00	56,788
445	2023-06-25 00:00	44,174
445	2023-06-25 12:00	59,933
445	2023-06-26 00:00	64,683
445	2023-06-26 12:00	71,026
445	2023-06-27 00:00	58,368
445	2023-06-27 12:00	41,027

Şekil 3. Dionaea Honeypot'un 445 portuna gelen saldırı sayıları

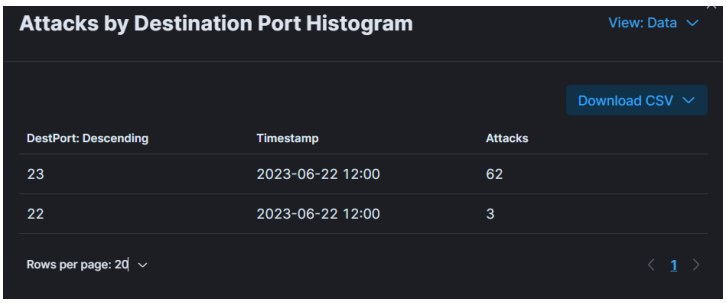
Üçüncü sırada ise 183 saldırı sayısıyla ConPot honeypot gelmektedir. Conpot, kolayca dağıtılabilen, değiştirilebilen ve genişletilebilen bir düşük etkileşimli Endüstriyel Kontrol Sistemleri sunucu tarafı honeypotudur. Şekil 4'te ConPot Honeypot'a gelen saldırılar görülmektedir.



DestPort: Descending	Timestamp	Attacks
1025	2023-06-22 12:00	178
10001	2023-06-22 12:00	5

Şekil 4. ConPot Honeypot'un 1025 ve 10001 portuna gelen saldırı sayıları

Servislerin yanıt süreleri, sürekli yük altındaki bir sistemin davranışını taklit etmek için yapay olarak geciktirilebilmektedir. Şekil 5'te sunulan Cowrie honeypot 156 atak sayısıyla dördüncü sırada yer almaktadır.

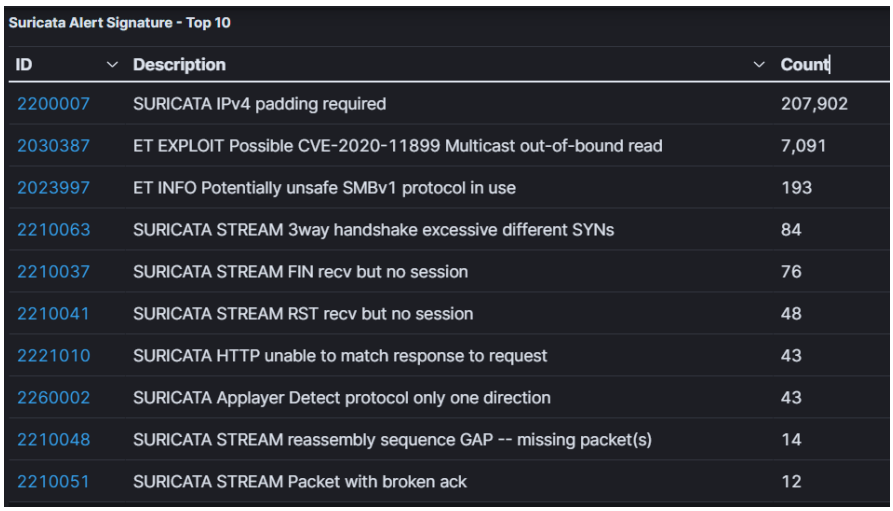


Şekil 5. Cowrie Honeypot'un 23 ve 22 portuna gelen saldırı sayıları

Cowrie, SSH (Secure Shell) protokolünü hedef alan bir honeypot veya tuzak sistemidir. Cowrie, gerçek bir SSH sunucusunu taklit ederek saldırganların SSH erişimi sağlamaya çalıştığı bir ortam sunar. Saldırganlar, Cowrie honeypotuna bağlanmaya çalıştıklarında, tüm etkileşimler kaydedilir ve analiz edilir. Cowrie honeypotu, saldırganların kullanıcı adları ve parolaları denemesi, komutlar göndermesi ve diğer SSH etkileşimlerini kaydeder. Bu sayede, saldırganların kullanılan saldırı vektörleri, sık kullanılan saldırı yöntemleri ve hedefledikleri servisler gibi bilgiler elde edilebilir. Ayrıca, Cowrie honeypotu, saldırganların hareketlerini izleyerek saldırılar hakkında daha fazla bilgi edinme ve güvenlik önlemlerini geliştirme imkânı sağlar. Cowrie honeypotunun bir diğer özelliği, saldırganlara sanal bir kabuk ortamı sağlamasıdır. Bu sayede, saldırganlar gerçek bir sistemdeymiş gibi davranabilir ve etkileşimlerini gerçekleştirebilir. Bu özellik, saldırganların daha fazla bilgi sağlamalarını ve saldırılarını derinlemesine incelemeyi hedefler. Mevcut yapıda honeypotun karakteristiği gereği şekil 5'te gösterildiği gibi 22 ve 23 SSH ve Telnet portları hedef alınmıştır.

83 atak sayısıyla beşinci sırada AdbHoney yer almaktadır. ADB Honey, Android Debug Bridge (ADB) protokolünü hedef alan bir honeypot sistemidir. ADB, Android cihazlarla iletişim kurmak için kullanılan bir protokoldür ve geliştiricilere cihazlara erişim ve kontrol imkânı sağlar. ADB Honey, bu protokolü hedef alarak, saldırganların Android cihazlara yönelik saldırılarını tespit etmek ve analiz etmek amacıyla tasarlanmıştır. ADB Honey, Android cihazlarının ADB portuna bağlanma girişimlerini izleyen ve kaydeden bir tuzak sunucusu olarak çalışır. Gerçek bir Android cihazı taklit eder ve saldırganın ADB komutlarını kullanarak cihaza erişmeye çalışmasını sağlar. Bu süreçte, saldırganın kullandığı komutlar, bağlantı denemeleri ve diğer etkileşimler kaydedilir ve analiz edilir. Mevcut saldırıların tamamının 5555 numaralı porta yapıldığı gözlemlenmiştir.

Suricata tarafından T-Pot servisi çalışırken oluşturulan ilk 10 alarm imzası, Şekil 6'da yer alan Kibana gösterge tablosunda gösterilmiştir. Alarm imzaları olay müdahalesinde kullanılabilirliği olduğundan oldukça önemlidir.



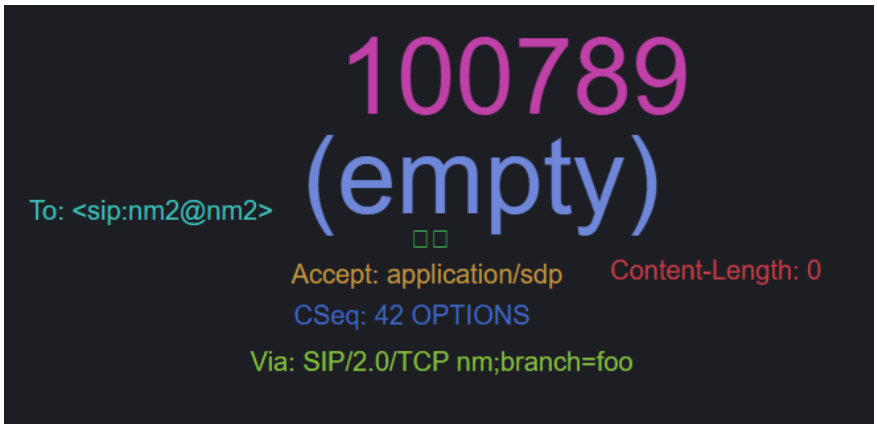
ID	Description	Count
2200007	SURICATA IPv4 padding required	207,902
2030387	ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read	7,091
2023997	ET INFO Potentially unsafe SMBv1 protocol in use	193
2210063	SURICATA STREAM 3way handshake excessive different SYNs	84
2210037	SURICATA STREAM FIN recv but no session	76
2210041	SURICATA STREAM RST recv but no session	48
2221010	SURICATA HTTP unable to match response to request	43
2260002	SURICATA Applayer Detect protocol only one direction	43
2210048	SURICATA STREAM reassembly sequence GAP -- missing packet(s)	14
2210051	SURICATA STREAM Packet with broken ack	12

Şekil 6. Tetiklenen Suricata alarm imzaları ve sayıları

Şekil 7'de saldırılar sırasında saldırganlar tarafından en çok kullanılan kullanıcı adı parametreleri kullanım sıklığıyla doğru orantılı olarak gösterilmiştir.

Şekil 7. Kullanım sıklığına göre kaba kuvvet saldırılarında en çok denenen kullanıcı adları

Şekil 8'de saldırılar sırasında saldırganlar tarafından en çok kullanılan parola parametreleri kullanım sıklığıyla doğru orantılı olarak gösterilmiştir.



Şekil 8. Kullanım sıklığına göre kaba kuvvet saldırılarında en çok denenen parolalar

Default olarak kullanılan kullanıcı adı ve parolaların belirlenmesi ve istatistiklerinin tutulması kurum içerisindeki mevcut yapıda uygulanacak sıkılaştırma işlemlerinde bir dayanak noktası olarak kullanılabilir. Son kullanıcıların ve sistem yöneticilerinin bu "default" denemelerde kayda geçen kullanıcı adı ve parolaları kullanmaması sağlayacak tedbirler alınmalıdır.

4. Öneriler ve Sonuç

Honeypotlar, siber güvenlik alanında önemli bir araç olarak kabul edilmektedir. Bu çalışmada, honeypot kavramı ve işleyişi üzerinde durulmuş, farklı honeypot türleri ve özellikleri hakkında bilgi verilmiştir.

Honeypotlar, siber tehdit aktörlerinin ağlara sızma girişimlerini izlemek ve analiz etmek için kullanılan tuzak sistemlerdir. Gerçek sistemler gibi görünen sanal ortamlar oluşturarak, saldırganların dikkatini çeker ve onların faaliyetlerini kaydetme imkânı sağlar. Bu sayede, saldırganların kullanmış oldukları teknikler, saldırı vektörleri ve hedefledikleri servisler hakkında önemli bilgiler elde edilebilir. Honeypotların kullanımı, siber güvenlik uzmanlarına birçok avantaj sunmaktadır. İlk olarak, saldırganların davranışlarını izleyerek saldırıları tespit etmek ve analiz etmek mümkün hale gelir. Bu bilgiler, güvenlik önlemlerinin geliştirilmesi ve ağların daha güvenli hale getirilmesi için değerli bir kaynak oluşturur. Bununla birlikte, honeypotlar saldırganların dikkatini gerçek sistemlerden uzaklaştırarak, gerçek hedeflere odaklanmalarını engeller. Bu da gerçek sistemlerin güvenliğini artırır ve saldırılara karşı daha iyi koruma sağlar. Bununla birlikte honeypotlar tek başlarına yeterli değildir. Çeşitli güvenlik enstrümanlarıyla kullanıldığında çok daha etkili hale gelebilirler. Çalışma kapsamında yönetici ağında

konuşlandırılan honeypotlara kampüs ağının farklı noktalarından ulaşılabildiği, çalışan ve zafiyet bulunduran servislere saldırıda bulunabildiği görülmüştür. Buradan yola çıkarak kampüs ağında hiyerarşik ya da kural setlerine dayalı bir ağ yapılandırmasının olmadığı gözlemlenmiştir.

Güvenlik açsından VLAN yapılandırmalarında erişim kontrol listeleri kullanarak aynı yapıdaki farklı lokal ağların birbirleriyle haberleşmesi denetime ve kurala tabii tutulmalıdır. Ağ segmentasyonu iç ağdaki saldırıları sınırlandırmada etkili olacaktır.

İç ağda meydana gelen saldırlar honeypotlar aracılığıyla tespit edilerek doğrudan ağ yapısından izole edilmelidir. Bunun için honeypot ile ana omurga veya kenar katman seviye üç switch'ler bir script aracılığıyla haberleştirilerek düzenli olarak bir kontrol sağlanabilir.

Kaynaklar

Spitzner, L. (2003) The honeynet project: Trapping the hackers, *IEEE Security and Privacy*, 1(2): 15–23.

Stoll, C. (1989) The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Doubleday, US.

Cohen, F. (1998) A note on the role of deception in information protection, *Computers and Security*, 17: 483-506.

Cheswick, B. (1991) An evening with berferd in which a cracker is lured, endured, and studied, AT&T Bell Laboratories.

SANS Institute. (2023) Cooperative research and education organization. https://www.sans.org/. Son erişim 03 Ağustos 2023

Karabay, M.S., Eyüpoğlu, C. (2023) Balküplerinin Saldırı ve Savunma Açısından İncelenmesi, *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 22(43): 15-32.

Campbell, R.M., Padayachee, K., Masombuka, T. (2015) A survey of honeypot research: Trends and opportunities, 10th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, pp. 208-212.

Zhang, F. et al. (2003) Honeypot: A supplemented active defense system for network security. Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 231–235.

Alata, E. et al. (2006) Lessons learned from the deployment of a high-interaction honeypot, Sixth European Dependable Computing Conference, pp. 39–46.

Telekom Security. (2023) T-Pot. https://github.com/telekom-security/tpotce. Son erişim 03 Ağustos 2023

Red Hat. (2023) Cockpit Project. https://cockpit-project.org. Son erişim 03 Ağustos 2023

Elastic Stack. (2023) https://www.elastic.co/elastic-stack. Son erişim 03 Ağustos 2023

Open Information Security Foundation (OISF). (2023). Suricata. https://suricata.io. Son erişim 03 Ağustos 2023

Combe, T., Martin, A., Di Pietro, R. (2016) To Docker or Not to Docker: A Security Perspective, *IEEE Cloud Computing*, Vol. 3, No. 5, pp. 54-62.

Seri, B. et al. (2019) Urgent/11: Critical vulnerabilities to remotely compromise VxWorks, the most popular RTOS. Armis, Inc. White Paper. https://info.armis.com/rs/645-PDC-047/images/Urgent11_Technical_White_Paper.pdf Son erişim 03 Ağustos 2023