Sızma Testleri (Pentest)

2025

Sızma Testi

- Penetration Test
- PenTest
- Sızma Testi
- Yazılım Güvenlik Testi
- Siber Güvenlik Tatbikatı
- Siber Tatbikat

gibi isimlerle de anılmaktadır.

Sızma Testi

Güvenlik uzmanları tarafından gerçekleştirilen, kötü amaçlı bir saldırganın sisteme verebileceği zararları raporlamak ve önceden savunma önlemleri almak amacı ile oluşturulan saldırı denemelerinin tamamıdır. (Burlu, 2010)

Sızma testlerinin amacı, kuruluşlara sistemlerini daha güvenli hale getirmelerinde yardımcı olmaktır.

Sızma Testi

- Beyaz şapkalı hacker,
- Etik hacker,
- Pentester,
- Sızma Testi Uzmanı,

gibi isimler adı altında ifade edilen siber güvenlik uzmanları tarafından gerçekleştirilmektedir.

Uzmanlar belirli kalite standartlarına göre çalışmaktadırlar.

Sızma Testi = Zafiyet Analizi mi?

- Sızma Testi ≠ Zafiyet Analizi
- Aynı şey değildir.
- Sızma testi, yazılım ve yöntemler kullanarak hedef sistemlere sızma girişimleridir.
- Zafiyet Analizi, otomatize araçlar kullanarak sistem güvenliğinin teknik açıdan incelenmesi ve raporlanmasıdır.

Zayifetten > Sızma Testine

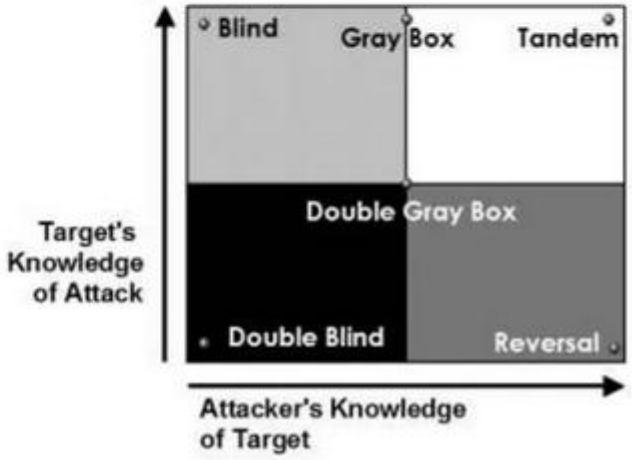
- Belirlenen bilişim sistemlerindeki mantık hataları ve zafiyetleri tespit ederek, söz konusu güvenlik açıklıklarının kötü niyetli kişiler tarafından istismar edilmesini önlemek ve sistemleri daha güvenli hale getirmek maksadıyla, “yetkili” kişiler tarafından ve “yasal” olarak gerçekleştirilen güvenlik testleridir.
- Pentest çalışmalarındaki asıl amaç, zafiyeti tespit etmekten öte ilgili zafiyeti sisteme zarar vermeyecek şekilde istismar etmek ve yetkili erişimler elde etmektir.

Sızma Testi Yöntemleri

Sızma Testi Yöntemleri

- Hedefe yapılacak testin türü uzmana verilecek yetki ve bilgiye göre değişiklik göstermektedir.
- Beyaz Kutu Sızma Testleri (White Box)
- Siyah Kutu Sızma Testleri (Black Box)
- Gri Kutu Sızma Testleri (Gray Box)

Şeklinde üç gruba ayırmak mümkündür.



Beyaz Kutu

- Güvenlik testi ekibi, sistemin kendisi ve arka planda çalışan ilave teknolojiler hakkında tam bilgi sahibidir.
- Test yapılan Firmaya daha büyük fayda sağlar.
- Hata ve zafiyetleri bulmak kolaylaşacağından bunlara tedbir alınma süresi de azalacaktır.
- Sistemin zarar görme riski çok azdır ve maliyet olarak da en az maliyetli olandır.

Siyah Kutu

- Başlangıçta güvenlik testi yapılacak sistemle ilgili bir bilgi yoktur.
- Tamamen bilinmeyen bir sistem ile ilgili bilgi toplanacak ve testler yapılacaktır.
- Bu yöntemde test ekibinin sistem ile ilgili bilgi düzeyi hiç olmadığından, yanlışlıkla sisteme zarar verme ihtimalleri de yüksektir.
- Bilgi toplama safhası oldukça zaman alır.
- Süre bakımından en uzun süren yaklaşım tarzıdır.

Gri Kutu

- Sistem ile ilgili bilgiler mevcuttur.
- *Örneğin; IP adres listesi, sunucu sistem ile ilgili versiyon bilgisi vb.*
- Bilgiler güvenlik testi yapacak ekibe önceden sağlanır.
- Black Box yaklaşımına göre daha kısa zaman alır.
- Kontrolü ve testi istenen IP adresleri belli olduğundan sistemin, istem dışı zarar görme ihtimali de azalmış olur.

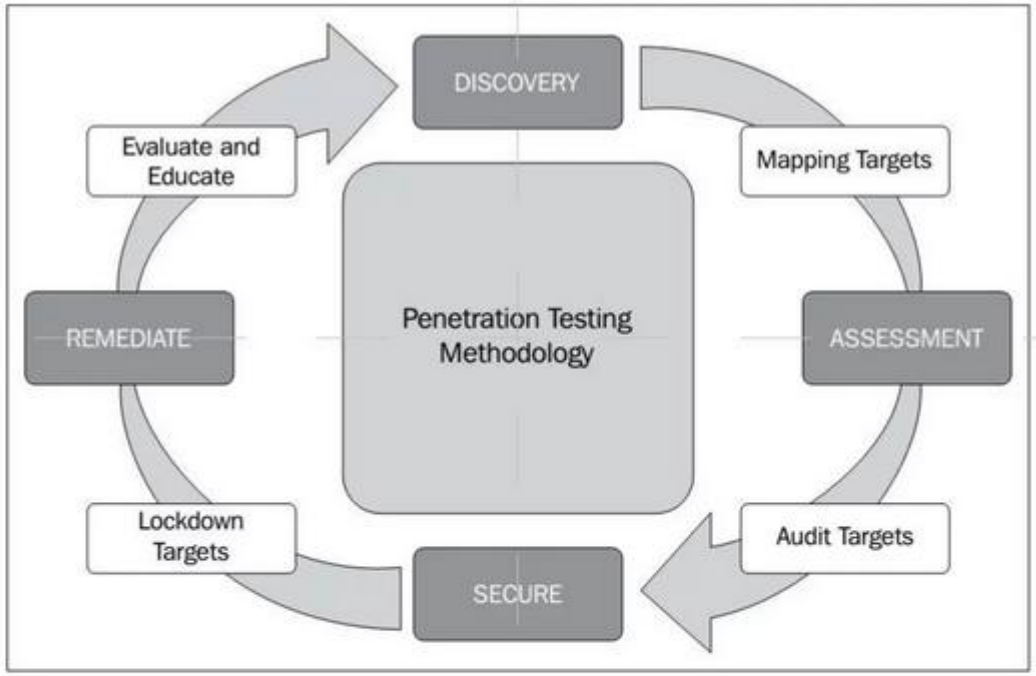
Metadoloji

Metadoloji

- Önceden belirlenmiş ve denenmiş, kalıplaşmış standartlar haline gelmiş kural ve yöntemler.
- OWASP (Open Web Application Project)
- OSSTIMM (The Open Source Secırity Testing Methodology Manual)
- ISSAF (Information Systems Security Assessment Framework)
- NIST (SP800-15)

Sızma Testi Metadolojisi

- Bilgi toplama
- Ağ Haritalama
- Zayıflık Tarama
- Sisteme Sızma
- Yetki Yükseltme
- Başka Ağlara Sızma
- Erişimleri Koruma
- İzleri Temizleme
- Raporlama



Kapsam Belirleme, Bilgi Toplama, Keşif ve Tarama, Zafiyet Taraması ve Analizi, İstismar Etme, Yetki Yükseltme, Yayılma, Bilgi-Doküman Toplama, İzleri Temizleme, Raporlama

Resim Kaynağı : CRYPTTECH

Sızma Testi Çeşitleri

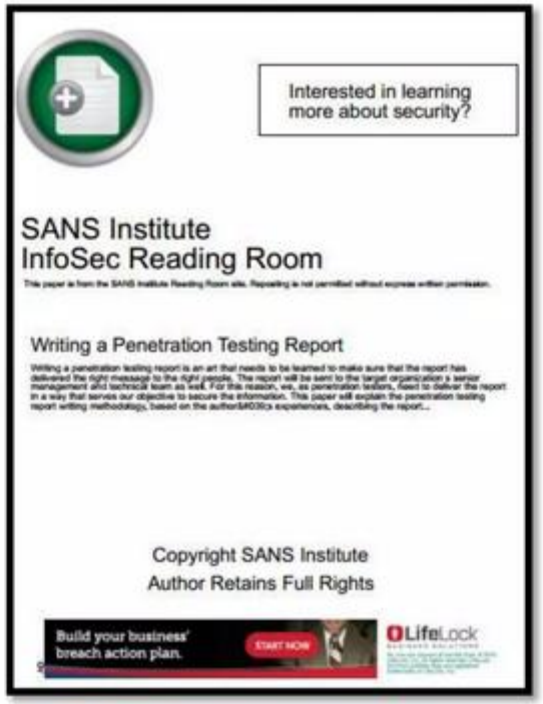
- İç Ağ
- Dış Ağ
- Web
- Kablosuz
- Mobil
- Sosyal Mühendislik
- Dos/DDoS

Resim Kaynağı: CRYPTTECH

Raporlar ve Standartlar

Pentest Rapor Örnekleri

1. https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf
2. https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343
3. http://www.niiconsulting.com/services/security-assessment/NII_Sample_PT_Report.pdf



Standartları Oluşturan Kuruluşlar

- IEEE
- ICANN
- ISO/IEC
- ETSI
- IETF
- NIST
- PCI SSC
- TSE

Standartlar

- ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi
- CC
- COBIT
- COSO
- ITIL
- CMMI
- TSE

ISO 27001

- Varlıkların sınıflandırılması,
- Gizlilik, bütünlük ve erişebilirlik kriterlerine göre varlıkların değerlendirilmesi,
- Risk analizi yapılması,
- Risk analizi çıktılarına göre uygulanacak kontrollerin belirlenmesi,
- Dokümantasyon oluşturulması,
- Kontrollerin uygulanması,
- İç tetkik,
- Kayıtların tutulması,
- Yönetimin gözden geçirmesi,
- Belgelendirme

şeklindedir.

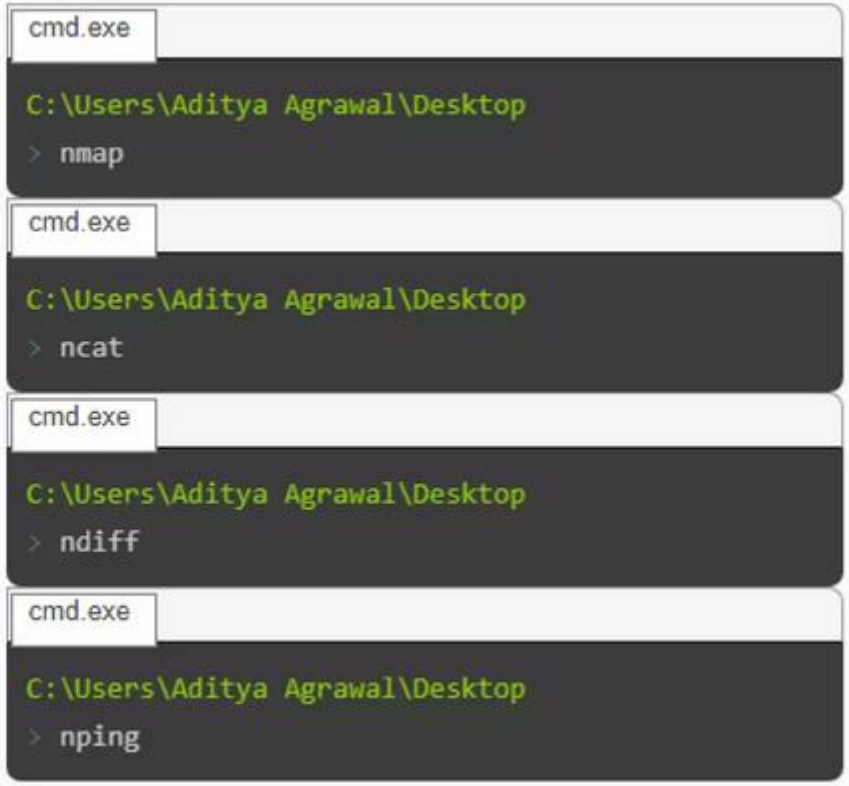
Sertifikalar

- CompTIA – Security+
- **CEH** (Certified Ethical Hacker)
- **LPT** (Licensed Penetration Tester)
- **OSCP** (Offensive Security Certified Professional)
- **CCSP** (Cisco Certified Security)
- **CISSP** (Certified Information Systems Security Professional)
- CPTE (Certified Penetration Testing Engineer)
- ECSA (EC-Council Certified Security Analyst)
- GIAC (GPEN, GWAPT, GXPN)
- CEPT (Certified Expert Penetration Tester)

Windows Pentest Box

- Windows ile Pentest araçları
- https://pentestbox.org

PentestBox



Bilişim Hukuku

Bilişim Hukuku

- Sayısal bilginin paylaşımını konu alan hukuk dalıdır.
- İnternetin kullanımına ilişkin yasal çerçeveyi belirleyen internet hukukunu kapsamaktadır.
- Yoğun olarak Ceza hukuku, Genel hukuk ve Fikir Sanat Eserler Kanunun Hukuk kuralları açısından ele alınır.
- https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

Bilişim Suçları

- Yetkisiz ve izinsiz erişim (Hacking)
- Verilere Yönelik Suçlar
- Bilişim Ağlarına Yönelik Suçlar
- Sanal Tecavüz
- Bilişim Ortamında Cinayet
- Tehdit ve Şantaj
- Hakaret ve sövme
- Taciz ve Sabotaj
- Dolandırıcılık
- Hırsızlık
- Sahtekarlık
- Manipülasyon
- Pornografi
- Röntgencilik
- Siber Terörizm
- Siber Propaganda

Bilişim Kanunları

- Türk Ceza Kanunu (Bilişim Suçları) (5237)
- Türk Ceza Kanunu (Bilişim Vasıtalı Suçlar)
- Fikir ve Sanat Eserleri Kanunu (FSEK-5846) (71,72,73)
- Ceza Muhakemesi Kanunu (5271-Madde 134)
- Kaçakçılıkla Mücadele Kanunu (4926 - Madde 12)
- 5651 Sayılı Kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun)
- 5809 Sayılı Elektronik Haberleşme Kanunu
- 5070 Sayılı Elektronik İmza Kanunu

Bilişim Kanunları

5237 sayılı Türk Ceza Kanunu'nun Bilişim Suçlarına İlişkin Hükümleri

- Madde 243
- Madde 244
- Madde 245
- Madde 124
- Madde 132
- Madde 133
- Madde 134
- Madde 135
- Madde 136
- Madde 137
- Madde 138
- Madde 140
- Madde 142
- Madde 158

Bilişim Kanunları

5237 sayılı Türk Ceza Kanunu'nun Bilişim Suçlarına İlişkin Hükümleri

- Madde 243: Bilişim Sistemine Girme
- Madde 244: Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme
- Madde 245: (5377 Sayılı Kanunun 27. Maddesiyle Değişik): Sahte Banka Veya Kredi Kartı Üretimi ve Kullanımı
- Madde 246: Tüzel kişiler hakkındaki tedbirler

Bilişim Kanunları

5237 sayılı Türk Ceza Kanunu'nun **Bilişim Vasıtalı** Suçlarına İlişkin Hükümleri

- Madde 124: Haberleşmenin Engellenmesi
- Madde 132: Haberleşmenin Gizliliğini İhlal
- Madde 133: Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması
- Madde 134: Özel Hayatın Gizliliğini İhlal
- Madde 135: Kişisel Verilerin Kaydedilmesi
- Madde 136: Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme
- Madde 137: Nitelikli Haller
- Madde 138: Verileri Yok Etmeme
- Madde 140: Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması
- Madde 142: Nitelikli Hırsızlık
- Madde 158: Nitelikli Dolandırıcılık
- Madde 226: Müstehcenlik

Bilişim Kanunları

Fikir ve Sanat Eserleri Kanunu (5846)

- Madde 71 – Manevi Haklara Tecavüz.
  - Yazılımı kamuya sunma hakkı,Yazılım sahibinin adını belitme hakkı, Değişiklik yapılmaması hakkı
- Madde 72 – Mali Haklara Tecavüz.
  - Değiştirmek, kopyalamak, çoğaltmak yaymak, ticaret konusu yapmak, aracılık etmek, suçtur.
- Madde 73 – Diğer Suçlar

Bilişim Kanunları

Ceza Muhakemesi Kanunu (5271)

- Madde 134 – Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma.
  - (1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.
  - (2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.
  - (3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.
  - (4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır. (5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır

Bilişim Kanunları

Kaçakçılıkla Mücadele Kanunu (4926)

- Madde 12 – Gümrük idarelerinde sahte beyan ve belge.
  - Gümrük idarelerinde işlem görmediği halde işlem görmüş gibi herhangi bir belge veya beyanname düzenleyenler veya bu suçları bilişim yoluyla işleyenler hakkında Türk Ceza Kanununun evrakta sahtekarlık ve bilişim alanındaki suçlarla ilgili hükümlerinde belirtilen cezalar bir kat artırılarak uygulanır.

Bilişim Kanunları

Türk Ceza Kanunu (243)

Türk Ceza Kanunu **Madde 243** *(Bilişim sistemine girme)*

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Bilişim Kanunları

Türk Ceza Kanunu (244)

Türk Ceza Kanunu **Madde 244** *(Sistemi engelleme, bozma, verileri yok etme veya değiştirme)*

(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.