GÜVENLİK ARAÇLARI

Erhan Anuk
erhana@be.itu.edu.tr
İTU Bilişim Enstitüsü
Bilgisayar Bilimleri

ÖZ

Güvenlik araçları bir bilgisayar sisteminin güvenilirliğinin sınanmasında çok önemli yer tutarlar. Bu yazıda günümüzde varolan ve en çok kullanılan, genelde ücretsiz yazılımlardan oluşan bazı güvenlik araçlarından bahsedilecektir.

GİRİŞ

Bilgisayar sistemlerinin güvenliklerini sağlama amacıyla birçok çalışma yapılır. Bu çalışmalar genelde sisteme güvenlik duvarları, saldırı tespit sistemleri kurmak, güvenli iletişim protokolleri sağlamak, zarar verici kodlara karşı yazılımlar kullanamak gibi çözümler olabilir. Fakat tüm bu yapılan çalışmalardan sonra bile sistemde saldırganların faydalanabileceği açıklar olabilir. Bu açıklar çeşitli güvenlik araçları kullanılarak tespit edilebilir ve gerekli önlemler alınabilir. Güvenlik araçları ayrıca sistemi izleme olanağıda sunarlar.

Varolan güvenlik araçları genelde bilgisayar sistemlerine saldırı amacıyla geliştirilmiştir. Buradaki temel düşünce sistemin açıklarını saldırganlardan önce ortaya çıkarmak ve gerekli önlemleri almaktır.

Bunadan sonraki bölümlerde çeşitli güvenlik araçları tanıtılacak ve özelliklerinden bahsedilecektir.

NMAP

Nmap (ing. “network mapper”) ağ araştırmasında ve güvenlik denetlemelerinde kullanılan açık kaynak kodlu bir programdır. Geniş ölçekli ağları tarama amacıyla tasarlanmasının yanında tek bir konak üzerinde de verimli bir şekilde çalışabilir. Alışılmışın dışında IP paketleri göndererek ağ üzerinde canlı bilgisayarları gösterir. Ayrıca bu bilgisayarlar üzerindeki ağa sunulan uygulamaları yespit edebilir, hangi işletim sistemi koştuklarını bulabilir, hangi güvenlik duvarını kullandıklarını bulabilir. Nmap birçok işletim sistemi üzerinde çalışabilir ve GNU GPL lisansıyla dağıtılır.

NESSUS

Nessus güçlü ve güncel bir uzaktan tarama aracıdır. Birçok UNIX türevi üzerinde ve Windows'ta çalışabilme özelliğine sahiptir. Nessus uyumlu ek yazılımları Gtk arayüzü ile çok kullanışlı bir güvenlik aracıdır. 1200'ün üzerinde güvenlik açığını yakalayabilir ve bunlar hakkında çeşitli biçimlerde raporlar sunabilir (HTML, LaTeX, ASCII, vs.). Nessus'un önemli özelliklerinden biri bilinenen kurallara bağlı olmadan tarama yapabilmesidir. Örneğin 1234 numaralı portta çalışan bir web sunucusunu tespit edebilir ve güvenlik taramasından geçirebilir. Bulduğu açıklar için kullanıcıya güvenlik çözümleri önerir.

ETHEREAL

Ethereal UNIX ve Windows platformları için ücretsiz bir ağ protokolü analizcisidir. Canlı bir ağdan veya daha önceden diske kaydedilmiş bir ağ verisi üzerinde çalışarak ağ incelemesi yapar. Kullanıcı interaktif bir şekilde incelenen veri hakkında ayrıntılı bir bilgi alabilir. Bu bilgi tek bir paket için de söz konusudur. Güçlü özellikleri arasında zengin bir süzme diline sahip olması ve TCP otrumunu birleştirerek analiz imkanı sağlaması vardır.

SNORT

Snort IP ağları için gerçek zamanlı trafik analizi yapabilen ve paket kaydedebilen açık kaynak kodlu bir sızma belirleme sistemidir. Protokol analizi, içerik araştırması/eşlemesi dahil daha birçok inceleme yaparak saldırıları veya yoklamaları (örn. Tampon taşırma, gizli port taraması, CGI saldırıları, SMB

yoklamaları, OS belirleme, vs.) tespit edebilir. Snort izin verilen veya verilmeyen trafik tanımlanması için esnek bir kural yazma diline ve modüler bir tespit etme motoruna sahiptir. Ayrıca çeşitli alarm mekanizmaları sayesinde herhangi bir saldırı tespitinden sonra kullanıcıyı uyarır.

TCPDUMP

Ağ izleme ve veri inceleme yapmaya olanak veren en eski ve en çok sevilen ağ analiz (dinleme) programıdır. Ağ hareketlerini incelem amacıyla kullanılır. Verilen deyimleri eşleyerek bir ağ arayüzündeki paket bilgilerini gösterebilir. Nmap tcdump'ın altyapısını oluşturan libpcap paket yakalama kkütüphanesini kullanır. Günümüzde tcpdump çok kullanılmamakla beraber ağ incelem için genellikle ethereal kullanılır.

DSNIFF

Dsniff ağ denetlemesi ve içeri sızma testleri yapmaya yarayan bir araçlar takımıdır. Dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf ve webspy gibi programlar içerir ve bu programlar pasif bir şekilde ağı dinleyerek ilgi çeken verinin (şifreler, e-postalar,vs.) yakalanmasını sağlarlar. Arpspoof, dnsspoof, ve macof normalde bir saldırganın erişemeyeceği ağ trafiğine (2. katman) ulaşmasını sağlar. Sshmitm ve webmitm araçları da yönlendirilmiş HTTPS ve SSH bağlantıları için araya girme saldırılarında kullanılır.

GFI LANguard

GFI LANguard windows platformları için ücretli bir ağ güvenliği tarama aracıdır. LANguard ağı tarayarak her makine için çeşitli bilgiler sunar. Bu bilgiler makinelerin hangi servis paketlerini kullandığı, eksik güvelik yamaları, herkese açık paylaşımları, açık portları, çalışan serviler ve uygulamalar, zayıf şifreler gibidir. Tarama sonuçları HTML formatında raporlanır ve sorgulanabilir. Web sayfasında deneme sürümü mevcuttur.

ETTERCAP

Ettercap ethernet ağlarında kullanılan terminal tabanlı bir koklama(sniff)/araya girme/kaydetme aracıdır. Aktif ve pasif olarak şifreli olanlar dahil birçok protokolü izleyebilir ve araya girebilir. Kurulmuş bir bağlantıya veri enjeksiyonu yapma ve hızlı bir şekilde süzme yapma özellikleri vardır. Uyumlu ek yazılımları vardır. Anahtarlamalı ağda olduğunu anlayabilir ve işletim sistemi izlerini kullanarak ağ geometrisini çıkarabilir.

JOHN THE RIPPER

John the Ripper çok güçlü bir şifre kırma aracıdır. Hızlı bir şekilde çalışma ve birden çok platform için şifre özü kırma özelliklerine sahiptir. UNIX'in neredeyse her versiyonu dahil DOS, Windows, BeOS ve OpenVMS'te çalışabilir. Sürekli güncellenen şifre kırmada yeralan şifre dosyaları web sitesinden alınabilir.

TRIPWIRE

Bütünlük kontrolü yapan araçların büyük babası olarak tanımlanan tripwire belirlenen dosya ve dizinlerin zaman içinde bütünlüklerinin bozulup bozulmadığını araştırır. Düzenli bir şekilde sistem dosyalarını kontrol ederek herhangi bir değişiklik halinde sistem yöneticisini uyarır. Linux için ücretsiz bir versiyonu olmakla birlikte diğer platformlar için ücretli bir yazılımdır.

KAYNAKLAR

1. www.insecure.org
2. www.nessus.org
3. www.ethereal.com
4. www.snort.org
5. www.tcpdump.org
6. hhtp://naughty.monkey.org/~dugsong/dsniff
7. www.gfi.com/lannetscan
8. http://ettercap.soureforge.net
9. www.openwall.com/john
10. www.tripwire.com