Güvenlik Riskleri ve Saldırı Yöntemleri

Fatih Özavcı
Security Analyst

holden@siyahsapka.com
http://www.siyahsapka.com
http://www.dikey8.com

Sunu İçeriği

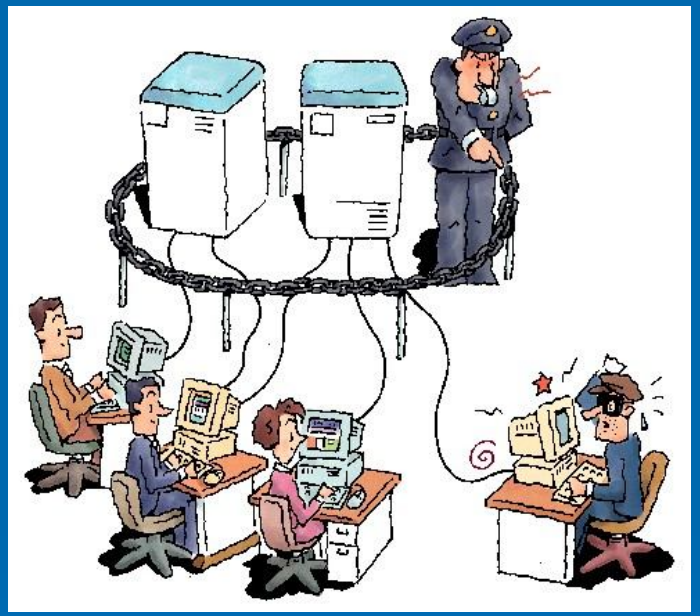
- Bilgi Güvenliği Kavramı ve Kapsamı
- Risk ve Tehditler
- Saldırı ve Saldırgan Kavramları / Gelişimleri
- Saldırgan Amaçları ve Ağdaki Hedefler
- Saldırı Yöntemleri ve Önlemler
- Görülebilecek Zararın Boyutu
- Genel Güvenlik Önlemleri

Bilgi Güvenliği Kavramı

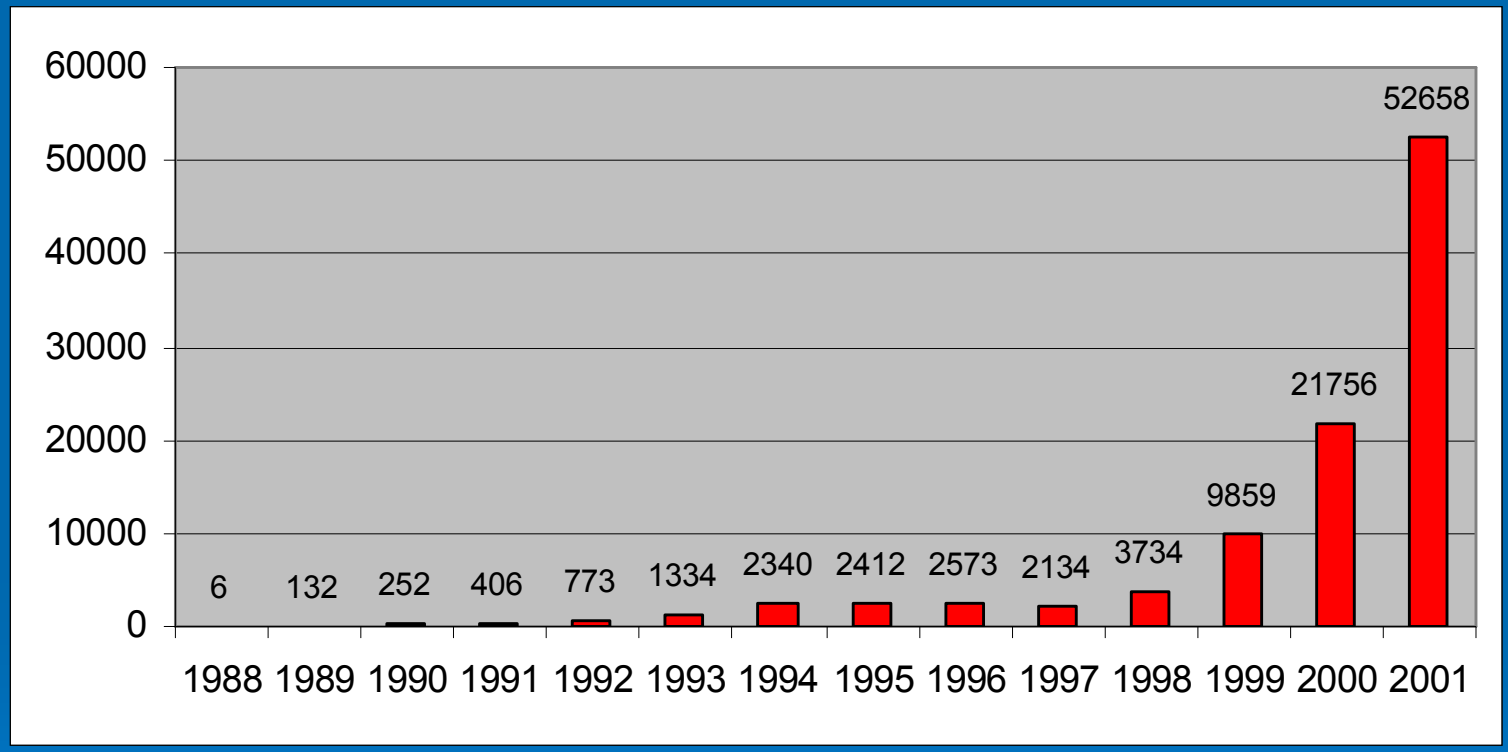
Bilişim ürünleri/cihazları ile bu cihazlarda işlenmekte olan verilerin bütünlüğü ve sürekliliğini korumayı amaçlayan çalışma alanıdır.

Bilgi Güvenliğinin Amacı

- Veri Bütünlüğünün Korunması
- Erişim Denetimi
- Mahremiyet ve Gizliliğin Korunması
- Sistem Devamlılığının Sağlanması



Cert/CC Yıllara Göre Rapor Edilen Olay Sayısı



Tehdit Türleri

Dahili Tehdit Unsurları

- Bilgisiz ve Bilinçsiz Kullanım
- Kötü Niyetli Hareketler

Harici Tehdit Unsurları

- Hedefe Yönelmiş Saldırılar
- Hedef Gözetmeyen Saldırılar

~ % 80 ~ % 20

Güvenlik Riskleri ve Saldırı Yöntemleri – Nisan 2002

Dahili Tehdit Unsurları

- Bilgisiz ve Bilinçsiz Kullanım
  - Temizlik Görevlisinin Sunucunun Fişini Çekmesi
  - Eğitilmemiş Çalışanın Veritabanını Silmesi

- Kötü Niyetli Hareketler
  - İşten Çıkarılan Çalışanın, Kuruma Ait Web Sitesini Değiştirmesi
  - Bir Çalışanının, Ağda "Sniffer" Çalıştırarak E-postaları Okuması
  - Bir Yöneticinin, Geliştirilen Ürünün Planını Rakip Kurumlara Satması

Harici Tehdit Unsurları

- Hedefe Yönelmiş Saldırılar
  - Bir Saldırganın Kurum Web Sitesini Değiştirmesi
  - Bir Saldırganın Kurum Muhasebe Kayıtlarını Değiştirmesi
  - Birçok Saldırganın Kurum Web Sunucusuna Hizmet Aksatma Saldırısı Yapması

- Hedef Gözetmeyen Saldırılar
  - Virüs Saldırıları (Melissa, CIH – Çernobil, Vote)
  - Worm Saldırıları (Code Red, Nimda)
  - Trojan Arka Kapıları (Netbus, Subseven, Black Orifice)

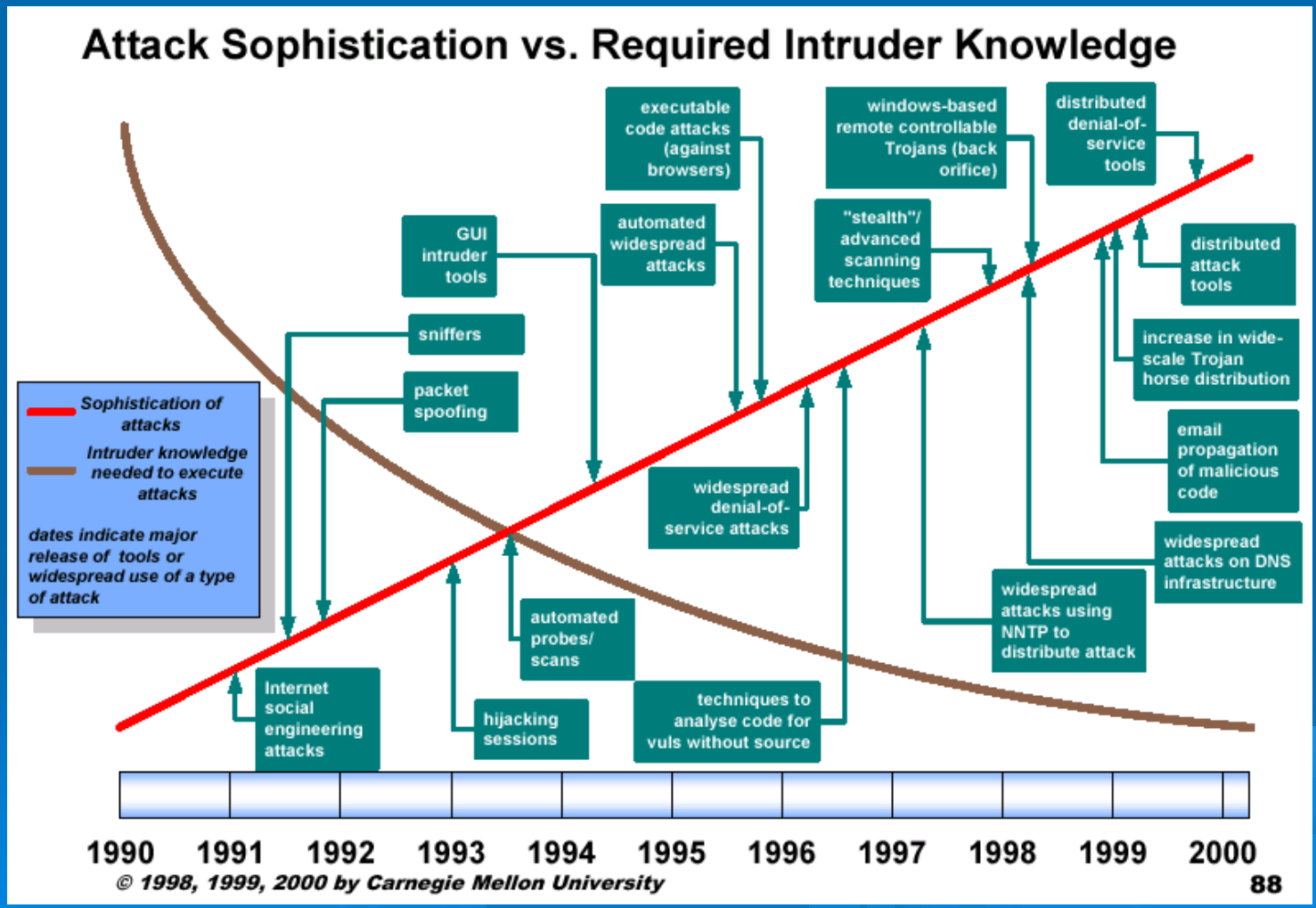
Saldırı Kavramı

Kurum ve şahısların sahip oldukları tüm değer ve bilgilere izinsiz erişmek, zarar vermek, maddi/manevi kazanç sağlamak için bilişim sistemleri kullanılarak yapılan her türlü hareket dijital saldırı olarak tanımlanabilir.

Saldırgan Türleri

- Profesyonel Suçlular
- Genç Kuşak Saldırganlar
- Kurum Çalışanları
- Endüstri ve Teknoloji Casusları
- Dış Ülke yönetimleri

Saldırı Kalitesi ve Saldırgan Yeteneklerinin Gelişimi (CERT/CC)



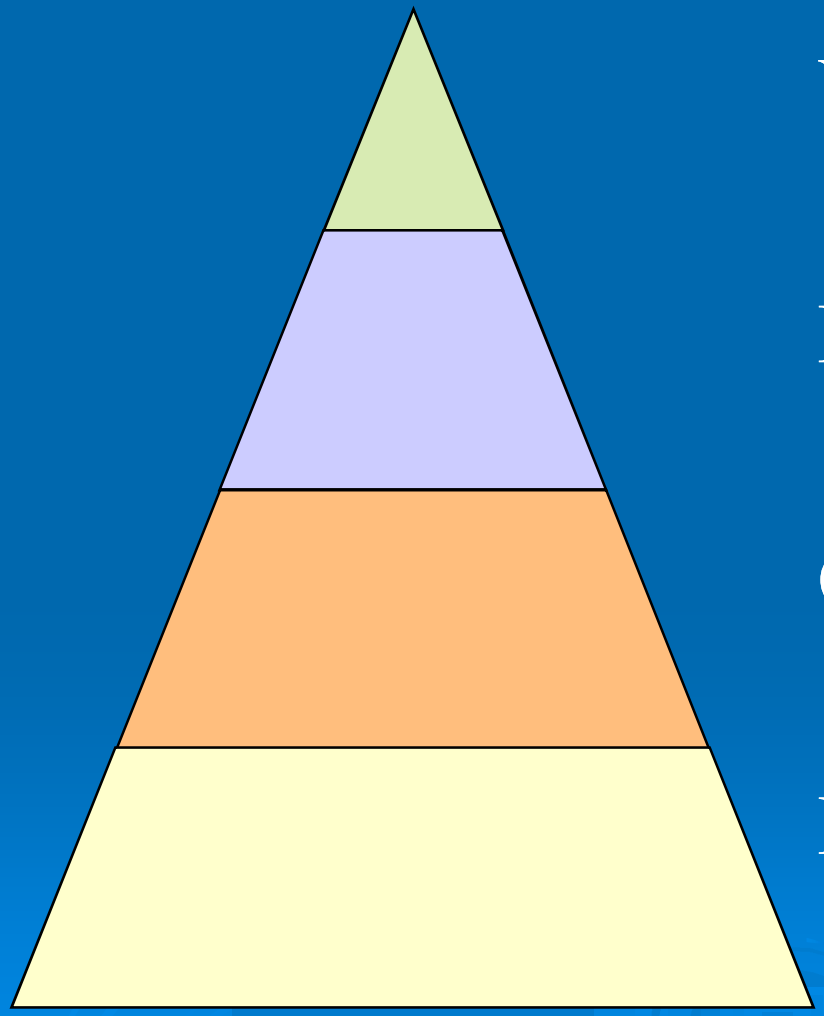
Saldırgan Kaliteleri ve Tahmini Sayıları

Çok Tehlikeli — Yüzlerce

Yırtıcı — Binlerce

Orta Seviye — Onbinlerce

Başlangıç Düzeyinde — Milyonlarca



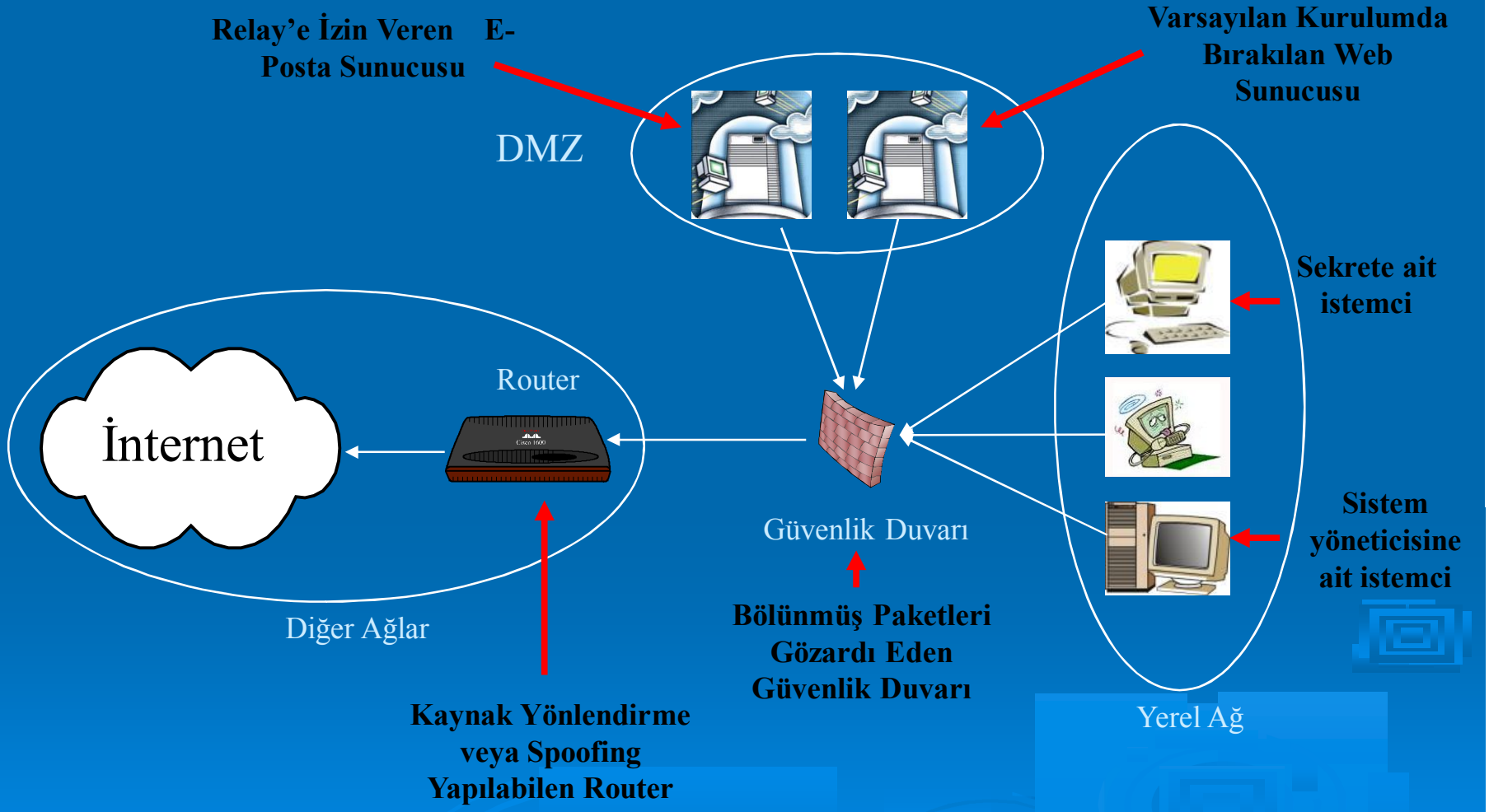
Güvenlik Riskleri ve Saldırı Yöntemleri – Nisan 2002

Carnegie Mellon University (1998-1999-2000)

Saldırgan Motivasyonu

- Maddi Menfaatler
- Rekabet Avantajı
  - Politik
  - Ekonomik/Ticari
- Ek Kaynaklara Erişme İsteği
- Kişisel Öfke veya İntikam
- Merak veya Öğrenme İsteği
- Dikkatsiz Davranışlar

Ağda Bulunan ve Potansiyel Risk İçeren Sistemler



Saldırı Yöntemleri

- Hizmet Aksatma Saldırıları
- Dağıtık Hizmet Aksatma Saldırıları
- Ticari Bilgi ve Teknoloji Hırsızlıkları
- Web Sayfası İçeriği Değiştirme Saldırıları
- Kurum Üzerinden Farklı Bir Hedefe Saldırmak
- Virüs , Worm , Trojan Saldırıları
- İzinsiz Kaynak Kullanımı

Saldırılarda Sıkça Kullanılan Teknikler

- Sosyal Mühendislik
- Ağ Haritalama
- Uygulama Zayıflıkları
- Yerel Ağ Saldırıları
- Spoofing
- Hizmet Aksatma Saldırıları (Dos , DDos)
- Virüs, Worm , Trojan Kullanımı

Sosyal Mühendislik

- İnsan ilişkilerini veya insaların dikkatsizliklerini kullanarak kurum hakkında bilgi toplamak olarak tanımlanabilir
- Amaç kurum yapısı, kurumsal ağın yapısı, çalışanların/yöneticilerin kişisel bilgileri, şifreler ve saldırıda kullanılabilecek her türlü materyalin toplanmasıdır
- Kuruma çalışan olarak sızmak, çalışanlarla arkadaş olmak, teknik servis yada destek alınan bir kurumdan arıyormuş gibi görünerek bilgi toplamak, bilinen en iyi örnekleridir

Sosyal Mühendislik – Önleme Yöntemleri

- Telefonda kuruma ait bilgiler, karşıdaki kişinin doğru kişi olduğuna emin olmadan verilmemelidir
- Çalışanları kuruma dahil ederken özgeçmişleri, alışkanlıkları ve eğilimleri mutlak incelenmelidir
- Kurum çöpleri (büro malzemeleri, not kağıtları, bordolar vs.) tamamen kullanılmaz hale getirilmeli daha sonra atılmalıdır
- Sistem yöneticilerinin, kurumsal bilgileri posta listelerinde, arkadaş ortamlarında ve benzeri yerlerde anması önlenmelidir
- Önemli sunuculara fiziksel erişimin olduğu noktalarda biometrik doğrulama sistemleri (retina testi, parmak izi testi vs.) ve akıllı kart gibi harici doğrulama sistemleri kullanılmalıdır

Ağ Haritalama

- Hedef ağda bulunan bileşenleri ve bu bileşenlere erişim haklarını saptamak için yapılmaktadır
- Aktif sistemlerin belirlenmesi, işletim sistemlerinin saptanması, aktif servislerin belirlenmesi ve bu bileşenlerin ağ üzerindeki konumlarının belirlenmesi gibi aşamalardan oluşur
- Saldırgan, hedef ağın yöneticisi ile aynı bilgi seviyesine ulaşana kadar bu süreç devam etmektedir
- Otomatize edilmiş yazılımlar ile yapılabilmektedir

Ağ Haritalamada Ulaşılmak İstenen Bilgiler

- Hedef ağdaki tüm bileşenler
- Hedef ağa ait olan alan adı, IP aralığı ve internet erişim hattının ait olduğu kurumlar, kişiler, bitiş süreleri
- Hedef ağdaki aktif bileşenlerin işletim sistemleri, sürümleri, yama seviyesi
- Sunucu sistemler üzerinde çalışan servisler, kullanılan uygulamalar ve yama seviyeleri
- Hedef ağdaki tüm bileşenlere ve servislere erişim haklarının belirlenmesi
- Hedef ağdaki tüm güvenlik uygulamaları, erişim listeleri, sürümleri, yama seviyeleri
- Hedef ağdaki aktif bileşenlerin ağdaki yerleşimi

Ağ Haritalamada Kullanılan Teknikler

- Sosyal Mühendislik
- Ping Taraması (Ping Sweep)
- Port Tarama (Port Scanning)
- İşletim Sistemi Saptama (Os Fingerprinting)
- Servis Açılış Mesajlarını Yakalama (Banner Grabing)
- Yol Haritası Belirleme (Tracerouting)
- Güvenlik Duvarı Kural Listesi Belirleme (Firewalking)
- Saldırı Tespit Sistemi Saptama/İnceleme

Ağ Haritalama – Önleme Yöntemleri

- Güvenlik Duvarı üzerinde, ağın devamlılığı için gerekli olmayan, internetten ağa yönelik her türlü IP paketini engelleyecek kurallar belirlemek
- Güvenlik Duvarını uygulama seviyesinde kullanmak veya ağdaki işletim sistemlerini ele vermeyecek şekilde yapılandırmak
- Güvenlik Duvarı üzerinde, ağdaki bileşenlerden, internetteki sistemlere ICMP hata mesajları gönderilmesini engellemek
- Sunucu ve servis sunan uygulamalardaki tüm açılış/hata mesajlarını değiştirmek, yok etmek
- Saldırı Tespit Sistemlerini gerekli olmadıkça tepki vermeyecek şekilde yapılandırmak

Uygulama Zayıflıkları

- Servis sunan uygulamalardaki yapılandırma yada programlama hatası sebebiyle oluşur ve sistemde komut çalıştırmaya yada servisin durdurulmasına sebebiyet verir
- Varsayılan yapılandırmayı kullanmak, zayıf şifreler belirlemek ve erişim hakları belirlememek en çok karşılaşılan yanlış yapılandırma örnekleridir
- Klasör dışına geçebilmek, bellek taşırmak, yazılımda erişim sınırlaması bulundurmamak ve normal dışı isteklere karşı önlem almamak ise en sık karşılaşılan programlama hatalarıdır

Uygulama Zayıflıkları – Önleme Yöntemleri

- Uygulamaların yeni sürümlerini kullanmak, yayınlanan tüm yamaları uygulamak
- Varsayılan yapılandırmayı değiştirmek ve kuruma/servise özel bir yapılandırma benimsemek
- Kolay tahmin edilemeyecek şifreler seçmek ve uygulamaya özel erişim haklarının belirlenmesini sağlamak
- Uygun şekilde yapılandırmak şartıyla, uygulama seviyesinde güvenlik duvarları, uygulama geçitleri ve saldırı tespit sistemleri kullanmak

Yerel Ağ Saldırıları

- Yerel ağda bulunan kullanıcıların, sahip oldukları hakları kötü niyetli kullanması sonucu oluşmaktadır
- Amaç genelde diğer çalışanların e-postalarını okumak, yöneticilerin şifrelerini yakalamak, kuruma veya farklı bir çalışana ait bilgilerin incelenmesi olmaktadır
- Paket yakalamak, oturum yakalamak, oturumlara müdahale etmek en sık kullanılan saldırılardır

Yerel Ağ Saldırılarında Kullanılan Teknikler

- Sniffer kullanarak paket yakalamak
- Switch'li ağlarda ARP Spoofing yaparak paket yakalamak
- Yakalanan paketlerin ait olduğu oturumları yakalamak ve müdahale etmek
- SSH ve SSL oturumlarını yakalamak, güvenli sanılan oturumlardan veri çalmak

Yerel Ağ Saldırıları – Önleme Yöntemleri

- Hub kullanılan ağlarda Switch kullanımına geçmek
- Switch'leri her porta bir MAC adresi gelecek yapılandırmak, kaliteli Switch'ler kullanarak MAC adresi tablosunun taşmamasını sağlamak
- Ağ üzerindeki tüm istemcilerde statik ARP tabloları oluşturmak ve değişiklikleri izlemek
- SSH / SSL kullanılan oturumlarda en yeni sürümleri ve en yeni şifreleme algoritmalarını kullanmak
- Gerekli görülen durumlarda harici doğrulama sistemleri kullanmak

Spoofing

- Basitçe kaynak yanıltma olarak tanımlanabilir
- Genelde hedeften ek haklar kazanmak, saldırı suçundan farklı kişilerin/kurumların sorumlu olmasını sağlamak, kendini gizlemek veya dağıtık saldırılar düzenlemek için kullanılmaktadır
- Çeşitli protokollerde, doğrulama sistemlerinde ve uygulamaya özel işlemlerde uygulanabilmektedir

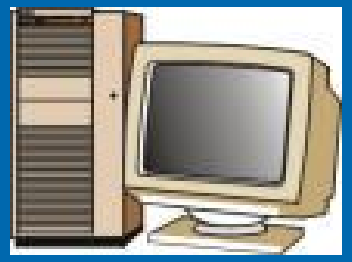
Spoofing Teknikleri

- MAC adreslerinin fiziki olarak değiştirilmesi veya ethernet paketlerindeki değişiklikler ile MAC Spoofing yapılabilir
- ARP protokolündeki paketlerde IP/MAC adresleri eşleşmesini yanıltarak ARP Spoofing yapılabilir
- IP Paketlerindeki kaynak IP adresini değiştirerek IP Spoofing yapılabilir
- DNS sunucularını ele geçirerek veya sorgulara sahte cevaplar vererek DNS spoofing yapılabilir
- Web sunucudan alınmış cookie'nin kopyalanması suretiyle kimlik yanıltması yapılabilir
- Parmak izi sistemlerinde, daha önce alınmış parmak izi örneği kullanılarak yapılabilir

Spoofing – Örnek Spoofing İşlemi

Yerine Geçilecek Sistem

Saldırılacak Sistem



1

Devre Dışı Kal

2

Ben “O”yum

Saldırgan

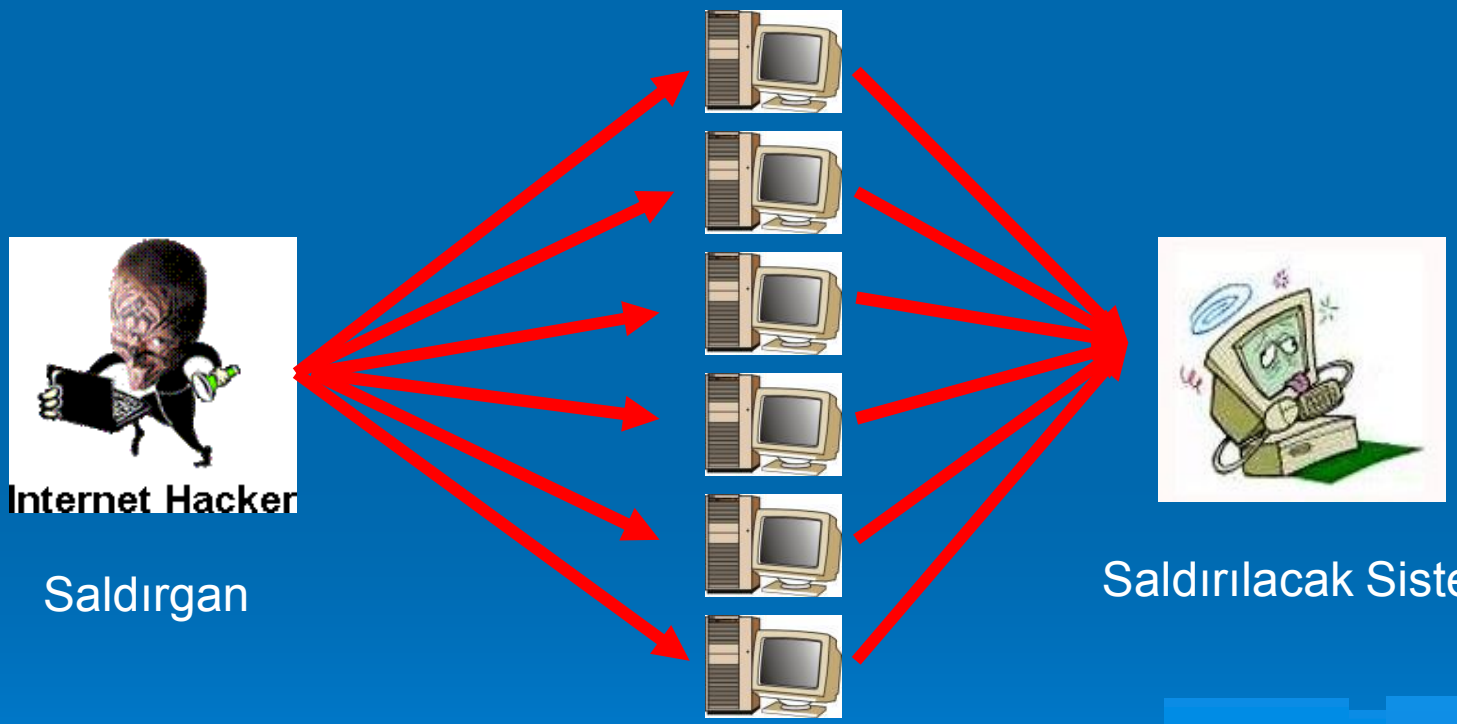
Spoofing – Önleme Yöntemleri

- Harici doğrulama sistemleri kullanmak
- IP, DNS, ARP, MAC adresleriyle doğrulama kullanan servisleri devre dışı bırakmak
- Statik ARP tabloları kullanmak, Switch'lerde her porta bir MAC adresi eşleşmesini sağlamak ve Swtich'leri tablo taşmalarından korumak
- Ters sorguları aktif hale getirmek (RDNS, RARP vb.)
- Doğrulama bilgilerinin (şifre, dosyalar vb.) istemci sisteminde tutulmasını engellemek

Hizmet Aksatma Saldırıları

- Protokol, işletim sistemi veya uygulamada bulunan zayıflıkların sonucunda, sunucunun servis veremez hale getirilmesidir
- Hedef bir sunucu, servis, uygulama veya ağın devre dışı bırakılması olabilir
- Tek merkezli yada çok merkezli olarak yapılabilir

Dağıtık Hizmet Aksatma Saldırıları

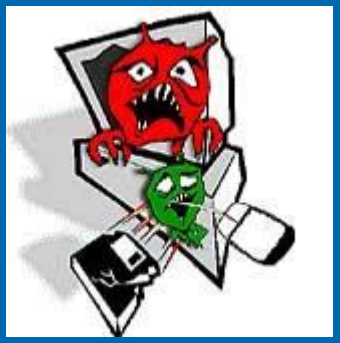


Hizmet Aksatma Saldırıları – Önleme Yöntemleri

- Uygulama ve işletim sistemlerinin yayınlanmış tüm güncelleme/yamaları uygulanmalı, yeni sürümlerle hizmet verilmelidir
- Uygulama seviyesinde güvenlik duvarları kullanılmalı ve uygulamalara yönelik tek merkezli saldırılar takip edilmelidir
- Güvenlik Duvarı üzerinde, ağın devamlılığı için gerekli olmayan, internetten ağa yönelik her türlü IP paketini engelleyecek kurallar belirlenmelidir
- Dağıtık saldırılardan korunmak için, internet servis sağlayıcısına iki yönlendirici ile bağlanılmalı ve biri devre dışı kaldığında diğeri devreye sokulmalıdır (Kısmi olarak çözüm sağlamaktadır)

Virüs, Worm ve Trojan Tehlikeleri

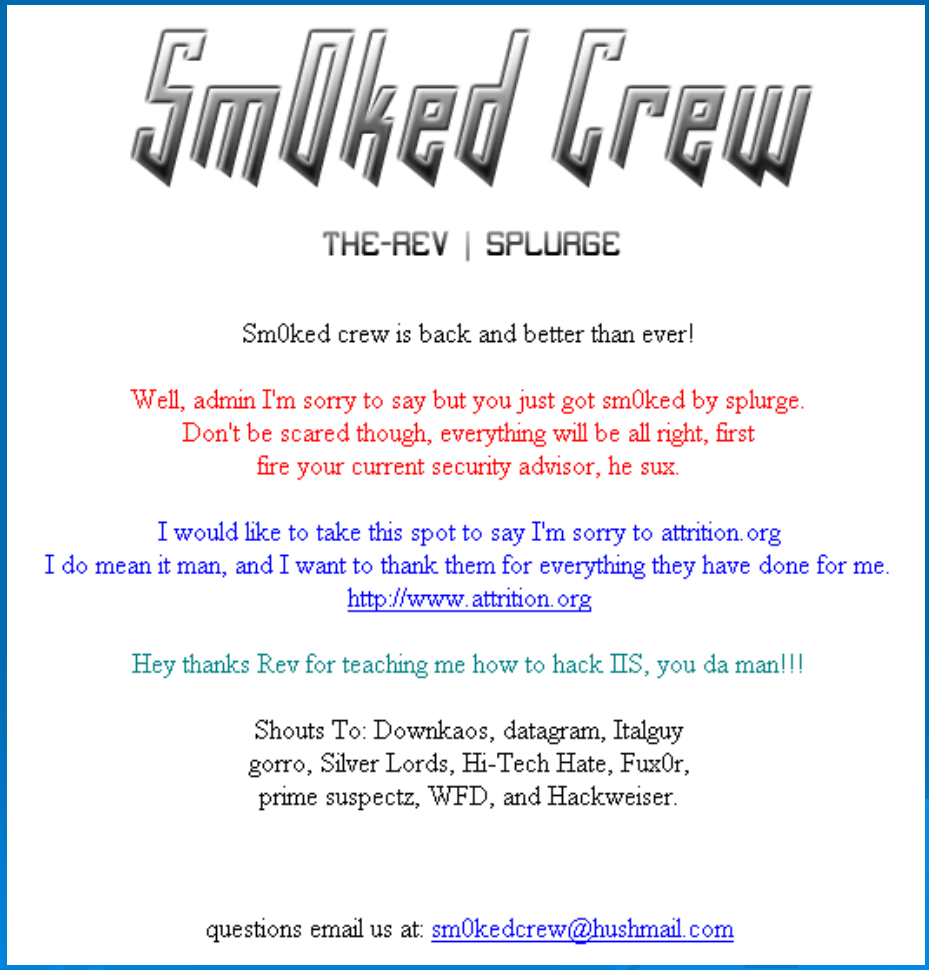
- Virüs, Worm ve Trojan'lar hedef gözetmeksizin bulaşan ve genelde sistemin işleyişini durdurmaya çalışan küçük yazılımlardır
- Virüs'ler e-posta, veri taşıma ortamları (disket, cd, dvd vb.) ve web sayfaları ile yayılabilir (Melisa, CIH)
- Worm'lar, Virüs'lerin kullandıkları yöntemlere ek olarak, uygulama/işletim sistemi zayıflıkları ile saldırılar düzenleyebilir ve bu şekilde de yayılabilir (Code Red, Nimda)
- Trojan'lar ancak ilgili uygulama çalıştırıldığında etkili olmaktadır (Netbus, Subseven)



Virüs, Worm ve Trojan'ları Önleme Yöntemleri

- Anti-Virüs sistemleri, tüm istemci ve sunucuları koruyacak şekilde kullanılmalıdır
- Worm saldırılarını engelleyebilmek için Saldırı Tespit Sistemleri (eğer mümkün ise Güvenlik Duvarı) üzerinde önlemler alınmalıdır
- İnternet üzerinden kurumsal ağa gelen FTP, HTTP, SMTP, POP3, IMAP gibi protokollere ait paketler Anti-Virüs sistemleri tarafından incelenmeli, mümkün ise Anti-Virüs ağ geçidi kullanılmalıdır

Web Sayfası Değişimleri – NY Times 15/2/2001



Sm0ked Crew

THE-REV | SPLURGE

Sm0ked crew is back and better than ever!

Well, admin I'm sorry to say but you just got sm0ked by splurge.
Don't be scared though, everything will be all right, first
fire your current security advisor, he sux.

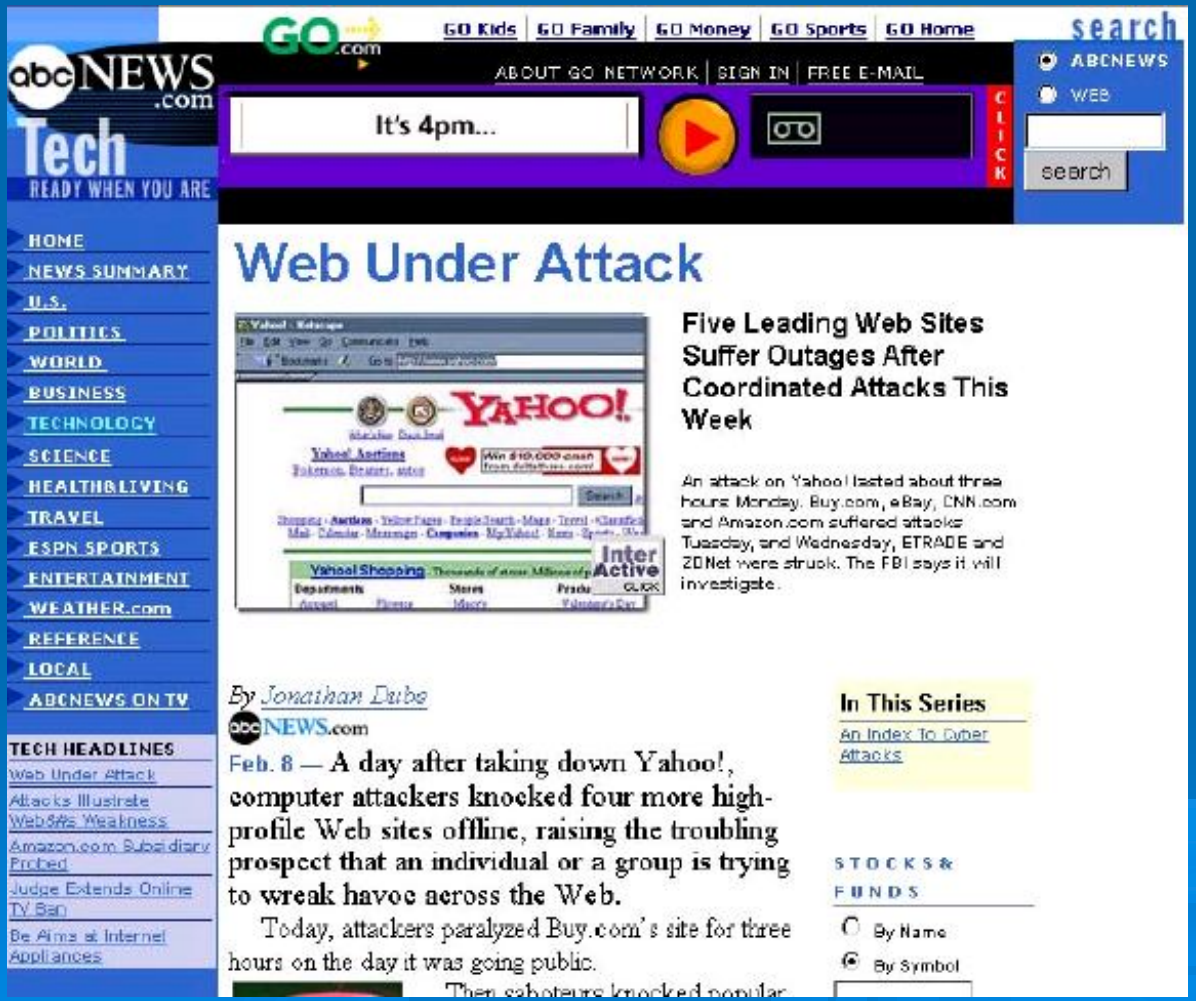
I would like to take this spot to say I'm sorry to attrition.org
I do mean it man, and I want to thank them for everything they have done for me.
http://www.attrition.org

Hey thanks Rev for teaching me how to hack IIS, you da man!!!

Shouts To: Downkaos, datagram, Italguy
gorro, Silver Lords, Hi-Tech Hate, Fux0r,
prime suspectz, WFD, and Hackweiser.

questions email us at: sm0kedcrew@hushmail.com

Web Sayfası Değişimleri – Yahoo 7/2/2000



Web Sayfası Değişimleri – nukleer.gov.tr 29/11/99

Web Sayfası Değişimleri – healt.gov.tr 11.27.1999

WE BROKE INTO TURKEY'S NUCLEAR LAB (www.nukleer.gov.tr) BUT WE DECIDED TO GO FOR TURKEY'S HEALTH PAGE TOO!

OySTr n KLaM hacking the health of TURKEY

GOBBLE GOBBLE, j00 g0t h4ck3d

WATCH OUT YOUR COUNTRY IS NEXT!

Web Sayfası Değişimleri – tk.gov.tr 4/11/2001

Web Sayfası Değişimleri – tapu.gov.tr 4/7/2001

Saldırıya Uğrayabilecek Değerler

- Kurum İsmi, Güvenilirliği ve Markaları
- Kuruma Ait Özel / Mahrem / Gizli Bilgiler
- İşin Devamlılığını Sağlayan Bilgi ve Süreçler
- Üçüncü Şahıslar Tarafından Emanet Edilen Bilgiler
- Kuruma Ait Adli, Ticari Teknolojik Bilgiler

Görülebilecek Zararın Boyutu

- Müşteri Mağduriyeti
- Kaynakların Tüketimi
- İş Yavaşlaması veya Durdurulması
- Kurumsal İmaj Kaybı
- Üçüncü Şahıslara Karşı Yapılacak Saldırı Mesuliyeti

Güvenlik İhtiyacının Sınırları

Saldırıya Uğrayabilecek Değerlerin, Kurum İçin Arzettiği Önem Seviyesi Güvenlik İhtiyacının Sınırlarını Belirlemektedir.

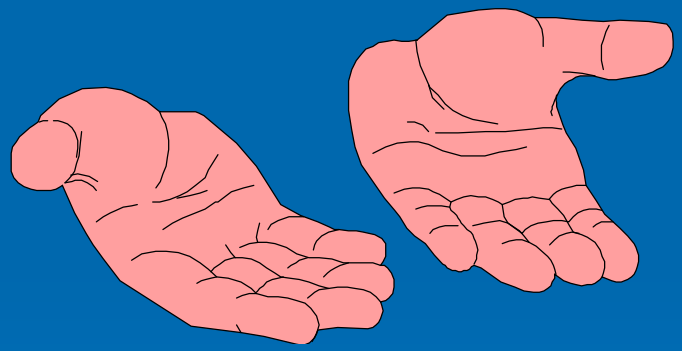
Genel Güvenlik Önlemleri

- Bir Güvenlik Politikası Oluşturulmalı
- Tüm Ağ Sorun Kaldırabilecek Şekilde ve Politikada Belirlendiği Gibi Yapılandırılmalı
- Düzenli Olarak Yedekleme Yapılmalı ve Yedekler Kontrol Edilmeli
- Gerek Duyulan Güvenlik Uygulamaları Kullanılmalı
  - Güvenlik Duvarı
  - Saldırı Tespit Sistemi
  - Anti-Virüs Sistemi
- Ağ Düzenli Olarak Denetlenmeli ve İzlenmeli
- Çalışanlar Politikalar ve Uygulamalar Konusunda Eğitilmeli

Kaynaklar

CERT	– http://www.cert.org
SANS	– http://www.sans.org
Security Focus	– http://www.securityfocus.com
Siyah Şapka	– http://www.siyahsapka.com
Dikey8	– http://www.dikey8.com
Olympos	– http://www.olympos.org
Güvenlik Haber	– http://www.guvenlikhaber.com
Alldas.org – Defacement Archive	– http://defaced.alldas.org/?tld=tr
Attrition.org – Defacement Archive	– http://www.attrition.org/mirror/attrition/tr.html
Security Space	– http://www.securityspace.com

Sorular ?



Teşekkürler ....