İSTANBUL TİCARET ÜNİVERSİTESİ FEN BİLİMLERİ DERGİSİ

İstanbul Commerce University Journal of Science

http://dergipark.org.tr/ticaretfbd

Araştırma Makalesi / Research Article

BALKÜPLERİNİN SALDIRI VE SAVUNMA AÇISINDAN İNCELENMESİ

EXAMINATION OF HONEYPOTS FROM OFFENSIVE AND DEFENSIVE PERSPECTIVE

Muhammed Sadık KARABAY[1] Can EYÜPOĞLU[2]

https://doi.org/10.55071/ticaretfbd.1245975

Sorumlu Yazar / Corresponding Author
ceyupoglu@hho.msu.edu.tr

Geliş Tarihi / Received
01.02.2023

Kabul Tarihi / Accepted
13.04.2023

Öz

Geçtiğimiz son 20 yıldaki teknolojik gelişmelerle beraber bilgisayar ağlarının kapasitesi ve bağlanan cihaz sayısı sürekli artmaktadır. Özellikle nesnelerin interneti (Internet of Things-IoT) teknolojisi ile internete bağlı cihaz sayısının 50 milyarı aşması beklenmektedir. Son kullanıcı tarafından kullanılan akıllı cihazlar ve bu cihazların kullanımındaki artış beraberinde devasa boyutlardaki veri akışını da getirmiştir. Covid-19 süreci ile uzaktan çalışma, çevrimiçi eğitim vb. durumlar neredeyse tüm işlemleri internet üzerinden yürütmeye ve verilere internet üzerinden erişime olanak vermiştir. Tüm bunlarla beraber, verilerin saklandığı, yürütüldüğü ve işlendiği sistemler saldırganların hedefi haline gelmiştir. Bu çalışmada olası siber saldırı senaryolarında saldırganların kurumsal ağ sisteminin içine sızması durumunda saldırganların dikkatini başka yöne çekmesine olanak sağlayacak balküpü sistemleri, hem saldırgan hem de savunan bakış açısıyla ele alınmıştır.

Anahtar Kelimeler: Balküpü, kızıl takım, siber saldırı, tuzak sistemler.

Abstract

With the technological developments in the last two decades, the capacity of computer networks and the number of connected devices are constantly increased. Especially with the Internet of Things (IoT) technology, the number of devices connected to the Internet is expected to exceed 50 billion. The smart devices used by the end users and the increase in the use of these devices have brought with them huge data flow. With the Covid-19 process, remote work, online education, etc. systems have made it possible to do almost all activities online and to access data over the internet. With all this, the systems in which data is stored, executed and processed have become the target of attackers. In this study, honeypot systems, which will allow attackers to divert the attention of attackers in case of infiltration into the corporate network system in possible cyber attack scenarios, are discussed from both the attacker and the defender perspective.

Keywords: Cyber attack, honeypot, red team, trap systems**.**

[1]Kuveyt Türk Katılım Bankası, Ar-Ge Merkezi, Kocaeli, Türkiye.
Milli Savunma Üniversitesi, Hezârfen Havacılık ve Uzay Teknolojileri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul, Türkiye.
karabay18@itu.edu.tr, Orcid.org/0000-0002-2524-439X.

[2]Milli Savunma Üniversitesi, Hava Harp Okulu, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye.
ceyupoglu@hho.msu.edu.tr, Orcid.org/0000-0002-6133-8617.

1. GİRİŞ

Kurumsal ağlarda güvenlik mekanizması genellikle dışarıdan gelebilecek saldırıları engelleme amaçlı tasarlanmaktadır. Ancak saldırgan bir şekilde sistem içerisine sızabilir. İşte bu noktada eğer ağda bir Saldırı Tespit Sistemi (Intrusion Detection System-IDS) yoksa saldırgan tespit edilemez ve dışarıya yönelik alınan tedbirler atlatılmış olur. Bu nedenle her noktada güvenlik prensibi ile hareket ederek, ağ içerisine bir IDS konumlandırılması gerekmektedir. Balküpü sistemleri saldırganı kendi üzerine çekerek ağ üzerinde bulunan değerli varlıkları korumayı ve saldırganı saldırı öncesi tespit etmeyi amaçlamaktadır. Balküpü sistemleri IDS'lere destek amaçlı kullanılmaktadır (Ng ve ark., 2018).

Literatürde balküpü sistemlerine ilişkin tasarımsal açıdan birçok çalışma bulunmaktadır. En kapsamlı çalışmalardan biri Bringer ve ark. (2012) tarafından gerçekleştirilmiş ve balküpleri birçok farklı açıdan değerlendirilmiştir. Bu çalışmada balküpü tasarım prensipleri, tespit uzmanlık alanları, limitleri ve fidye balküplerine değinilmiştir. İlgili çalışmada daha çok savunma amaçlı yaklaşımlara odaklanılmıştır. Zimmerman (2014) tarafından MITRE kuruluşunun desteği ile yayımlanan kitapta birinci sınıf siber güvenlik operasyon merkezleri için on stratejiden bahsedilmiştir. İlgili çalışmada siber operasyon tatbikatları ve bu tatbikatlarda ekiplerin rollerinden bahsedilmiş olup balküplerinin görevlerine değinilmiştir.

Giderek daha önemli hale gelen siber uzay güvenliği sorunlarıyla başa çıkmak için balküpü teknolojileri uygulanmaktadır. Bunun nedeni, mevcut siber çatışmalardaki tipik savunma stratejilerinin sıklıkla dezavantajlı duruma düşmesi sorunudur. Yang ve ark. (2023) bu sorunların üstesinden gelmek için etkileşimli bir balküpü tabanlı sistem önermiştir. Bu sistem, ekipman ve bilgi güvenliğini daha iyi korumak için saldırganın davranışını ve saldırı yöntemlerini gözlemlemek üzere saldırganları önceden belirlenmiş bir sanal alana çekmektedir. Priya ve Chakkaravarthy (2023) tarafından yapılan çalışmada saldırganların davranışlarını izlemek, analiz etmek ve değerlendirmek için bulut tabanlı araştırma balküpleri konuşlandırılmıştır. Çalışmanın sonuçlarında kötü niyetli kişilerin faaliyetleri ve amaçları hakkında önemli yargıların çıkarılabileceği sayısız veri noktası oluşturulduğu gözlemlenmiştir. Son zamanlarda yapılan diğer bir çalışmada (Amal & Venkadesh, 2023), saldırgan davranışlarını tespit etmek ve saldırıları önlemek için Docker'da konuşlandırılan bir hibrit honeynet önerilmiştir. Önerilen modelin fidye yazılımlarını ve saldırı eğilimlerini tespit etmenin yanı sıra güvenlik duvarını da ayarladığı görülmektedir.

Bu çalışmada balküpü sistemleri ve balküpü sistemlerinin çeşitlerinden bahsedilmiş, balküpü uygulama çalışmaları yapılmış, balküpü sistemlerinin saldırgan (karşı balküpü) ve savunan taraf bakış açısı ile incelenmesi gerçekleştirilmiştir. Çalışma kapsamında karşı balküpü sistemleri kırmızı takım (saldırgan) odaklı olarak değerlendirilmiştir.

2. BALKÜPÜ SİSTEMLERİ VE ÇEŞİTLERİ

2.1. Balküpü Sistemleri

Balküpleri, siber suçluları herhangi bir yasadışı kullanım için ağın içerisine girmeye çalıştıklarında aldatmaya ikna etmek için kullanılan bir tür güvenlik sistemidir. Balküpleri, genellikle saldırganın ağdaki faaliyetini anlamak için kurulmaktadır. Balküplerinin temel amacı, kötü amaçlı trafiği önemli sistemlerden uzaklaştırmak, kritik sistemlere saldırı yapılmadan önce saldırıya karşı erken uyarı almak, saldırgan ve saldırı yöntemleri hakkında bilgi toplamaktır. Balküpleri kullanılarak bir saldırgan kritik olmayan ve iyi izlenen bir sisteme saldırısını gerçekleştirmesi için kandırılır. Ardından saldırganın saldırı yöntemleri hakkında değerli bilgiler

elde edilebilir ve bu bilgiler adli amaçlar için toplanabilir. Bu sayede kurum ağına izinsiz girişlere karşı daha güçlü önleme yöntemleri geliştirilebilir. Ayrıca balküpleri, ağ trafiğinin günlüğe kaydedilmesine yardımcı olan sahte bir vekil (proxy) olduğundan ve gerçek bir sistem olmadığından değerli veriler taşımazlar (Uitto ve ark., 2017). Balküpleri ile genellikle yakalanan veri çeşitleri;

- Saldırgan tarafından gerçekleştirilen girişler ve kullandığı tuşlar,
- Saldırganın IP adresi,
- Saldırgan tarafından kullanılan kullanıcı adları ve ayrıcalıkları,
- Saldırgan tarafından erişilen, ele geçirilen, silinen veya değiştirilen verilerin türü

şeklindedir.

2.2. Balküpü Çeşitleri

Balküpleri fikirsel olarak olası saldırıları önleme amaçlı geliştirilir. Bu doğrultuda ağ sistem altyapısı olan Windows, Linux, Android, PLC ve Scada gibi birçok sistemde kullanılabilirler. Balküpleri etkileşim seviyelerine göre;

- Düşük etkileşimli balküpleri,
- Orta etkileşimli balküpleri,
- Yüksek etkileşimli balküpleri,
- Saf balküpleri,

Geliştirilme amaçlarına göre;

- Araştırma balküpleri,
- Sistem balküpleri,

Aldatma amaçlarına göre;

- Zararlı yazılım balküpleri,
- Veritabanı balküpleri,
- Spam/gereksiz e-posta balküpleri,
- E-posta balküpleri,
- Örümcek balküpleri,
- Balküpü ağları,
- İstemci balküpleri

olarak incelenmiştir.

2.2.1. Etkileşim Seviyelerine Göre Balküpleri

2.2.1.1. Düşük Etkileşimli Balküpleri

Düşük etkileşimli balküpleri, ağda veya sistemde bulunan çok sınırlı sayıda hizmet ve uygulama ile eşleşirler. Bu tür balküpleri; Kullanıcı Veribloğu İletişim Kuralları (User Datagram Protocol-UDP), İletim Kontrol Protokolü (Transmission Control Protocol-TCP) ve İnternet Kontrol Mesaj Protokolü (Internet Control Message Protocol-ICMP) bağlantı noktalarını ve hizmetlerini takip etmek için kullanılabilmektedir. Burada, gerçek zamanlı olarak meydana gelebilecek saldırıları anlamak üzere saldırganları tuzağa düşürmek için sahte veritabanları, veriler ve dosyalar oluşturulabilmektedir. Düşük etkileşimli balküpü araçlarına örnek olarak; Honeytrap, Spectre, KFsensor vb. verilebilir (Al-Jameel ve ark., 2021).

2.2.1.2. Orta Etkileşimli Balküpleri

Orta etkileşimli balküpleri, gerçek zamanlı işletim sistemlerini taklit etmeye dayanmaktadır. Tüm uygulamalarına ve hizmetlerine bir hedef ağ olabilecek kadar sahiptirler. Amaçları

saldırganı durdurmaktır. Olduğundan daha fazla bilgi yakalama eğilimindedirler. Böylece kuruluş, tehdide uygun şekilde yanıt vermek için daha fazla zaman kazanmaktadır. Orta etkileşimli balküpü araçlarına örnek olarak; Cowrie, HoneyPy vb. verilebilir.

2.2.1.3. Yüksek Etkileşimli Balküpleri

Yüksek etkileşimli balküpleri, bir sistemin genel olarak sahip olabileceği çeşitli uygulamalarla gerçek bir işletim sistemi üzerinde çalıştırılan gerçek savunmasız yazılımlardır. Bu balküpleri kullanılarak toplanan bilgiler daha verimlidir ancak sürdürülmesi zordur. Yüksek etkileşimli balküpü araçlarına verilebilecek en güzel örnek ise honeynet'tir.

2.2.1.4. Saf Balküpleri

Saf balküpleri genellikle bir organizasyonun gerçek sistem ortamını taklit eder. Bu sayede saldırgan onun gerçek bir ortam olduğunu varsayar ve onu kullanmaya daha fazla zaman ayırır. Saldırgan güvenlik açıklarını bulmaya çalıştığında, kurum uyarılır ve böylece her türlü saldırı daha erken önlenebilir (Dalamagkas ve ark., 2019).

2.2.2. Geliştirilme Amaçlarına Göre Balküpleri

2.2.2.1. Araştırma Balküpleri

Araştırma balküpleri, etkileşimi yüksek balküpleridir. Ancak saldırganların davranışları hakkında daha fazla bilgi edinmek için çeşitli hükümet veya askeri kuruluşların alanlarında araştırma odağıyla oluşturulmuşlardır. Farklı ağları hedef alan saldırgan/Gelişmiş Sürekli Tehdit (Advanced Persistent Threat-APT) gruplarının amaçları ve saldırı taktikleri hakkında bilgi toplama, kuruluşların karşılaştıkları tehditleri araştırma ve kuruluşların bu tehditlere karşı daha iyi nasıl korunabileceklerini öğrenmek için kullanılırlar. Araştırma balküplerinin kurulumu ve bakımı zordur. Ayrıca daha kapsamlı bilgi tutarlar.

2.2.2.2. Sistem Balküpleri

Sistem balküpleri genellikle kuruluşun gerçek iç sistem ağına kurulur ve kısıtlı bilgi içerirler. Bu balküpleri genel olarak diğer sistem sunucuları ile sistem iç ağına yerleştirilir. Genelde kurulumu ve kullanımı daha kolay olan, düşük etkileşimli balküpleridir. Araştırma balküplerine kıyasla saldırılar ve saldırganlar hakkında daha az bilgi elde ederler. Ayrıca dahili olarak ağda mevcut olduklarından herhangi bir dahili güvenlik açığını veya saldırıyı bulmaya yardımcı olurlar (Borkar ve ark., 2011).

2.2.3. Aldatma Amaçlarına Göre Balküpleri

2.2.3.1. Zararlı Yazılım Balküpleri

Bir ağdaki zararlı yazılımları tuzağa düşürmek için kullanılan balküpleridir. Amaçları, saldırganı veya herhangi bir zararlı yazılımı cezbetmek ve saldırı modelini anlamak için kullanılabilecekleri belirli saldırıları gerçekleştirmelerine izin vermektir. Bunlar, zararlı yazılımları tespit etmek için bilinen çoğaltma ve saldırı vektörlerini kullanabilir. Örneğin, yetkisiz değişikliklerin kanıtı için kontrol edilebilen bir USB sürücüsünü taklit etmek için balküpü yapılabilir (Nawrocki ve ark., 2016).

2.2.3.2. Veritabanı Balküpleri

Veritabanı balküpleri, adından da anlaşılacağı üzere savunmasız olan ve genellikle SQL enjeksiyonları gibi saldırıları çeken gerçek veritabanları gibi görünürler. Saldırganları, kuruma gerçekleştirilen saldırıların modelini anlamasını sağlayacak şekilde kredi kartı bilgileri gibi hassas bilgiler içerebileceklerini düşünmeye ikna etmeyi amaçlarlar.

2.2.3.3. Spam/Gereksiz E-Posta Balküpleri

Spam/gereksiz e-posta balküpleri, spam gönderenleri savunmasız e-posta öğelerinden yararlanmaya çekmek ve bunlar tarafından gerçekleştirilen etkinlikler hakkında ayrıntılar vermek için sahte e-posta sunucularından oluşurlar. Açık posta geçişlerini ve açık proxy'leri taklit etmek için kullanılabilir. Spam/gereksiz e-posta gönderenler önce kendilerine bir e-posta göndererek açık posta aktarımını test edeceklerdir ve bu başarılı olursa, büyük miktarlarda spam/gereksiz e-posta göndereceklerdir. Spam/gereksiz e-posta balküpleri testi algılayıp tanıyabilir ve ardından gelen çok büyük miktardaki spam/gereksiz e-postaları başarıyla engelleyebilir (Campbell ve ark., 2015).

2.2.3.4. E-Posta Balküpleri

E-posta balküpleri, internetteki saldırganları çekmek için kullanılan sahte e-posta adresleridir. Herhangi bir kötü niyetli kişi tarafından alınan e-postalar izlenebilir, incelenebilir ve kimlik avı e-posta dolandırıcılıklarının düşmesine yardımcı olmak için kullanılabilir.

2.2.3.5. Örümcek Balküpleri

Örümcek balküpleri, web uygulamalarından önemli bilgileri çalma eğiliminde olan çeşitli web gezginlerini ve örümcekleri tuzağa düşürmek amacıyla kurulmaktadır.

2.2.3.6. Balküpü Ağları

Balküpü ağları, saldırganların faaliyetlerini kaydetmek ve potansiyel tehditleri anlamak için sanal ve izole bir ortama çeşitli sunucularla birlikte kurulan ağlardır.

2.2.3.7. İstemci Balküpleri

Çoğu balküpü, bağlantıları dinleyen sunuculardan oluşurken istemci balküpleri, kötü amaçlı sunucuları aktif olarak arayan ve sistemlerde beklenmedik değişiklikleri izleyen istemci sistemleridir. Genellikle bu sistemler sanallaştırma teknolojisi ile çalışmaktadır. Böylece virüs bulaşmış sistemler enfeksiyon sonrası temizlenebilmektedir.

3. UYGULAMA ÇALIŞMASI

Uygulama çalışması esnasında kullanılan sistemler aşağıdaki gibidir:

- Honeydrive sanal balküpü laboratuvarı
- Kali-Linux

Honeydrive sisteminde kullanılan araçlar:

- Kippo balküpü sistemi
- Kippo Graph izleme sistemi
- Honeyd balküpü sistemi

- Dionaea balküpü sistemi
- DionaeaFR izleme sistemi

Kali-Linux sisteminde kullanılan araçlar:
- Nmap network ve zafiyet tarama aracı
- Medusa kaba kuvvet saldırı aracı
- Metasploit çoklu saldırı aracı
- Metasploit üzerinde bulunan karşı balküpü detect_kippo aracı

Uygulama çalışması üç sistemin test edilmesine dayanmaktadır. Bu adımlar aşağıdaki gibidir:

i. İlk aşamada Honeydrive sisteminde bulunan Kippo honeypot ve Kippo izleme sistemi kurulmuştur. Daha sonra Kali-Linux sistemi üzerinden nmap aracı ile tarama çalışması yapılmıştır. Elde edilen sonuçlar neticesinde Güvenli Kabuk (Secure Shell-SSH) bağlantı portunun açık olduğu gözlemlenmiştir. Kaba kuvvet saldırılarına karşı açık olan SSH portuna root kullanıcısı ile parola denemeleri yapılmıştır. Basit parola olması nedeni ile kısa zamanda parola 123456 olarak tespit edilmiştir. Daha sonra user kullanıcısı ile denemeler yapılmıştır. Denemeler sonucu neticesiz kalmıştır. Parolası tespit edilen root kullanıcısı ile sisteme SSH bağlantısı yapılmıştır. Sistemde kritik dizilerde gezintiler yapılmıştır. Tüm bu saldırılar Kippo Graph izleme sistemi üzerinden takip edilmiştir. Metasploit aracı çalıştırılarak detect_kippo aracı ile hedef sistem taranmıştır. Sistemin balküpü olduğu tespit edilmiştir.

ii. İkinci aşamada da Honeydrive sisteminde bulunan Honeyd balküpü sistemi kurulmuştur. Bu kısımda sistem konfigürasyonları değiştirilerek sistemdeki değişikler loglar üzerinden gözlemlenmiştir.

iii. Üçüncü aşamada ise Honeydrive sisteminde bulunan Dionaea balküpü sistemi ve DionaeaFR izleme sistemi kurulmuştur. Dionaea sistemine karşı nmap aracı ile farklı çeşitlerde taramalar yapılmıştır. Tarama çalışmaları Dionaea sistemi üzerinden takip edilmiştir.

3.1. Kullanılan Sistemler

3.1.1. Honey Drive

BruteForce Laboratuvarı tarafından geliştirilen Honey Drive balküpü laboratuvarı farklı tiplerdeki balküplerini ve adli bilişim araçlarını bünyesinde bulundurmaktadır. Sistem üzerindeki balküplerinden istenilen balküpünün seçilerek kullanımına ve izlenmesine olanak sağlamaktadır.

3.1.1.1. Kippo

Kippo orta etkileşimli bir balküpü sistemi olup, Kippo-Graph ve Kippo2MySQL sistemlerini ile de beraber çalışabilmektedir. SSH bağlantılarını üzerine çekmesi için geliştirilmiştir. Kippo-Graph aracı ile gerçekleştirilen bağlantı denemeleri ve başarılı bağlantılar sonrası gerçekleştirilen komutlar tespit edilip izlenebilmektedir. Farklı tablo formatlarında birçok görsel ile çeşitli istatistik sonuçlar verebilmektedir.

3.1.1.2. Honeyd

Honeyd balküpü sistemi düşük etkileşimli balküpleri arasındadır. Değişik konfigürasyon ayarlamaları yapılarak saldırganların ilk aşaması olan keşif adımında yanılmalarına olarak tanımaktadır. Bu sistem ile loglar üzerinden gerçekleştirilen port taramaları tespit edilebilmektedir.

3.1.1.3. Dionaea

Dionaea, zararlı yazılımları ve zafiyetlerden yararlanarak saldırı girişiminde bulunan saldırganları tespit etme amaçlı geliştirilmiştir. Orta etkileşimli bir balküpüdür. DionaeaFR izleme aracı ile sistem üzerinde gerçekleştirilen taramalar, bağlantılar, zararlı bağlantılar, URL adresleri, zararlı yazılımlar, saldırganlar ve IP lokasyon bilgileri izlenebilmektedir.

3.1.2. Kali-Linux

Kali Linux, gelişmiş sızma testi ve güvenlik denetimini hedefleyen açık kaynak kodlu Debian tabanlı bir Linux dağıtımıdır. Kali Linux; sızma testi, güvenlik araştırması, adli bilişim ve tersine mühendislik gibi çeşitli bilgi güvenliği çalışmalarına yönelik 600'den fazla araç içermektedir.

3.1.2.1. Nmap

Nmap (Network Mapper), ağ keşfi ve güvenlik denetimleri için geliştirilmiş ücretsiz ve açık kaynak kodlu bir araçtır. Nmap, ağ üzerinde;

- hangi bilgisayarların kullanılabilir olduğunu,
- bu bilgisayarların hangi hizmetleri (uygulama adı ve sürümü) sunduğunu,
- hangi işletim sistemlerini (ve işletim sistemi sürümlerini) çalıştırdıklarını,
- ve bu sistemlere ait zafiyetleri,

tespit etmek amaçlı kullanılır.

3.1.2.2. Medusa

Medusa, kaba kuvvet saldırıları için geliştirilmiş hızlı, paralel ve modüler bir oturum açma aracıdır. Uzaktan kimlik doğrulamaya izin veren çok sayıda hizmeti desteklemekte ve paralel testler ile aynı anda birçok deneme gerçekleştirebilmektedir. Kaba kuvvet testi, aynı anda birden fazla ana bilgisayara, kullanıcıya veya parolaya karşı gerçekleştirilebilir. Esnek kullanıcı girdilerine olanak tanır. Hedef bilgileri (ana bilgisayar/kullanıcı/şifre) çeşitli şekillerde belirlenebilir. Örneğin, her öğe tek bir girdi veya birden çok girdi içeren bir dosya olabilir. Çoklu protokoller desteklenmektedir. Bunlardan bazıları aşağıdaki gibidir;

- Sunucu İleti Bloğu (Service Message Block-SMB): Sunucu ve istemci arasındaki iletişimi sağlayan ağ protokolüdür.
- Hiper Metin Transfer Protokolü (Hyper Text Transfer Protocol-HTTP): Web sistemlerinde, kullanıcı ile sunucu arasındaki protokoldür.
- Microsoft Yapılandırılmış Sorgu Dili (Microsoft Structured Query Language-MS-SQL): Microsoft tabanlı veritabanları için haberleşme protokolüdür.
- Uzak Masaüstü Protokolü (Remote Desktop Protocol-RDP): Uzak masaüstü bağlantısı için kullanılan protokoldür.
- Güvenli Kabuk sürüm 2 (Secure Shell version 2-SSHv2): Güvenli kabuk bağlantıları için şifreli bir trafik kullanmak için geliştirilmiş protokoldür.

3.1.2.3. Metasploit

Metasploit platformu, saldırganlar ve sızma testi çalışmaları yapan siber güvenlik uzmanları tarafından kullanılmaktadır. Sistemlerdeki açıklıkları tespit amaçlı kullanılır. Özellikle sistemde tespit edilen bir açığın sistemde var olup olmadığını kontrol ve istismar etme amaçlı kullanılır. İstismar kodları, zararlı kodlar, ek fonksiyonlar, port dinleyicileri, kabuk kodları, istismar sonrası kullanılan kodları gibi birçok modülden oluşmaktadır. Bunlarla beraber sistemleri tespit modülleri de bulunmaktadır.

3.1.2.4. Detect_kippo

Metasploit üzerindeki ek modüllerden biri olan detect_kippo aracı Kippo sistemine odaklanmaktadır. Karşı balküpü sistemlerinden olan bu araç çalışma prensibi olarak aşağıdaki yolları izler;

i. Karşı sisteme SSH bağlantı denemesi yapar,
ii. Open SSH protokolü desteğini sorgular,
iii. Balküpü sistemleri tarafından kullanılan varsayılan bayrak dönüşü olursa balküpü tespitini yapar.

3.2. Uygulama Çalışmaları

3.2.1. Kippo Honeypot, İzleme ve Tespit Uygulama Çalışması

3.2.1.1. Kurulum

Aşağıdaki komut yazılarak kurulum yapılır.

```
./honeydrive/kippo/start.sh
```

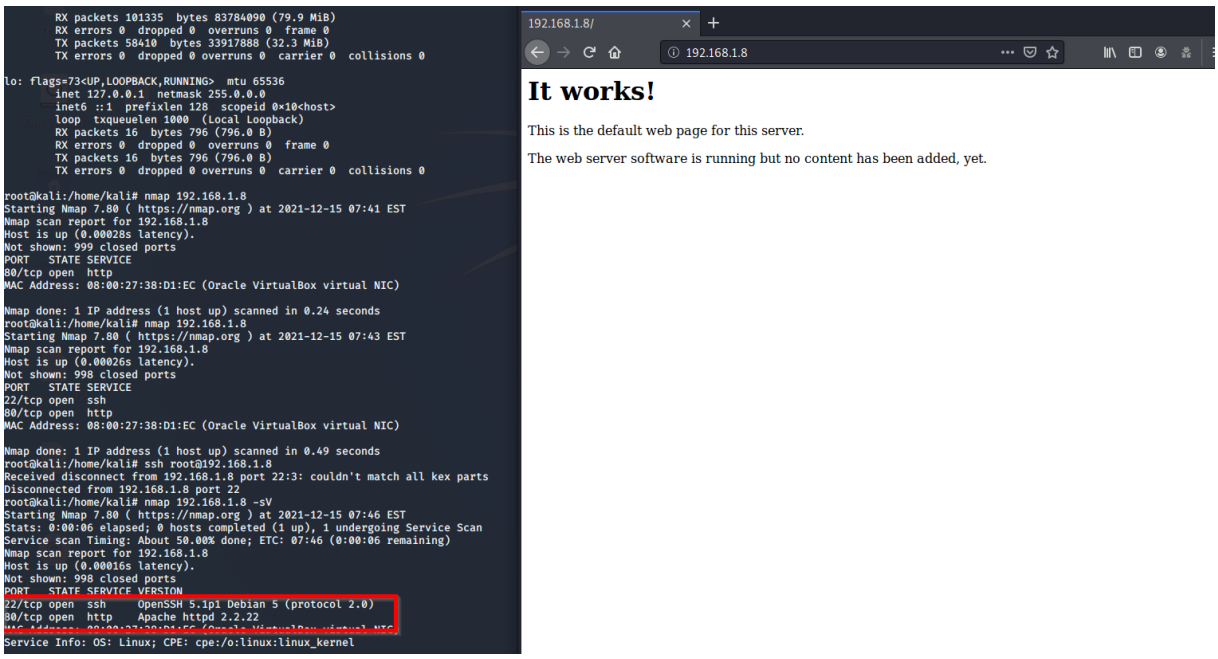
3.2.1.2. Test Çalışması

Kali Linux üzerinden nmap aracı ile Kippo sistemine tarama çalışması yapılır (Şekil 1).

```
ifconfig
nmap <<Hedef Sistem IP adresi>> -sV
```

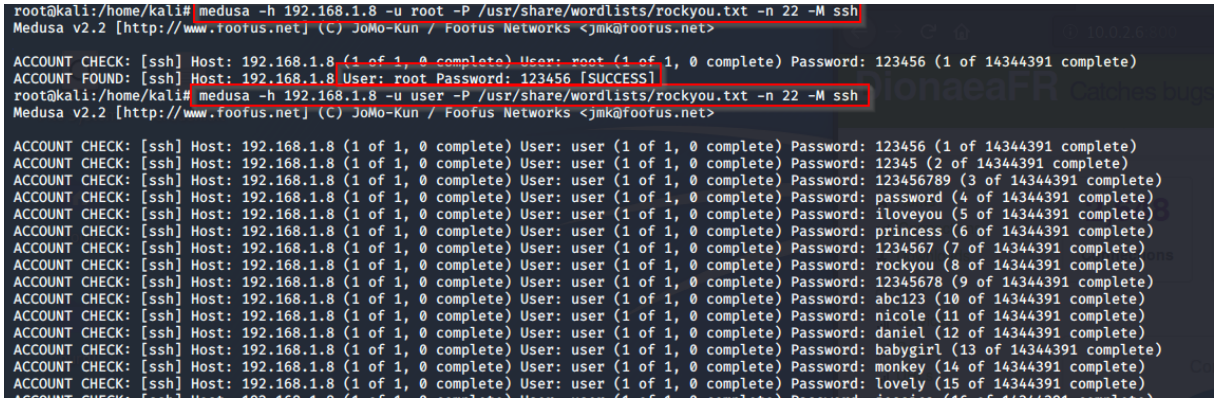
Tarama sonrası sistem üzerinde 22/SSH portunun açık olduğu gözlemlenmiştir. Bunun üzerine medusa aracı kullanılarak root ve user kullanıcıları için kaba kuvvet denemeleri gerçekleştirilmiştir. Root kullanıcısına ait parola “123456” olarak tespit edilmiştir. Kaba kuvvet deneme komutları;

```
medusa -h <<Hedef IP adresi>> -u <<Kullanıcı adı>> -P <<kullanılan parola listesi>>
```



Şekil 1. Kippo – Nmap Taraması

Kaba kuvvet saldırıları ile SSH parola tespiti sağlanmıştır (Şekil 2).

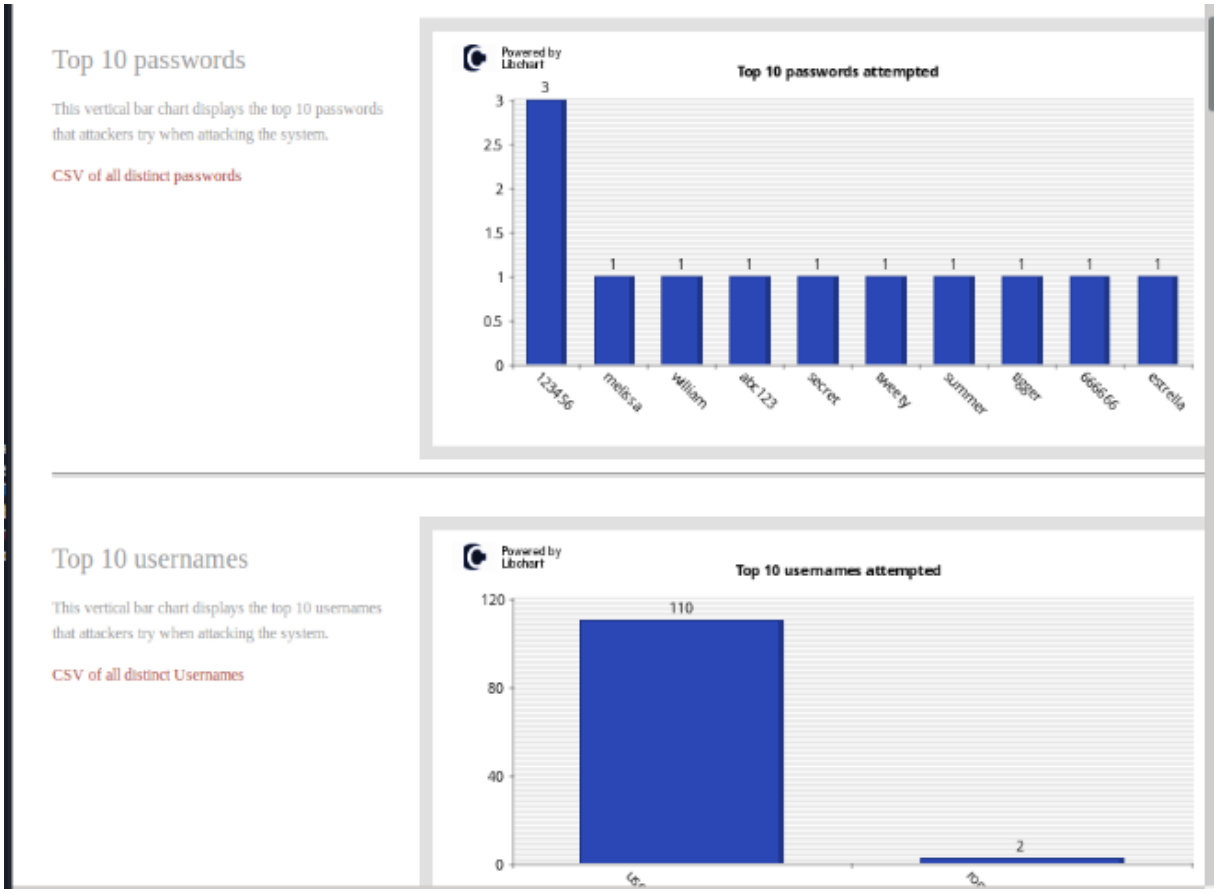


Şekil 2. Kippo – Medusa SSH Bağlantısı Kaba Kuvvet Denemesi

Tespit edilen parola ile sisteme SSH bağlantısı gerçekleştirilmiştir (Şekil 3). Dizinlerde geçişler yapılmış ve kritik dosyalara erişim sağlanmıştır.

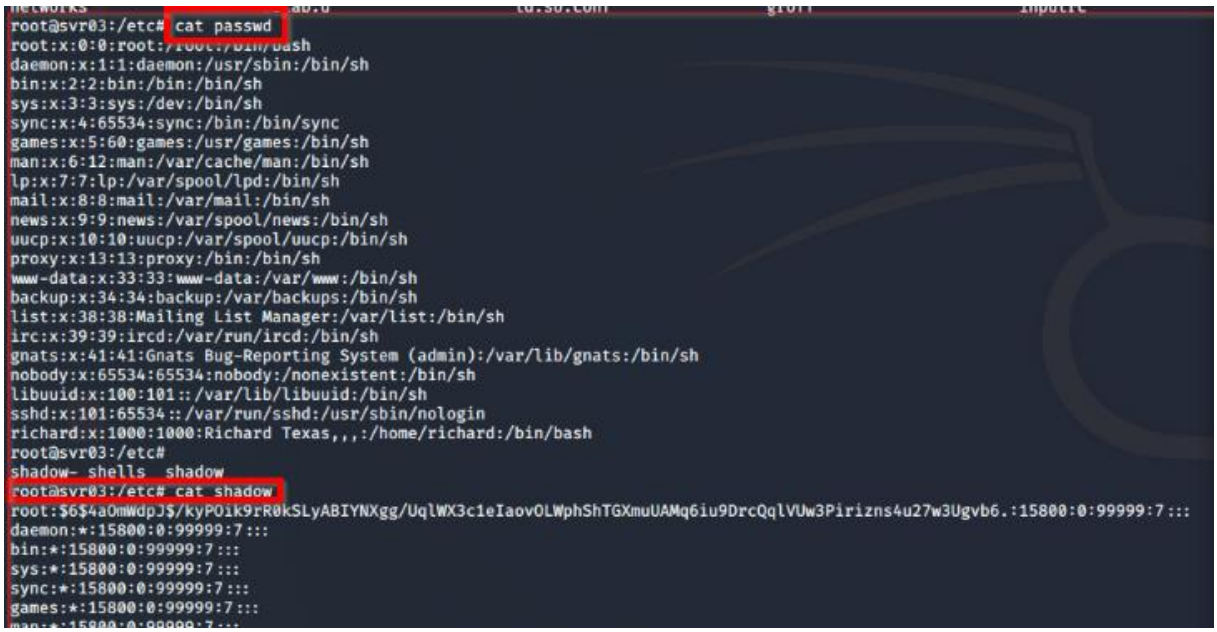
Şekil 3. Kippo – SSH Bağlantısı

Kippo arayüzü kullanılarak gerçekleştirilen parola denemeleri gözlemlenmiştir (Şekil 4).



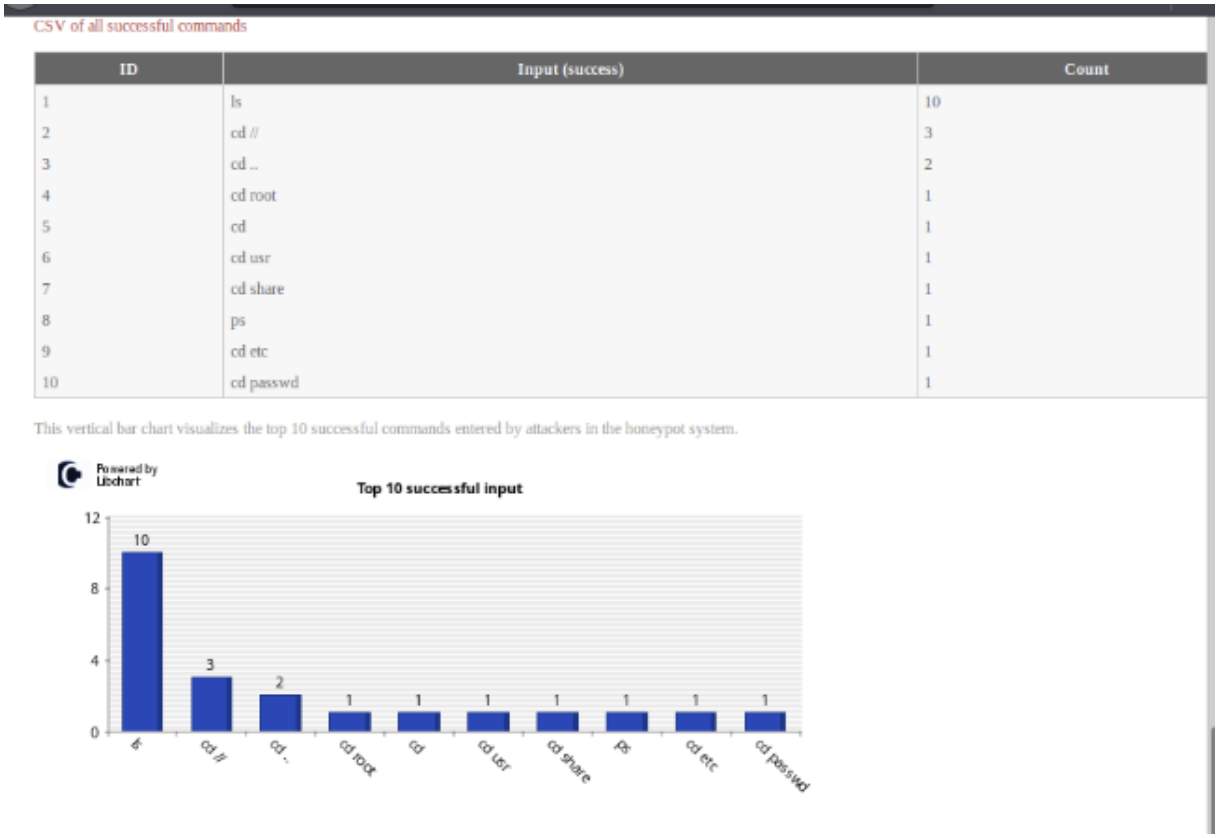
Şekil 4. Kippo – Bağlantı Denemelerinin Gözlemlenmesi

Çalıştırılan komutlar ile kritik dizinlerdeki dosyalar okunmuştur (Şekil 5).



Şekil 5. Kippo – Kritik Dizinlerde Dolaşma

Çalıştırılan komutlar Kippo-Graph üzerinden de gözlemlenmiştir (Şekil 6).



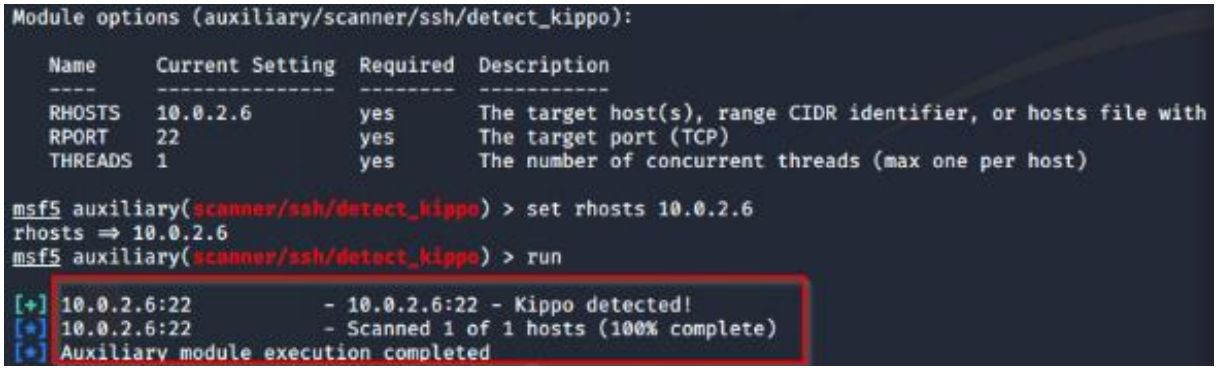
Şekil 6. Kippo – Çalıştırılan Komutların Kippo-Graph Üzerinden Gözlemlenmesi

3.2.1.3. Tespit Çalışması

Kali Linux üzerinde Metasploit aracı çalıştırılmıştır. Metasploit üzerinde bulunan detect_kippo aracı ile hedef sistem taranmıştır. Balküpü olduğu tespit edilmiştir. Kullanılan komutlar aşağıdaki gibidir:

```
search kippo
use 0
show options
set rhosts <<Hedef IP adresi>>
run
```

Metasploit platformunda bulunan detect_kippo aracı çalıştırılarak balküpü tespiti sağlanmıştır (Şekil 7).



Şekil 7. Kippo – Balküpü Tespiti

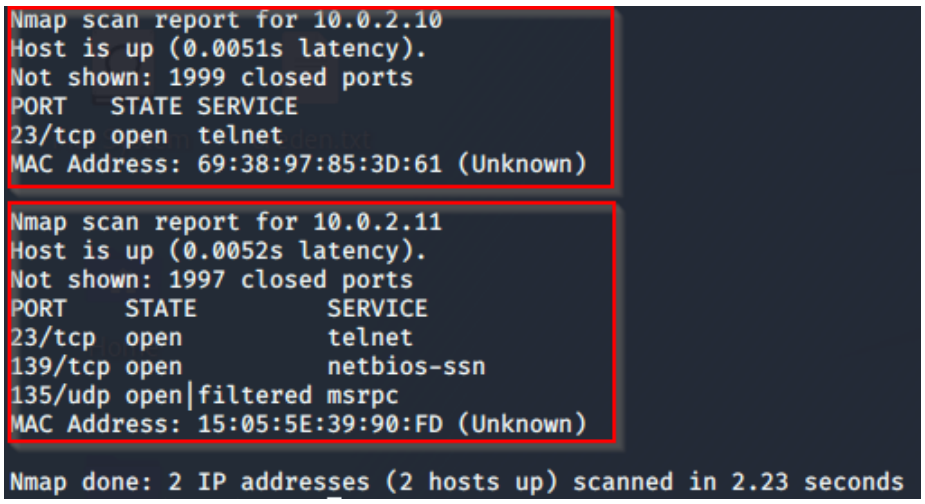
3.2.2. Honeyd Balküpü Uygulama Çalışması

3.2.2.1. Kurulum ve Konfigürasyon

"/etc/honeypot/huten-honey.conf" dizininde bulunan konfigürasyon dosyasına ait bilgiler aşağıdaki gibi belirlenmiştir. Konfigürasyon dosyasına gerekli ayarlamalar yapıldıktan sonra aşağıdaki komutlar ile balküpü sistemler çalıştırılmıştır.

```
create winxp
set winxp personality "Microsoft Windows XP Professional SP1"
add winxp tcp port 23 "perl /usr/share/honeyd/scripts/telnet/faketelnet.pl"
add winxp tcp port 139 open
add winxp tcp port 137 open
add winxp udp port 135 open
set winxp default tcp action reset
set winxp default icmp action open
set winxp ethernet "15:05:5E:81:19:0A"
set winxp default udp action reset
bind 10.0.2.11 winxp
create cisco
set cisco personality "Cisco 1601R router running IOS 12.1(5)"
add cisco tcp port 23 "perl /usr/share/honeyd/scripts/router-telnet.pl"
set cisco default tcp action reset
set cisco default udp action reset
set cisco uid 32767 gid 32767
set cisco ethernet "69:38:97:29:AB:56"
bind 10.0.2.10 cisco
sudo honeyd -d -i eth0 -f /etc/honeypot/huten-honey.conf -l /var/log/honeypot/honeyd.log
```

Oluşturulan sistemler Kali Linux üzerinden nmap kullanılarak ağ taraması ile gözlemlenmiştir (Şekil 8).



Şekil 8. Honeyd – Nmap ile Port ve Servis Tespiti

3.2.3. Dionaea Honeypot ve İzleme Uygulama Çalışması

3.2.3.1. Kurulum

Aşağıdaki komutu çalıştırılarak Dionaea balküpü sistemi kurulur.

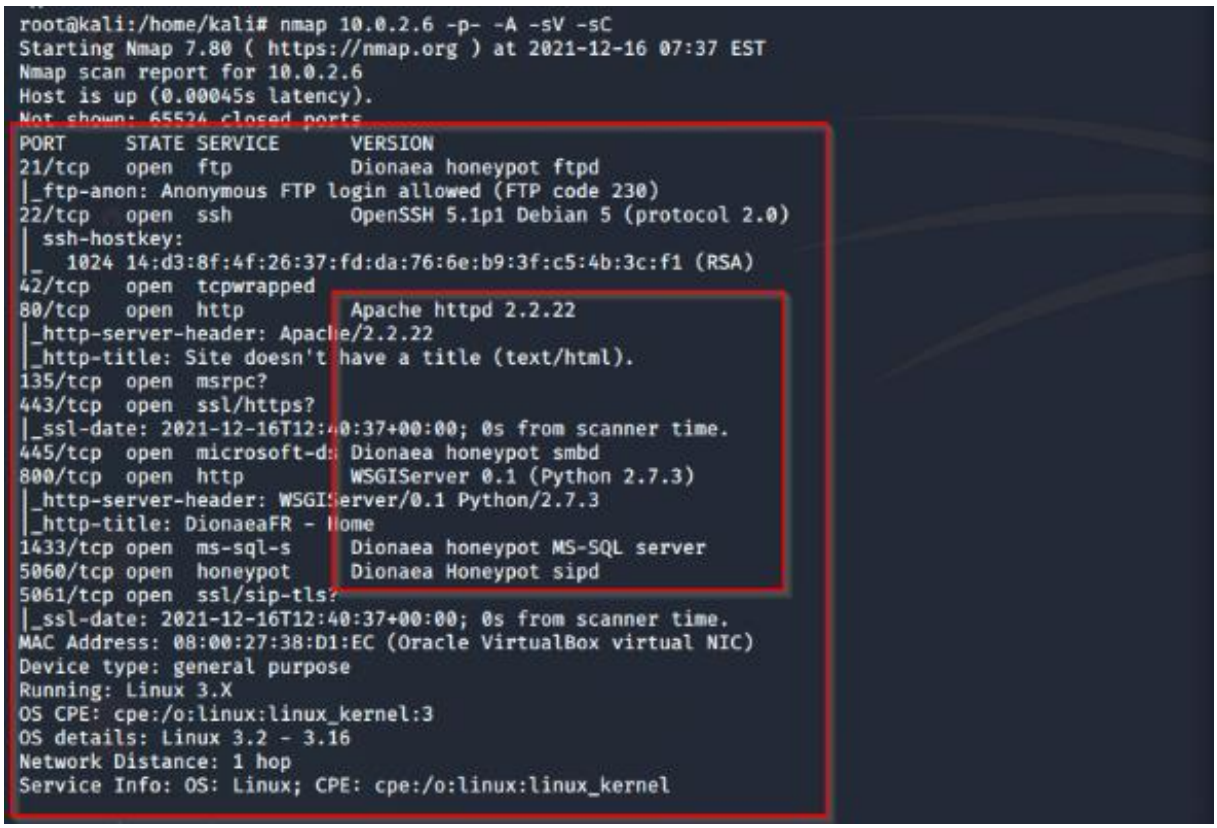
```
./honeydrive/dionaea-vagrant/runDionaea.sh
```

Balküpü üzerindeki etkileşimleri gözlemlemek için DionaeaFR izleme aracı kurulumu yapılır.

```
cd /honeydrive/DionaeaFR
python manage.py collectstatic
python manage.py runserver <<Sistem IP adresi>>:<<hizmet verilecek port>>
```

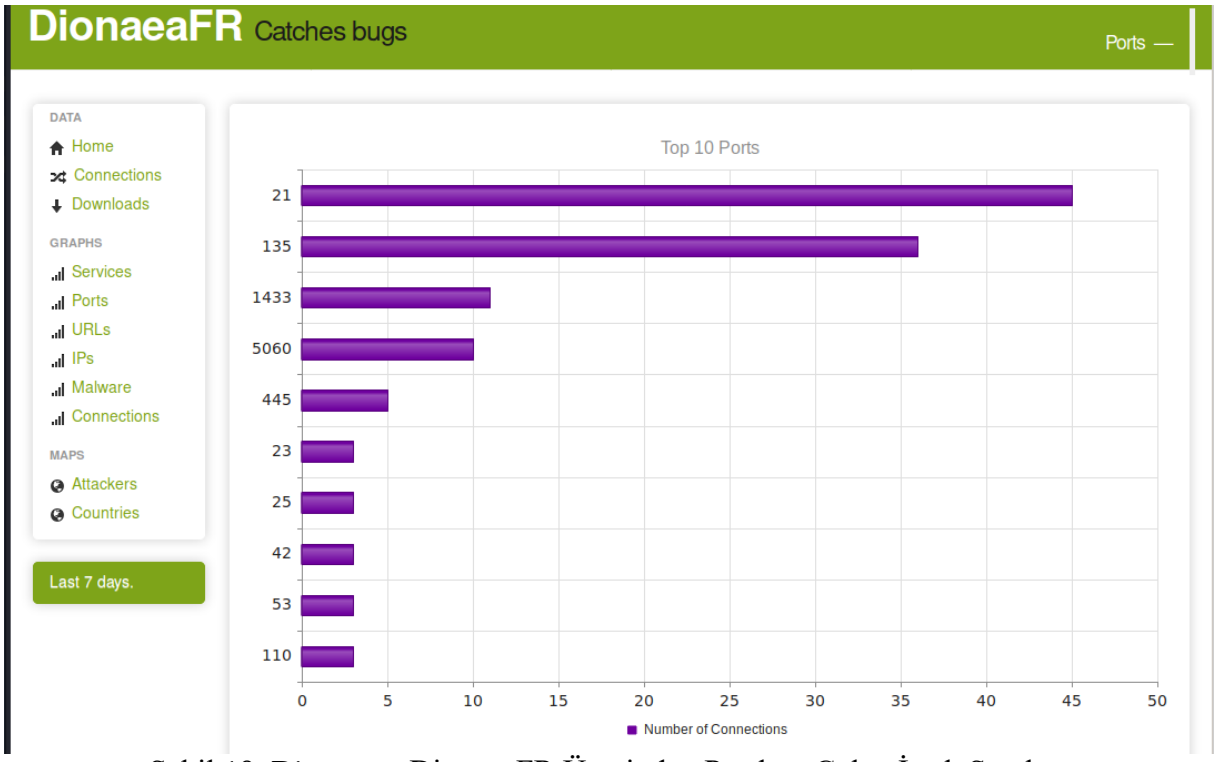
3.2.3.2. Test ve İzleme Çalışması

Kurulum sonrası Kali Linux üzerinden nmap aracı ile zafiyet, port, servis ve versiyon taraması yapılır (Şekil 9)



Şekil 9. Dionaea – Nmap Taraması

Nmap aracı ile hedef sistemin tüm portları taranmıştır. DionaeaFR ile ilgili taramalar izlenmiştir (Şekil 10).



Şekil 10. Dionaea – DionaeaFR Üzerinden Portlara Gelen İstek Sayıları

4. SALDIRI VE SAVUNMA AÇISINDAN BALKÜPLERİNİN DEĞERLENDİRİLMESİ

Balküpleri, saldırganlar için hedef haline getirilmekte ve kuruluma bağlı olarak tespit edilmesi genellikle zor olabilmektedir. Yüksek etkileşimli bir balküpü, gerçek bir sistemin çalışması için beklenebilecek her şeyi çalıştırmakta ve bu nedenle tespit edilmesi çok zor olabilmektedir. Düşük etkileşimli bir balküpünün ise, saldırgan içerideyken tespit edilmesi oldukça kolaydır. Düşük etkileşimli bir balküpü; basit işlemlere sahip olacak, birçok temel araç eksiklikleri barındıracak veya beklendiği gibi çalışmayacaktır. Bu durum da saldırganın balküpünü tespit etmesine neden olacaktır. Tüm bu olasılıklar tamamen balküpünün nasıl kurulduğuna bağlıdır. Balküplerini tespit etmek için kesin olarak belirlenmiş bir yöntem yoktur. Balküplerini tespit etmek için belirli bir yöntem keşfedilirse, yöntemi geçersiz kılmak için hemen yeni balküpleri duruma göre geliştirilecektir (Uitto ve ark., 2017).

4.1. Savunma Açısından Balküpleri

Siber savunmada balküplerinin kuşkusuz birçok faydası bulunmaktadır. Kurum güvenliğinde kullanılan cihazlar arasında duruma göre güvenlik duvarları, web uygulama güvenlik duvarı, Dağıtık Hizmet Reddi (Distrubuted Denial of Service-DDOS) atağı engelleme cihazı, yeni nesil antivirüsler, Sandbox'lar, ağ güvenlik cihazları, Güvenlik Bilgileri ve Olay Yönetimi (Security Information and Event Management-SIEM), Güvenlik Düzenleme, Otomasyon ve Müdahale (Security Orchestration, Automation and Responce-SOAR) gibi dışarıdan gelebilecek saldırıları karşılamak, yönetmek, engellemek amaçlı birçok sistem bulunmaktadır. Tüm bu sistemlerle beraber balküpleri iç ağa yerleştirilerek olası bir saldırıda sisteme alarm üretmektedir. İçeri sızan bir saldırganı balküpleri ile tespit etmek kurumların ciddi kayıplar vermesini engellemektedir.

Balküplerinin ağa yerleştirildikten sonra sağladığı avantajlar aşağıdaki gibi sıralanabilir:

- Balküplerinin herhangi bir trafiğe sahip olmaması gerekmektedir. Eğer üzerinde herhangi bir trafik var ise bu kötü amaçlıdır. Bu sayede daha az hatalı alarm sonucu alınabilmektedir.
- Saldırı anında tüm trafikteki verileri toplamak yerine sadece adli verileri toplayarak daha küçük ve yüksek değerli veri kümelerinin oluşturulmasına olanak tanımaktadır.
- Saldırıları kritik olmayan hatta kullanım dışı bir sisteme yönlendirerek saldırganın zamanını boşa harcamasına sebep olabilir ve bu sayede saldırı hakkında erken uyarı alınmış olur.
- IDS'lerin aksine bilinen saldırı imzaları gerektirmez.

Balküpü konfigürasyonları gerçekleştirilirken dikkat edilmesi gereken hususlar aşağıdaki gibidir:

- Konumlandırması yapılacak balküpünün bulunduğu alt ağdaki (subnet) ve alan adındaki (domain) makinalarla benzerlik teşkil etmesi gerekmektedir. Makine adı sistemdeki makine isimleri ile benzer olmalı, benzer portlar aktif olmalı ve servisler çalışmalıdır. Kurum politikasına bağlı olarak IP adres bloğuna göre kullanıcı isimlendirmeleri yapılmalıdır.
- Sistemlerde oluşan alarmlar ve konfigürasyonlar düzenlenmelidir. Aksi halde birçok alarm alınır ve bu da siber güvenlik takımının gereksiz yere çaba harcamasına sebep olur. Sonuç olarak sistemin verimliliği düşmüş olur.

Balküpü tespit araçlarının kaynak kodları incelendiğinde varsayılan ayarları kontrol ederek tespit etme işlemlerini gerçekleştirdikleri gözlemlenmiştir. Bu nedenle konfigürasyonlar kurum politikalarına göre düzenlenmelidir.

4.2. Saldırı Açısından Balküpleri

Siber savunmada savunma takımı ve savunma cihazları ne kadar önemli ise saldırı takımı da yani saldırgan bakış açısı ile sistemi test etmek de en az o kadar önemlidir. Bu nedenle balküpleri, sisteme yerleştirilirken aynı zamanda istismarları ve atlatma yöntemleri de düşünülerek tasarım yapılması gerekmektedir. En önemli ve can alıcı noktayı bu adım oluşturmaktadır. Çünkü bir sistemin güvenliğinden bahsedildiğinde bu sistemin saldırgan bakışı ile atlatılarak limitlerinin bilinmesi gerekmektedir. Karşı balküpü sistemleri ve çalışmaları da kızıl takım tatbikatları esnasında gelişmektedir. Bazıları da saldırganlar tarafından saldırılarını kolaylaştırma amaçlı geliştirilirler.

Saldırgan bakışı ile bakıldığında; neler çalışıyor, hangi teknolojileri kullanmakta, kimler çalışıyor, hangi algoritmaları kullanıyor, hangi portlar açık bilmek gereklidir. Bu konu daha çok savunma tarafı değil de saldırı tarafı için önemlidir. Bir sisteme sızma testi gerçekleştirilirken o sistemde balküpüne yakalanma oranı yüksektir. Ayrıca iyi kurgulanmış ve amacına uygun konfigüre edilmiş bir balküpü gerçekten tespit edilemez bile olabilir. Bu bilgilere göre karşı balküpü sistemleri geliştirilebilir.

Balküplerinin tespiti zordur. Çünkü emülasyon olsa bile saldırgana gerçek bir sistemmiş gibi gözükebilir. Balküplerini tespit etmek için bazı karşı balküpü yazılımları bulunmaktadır. Bunlardan öne çıkan yazılım Send-Safe Honeypot Hunter'dır. Bunun gibi yazılımlar portları ve portlarda çalışan servisleri analiz ederek sistemin gerçek veya tuzak bir sistem olup olmadığını anlamaya yarayan araçlardır. Diğer bir karşı balküpü yazılımı ise Nessus'tur. Bu da uzak sistemde balküpü olup olmadığını tespit etmek için sistemi analiz eden bir yazılımdır. Ayrıca metasploit modülünde bulunan karşı balküpü araçlarından olan detect_kippo aracı kullanılarak ilgili testler gerçekleştirilebilir.

Savunma bakış açısı ile balküpü sistemlerinin tasarlanması için dikkat edilmesi gereken hususlar yine aynı şekilde saldırgan bakış açısı için de geçerlidir. Benzer şekilde aşağıdaki hususlara dikkat edilmesi gerekmektedir:

- Açık portlar, çalışan servisler, uygulamalar kontrol edilir ve bariz bir zafiyet varsa diğer sistemler ile karşılaştırılır. Buna göre balküpü kestirimi yapılır ve uygun karşı balküpü sistemi ve tekniği denenir.
- IP adresi, makine isimleri, alan adları ve kullanıcı isimleri gibi diğer makinelerle karşılaştırmalar yapılır.

Benzer karşılaştırmalar yapılarak ilgili makinelerin sistem ile entegrasyonu incelenir. Bu sayede ilk aşama olan balküpü şüphesi oluşturulabilir. Şüphenin oluşması ile geri kalan aşamalar hızlı bir şekilde gelişir. Balküplerindeki amaç saldırganı şüphelendirmemek olduğu için tüm ayrıntılara dikkat edilmelidir.

5. SONUÇ

Bu çalışmanın amacı balküplerinin kurumsal ağ sistemlerindeki önemini vurgulamak ve saldırgan/savunan taraf bakış açısının değerlendirilerek balküplerinin geliştirilmesini sağlamaktır. Saldırıları tespit amaçlı birçok sistem bulunmaktadır. Ancak balküplerinin çeşitli varyasyonları bu tespit verilerini zenginleştirmekte ve saldırganın enerjisini boşa harcamasını sağlamaktadır. Bu çalışmada karşı balküpü sistemleri kullanılarak tavsiye edilen adımlar uygulanmadan entegre edilen balküplerinin nasıl kolayca tespit edilebildiği gösterilmiştir. Ayrıca balküpleri saldırı ve savunma bakış açısı ile incelenerek, literatür ve tecrübelerden yola çıkılarak bir takım tavsiye niteliğinde değerlendirmelerde bulunulmuştur.

Günümüzde teknolojinin çeşitlenmesi ve gelişmesi ile birçok farklı alan oluşmaktadır. Benzer adımlar ve teknolojiler kullanılarak yeni teknolojilere karşı gerçekleştirilmesi muhtemel saldırılar için önceden önlemler alınabilir. Bundan sonra yapılacak çalışmalarda, farklı saldırılar için balküpü sistemleri geliştirilebilir ve geliştirilen bu sistemler çeşitli senaryolar üzerinde test edilebilir.

Yazarların Katkısı

Yazarların makaleye katkıları eşit orandadır. Bu çalışmada Muhammed Sadık KARABAY fikir, araştırma, kaynak taraması, değerlendirme, analiz, bilgisayar ortamında testlerin gerçekleştirilmesi ve makalenin yazımı konusunda katkıda bulunmuştur. Can EYÜPOĞLU fikir, eleştiri, danışmanlık, yazım dili, araştırma, kaynak taraması, makalenin yazımı ve değerlendirilmesi 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

Al-Jameel, S., & Alanazi, A. A. (2021). Honeypots Tools Study and Analysis. *International Journal of Computer Science & Network Security*, 21(1), 162-173.

Amal, M. R., & Venkadesh, P. (2023). H-Doctor: Honeypot based firewall tuning for attack prevention. *Measurement: Sensors*, *25*, 100664.

Bagyalakshmi, G., Rajkumar, G., Arunkumar, N., Easwaran, M., Narasimhan, K., Elamaran, V., & Ramirez-Gonzalez, G. (2018). Network vulnerability analysis on brain signal/image databases using Nmap and Wireshark tools. *IEEE Access*, 6, 57144-57151.

Borkar, A., Salunke, A., Barabde, A., & Karlekar, N. P. (2011, February, 25-26). *Honeypot: a survey of technologies, tools and deployment.* Proceedings of the International Conference & Workshop on Emerging Trends in Technology, India, 1357-1357.

Bringer, M. L., Chelmecki, C. A., & Fujinoki, H. (2012). *A survey: Recent advances and future trends in honeypot research.* International Journal of Computer Network and Information Security, 4(10), 63-75.

Campbell, R. M., Padayachee, K., & Masombuka, T. (2015, December, 14-16). *A survey of honeypot research: Trends and opportunities.* In 10th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 208-212.

Chen, P. T., Laih, C. S., Pouget, F., & Dacier, M. (2005, November, 07-09). *Comparative survey of local honeypot sensors to assist network forensics.* In First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05), IEEE, 120-132.

Dalamagkas, C., Sarigiannidis, P., Ioannidis, D., Iturbe, E., Nikolis, O., Ramos, F., ... & Tzovaras, D. (2019, June, 24-28). *A survey on honeypots, honeynets and their applications on smart grid.* In 2019 IEEE Conference on Network Softwarization (NetSoft), IEEE, 93-100.

Denis, M., Zena, C., & Hayajneh, T. (2016, April, 29-29). *Penetration testing: Concepts, attack methods, and defense strategies.* In 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), IEEE, 1-6.

Fan, W., Du, Z., Fernández, D., & Villagra, V. A. (2017). Enabling an anatomic view to investigate honeypot systems: A survey. *IEEE Systems Journal*, 12(4), 3906-3919.

Grimes, R. A. (2005). Honeyd Configuration. Honeypots for Windows. *Apress Berkeley*, CA.

Hong-Xia, L., Pu, W., Jian, Z., & Xiao-Qiong, Y. (2010, May, 7-9). *Exploration on the connotation of management honeypot.* In 2010 International Conference on E-Business and E-Government, IEEE, 1152-1155.

Nawrocki, M., Wählisch, M., Schmidt, T. C., Keil, C., & Schönfelder, J. (2016). A survey on honeypot software and data analysis, *arXiv preprint arXiv:1608.06249*.

Ng, C. K., Pan, L., & Xiang, Y. (2018). Honeypot frameworks and their applications: a new framework. *Springer*, Singapore.

Perevozchikov, V. A., Shaymardanov, T. A., & Chugunkov, I. V. (2017, February, 1-3). *New techniques of malware detection using FTP Honeypot systems.* In 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), IEEE, 204-207.

Priya, V. D., & Chakkaravarthy, S. S. (2023). Containerized cloud-based honeypot deception for tracking attackers. *Scientific Reports*, 13(1), 1437.

Sembiring, I. (2016, October, 19-20). *Implementation of honeypot to detect and prevent distributed denial of service attack.* In 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), IEEE, 345-350.

Sochor, T., & Zuzcak, M. (2014, June, 23-27). *Study of internet threats and attack methods using honeypots and honeynets*. In International Conference on Computer Networks, Springer, Cham, 118-127.

Uitto, J., Rauti, S., Laurén, S., & Leppänen, V. (2017, April, 04-06). *A survey on anti-honeypot and anti-introspection methods*. In World Conference on Information Systems and Technologie, Springer, Cham, 125-134.

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), 127.

Zimmerman, C. (2014). Ten Strategies of a World-Class Cybersecurity Operations Centre. *The Mitre Corporation*, Ukrainian.