

# Açıklık Tarama ve Sızma Testi

MSÜ-2020

Deniz DEMİRÇİ

# AMAC:

- ▶ Bilgi güvenliğini sağlamak maksadıyla; güvenlik zayıflıklarının tespit edilerek risklerin azaltılmasına ve açıklıkların giderilmesine yönelik bilgi sahibi olunması.

# KAPSAM:

3

## SIZMA TESTİ VE YÖNTEMLERİNİN TANITIMI

Planlama ve Hazırlık, Keşif/Bilgi Toplama

Tarama ve Tarama Araçları

Risk ve Zafiyet Analizi

Zafiyetlerin Sömürülmesi - Temel Bilgiler

Zafiyetlerin Sömürülmesi - Tersine Mühendislik ve Exploit Geliştirme

Ara Sınav

# KAPSAM:

4

Web Uygulama Zafiyetlerinin Sömürülmesi - OWASP Top 10

Web Uygulama Zafiyetlerinin Sömürülmesi - OWASP Top 10

Yetki Yükseltme ve Yatay Hareket Etme Teknikleri

Parola Kırma ve Oturum Bilgileri Saldırıları

Özet Analiz ve Rapor Hazırlama

Sızma Testi İleri Düzey Başlıklar ve Sertifika Süreçlerinin Tanıtılması

Final Sınavı

## DEĞERLENDİRME:

Yarı Yıl Çalışmaları	Adet	Puan (%)
Ödev	3	20
Ara sınav	1	30
Final Sınavı	1	50
<b>TOPLAM</b>		<b>100</b>



# BİLGİ GÜVENLİĞİ

# GİZLİLİK

Bilginin yetkisiz kişilerin eline geçmesini engellemeyi amaçlamaktadır.

Bilgi hem bilgisayar sistemlerinde **işlenirken** (process), hem saklama ortamlarında **depolanırken** (storage), hem de ağ üzerinde gönderici ve alıcı arasında **taşınırken** (transport) yetkisiz erişimlerden korunmalıdır.

Saldırgan bir yapılandırma veya yazılım hatasını istismar ederek yahut Sosyal Mühendislik teknikleri ile yetkili insanların hatalarını istismar ederek bilgilere izinsiz olarak erişebilir.

Bu prensipte dikkat edilmesi gereken nokta, bilginin tamamen gizlenmesini sağlamak değil, **yetkisiz bir şekilde** elde edilmesini engellemek ve erişilebildiği durumunda da bundan haberdar olmaktır.



# GİZLİLİK

- ▶ Gizlilik prensibi ile ilgili temel kavramlar aşağıdaki gibi sıralanabilir.
  - ▶ Sensitivity: Verinin hassaslığı
  - ▶ Discretion: Bilginin paylaşımında ihtiyatlı davranış(ağzı sıkılık)
  - ▶ Criticality: Kritiklik
  - ▶ Concealment: Açıklamanın gizlenmesi veya önlenmesi
  - ▶ Secrecy: Gizlilik
  - ▶ Privacy: Gizlilik, mahremiyet
  - ▶ Seclusion: Tecrit
  - ▶ Isolation: Bilginin, diğer bilgilerden ayrılarak saklanması

# BÜTÜNLÜK

Amaç, bilgiyi olması gerektiği şekilde tutmak ve korumaktır. Bilginin bozulmasını, değiştirilmesini, yeni veriler eklenmesini, bir kısmının veya tamamının silinmesini engellemeyi hedefler.

Bu amaçla kritik bilgi için **erişim kontrolünün** gerçekleşmesi ve belli aralıklarla **yedeklemenin** gerçekleşmesi gerekmektedir.

Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır.

# BÜTÜNLÜK

- ▶ Bütünlük prensibi temel olarak Sistem Bütünlüğü ve Veri Bütünlüğü olarak ikiye kısımda incelenebilir.
- ▶ Bu prensipte dikkat edilmesi gereken nokta, bilginin değiştirilmemesini sağlamak değil, **yetkisiz bir şekilde** değiştirilmesini engellemek ve değişiklik durumunda da bundan haberdar olunabilmektir.

# BÜTÜNLÜK

- ▶ Bütünlük prensibi ile ilgili temel kavramlar aşağıdaki gibi sıralanabilir.
  - ▶ Accuracy: Doğruluk, kesinlik
  - ▶ Truthfulness: Doğruluk
  - ▶ Authenticity: Doğruluk
  - ▶ Validity: Geçerlilik
  - ▶ Nonrepudiation: İnkar edilememezlik
  - ▶ Accountability: Hesap verilebilirlik
  - ▶ Responsibility: Sorumluluk
  - ▶ Completeness: Tamlık
  - ▶ Comprehensiveness: Kapsamlılık, kapsayıcılık

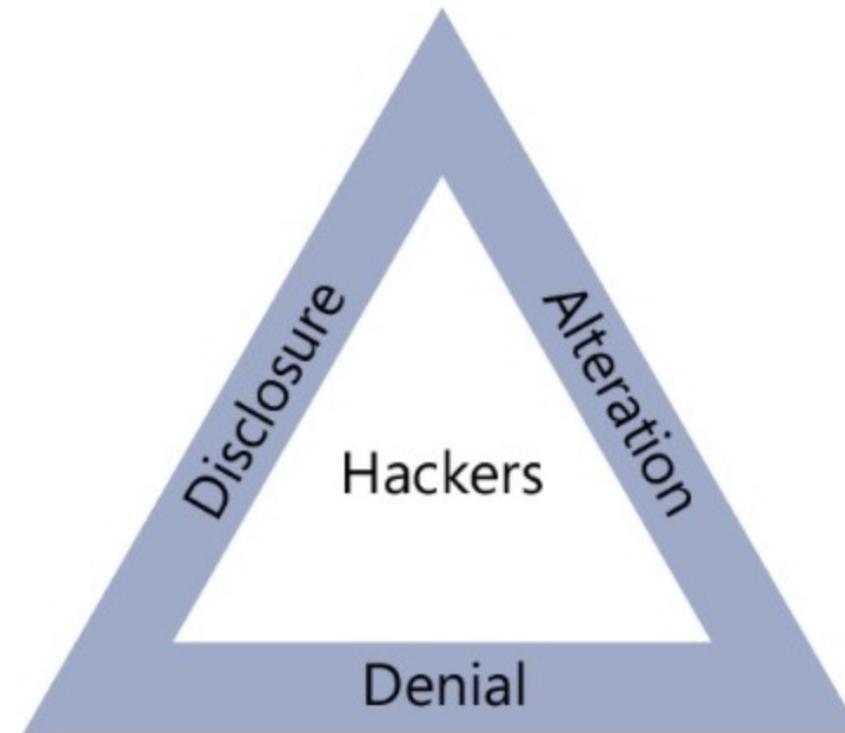
# ERİŞİLEBİLİRLİK

- ▶ Bilginin (verinin, kaynağın, sistemin,...) **belirlenen / beklenen / hedeflenen / ihtiyaç duyulan süre boyunca** ulaşılabilir ve kullanılabilir olmasını, tam ve eksiksiz olarak yapılmasını amaçlayan prensiptir.
- ▶ Erişilebilirlik; bilişim sistemlerini, kurum içinden ve dışından gelebilecek başarım düşürücü tehditlere karşı korumayı hedefler.
- ▶ Erişilebilirlik hizmeti sayesinde, kullanıcılar, **erişim yetkileri dahilinde** olan verilere, **veri tazeliğini yitirmeden**, zamanında ve güvenilir bir şekilde ulaşabilirler.
- ▶ Bu prensipte dikkat edilmesi gereken nokta, erişilebilirlik ile sistemin %100 ayakta kalmasını sağlanmaz, **belirlenen süre boyunca** (SLA - Service Level Agreement) hizmet verilmesinin sağlanmasıdır.

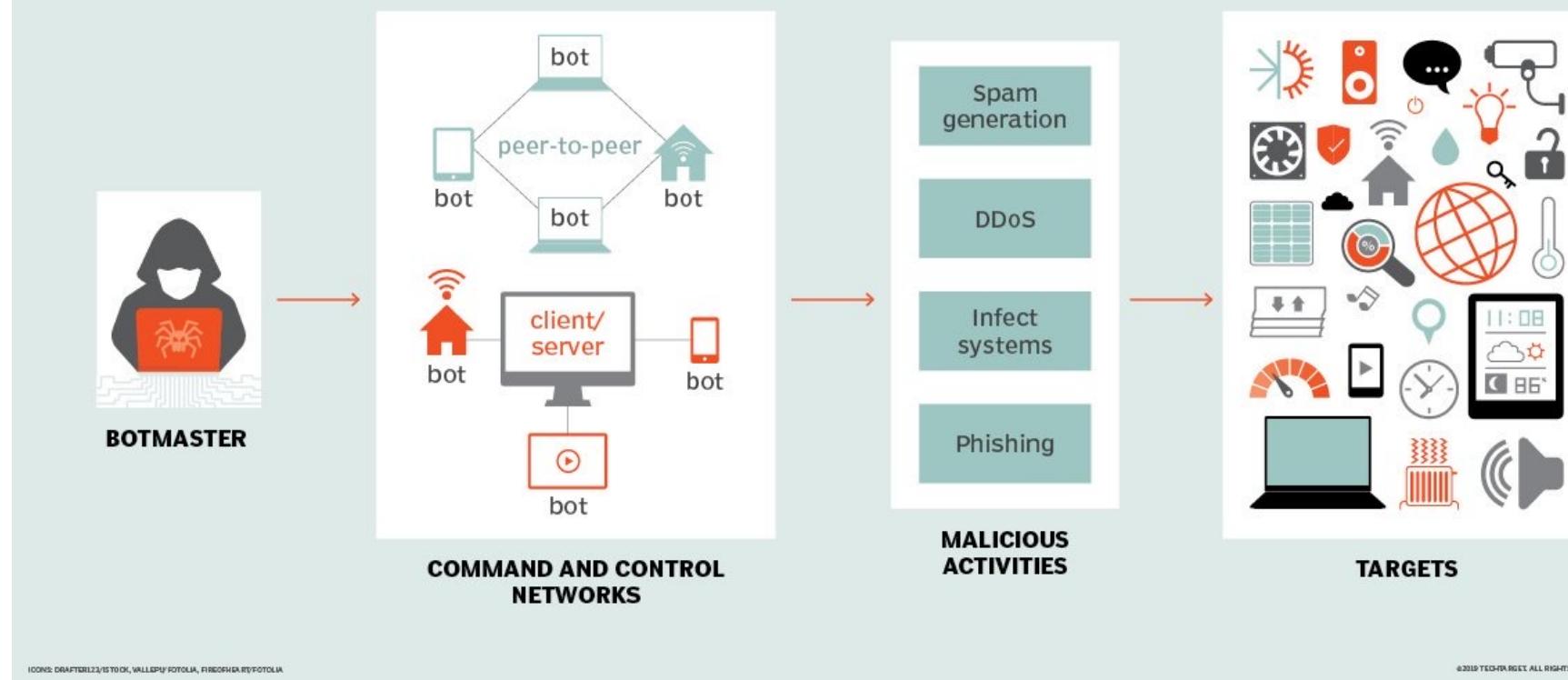
# ERİŞİLEBİLİRLİK

- ▶ Erişilebilirlik prensibi ile ilgili temel kavramlar aşağıdaki gibi sıralanabilir.
  - ▶ Usability: Kullanılabilirlik
  - ▶ Accessibility: Erişilebilirlik
  - ▶ Timeliness: Vaktindelik

# BİLGİ GÜVENLİĞİ - PRENSİPLER:



# Botnet command and control architecture



[fortune.com/2016/10/31/nsa-shadow-brokers-hack-ip-addresses/](http://fortune.com/2016/10/31/nsa-shadow-brokers-hack-ip-addresses/)

**FORTUNE** SUBSCRIBE

# NSA-Hacking 'Shadow Brokers' Reveal Spy- Penetrated Networks

The Shadow Brokers, a mysterious hacker group, released a new cache of files online on Halloween morning.

The group claimed its latest dump reveals the IP addresses, or network designations, of computer servers supposedly compromised by The Equation Group, a hacker outfit widely believed to be linked to the United States National Security Agency. The list allegedly

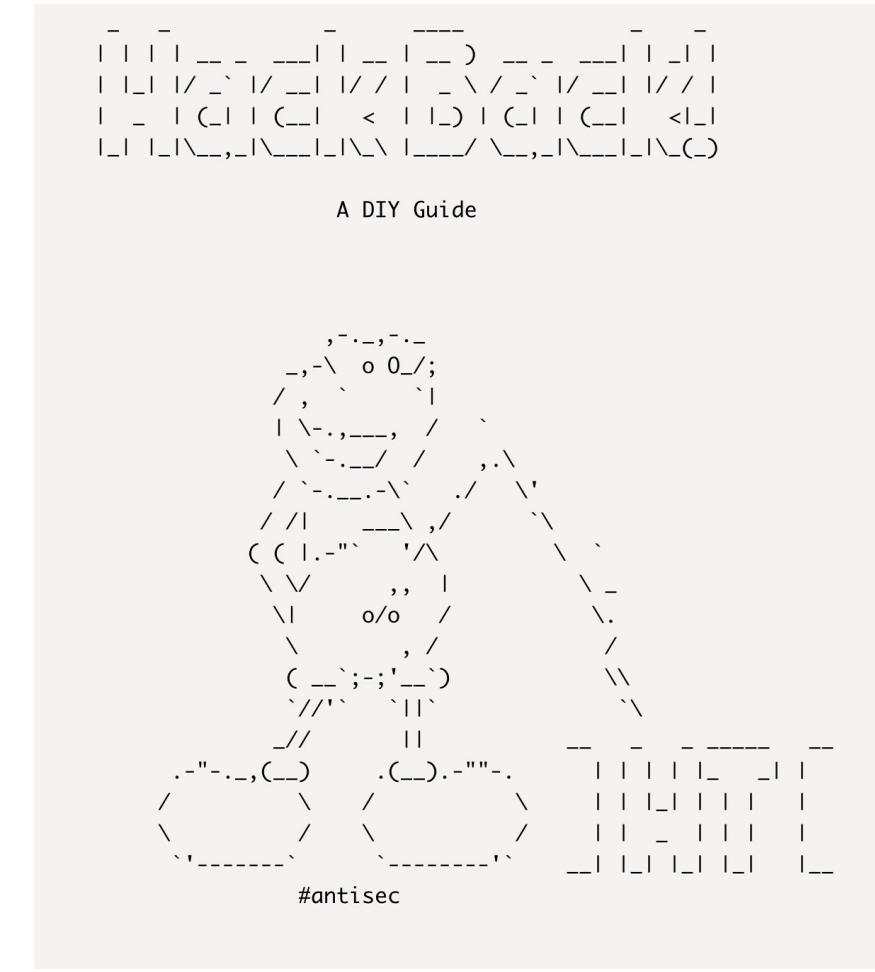
]

Rely on us.



*Remote Control System*

**THE HACKING SUITE FOR GOVERNMENTAL INTERCEPTION**



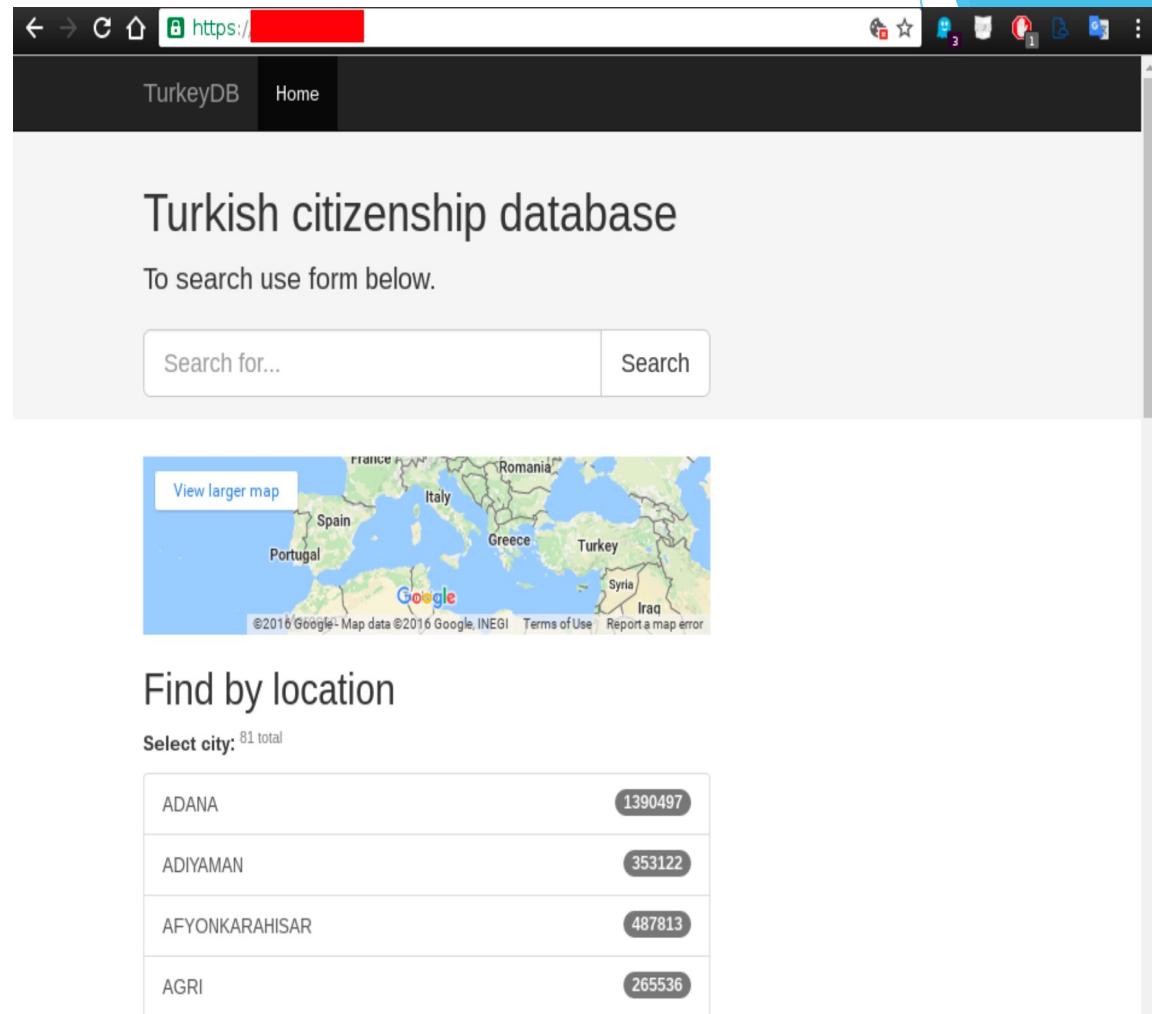
Turkish citizenship database leaked ? <http://185.100.87.84/>  
[pic.twitter.com/16pspqyr3S](https://pic.twitter.com/16pspqyr3S)  
— Dmitry Chestnykh (@dchest) April 4, 2016

This leak contains the following information for **49,611,709** Turkish citizens: (IN CLEARTEXT)

- National Identifier (TC Kimlik No)
- First Name
- Last Name
- Mother's First Name
- Father's First Name
- Gender
- City of Birth
- Date of Birth
- ID Registration City and District
- Full Address

#### Lesson to learn for Turkey:

- Bit shifting isn't encryption.
- Index your database. We had to fix your sloppy DB work.
- Putting a hardcoded password on the UI hardly does anything for security.



The screenshot shows a web browser window with the URL <https://185.100.87.84/>. The page title is "TurkeyDB". The main content area has a heading "Turkish citizenship database" and a sub-instruction "To search use form below." Below this is a search form with a "Search for..." input field and a "Search" button. Underneath the search form is a map of the Mediterranean region, including parts of France, Spain, Portugal, Italy, Greece, Turkey, Syria, and Iraq. A "View larger map" link is visible on the map. At the bottom of the map, there is a copyright notice: "©2016 Google Map data ©2016 Google, INEGI Terms of Use Report a map error". Below the map, there is a section titled "Find by location" with a heading "Select city: 81 total". A table lists four cities with their respective counts: ADANA (1390497), ADIYAMAN (353122), AFYONKARAHISAR (487813), and AGRI (265536). The table has alternating row colors.

City	Count
ADANA	1390497
ADIYAMAN	353122
AFYONKARAHISAR	487813
AGRI	265536



## The Mindset of Penetration Testers and Ethical Hackers

- Successful penetration testers and ethical hackers must maintain a mindset that involves two often contradictory sounding concepts
  - Think outside of the box, be pragmatic, do things differently
  - But, at the same time, be thorough, methodical, and careful, take good notes, and make your work repeatable
- Balance between these two is crucial for success

# PENTEST YONTEMLERI

- ▶ Open Source Security Testing Methodology Manual (OSSTMM)
- ▶ Pen Testing Execution Standard (PTES)
- ▶ NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment
- ▶ Open Web Application Security Project (OWASP)
- ▶ Penetration Testing Framework

# Terminal?

- ▶ A Windows cmd.exe with the prompt: **C : \>**
- ▶ A Windows PowerShell with the prompt: **PS C:\>**
- ▶ A Linux bash shell (which we'll run as root) with the prompt: **#**
- ▶ The Metasploit Framework Console with the prompt: **msf >**
- ▶ A Meterpreter shell with the prompt: **meterpreter >**

- ▶ Hazırlık
  - ▶ Gizlilik Sözleşmesi (NDA)
  - ▶ Hedef Kurum için en önemli alanların kurum personeli ile ortaya çıkarılması
  - ▶ Angajman Kuralları (Rules of Engagement ) , test nasıl yapılacak?
  - ▶ Test kapsamının belirlenmesi
  - ▶ Resmi izin belgesi (Jail Free Card)
  - ▶ Takımı belirleme
- ▶ Testin Gerçekleştirilmesi
- ▶ Detaylı Analiz ve Tekrar Test Gerçekleştirilmesi
- ▶ Raporlama

# Sızma Testi Uzmanı

- ▶ Programlama
  - ▶ Scripting
  - ▶ Python, c, c#, c++, asm ...
- ▶ Ağ
  - ▶ OSI
  - ▶ TCP/IP
  - ▶ Trafik Analizi ...
- ▶ Web
  - ▶ Frontend
  - ▶ BackEnd
  - ▶ DB ...
- ▶ Tersine Mühendislik
  - ▶ X86
  - ▶ X64
  - ▶ ARM
- ▶ İlgili

“With great power comes  
great responsibility.”

Voltaire