Proje Raporu

Sanallaştırmada Güvenlik Açıkları, Tehditleri ve Bunların Çözümleri

Mert Doğukan Soyer

12 Ocak 2021

İçindekiler

1.Giriş 1
2.Sanallaştırma Tarihi 1
3.Sanallaştırma Teknolojileri 2
3.1. Hipervizör Tabanlı Sanallaştırma 2
3.1.1 Hipervizör Tip 1 2
3.1.2. Hipervizör Tip 2 Tabanlı Sanallaştırma 3
3.2. Konteyner Tabanlı Sanallaştırma 4
4. Sanallaştırılmış Sistemlerin Özellik ve Avantajları 5
4.1. Kaynak Kullanımına Yönelik Özellikleri Ve Avantajları 5
4.2. Kaynak Yönetimindeki Özellikleri ve Avantajları 6
5.Sanallaştırma Türleri 7
5.1. Sunucu sanallaştırma 7
5.2. Depolama Sanallaştırma 7
5.3. Ağ Sanallaştırma 8
5.4. Masaüstü ve Dizüstü Sanallaştırma 8
5.5. Uygulama Sanallaştırma 8
6. Sanallaştırmada Güvenlik 8

6.1. VM Sprawl 9
6.1.1. VM Spwarl'a Karşı Önlemler 9
6.2. VM Kaçışı (VM Escape) 10
6.2.1. VM Kaçışına Karşı Önlemler 10
6.3. Çapraz VM Yan Kanal Atakları (Cross VM Side Channel Attacks) 10
6.3.1. Çapraz VM Yan Kanal Ataklarına Karşı Önlemer 11
6.4. Güvensiz VM Göçü 11
6.4.1. Güvensiz VM Göçüne Karşı Önlemler 12
6.5. Hyperjacking 12
6.5.1. Hyperjacking'e Karşı Önlemler 13
6.6. Kötücül VM Atakları (MaliciousVM Attacks) 13
6.6.1. Kötücül VM Ataklarna Karşı Önlemler 13
6.7. VM Geri Alma Saldırısı (VM Rollback Attack) 13
6.7.1. VM Geri Alma Saldırısına Karşı Önlemler 14
7.Vargılar 14
Kaynakça 16

1.Giriş

Günümüzün en çok kullanılan ve her geçen gün rağbetin arttığı bir teknoloji olan sanallaştırma kelimesini bir çok yerde bir çok farklı kullanım şekilerinde duymak mümkün. Bunun sebebi sanallaştırma teriminin bir çok anlamı ve sanallaştırmanın farklı yöntemleri olmasıdır. Temel olarak sanallaştırmayı mevcut olan bir fiziksel bilgisayarın veya fiziksel donanımın, sanallaştırma teknolojisinin yardımıyla daha verimli kullanılmasını olanak veren ve aynı zamanda bir çok yazılımsal ve donanımsal gereksinimleri ortadan kaldıran bir yazılım çözümüdür. Daha basit ve yalın bir anlatımla, sanallaştırma fiziksel kaynakların farklı yöntemler kullanılarak işletim sistemleri ve kullanıcılardan soyutlanması olarakta açıklanabilir.

Geleneksel yazılımla karşılaştırıldığında sanallaştırma maliyette büyük avantajlar sunmaktadır. Sanallaştırma teknolojisi ile mevcut bir bilgisayara ait donanımsal ve yazılımsal kaynakları soyutlayarak, başka bilgisayarlarla paylaştırabilir. Bu işlem ile birlikte ana bilgisayarda kullanılan donanımlar (ram, ekran kartı, harddisk vb.) ve yazılımlar başka bilgisayarlara soyut olarak paylaştırır ve bu şekilde maliyet olarak büyük tasarruflar sunmaktadır. Bunun yanında sanallaştırma teknolojisinden faydalanılmasıyla mevcut eski donanımların daha uzun süre kullanımı mümkündür. 2002 yılında IBM firması tarafından yapılan bir araştırmanın sonuçlarına göre; dünya üzerindeki birçok şirketin sunucu bilgisayarlarının yıl içerisinde çoğu zaman boş kaldığı, masaüstü bilgisayar kullanıcılarının da, mevcut sistemlerini %5 den daha az kapasite ile kullandıkları ortaya çıkmıştır [1]. Bunun yanında kullandığı alt yapı sistemi , erişelebilir olması gibi bir çok avantajı bulunmaktadır.

2.Sanallaştırma Tarihi

Bilgisayar teknolojisi ortaya çıktığı günden beri kaynakların daha verimli nasıl kullanılabileceği daima gündemdeydi. Bu sebeple sanallaştırma kavramının ortaya çıkması bir hayli eskidir. 1960'ın başlarında işletim sistemlerinde toplu işlem (batch processing) teknolojisi ve ardından 1967 yıllarından sonra zaman paylaşımı (time sharing) teknolojisi ile sanallaştırmanın temelleri atılmış oldu. Sanallaştırma kavramının kökenin IBN'in zaman paylaşımı (time sharing) teknolojisi hem kullanıcıların hem de paylaştıkları dönemin pahalı bilgisayar kaynaklarının verimliliğini arttırmayı amaçlayan, geniş bir kullanıcı grubu arasındaki bilgisayar kaynaklarının paylaştırılmasıdır [2]. Bu yaklaşım bilgisayar teknolojisinine büyük bir atılım anlamına geliyordu. Bilgisayar teknolojisinde çığır açan bu kavram kurum ve kişiler için bir bilgisayara sahip olmadan kullanmayı mümkün hale getirdi. Zaten pahalı olan donanımsal maliyetler bu yöntemle sanal makineler ilk olarak 1972 yılında IBM tarafından ana bilgisayarlarında ticari olarak kullanılmaya başlandı [3]. Bu tarihten itibaren sanallaştırma teknolojisi sunduğu maliyet avantajlarından ötürü kullanımında artış sağlandı.

Gerek o dönemde donanım maliyetlerinin çok yüksek olması, gerekse de kişisel bilgisayar kullanımın oranının çok düşük olmasından ötürü, 1970'li yıllarda sanallaştırma teknolojisi üzerine yoğun çalışmalar yapılmıştır. Bu durum 1980 ve özellikle 1990'lı yıllarda yavaş yavaş tersine dönmeye başlamıştır. 1980 ve 1990 yıllarda donanım maliyetlerinde yaşanan ucuzlama ve kişisel bilgisayar kullanımında olan artış sanallaştırma teknolojisinin gündemden düşmesine, eskisi kadar geliştirilmemesine ortam hazırlamıştır.

1990'lı senelerin ortalarına doğru Stanford Üniversitesinde bir araştırma projesi olarak tekrardan ele alınan sanal makine teknolojisi, Vmware şirketi ile tekrardan gündeme gelip yeniden geliştirmeler başlamıştır [4]. Bu süreçten sonra tekrardan gündem olmaya başlayan sanallaştırma teknolojisi alanına bir çok şirket girmiş ve bu alanda yatırımlar artmıştır. Bu teknoloji firmalarının aralarında XenSource, Swsoft, Microsoft, Oracle bir çok teknoloji firması bulunmaktadır.

Günümüzde veri merkezleri, fiziksel donanımın soyutlanması CPU'lar, bellekler, diskler , dosya depolama, uygulamalar gibi büyük toplu kaynak havuzları oluşturmak için sanallaştırma teknikleri kullaılmaktadır. Teknoloji ve teknoloji kullanımının günümüzde değişmesine rağmen, sanallaştırmanın temel prensip ve mantığı aynıdır; bir kaynağın aynı anda birden fazla bağımsız sistemin çalıştırabilmesini sağlamaktır.

Sanallaştırma teknolojisi ve sanal makine hipervizör tabanlı sanallaştırma olarak bilinmektedir. Günümüzde konteyner tabanlı sanallaştırma olarak bilinen farklı ve daha performanslı bir teknoloji geliştirilmiştir.

3.Sanallaştırma Teknolojileri

Sannallaştırma teknolojileri sanallaştırma katmanının uygulandığı katmana ve kullanılan teknolojiye göre ikiye ayrılmaktadır :

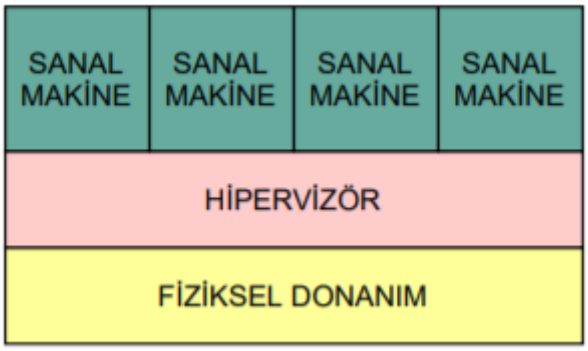
3.1. Hipervizör Tabanlı Sanallaştırma

Hipervizör tabanlı sanallaştırma , Hipervizör Tip 1 ve Hipervizör Tip 2 olarak iki farklı çeşitte uygulanmaktadır. Tip 1 ve Tip 2 sanallaştırmada farkı yaratan konu , sanallaştırma yazılımı olan hipervizör katmanının nerede olduğudur. Tip 1 ' de sanallaştırma yazılımı fiziksel kaynaklara doğrudan erişim sağlarken , Tip 2 'de bu mümkün değildir.

3.1.1 Hipervizör Tip 1

Tip 1 hipervizör tabanlı sanallaştırmada arada herhangi bir işletim sistemi katmanı olmadan doğrudan donanıma kurulmaktadır. Donanım üzerinede çalışan hipervizör yazılımı sanal

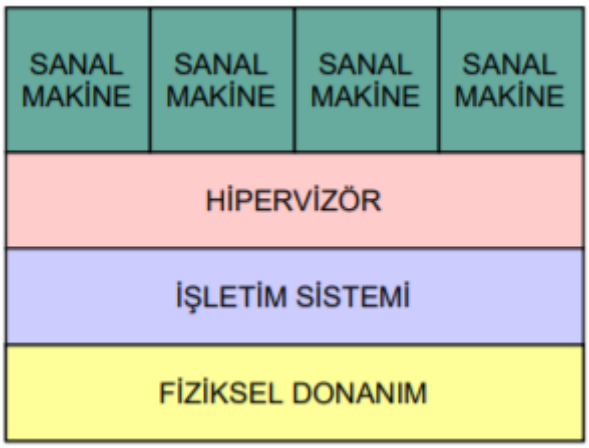
makineleri kendi üzerinde barındırır. Kaynakların sanallaştırılması doğrudan bu katmanda yapılır. Fiziksel bir sunucu üzerinde çalışan hipervizör yazılımı ile birden fazla işletim sistemi kurulabilir ve yönetimi sağlanabilir [5]. Örnek olarak ESX Server ve Xen verilebilir. Hipervizör Tip 1 aynı zamanda "Bare Metal" olarak da adlandırılmaktadır. Tip 1 hipervizör tabanlı sanallaştırma örneği Şekil 1 ' de gösterilmiştir.



Şekil 1. Hipervizör Tip 1 Tabanlı Sanallaştırma

3.1.2. Hipervizör Tip 2 Tabanlı Sanallaştırma

Tip 2 'de hipervizör uygulama gibi doğrudan işletim sisteminin üzerine kurulur. Bu şekilde hipervizör fiziksel kaynaklara işletim sistemi üzerinden erişir. Kurulumu tip 1' e göre daha kolaydır. Performans kaybına neden olmasından ötürü tip 2 hipervizör tabanlı sanallaştırma çoğunlukla kişisel kullanım veya test amaçlı kullanılmaktadır. VmareWorkstation , Hyper V , Oracle Virtualbox tip 2 sanallaştırma örnekleridir. Tip 2 hipervizör tabanlı sanallaştırma örneği Şekil 2 ' de gösterilmiştir.



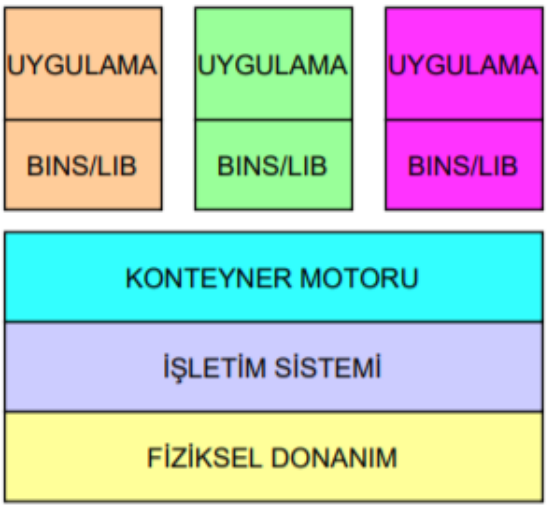
Şekil 2. Hipervizör Tip 2 Tabanlı Sanallaştırma

3.2. Konteyner Tabanlı Sanallaştırma

Konteyner tabanlı sanallaştırma sistemi günümüzde sıklıkla kullanılan ve hipervizör tabanlı sanallaştırmaya göre daha performanslı bir teknolojidir. Konteyner tabanlı sanallaştırmada hipervizör katmanının yerinde host işletim sistemi ve bu işletim sisteminin üzerinde konteyner motoru bulunur. Hipervizör tabanlı sanallaştırmaya göre daha hafif bir sanallaştırma sistemidir. Konteyner içinde çalışan uygulamalar ve işletim sistemleri kurulu olduğu sistemin çekirdek sistemini ortak kullanmaktadır.

Günümüzde en popüler konteyner mimarisi olarak kullanılan Docker olsa da konteyner tabanlı sanallaştırmanın atası 2008 yılında ilk sürümü çıkan Linux Containerdır. Yani aslında hipervizör tabanlı sanallaştırma kadar eskiye dayanan LXC geliştirilmiş , manuel olarak yapılan bir çok işlem ustaca otomatikleştirilmiş ve kullanım kolaylığının artmasıyla yaygınlığı da artmıştır.

Endüstride en çok kullanılan sanallaştırma teknolojilerine örnek olarak LinuxVServer, OpenVZ, LXC, Solaris Konteynerleri, FreeBSD Jails ve Docker örnek olarak verilebilir.



Şekil 3. Konteyner Tabanlı Sanallaştırma

4. Sanallaştırılmış Sistemlerin Özellik ve Avantajları

Silberschatz , Galvin ve Gagne (2018 , 704) sanallaştırmanın avantajlarını aşağıdaki gibi sıralamaktadır [3] ;

4.1. Kaynak Kullanımına Yönelik Özellikleri Ve Avantajları

Sanallaştırmanın en önemli avantajı sanal makinaların birbirinden bağımsız oluşu ve birbirinden korunmalarıdır. Güvenli olmayan, ya da risk taşıyan uygulamaları oluşturacağımız sanal makineler üzerinde birbirinden izole olarak çalıştırarak daha güvenli bir ortam oluşturulabilir. Eğer her hangi bir sanal makinaya virus girmiş olursa bu virüsten diğer makinalar etkilenmez çünkü herbir sanal makina hemen hemen diğerlerinden tamamen izoledir ve neredeyse hemen hemen bulaşma sorunu yaşamaz. Sanal makinalardaki bu izolasyonun olası dezavantajı ise kaynakların paylaşımını önleyebileceğidir. Bu paylaşımı sağlamanın nasıl olacağına yönelik iki yaklaşım mevcuttur: Birincisi, dosya system birimi aracılığıyla dosyaları paylaşmaktır. Ikincisi sanal makinaların bir networkunun tanımlanmasıdır ki böylece bilgiler sanal iletişim ağı üzerinden gönderilebilir. Bu ağ fiziksel haberleşme sistemlerinden modellenmiş ancak, yazılıma uygulanmıştır. Şüphesiz ki sanal makina yönetimi (virtual machine manager -VMM) ağındaki uygulayıcılara fiziksel bağlantının kurulmasına fiziksel bağlantı yoluyla olanak tanımaktadır.

Sanallaştırma uygulamalarının en yaygın bir özelliği, işleyen bir sanallaştırma makinasının askıya alma veya dondurma yeteneğidir. Birçok işletim sistemi sürece yönelik temel özelliğe sahiptir fakat sanal makina yönetimi bir adım daha ileriye giderek misafir kullanıcılarına kopya alma ve anlık görüntü alma olanağı sağlar. Bu kopyalama olanağı yeni bir sanal makina oluşturma veya bir makinadan sanal bir makinaya geçme olanağı tanır. Bu yetenek sanal ortamda iyi bir avantaj olanağı sunar.

Normal koşullarda işletim sistemleri büyük ve karmaşık sistemlerdir bu sistemlerin birinde meydana gelen değişiklik başka bir kısımda belirsiz hataların yaşanmasına neden olabilir bu nedenle işletim sistemlerinde değişim zor bir iştir. Sanal makinalar bu değişimi kolaylaştırır. Tabii ki, işletim sistemi tüm makineyi çalıştırır ve kontrol eder, bu nedenle değişiklikler yapılırken ve test edilirken sistem durdurulmalı ve kullanımdan kaldırılmalıdır. Bu döneme genellikle sistem geliştirme süresi denir. System geliştirme zamanı kullanımcıları etkilemeyecek şekilde uygun bir zamana göre planlanmalıdır. Eğer elinizde bir sanal makine sistemi varsa bu sorunun çoğu ortadan kaldırabilir. Sistem programcılarına kendi sanal makineleri verilir ve sistem geliştirme fiziksel bir makine yerine sanal makine üzerinde yapılır. Böylece kullanıcılar da etkilenmemiş olur.

Sanal makinelerin geliştiriciler için bir başka avantajı ise işletim sistemlerinin geliştiricinin iş istasyonunda eşzamanlı olarak çalışmasıdır ki bu durum geliştiriciler için sanal makinaların bir başka avantajıdır. Eğer iş ortamı/çalışma istasyonu sanallaştırılmışsa, çeşitli ortamlarda programların hızlı bir şekilde taşınmasına ve test edilmesine olanak tanır. Ayrıca, bir programın birden çok sürümü, her biri

kendi izole işletim sisteminde tek bir sistem içinde çalışabilir. Bu durum sanal makinaların sahip olduğu ve program geliştiricilere sunduğu önemli bir avantajdır. Sanal makinaların sunduğu bu avantaj, kalite güvence mühendislerinin her ortam için bir bilgisayar satın almadan, çalıştırmadan ve bakımını yapmadan uygulamalarını birden çok ortamda test edebilmelerine olanak sağlar.

Üretim veri merkezi kullanımında sanal makinelerin önemli bir avantajı, iki veya daha fazla ayrı sistemi alıp tek bir sistemdeki sanal makinelerde çalıştırmayı içeren sistem konsolidasyonudur. Bu avantajıyla sanal makinalar fizikselden sanala dönüşümler yoluyla kaynak optimizasyonuyla sonuçlanır, çünkü çok az kullanılan birçok sistem, tek bir sistemde birleştirilebilir ve bu system rahatlıkla yoğun bir şekilde kullanılabilir

Bir sanal ortam, her biri 20 sanal sunucu çalıştıran 100 fiziksel sunucu içerebilir. Sanallaştırma olmadan, 2.000 sunucu birkaç sistem yöneticisine ihtiyaç duyacaktır. Sanallaştırma ve araçlarıyla aynı iş bir veya iki yönetici tarafından yönetilebilir. Bu şekilde VMM'nin bir parçası olan yönetim araçları, sistem yöneticilerinin normalde yapabileceklerinden çok daha fazla sistemi yönetmelerine olanak tanır.

İş yükünü, daha az sayıda fiziksel sunucu üzerinde birleştirerek, sunucu sayısından ve buna bağlı olarak, veri merkezlerinde kullanılan alandan, elektrik ve soğutma gibi giderlerden tasarruf etmemizi sağlar. Aynı zamanda, fiziksel sunucu yerine sanallaştırımış sistem kullanılması sistemin, bakım, onarım masraflarının yanısıra yönetimsel masrafların da azalmasını sağlamaktadır.

4.2. Kaynak Yönetimindeki Özellikleri ve Avantajları

Bir sunucu aşırı yüklenmişse, bazi VMM'ler, çalışan bir konuğun çalışmasını veya etkin ağ bağlantılarını kesintiye uğratmadan bir fiziksel sunucudan diğerine taşıyan canlı geçiş özelliği içerir. Bu dinamik geçiş, konuğu kesintiye uğratmadan ana bilgisayardaki kaynakları serbest bırakabileceğini ifade etmektedir. Aynı zamanda, ana bilgisayar donanımının onarılması veya yükseltilmesi gerektiğinde, işlemde bir kesinti olmadan ve kullanıcılar kesintiye uğramadan konuklar başka sunuculara taşınabilir, tahliye edilen ana bilgisayar korunabilir ve ardından konuklar geri taşınabilir. Bu durum sanal makinalara özgüdür ve kullanıcılara önemli bir avantaj sağlar.

Çeşitli uygulamaların sanal bir makinaya sonradan yüklenip kullanılması yerine sanal bir makinede ayarlanmış ve özelleştirilmiş bir işletim sistemine önceden yüklenebilir. Bu yöntem, uygulama geliştiricileri için çeşitli avantajlar sunacaktır. Uygulama yönetimi daha kolay hale gelir, daha az ayarlama olur ve uygulamanın teknik desteği daha kolay olacaktır. Sistem yöneticileri de ortamı daha kolay yönetebilir. Kurulum basit olacaktır ve uygulamayı başka bir sisteme yeniden dağıtmak, normal kaldırma ve yeniden yükleme adımlarından çok daha kolay olacaktır. Eğer Sanal makinelerin formatı, herhangi bir sanal makinenin herhangi bir sanallaştırma platformunda çalışması için standartlaştırılsa yaygın kullanım olanağı bulacaktır. Sanal makinaların bu hizmeti sunması için yani, yeni uygulamaların

sisteme yerleştirilmesi için "Açık Sanal Makine Formatı"na dönüşmesi gerekir. Açık sanal makina formatı yoluyla hem standardizasyon sağlanır hem sanal makine formatlarını birleştirme sağlanır.

Sanallaştırma, bilgisayar tesisi uygulaması, yönetimi ve izlemesindeki diğer birçok ilerlemenin temelini atmıştır. Örneğin, bulut bilgi işlem, CPU, bellek ve G / Ç gibi kaynakların İnternet teknolojilerini kullanan müşterilere hizmet olarak sunulduğu sanallaştırma ile mümkün hale gelir. çoklu oyun ortami, fotoğraf paylaşimi ve diğer web tabanlı sanal sosyal platfomlar gibi birçok uygulama internet üzerinden erişilebilecek belirli bir işletim sistemini çalıştıran binlerce sanallaştırımış makinalar oluşturulabilmektedir (Bir program, API'leri kullanarak bir bulut bilişim tesisine hitap eder).

Sanal makinalar bize evimizden veya bir başka uzak noktadan masa üstü veya dizüstü bilgisayarlarımızı kullanarak uzak veri merkezlerine uzaktan bağlanmamızı ve uygulamalarına yerelmiş gibi erişilmesine olanak sağlamaktadır. Kullanıcının sitesindeki yerel disklerde hiçbir veri depolanmadığından bu uygulama güvenliği artırabilir. Kullanıcının bilgi işlem kaynağının maliyeti de düşebilir. Kullanıcının ağ bağlantısı, CPU ve bir miktar belleğe sahip olması gerekir, ancak bu sistem bileşenlerinin yapması gereken tek şey, konuğun uzaktan çalışırken (RDP gibi bir protokol aracılığıyla) bir görüntüsünü görüntülemektir. Bu nedenle verilere ulaşmak oldukça ucuz ve kolayca gerçekleşebilmektedir.

5.Sanallaştırma Türleri

Sanallaştırma teriminin bir çok anlamı ve sanallaştırmanın farklı yöntemleri bulunmaktadır. Her sanallaştırma türünün kendine ait kullanım alanı ve kullanım özellikleri vardır. Kullanıcıların sıklıkla kullandığı sanallaştırma türleri arasında; ağ sanallaştırması, sunucu sanallaştırması, işletim sistemi (Operating System – OS) sanallaştırması ve depolama alanı sanallaştırması yer almaktadır.

5.1. Sunucu sanallaştırma

Sunucu sanallaştırma ile birden çok sunucunun sanallaştırılarak daha az bir miktarda sunucu üzerinden çalışmasını sağlayan bir sanallaştırma türüdür. Örnek olarak 10 fiziksel sunucu sanallaştırılarak 2 sunucu üzerinde sanal olarak çalışması sağlanır.

5.2. Depolama Sanallaştırma

Son kullanıcının sıklıkla kullandığı depolama sanallaştırma ise verilerin sanallaştırılmış bir ortamda tutulmasını sağlar.

5.3. Ağ Sanallaştırma

Ağ sanallaştırmanın da mantığı temel sanallaştırma mantığı ile aynıdır. Daha az ekipman ile maksimum verim. Bu bağlamda ağ sanallaştırmada da bileşenlerin azaltılıp bir fiziksel ağ bağlantısı yapılmış gibi çalışmasını sağlar. Daha az ekipman ile çok daha fazla sanal ağ kurup çalışmasını sağlanır.

5.4. Masaüstü ve Dizüstü Sanallaştırma

Veri merkezlerine taşınarak sanallaştırılan bu cihazlara kullanıcıların ağ ile bağlanması ve bu sistemleri kullanmasına olanak tanır.

5.5. Uygulama Sanallaştırma

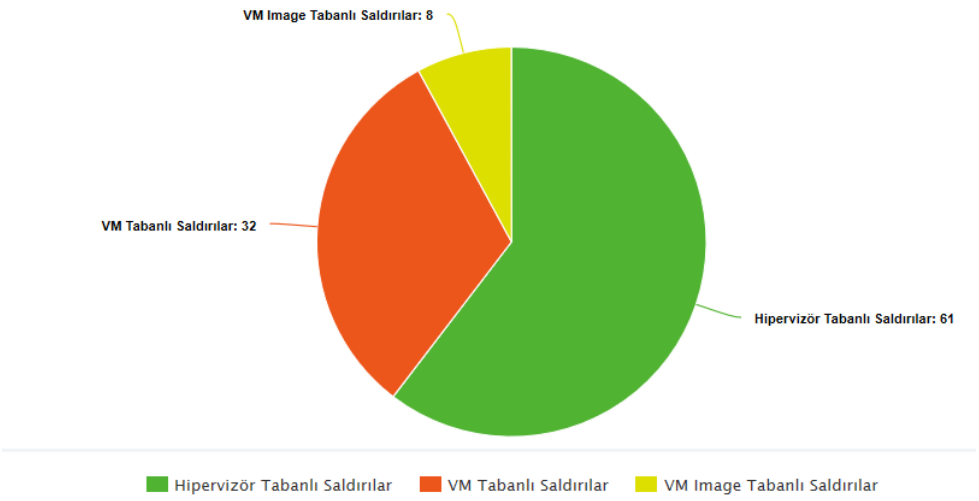
Kendi bilgisayarınıza kurulmadan, bir sanal makine ve sunucu yardımıyla sanki sizin bilgisayarınızda çalıştırılıyormuşcasına çalışması ve kullanılmasıdır. Ciddi performans gereksinimi isteyen uygulamalarda özellikle tercih edilmektedir

6. Sanallaştırmada Güvenlik

Büyük avantajlarının yanında sanallaştırma teknolojilerinin getirdiği bazı güvenlik açıkları ve tehditleri de mevcuttur. Sanallaştırma sistemlerinde , sanallaştırmayı uygulamamızı sağlayan yazılım katmanı ve bazen de kullanılan donanımlar güvenlik tehditlerine maruz kalabilir ve saldırılara uğrayabilir.

Sanallaştırma işleminin ardından güvenlik altına alınması gereken yeni bir katman ortaya çıktığından ötürü , saldırılar bu katmanı kullanarak gerçekleşebilir. Saldırganlar bu katmanı kullanarak sisteme sızabilir ve zarar verebilir. Sanal makinelerin güvenliği en az fiziksel makineler kadar önemlidir. Aynı zamanda bu iki tarafta da oluşabilecek hatalar birbirini etkilemesi kaçınılmaz olacaktır. Sanallaştırmanın oluşturulma mantığından ötürü giriş noktalarının artmasından kaynaklı ve oluşan ara bağlantılar ortaya bir kamaşıklık çıkardığından dolayı güvenliği sağlamak büyük bir sorun ve bu sorunların oluşmamasını veyahut oluşan sorunları çözmek büyük önem arz etmektedir.

Sanallaştırmada güvenliği sağlamak için öncelikle mevcut güvenlik tehditlerini tanımlamak ve bunların üzerine yoğunlaşmak gerekir. Son yıllarda sanallaştırma üzerine bir çok tehdit unsuru vardır. Bunlar hipervizör tabanlı saldırılar , sanal makine tabanlı saldırılar ve sanal makine image saldıları (VM Image). Bunların arasında en çok saldırı yüzdesi sırasıyla hipervizör tabanlı saldırılar , VM (virtıal machine) tabanlı saldırılar ve VM Imaj tabanlı saldırılar olarak sıralanmaktadır. Şekil 4. ‘de bu saldırıların yüzdelik halleri gösterilmektedir.



Şekil 4. Sanal makinlerde en çok görülen saldırı türleri

Aşağıda sanallaştırmada sıklıkla görülen görülen güvenlik riskleri ve tehdit unsurları ele alınmıştır. Ayrıca , her bir risk ve tehditi önleyici çözüm uygulama örnek ve önerileri sunulmuştur.

6.1. VM Sprawl

Bir ağda kontrol edilemeyecek ve yönetilemeyecek derecede fazla sanal makine oluşturulması sonucu ortaya çıkan bir durumdur. Bu VM'ler ağın verimliliğinin kaybolmasına sebep olurlar. Oluşan bu durum sanallaştırmanın mantığı ve prensibine aykırı olup, kontrol mekanizması kurulmazsa yaşanılması kaçınılmaz olan bir durumdur. Bu şekilde yayılım olması durumunda oluşan bu sanal makinelerin kontrol ve güvenlik altına alınması mümkün olmayacaktır.

6.1.1. VM Spwarl'a Karşı Önlemler

Bu durumun oluşmasının en büyük etmeni , artık ihtiyaç kalmayan sanal makinenin çalışmasına devam ettirilmesidir. Sanal makineler için bir yaşam döngüsü planı oluşturulmalıdır. Gereksiz ve süresi geçen bir sanal makinenin kaynakları tüketmesini engellemek sistem kaynaklarının hem verimsiz yere harcanmamasına hemde takip edilemeyen sanal makinelerin ortada kalıp güvenlik riskleri oluşturmasına sebep olur.

Sanal makine görüntülerinin oluşturulmasını , depolanmasını ve kullanımı kontrol altına alınmalıdır. Yeni yapılacak eklemeler yalnızca gerektiği durumlarda uygulanmalıdır. Her bir sanal makine ile ilişkili ağ bağlantıları için en uygun güvenlik kontrollerinin sınıflandırması ve oluşturulan yol haritasının uygulanması riski azaltacaktır.

6.2. VM Kaçışı (VM Escape)

Sanal makineler ana bilgisayar ile VM (virtual machine) arasında güçlü izolasyonu destekleme amacıyla tasarlanmıştır. Sanal makinelerin de içinde işletim sistemleri çalışmaktadır ve bu işletim sistemlerinde yer alan açıklar saldırganlar için uygun platformun sağlanmasına yardımcı olmaktadır.

VM kaçışı , art niyetli bir kullanıcının veya oluşturulan bir sanal makinenin , sanal makine mönitörü (VMM) veyahut hipervizör kontrolünden kurtulduğu durumlarda oluşur.

Bu tarz art niyetli bir program çalıştırılması mümkün kılınırsa, VM izole alanda olan sınırlardan ayrılıp doğrudan VMM katmanını atlar ve işletim sistemiyle iletişim kurar. Gerçekleşen bu durum VM Escape olarak adlandırılmaktadır. VMM katmanının atlanıp doğrudan işletim sistemiyle iletişim kurulması saldırganın ana makine erişim elde etmesine ve doğrudan başka saldırılar gerçekleştirmesine olanak tanıyacaktır.

6.2.1. VM Kaçışına Karşı Önlemler

VM Kaçışını engellemek için bir kaç yöntem kullanılabilir. Hipervizör akış kontrol mekanizmasını sağlayan ve bütünlük oluşturan bir kavramdır.

Hipervizör kavramında asıl hedef , yazmaya karşı korumalı olan bellek sayfalarının değiştirilmesine olanak tanımayan “bellek kilidi” ve kontrol verilerini işaretçi dizine dönüştüren “kısıtlı indeksleme” olmak üzere Hipervizör Tip 1 korunması Hypersafe yöntemi ile sağlanabilir [6].

Kullanılacak olan güvenlir bulut bilişim platformu aynı zamanda güvenilir sanal makine mönitörü ve güvenilir bir koordinatörden oluşan TCCP (Tursted Cloud Computing Platform) , sağlayacıların hepsine kapalı kutu çalışma imkanı sağlar ve sanal makineleri başlatmadan önce ortam güvenliğini belirlemeye izin verir .

VM Kaçışı ile mücadele etme konusunda önem arz eden bir diğer kısım ise güvenilir sanal veri merkezidir. Bu method bulut çevresinde bütünlüğü ve izalasyonu sağlamaktadır. Ortak amaçlar doğrultusunda kullanılan sanal makineleri , güvenilir sanal alanlar oluşturup iş yüklerine göre gruplandırıp iş yükleri arasında izalasyon sağlanmasını sağlar.

6.3. Çapraz VM Yan Kanal Atakları (Cross VM Side Channel Attacks)

Sanal makine taraflı kanal saldırıları , seçilmiş bir sanal makineyi kullanarak saldırganın sanal makine dönüşümünü gerçekleştirdiği ve seçilen sanal makinenin davranışını çıkarmak için işlemci kasalarını güçlendirdiği erişim odaklı bir saldırı yöntemidir. Çapraz VM yan kanal saldırılarında ,

kurban sanal makinenin kullanılarak aynı fiziksel donanım üzerinde saldırganın farklı bir sanal makine üzerinde bulunmasını gerektirir. Güvenlik ile ilgili hassas bilgileri kopyalamak veya sızdırmak için bir sistemde düşük bant genişliğini sonuna kadar kullanan Çapraz VM yan kanal saldırısı günümüz bilgisayar teknolojisine yönelik hassas ve dikkat edilmesi gereken bir tehdittir.

6.3.1. Çapraz VM Yan Kanal Ataklarına Karşı Önlemer

Azab ve arkadaşları literatürde önerilen çözümlerin donanım, istemci sanal makineleri ya da hipervizörler gibi yapılarda önemli değişimler gerektirdiği ve saldırı çeşitlerine özel geliştirilmiş yöntemler olduğunu öne sürerek bu çözümlerin genel olmadığını ve saldırının mutasyona uğramış sürümleri ile başa çıkılamayacağını belirtmiştir. Bu yüzden birlikte yaşayan bulutlardaki yan kanal saldırılarına genel bir çözüm olarak VM göçünü önererek kaynak verimli, ölçeklenebilir, gerçek zamanlı hareketli hedef savunmasını kullanan MIGRATE isimli bir konteyner yönetim çerçevesi geliştirmişlerdir. Önerilen çerçevenin farklı ana bilgisayarlar arasında Linux kapsayıcılarında bulunan bulut kiracı uygulamalarının etkili bir şekilde gerçek zamanlı olasılıksal rastgele göçlerini kullandığı belirtilmektedir. Göç süreci, konteyner içerisinde yapılan işleri kaydetmek için çalışan konteyneri kontrol ederek başlamaktadır ([7] akt: Aksakallı 2019).

Bu özellik mevcut hipervizörler tarafından varsayılan olarak etkin değildir. Çalışan uygulamaların kontrol noktasını etkinleştirmek için kullanılan kontrol işaretleme aracı, kullanılan dosyaların ve bellek içeriğinin anlık görüntüsünü alarak çalışan konteyner ve içerisindeki uygulamaları anlık olarak dondurmaktadır. Yapılan deneyler sonucunda saldırganın konteyner konumlarını önceden bilmemekle birlikte, göç sayısını artırmanın başarılı yan kanal saldırılarını hafiflettiği görülmüştür ([7] akt: Aksakallı 2019).

6.4. Güvensiz VM Göçü

Sanal makineler arasında donanım paylaşımı yapılması esnasında , bazı durumlarda yük dengesini sağlamak veya kurallara uymak için sanal makineler farklı platformlar arasında dolaşmaya zorlanır. Bu sürec VM Göçü olarak adlandırılır. Yaşanan bu durumda sanal makinelerin durum dosyalarını ağa açık bir duruma getirmektedir. Bu durum riskler barındırmakta ve bu durumdan yararlanmak isteyen bir saldırgan göç sırasında verilere illegal olarak erişebilir. Güvenli olmayan bir makineye sanal makine transferi gerçekleştirebilir ayrıca yaşanan bu durum Dos ataklarına yol açan birden fazla sanal makine oluşturabilir.

6.4.1. Güvensiz VM Göçüne Karşı Önlemler

Bu konu üzerine yapılan bir çok çalışma mevcuttur. Genel olarak uygulananması tavsiye edilen yöntemler şu şekildedir; Göç esnasında ve göç tamamlandıktan sonra gizliği koruma altına alan ve işlem bütünlüğünü destek olan güvenli bir göç çerçevesi uygulanmalıdır. Bu işlem uygulandığı taktirde şifreleme işlemlerinin katkısıyla kesintiler azalmaktadır. Sanal makinelerin güvenlik politikalarının özelleştirilmesi kapsamında güvensiz sanal makine göçü kontrol ve koruma altına alınmaktadır.

Önemli olarak değerlendirebilecek konuysa kimlik doğrulama işlemlerini de kapsayan güvenli sanal platformdur (VM-VTP). Bu güvenlik protokolü bu süreçler için önerilmektedir. Sistem başlangıçta iki tarafın karşılıklı olarak birbirini doğrulamasıyla başlar. Bu aşamadan sonra iletişim için güvenli oturum oluşturulmaktadır. Bu işlemlerin başarılı bir şekilde oluşmasının ardından sistemi kontrol etmek amacıyla kaynak kısmından uzak doğrulama ve onaylama yapılmalıdır. Kaynak bilgisayar ilk önce sanal makineyi güvenli sanal platform aracılığıyla (VM-VTP) askıya alır ve şifreler. Sonrasında hedef makineye aktarım işlemini gerçekleştirir.

6.5. Hyperjacking

Hyperjacking , bir bilgisayar korsanının bir sanal makine (VM) ana bilgisayarı içinde sanal ortamı oluşturan hiper yönetici üzerinde kötü niyetli kontrolü ele geçirdiği bir saldırıdır . Saldırının amacı, sanal makinelerin altındaki işletim sistemini hedeflemektir, böylece saldırganın programı çalışabilir ve üzerindeki VM'lerdeki uygulamalar, varlığından tamamen habersiz olur.

Hyperjacking, tüm sunucu sistemini yönetebilecek kötü niyetli, sahte bir hiper yönetici yüklemeyi içerir . Düzenli güvenlik önlemleri etkisiz kalmaktadır, çünkü işletim sistemi makinenin tehlikeye girdiğinin farkında olmadan bu saldırı ortaya çıkar. Hiperjacking işleminde, hypervisor özellikle gizli modda ve makinenin altında çalışır, tüm kurumun veya şirketin işleyişini etkileyebilecek bilgisayar sunucularının tespit edilmesini ve daha büyük olasılıkla erişilmesini zorlaştırır. Bilgisayar korsanı hypervisor'e erişim kazanırsa, bu sunucuya bağlı olan her şeyi değiştirilebilir ve saldırılar yapabilir. Hypervisor, hassas bilgilerin güvenliği ve korunması söz konusu olduğunda tek bir hata noktasını temsil eder.

Bir hiperjacking saldırısının başarılı olması için, bir saldırganın aşağıdaki yöntemlerle hiper denetleyicinin kontrolünü ele geçirmesi gerekir:

- Orijinal hipervizörün altına sahte bir hiper yönetici enjekte etmek
- Doğrudan orijinal hipervizörün kontrolünü elde etme
- Mevcut bir hiper yönetici üzerinde hileli bir hiper yönetici çalıştırma

6.5.1. Hyperjacking'e Karşı Önlemler

Hyperjacking ciddi bir sorun olmasına karşın alınacak basit önlemler bu durumu önlemeye yardımcı olmaktadır. İlk önce hipervizörün güvenlik yönetimi normal trafikten ayrılmalı ve ayrı tutulmalıdır. Konuk işletim sistemleri bu aşamada en çok dikkat edilmesi gereken hususların başında gelmektedir. Konuk işletim sistemlerinin hipervizöre erişimi tamamen kesilmelidir. Yönetimsel araçlar konuk işletim sisteminden asla yüklenmemeli ve kullanılmamalıdır ve hipervizörde düzenli olarak patch işlemleri yapılmalıdır.

6.6. Kötücül VM Atakları (MaliciousVM Attacks)

Sanal makine imajları sanal makine oluşturmak için kullanılan bir sanal aygıt şeklidir. Bu imajlar sanal makine için başlangıç dosya sistem durumunu ve yazılımlarını içerir [8]. Sanal makinede geçerli bir hesaba sahip olan bir kişi şayet kötü niyetliyse trojan tarzı sistemi etkileyebilecek yazılımlarla sanal makine imajı oluşturabilir. Diğer kullanıcılar bu imajı kullandıkları zaman veyahut kendi sanal makinelerini oluşturdukları zaman , art niyetli kullanıcının oluşturduğu trojan bu makinelere de bulaşma riski taşımaktadır. Oluşan bu durum akabinde saldırıyı gerçekleştiren kişi sunucuda tutulan gizli verilere de erişim sağlaması kaçınılmaz olacaktır.

6.6.1. Kötücül VM Ataklarna Karşı Önlemler

Art niyetli saldırıların hedefi olan sanal makineleri bu tarz saldırılardan korumak için , sanal makinelerin anlık ve güncel durumlarını gösteren sanal makine izleme sistemi kurulabilir. Bu sistem birbirine saldıran sanal makinelerin tespitini yapmakta ve bu durumların analizini Nitro VM izleme aracıyla takip etmek mümkün olacaktır.

6.7. VM Geri Alma Saldırısı (VM Rollback Attack)

Sanallaştırma teknolojisi içerisinde en kolay saldırı türlerinden biridir. Bu saldırıda bir hipervizör her hangi bir sanal makineyi askıya alabilir. Bunun yanında sanal makinenin farkında olmadan işlemci durumlarını , disk ve hafıza anlık görüntülerini çekebilir. Bu işlemleri sanal makine farkında olmadan yapmaya devam edebilir.

Genel olarak geri alma ataklarında , saldırıyı yapan kişi önceki anlık görüntülerden yararlanabilir ve kullanıcı anlamadan makineyi çalıştırıp daha sonra işlem geçmişini temizleyebilir. Bu süreç tekrar ve tekrar olacak şekilde çalışmaya ve uygulanmaya devam edebilir. Geçmişin temizlenmesi saldırıyı yapan kişinin yakalanmamasına yardımcı olur.

Bu durumun oluşmasına yetersiz güvenlik standartı ve denetimsizlik, tarayıcı güvenliği, hatalı güvenlik kurguları gibi zafiyetler sebep olmaktadır.

6.7.1. VM Geri Alma Saldırısına Karşı Önlemler

Rollback atakları önlemek adına yapılan çalışmalarda , hyperwall mimarisi yapılan çalışma ve araştırmalarda öneri olarak ön plana çıkmıştır [9] . Bu bakış açısında hipervizörün askıya alma ve devam etme fonksiyonlarının aktif olmamasına dayandırılmaktadır. Askıya alma ve devam etme fonksiyonlarının sanallaştırma için önem arz eden bir durum olduğu bilinmektedir , bu sebeple aktif olmamasının daha iyi bir sonuç ve çözüm ortaya çıkarmadığı aynı zamanda sanal makinelerin askıya alınması ve devam ettirilmesi esnasında son kullanıcının eşlik etmesi gerektiği belirtilmektedir , bu da askıya alma işlemi esnasında her bir tekrar için kullanıcıdan izin almak anlamına gelmektedir.

Hyperwall mimarisinin yanında , konuyla ilgili yapılan çalışma ve araştırmalarda konun çözümü ve sorunla baş edilebilmesi için bir başka yöntemde hipervizörün temel işlevini devre dışı bırakmadan çalışan , yalnızca sanal makine aktivitelerinin günlüğünü denetleyen bir geri alma eylemlerinin günlüğe kaydedilmesi ve denetlenmesi akabinde eylemin amacının art niyetli olup olmadığının tespiti söylenebilmesidir [10].

7.Vargılar

Bu tarama çalışmasında popüler olarak sanallaştırma teknolojisinde kullanılan saldırı yöntemleri ve bu tehditlere karşı güvenliği arttıran ve tehditlerle başa çıkma yöntemleri ele alınmıştır. Literatür taraması sonucunda varılan sonuçlar özetle aşağıda ele alınmıştır.

Sanallaştırma teknolojisi günümüzde hem son kullanıcılar hem de şirketlerin kullanımı açısından giderek artmaktadır. Paylaşılan kaynakların çok daha etkin kullanılması , performanslı ve düşük maliyetli bir çözüm olması bu alanın gelişme hızını arttırmaktadır. Bu avantajlarının yanında güvenlik riskleri ve tehditleri de söz konusudur. Bu kapsamda örnek olarak depolama sanallaştırma teknolojisini önemli kuruluşlar , önemli ve gizli verileri saklamak , depolamak amacıyla kullanmayı tercih etmemektedir. Bu alanlarda önem düzeyi düşük olan bilgi ve veriler saklanmaktadır.

Sanallaştırma teknolojisinde var olan katmanlı mimariden ötürü her katmanın güvenliği çok fazla önem arz etmektedir. Bu katmanlı yapının güvenlik sorun ve tehditleri ele alınarak yapılan araştırma ve incelemelerde , art niyetli kullanıcılar ve saldırganlar tarafından yapılan ,

sanallaştırma ortamında yaygın olarak karşılaşılan atak türleri ele alınıp bu ataklara karşı alınabilecek önlemler açıklanmıştır.

Sanallaştırma ortamında güvenlik olarak en başta ele alınacak ve uygulanması gereken işlemler fiziksel ve mantıksal kavramların ayrıştırılması , sanallaştırma ortamında güvenliği arttracaktır. Aynı zamanda sanallaştırma ortamının doğasında olan çok kullanıcılı hali , kullanıcılar arasında izalasyonun sağlanması için , yukarıda da belirtilen yöntemlerle uygun şekilde yönetilmelidir.

Özetle , yapılan tarama çalışmasında sanallaştırma ortamında tehditlere sebebiyet veren çeşitli güvenlik açıkları analiz edilmiş ve bu durumların olası savunma çözümleri ele alınmıştır.

Kaynakça

[1] S. Buyukgoze, "KIRKLARELI UNIVERSITY KAYALI CAMPUS' DESKTOP VIRTUALIZATION," *Research Journal of Business and Management,* vol. 3(4):, pp. 306-313, 2016.

[2] "Brief History of Virtualization," Oracle, [Online]. Available: https://docs.oracle.com/cd/E26996_01/E18549/html/VMUSG1010.html.

[3] Abraham Silberschatz, Peter Bear Galvin, Greg Gagne, Operating System Concepts, Laurie Rosatone, 2018.

[4] A. Doğru, "Sunucu Sanallaştırma ve Uygulama Sanallaştırma Teknolojileri Performans Karşılaştırılması - Yüksek Lisans Tezi," Maltepe Üniversitesi, İstanbul, 2019.

[5] G. S. Bohar Singh, "A Study on Virtualization and Hypervisor in Cloud Computing," *International Journal of Computer Science and Mobile Applications,* vol. 6, no. 1, pp. 19-21, 2018.

[6] Junjun Sun, Ying Zeng, Guowei Shi, Wei Li and Zhihong Li, "he Research for Virtualization Network Security on Cloud Computing," ICAITA , Xinjiang Karamay, 2018.

[7] I. K. AKSAKALLI, "BULUT BİLİŞİMDE GÜVENLİK ZAFİYETLERİ,TEHDİTLER VE BU TEHDİTLERE YÖNELİK GÜVENLİK ÖNERİLERİNİN İNCELENMESİ," *ULUSLARARASI BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ DERGİSİ,* vol. 5, no. 1, pp. 8-34, 2019.

[8] Hashizume K., Yoshioka N., and Fernandez, "Patterns for Cloud Computing," in *AsianPLoP '11 Proceedings of the 2nd Asian Conference*, Tokyo, Japan, , 2011.

[9] Jakub Szefer, Ruby B. Lee, "Architectural Support for Hypervisor-Secure Virtualization," *Computer Architecture News ,* vol. 40, no. 1, pp. 437-450, 2012.

[10] Yubin Xia , Yutao Liu , Haibo Chen , Binyu Zang, "Defending against VM Rollback Attack," in *Dependable Systems and Networks Workshops*, 2012.