ACTA INFOLOGICA, 2018; 2(1): 1-11
Research Article

ACTA INFOLOGICA
ISSN: 2602-3563

Bir Güvenlik Trendi: Bal Küpü

Süleyman Muhammed Arıkan*, Recep Benzer

ÖZ

Bu çalışma, bilişim dünyasında güvenliği sağlamak adına kullanılmakta olan ve her geçen gün popülerliği artan bal küpleri hakkında bir araştırma niteliğindedir. Honeypot olarak kullanılan bu terim dilimize bal küpü olarak geçmiştir. Balküpleri, izinsiz yapılmış girişlerin veya zararlı aktivitelerin tespitinde kullanılmasına ek olarak asıl amaçları sadırganın veya zararlı aktivitenin kullanmış olduğu metod ve araçlar hakkında bilgi edinmektir. Bal küplerinin birçok çeşidi vardır. Çalışmamızda bu çeşitleri açıklamaya odaklanılmıştır. Dinamik bal küpü dizaynı, bal küpü sistemleri için saldırgan web uygulaması, ssh ataklarının analizi ve görselleştirilmesi gibi çalışmalar incelenmiştir. Ayrıca Glastopf ile sql enjeksiyonu saldırısına ve yapılan saldırının kayıtlardan görüntülenmesine örnek bir uygulama yapılmıştır. Gelişen modern dünyada her geçen gün farklı alanlar oluşmakta ve gereksinimler değişmektedir. Bu gereksinimlere bal küpü sistemlerinin kendini adapte etmesi her ne kadar hızlıda olsa bazı konularda eksikleri devam etmektedir. Ancak esnek yapıları ve herhangi bir sisteme kolay adapte olmaları sayesinde yeni moduller geliştirilerek eksikliklerin büyük kısmı kullanıcılar tarafından giderilebilmektedir.

Anahtar Kelimeler: Bal küpü, malware, sql injection, ransomware, worm.

New Security Trend: Honeypot

ABSTRACT

This study is a research about the honeypots which is being used to provide security in the world of information and increasing in popularity day by day. This term used as a honeypot is passed down to our slice as honey cube. In addition to being used in the detection of unauthorized entries or harmful activities, it is also necessary to obtain information about the methods and means by which the original purpose is to use the malicious or harmful activity. There are many kinds of honeypots. Our work focuses on explaining these species. Dynamic honeypot design, aggressive web application for honeypot systems, analysis and visualization of ssh attacks have been studied. In addition, Glastopf, sql injection attack and the attack is displayed on the records of a sample application has been done. In the developing modern world, different fields are formed every day and requirements are changing. Although these requirements are fast for the honeypot systems to adapt themselves but some are still missing. However, due to their flexible structure and easy adaptation to any system, new modules can be developed and most of the deficiencies can be eliminated by the users.

Keywords: Honeypot, malware, sql injection, ransomware, worm.

Information of Author(s):

Süleyman Muhammed Arıkan
ORCID: 0000-0003-1526-2970
suleyman.arikan@tubitak.gov.tr
Gazi University, Information Institute

Recep Benzer
ORCID: 0000-0002-5339-0554
rbenzer@kho.edu.tr
National Defense University, KHO

DOI: 10.30801/acin.356815

Submit Date:	21.11.2017
Accept Date:	02.05.2018
Publish Date:	26.06.2018

(*) Contact Author
Address: National defense University, Department of Computer Engineering, Ankara, Turkey
Telephone Number: +90 419 75 58 /5453

ACTA INFOLOGICA
ISSN: 2602-3563

1. GİRİŞ

Günümüz modern dünyasında güvenliği sağlamak amacıyla birçok teknik ve yöntem kullanılmaktadır. Her geçen gün inanılmaz bir hızla arttığı görülen saldırı tekniklerine nazaran savunma teknikleri için aynı şeyi söylemek oldukça güçtür. Fakat her geçen gün saldırılar hakkında yeni teknikler keşfedilmekte ve karşı önlemler alınmaya çalışılmaktadır. Tüm bunlara ek olarak sıfırıncı gün atakları (zero-day attacks) ile tanımlanan ataklar günlerce hatta yıllarca gizemini korumaktadırlar. Keşfedilmemiş bu atakları, modern çözümlemelerin birçoğu engelleyememekte hatta birçok durumda saldırıya uğradığını dahi fark edememektedirler. Çalışmamızın devam eden kısmında günümüz güvenlik tekniklerine yüzeysel olarak bir bakış atılacaktır.

İstemci tarafında güvenliği sağlamak adına en çok kullanılan teknolojilerin başında şüphesizki antivirüs yazılımları gelir. Antivirüsler, sistem üzerindeki zararlı yazılımları tespit edip amaçlanan işlemin gerçekleşmesini engelleyerek zararlı yazılımı sistemden kaldırmayı hedefleyen programlardır. Modern antivirüsler; solucanlar (worm), truva atları (trojan horses), arka kapılar (backdoor), fidye yazılımlar (ransomware), tarayıcı ele geçirme (browser hijacking), casus yazılım (spayware), çevrimiçi bankacılık atakları ve sosyal mühendislik gibi birçok saldırıya karşı kullanıcıyı ve sistemi koruma yetenekleri geliştirmiştir (Anonymous, 2017). İstemci taraflı saldırılarda son kullanıcıyı korumada antivirüslerin faydası göz ardı edilemez. Fakat tüm saldırılar yalnızca son kullanıcıya yönelik değildir. Ev ortamında antivirüs kullanımı yeterli bir güvenlik önlemi olarak sayılabilmesine karşın kurumsal iş ortamlarında tek başına bir yeterliliği olduğunu söylemek güçtür. Ayrıca, antivirüslerin son kullanıcı nezninde sistem kaynaklarını fazla kullanma gibi bazı olumsuzlukların olduğuda ortadadır.

Güvenliği sağlamak adına kullanılan bir diğer teknoloji olarak ise güvenlik duvarı (firewall) sayılabilir. Güvenlik duvarı olmayan bir iş veya kurumsal ağ bulmak neredeyse imkansızdır. Güvenlik duvarı, paketler üzerinde incelemeler yaparak filtrelemeye olanak sağlar (Yang ve ark., 2011). Filtrelemeler kural tabanlıdır. Kurala uyan / uymayan paketler düşürülür. Güvenlik duvarlarını yapılarına göre yazılımsal ve donanımsal olarak ikiye ayırabiliriz. Donanım tabanlı güvenlik duvarları oldukça performanslı çalışır. Üzerindeki donanım, barındırdığı yazılıma özgü hazırlandığından yetenekleri haliyle daha da gelişmiştir. Donanımsal güvenlik duvarlarında hedef, ağların birbirinden izole edilmesidir. Kurulumları ve konfigürasyonları kolay değildir. Ayrıca satış ücretleri oldukça yüksektir. Yazılımsal güvenlik duvarlarında ise maliyet düşüktür. Zaten hali hazırda, işletim sistemleri ve antivirüslerin büyük bir çoğunluğu içerisinde güvenlik duvarı barındırmaktadır. Farklı bir yazılım ile koruma amaçlanırsa, internet üzerinden ücretsiz güvenlik duvarı edinebilmenin yanı sıra cüzi miktarlar ile lisanslı yazılımsal güvenlik duvarları da satın alınabilir. Yazılımsal güvenlik duvarları, bilgisayar ile ağ arasında gerçekleşen trafiğin filtrelenmesine olanak sağlar. Her türlü sisteme uyum sağlayabilirler. Yazılımsal olduklarından dolayı sistem kaynaklarını kullanılar. Bu yüzden çoğu zaman performansları düşüktür.

Ağ içerisinde gerçekleşen atakların tespiti ve engellenmesi için IDS ve IPS araçları kullanılabilir. Ağ trafiğinin izlenerek yetkisiz giriş ve aktivitelerin tespitinde, dilimize saldırı tespit sistemi olarak çevrilmiş IDS (Intrusion Detection Systems) kullanılır. Ağ trafiğini inceleyerek saldırıları engellemek adına ise IPS (Intrusion Prevention Systems) kullanılır. Dilimize saldırı engelleme sistemi olarak çevrilmiştir. IDS ve IPS arasındaki fark oldukça basittir. IDS, saldırıları tespit ederek ağ yöneticisine durumu raporlar ve bir alarm oluşturur. IPS ise, aynı IDS gibi çalışmasına ek olarak aynı zamanda bu saldırıyı engellemeye çalışır. ID/PS araçları iki basit tipe ayrılır: Anasistem tabanlı (Host-based) ve Ağ tabanlı (Network-based). Anasistem tabanlı ID/PS araçları, bireysel bilgisayarlar üzerindeki verileri inceler. İçeriden kaynaklı kötüye kullanımların tespitinde ve engellemesinde oldukça verimlidir. Anasistem tabanlı IDS araçlarına Windows NT/2000 Security Event Logs ve UNIX Syslog örnek olarak gösterilebilirken anasistem tabanlı IPS araçlarına Cisco Security Agent (CSA) örneği verilebilir (Kuwatly ve ark., 2004). Diğer taraftan ağ tabanlı ID/PS araçları, mevcut ağ üzerinde taşınan tüm paketleri analiz eder. Çoğu zaman paketler deneysel bir veri ile kıyaslanarak incelenir. Ağ tabanlı IDS araçlarına açık kaynak kodlu Snort örnek olarak verilebilir. Snort, gerçek zamanlı ağ tarafiği üzerinde paketleri inceleyerek arabellek taşması (buffer overflow) ve gizli port taraması (stealth port scan) gibi daha birçok geniş çeşitlilikteki atakları tespit eder. Ayrıca Snort ‘a ek olarak Suricata, Bro Ids, OpenWPS-ng ve Security Onion gibi yine

ISSN: 2602-3563

ücretsiz araçlar örnek gösterilebilir. Ağ tabanlı IPS araçlarına ise McAfee's Network Protection System örneği verilebilir.

2. YÖNTEM

Bal küpü terimi için esin kaynağı, ayılar için kurulan tuzaklara yerleştirilen içi bal dolu kaplardır (Zakaria ve Kiah, 2012). Bal küpleri ile ayıların tuzağa gelmesi sağlanmaktaydı. Günümüz bilişim dünyasında ise bal küpleri, saldırganları üzerine çekmek için kullanılmaktadırlar. Bal küpü sistemleri zararlı aktiviteyi ya da saldırganı durdurmakta aktif görev almazlar. Balküpleri, izinsiz yapılmış girişlerin veya zararlı aktivitelerin tespitinde kullanılmasına ek olarak asıl amaçları sadırganın veya zararlı aktivitenin kullanmış olduğu metod ve araçlar hakkında bilgi edinmektir (Song ve ark., 2012). Edinilen bu bilgiler ışığında istenmeyen faaliyetlerin engellenmesi adına çalışmalar yapılır. Dolayısı ile bal küpü sistemlerini, saldırganın veya zararlı aktivitenin kullandığı teknikler ve araçlar hakkında çalışmamıza olanak sağlayan platformlar olarak tanımlayabiliriz (Chauhan ve Shiwani, 2017).

Bal küpü sistemlerine yönlendirilmiş hiçbir trafik yoktur. Buna ek olarak bal küpü sistemleri herhangi bir üretim değeri bulundurmaz. Dolayısı ile balküpleri üzerinde hiçbir trafik görülmemelidir. Eğer bal küpü sistemleri ile bir etkileşim söz konusu ise, etkileşime geçen kaynak yüksek olasılıkla saldırgan ya da zararlı aktivitedir.
Bal küpü sistemleri bir ağa kurulduğunda, ağdaki diğer makineler gibi gözükmesine dikkat edilmelidir. Bulunduğu ağın özelliklerine göre servisler seçilmelidir. Bilinen açıklıklar bırakılarak saldırganların dikkatleri bal küpü üzerine çekilerek gerçek sistem ve servisler korunur. Birçok saldırı tespit ve engelleme sisteminin aksine yanlış alarm (false positive) oranı oldukça düşüktür. Bal küpü sistemleri kurulum için büyük sistem kaynaklarına gerek duymaz.

İlk bal küpü yazılımı 1998 yılında yazılmış Cybercop Sting adındaki yazılımdır. Aynı zamanda Decoy Server olarak da bilinmektedir. Decoy Server, Telnet ve SMTP gibi servisleri simüle edebilmekteydi. Oldukça limitli bir kullanıma ve kayıtlama yeteneğine sahip olsa da saldırgan ataklarını analiz etmede oldukça faydalıydı (Sharma, 2016).

Günümüz balküpleri etkileşim seviyelerine göre Düşük etkileşimli (Low-Interaction) ve Yüksek Etkileşimli (High-Interaction) olarak ikiye ayrılır (Singh ve Joshi, 2011). Buradaki etkişim ile kastedilmek istenilen, aktivite düzeyi veya faaliyet alanıdır.

Düşük etkilişimli bal küpü sistemlerinin faaliyet alanı oldukça kısıtlıdır. Bu kısıtlılık taklitten kaynaklanır. Çünkü düşük etkileşimli bal küpü sistemlerinde servisler ve servislerin üzerinde çalıştığı işletim sistemi tamamen simüle edilmektedir. Bu simülasyondan dolayı saldırganın bal küpü sistemi üzerinde gerçekleştirebileceği işlemler limitlidir. Bir düşük etkileşimli bal küpü sisteminde ftp protokolü simüle edilmek istendiğini düşünelim. Bu durumda 21. port dinleniyormuşcasına cevaplar döndürülür. Bu portta login komutlarının çalışmasına olanak sağlanır. Buna ek olarak çeşitli ftp komutlarıda çalıştırılır. Saldırgan veya zararlı aktivite burada ftp servisinin çalıştığını düşünür. Fakat yapılan tüm işlemler taklitten ibarettir. Bunlara ek olarak; saldırganın, taklit servisin desteklemediği bir komutu çalıştırması sonucu sistemin bir bal küpü olduğu anlaşılabilir. Düşük etkileşimli balküplerinden sınırlı bilgi edinilir. Saldırganın ve zararlı aktivitenin gerçek bir sistemde yapacağı tüm işlemleri, taklit sistemde uygulayamayacağı ihtimalinden dolayı her konuda bilgi edinilemeyebilir. Buna karşın kurulumları ve bakımları oldukça basittir. İçerisinde barındırdıkları sistemler taklit olduklarından dolayı ağ için herhangi bir risk oluşturmazlar. Bilinen aktivitelerin yakalanmasında oldukça etkilidirler. En çok kullanılan düşük etkileşimli bal küpü sistemleri olarak Honeyd, Specter, KFSensor ve Dionaea örnek verilebilir. KFSensor, bir windows tabanlı bal küpü sistemidir. Servisleri windows işletim sistemi üzerinde çalışıyormuş gibi taklit eder. Servisler OSI katmanlarından uygulama katmanında taklit edilir. Dolayısı ile çoğunlukla yeni güvenlik duvarı kuralları oluşturmak için veya yeni IDS imzaları yazmak için kullanılmaktadır (Singh ve Joshi, 2011). Honeyd en çok kullanılan düşük etkileşimli bal küpü sistemlerinin başında gelir. Bir ağda sanal sistemler oluşturan uygulamadır. Oluşturulan sanal sistemler uzaktan kontrol edilebilir. Konfigürasyonlarına göre işletim sistemi ve servisler taklit edilir. İşletim sistemi ve servis çeşitliliği geniştir. Ayrıca tek bir sisteme birden fazla ip adresi atanmasının mümkün olması önemli bir özelliktir. GNU

ISSN: 2602-3563

lisansı altında açık kaynak kodlu bir yazılımdır. Specter, honeyd gibi herhangi bir işletim sistemini üzerinde belirlirlediğimiz servisler çalışıyormuşcasına simüle eder. Honeyd'den ayıran en büyük özelliği, içerisinde tuzak uygulamalar barındırmasıdır. Bu sayede saldırgana ait bilgiler edinmeye çalışmaktadır.

Yüksek etkileşimli bal küpü sistemleri, düşük etkileşimli bal küpü sistemlerine nazaran daha karmaşık yapıya sahiptirler. Kurulumları ve bakımları zaman almakla birlikte zor olduğu söylenebilir. Gerçek işletim sistemi ve uygulamalar kullanılır. Dolayısı ile saldırgan veya zararlı aktivite hakkında çok geniş çapta bilgiler edinilebilir. Sıfırıncı gün ataklarının tespitinde veya saldırganın kullandığı teknikler üzerinde çalışmak için idealdirler. Symantec Decoy Server ve Sebek bu balküplerine örnek olarak gösterilebilir (Djanali ve ark., 2014). Sebek, iki modül barındırır. Birinci modül yüksek etkileşimli bal küpü üzerinde çalışarak büyük çapta kayıt toplar. Toplanan bu kayıtlar ikinci modül olan sunucuya gönderilir. Bu sunucu genellikle bal küpü sistemlerinin önünde duran ağ geçididir. Fakat bağımsız olarakta kullanılabilir. Sunucu sayesinde tüm kayıtlar merkezi bir noktada toplanır. Sebek sunucu modülü ve bal küpü modülü aynı makine üzerine kurulamamaktadır.

Yüksek etkileşimli bal küpü sistemlerine birçok kaynakta ayrıca honeynet örneğine rastlamak mümkündür. Honeynet kavramı, iki ya da daha fazla bal küpü sistemlerinin bir arada kullanılmasına verilen addır (Zakaria ve Kiah, 2012).

3. BULGULAR

Bal küpü istemleri ile birçok konuda örnek çalışmalar yapılmıştır. Makalemizde bu çalışmalardan bazılarına yer verilmiştir. İlgili çalışmalar incelenmiş ve yararlı olacağı düşünülen araştırmalar okuyucuya aktarılmıştır.

Dinamik bal küpü dizaynı (Kuwatly ve ark., 2004), bal küpü sistemleri için saldırgan web uygulaması (Djanali ve ark., 2014), ssh ataklarının analizi ve görselleştirilmesi (Koniaris ve ark., 2013) gibi çalışmalar incelenerek okuyucuya aktarılması hedeflenmiştir. Bu bölümde ayrıca Glastopf ile sql enjeksiyonu saldırısına ve yapılan saldırının kayıtlardan görüntülenmesine örnek oluşturmak adına tarafımca yapılmış uygulama okuyucuya sunulacaktır.

3.1. Dinamik Bal Küpü Dizaynı

Bal küpü sistemleri; genellikle yönetici tarafından atanmış ip adreslerinde oluşturulmaktadır. Statik atamanın aksine, dinamik bal küpü ile kullanılmayan ip adresleri tespit edilerek bu iplerde sanal balküpleri oluşturulması hedeflenmiştir. Bu sayede saldırganların gözden kaçması minimuma indirilecektir. Dinamik bal küpü sistemi aynı zamanda, ip kullanımına göre kendini güncelleyecektir. Bir ip boşa çıktığında ilgili adrese bir sanal bal küpü kurulacak, ip kullanılmaya başladığında ise ilgili bal küpü sistemden kaldırılacaktır.

Dinamik bal küpü yaklaşımının uygulanması için şu bileşenlere ihtiyaç duyulmaktadır: Aktif tarama aracı, pasif tarama aracı, düşük etkileşimli bal küpü, yüksek etkileşimli fiziksel bal küpü, veri tabanı, dinamik bal küpü motoru.

Aktif tarama, kullanılan işletim sistemleri ve portları bulmak amacıyla kullanılacaktır. Nmap uygulaması seçilmiştir. Nmap içerisinde işletim sistemi ve servislerin imzalarını barındırmaktadır. Hedef makineye paketler göndererek cevap ister. Aldığı cevapları veritabanındaki imzalarla karşılaştırarak, hedef sistemin ne olduğuna karar verir.

Pasif tarama, ağdaki paketlerin dinlenemesi ile hedef sistemin bilgilerini bulma işlemine dayanır. Aktif tarama ile pasif tarama arasındaki fark, pasif taramada aktif taramada olduğu gibi hedef ile etkileşimin olmamasıdır. Pasif tarama araçlarına örnek olarak p0f ve Snort gösterilebilir.

p0f, ağda yakaladığı SYN paketlerini içinde barındırdığı veri tabanındaki imzalarla karşılaştırarak işletim sistemine karar verir. Bu karar için paketlerin içerisinde bulunan TCP/IP alanlarına bakar. Tamamıyla sessizdir.

ACTA INFOLOGICA
ISSN: 2602-3563

Pasif tarama ağda çok az bir trafiğe sebep olur. Buna nazaran aktif tarama ağ içerisinde çok fazla faaliyete sebebiyet verir. Aktif taramada sonuçlar birer anlık fotoğraf gibidir. Pasif taramada ise sonuçlar gerçek zamanlı olarak sürekli toplanmaktadır. Aktif tarama tüm açık port ve servisleri bulabilmesine karşın, pasif tarama yalnızca trafik oluşturan portları bulabilir.

Düşük etkileşimli bal küpü olarak ise honeyd kullanılmıştır. Çünkü honeyd bal küpü sistemi hem uzaktan oluşturulabilmekte hemde üzerinde konfigürasyon değişiklikleri yine uzaktan yapılabilmektedir. Honeyd balküpleri, oluşturulduktan sonra bir etkileşimle karşılaştıklarında bu trafiği doğruca fiziksel yüksek etkileşimli bal küpü sistemi olan Sebek bal küpüne yönlendirir. Böylece saldırgan yüksek etkileşimli bal küpü sistemi ile karşılaşarak hakkında daha fazla bilgi toplanmasına olanak sağlar.

Yüksek etkileşimli bal küpü sistemi olarak Sebek kullanılmıştır. Sebek bal küpü modülleri, honeyd balküplerinden yönelendirilen trafik ile girdiği etkileşimlerin kaydını tutarak Sebek sunucusuna tutulan kayıtları yollar. Sunucuda merkezi olarak tutulan bu kayıtlar, belirli periyotlarla sunucu tarafından incelenerek risk farkedildiği takdirde SMS ile yöneticiyi bilgilendirmektedir.

Veri tabanı içerisinde; IPInformaiton, Ports, OperatingSystems, ServicesScripts, HoneydLogs ve SebekLogs olmak üzere altı tablo vardır. IPInformation tablosu içerisinde belirli ip adresine ait; işletim sistemi bilgisi, verinin edinildiği zaman ve ip adresinin gerçek bir sistem veya sanal bir sistem tarafından kullanıldığına dair kayıtları içerir. Ayrıca bu bilgilerin hangi tarama aracı ile edinildiği bilgiside içerilmektedir. Çünkü tarama araçları bazı durumlarda diğerlerine göre daha güvenilir sonuçlar vermektedir. Ports tablosu içerisinde belirli ip adresine ait sistemdeki açık tüm portlar ve bu portlarda çalışan servisler tutulur. Yine bu tablodada veriye hangi tarama aracı ile ulaşıldığının yanı sıra zaman bilgiside bulunmaktadır. OperatingSystems tablosunda her işletim sistemine benzersiz bir numara verilerek açıklaması yazılmıştır. ServicesScripts tablosunda ise honeyd tarafından simüle edilen servisler ve bu servislerin simüle edilmesi için gerekli senaryolar tutulmaktadır. HoneydLog tablosunda honeyd tarafından tutulmuş kayıtlar bulunmaktadır. SebekLogs tablosunda ise Sebek sunucusunda toplanmış kayıtlar tutulmaktadır.

Dinamik bal küpü sistemi motor aracının şu işlemlerde kullanılması amaçlanmıştır: yerleştirilecek sanal balküpü sayısının hesaplanması, konfigürasyon komutlarının gönderilmesi, kayıtların toplanması ve çıktı oluşturulması ile hesaplamalarda yanlışlık oluşmasını engellemek adına veri tabanında eski kayıtların silinerek güncel kalmasını sağlamak.

Sonuç olarak, kullanılmayan ip adreslerine düşük etkileşimli bal küpü sistemleri kurularak saldırganın ağda yaptığı tüm hareketlerin kayıt altına alınması hedeflenmiştir. Honeyd ile etkileşime geçen her trafik Sebek bal küpüne yönlendirilmiştir. Sebek bal küpü ise kayıtları merkezi sunucuda toplayarak belli zamanlarda bu kayıtları incelemiş ve yüksek risk gördüğünde durumu yöneticiye bildirmiştir. Bu sayede izinsiz giriş yapan saldırgan veya ağda bulunan zararlı aktiviteler kısa sürede farkedilmiştir. Sanal balküplerinin ağdaki makinelerin karakteristik özellikleri ile aynı oranda kurulması ile sistemdeki varlıkları gizlenmiştir. Bu sayede saldırgana durum farkettirilmeden gerçek ve taklit sistemler paralel olarak çalıştırılmıştır.

3.2. Bal Küpü Sistemleri için Saldırgan Web Uygulaması

Web uygulamalarında en ciddi açıklıkların başında şüphesiz ki Sql Enjeksiyonu (Sql Injection) ve XSS (Cross – Site Scripting) gelir.

Sql Enjeksiyonu, sayfadaki ilgili alana girilen meta karakterler (‘, ; vb.) ile arka planda çalışacak olan sql sorugusuna eklemeler yaparak sorguyu değiştirme işlemine denir. Çoğunlukla web uygulamalarında kullanılır. Fakat sql sorgusunun olduğu heryerde bu saldırı tipi ile karşılaşabiliriz. Komut-1 üzerinde görülen sorgu cümlesi arka planda kulanılan sql cümleciği olarak kabul edelim.

ISSN: 2602-3563

```
sql = “SELECT * FROM users WHERE name=’ ”+kullanici+” ’ ;”
calistir(sql)
```

Komut 1. Arka plan Sql Sorgusu

Bu sorgu ile kullanici adi kısmına girilen değere eşit kullanıcılar veri tabanından çekilmek istenmektedir. Sql enjeksiyonu yapılarak tüm kullanıcıların veri tabanından çekilmesi sağlanabilir. Kullanıcı adı alanına Komut-2 üzerindeki gibi kullanıcı tarafından giriş yapıldığını kabul edelim.

```
1’ or ‘1’ = ‘1
```

Komut 2. Sql Enjeksiyonu İçin Girdi Değeri

Bu durumda arka planda çalıştırılacak olan sql sorgumuz Komut-3 üzerinde görüldüğü gibi bir sorguya dönüşmüştür.

```
SELECT * FROM users WHERE name=’1’ or ‘1’=’1’
```

Komut 2. Sql Enjeksiyonu Yapılmış Sorgu

İkinci şart doğru olduğundan dolayı sorgu çalışacak ve veri tabanındaki tüm kullanıcı adlarını döndürecektir. Böylece veri tabanından tüm kullanıcı adlarının çekilmesi sağlanmıştır.

XSS, çapraz betik saldırıları (Cross-Site Scripting) kelimelerinin baş harfleridir. Web sayfasında kullanıcıdan giriş alınacak alanlarda; herhangi bir kontrol mekanizması olmaması durumunda, html ya da javascript gibi kodların bu alana girilerek ilgili sayfanın kodları yorumlamasını sağlamaktır. Kullanımına göre 3 farklı tipi mevcuttur. Bunlar Reflected XSS, Stored XSS ve DOM XSS olarak listelenebilir (Anonymous, 2013). Bunlar arasından DOM, belge nesnesi modeli (Document Object Model) kelimelerinin baş harflerinden oluşmaktadır. XSS saldırıları içinde en tehlikeli olanı kabul edilmektedir. Web sayfaları belge olarak kabul edilerek, bu belge içerisindeki her eleman (resim, video vb.) nesne olarak görülmektedir. Javascript kodları ile bu nesneler üzerinde değişiklik yapılması mümkündür. İşte bu XSS saldırı yöntemi kullanılarak sayfa içersindeki hemen hemen herşey değiştirilebilir.

Tüm bu saldırıların tespit edilmesi ve saldırgan hakkında bilgi edinmek adına bir bal küpü sistemi geliştirilecektir. Öncelikle bal küpü üzerinde kullanıcılacak sayfanın XSS ve Sql enjeksiyonu açıklıklarını içeren gerçek bir web sayfası gibi görünmesi gerekmektedir. Bu amaç doğrultusunda web sitesi 3 sayfadan oluşturulmuştur. Bunlardan birincisi anasayfadır. Anasayfa saldırganın bir kuruluşun web sitesi olduğuna inanması için sahte bilgilerle doldurulmuştur. Diğer sayfalardan ilki XSS açıklığı diğeri ise Sql enjeksiyonu açıklığı bulunduran sayfalardır. Eğer saldırgan XSS veya Sql enjeksiyonu saldırılarında bulunursa, ilgili sayfa bu saldırıları emüle edecek ve başarılı olduğu izlenimi bırakacaktır. Fakat bunların yanında kullanılmış farklı saldırılar varsa XSS ve Sql enjeksiyonu dışındaki saldırılar simüle edilemez. XSS saldırısının simüle edileceği sayfada, 3 adet sahte makale bulunmaktadır. Sayfada gerekli alana girilecek birden üçe kadar olan sayılarla ilgi makale sayfada gösterilmektedir. Sayfa içerisinden istek yapıldığında, bal küpü isteğin beklendiği gibi olması durumunda makaleleri kullanıcıya sunar. Fakat farklı bir istek görüldüğünde tarayıcıda çalıştırılacak ancak saldırganın kimliğine ilişkin veri toplayan javascript kodu sayfaya eklenecektir.

Öncelikle sayfaya gelen http isteği incelenir. Bu isteğin Sql enjeksiyon açıklığı bulunduran sayfadan ya da XSS açıklığı bulunduran sayfadan geldiğine karar verilir. İlgili sayfanın açıklığının sömürülmeye çalışıldığına dikkat edilir. Eğer bahsi geçen açıklık sömürülmeye çalışılıyorsa bal küpü tarafından başarılı olduğuna dair cevap döndürülür. Cevap yollanmadan önce içerisinde javascript kodu eklenir. Javascript kodu, bir önlem olarak

ISSN: 2602-3563

karartılmıştır. Bu sayede saldırganın geri dönen cevabı incelemesi halinde kolaylıkla amacımızı anlaması engellenmek istenmiştir.

3.3. SSH Ataklarının Analizi ve Görselleştirilmesi

Saldırganlar sürekli olarak internette kötü amaçları için kullanabilecekleri sunucu aramaktadırlar. En belirgin hedeflerinin yöneticisinin uzaktan erişim için yapılandırdığı sunucular olduğu açıktır. Bu tip uzaktan erişim ile kullanılmak istenilen sunucularda çoğunlukla SSH (Secure Shell) servisi kullanılır.

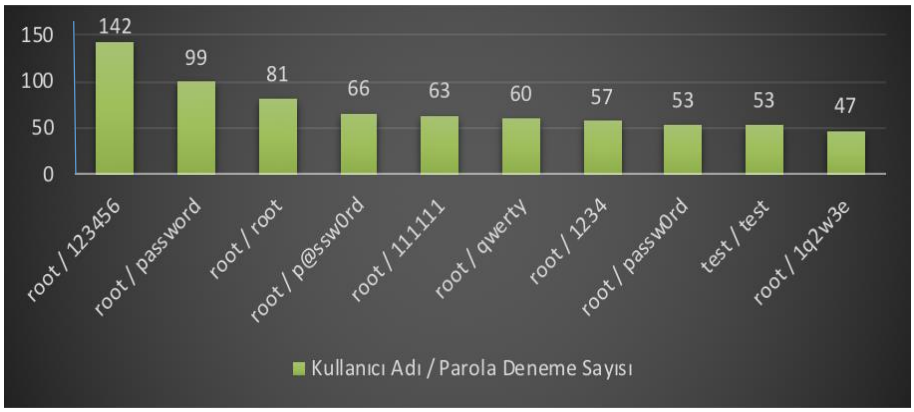
SSH şifreli bir uzak bağlantı mekanizmasıdır. Genellikle Linux ve Unix tabanlı işletim sistemlerinde kullanılır. Bağlantı sağlandığında ilgi işletim sisteminin konsoluna düşülür. İstenilen komutlar böylece uzaktan çalıştırılabilmektedir. Varsayılan olarak 22. portu kullanır.

SSH servisi, zayıf parola ile korunduğu taktirde kolaylıkla saldırganlar tarafından kullanılabilmektedir. Herhangi bir şekilde bahsi geçen ssh servisi bulan saldırganlar, sürekli olarak kullanıcı adı ve parola çiftleri deneyerek sunucuya erişim sağlamayı hedefler. Eğer bu kullanıcı adı – parola çiftlerinden herhangi biri erişim sağlamada başarılı olursa; sunucu, saldırgan tarafından kötü amaçları adına kullanılmaya başlar.

SSH servisi açık bir bal küpü sistemine statik ip adresi verilerek internete açılır. Bal küpü sistemi olarak Kippo SSH bal küpü kullanılmıştır. Kippo SSH, python programlama dili ile yazılmış bir bal küpüdür. Varsayılan 22. portta bir ssh servisi simüle etme kabiliyetine sahip olduğundan dolayı tercih edilmiştir. Bu port ile gerçekleştirilen her etkileşim kayıt altına alınır. Bu kayıtlar ayrıca MySQL veri tabanına kaydedilebilmektedir. Bu özelliğin kullanılması için sisteme ek olarak MySQL veri tabanı kurulmuştur. Kippo bu özelliklerinin yanı sıra kullanıcı adı – parola listesi alarak, bu listedeki kayıtlar ile eşleşen erişim isteklerine başarılı olduğuna dair cevap döndürür. Sisteme girdiklerini düşünen saldırganlar, işletim sisteminin simüle edildiğinden habersiz komutlar çalıştırır. Bu komutlarda kayıt altına alınarak, başarılı bir saldırının ardından yapılacak işlemler üzerinde analizlerde bulunmamıza imkân sağlanmaktadır.

Tüm bu kayıt toplama işlemlerinin ardından daha iyi analizler elde etmek adına sonuçların görselleştirilmesi amaçlanmıştır. Görselleştirme aracı olarak MySQL de tutulan veriler ile uygun olarak çalışabilen Kippo Graph uygulaması seçilmiştir. Kippo Graph, php programlama dili ile yazılmıştır. Oluşturulacak grafikler Libchart kütüphanesi kullanılarak çizdirilir.

Kippo SSH bal küpü, dört ay boyunca statik ip adresi ile internete bağlı olarak kalmıştır. Dört ay sonunda, saldırılarda 298 ip kullanılarak, SSH servisi üzerinde toplamda 23.271 adet deneme yapıldığı görülmüştür.



Şekil 1. En Sık Kullanılmış K. Adı / Parola Çifti [10]

ACTA INFOLOGICA
ISSN: 2602-3563

En çok erişim sağlanmaya çalışılan kullanıcı adı – parola çifti "root" ve "123456" olarak tespit edilmiştir. Zararlı aktiviteleri gerçekleştirmek için sisteme en yüksek haklara sahip olan kullanıcı olarak bağlanmak istemeleri şaşırtıcı değildir. Sisteme bağlanmak için; test, user ve guest gibi geçici kullanıcı adlarınında denendiği görülmüştür. En çok denenen diğer kullanıcılar ise adını kullanılacak olan servisden alan kullanıcılardır. Bunlara örnek olarak oracle, postgres veya tomcat verilebilir. Bu tip kullanıcıların yanında michael, alex veya amanda gibi sık kullanılan isimlerde denenmiştir. Şekil-1 'de kullanılmış kullanıcı adı-parola çiftleri incelenmiştir. Bal küpü, 12.269 benzersiz kullanıcı adı-parola çifti yakalamıştır. Bunların başında 142 deneme ile "root/123456" gelmektedir.

Kippo SSH bal küpüne bir kullanıcı adı – parola listesi verilerek bu kimlik bilgilerine erişimi başarılı olarak göstermesi amaçlamıştı. Bu kapsamda listeye "root/123456" çifti doğru kullanıcı adı – parola olarak verilmiştir. Fakat 23.271 denemeden 152 adet başarılı giriş olduğu görülmüştür. Ancak "root/123456" çiftini kullanan 142 adet deneme olduğu hali hazırda Şekil 1 üzerinde görülmüştü. Buradaki 10 adet fazlalık, doğru kimlik bilgilerini tespit eden saldırganların parolayı değiştirdiklerini göstermektedir.

Bağlanan kullanıcıların sistemde yaptıkları işlemlere ait kayıtlar elde edilmiştir. En çok çalıştırılmış komut, sistem bilgilerini geri döndüren "w" komutudur. Tahmin edildiği üzere, diğer en sık kullanılan komut ise ilgili klasördeki dosyaları listelemek için kullanılan "ls" komutudur. Birçok defa "-a" parametresi ile gizli dosyalarıda listelemeyi amaçladıkları görülmüştür. En sık kullanılan bir diğer komut ise "chmod +x *" komutudur. İlgili klasördeki tüm dosyalara çalıştırma izni verir. Bunlara ek olarak dosya indirmek için kullanılan "wget" ve parola değiştirmek için kullanılan "passwd" gibi birçok komutta çalıştırılanlar arasındadır.

3.4. Glashtopf Bal Küpü ile Sql Enjeksiyonu Uygulaması

Glastopf web uygulamaları için kullanılan bal küpü sistemlerinde sıklıkla tercih edilmektedir. Düşük etkileşimli bir bal küpü olduğu için kolaylıkla kurulmakta ve konfigüre edilebilmektedir. Python programlama dili ile yazılmıştır. Birçok bal küpü sisteminin aksine Glastopf, saldırıları simüle etmekte ve uygun bir cevabı üretmektedir. Bu sayede saldırganlar bir bal küpü ile etkileşimde olduklarını kolaylıkla farkedemezler. Böylece saldırganın teknikleri ve yöntemleri hakkında birçok bilgi edinilebilir. Uygulama olarak sql enjeksiyonu yapılacaktır.

Windows 10 işletim sistemi yüklü makine üzerinde bulunan sanallaştırma uygulaması ile Ubuntu 12.04 işletim sistemi kurulmuştur. Glastopf, Ubuntu içerisinde yüklenmiş ve konfigürasyonu yapılmıştır. Yine sanallaştırılmış Ubuntu üzerinden yerel olarak saldırı geçekleştirilecektir. Yapılan saldırılara ait kayıtlar sqlite veri tabanı kullanılarak Windows 10 üzerinde incelenmiştir. Gerekli konfigürasyonlar tamamlandığında Glastopf balküpü Şekil 2 üzerinde görüldüğü gibi başlatılır.

Şekil 2. Glastopf Başlatma Komutu Ve Çalıştırılması

Glastopf başlatıldıktan sonra konfigürasyonunda belirtilen çalışma dizinine gider. İlgili dizindeki db klasörü altına kayıtları tutacağı glastopf.db veri tabanını oluşturur. Eğer bu veri tabanı daha önceden mevcutsa kaldığı yerden devam ederek eklemeler yapar. Sqlite kullanıldığı için ve veri tabanı dizininin db klasörü olduğu belirtildiğinden dolayı ilgili dosya burada oluşturulmuştur.

Şekil 2 üzerinde görüldüğü gibi Glastopf hazır olarak beklemektedir. Aynı işletim sisteminde bulunan web tarayıcısı ile yerel ip adresimizin konfigürasyonda belirtilen portuna bağlanarak bal küpü ile etkileşime geçebiliriz. Bu durumda yerel ip adresimiz 192.168.5.136 olarak görülmüş ve bal küpüne konfigürasyonda 8080 portu atandığı için adres satırına http://192.168.5.136:8080/ yazarak bal küpüne Şekil 3'de görüldüğü gibi bağlanılmıştır.

ACTA INFOLOGICA
ISSN: 2602-3563

Şekil 3. Glastopf Web Arayüzü

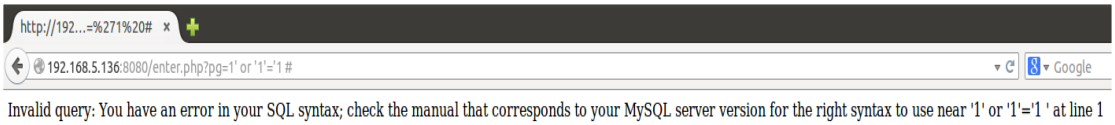
Web arayüzü oldukça basit olarak dizayn edilmiştir. Fakat istenildiği gibi üzerinde değişiklikler yapılabilmektedir. Görüldüğü gibi üzerinde giriş formu ile bir yazı ve ayrıca sayfa sonunda yorum yazılabilecek bir alan bulunmaktadır.

```
root@ubuntu:/opt/balkupuGlastopf# glastopf-runner
                    (glastopf.glastopf) Initializing Glastopf 3.1.2 using "/opt/balkupuGlastopf" as work directory.
                    (glastopf.glastopf) Connecting to main database with: sqlite:///db/glastopf.db
                    (glastopf.glastopf) Glastopf started and privileges dropped.
                    (glastopf.glastopf) 192.168.5.136 requested GET / on ubuntu.local:8080
                    (glastopf.glastopf) 192.168.5.136 requested GET /style.css on ubuntu.local:8080
```

Şekil 4. Glastopf Etkileşim Kaydı

Bal küpü ile etkileşime geçildiği anda bağlanan tarafın ip adresi ve yapılan istek kayıt altına alınmaktadır. Şekil-2 üzerinde görüldüğü gibi hazır olarak bekleyen Glastopf, Şekil 3'deki bağlanma işlemi ile Şekil 4'da görüldüğü gibi bir kayıt oluşturmuştur. Yerel işletim sisteminden saldırıyı gerçekleştirdiğimiz için ip adresimiz etkileşime geçen ip adresi olarak görülmektedir.

Glastopf, yapılan istek ve saldırıları emüle ettiğinden dolayı olmayan bir sayfanın olmayan bir pg değişkenini varmış gibi simüle etmekte ve yapılan sql enjeksiyonunu emüle ederek geriye Şekil-5 da görüldüğü gibi cevap döndürmektedir. Bu saldırının ardından Şekil 6 üzerinde görülebileceği gibi yapılan saldırıya ait kayıt düşmüştür.



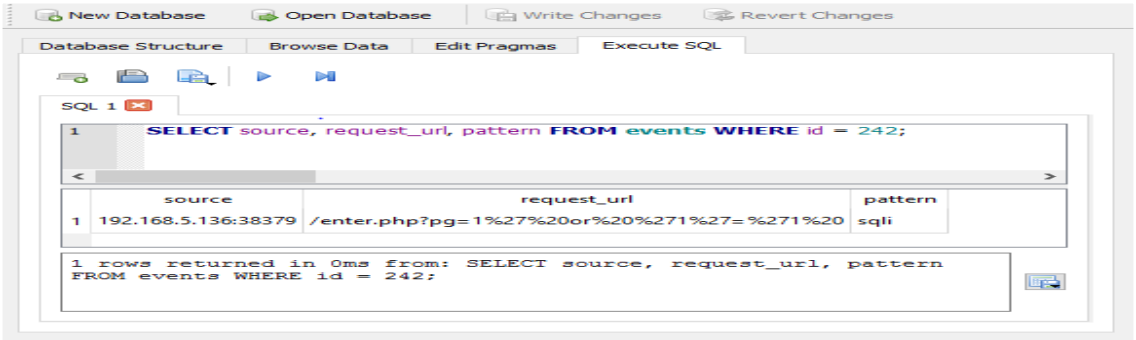
Şekil 5. Glastopf Sql Enjeksiyonu Cevabı

```
root@ubuntu:/opt/balkupuGlastopf# glastopf-runner
                    (glastopf.glastopf) Initializing Glastopf 3.1.2 using "/opt/balkupuGlastopf" as work directory.
                    (glastopf.glastopf) Connecting to main database with: sqlite:///db/glastopf.db
                    (glastopf.glastopf) Glastopf started and privileges dropped.
                    (glastopf.glastopf) 192.168.5.136 requested GET / on ubuntu.local:8080
                    (glastopf.glastopf) 192.168.5.136 requested GET /style.css on ubuntu.local:8080
                    (glastopf.glastopf) 192.168.5.136 requested GET /enter.php?pg=1%27%20or%20%271%27=%271%20 on ubuntu.local:8080
```

Şekil 6. Glastopf Sql Enjeksiyonu Kaydı

ISSN: 2602-3563

Windows 10 işletim sistemi üzerinde bulunan sqlite ile glastopf.db açılmış ve yalnızca ilgili kaydın görüntülenmesi adına select sorgusu yapılmıştır. Şekil 7 üzerinde görüldüğü gibi yapılan isteğimiz sql enjeksiyonu olarak tanımlanmış ve "sqli" etiketi ile kayıt altına alınmıştır.



Şekil 7. Glastopf Veri Tabanı Sql Enjeksiyonu Kaydı

4. TARTIŞMA VE SONUÇ

IDS, IPS ve ACL (erişim denetleme listeleri) gibi birçok pasif korunma yöntemleri, bilinen saldırı teknikleri üzerinde verimli bir şekilde çalışmasına karşın henüz keşfedilmemiş yöntemleri kullanan zararlı aktivitelerinin tespiti ve engellemesinde zayıf kalmaktadırlar. Bal küpü sistemleri bu eksikliği gidererek bilinmeyen yöntemleri kullanan saldırıları yakalamayı ve üzerinde analizler yapmayı olanaklı hale getirmiştir. Hemen hemen her alanda kullanımlarını sağlamak adına birçok bal küpü sistemi geliştirilmiştir. Gelişen modern dünyada her geçen gün farklı alanlar oluşmakta ve gereksinimler değişmektedir. Bu gereksinimlere bal küpü sistemlerinin kendini adapte etmesi her ne kadar hızlıda olsa bazı konularda eksikleri devam etmektedir. Ancak esnek yapıları ve herhangi bir sisteme kolay adapte olmaları sayesinde yeni moduller geliştirilerek eksikliklerin büyük kısmı kullanıcılar tarafından giderilebilmektedir.

KAYNAKLAR

Anonymous (2013). On Security Issues in Web Applications through Cross Site Scripting (XSS). In 2013 20th Asia-Pacific Software Engineering Conference (APSEC). IEEE.

Anonymous (2017). Antivirus software. En.wikipedia.org. Retrieved 1 February 2017, http://en.wikipedia.org/wiki/Antivirus_software.

Chauhan, S., & Shiwani, S. (2017). A honeypots based anti-phishing framework. In 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). IEEE.

Djanali, S., Arunanto, F., Pratomo, B., Baihaqi, A., Studiawan, H., & Shiddiqi, A. (2014). Aggressive web application honeypot for exposing attacker's identity. In 2014 The 1st International Conference on Information Technology, Computer, and Electrical Engineering. IEEE.

Koniaris, I., Papadimitriou, G., & Nicopolitidis, P. (2013). Analysis and visualization of SSH attacks using honeypots. In Eurocon 2013. IEEE.

Kuwatly, I., Sraj, M., & Al Masri, Z. (2004). A Dynamic Honeypot Design for Intrusion Detection. In The IEEE/ACS International Conference on Pervasive Services. IEEE.

Sharma, S. (2016). Detection and analysis of network & application layer attacks using Maya Honeypot. In 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence). IEEE.

Singh, A., & Joshi, R. (2011). A honeypot system for efficient capture and analysis of network attack traffic. In 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies. IEEE.

Song, Y., Zhu, X., Hong, Y., Zhang, H., & Tan, H. (2012). A Mobile Communication Honeypot Observing System. In 2012 Fourth International Conference on Multimedia Information Networking and Security. IEEE.

ISSN: 2602-3563

Yang, Y., Yang, H., & Mi, J. (2011). Design of distributed honeypot system based on intrusion tracking. In 2011 IEEE 3rd International Conference on Communication Software and Networks. IEEE.

Zakaria, W., & Kiah, M. (2012). A review on artificial intelligence techniques for developing intelligent honeypot. In 2012 8th International Conference on Computing Technology and Information Management (NCM and ICNIT). IEEE.

Bu çalışma 4. Uluslararası Yönetim Bilişim Sistemleri konferansında sunularak, özeti konferans özet kitabında yayınlanmıştır.