TÜBİTAK

Sızma Testi Uzmanlığı Eğitimi

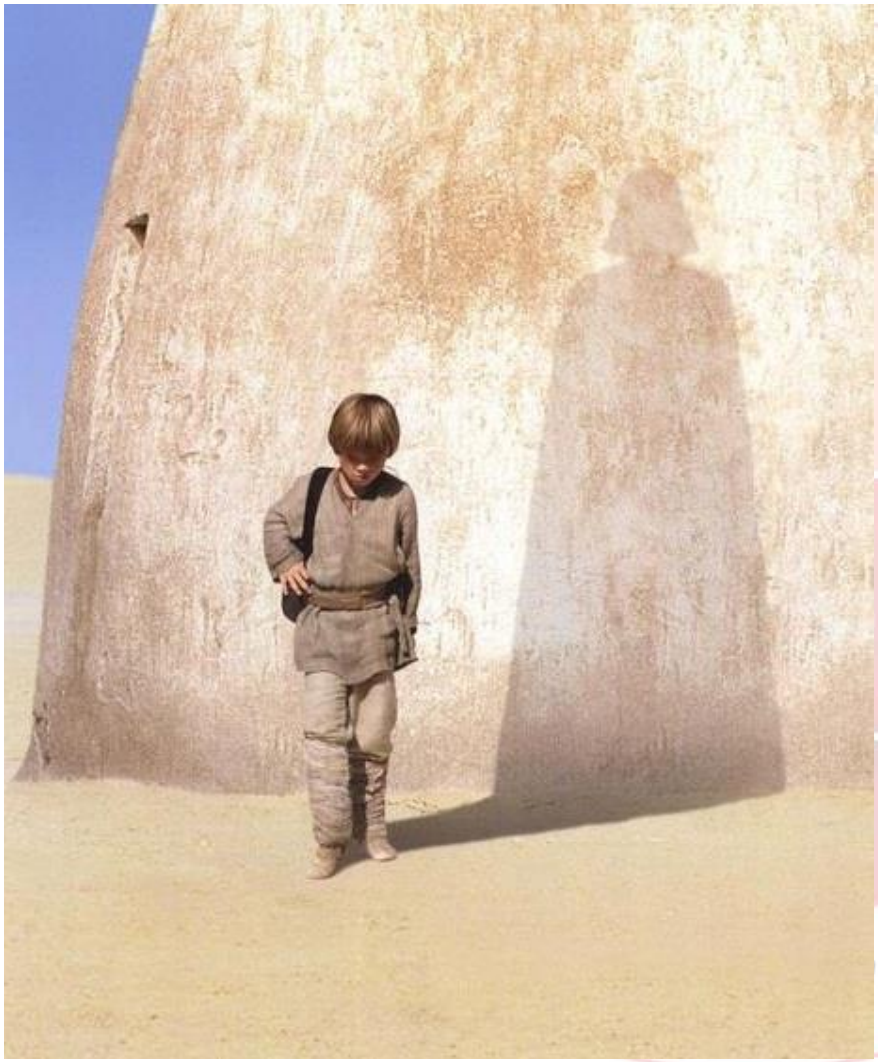
TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Sunum İçeriği

- Temel Kavramlar
- Neden Pentest?
- Pentest Yaklaşımları
- Planlama
- Amaç
- Süreçler
- Riskler
- Yasal Durumlar
- Standartlar
- Raporlama

Penetrasyon Testi (Pentest)

Penetrasyon Testi Nedir?

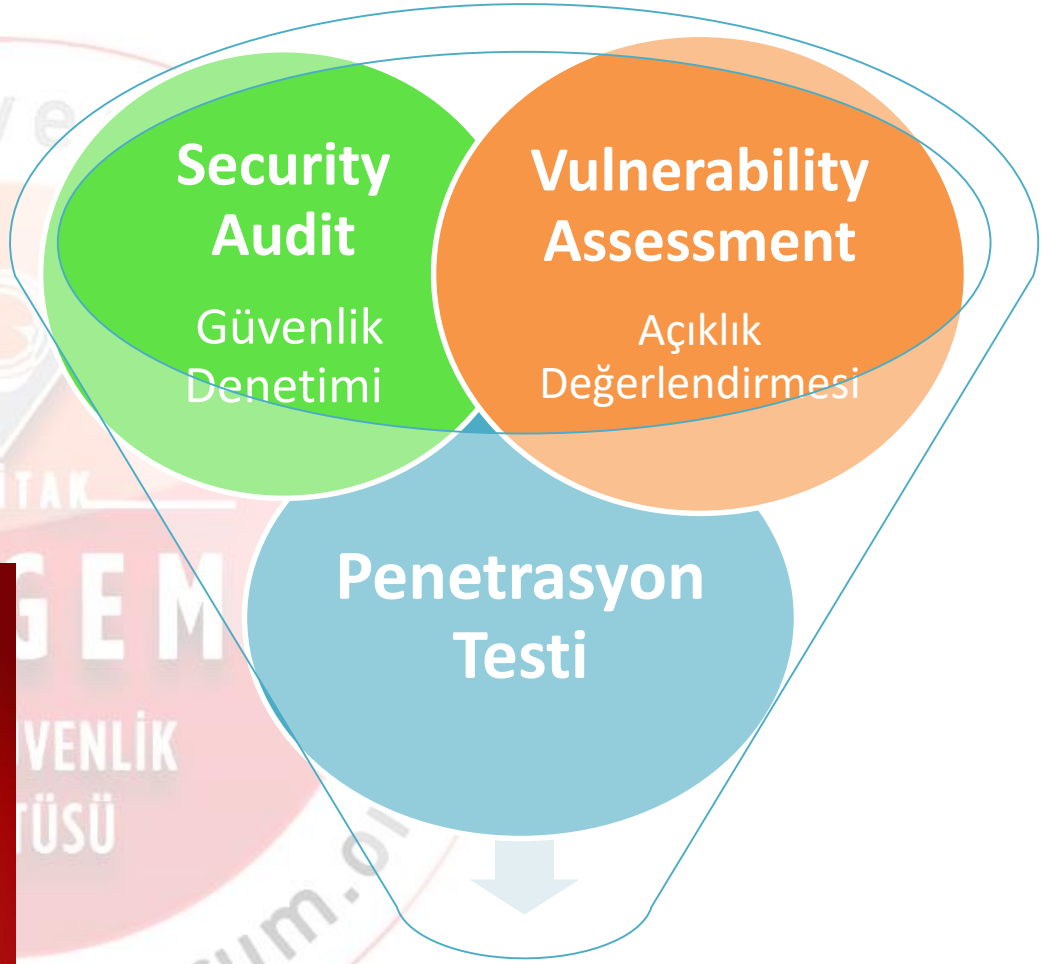


Tanım

- Tespit edilen açıklıkların ve zafiyetlerin kullanılmasıyla sistemlere sızma girişimi

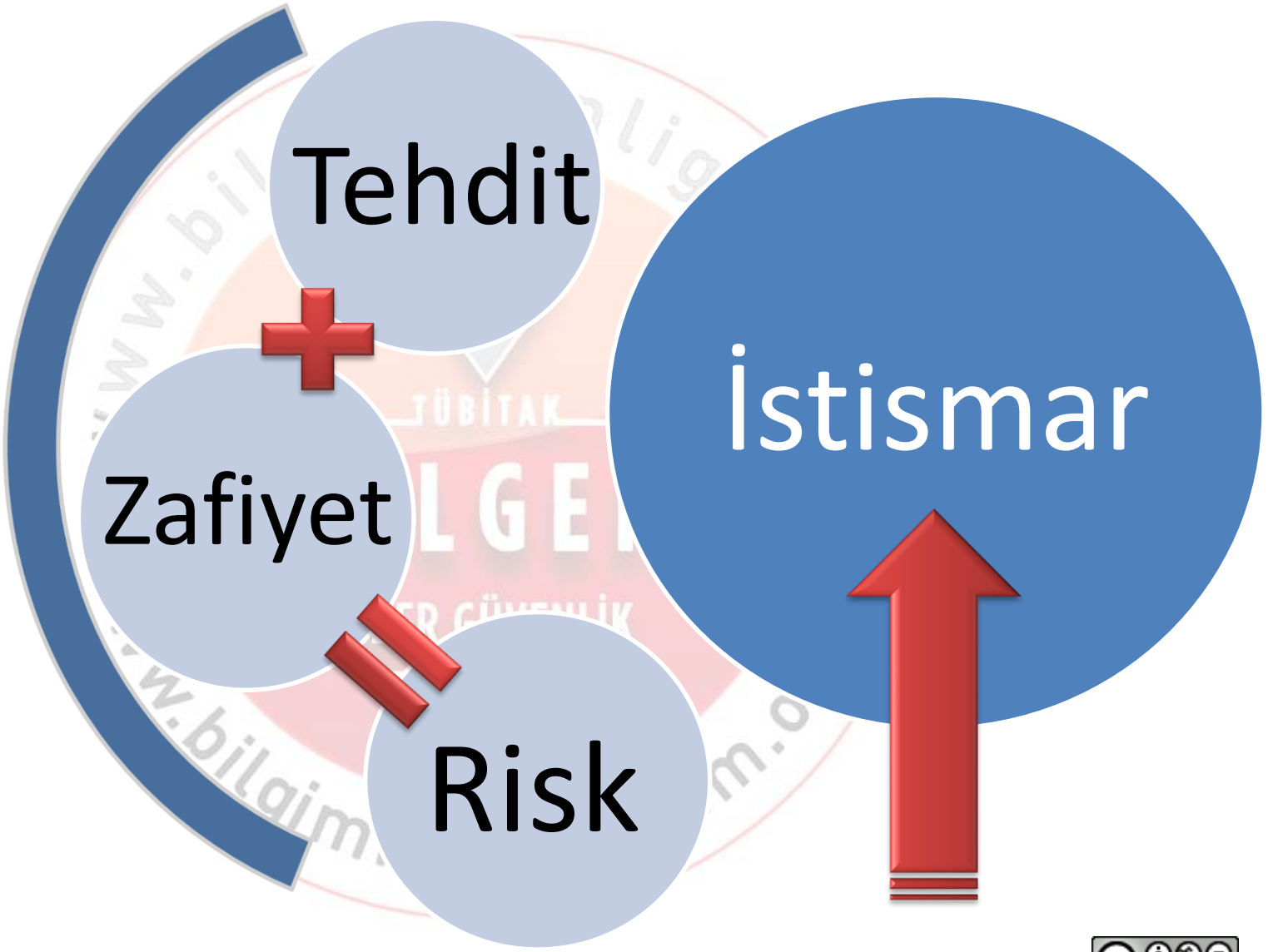
Temel Kavramlar

Temel Kavramlar-I



Ethical Hacking

Temel Kavramlar - II



Neden Pentest yaptırmalıyım?

Zayıf Yönlerim

Güçlü Yönlerim

Tehditler

Savunma

Pentest Yaklaşımları

- **Zero-knowledge** (Black-Box)
- **Partial-knowledge** (Gray box)
- **Full-knowledge** (White Box)

Pentest Planlaması

1 - Amaç

- Müşterinin ihtiyaçları nelerdir?
- Hedef-Kapsam Belirlenmesi

2 - Kapsam

- Dış Ağ
- İç Ağ
- Web Uygulamaları
- Kablosuz Ağ
- Sunucular
- Aktif cihazlar
- Veritabanı
- Uygulamalar
- Sosyal mühendislik
- DDoS
- Fiziksel güvenlik ....

3 - Gereksinimler

- Gerekli araçlar
- Alt yapı kurulumu
  (yazılım, donanımsal ağ mimarisi)
- Acil önlem planı
- Yedekleme yapılması gerekenler

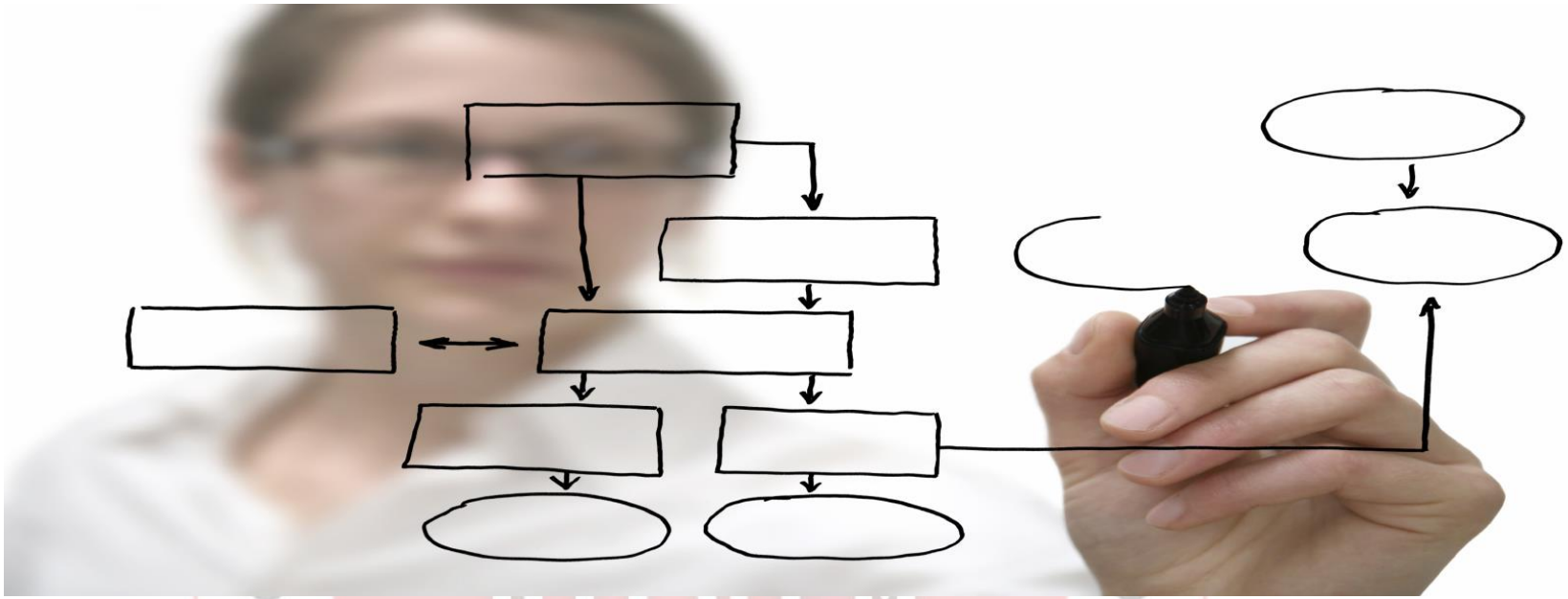
4 - Sınırlamalar

- Kapsam (Scope)
- Zaman
- Erişim (sunucu ağı,intranet)
- Method
  (Atak teknikleri)
  Örnek: Brute force yapılmasın!

5 - Uzman Seçimi

- Kabiliyetler
- Sertifikasyonlar
  C|EH, L|PT, GSEC, GPEN, OSCP
- Referanslar

Pentest Süreci



Operasyonel Süreç

Genel Süreç

Operasyonel Süreç

Genel Süreç

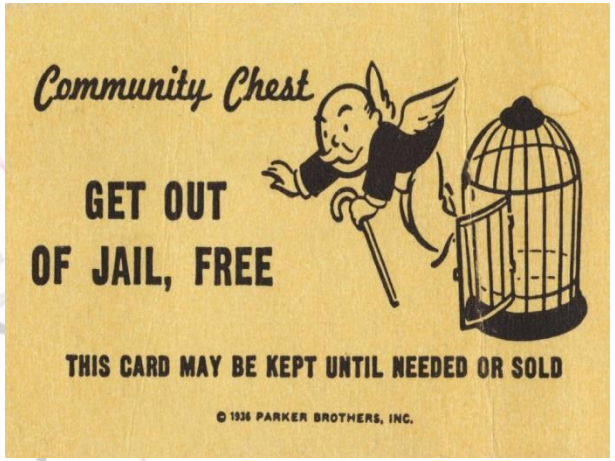
Pentest Hedefleri

Pentest Riskleri

- Bilgi Kayıpları
- Sistem çökmesi
- Konfigürasyon değişiklikleri

Yasal Durumlar

- Get Out of Jail Free Card
  (Hapisten kurtuluş belgesi)



- NDA (Non Disclosure Agreement)
  Gizlilik Sözleşmesi

- ROE (Rule of Engagement Kuralı)
  Pentest Kapsamı, yasal izinler ve yaptırımlar

Yasal Durumlar ve Standartlar

- PCI DSS
- OWASP
- PTES
- OSSTMM
- NIST SP 800-115

Pentest sırasında kullanılan bazı araçlar

Keşif	• Nmap • Hping • Scapy...
Sniffer	• Cain & Abel • Tcpdump • Wireshark...
Zafiyet Tarama	• Nessus • Metasploit • Immunity Canvas
Brute Force	• Hydra • John the Ripper • Cain, Ophcrack...
Web	• Burp • Acunetix • Net Sparker...

Pentest Raporlama

- Giriş - Özet
  -Amaç, hedef, kapsam, genel bilgiler
- Yönetici Özeti
- Bulgular
- Tavsiyeler
- Referanslar
- Raporlamada dikkat edilecek hususlar

TÜBİTAK

Teşekkürler