Ağ Saldırı Konseptleri ve Senaryoları
(Network Attack Concepts and Scenarios)

Ağ Haritaları

Bulut sistemlerin haricinde bakıldığında, tüm bilişim altyapıları; kendi habitatları dahilinde farklı ağ haritalarına sahip olabilirler.

*Birden fazla ve farklı işlevlerde ağ elemanı barındırdıkları
*Farklı sunucu ve istemci bloklarına sahip oldukları
*Farklı VLAN yapıları üzerine kurgulandıkları
*Farklı Kablosuz Ağ sistemleri kullandıkları

ADIM: Ağ haritaları çıkartılmalıdır.

HUB

Kendine bağlı olan tüm ağ cihazlarını birbirine bağlayan merkezi bir iletişim cihazıdır.

ADIM: Ağda HUB cihazı var ise, trafik pasif olarak dinlenebilir.

Switch

Hub'da olduğu gibi, kendisine bağlı olan ağ cihazlarının haberleşmesini sağlar. Ancak Hub cihazlarından farklı olarak anahtarlamalı bir veri akışı sunar.

Yani, ağ yapısına dahil iki cihaz birbiri ile haberleşirken bu veriler sadece o iki cihaz arasında akar, diğer cihazlara gönderilmez. Bundan dolayı Hub cihazlarına göre daha yüksek performans gösterirler.

ADIM: Ağda switch cihazı var ise, üzerindeki her servis incelenmeli, SNMP bakılmalı, varsayılan yetkilendirmeler denenmeli, MITM saldırıları gerçekleştirilmelidir.

Wi-Fi Sniffing

Kablosuz ağ yapıları, kablo üzerindeki verilerin antenler ve dağıtıcılar sayesinde fiziksel olarak havaya yayılması olarak tanıtılabilir.

Bu yapılar, doğru yapılandırmalar konfigüre edilmediği veya uygun güvenlik önlemleri alınmadığı takdirde, saldırganlar tarafından sezilmeye ve sniff edilmeye müsaittirler.

Adaptör modunda bir NIC kullanan saldırgan, havadaki sinyal trafiği dahilindeki bazı değerleri izleyebilir ve buna saldırı vektörleri hazırlama fazlarında kullanabilir.

ADIM: Wi-Fi sistemleri sniff edilmeli, MAC Spoof denenmelidir. Misafirlere hizmet eden düşük yetkili ağlarda, izolasyonlar sınanmalıdır. Aynı zamanda, fiziksel erişim güvenlikleri gözlemlenmelidir.

Wi-Fi marka model, exploitleri olduğu için; fiziksel olarak görülmemelidir.
Diğer ağ elemanları da erişilebilir olmamalıdır.

Agent Misconfigs

Yapılandırmalardaki bazı hata ve eksiklikler, haberleşmelerin P2P olmak yerine Broadcast olmalarını sağlayabilir.

Aynı zamanda, genellikle agent veya discovery yapısına sahip olan bir çok ürün, yaptıkları işlemler fazında bilgi ifşalarına sebebiyet verebilir. Özellikle, VOIP, Antivirüs, PDKS, NOC gibi sistemlerin pasif yapılarda çalışması durumu, buna bir örnek verilebilir.

ADIM: Aktif ajan sisteminde çalışan yapılar tespit edilir ise, sunucu servisi hizmet reddi çalışmalarına tabi tutulmalıdır. Bu, loglama ve takip sistemlerini durdurabilir.

Network Mapping

Sniffing, ağ haritalarının hızlı bir şekilde çıkarılabilmesi için iyi bir yöntemdir. Güvenlik olarak belli bir pratiğin üzerinde kaliteye sahip yapılar, genellikle VLAN ve Subnetting mekanizmaları kullanırlar. Bu durumlar, IP Bloklarının çok geniş aralıklarda tercih edilmesine de sebebiyet verir.

Bir saldırgan, elde ettiği bağlantı sonrasında ağ haritasını çıkartmak için ağ üzerinde gürültü oluşturmak veya uzun zamanlar beklemek ve risk almak durumundadır. Eğer IP Blok aralıkları çok geniş ise, bu durum saldırganın işini daha da zorlaştırır.

Fakat, özellikle zehirlenmeler sonrasında sniffing özelliklerine sahip olan saldırgan, ağda yapılan trafiklerin sadece akışlarını filtreleyerek, ağda bulunan belki de tüm envanteri dakikalar içerisinde elde edilebilir.

Netdiscover, ettercap ve bettercap gibi araçlar, bu konuda yardımcı olabilir.

ADIM: VLAN Hopping aşamaları denenmeli ve izolasyon kontrolleri gerçekleştirilmelidir.

Turtles

Genellikle LAN Turtle adı verilen ve saldırganlar tarafından özellikle fiziksel siber saldırılar dahilinde kullanılan bu cihazlar, kablolama yapısına göre ilgili noktaların üzerinden geçen tüm trafiği kopyalayabilirler.

ADIM: Fiziksel erişim güvenlikleri gözlemlenmelidir.

FTP Hardening

*Rate Limiting,
*SFTP ve FTPS(SSH bazlı) kullanımı
*Doğru parola politikası kullanımı
*IP erişim kurallarının tanımlanması
*Dosya tiplerinin kontrolü
*Log Management
*Güncellemeler
*PUT ve DEL fonk. Devre dışı bırakılması
*Web panellerinde Basic Auth kullanılması

*Sunucuların sadece DMZ yapılarında barındırılması
*Anonim ve Guest kullanıcılarının deaktif edilmesi
*Whitelisting

ADIM: Service Exploiting denemeleri gerçekleştirilmeli, varsayılan ve anonim erişim denemeleri sınanmalıdır.

IP Spoofing

Yazılımsal bazda çalışan güvenlik duvarlarının bazı kontrol yapıları, doğru güncelik önlemleri alınmadığı surette atlatılabilir. Centos 7 makinelerinin firewalld sistemleri, Source IP Spoofing saldırılarına karşı güvende değildir.

Bu durumun üstesinden gelebilmek için, kernel dahilinde kaynak adres doğrulaması ayarlanmalıdır. Kaynak adres doğrulama, ilgili işleme yetkisi varmış gibi görünen sahte kaynak adresli paketleri engelleyen bir özelliktir.

2.4 ve sonraki çekirdek sürümleri, bu özelliğe sahiptirler. Basitçe anlatmak gerekirse; alınan paketin kaynağına, paketin geldiği arayüz üzerinden ulaşılıp ulaşılamadığı kontrol edilir.

ADIM: Service Exploiting denemeleri gerçekleştirilmeli, varsayılan ve anonim erişim denemeleri sınanmalıdır.

Rp_filter -> eğer ip spoof keşfedersen, otomatik olarak ip adresine (kaynağa git) ve bütün paketleri reject/drop yap.

```
#!/bin/sh
#author's name: Michael K Aboagye
#purpose of program: to enable reverse path filtering
#date: 7/02/18
#displays "enabling source address verification" on the screen
echo -n "Enabling source address verification…"
#Overwrites the value 0 to 1 to enable source address verification
echo 1 > /proc/sys/net/ipv4/conf/default/rp_filter
echo "completed"
```

```
iptables -A INPUT -i internal_interface -s IP_address -j REJECT / DROP

iptables -A INPUT -i internal_interface -s 192.168.0.0/16  -j REJECT/ DROP
```

ICMP Smurfing

Bu saldırıda, saldırgan bir ping paketi oluşturur ve bu pakete cevap verilecek IP adresini kurban makinenin IP adresi ile değiştirir. Sonrasında ise bu ping istekleri, IP bloğunun broadcast adresine flood şeklinde gönderilir.

İşlemin sonucunda istekleri alan her eleman bu isteklere cevap verir. Cevap adresi daha önceden değiştirildiğinden ve kurban makineyi hedef aldığında, tüm cevaplar kurban IP adresine gönderilir.

Bu iletişim akışı bir süre sonra hedef makinenin bu paketlere cevap veremez ve iletişime geçemez hale gelmesine sebep olur.

ADIM: ICMP erişimleri tespit edilmeli ve ICMP paketlerinin engellenmesi gerekmektedir.

DHCP Exhausting & Starvation

DHCP, ağa bağlanan cihazlara ip adresi, ağ maskesi, DNS sunucusu, varsayılan ağ geçidi gibi gerekli bilgi ve kimlikleri otomatik olarak veren bir sistemidir. Bir cihaz ağa bağlandığında DHCP sunucusuna haber verir, ve ihtiyacı olan bu bilgiler ona verilir.

ADIM: Saldırı gerçekleştirilmeli, fakat uzun süre açık tutulmamalıdır. Bu durum, hizmet reddine sebep olabilir.
Korunma; zaman kaynak rezervasyon limitleri konulmalıdır.

VOIP Sniffing

Voice IP yapıları, kendi aralarında iletişim gerçekleştirebilmek adına TCP/IP yöntemlerini kullanırlar.

Sniffing mekanizmalarını doğru filtrelemeler ile yapılandırabilmiş bir saldırgan, haberleşmekte olan VOIP cihazları arasındaki trafikleri koklayarak geçen RTP paketlerini elde edebilir ve paketlerin birleşimleri ile bir yayın oluşturarak konuşmaları dinleyebilir.

Aynı zamanda RTSP paketlerini yenileyebilen bir saldırgan, ilgili yayınlar üzerinde kontrol sahibi olabilir. Bu gibi durumlardan korunmanın en kolay ve mantıklı yolu, şifrelenmiş iletişimler kullanmaktır.

ADIM: RTP trafikleri filtrelenmeli ve var ise kayıt altına alınmalıdır.

ADIM: Brute Force
SMB, Telnet, SSH, FTP, Web Basic Auth, SQL Services vb. olası yapılar tespit edildiğinde, kaba kuvvet ve sözlük saldırıları gerçekleştirilmeli, olası erişimler denetlenmelidir.

Aynı zamana, düz metin olarak iletişim kuran ürün ve cihazlar tespit edilerek listelenmelidir. Desteklenmesi durumunda, bu cihazların şifreleme özellikli servisler ile yapılandırılması gerektiği belirtilmelidir.

Ağ Elemanları ve Topoloji - DMZ

DMZ, yani tam adı ile Demilitarized Zone; Web, DNS ve FTP gibi kurum dışına hizmet vermek için tasarlanmış ve barındırılan sunucuların firewall'un önüne alınarak, çok daha kritik bilgiler barındırmakta olan kurum yerel ağının dışında bırakılmasıdır. Bunun iki ana sebebi olduğu söylenebilir;

Yapılan bir siber saldırı sonucunda bu sunucular üzerinde RCE türevinde bir yetkilendirme alınır ise, saldırganın ağda bulunan diğer cihazlara erişmesini yerel bir firewall ile engellemek.

Sunuculara gelen trafiğin yerel ve yüksek oranda sıkılaştırılmış olan firewall tarafından engellenmesinin önüne geçmek,

ADIM: DMZ yapılarının varlığı ve LAN tarafından olan erişimin yüzeyi hesaplanmalıdır.

Zafiyetler ve Zafiyet Örnekleri

ADIM: Zafiyetlerin varlığı denetlenmelidir. Aynı zamanda, AD makineleri üzerindeki Zerologon zafiyetleri de denetlenmelidir.

MS17-010
Win7 for x64 SP1
Win 8.1 for x64 SPO
Win 10 ver. 1607 x64 SP0
Server 2008 R2 x64 SP1
Server 2012 R2 SP0

MS15-034
'HTTP.sys Remote Code Execution' olarak adlandırılan bir zafiyete yer aldı.

Win7
Server 2008 R2
Win 8 / 8.1
Server 2012 / R2

BlueKeep
CVE-2019-0708

RDP protokolü dahilindeki bir açıktan faydalanarak RCE durumuna olanak sağlayan kritik bir problemdir.

Win XP, 2003, 7, Server 2008 / R2

Open Relay
SMTP (25port) Open Relay Zafiyeti, e-posta adreslerinin çalışması için ayarlanmış SMTP servisinde yapılan bazı yapılandırma hataları dolayısıyla karşılaşılabilir. Bu durumda, saldırgan içeriden içeriye veya dışarıdan dışarıya(kritik) sahte bir e-posta trafiği oluşturabilir.

Üretilen bu postanın göndericisi, kurum dahilinde olan herhangi bir kullanıcının adına olabilir. Zafiyet kritik olmakla birlikte, hem 'Security Misconfiguration' hem de 'Authenticated Social Engineering' sınıflarına tabidir.

Shares ve Dosya Paylaşımları

Kurum ve kuruluşlarda kullanıcılar arasındaki dosya paylaşımlarının kolay olabilmesi açısından, Ağ Paylaşım adı verilen bir sistem uygulanır.

Bu özelliğin çalışabilmesi için öncelikle her istemci ve sunucu üzerinde; denetim masası panelinden ilgili ayarların yapılması gerekmektedir.

Dosya paylaşımının kullanılacağı ortak makine üzerinde belirlenen diskte bir klasör oluşturulur ve düzenleme sekmesinden ağa paylaşımı gerçekleştirilir.

Klasör izinleri oluşturulurken, herkesin yazabileceği ve okuyabileceği bir izin türü kullanılması önemlidir.

ADIM: Doğru yapılandırılmamış olmasına karşın, dosya paylaşım sistemleri denetlenmelidir.

Password Spray Attack

İlgili saldırı, kullanıcı adı ve parola sözlüklerini kullanarak, AD kullanıcılarının hesabına giriş yapmak amacı ile istekler gönderir. Brute Force saldırısından farkı, aynı hesaba birden çok parola denemektense, aynı parolayı farklı hesaplara denemesidir.

Crackmapexec aracı, DA kull. İle çalıştırıldığında, hedef sistemin parola politikalarını görüntüleyebilir.

python3 -m pip install pipx; pipx ensurepath
pipx install crackmapexec; pipx ensurepath

ADIM: Uygun parolalar elde edilir ise, saldırı vektörü kullanılmalıdır.

WiFi - Rogue AP ve Sosyal Mühendislik

Kablosuz ağ sızma testleri dahilinde gerçekleştirilebilecek saldırı vektörlerinden biri de, sosyal mühendislik tabanına dayanan, 'Rogue - Fake' Access Point saldırısıdır.

Bu saldırı türünde saldırgan, orijinal (hedef) AP aygıtı SSID'sine sahip olan bir AP kullanır ve kullanıcıların bu AP'e bağlanması için bekler. Saldırgan, ikinci bir adım olarak, orijinal AP'yi bir deauthentication saldırısına maruz bırakır ve böylece orijinal AP'ye bağlı olan kullanıcılar; aynı ismi taşıdığından dolayı sahte AP ile bağlantı kurarlar. Saldırının devamında saldırgan kullanıcılarının ürettiği tüm şifresiz trafiği okuyabilir ve kayıt altına alabilir.

Karşıt Önlemler / Sıkılaştırma / Karşılaşılanlar

*Sistemlerin otomasyon şekilde güncellenmesi,
*Parola politikalarının uygulanması
*Güvenli olduğu emin olunan bir imajın tüm istemci sistemlere dağıtılarak kullanılması,
*WAF, IPS ve IDS sistemlerinin kullanılması ve yapılandırılması,
*DMZ ağlarının oluşturulması,
*NOC Operasyonlarının oluşturulması,
*Ağ cihazlarının doğru konumlandırılması,

*Static Routing kurallarının tanımlanması,
*VLAN parsellerinin ayarlanması,
*Air Monitoring donanımı kurulması ve konfigüre edilmesi,
*Tüm trafikte TLS sertifikaları kullanımı,
*Doğru yetkilendirme ve erişimlerin verilmesi,
*Servis yazılım konfigürasyonlarının 'Best Security Practice' olarak gözden geçirilmesi,
*Sudo yetkilerinin ayarlanması,
*Kullanılan her türlü Disk aracının şifrelenmesi,
*Sunucu kategorisindeki cihazların fiziksel medya (CD, USB, Disket) gibi haricileri kabul etmemesi için yapılandırılması,
*Minimalizasyona gidilmesi ve gereksizlerin devre dışı bırakılması,
*Vulnerability Patch Management, Antivirüs ve Endpoint Sec. Ürünlerinin kullanılması,
*Kurum içi uyg. 'Güvenli Yazılım' ilkelerine göre hazırlanması,
*Her türlü yetkilendirmede 'Rate Limiting' ve mümkün ise Captcha sisteminin kullanılması, SCP Only Shell gibi, sadece belli amaçlar için üretilmiş yardımcıların kullanımı,
*Radius Server ile 802.1.x / NAC sisteminin yapılandırılması,
*Sürekli olarak otomasyon zafiyet taramaları yapılması ve raporlanması,
*Düzenli olarak profesyonel sızma ve zafiyet testlerinin uygulanması,
*En az bir adet Siber güvenlik elemanının kadroya dahil edilmesi,