



Bilgi Güvenliđi Denetim Sürecinde Özgür Yazılımlar

Fatih Özavcı

Bilgi Güvenliđi Danışmanı

fatih.ozavci@gamasec.net

- Kurumların sahip olduđu politikaların ve uygulamalarının, güvenlik perspektifinde deđerlendirilmesi sürecidir.
- Belirli standartlar dođrultusunda yapılabilir
 - Cobit
 - BS7799 / ISO 27001 / TSE 27001
- Sunumun Odađı
 - Yazılımların Güvenlik Denetimi
 - Zaafiyet Deđerlendirme Denetimleri
 - Sisteme / Ađa Sızma Denetimleri
 - Yerel Ađ ve Kablosuz Ađ Denetimi

- Denetim kuruma/sisteme/yazılıma özel olmalıdır, bu nedenle her bir testin özelleştirilmesi gerekmektedir
- Farklı denetim adımlarında alınan çıktıların birleştirilmesi ve beraber değerlendirilmesi gerekmektedir
- Bazı özel testlerin tanımlanabilmesi, kullanılacak test şekillerinin döngülere sokulabilmesi gerekmektedir
- Basit, hızlı ve amaca hizmet eden yazılımlar denetim sürecinin verimini arttırmaktadır
- Kaynak kodu açık, yapılan işlemin net olarak görünebileceği araçlar tercih edilmelidir
- Özgür yazılımlar genellikle bu şartları veya fazlasını sunmaktadır

- **Kaynak Kod Analizi**
 - Kodun Bütünselliği ve Kalitesi
 - Kullanılan Ortak Kütüphane veya Bileşenler
 - Platformun Sunduğu Fonksiyonlar ve Bileşenler

- **Çalışılan Platform Üstünde Analiz**
 - Etki/Tepki Analizi
 - Süreçleri İzleme ve Çözümleme
 - Hata Ayıklama
 - Ağ Protokolü Yakalama ve Çözümleme

- Vi, Grep, Cat, Awk, Sed
- Flawfinder
Kaynak kod açık, GPL, Python ile çalışıyor
C/C++ Kaynak Kod Analizi
<http://www.dwheeler.com/flawfinder/>
- LAPSE: Web Application Security Scanner for Java
Kaynak kod açık, GPL, Eclipse için hazırlanmış ve Java ile çalışıyor
Java J2EE Kaynak Kod Analizi
<http://suif.stanford.edu/~livshits/work/lapse/>
- SWAAT
Kaynak kod açık, SINIRLI LİSANS, .NET ve Mono ile çalışıyor
Java, JSP, ASP.NET ve PHP Kaynak Kod Analizi
http://www.owasp.org/index.php/Category:OWASP_SWAAT_Project

Çalışılan Platform Üzerinde Analiz



- For/While, Grep, Cat, Awk, Sed, Netcat, Strace ...
- BFBTester
 - Kaynak kod açık, GPL, C
 - Komut satırından programların parametrelerinin analizi
 - <http://sourceforge.net/projects/bfbtester/>
- Paros
 - Kaynak kod açık, GPL, Java ile çalışıyor
 - Tüm Web Uygulamaları Denetimi
 - <http://www.parosproxy.org/>
- WebScarab
 - Kaynak kod açık, GPL, Java ile çalışıyor
 - Tüm Web Uygulamaları Denetimi
 - http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
- WSFuzzer
 - Kaynak kod açık, GPL, Python ile çalışıyor
 - SOAP Temelli Web Servislerinin Analizi
 - http://www.owasp.org/index.php/Category:OWASP_WSFuzzer_Project

➤ Sunucu/Ağ Cihazı

➤ Yerel Güvenlik Denetimi

- Dosya Sistemi
- Kullanıcı Yönetimi ve Yetkilendirme
- Yama Yönetimi
- Çalışan Uygulamalar
- Yerel Servisler

➤ Ağ Üzerinden Güvenlik Denetimi

- Ağ Servislerinin Analizi
- Paylaşım ve Haberleşme Yazılımları
- İşletim Sistemi TCP/IP Altyapısı

- For/While, Grep, Cat, Awk, Sed, Netcat
- Sussen
 - 0.35 / GPL
 - OVAL Desteği, Yorumlayıcı/Arabirim
 - <http://dev.mmgsecurity.com/projects/sussen/>
- Nessus
 - 3.x / Non-Commercial
 - NASL, Scada Testleri, Çoklu Platform, Yerel Analiz, 12000+ Test
 - <http://www.nessus.org>
 - 2.2.x / GPL
 - NASL, Açık Kaynaklı, Çoklu Platform, Çok Sayıda Eklenti Desteği, Yerel Analiz
 - <http://www.nessus.org>

- **Sistem Sızma Denetimleri**
 - Güvenlik Açıklarının Doğrulanması
 - Açığın Kullanımı ve Exploit Hazırlanması
 - Kabuk Kodu Kullanımı

- **Ağa Sızma Denetimleri**
 - Yapılandırma Zaafiyetlerinin Doğrulanması
 - Güvenlik Teknolojilerinin Analizi
 - IP Sahteciliği ve TCP/IP Oyunları
 - Kriptolama, Kodlama

- Hping, Nemesis, Isic, Xprobe2, Netcat ...
- Nmap
 - 4.20 / GPL / C
 - Port tarama, servis analizi, işletim sistemi saptama, IP sahteciliği
 - <http://www.insecure.org/nmap/>
- Scapy
 - 1.1.x / GPL / Python
 - Python arayüzü ile diğer araçların kullanımı, kolay programlama
 - <http://www.secdev.org/projects/scapy/>
- Metasploit Framework
 - 3.x / Non-Commercial / Ruby+C+Assembler
 - 177+ Exploit, 104+ Payload, IDS/IPS Modülleri, Kodu Açık Exploitler, Wi-fi
 - <http://www.metasploit.com>
 - 2.7 / GPL / Perl+C+Assembler
 - 130+ Exploit, 40+ Payload, Kodu Açık Exploitler
 - <http://www.metasploit.com>

➤ Yerel Ağ Altyapısı

- IP/MAC Erişim Denetimi Analizi
- Paket Yakalama ve Çözümleme
- ARP Sorguları Analizi

➤ Kablosuz Ağ Altyapısı

- Kablosuz Ağ Haritalama
- IP/SSID/MAC Erişim Denetimlerinin Analizi
- WEP/WPA Analizi
- Erişim Noktaları Analizi
- Kablosuz İstemcilerin Analizi

➤ Yerel Ağ Altyapısı

- Ettercap NG / 0.7.3 / GPL / C

Yerel ağ haritalama, ARP sahteciliği, Oturum Yakalama

<http://ettercap.sourceforge.net/>

- Yersinia / 0.7.1 / GPL / C

Yerel ağ haritalama, ARP sahteciliği, Servis Engelleme

<http://www.yersinia.net/>

➤ Kablosuz Ağ Altyapısı

- Kismet / 2007-1-R1 / GPL / C

Kablosuz ağ ve istemci haritalama, Paket yakalama

<http://www.kismetwireless.net/>

- Aircrack / 0.8 / GPL / C

Kablosuz ağ haritalama, WEP / WPA-PSK Kırma, Sözlük Saldırıları

- Paket Yakalama ve Çözümleme
 - Wireshark, Tcpdump, Ngrep
- Ağ Haritalama Araçları
 - Nmap, Hping, Traceroute, Netcat
- Hızlı Betik Programlama
 - Bash, Ruby, Python, Awk, Sed, Netcat, Grep
- Şifre Kırma
 - Ophcrack, John The Ripper, Aircrack
- Netbios / SNMP
 - Samba, RPCClient, Snmpwalk, Tkined/Scotty
- Denetim Rehberleri
 - ISECOM - OSSTM

- GamaLAB
<http://www.gamasec.net/gamalab.html>
- Enderunix - Belgeler
<http://www.enderunix.org/?lng=tr&page=papers>
- OWASP
<http://www.owasp.org>
- Sectools 2007
<http://sectools.org>
- Open Source Testing - Security
<http://www.opensourcetesting.org/security.php>

Teşekkürler....