Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBIM)
Ulak-CSIRT(Computer Security Incident Respose

Döküman Kodu: ULAKCSIRT-2008-01

KURUMSAL AĞLARDA ZARARLI YAZILIMLARLA MÜCADELE KILAVUZU

Sürüm 0.1

NİSAN 2008-04-16

Hazırlayanlar:

Enis KARAARSLAN

Gökhan AKIN

Vedat FETAH

ULAK-CSIRT, http://csirt.ulakbim.gov.tr

TÜBİTAK - ULAKBİM

ÖZET

Ulak-CSIRT Ulusal Akademik Ağ kapsamında kurulmuş bir güvenlik birimidir. Bu birimin kurulmasında takip edilen yöntem için RFC2350 dökümanına başvurabilirsiniz. Ulak-CSIRT (Computer Security Incident Response Team), dış ağlardan UlakNet'e yapılabilecek güvenlik ihlallerini önleme, gerçekleşen saldırı ve sorumlularını tespit etme ve aynı şekilde, UlakNet'ten dış dünyaya yapılan saldırıları önleme, eğer saldırı oluşmuşsa saldırı sorumlusunu tespit ederek saldırıyla karşılaşan ağın yöneticileriyle bilgileri paylaşmakla sorumludur.

Bu belgede, kurumsal ağlarda zararlı yazılımlala mücadele yöntemleri ele alınmıştır. Zararlı yazılımlar (trojan, virus, worm vb), makinelerde sorun yaratmaları dışında, büyük kurumsal ağlarda yarattıkları trafik ile ağ sistemlerinin yavaşlamasına ve hatta devre dışı kalmasına yol açabilmektedir. Bu bildiride, bu güvenlik sorunu ile savaşmak için gerekli önlemler anlatılacaktır. Bu önlemler alındığında, bilgi sistemleri daha tutarlı ve sağlam bir şekilde çalışacaktır.

Anahtar Kelimeler: Ağ yönetimi, kampüs ağları, güvenlik, zararlı yazılım, çok katmanlı güvenlik.

Teşekkürler:

Dökümana katkıda bulunan Hüsnü Demir'e teşekkürler.

İÇİNDEKİLER

1 GİRİŞ

İngilizce "malicious software" in kısaltılmış hali olan malware, yani zararlı yazılımlar çeşitli yollar ile bir bilgisayara bulaşıp, bulaştığı bilgisayar ve çevresine zarar vermesi için yazılmış programlardır. Zararlı yazılımlar (trojan/virus/worm gibi) bilgisayarlarda sorun yaratmaları dışında, kurumsal ağlarnda yarattıkları yoğun trafik ile bant genişliğin doldurulmasına ve ağ cihazlarının işlemci güçlerinin boşuna harcanmasına sebep olmaktadırlar. Bunlardan dolayı hattın devre dışı kalmasına bile yol açabilmektedirler.

Zararlı yazılımlar aşağıdaki zayıflıklardan yararlanarak sistemlere bulaşmaktadır:

- İşletim sistemindeki veya işletim sistemi üzerinde çalıştırılan çeşitli yazılımlarda bulunan güvenlik açıkları,Kullanıcının bilgisayarına basit şifre ataması,
- Kullanıcının harici bir kaynaktan (e-posta, sohbet yazılımları...vs) den gelen eklentileri /yazılımları kontrolsüz şekilde çalıştırması,
- USB ve benzeri ara birimlerden bağlanan hafıza ve sabit disk cihazlarında bulunan otomatik çalıştırma betiğine gizlenen kötü yazılımın, kullanıcının farkında olmadan çalışmasıdır.

Kampüs ağlarında, bu konuda ne tür önlemler alınabileceğini üç ana başlıkta incelememiz mümkündür:

- Kurumsal politika ve bilinçlendirme çalışmaları
- Makinelerde alınabilecek temel önlemler
- Ağda alınabilecek temel önlemler

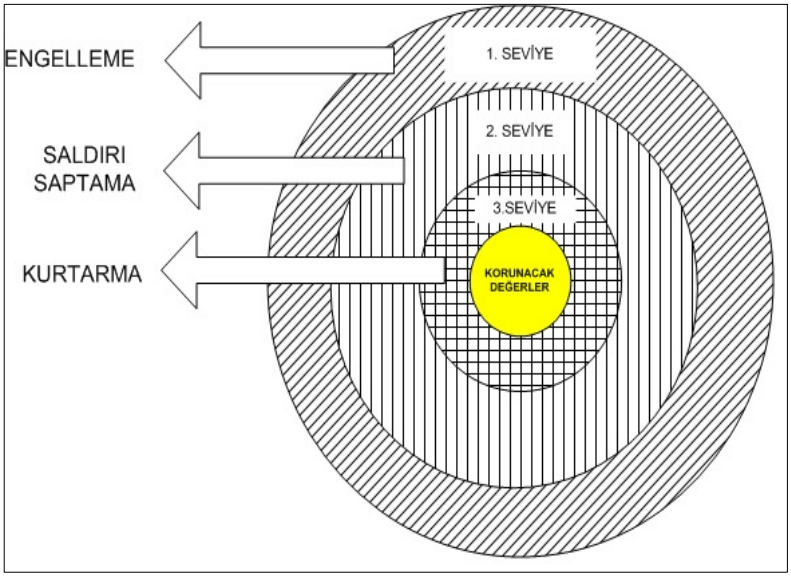
Güvenlik önlemleri, hiçbir zaman mükemmel değildir ve her güvenlik önleminin bazı zayıflıkları bulunabilmektedir. “Bir zincir ancak en zayıf halkası kadar güçlüdür.” sözünün de belirttiği üzere, güvenliğin sağlanması için zayıf noktalardan doğacak sorunların olabildiğince çözülmesi gerekmektedir. Bu da birbirini tamamlayan ve birlikte etkileşimli çalışan güvenlik sistemleri ile olasıdır. Bu tür bir yapıya çok katmanlı güvenlik ve savunma derinliği (defense in depth) denilmektedir. Sel suyunu engelleyen ardışık bentler gibi; her katman, bir sonraki katmana geçilmeden önce sorunun bir kısmını çözmüş olacaktır. Çok katmanlı güvenlik mimarisi ve derinliğine güvenlik anlayışı, gerçek yaşamda askeri güvenlik başta olmak üzere birçok farklı güvenlik önlemi için geçerlidir.

Şekil 1'de yıldız şeklinde olan ve çok katmanlı güvenlik özelliğine sahip Bourtange istikhamı gösterilmiştir [1].

Şekil 1. Çok katmanlı güvenlik örneği Bourtange İstihkamı

Güvenlik için bu süreçleri tanımlarken, farklı ve birbirini tamamlayan işlevlere ait çok katmanlı güvenlik sistemlerinden söz edilmektedir. Katman yapısını, kurulacak güvenlik sistemlerinin özelliğine göre farklılaştırmak ve her katmanda alt katmanlar kullanmak mümkündür. Genel olarak üç katmandan oluşan bir yapıdan söz etmek mümkündür. Bu genel model Şekil 2'de gösterilmiştir. Katmanlar aşağıdaki gibidir [1], [2]:

- İlk katman- Engelleme: Zararlı yazılımların bulaşmasını ve yayılmasını engellemek.
- İkinci katman - Saptama: Bulaşmış bilgisayarları saptamak.
- Üçüncü katman – Kurtarma: Bulaşmış bilgisayardaki etkilerin temizlenmesi ve bu bilgisayarların başkalarına bulaştırmasına ve ağa zarar vermesini engellemek



Şekil 2: Çok Katmanlı Güvenlik Modeli

2 KURUMSAL POLİTİKA VE BİLİNÇLENDİRME ÇALIŞMALARI

Kurumsal kullanım politikaları tüm yerel ağlarda olmazsa olmaz bir gereksinimdir. Bu gereksinimi karşılayacak pek çok taslak İnternet'te bulunabilmektedir. ULAK-CSIRT Güvenlik Politikaları sayfası (http://csirt.ulakbim.gov.tr/politika/) buna örnek olarak verilebilir. Bu taslaklar yasalara ve kuruma uygun hale getirilerek uygulanabilir.

İşletim sistemi sayısının fazla olması ve hepsine kurum tarafından destek verilmesinin zor olmasında dolayı kurum politikası dahilinde; kullanıcılar kurumun belirlendiği işletim sistemlerinden birini kullanmaya yönlendirmelidir. Bu konuda bir alternatif olarak açık kaynak kodlu işletim sistemlerinin ele alınması yararlı olabilecektir. Bunlardan GNU/Linux başı çekmektedir. Pardus işletim sisteminin son yıllardaki başarıları da dikkate değerdir.

Bunun yanı sıra kurumlar, anti-virus yazılımı kullanımı, şifre belirlenmesi gibi başlıkları da politikaları dahilinde belirtmelidir. Belirlenen işletim sistemleri ve diğer politikalara göre kullanıcıların kötü yazılımlardan korunabilmeleri için gereken eğitimlerin hazırlanması önem arz etmektedir. Bu eğitimler, belli seviyelerde ve devamlı olmalıdır. Eğitimde devamlılığı sağlamanın ve maliyeti indirmenin en yeni yöntemlerinden biri de teknolojiyi devreye sokmaktır. Verilen eğitimlerin video kaydına alınması, demo koruma uygulamaları yapılması, çeşitli açık kaynak kodlu yazılımların kullanımlarının anlatılması gibi örnekler verilebilir.

Kullanıcı bağlantı sorunu yaşadığında danıştığı mekanizmalara zararlı yazılım bulma/koruma yöntemleri de eklenmelidir. Mesela; yavaşlıktan şikayet eden bir kullanıcıya virüs taraması yapması konusunda uyarı gönderilmesi genel bir uygulamadır. Ama bu uygulamayı nasıl yapması gerektiği de ayrıntılı olarak kurumsal politikalarda belirtilmelidir.

Özel olarak hazırlanmış alan adı sunucusu kurularak kullanıcıların bu sunucuyu kullanmasını sağlaması önemli önlemlerden biridir. Karadelik DNS yapılandırması olarak da adlandırılan bu teknik yapılandırmanın en önemli kısmı kurumsal olarak bu politikayı dikte etmektir.

Farkındalık yaratmak için kullanıcıların İnternet'i ücretsiz kullanmadığını bilmesi gerekmektedir. Gereksiz indirdiği pek çok dosyanın esasen bir maliyeti olduğu kullanıcılara anlatılmalıdır. Çeşitli vesilelerle bu maliyetler kullanıcılara aktarılmalı ve ağın kurumun amaçlarına uygun kullanılması gerektiği hatırlatılmalıdır. Kampüs ağları örneğinde, amacın eğitim ve araştırmanın teşviği olduğu belirtilmelidir. Bu dosyalardan

kaynaklanan zararlı yazılım sorunlarının; bilgi işlem birimlerine ve kendilerine kaybettirdiği zaman, mümkünse parasal olarak ifade edilebilmelidir.

Son olarak da kurumsal politikaların uygulanması ve bu uygulamanın denetlenmesi gereklidir. Bu denetleme, ağın büyüklüğüne ve personel sayısına göre değişmektedir. Kurumsal politikalara uyulmaması durumundaki yaptırımların da belirlenmesi gereklidir.

3 MAKİNELERDE ALİNABİLECEK TEMEL ÖNLEMLER

Makinelerde alınabilecek temel önlemler aşağıdaki gibidir:

- Güvenlik yamalarının sürekli uygulanması: Örneğin, Microsoft işletim sistemi ile çalışan bilgisayarın en son çıkmış "service pack" ile kurulması, (Şu an için XP işletim sistemi için son service pack 'SP2', Windows Vista için son service pack SP1'dir.) Bunun dışında kalan güvenlik yamalarının güncelleme web sayfasından tamamlanması veya otomatik güncelleme ayarlarının her bilgisayarda yapılması. Açık kaynak kodlu işletim sistemlerinde yum, apt ve benzeri güncelleme yazılımları ile gereken güncellemelerin yapılması,
- Yama Yönetimi: Zararlı yazılımların mümkün olduğunca etkinliğini azaltmak için, kurumsal ağlarda bu yamaların merkezi bir makineye çekilmesi ve buradan diğer makinelere dağıtılmasını sağlayan yama yönetimi sistemleri de kullanılmalıdır.[5] Bu aynı zamanda hangi makinelerde yamaların geçildiğinin takibi açısından da önemlidir. Microsoft "Active directory" kullanılan ortamlarda, sistemlerin domain yöneticisi üzerinde kurulu SUS'dan (Smart Update Services) otomatik güncelleme alması sağlanabilir. "Active directory" olmayan ortamlarda, yine de bu tür bir hizmetin çalışmasını sağlayan çeşitli ücretli yazılımlar bulunmaktadır. Tabii ki bu tür sistemlerin çalışması için her makineye tek tek kurulmaları gerekecektir [5]. Kısıtlı haklarla kullanılabilmesi ve yönetilmesi kolay olan açık kaynak kodlu Linux, Unix, BSD benzeri sistemlerin tercih edilmesi,
- En az servis: İşletim sistemlerinde gereksiz tüm servislerin kapalı olması, (Bazı açık kaynak kodlu işletim sistemleri bu şekilde gelmektedir.)
- Antivirüs: Kurumun, kullanıcılarını antivirüs yazılımı bulundurmaya teşvik etmesi ve bunların güncel tutulması için gerekli mekanizmaları devreye alması. Bu konuda gereken bilgilendirmeyi yapması,
- İnternet tarayıcısı seçimi: Zararlı yazılımların bulaşma yöntemlerinden olan İnternet tarayıcısı seçimine göre, gereken güvenlik ayarlarının ve yamaların sürekli yapılması, (Kurumlar, çeşitli tarayıcıları takip ederek kullanıcılarına güvenli olduğunu düşündüğü tarayıcıyı önerebilir ve bu tarayıcının güvenlik ayarlarını ve gerekli güncellemelerini kullanıcılara ulaştırabilirler. Ayrıca kullanılan tarayıcıların üzerine eklenebilecek eklentiler sayesinde güvenlik arttırılabilmektedir. Mesela; "NoScript" yazılımı bu konuda çok başarılı bir yazılımdır.)

- Kişisel güvenlik duvarı, IDS/IPS yazılımlarının kullanılmasının teşvik edilmesi. (Örneğin Windows Personal Firewall, Zonealarm, iptables, PF, vb.)
- Windows SP2 ile bir kullanıcının ve/veya IP adresinin ne kadar bağlantı oluşturabileceğinin denetlenmesi sağlanabilmektedir. Saniyedeki paket sayısını (PPS) düşürmek için her bağlantıdan en fazla ne kadar paket geçeceği şekillendirilebilir. Bu sayede, kullanıcıdan habersiz olarak zararlı yazılımların oluşturulan bağlantı sayısını yükseltmesi ve sınırı doldurması durumunda, kullanıcının erişiminin yavaşlaması ve durması söz konusudur. Kullanıcı bağlanamayıp ağ/güvenlik birimine başvurması durumunda sorunlu bilgisayar tespit edilmiş olur.

4 AĞDA ALINABİLECEK TEMEL ÖNLEMLER

Ağda alınabilecek önlemler Tablo 1'de gösterilmiştir. Cihazların OSI'nin hangi seviyesinde çalışma yeteneğine sahip olduğuna göre L2 ve L3 cihazlar olarak tanımlanmıştır. Ağda alınabilecek önlemleri dört ana başlıkta sınıflamak mümkündür:

- L2 Cihazlar ile Alınabilecek Önlemler
- L3 Cihazlar ile Alınabilecek Önlemler
- Güvenlik Cihazları ile Alınabilecek Önlemler
- Diğer Sistemler ile Alınabilecek Önlemler

AĞDA ALINABİLECEK ÖNLEMLER	Birinci Katman	Ikinci Katman	Üçüncü Katman	Kaynak No
	Bulaşmasını Engelleme	*Bulaşmış Sistemi Saptama*	*Kurtarma ve Etkileri Azaltma*	
4.1. L2 Cihazlar ile Alınabilecek Önlemler				
4.1.1. MAC Adresi Bazında Güvenlik		X	X	6
4.1.2. 802.1x Tabanlı Kimlik Tanımlama	X	X		7,8
4.1.3. Broadcast/Multicast Sınırlandırması		X	X	9
4.2. L3 Cihazlar ile Alınabilecek Önlemler				
4.2.1. VLAN Bazlı Güvenlik Çözümleri	X		X	10
4.2.2. Erisim Listeleri Alınabilecek Çözümler	X	X	X	11,12,13
4.2.3. QoS ile Bandgenişliği Sınırlaması			X	14,15
4.2.4. Yeni Nesil Güvenlik Çözümleri		X	X	16,17
4.3. Güvenlik Cihazları ile Alınabilecek Önlemler				
4.3.1. Firewall (Güvenlik Duvarları)	X	X	X	18
4.3.2. Antivirüs Geçitleri	X	X	X	19
4.3.3. IDS/IPS Sistemleri	X	X	X	20
4.4. Diğer Sistemler ile Alınabilecek Önlemler				
4.4.1. Saldırgan Tuzağı Ağları (Honeynet)		X		21,22
4.4.2. Merkezi Log Kontrolü		X		23,24,25
4.4.3. Trafik Analizi		X		4, 26
4.4.4. DNS Sunucu			X	13,27,28,29
4.4.5. Arp Saldırılarını Tespit Edebilen Uygulamalar		X		30

Tablo 1. Ağda Alınabilecek Önlemler

4.1 L2 Cihazlar ile Alınabilecek Önlemler

OSI'nin 2. katmanında çalışan yerel ağ cihazlarında alınabilecek önlemler aşağıdaki gibidir:

- MAC Adresi Bazında Güvenlik
- 802.1x Tabanlı Kimlik Tanımlama
- Broadcast/Multicast Sınırlandırması

4.1.1 MAC Adresi Bazında Güvenlik

Switch'lerde port bazında MAC adresi güvenliği uygulaması zor bir çözümdür. Böyle bir işleme gidebilmek için önce bütün kullanıcıların MAC adresleri toplanmalı ve bu bilgiler sürekli güncel tutulmalıdır. Kaldı ki, günümüzde MAC adresi çok kolay değiştirilebilmektedir. Yani o porttan, switch'de izin verilen MAC adresini giren başka bir kullanıcı da erişebilecektir. Günümüzde zararlı yazılımlar bulaştıkları bilgisayarların tespitini zorlaştırmak için IP adreslerini ve MAC adreslerini bile değiştirebilmektedirler.

MAC adresi güvenliğinin cihazlarda uygulanması durumunda aşağıdakiler sağlanabilecektir:

- Ağa kontrolsüz bilgisayar erişimi ve MAC adres değiştirme durumunda bağlantı engellenecek,
- MAC flood saldırısı ile switch'in MAC adresi tablosu doldurulup Hub gibi çalışması engellenecek,
- Bu tür durumlar loglanacak ve bilgisayarın yeri tespit edilecektir.

Birçok markanın yönetilebilir anahtarlama cihazları ile bu önlemler alınabilmektedir. Aşağıda Cisco marka anahtar cihazlarında uygulanabilecek komutlar verilmiştir:

- Portta MAC adres güvenliğinin açılması:

```
switch(config)#Interface <int adı> <int.no>
switch(config-if)# switchport port-security
```

- Switch'in o portundan erişimine izin verilen MAC adresinin tanımlanması:

```
switch(config-if)# switchport port-security mac-address <PC'nin MAC
adresi>
```

- Porttan bağlanması istenen maksimum PC sayısının belirlenmesi

```
switch(config-if)# switchport port-security maximum <toplam PC sayısı>
```

- Belirtilen MAC adresi dışında bir PC'nin porta dahil olması veya belirtilenden daha fazla PC'nin porta dahil olması durumunda uygulanacak işlemin tanımlanması. Bu işlemler ayrıntılı olarak aşağıdaki tabloda belirtilmiştir

```
switch(config-if)# switchport port-security violation <protect | restrict
| shutdown>
```

Kuralldışı Erişimde	Trafiğin Bloklaması	SNMP Trap Yollanması	Syslog Mesajı Yollanması	Portun Kapatılması
Protect	Evet	Hayır	Hayır	Hayır
Restrict	Evet	Evet	Evet	Hayır
Shutdown	Evet	Evet	Evet	Evet

Cisco marka anahtar cihazları için örnek konfigürasyon aşağıda gösterilmiştir.

```
switch(config)#Interface fastethernet 0/0
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security maximum 2
switch(config-if)# switchport port-security violation restrict
switch(config-if)# switchport port-security mac-address 1010.1010.1010
switch(config-if)# switchport port-security mac-address 2020.2020.2010
```

4.1.2 802.1x Tabanlı Kimlik Tanımlama

IEEE 802.1X, port tabanlı ağ erişim kontrol standardıdır. Kullanıcı bilgileri (kullanıcı adı, parola ve bazı özel durumlarda MAC adresi) yardımı ile ağa bağlanılmasına izin verilmesini sağlar. Kullanıcı doğrulama sırasında EAP (extensible authentication protocol-RFC2284) yöntemi kullanılır [7].

802.1x için ağ altyapısındaki yönetilebilir (switch, kablosuz ağ cihazı gibi) cihazlarda gerekli ayarlar yapılmalı ve kullanıcı bilgilerini denetleyip gerekli düzenlemeleri yapacak bir sunucu bulundurulmalıdır. Ayrıntılı bilgi için bkz [8].

Bu protokol sayesinde, sadece kurumun kullanıcıları izin verilen ağlara bağlanılacaktır. Güvenlik açısından, misafir bilgisayarların ayrı bir VLAN'a bağlanması ile yetkileri, ulaşabilecekleri ağlar ve kullanacakları iletişim kapıları kısıtlanabilecektir. Bu da zararlı yazılımların dağılmasını kısıtlayabilecektir.

Kullanıcının bu tür bir yöntemle sisteme bağlanması anında, kişisel antivirüs yazılımını ve imza güncelliğini denetleyen ticari sistemler de bulunmaktadır. Böylece kullanıcı, kurumun antivirüs yazılımını kurana ve/veya güncel imzaya sahip olana kadar, sistem tarafından ayrı bir sanal ağa alınacaktır. Ancak gerekli yüklemeler gerçekleştikten

sonra kendi ağına bağlanabilecektir. Bu da, zararlı yazılımların etkin olmasını engelleyecek yöntemlerden birisidir.

4.1.3 Broadcast/Multicast Sınırlandırması

DoS veya DDoS saldırılarının bir kısmı broadcast (genel yayın) adresi üzerinden yapılmaktadır. Bu tür saldırıların etkisinin azaltılması için broadcast sınırlaması yapılmalıdır. Broadcast düşünülürken, kullanılan protokol dikkate alınmalıdır. En yaygın olanları Ethernet ve IP'dir.

Broadcast/multicast/unicast trafiğinin 1 saniyede belirli bir yüzdeyi aşması durumuna, Broadcast/multicast/unicast fırtınası (storm) denilmektedir. Anahtarlama cihazlarında yapılan ayarlama, 1 sn içinde interface'in toplam bant genişliğinin belirlenen yüzdeyi geçmesi veya belirlenen paket sayısını aşaması durumunda eşik değerinin üstündeki trafiğin bloklanmasıdır. Kullanılan cihaza ve modüle bağlı olarak broadcast, multicast ve unicast trafik kontrol edilebilir. Örneğin Cisco cihazlarda bu kontrol donanım seviyesinde yapılmaktadır. Yapılabilecek bazı denetimler ve çalışma şekli aşağıdaki gibidir:

- Tek başına Broadcast Traffic Storm Control özelliğinin açılması: 1sn içinde eşik değeri aşılırsa eşik değeri üstündeki bütün broadcast trafiği bloklanır.
- Multicast ve Unicast Traffic Storm Control aynı anda açılması:
    - Multicast ve broadcast trafiği toplam eşik değerini aşarsa, o birim zamandaki bütün aşan multicast ve broadcast trafiği bloklanır.
    - Sadece broadcast trafiği toplam eşik değerini aşarsa, o birim zamandaki bütün aşan multicast ve broadcast trafiği bloklanır.
    - Sadece multicast trafiği toplam eşik değerini aşarsa, o birim zamandaki bütün aşan multicast ve broadcast trafiğini bloklanır.

Cisco marka cihazlarda bu düzenlemelerin yapılması durumunda, aşağıdaki özellikler dikkate alınmalıdır:

- BPDU paketleri bazı cihazlarda multicast trafiğinden sayılır ve eşik değeri aşılırsa BPDU paketleri de bloklanır. Bazı modeller BPDU trafiğini storm kontrolü dışında tutabilmektedir. Eşik değeri aşılsa bile bu cihazlarda BPDU trafiği bloklanmaz.
- Eşik değeri 0 yapılırsa bütün trafik bloklanır
- Eşik değeri 100 yapılırsa hiç bloklanma yapılmaz.
- Default'ta bütün traffic storm control özellikleri kapalıdır.

- EtherChannel interface'lerinde storm control açılabilir. Ancak konfigürasyon, fiziksel interface'lerde değil sadece mantıksal port channel interface'inde uygulanmalıdır.

Aşağıda Cisco marka cihazlarda "storm control" komutları açıklanmıştır. Bu komutlarda, "*Level"* değeri ile belirtilen yüzde veya paket değerinin aşılması durumda aşan trafik bloklanmaktadır. "Level-low" ise seçimlidir ve "Level" ile belirtilen değerin aşılmasından sonra, trafiğin hangi değer altına inmesi durumunda tekrar bloklanmanın kaldırılacağı belirtilmektedir. Temel komutlar:

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# storm-control broadcast level <level:Yüzde.Küsüratı
şeklinde> {level-low Yüzde.Küsüratı şeklinde}
Switch(config-if)# storm-control multicast level <level:Yüzde.Küsüratı
şeklinde> {level-low Yüzde.Küsüratı şeklinde}
Switch(config-if)# storm-control unicast level <level:Yüzde.Küsüratı
şeklinde> {level-low Yüzde.Küsüratı şeklinde}
Switch(config-if)# storm-control broadcast level pps <level:pps şeklinde>
{level-low pps şeklinde}
Switch(config-if)# storm-control multicast level pps <level:pps şeklinde>
{level-low pps şeklinde}
Switch(config-if)# storm-control unicast level pps <level:pps şeklinde>
{level-low pps şeklinde}
```

Varsayılan olarak, eşik değeri aşılan trafik bloklanacak ve bir uyarı yollanmayacaktır. Eşik değeri aşılınca SNMP trap yollayacak şekilde de ayarlanabilir. Ayrıca "shutdown" parametresi ile interface "err-disable" durumuna da getirilebilir.

```
Switch(config-if)# storm-control action <shutdown | trap>
```

Cisco marka anahtar cihazları için örnek konfigürasyon aşağıda verilmiştir:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# storm-control multicast level 80.0 50
Switch(config-if)# storm-control broadcast level pps 200 100
storm-control action shutdown
```

4.2 L3 Cihazlar ile Alınabilecek Önlemler

OSI'nin 3. katmanında çalışan cihazlarda alınabilecek önlemler aşağıdaki gibidir:

- Vlan Tabanlı Güvenlik Çözümleri
- Erişim Listeleri ile Alınabilecek Çözümler

- QoS ile Kişi Başına Bant Genişliği Sınırlaması
- Yeni Nesil Güvenlik Çözümleri

4.2.1 VLAN Tabanlı Güvenlik Çözümleri

Üçüncü katman ağ cihazlarında yapılacak ayarlamalar ile kötü amaçlı yazılımların ağ üzerindeki etkileri azaltılabilir. Aşağıda Cisco marka cihazlarda vlan bazında uygulanabilecek ayarlar ve açıklamaları bulunmaktadır. Konfigürasyon genel olarak kullanılması tavsiye edilen ayarları içermektedir, ancak kullanmadan önce uygulanacak ağın ihtiyaçları da göz önüne alınmalıdır [10].

```
int Vlan Vlan_Numarası
…
ip verify unicast source reachable-via rx allow-default
! VLAN altında belirtilmiş IP adresleri dışında başka kaynak IP adresi
ile o VLAN'den trafik çıkmasını engeller.
no ip redirects
! ICMP redirect desteğini kapatır.
no ip unreachables
! ICMP unreachable paketlerinin geri yollanması engeller. Bu özellik
raslansal hedef IPler seçerek DoS atağı yapmaya çalışan bir bilgisayara
ulaşılamadı mesajı geri gönderilmeyerek hem yönlendirici üzerindeki yük
azaltılır, hem de atak yapan bilgisayarın time-out süresine kadar
beklemesine sebep olur.
no ip proxy-arp
! Ağ geçidi (gateway) tanımlamamış veya yanlış tanımlamış bir istemcin
yönlendirici tarafından tespit edilerek o istemcilere ağ geçidi
hizmetinin otomatik verilmesi özelliğini kapatır.
```

4.2.2 Erişim Listeleri ile Alınabilecek Çözümler

Erişim listelerini kullanılıp yönlendiricilerde aşağıdaki önlemler alınarak kötü amaçlı yazılımların ağ üzerindeki yükü azaltılabileceği gibi kendilerini yaymaları da engellenebilir. Temel önlemler aşağıdaki gibi özetlenebilir:

- Yönlendiriciye gelen paketlerdeki kaynak IP adresleri kontrol edilmelidir. Dış ağdan iç ağa gelen paketlerde, gelen paketlerdeki kaynak ip'lerin kontrolüne giriş (ingress) filtreleme denmektedir. İç ağdan dış ağa giden paketlerde, gelen paketlerdeki kaynak ip'lerin kontrolüne çıkış (egress) filtreleme denmektedir. Bu

filtrelemeler dahilinde RFC 3704'de [11] tarif edildiği gibi kaynağı olmayan 0.0.0.0/8, 10.0.0.0/8, 192.168.0.0/16, 127.0.0.0/8 ve 169.254.0.0/16 adresleri bloklanmalıdır. Ayrıca kurumun IP adresi aralığını, kaynak IP adresi olarak kullanarak yapılabilecek saldırıları engellemek için dışarıdan kurumun IP adresi kaynaklı trafik yasaklanmalıdır. Ayrıntılı bilgi için bkz [12,13].

- Güvenlik açıklarının kullandığı bilinen bazı portların kapatılması veya kısıtlanmasıdır. Bunlara örnek olarak şu portları belirtmek mümkündür: TCP 135, 137, 139, 445 UDP: 137, 138, 161, 162
- SMTP trafiğinin sadece iç mail sunuculara doğru açılmalı, diğer SMTP trafiğinin bloklanmalıdır.
- ICMP trafiğinde "packet-too-big", "time-exceeded", "echo-reply", "echo" ya izin vermek, geriye kalan ICMP türlerini bloklamaktır.
- Erişimi engellenen trafik loglanarak saldırgan bilgisayarın kimliği de tespit edilebilir. Ancak bunun çok sistem kaynağı tüketme riski de vardır.

Cisco marka yönlendiricilerde kullanılabilecek ve dışarıdan gelecek trafiği filtreleyecek örnek erişim listesi aşağıda gösterilmiştir. Örneklerde, VLAN'in kendi IP adresi aralığı ve wildcard maskesi, İçAğTanımı değişkeni ile gösterilecektir. Sunucuların bulunduğu ağ, SunucuAltAğı değişkeni ile gösterilecektir.

```
ip access-list Vlan_disardan
remark ******* icmp **********
permit icmp any any packet-too-big
permit icmp any any time-exceeded
permit icmp any any echo-reply
permit icmp any any echo
deny icmp any any
remark * bloklanacak portlar *
deny tcp any any eq 445
deny tcp any any range 135 139
deny udp any any range 135 139
deny udp any any range 161 162
...
remark * bloklanacak IPler *
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
deny ip 169.254.0.0 0.0.255.255 any
deny ip İçAğTanımı any  # dışarıdan iç ağa ait IP adresli paket gelemez
permit ip any any
```

Kurumun, sunucu bulunmayan alt ağları için, dışarıdan gelen tcp paketlerinde ACK alanı bulunması durumunda kabul edilmesi ve diğer durumlarda kabul edilmemesi sağlanabilir. Böylece birçok ağ kapısı tarama ve virüs yayılımı engellenebilecektir. Sunucu servislerinin bulunması durumunda, sunuculara gelen trafik öncesinde izin verilmelidir. Bu ayarlar için yukarıdaki erişim listesinin son satırının önüne aşağıdaki satırların eklenmesi yeterli olacaktır.

```
permit tcp any host SunucuIPAdresi eq 80  <veya başka ağ kapıları>
permit tcp any İçAğTanımı established
deny tcp any any
```

Erişim listeleri ile istenmeyen trafikler bloklanabileceği gibi kara delik oluşturmak amaçlı olarak, L3 cihazda policy-routing ile honeynet'lere veya IDS/IPS güvenlik sistemlerine de yönlendirilebilecektir.

Kurumun iç ağından dışarıya veya kurumun sanal ağları arasında trafiğin de filtrelenmesi önerilmektedir. Örneğin, ağ üzerinden oyun ve P2P protokollerinin kullandığı UDP paketlerinin filtrelenmesi önerilebilir. Kurum için kritik bir uygulamanın UDP

kullanması durumunda, kısıtlı olarak belirtilen sunucunun belirtilen ağ kapısı için UDP ye izin verilmesi ve geriye kalan UDP paketlerinin engellenmesi önerilmektedir.

```
ip access-list extended Genel_icerden
 permit ip any host 255.255.255.255   <dhcp'ye erişime izin>
 remark *** kısıtlama olmadan ulaşakları adreslere erişim **
 permit ip İçAğTanımı host SunucuAdresi
 ...
remark Kara Delik uygulaması
 permit ip any host KaraDelikSunucuIP
remark **** Sadece izin verilen sunuculara smtp atmalı ************
 permit tcp İçAğTanımı SunucuAltAğı eq smtp
 deny   tcp İçAğTanımı any eq smtp
remark **bilinen virüs portlarının kapatılması
 deny   tcp any any eq 445
 ...
remark * Microsoft Portlarının kullanımının sınırlandırılması
 permit tcp İçAğTanımı İçAğTanımı eq 137
 permit tcp İçAğTanımı host SunucuIP eq range 138 139
 deny   tcp any any range 135 139
remark ******* icmp kısıtlamaları **********
 permit icmp İçAğTanımı any packet-too-big
 permit icmp İçAğTanımı any time-exceeded
 permit icmp İçAğTanımı any echo-reply
 permit icmp İçAğTanımı any echo
 deny   icmp any any
remark *********
 permit udp İçAğTanımı İçAğTanımı      <iç ağda udp ye izin ver>
 permit udp İçAğTanımı any eq domain   <iç ve dış dnslere erişime izin>
 deny   udp any any                    <diğer udp'leri blokla>
 permit ip İçAğTanımı any
 permit igmp İçAğTanımı any
 deny  ip any any log
```

4.2.3 QoS ile Kişi Başına Bant Genişliği Sınırlaması

Birim kullanıcının dışarı veya içeri doğru kullanabileceği trafik miktarı QoS teknikleri ile kısıtlanabilir. Bu şekilde kötü bir yazılım bulaşmış bir bilgisayarın ağ kaynaklarını sömürmesi engellenir. Bu çözüm aynı zamanda P2P yazılımlarının da bant

genişliğini tüketmesini engeller. Bunun için L3 bazlı anahtarlama cihazlarında yapılabilecek ayarlamalar kullanılabileceği gibi, açık kaynak kodlu ipfw gibi uygulamalarda kullanılabilir [14,15].

4.2.4 Yeni Nesil Güvenlik Çözümleri

Kötü amaçlı yazılımların IP adreslerini değiştirmelerini, DHCP ve ARP zehirleme saldırıları yapamalarını engellemek için L3 anahtarlama cihazlarında çeşitli çözümler bulunmaktadır. (Ayrıntılı bilgi için bkz [16,17]). Cisco marka anahtar cihazlarında bu amaçlarla DHCP Snooping, Dynamic ARP Inspection, IP Source Guard çözümleri vardır. Aşağıda bu çözümler için örnek konfigürasyon bulunmaktadır.

```
ip dhcp snooping
ip dhcp snooping vlan <vlan no>
ip arp inspection vlan <vlan no>
!
interface <int adı> <int.no>
description Istemci bilgisayar portu
ip verify source port-security
!
interface <int adı> <int.no>
description DHCP sunucusunun portu veya Uplink portu
ip dhcp snooping trust
ip arp inspection trust
```

4.3 Güvenlik Cihazları ile Alınabilecek Önlemler

Ağ üzerinde güvenlik amaçlı kurulacak sistemlerle alınabilecek önlemler aşağıdaki gibidir:

- Güvenlik Duvarları (Firewall)
- Antivirüs Geçitleri
- IDS/IPS Sistemleri

4.3.1 Güvenlik Duvarları (Firewall)

Güvenlik duvarları, durum korumalı (statefull) çalıştıkları için, düzgün ayarlanmaları durumunda zararlı yazılım aktivitesi içeren birçok bağlantıyı engelleyebilecektir. Servis sağlayan sunucuların belirli portları hariç, bütün portlar kurum dışından içeri doğru erişime kapatılmalıdır. 4.2.2'de Erişim kural listeleri ile alınacak

bütün çözümler güvenlik duvarlarında da alınmalıdır [19]. Güvenlik duvarının en basit kural tablosunun mantığı aşağıdaki gibi olmaldır.

```
# Kurum içinden dışarı trafik
Bilinen zararlı yazılım portlarını kapat
Bütün trafiğe izin ver
# Kurum dışından içeri
Sunuculara sunucu portlarından erişim izni
Geriye kalan bütün trafiği blokla
```

Güvenlik duvarı için ticari çözümler olduğu gibi, açık kaynak kodlu başarılı çözümler de bulunmaktadır. Açık kaynak kodlu çözümler için destek veren firmalar da bulunmaktadır. Güvenlik duvarı çözümü seçmeden önce, [18] referansının incelenmesi önerilmektedir.

4.3.2 Antivirüs Geçitleri

Geçen trafiği zararlı içeriğe göre kontrol eden sistemlerdir. Özellikle büyük ağlarda sadece eposta trafiği için bu tür çözümler kullanılmaktadır. Kötü amaçlı yazılımların kendilerini bulaştırmak için en sık kullandığı tekniklerden biri eposta olduğundan, kullanılması ciddi bir fayda sağlamaktadır. Bunun için ticari çözümler kullanılabileceği gibi Clamav[19] gibi GPL lisansına sahip çözümler de kullanılabilir.

4.3.3 IDS/IPS Sistemleri

Günümüzde güvenlik duvarları bütünleşik olarak IDS/IPS mekanizmalarına sahip oldukları gibi, bu sistemler ayrı olarak da kurulabilmektedir. İyi yapılandırılmış bir IDS/IPS sistemi; ağı pek çok kötü yazılımdan izole edebileceği gibi, sorunun kaynağını tespitini de hızlandırmaktadır. Ancak bu sistemlerin iyi bir şekilde ayarlanmaması ve devamlı takip edilmemesi, yanlış tespitler sonucu sorununu da çıkarabilmektedir. Bu sistemler için, ticari çözümler kullanabileceği gibi Snort [20] gibi açık kaynak koduna sahip çözümler de kullanılabilir. Snort için http://www.bleedingsnort.com/ adresinde bulunan bleeding-malware.rules" dosyasındaki güncel zararlı yazılım imzaları kullanılmalı ve sistem sorumluları gözlemledikleri yeni saldırılara ait imzaları da kendileri eklemelidir.

4.4 Diğer Sistemler ile Alınabilecek Önlemler

Alınabilecek önlemler aşağıdaki gibidir:

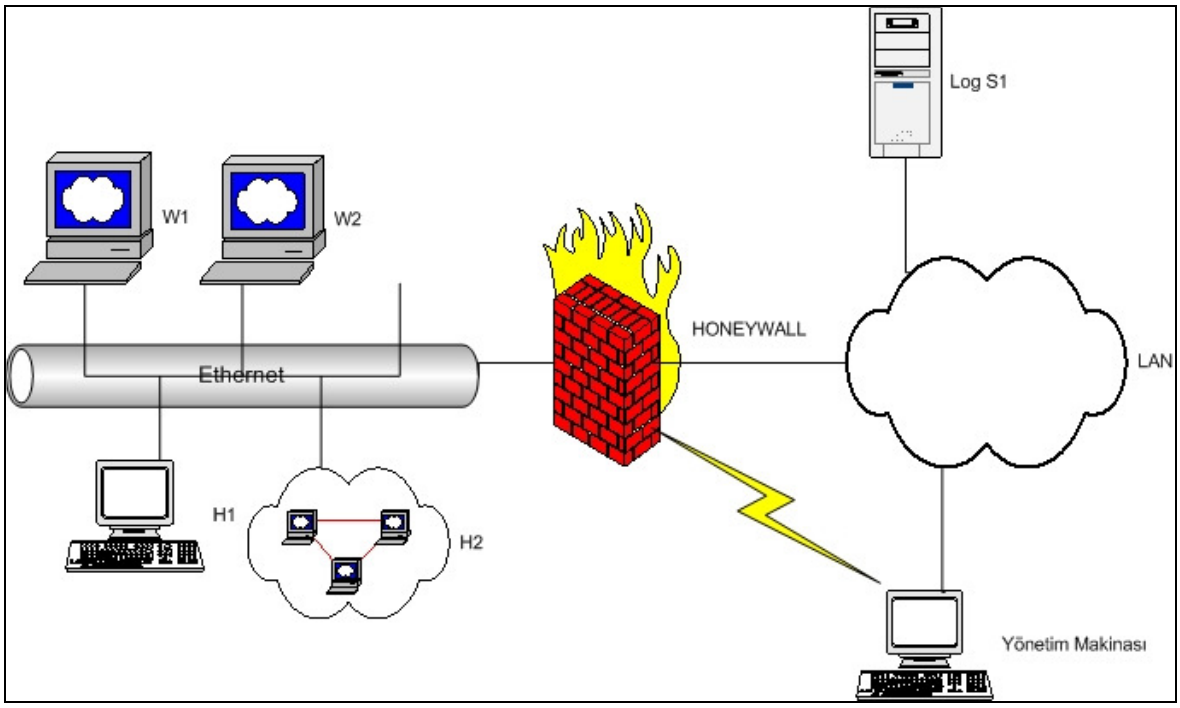
- Saldırgan Tuzağı Ağları (Honeynet)
- Merkezi Log Sunucu Sistemi
- Trafik Akış Analizi Sunucuları
- DNS Sunucu
- Arp Saldırılarını Tespit Edebilen Uygulamalar

4.4.1 Saldırgan Tuzağı Ağları (Honeynet)

Zararlı yazılım ve saldırganların saldırılarını saptamak için tuzak sistemleri (honeypot) kullanılabilir. Tuzak ağı (honeynet), tuzak sistemlerinden oluşan bir ağdır. Açık kaynak kodlu yazılımlarla bu tür sistemler kurmak ve yenilerini geliştirmek mümkündür.

Saldırgan tuzağı ağı (honeynet), kurum tarafından kullanılmayan bir alt ağı kullanacak şekilde ayarlanmalıdır. Güvenlik duvarından, bu ağa gelen bütün trafiğe izin verilmelidir. Bu ağ, normalde dışarı hiç trafik oluşturmadığı için, bu ağa gelen bütün trafik incelenilmesi gereken ağ trafiğidir. Bu trafik, saldırı trafiği olmaktadır [1].

Çeşitli bilinen zayıflıkları simüle eden, virüs ve worm etkinliğini yakalama amaçlı kurulan sistemlere örnek olarak "Nepenthes" ve "Amun" yazılımları verilebilir [21]. Bunun yanı sıra, "Honeyd" yazılımı ile bir makine üzerinde farklı işletim sistemlerini simüle eden sanal makineler, sanal yönlendiriciler ve sanal ağlar oluşturulabilir. Burada amaçlanan, bu makinelere saldırganların veya zararlı yazılımların erişimlerini takip etmektir. Ayrıca transparan olarak çalışan "Honeywall" yazılımı çalışan sistem, üzerinden geçen trafiği analiz etmekte, düzgün ayarlanması durumunda alt ağdaki tuzak sistem makinelerinin ele geçirilmesini ve buradan dışarı saldırı yapılmasını engelleyebilmektedir. ULAK-CSIRT Honeynet çalışma grubu bu konuda çalışmalarına devam etmektedir [22]. Ege Üniversitesi'nde kurulan tuzak ağının mantıksal mimarisi Şekil 3'de verilmiştir. Honeywall'in arkasında çeşitli honeypot sistemleri kurulmuştur [1].



Şekil 3. Ege Üniversitesi saldırgan tuzağı ağı mimarisi

4.4.2 Merkezi Log Sunucu Sistemi

Sistem loglarının düzenli takip edilmesi gerekmektedir. Birden fazla ve farklı sistemlerin loglarını; hepsine tek tek girip bakmaktansa, merkezi bir log sunucusuna atmak en etkin çözümdür. Büyük miktardaki log'u analiz etmek ve içlerinden kritik mesajları çıkarmak için çeşitli yazılımlara ve betiklere(script) ihtiyaç duyulmaktadır. Sistem yöneticileri, Ranum'un log analizi konusundaki ayrıntılı belgesini [32] mutlaka incelemelidir. Gelişmiş log analizi için [33], [34], [35] nolu referanslar incelenmelidir.

Ağ cihazlarından gelecek logları sürekli ve kesintisiz tutacak bir log sunucusu mutlaka bulundurulmalıdır. Bu sunucudaki kayıtlar incelenerek, kötü bir yazılım bulaşmış bilgisayarın yeri tespit edilebilir. 4.1.1, 4.1.3, 4.2.2, 4.2.4 ile 4.3.1 tarif edilen engelleme çözümleri, log sunucu sistemi ile kayıt altına alınmış olacaktır. Ayrıca NAT ve DHCP gibi kaynak IP adresinin değişme ihtimali olan çözümlerde, bulaşmış bir bilgisayarın tespiti için mutlaka log sunucuları yardımı ile kaynak adres takip altına alınmalıdır [25].

Bu amaçlar için, açık kaynak kodlu syslog veya syslog-ng uygulamaları kullanılabilir. Bu durumda merkezi sunucuda da gelen logları bekleyecek bir yazılımın çalışması gerekmektedir. Syslog-ng, ek özellikleri ve Stunnel (http://www.stunnel.org) ile log'ları şifreli gönderebilmesi yeteneklerinden dolayı tercih edilmelidir [23]. Syslog hakkında ek bilgi ve referanslar için [36]'yı inceleyiniz.

Log analizi için Sawmill gibi çeşitli ticari yazılımlar bulunmaktadır. Bu yazılımların bazılarının kısıtlı versiyonlarını açık kaynak kodlu olarak temin etmek mümkündür. Log bilgisinin çok fazla olması durumunda ihtiyaca göre filtrelenip, gerekmesi durumunda da yöneticiyi eposta ile uyaran Swatch benzeri yazılımlarda karmaşayı azaltmak için kullanılabilir [24]. Swatch yazılımının uygulanması örneği için bkz [31]. Benzer bir süreci gerçekleştiren Logwatch (http://www.logwatch.org) da incelenebilir.

4.4.3 Trafik Akış Analizi Sunucuları

Bilmediğimiz saldırı türleri olabilir. Bilinmeyen ve saldırı saptama sistemleri tarafından saptanamayan saldırılar için trafik çözümleme süreçleri kullanılmalıdır. Kurum ağı trafiği ve özellikle saldırgan tuzağı ağına gelen trafik, ayrıntılı olarak incelenmelidir.

Trafik akış ile bahsedilen, iki makine arasındaki iletişimin özetlenmesidir. İletişime ilişkin yön, adres, ağ kapısı ve trafik büyüklüğü gibi bilgilerin çözümlenme için elde edilmesidir. Ağ trafiği çözümlenerek ağın normal davranışını modellemek olasıdır. Haftanın herhangi bir günü için, çeşitli zaman aralıklarında trafiğin özelliğini belirtecek veriler elde edilebilir. Trafik bilgisinde, incelenmesi ve saptanması gerekenlere örnek olarak aşağıdakilerden söz edilebilir [1]:

- O an çalışmayan makinelere/alt IP ağlarına giden trafik
- Yüksek ağ kapılarına giden/gelen servis isteği trafiği
- Yüksek bağlantı oranları
- Yüksek paket oranları
- İzlenmeyi engellemek için veriyi başka veri akışlarında saklayarak yapılan saldırılar (Covert channels)

Elde edilen ortalama değerlerden yaşanan sapmalar, kurum ağında farklı bir etkinliğin gerçekleştiği konusunda bize ipucu verecektir. Özellikle servis aksatma saldırıları, güvenlik açığı tarama girişimleri veya saldırı sonrasında sunucuların farklı amaçlar için kullanılması gibi saldırılar bu şekilde saptanabilir. Bunun yanı sıra, saldırının boyutu, saldırganın başka hangi sunucu ve servislere erişim kurduğu/kurmaya çalıştığı da incelenebilecektir [1].

Ağ cihazlarının bize sağladığı monitor port özellikleri ile trafik bir bilgisayara yönlendirebilir ve trafik bu bilgisayardaki programlarla analiz edilebilir. Aşağıda Cisco marka anahtarlama cihazlarında monitor özelliğini devreye almak için kullanılacak komutlar bulunmaktadır.

```
monitor session 2 source interface <kaynak interface adı> <kaynak interface no>
monitor session 2 destination interface <hedef interface adı> <hedef interface no>
```

Geleneksel yöntemlere göre, ağ trafiği tcpdump programı ile pcap biçiminde kaydedilecek ve sistem yöneticisi bu dosyayı Ethereal/Wireshark programları ile çözümlemeye çalışacaktır. Küçük miktarda veri trafiği için bu yöntem geçerli olmakla beraber, günümüzün artan veri trafiğini çözümlemek için daha ayrıntılı süreçlere gereksinim duyulmaktadır. Bu süreçler için ticari ürünler kullanılabileceği gibi açık kaynak kodlu yazılımlar da kullanılabilir. Örneğin, kaydedilen trafik bilgisi Argus (http://www.qosient.com/argus/flow.htm) biçimine dönüştürülerek ayrıntılı olarak incelenebilir. Argus, ağ cihazı firmasından bağımsız bir yazılım olduğu için birçok ortamda kullanılabilecektir. Argus yazılımı ile birlikte çeşitli ağ trafiği akış çözümleme programları (ra, racluster, ragraph, ragrep, racount, rahosts …) gelmektedir. Ayrıntılar için bkz [4].

Pcap dosyasından trafik akış bilgisini oluşturarak argus biçimine dönüştürme komutu aşağıda verilmiştir:

```
argus -r tcpdump_dosyasi.pcap -w argus_dosyasi.arg
```

Oluşturulan dosyadan, en fazla trafik yaratan 20 makinayı (kaynak adres, kaynak paket sayısı, hedef paket sayısı, trafik) çıkarmak için aşağıdaki komut kulanılabilir:

```
racluster -n -r argus_dosyası.arg -M rmon -m saddr -w - - ip | rasort -m bytes -w -| ra -N 20 -s saddr spkts dpkts bytes
```

Ağ cihazları, üzerlerinden geçen trafik akış (flow) bilgisini, incelenmesi ve normal dışı davranışlar belirlenmesi için harici bir sunucuya yollayabilir. Cisco yönlendiricilerden trafik akış bilgisi (netflow) alınabilmektedir. Aşağıdaki örnekte, Ethernet1 arayüzünden geçen ağ verisine ait trafik akış bilgisi, FlowSunucuIPAdresi ile belirtilen sunucunun 3737 numaralı ağ kapısına gönderilmektedir.

Cisco cihazlarda devreye almak icin kullanılacak komutlar aşağıdaki gibidir. Flow-export versiyon numarası (Örneğin 1, 5, 9 gibi) , sunucuda kullanılan analiz yazılımın desteğine göre girilmelidir. Bunun yanı sıra, akış bilgisinin gönderileceği sunucu adresi ve port numarası da girilmelidir. Hangi arayüzden dinleme yapılacağı da belirtilmelidir.

```
router(Config)# ip flow-export version  <netflow VersiyonNumarası>

router(Config)# ip flow-export destination <Flow sunucusunu IP adresi>
<Sunucun flow dinlemek icin kullandigi UDP port numarasi>

router(Config)# ip flow-export source <Dinlenecek Arayüz Adi>
```

Akış bilgisinin alınacağı interface'e girilir ve akış bilgisinin alınacağı tanımlanır. Eger kullanılan cihaz 7200,7500 gibi güçlü bir cihaz ise WAN veya LAN interface'inde aşağıdaki komutlar girilir:

```
router(Config-if)# ip flow ingress
router(Config-if)# ip flow egress
```

Eğer küçük bir yönlendirici ise (Örn: 2800), komut sadece in yönünde uygulanabilir. Eğer bu cihazda hem "download" hem de" upload" trafiğini dinlemek istiyorsan, hem WAN hemde LAN interface'ine girip aşağıdaki komut yazılmalıdır.

```
router(Config-if)# ip route-cache flow
```

Daha etkin akış yönlendirmesi için timeout değerleri aşağıdaki şekilde değiştirilebilir:

```
router (config)# ip flow-cache timeout active 1
router (config)# ip flow-cache timeout inactive 15
```

Gönderilen akış bilgisi çeşitli yazılımlarla incelenebilir. http://www.networkuptime.com/tools/netflow/ adresinde kullanılabilecek yazılımlar listelenmiştir. Scrutinizer yazılımının ücretsiz sürümü, kurulum ve kullanım açısından etkin bir çözümdür.

Trafik akış analizi ile fazla paket ve fazla trafik yaratan makineler takip edilebilir. Bu tür ağın çalışmasına zarar verebilecek makineler, 4.2.2'de belirtildiği şekilde akıllı yerel ağ cihazları üzerinden kapatılmalıdır. Bu akış bilgilerini analiz edebilen açık kaynak kodlu birden fazla yazılım vardır. [26] numaralı referanstan bu yazılımların listesi temin edilebilir.

4.4.4 DNS Sunucu

Zararlı yazılımların bir kısmı IRC kanalları ile yönetilmektedirler [27]. Yazılım önceden belirlenmiş domain adı ile belirli bir IRC sunucusuna bağlanır ve istenen komutları alır. İletişimi sağlayan IRC sunucusuna dinamik DNS adreslemesi ile ulaşmalarını engelleyerek, özellikle botnet türündeki kötü yazılımların etkinlikleri engellenebilir. Tabii ki bu önlemler de, muhtemelen bir sonraki nesil botnet'lerde geçersiz kalacaktır.

DNS sunucularını, zararlı yazılımlardan dolayı üzerlerine gelebilecek gereksiz trafik yükünü azaltmak için RFC 3704'de [11] tarif edildiği gibi kaynağı olmayan 0.0.0.0/8, 10.0.0.0/8, 192.168.0.0/16, 127.0.0.0/8 ve 169.254.0.0/16 adresleri bloklanmalıdır. [13,28]

Ayrıca DNS sunucularına saldırı gibi gelebilecek istekleri gözlemliye bilmek için "dnstop" gibi açık kaynak kodlu yazılımlar kullanılabilir. [29]

4.4.5 Arp Saldırılarını Tespit Edebilen Uygulamalar

Son dönemde arp zehirlemesi tekniği, kötü amaçlı yazılımlar tarafından da kullanılan bir teknik haline gelmiştir. Bu teknik ile aradaki adam saldırısı ile (man in the middle attack) hedef bilgisayarın bütün veri akışı dinlenebilmektedir. Arp tabanlı bu türden saldırılar için Arpwatch gibi uygulamalar bize yardımcı olabilecek açık kaynak kodlu yazılımlardır. Arpwatch ile ağdaki ARP aktiviteleri izlenerek loglanabilir.[30]

5 SONUÇ

Bruce Schneier'in de belirtiği gibi "Güvenlik bir ürün değil, bir süreçtir." Kurumsal ağların ayakta tutulabilmesi için yapılması gerekenler bu bildiride özetlenmiştir. Ciddi yatırımlarla yapılabilecek önlemler var olduğu gibi; açık kaynak kodlu çözümler ve kurumsal bilinçlendirme ile birçok güvenlik ihlalinin önüne geçmek mümkündür.

Bu rapor, sürekli olarak yenilenmekte ve yeni bölümler eklenmektedir. Botnet 'ler hakkındaki kısım en kısa zaman içerisinde bu belgeye eklenecektir. Belgeye her türlü katkınızı bekliyoruz.

6 KAYNAKLAR

[1] Karaarslan E., 2008, Doktora Tezi

[2] Magiera J., Pawlak A., 2005, Security Frameworks for Virtual Organizations, In Virtual Organizations: Systems and Practices, Springer

[3] Deep Rants; CYA from botnets to phisherZ, Malware Acquisition postponed, http://isc.sans.org/diary.html?storyid=621

[4] Karaarslan E., Ağ Güvenlik Takibi(Network Security Monitoring) Süreçleri, http://blog.csirt.ulakbim.gov.tr/?p=38

[5] Karaarslan E., Yama Yönetimi, ULAK-CSIRT, http://csirt.ulakbim.gov.tr/dokumanlar/YamaYonetimi.pdf

[6] Akın G., Cisco Switchlerde MAC Adresi Güvenliği ile Kullanıcı Takibi http://blog.csirt.ulakbim.gov.tr/?p=59

[7] PPP Extensible Authentication Protocol (EAP), http://www.ietf.org/rfc/rfc 2284.txt

[8] Demir H., IEEE 802.1X ve Kurulumu http://blog.csirt.ulakbim.gov.tr/?p=52

[9] Akın G., Anahtarlama Cihazlarındaki Traffic Storm Control Özelliği http://blog.csirt.ulakbim.gov.tr/?p=55

[10] Akın G., Cisco Cihazlarda VLAN veya Fiziksel Interface Bazında Alınabilecek Güvenlik Önlemleri, http://blog.csirt.ulakbim.gov.tr/?p=69

[11] RFC3704, Ingress Filtering for Multihomed Networks, http://www.ietf.org/rfc/rfc3704.txt

[12] Kulduk S., Karaarslan E., Yönlendirici Güvenliği, Akademik Bilişim 2004, http://csirt.ulakbim.gov.tr/dokumanlar/RouterGuvenligi.pdf

[13] Akın G., Marslılar Aramızda, http://blog.csirt.ulakbim.gov.tr/?p=53

[14] Karaarslan E., Cisco cihazlarda QOS uygulaması - UBRL, http://blog.csirt.ulakbim.gov.tr/?p=60

[15] Kırık Ö. , FreeBSD sistemlerde IPFIREWALL Kurulumu ve Konfigürasyonu, Akademik Bilişim 2003, http://ab.org.tr/ab03/tammetin/32.pdf

[16] Karaarslan E., OSI 2. Seviye Güvenliği, http://blog.csirt.ulakbim.gov.tr/?p=29

[17] Cisco arp çözümleri veye IP table dokumanı

[18] Karaarslan E., Ağ Güvenlik Duvarı Çözümü Oluştururken Dikkat Edilmesi Gereken Hususlar, http://csirt.ulakbim.gov.tr/dokumanlar/GuvenlikDuvariCozumuOlusturmaSureci.pdf

[19] Linux Belgelendirme Çalışma Grubu, Posta Sunucuları için Spam Önleme Araçları Clamav Antivirus, http://belgeler.org/howto/antispam-clamav.html

[20] Demirkol Ö. E., Snort 2.3 ve Acid Kurulumu, http://csirt.ulakbim.gov.tr/dokumanlar/SnortKurulum.pdf

[21] Karaarslan E., Zararlı yazılımla (malware) mücadelede honeypot kullanımı, http://blog.csirt.ulakbim.gov.tr/?p=61

[22] Soysal M. , Bektaş O., HoneyWall Kurulumu,
http://csirt.ulakbim.gov.tr/dokumanlar/HoneyWall.pdf
[23] Karaarslan E., Merkezi Loglama, http://blog.csirt.ulakbim.gov.tr/?p=68
[24] Karaarslan E., Swatch ile log dosyalarını takip etme,
http://blog.csirt.ulakbim.gov.tr/?p=67
[25] Cisco cihazlarda Nat loglaması
[26] Demir H.Flow toplama gereçleri, http://blog.csirt.ulakbim.gov.tr/?p=50
[27] Akın G. , Güneş A., Bir Wormun Anatomisi, Akademik Bilişim 2007,
http://csirt.ulakbim.gov.tr/dokumanlar/BirWormunAnatomisi.pdf
[28] Demir H. , BIND ile RFC 1918 IP Adresleri,
http://blog.csirt.ulakbim.gov.tr/?p=51
[29] Demir H. , dnstop, http://blog.csirt.ulakbim.gov.tr/?p=66
[30] Demir H. , arpwatch, http://blog.csirt.ulakbim.gov.tr/?p=54
[31] Önal H., http://blog.lifeoverip.net/index.php/2007/06/06/log-dosyalarina-aktif-izleme/
[32] Ranum M., System Logging and Log Analysis,
http://www.ranum.com/security/computer_security/archives/logging-notes.pdf
[33] Chuvakin A., Advanced Log Processing
http://www.securityfocus.com/infocus/1613
[34] http://www.loganalysis.org/
[35] Bird T., The Top 10 Log Entries that show You've Been Hacked,
http://www.loganalysis.org/presentations/syslog_sans_webcast.pdf
[36] Syslog Faq, http://www.campin.net/syslog-ng/faq.html