Siber Güvenlik KURUMSAL BİLGİ GÜVENLİĞİ

@2023

Ertuğrul DUMAN dumanertugrul@gazi.edu.tr ertugrul.eduman@gmail.com

İçerik (Hafta/Konu)

1. Temel Terim ve Kavramlar, Siber Güvenliğe Giriş
2. Bilişim Etiği ve Bilgi Güvenliği
   (Bilgi Güvenliği Nedir? Siber Güvenlik Nedir? Hacker Kimdir? Hacking Nedir?)
3. Siber Güvenlik - Tehditler / Saldırı Yöntemleri
   (*Ransomware – Fidye Yazılımları, Sosyal Mühendislik*)
4. Sanal Makinalar ve Kurulumları
5. Siber Saldırı/Sızma Testi (Pentest) - Bilgi Toplama Araçları
6. Tarama, Zafiyet Tespiti ve Parola Kırma Araçları
7. Kriptoloji-Kriptografi(Şifreleme) – Steganografi (Veri Gizleme)
8. Bilgisayar Ağları(Network) ve Sunucu Sistemleri
9. İşletim Sistemleri ve Linux (Kali Linux)
10. Kablosuz Ağ Güvenliği (Saldırı-Savunma)
11. Siber Suç ve Siber Suçlular
12. Standartlar ve Uyum
13. Siber Güvenliğin Hukuki Boyutu ve Bilişim Hukuku
14. Adli Bilişim (Forensic)
15. Web Güvenliği Saldırı ve Savunma Yöntem -Araçları (Temiz Kod)

Siber Saldırı ve Savunma Yöntemleri
*Sanallaştırma Teknolojileri
*Bulut Bilişim Sistemleri
Veritabanı Yönetim Sistemleri

Algoritma ve Programlama
Nesne Tabanlı Programlama
Bilgi Güvenliği ve Kriptoloji
Sayısal Filigran. ve Veri Gizleme

Bilgisayar Ağları
Sunucu İşletim Sistemleri
Bilgi ve Ağ Güvenliği
İleri Ağ Teknolojileri
Siber Saldırı ve Savunma Yöntemleri

Bilişim Hukuku
*Adli Bilişim

İnternet Programcılığı
Güvenli Yazılım Geliştirme
Veritabanı Yönetim Sistemleri
*Mobil Programlama

AJANDA- İÇERİK

1. Temel Terim ve Kavramlar

2. Bilişim Etiği ve Bilgi Güvenliği

3. Siber Tehditler ve Saldırı Yöntemleri

3.1 Ransomware Fidye Yazılımları

3.2 Sosyal Mühendislik

4. Sanal Makina Kurulumları

5. Siber Saldırı Yöntemleri - Bilgi Toplama Araçları

6. Tarama, Zafiyet Tespiti ve Parola Kırma Araçları

7. Kriptografi Steganografi

8. Bilgisayar Ağları Ve Sunucu Sistemleri

9. İşletim Sistemleri Linux (Kali Linux)

10. Kablosuz Ağ Güvenliği

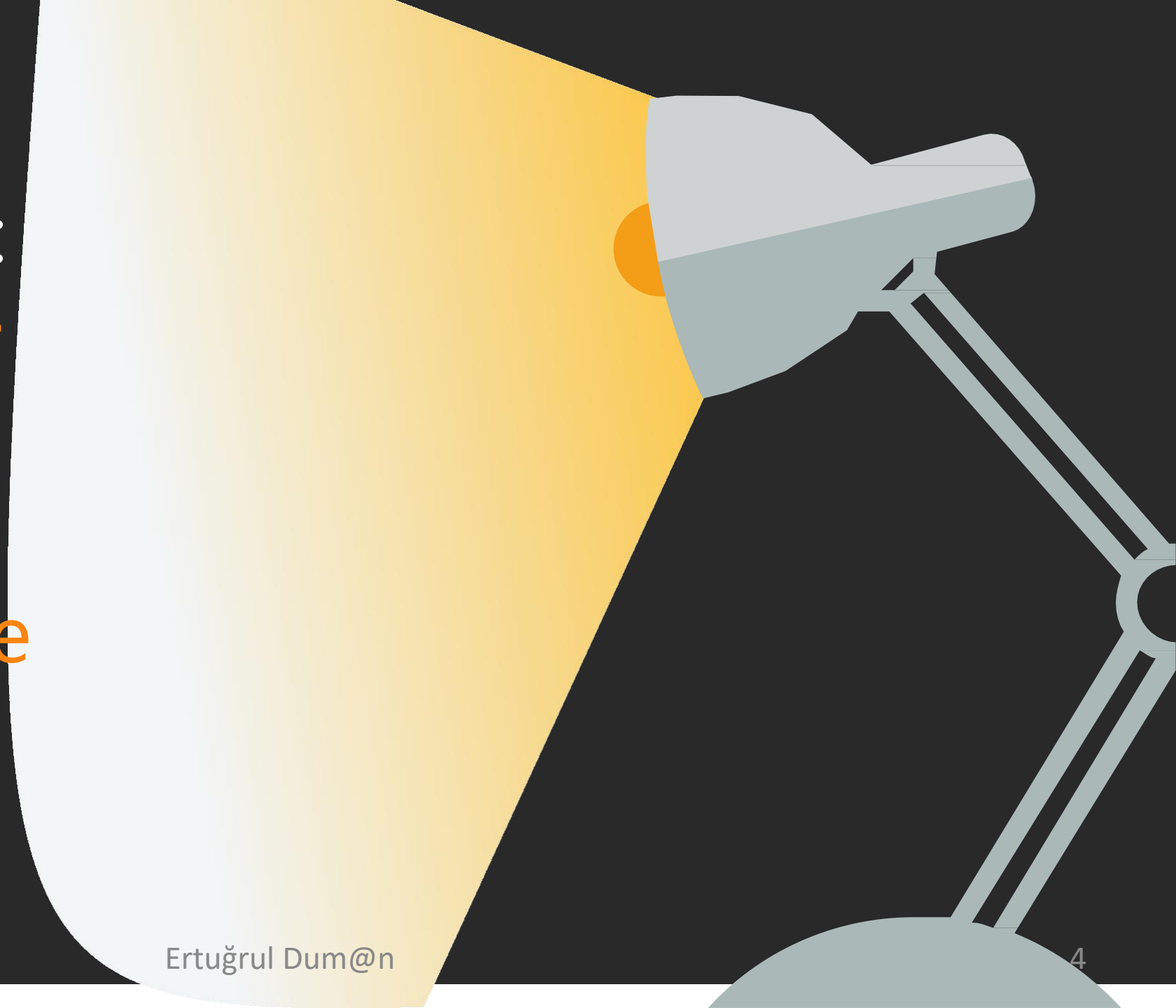
11. Siber Suç ve Siber Suçlular

12 – 13 – 14 Standartlar ve Uyum Bilişim Hukuku Adli Bilişim

15. Web Güvenliği Saldırı ve Savunma Yöntem - Araçları

Bölüm/Hafta 1:
Temel Terimler ve Kavramlar

Siber Güvenliğe Giriş



Temel Terimler ve Bazı Kavramlar

- Bilgi
- Güvenlik
- Bilgi Güvenliği
- Siber
- Siber Güvenlik
- Etik
- Hack
- Hacker
- Hacking
- Etik Hacker
- Etik Hacking
- Saldırı
- Savunma
- Zafiyet
- Kriptoloji
- Şifre
- Adli Bilişim
- Network
- Server
- Linux
- Kali Linux
- Pentest
- Metasploit able
- Exploit
- Payload
- Owasp

Temel Terim ve Kavramlar

- **Bilgi:** Verilerin anlam kazanmış halidir.
- **Güvenlik:** Toplumsal yaşamda düzenin aksamadan yürütülmesi.
- **Bilgi Güvenliği:** Bilginin korunması, bütünlüğü ve erişilebilir olmasını sağlayan önlemler.
- **Siber:** *Cyber* kelimesinden uyarlanmış, İnternet ve bilgisayar ağlarının tamamını kapsayan sanal ortam.
- **Siber Güvenlik:** Sanal ortamda bulunan bilginin korunması ile ilgili bileşen/teknolojiler bütünüdür.

Temel Terim ve Kavramlar

- **Etik:** Ahlak ile ilgili (meslek ahlakı), karakter/kültür olarak doğru tutum ve davranış
- **Hack:** Bir sistemin işleyiş kurallarının dışına çıkabilmektir. (Bir açıklığı kullanmak)
- **Hacker:** Bilişim alanında üst düzey bilgisi ile yazılım geliştiren/ kullanan ve aradığı bilgiye erişen kişidir. *(Tdk:* Siber korsan)
- **Hacking:** Bir sistemin, açıklarından faydalanıp izinsiz erişim veya sistemi ele geçirmek.

  (Programı/İşleyişi Değiştirmek)

Temel Terim ve Kavramlar

- **Etik Hacker :** Bilgi ve yeteneğini etik kurallar çerçevesinde kullanan (hacker) kişilerdir. (Ahlaklı korsan)
  - Zayıflığı t espit eden, güvenlik açığını kapatmaya yardımcı olan kişidir.

- **Etik Hacking :** Sistemin açık ve tehlikeli yönlerini ortaya çıkarmak için yapılan erişim veya ele geçirme işlemi. (Sızma Testi)

Temel Terim ve Kavramlar

- **Saldırı:** Saldırganların (Devlet, kurum, şahıs, terörist v.b.) amaçları için uyguladıkları (siber) faaliyetlerdir.

- **Savunma :** Bilişim sistemlerini siber tehditlere karşı korumak için alınan önlemlerdir.



Temel Terim ve Kavramlar

- **Tehdit:** Bir sistem veya kuruluşta zarara neden olabilecek istenmeyen bir olayın potansiyel nedeni.

- **Zafiyet:** (Vulnerability): Saldırgana fırsat verebilecek, yazılım, donanım ve prosedürler (açıklık-güvenlik boşluğu)

Temel Terim ve Kavramlar

- **Şifre:** Gizliliği olan şeylerin açılması, kullanılması veya iletilmesi için gerekli olan işaretler (harf, rakam, sembol, vb.) bütünüdür.

  deneme => **8F10D078B2799206CFE914B32CC6ASE9** (mdS)

- **Parola:** Gizlilik ortamında tanıma veya iletişim için gerekli anahtar (kelime) ifadedir. (Gizli)

  pArola123

Temel Terim ve Kavramlar

- **Kriptoloji:** Şifre Bilimidir. Belge veya mesajın şifrelenip iletilmesi ardından deşifre edilmesini gerçekleştirmek. (İletişimde gizlilik bilimi) (Kriptografi-Kriptoanaliz)

- **Adli Bilişim** (Forensic): Bilişim sistemleri üzerinden elde edilen nesnelerinin (yazı, resim, program vb.) mahkemede sunulmak üzere (delillerin) toplanması, saklanması, derlenmesi, analizi ile ilgili standartların ve işlemlerin bütünüdür.

Temel Terim ve Kavramlar

- **Network(Ağ):** İki veya daha fazla bilgisayarın kablolu ya da kablosuz iletişim araçları üzerinden yazılım ve donanım bileşenleriyle birbirine bağlanması ile meydana getirilen sistem bütünüdür.

- **Server(Sunucu):** Bir ağ üzerinde, program veya bilgiyi, farklı kullanıcılara/sistemlere paylaştıran/dağıtan donanım veya yazılıma verilen genel isimdir.

Temel Terim ve Kavramlar

- **Linux:** Unix işletim sistemine fikirsel ve teknik anlamda atıfta bulunarak geliştirilmiş açık kaynak kodlu, özgür ve ücretsiz (destek hariç) bir işletim sistemi çekirdeğidir. (GNU-GPL) (Unix türevidir.)

- **Kali Linux:** Sızma testleri için geliştirilmiş Debian tabanlı bir linux dağıtımıdır. Backtrack S devamı niteliğindedir.

Temel Terim ve Kavramlar

- **Pentest:** (Penetrasyon-Sızma Testi) Belirlenen bilişim sistemlerine mümkün olabilecek her yolun denenmesi ile sızılması..
- Kurumların kendi iletişim alt yapısı, sunucu, uygulama veya sistemlerine uyguladıkları sızma testleri..
- Test sonucu tespit edilen açıklıkların raporlanması ve yöneticilere iletilmesi işlemleridir.

- **Pentester:** Sızma testi yapan uzman kişi

Temel Terim ve Kavramlar

- **Meta sploitable :** Pentestler gerçekleştirmek için güvenlik açıkları hakkında bilgi sağlayan, sızma testleri amacıyla içerisinde çeşitli araçlar (exploit, payload, auxiliary, encoder) olan bir (framework yapısı) bilgisayar güvenlik projesidir.

- **Exploit :** Sistemler ve servisler üzerinde yer alan güvenlik açığının kullanılmasınısağlayan araçlara denilmektedir.

- **Payload:** Hedef sistem veya servis üzerinde çalıştırılması istenen kodlara denir. *(Exp/oit işleminin ardından)*

Temel Terim ve Kavramlar

- **Owasp:** Open Web Application Security Project Açık web uygulama güvenliği projesi
- Güvensiz web yazılımlarının oluşturduğu problemlere karşı mücadele etmek için kurulmuş bir topluluktur.

OWASP
Open Web Rppllcatlon Securlty Proȷect

- Top 10 list (Al ... AlO)
  Al: Injection
  A2: Broken Authentication and Session Management
  A3: Cross-Site Scripting (XSS)

OWASP TOP 10

Open Web Application Security Project

2017		2021
A01:2017-Injection - Enjeksiyon		A01:2021-Broken Access Control Bozuk/Hatalı Erişim Kontrolü
A02:2017-Broken Authentication Bozuk/Hatalı Kimlik Doğrulaması		A02:2021-Cryptographic Failures Kriptografik Hatalar
A03:2017-Sensitive Data Exposure Hassas Verilerin Açıklanması		A03:2021-Injection - Enjeksiyon
A04:2017-XML External Entities (XXE) XML Harici Varlıkları (XXE)	(Nueva)	A04:2021-Insecure Design - Güvenli Olmayan Tasarım
A05:2017-Broken Access Control Bozuk/Hatalı Erişim Kontrolü		A05:2021-Security Misconfiguration Güvenlik Yanlış Yapılandırması
A06:2017-Security Misconfiguration Güvenlik Yanlış Yapılandırması		A06:2021-Vulnerable and Outdated Components Güvenlik Açığı Olan ve Eski Sürüm Bileşenler / 3 TD Parti
A07:2017-Cross-Site Scripting (XSS) Siteler Arası Komut Dosyası Çalıştırma (XSS)		A07:2021-Identification and Authentication Failures Tanımlama ve Kimlik Doğrulama Hataları
A08:2017-Insecure Deserialization Güvenli Olmayan Serileştirme	(Nueva)	A08:2021-Software and Data Integrity Failures Yazılım ve Veri Bütünlüğü Hataları
A09:2017-Using Components with Known Vulnerabilities Bilinen Güvenlik Açıklarına Sahip Bileşenleri Kullanma		A09:2021-Security Logging and Monitoring Failures* Güvenlik Kaydı ve İzleme Hataları*
A10:2017-Insufficient Logging & Monitoring Yetersiz Kayıt ve İzleme	(Nueva)	A10:2021-Server-Side Request Forgery (SSRF)* Sunucu Tarafı İstek Sahteciliği (SSRF)*

OWASP TOP10

https://owasp.org/API-Security/editions/2023/en/0x11-t10/

https://owasp.org/API-Security/editions/2019/en/0x11-t10/

Güvenlik

%100 Güvenlik <u>yoktur!</u>

- Bilgi Güvenliği
  - Siber Güvenlik
    - İnternet güvenliği
    - Ağ güvenliği
    - Bilgisayar güvenliği
    - Mobil güvenlik
    - Siber Savaş

Bölüm/Hafta 2:

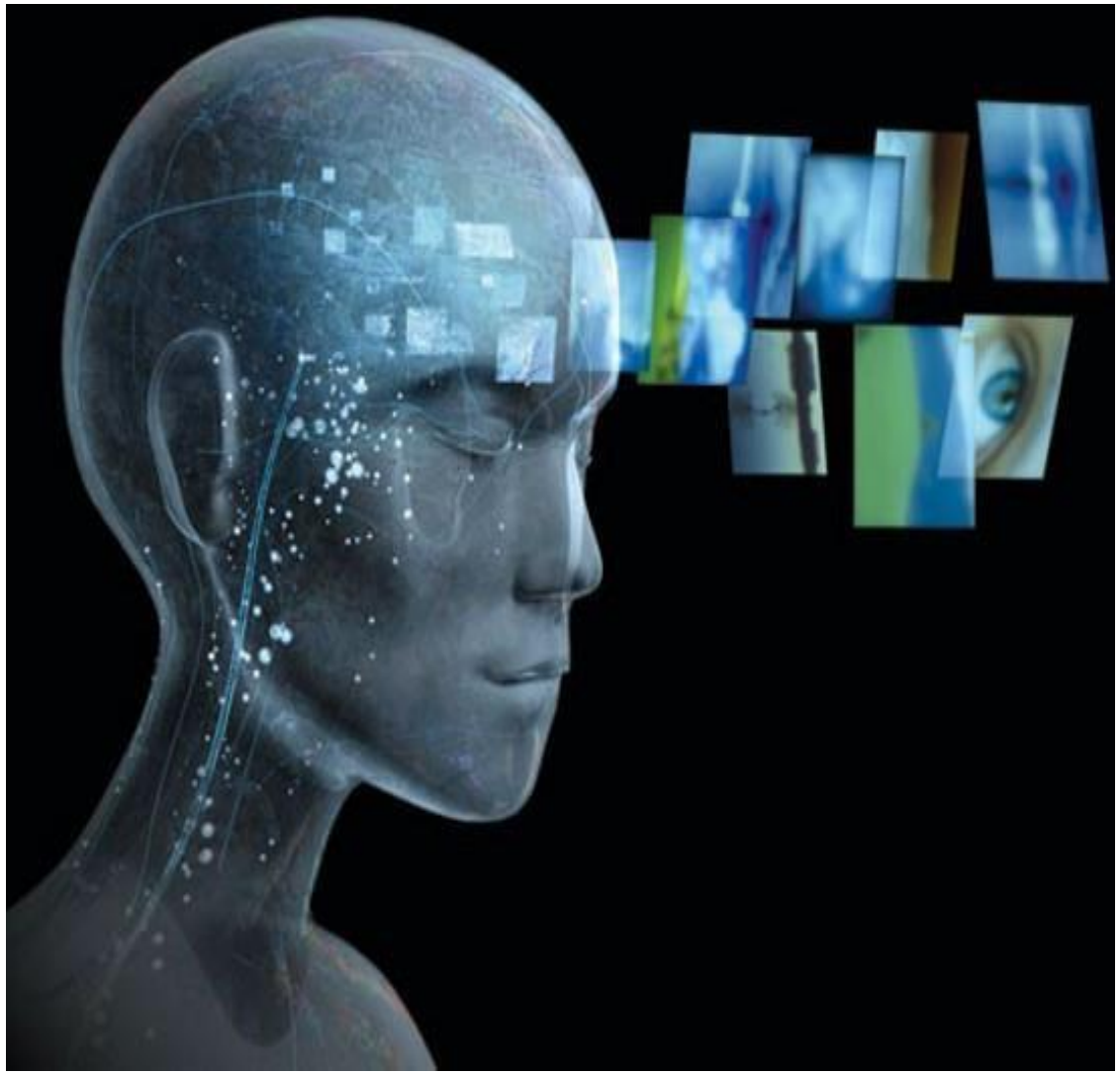
Bilişim Etiği ve Bilgi Güvenliği

2.Hafta

BİLGİ GÜVENLİĞİ NEDİR?
SİBER GÜVENLİK NEDİR? NASIL?
HACKER KİMDİR? HACKING NEDİR?

Bilişim Etiği Nedir?

- Bilgisayar dünyası ve ağ ortamında uyulması gereken kuralları tanımlayan normlar ve kodlar bilişim etiğini ifade eder.
- Bilgisayar teknolojisinin kullanımı için ilkeler sağlayan kendi doğrusu içinde bir disiplindir.
- Bilişim etiği kavramı bilgisayar dünyası içindeki insanların davranışlarını inceleyen felsefe dalıdır.
- Bilişim etiği konusunda hackerlık, dosya paylaşımı, internetin demokratik olup olmaması, lisanslar sıklıkla tartışılan konulardır.
- The Ten Commandments of Computer Ethics 1992 yılında Computer Ethics Institute tarafından oluşturuldu.



1. Bilgisayar başka insanlara **zarar vermek** için kullanılamaz.
2. Başka insanların bilgisayar çalışmaları **karıştırılamaz**.
3. Bilgisayar ortamında başka insanların **dosyaları karıştırılamaz**.
4. Bilgisayar **hırsızlık** yapmak için kullanılamaz.
5. Bilgisayar **yalan bilgi**yi yaymak için kullanılamaz.
6. Bedeli ödenmeyen yazılım **kopyalanamaz** ve kullanılamaz.
7. Başka insanların **bilgisayar kaynakları** izin almadan kullanılamaz.
8. Başka insanların entelektüel bilgileri **başkasına mal edilemez**.
9. Kişi yazdığı programın **sosyal hayata etkilerini** dikkate almalıdır.
10. Kişi, bilgisayarı, diğer insanları dikkate alarak ve **saygı göstererek** kullanmalıdır.

Kaynak : Computer Ethics Institute

Bilgi Güvenliği - Kavramlar

Bilişim sistemleri → Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda yer alan sistemler

Siber ortam → Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortam

Siber güvenlik → Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını

Bilgi Güvenliği → Bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi

Siber Güvenlik

Siber uzayı içerir.

Yalnızca digital verileri korumayı hedefler.

Bilgi güvenliğinin bir alt kümesidir.

Bilgi Güvenliği

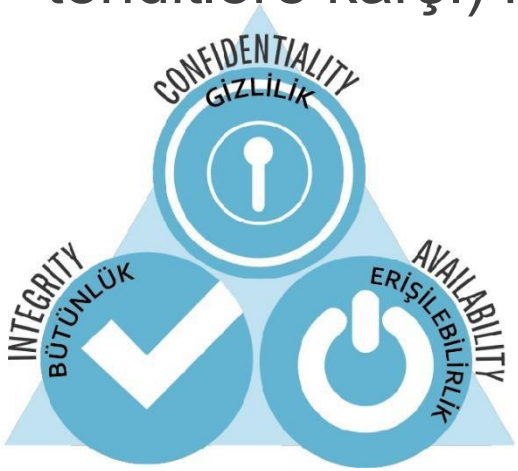
Siber uzayın dışındaki noktaları da içerir.

Tüm verileri korumayı amaçlar.

Kapsayıcıdır.

Bilgi Güvenliği Nedir?

Bilginin **gizliliği, bütünlüğü ve kullanılabilirliğinin** (dış ve iç kaynaklı tüm tehditlere karşı) korunmasıdır*



- **Gizlilik:** Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliği

- **Bütünlük:** Varlıkların doğruluğunu ve tamlığını koruma özelliği

- **Kullanılabilirlik/ Erişilebilirlik :** Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği

*Kaynak ISO/IEC 27001

Bilgi Güvenliği

- **Gizlilik** - Confi dent ial it y
  Herşeyi herkesten gizlemek değil, veriye/bilgiye sadece yetkisi onların ulaşılabilmesini sağlamak. Şifreleme gibi..
- **Bütünlük** - Integrity
  Yetkisiz ve izins iz değişikliklerin engellenmesi, ver inin amacına uygun derecede doğru olması.
- **Erişilebilirlik** - Availability
  Veriyi iletmek, depolamak ve işlemekten sorumlu hizmetlerin devamlılığının sağlanması.

- Bilgi güvenliğinin sağlanmasından **herkes sorumludur.**

(Bilginin sahibi, kullanan, sistemi yöneten, vb..)

*Yetki **paylaşılır,** sorumluluk **paylaşılmaz.** Bilgi ise **payla şıldıkça** ortar.*

Bilgi Güvenliği Kategorileri

- **Ağ güvenliği** (Network security)
- **Uç/Son nokta** veya **Kullanıcı güvenliği** (Endpoint security)
- **Veri güvenliği** (Data security)
- **Uygulama güvenliği** (Application security)
- **Kimlik ve Erişim Yönetimi** (Identity and access management)
- **Güvenlik yönetimi** (Security management)
- **Sanallaştırma ve bulut** (Virtualization and cloud)

Yasal Uyarı !

Türk Ceza Kanunu, Onuncu Bölüm, Bilişim Alanında Suçlar Kısmında;

Madde 243 ve Madde 244 de açıkça belirtildiği gibi;

- Bilişim sistemine girme (243)
- Sistemi engelleme, bozma, verileri yok etme veya değiştirme (244)
- **SUÇTUR** ve cezası vardır.
- İki yıldan altı yıla kadar hapis ve beşbin güne kadar adlı para cezasına hükmolunur.

Uyarı ! TCK 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 adlı para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, 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.

Uyarı ! TCK 244

Türk Ceza Kanunu **Madde 244** */Slsreml engelleme,bozma,verileri yakeımeveya deOişılrme/*

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

(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.

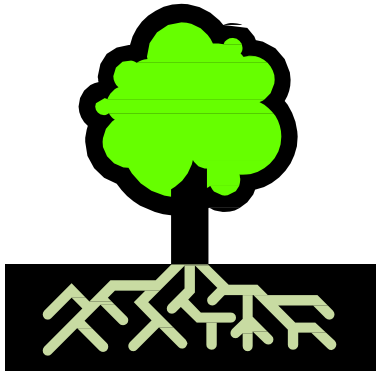
(4) Yukarıdaki fıkralarda tanımlanan fiill erin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükm olunur .

Bölüm/Hafta 3 :

Siber Güvenlik-

Tehditler ve Saldırı Yöntemleri

Siber Tehditler

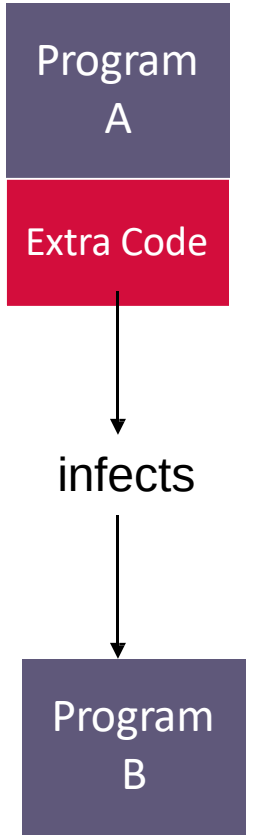


Siber dünyada en çok karşımıza çıkan tehditler :

- Virüsler
- Worms
- Trojan Horses / Logic Bombs
- Social Engineering
- Rootkits
- Botnets / Zombies

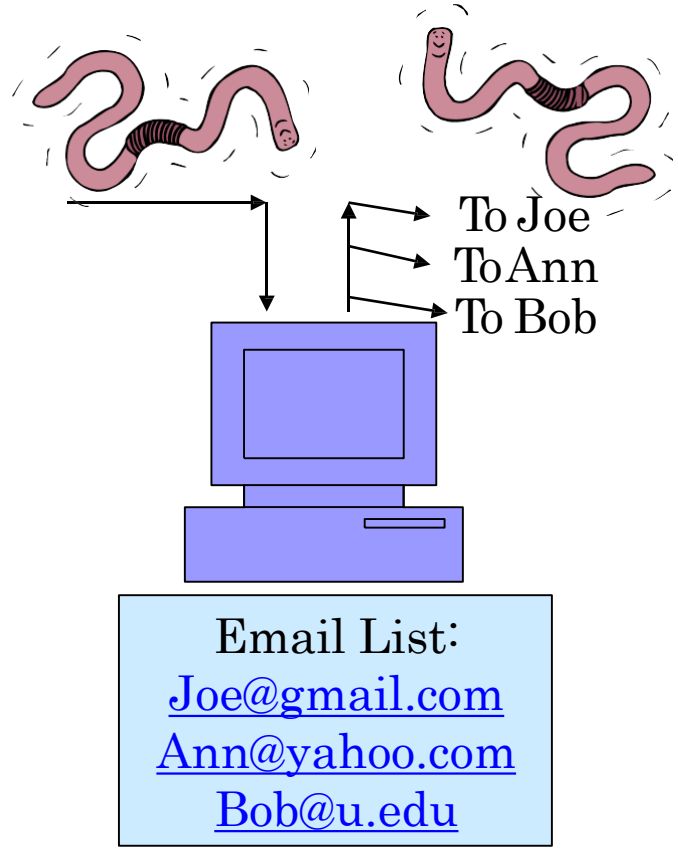
Siber Tehditler / Virüsler

- Kendini bir dosyaya, programa, diske ekleyen küçük program parçalarıdır.
- Program çalıştırıldığında virüs kodu da çalışmış olur ve kendini çoklar.
- Bilgisayarın çalışmasına müdahale etmeyi amaçlar.
- Altta yatan gizli amacına şartlar uygun olduğunda ulaşmak için bekler.



Siber Tehditler / Worms (Solucan)

- Bilgisayarınızda bulunan ağ bağlantısı sayesinde çoğalır.
- Herhangi bir dosyaya gizlenmek zorunda kalmayan virüs her bilgisayara ağ bağlantısı üzerinden çoğalabilir.
- Program çalıştırıldığında virüs kodu da çalışmış olur ve kendini çoklar.



Siber Tehditler / Makro

- Makro virüsler kendi kodlarını belgeler, elektronik tablolar ve diğer veri dosyalarıyla ilişkili makrolara ekler.

- Makro içeren belge çalıştırılmadan aktive olmazlar.
- Makro bir dizi komutun sırayla çalıştırılmasını gerçekleştirir.

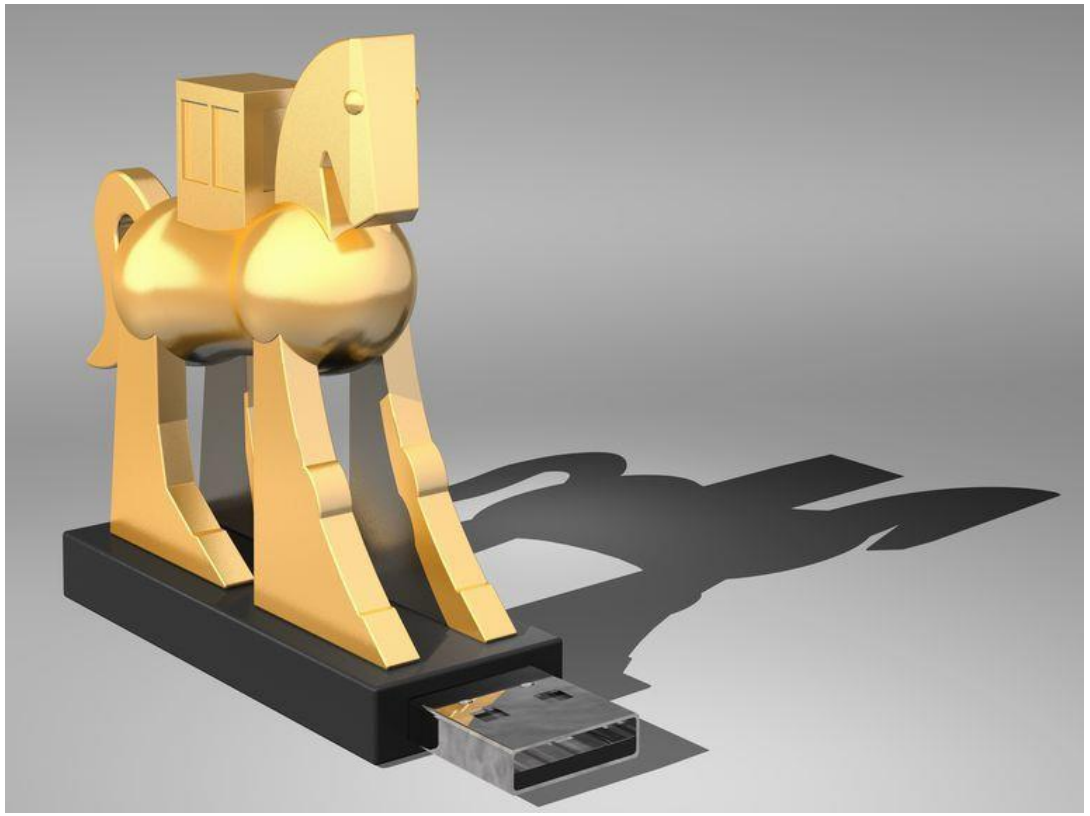
Siber Tehditler / Logic Bombs

- Mantık Bombaları, herhangi bir programın içerisine yerleştirilen virüs programlarıdır. Bazı şartların sağlanması durumunda patlayarak yani çalışmaya başlayarak sisteme zarar verirler.

- Bombalar, tüm dosyaları ve bilgileri veya sistemi silebilir.
- Örnek : Ödemesi yapılmayan bir yazılımın çalışmaması,
- Örnek : İşten kovulan bir çalışanın ardından veri tabanının silinmesi.

Siber Tehditler / Trojan Horse

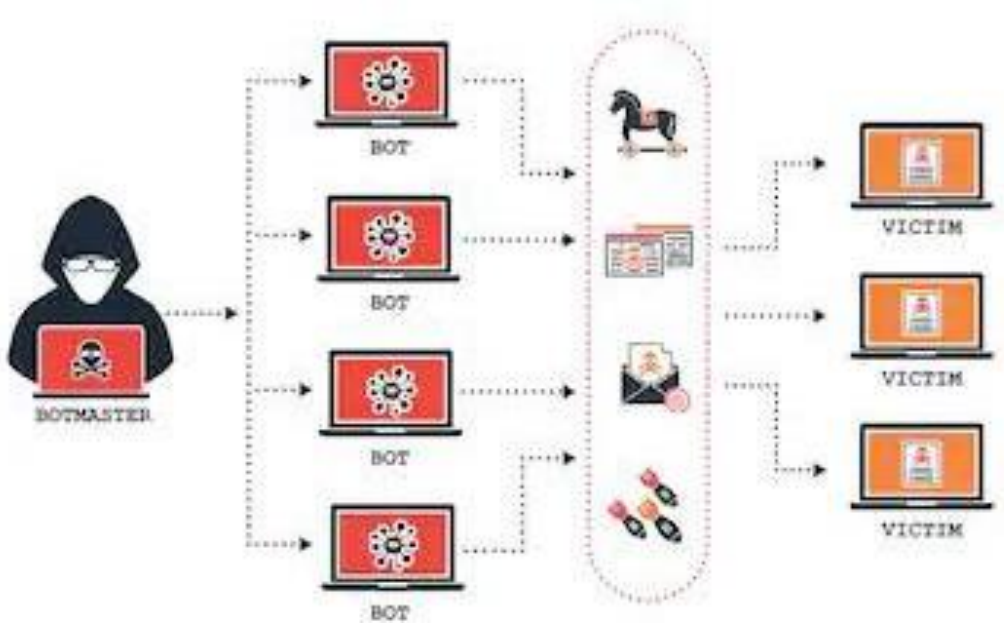
- Truva Atı, bir program ile bilgisayarınıza yüklenir, arka planda gizli olarak çalışır ve amacına uygun farklı işler yapar. Bir iş yapılırken gözükürken aslında başka iş yaparlar.
- Genellikle sonradan erişim için «Açık Kapı» bırakmak için kullanılırlar.
- Örnek : Oyun yüklenirken arka planda kişisel bilgilerinizi toplayıp gönderir.



Siber Tehditler / Botnet

- Siber suçlular, çok sayıda kullanıcının bilgisayar güvenliğini ihlal ederek, her bir bilgisayarın kontrolünü ele geçirerek, tüm virüslü makineleri suçlunun uzaktan yönetebildiği bir "bot" ağı halinde organize ederler.

- Botnet sözcüğü, "robot" ve "network" (ağ) sözcüklerinin birleşiminden türetilmiştir.

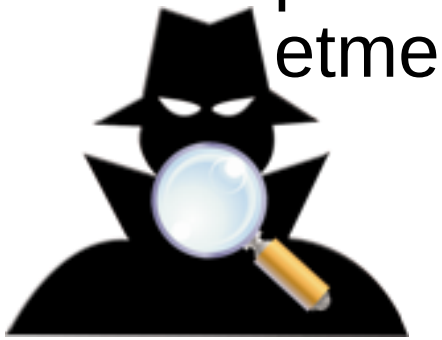


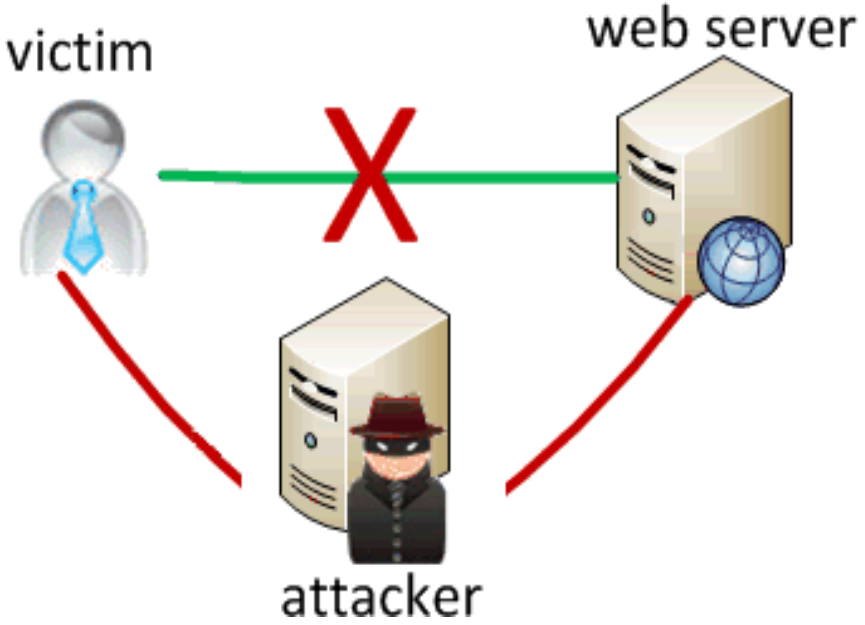
Siber Tehditler / DDoS

- DDoS saldırısı, saldırıya uğrayan web kaynağına birden çok istek göndererek web sitesinin çok sayıda isteği işleme kapasitesini aşmayı ve doğru şekilde çalışmasını engellemeyi amaçlar.
- Dağıtılmış Ağ Saldırıları, genellikle Dağıtılmış Hizmet Reddi (DDoS) saldırıları adıyla bilinir.
- Botnet'ler kullanılır.

Siber Tehditler / Man in the Middle

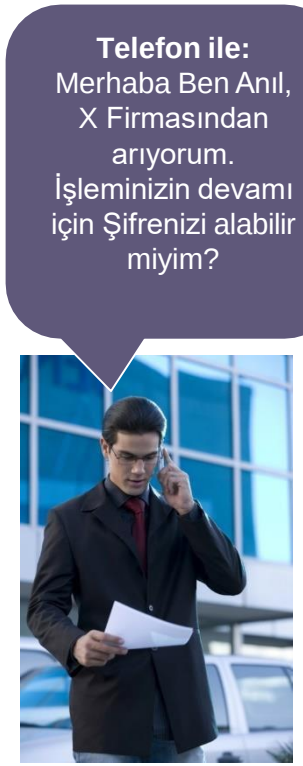
- Saldırganın birbiri ile doğrudan iletişim kuran iki taraf arasındaki iletişimi gizlice ilettiği veya değiştirdiği saldırı türüdür.
- İlkesel olarak hedefinde kendi IP'si olmayan bir paketi alan makinelerin, bu paketlerle ilgili herhangi bir işlem yapmamaları gerekir.
- Ancak istenirse bu paketlere müdahale edebilir ya da içeriğini öğrenebilirler.
- Aradaki adam saldırısı ağ üzerindeki paketleri yakalayarak manipüle etmek olarak özetlenebilir.

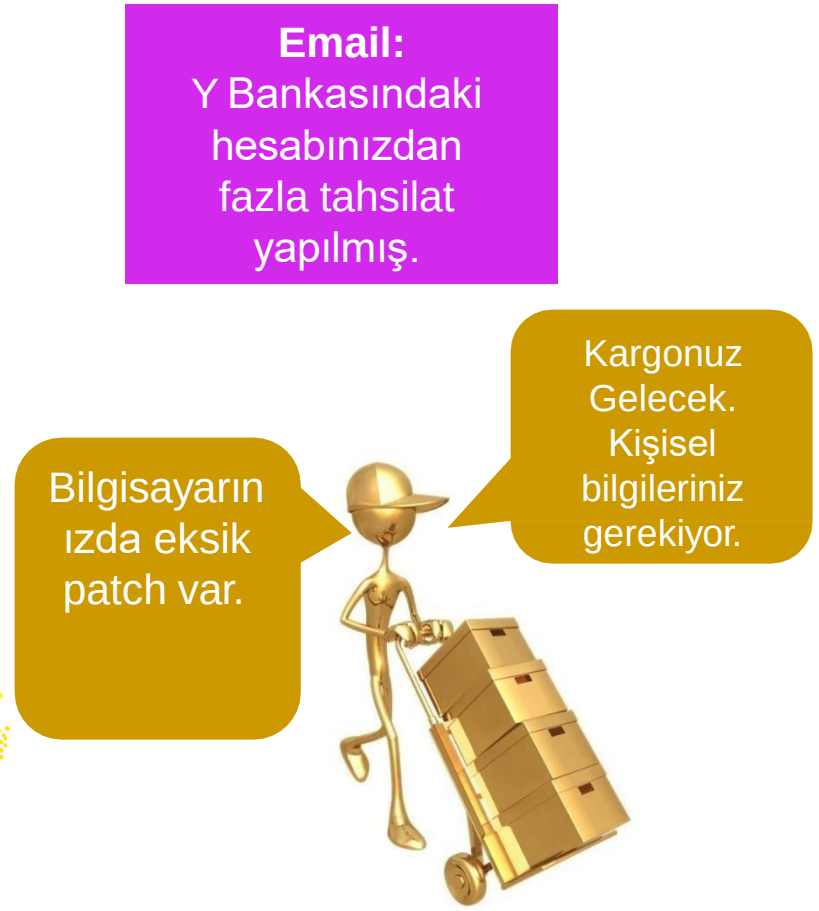




Siber Tehditler / Social Engineering

- Sosyal mühendislik basitçe elde edilmek istenen bilgiyi, karşıdaki insanı yanıltarak elde etmektir.
- Hayatın her anında karşımıza çıkabilir.
- Güzel hazırlanmış senaryolar kullanılır.





Siber Tehditler / Phishing

- Güvenilir bir elektronik haberleşme aracı gibi görünerek kullanıcı adı, şifre,kredi kartı bilgisi gibi özel bilgilerin ele geçirilme girişimidir.
- Password ve Fishing kelimelerinin birleştirilmesi ile oluşturulmuştur.
- Sahte bir e-posta ile başlatılır ve genelde kullanıcıları gerçek gibi görünen sahte bir web sitesine yönlendirdikten sonra kişisel bilgilerini girmelerini talep ederek devam eder.

Siber Tehditler / Pharming

- İnternet korsanları tarafından kullanıcıların kişisel verilerini ele geçirmek amacıyla bir web sitesini kopyasının hazırlaması ve siteyi asıl site olarak kullanıcıya sunmasıdır.

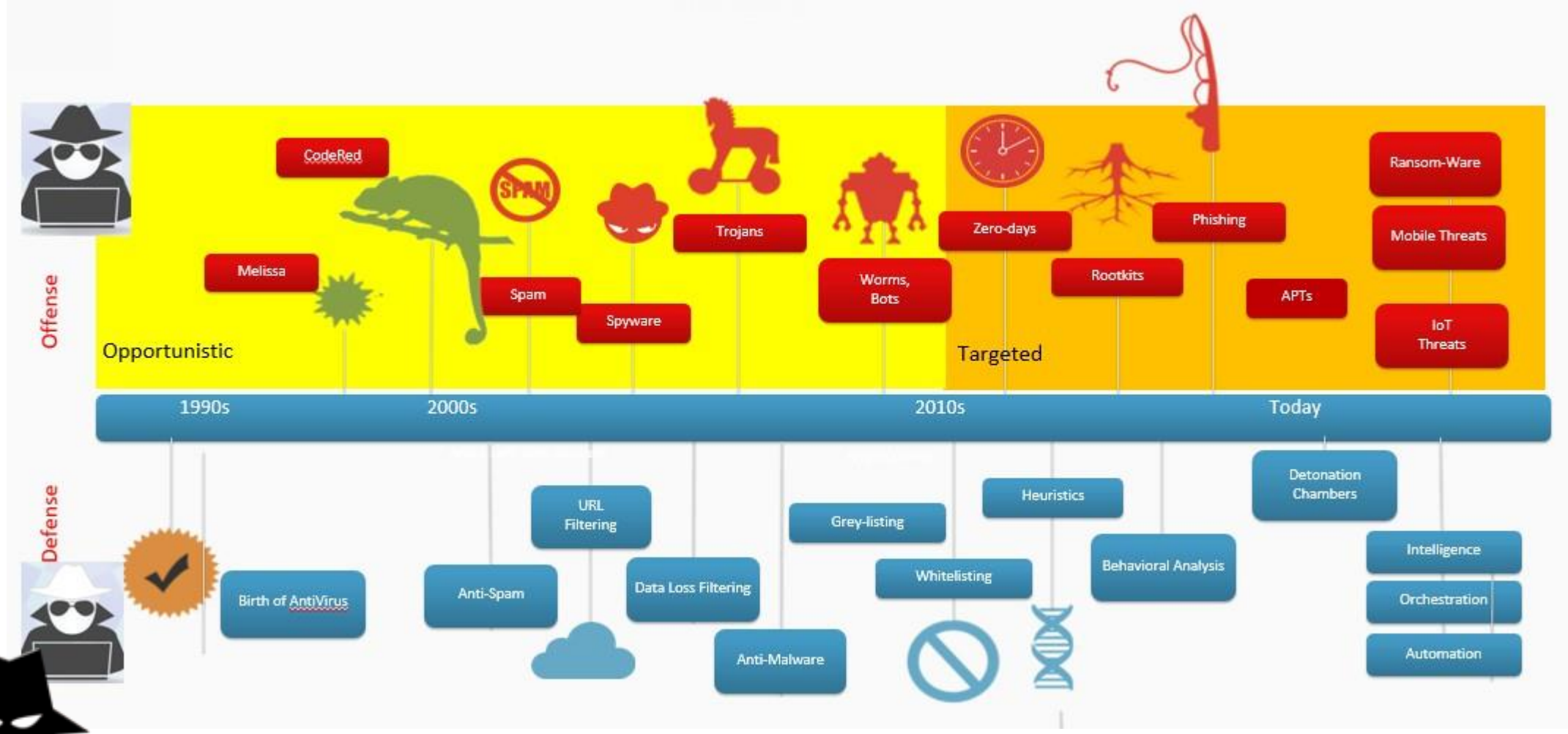
- Örnek : Hesabınızın kullanım süresi sona eriyor
- Örnek : Bilgilerinizi güncellemeniz gerekiyor
- Örnek : Hesabınızın güvenliği için yapmanız gerekenler

Siber Tehditler / Ransomware

- Fidye yazılımları, sistemleri ve verileri şifreleyerek arkasında bulunan siber suçlulara bir fidye bedeli ödemeden bu verilere ulaşımı engelleyen bir çeşit zararlı yazılım.

- Kötü niyetli kişilerin sitesine girildiğinde yüklenebilir.
- Bir uygulama içine gizlenmiş olabilir.
- Bir emailin ekinde yer alabilir.

Gelişen Teknik ve Araçların Yıllara göre değişimi



Siber Tehditler / Exploits

- Bir sistemin zaafiyetini kullanarak sistemi sömürmek, ele geçirmek veya bilgi çekmek için kullanılan, oluşturulan yazılım ve araçlardır.
  - Remote Exploits : Uzaktan yapılan sömürme işlemleri için kullanılır.
  - Local Exploits : Sistem üzerinde doğrudan yapılan sömürme işlemleri (hak yükseltme)
  - Zero Days Exploits : Sistem açıkları bulunduğu anda yazılır. En tehlikelisidir çünkü çözümü henüz üretilmemiştir.

APT – Advanced Persistent Threat

- Türkçeye : Gelişmiş sürekli tehdit" veya "hedef odaklı saldırı" olarak çevrilen özel bir saldırı türüdür.

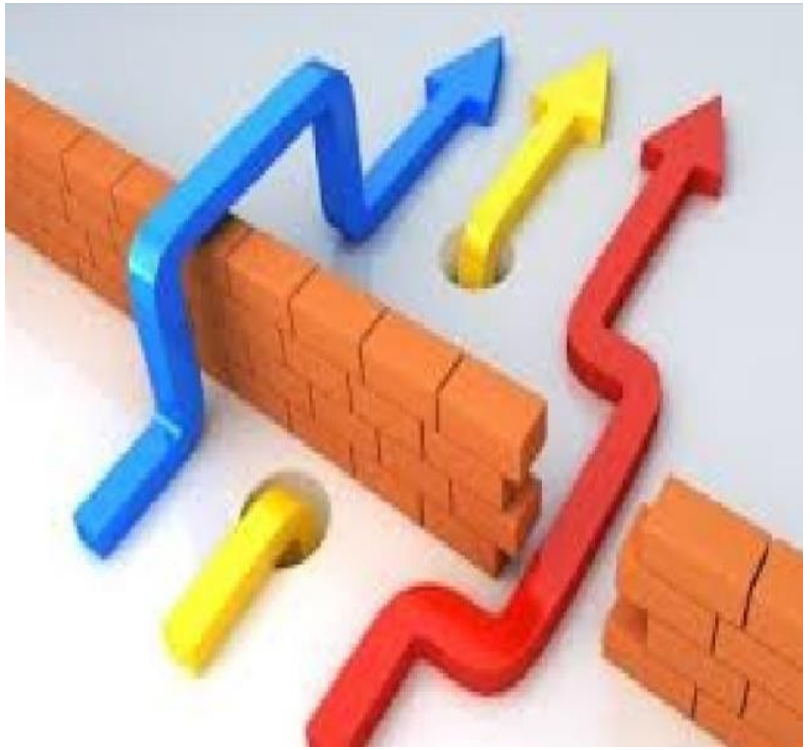
- Siber suçlular, Hacktivistler veya suç örgütlerinin motivasyon düzeyi : Birkaç deneme sonrası başka (kolay) hedefe yönlenme
- APT saldırıları : Amaçlarına ulaşana kadar saldırmaya devam ederler.

Hedefli Odaklı Bir Siber Saldırının Hikayesi

APT – Tehdit Sınıflandırması

- Basit tehdit: “wifi hackleme” ve “facebook patlatma” seviyesinde 1-2 kaynak okumuş “meraklı”, metodoloji bilmeyen, başlangıç seviyesi saldırganlardır.

- Akıllı tehdit : Sürekli akıllı tehdit : İleri düzey teknik becerisi, hedef aldığı şirket veya kuruma sızmak için yürüttüğü sosyal mühendislik çalışmalarını yapan saldırganlardır.
- İleri seviye tehdit : Sürekli İleri Seviye Tehdit : APT olarak adlandırdığımız tehdit türü (sürekli ileri seviye tehdit) en gelişmiş teknik beceri ve en yüksek seviyede motivasyon gerektiren saldırılardır. Örnek : Rusya’nın APT28 ve Çin’in APT1 grupları.



Bölüm 3.1 :

Siber Güvenlik (Ransomware – Fidye Yazılımları)

Ransomware (Fidye Yazılımları)

NEDİR ?

- Fidye yazılımları, sistemleri ve verileri şifreleyerek arkasında bulunan siber suçlulara bir fidye bedeli ödemeden bu verilere ulaşımı engelleyen bir çeşit zararlı yazılım.

NASIL BULAŞIR?

- Bir link tıklamak kadar uzakta. PTT Kargo, Turkish Kargo, Telekom Faturaları vs.
- Sosyal Mühendislik, Zararlı Reklam (Malvertising), İstismar Kitleri (Exploit Kits), Bir siteye göz atarken (Drive by Downloads)

NE İSTER?

- Bitcoin, Başkasına yükle, para edecek görüntü, video, bilgi..

Ransomware (Fidye Yazılımları)

WANNACRY RANSOMWARE

CR&T Computer Research & Technology

WannaCry has been making headlines but ransomware is nothing new right? WannaCry is a much more aggressive variant. While you may be internet savvy, if a user on your network gets infected and your machine is not patched, you may get infected and encrypted as well.

CR&T recommend immediate patching of computers to protect against this particular variant and to test backup procedures as a more general protection against all types of encryption malware.

1

1 - A MALICIOUS EMAIL
An email either with a malicious attachment or linking to a malicious website is clicked by a user.

2

2 - INFECTION SPREADS
Most ransomware stops here and encrypts the user's computer. WannaCry instead uses a Windows Exploit to spread to other network computers. This exploit (CVE-2017-0144) affects from Windows XP through to Windows 10, including Windows Server editions. This means that one computer can encrypt the entire network, regardless of their permissions on other computers.

3

3 - ENCRYPTION BEGINS
The encyption routine can take as little as 28 seconds to encrypt a single computer.

4

4 - RANSOM NOTE GIVEN

5

5 - PAY RANSOM OR RESTORE BACKUP

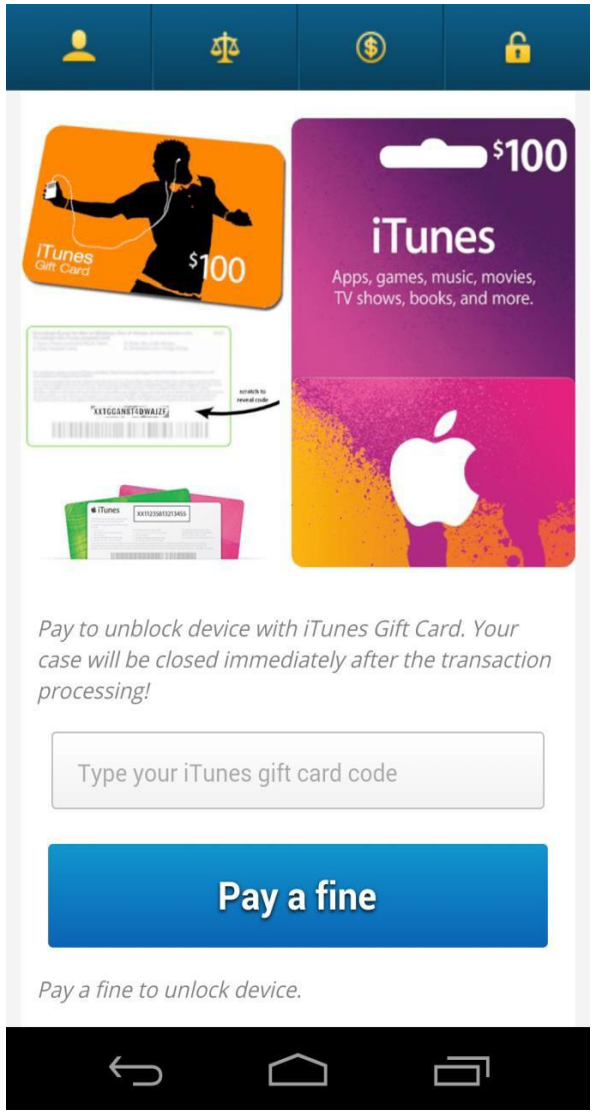
Along with security software and patch management, a strong backup practice is an essential part of ransomware prevention. In fact nowadays more backup restores are due to ransomware infections than traditional disaster recovery reasons.

SOURCES
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
CREATED BY
David Graham - Computer Research & Technology (team@crt.net.au)

visme

Ransomware – WinLocker, FileLocker

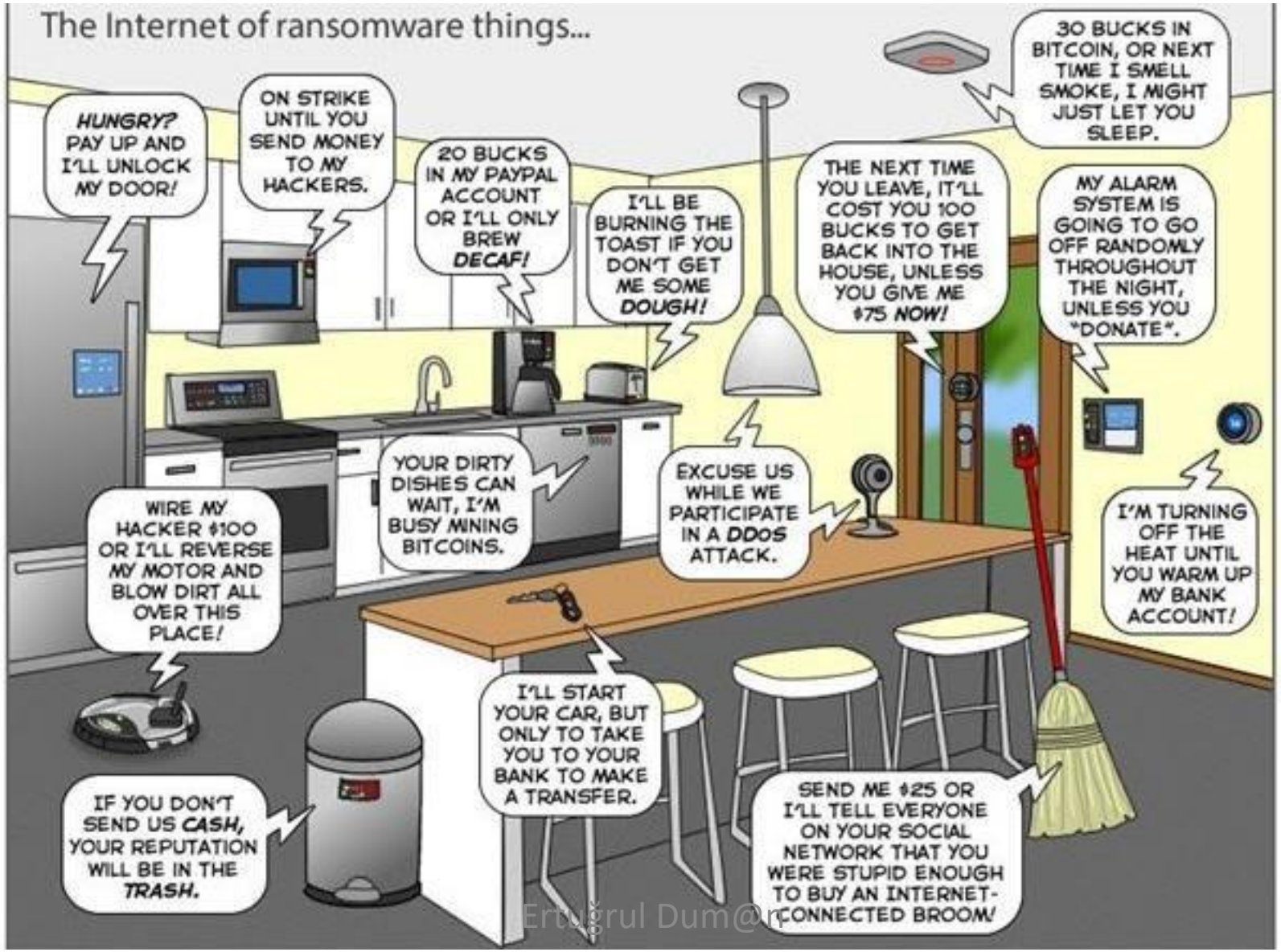
Ransomware – Mobil Cihaz



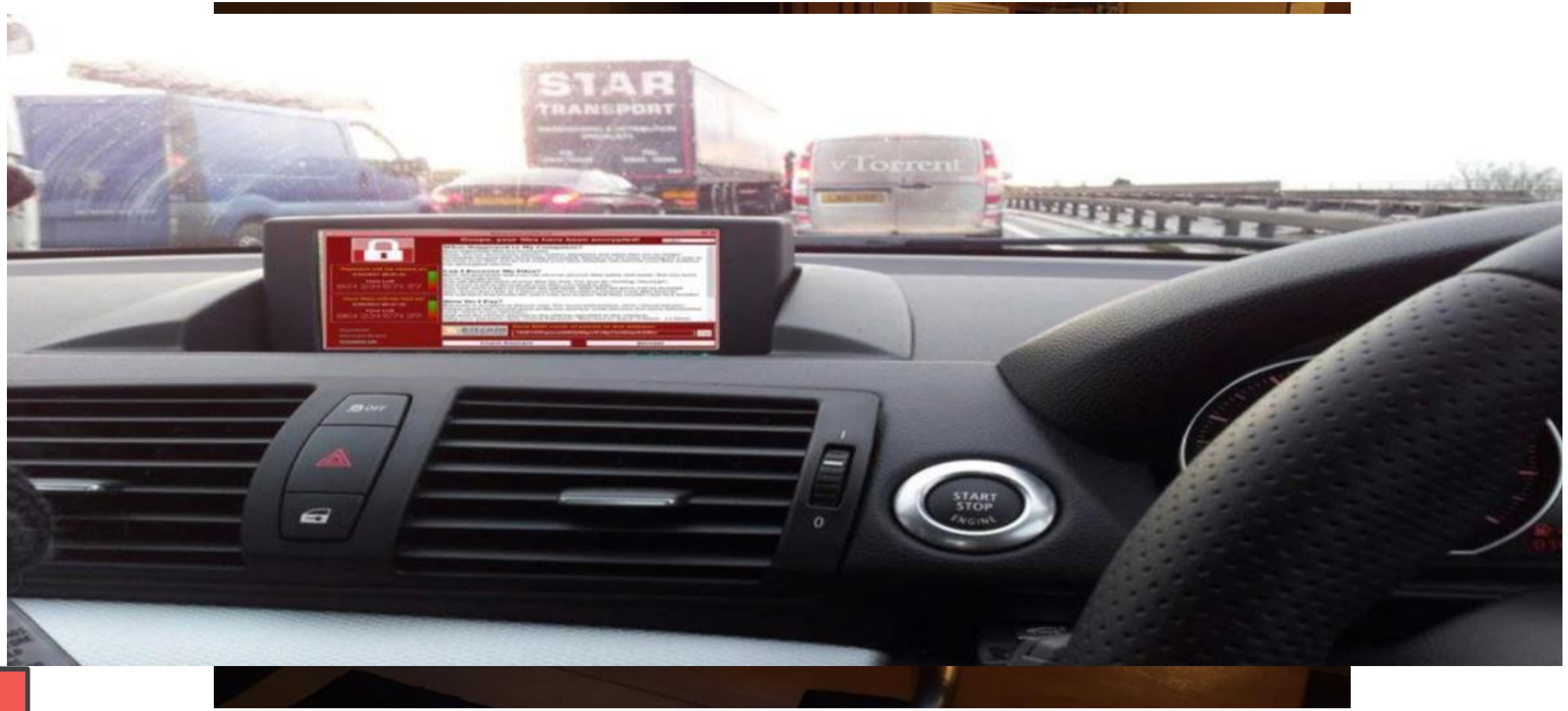
IoT – Internet of Things

- Internet of Things (Nesnelerin İnterneti)
- 2023 yılında toplam cihaz sayısı tahmini 29 milyar.
- 2020 yılında toplam cihaz sayısı 20.8 milyar.
- 2016 yılında tehdit bu cihazların tehdit olarak kullanılmaya başladı.

Ransomware – Nesnelerin İnterneti



Ransomware – Nesnelerin İnterneti



Ransomware – Önlem

Back Up and Restore
Automated: 3 copies, 2 formats, 1 air-gapped from network

Control Access
Limit access to business-critical data

Patch
Minimize vulnerability exploitation

Don't Pay the Ransom
Pay-offs encourage further attacks

Educate employees on phishing
Awareness, best practices, simulation testing

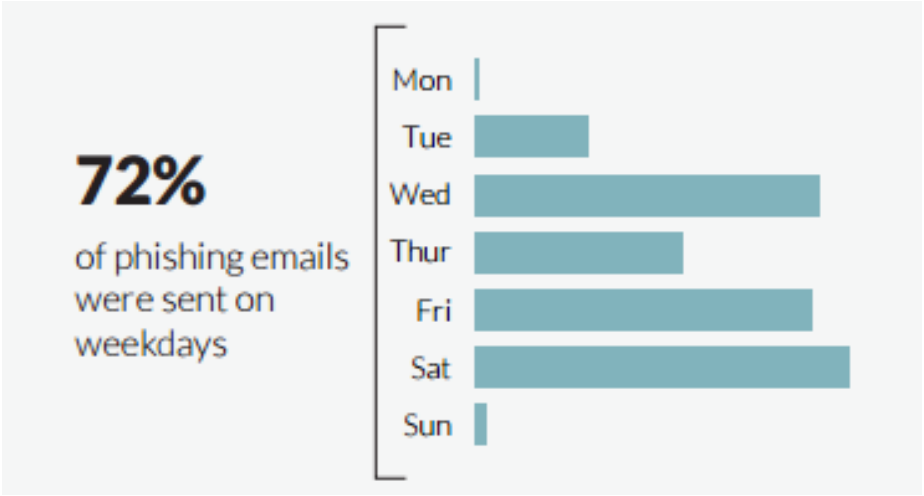
Improve Security Posture
Behavior monitoring, additional technologies

Bölüm 3.2 :

Siber Güvenlik (Sosyal Mühendislik/Oltalama)

Social Engineering – Sosyal Mühendislik

- Phishing (Oltalama) : Bilindik sitelerin kopyalarını yaparak bu siteler üzerinden bilgi çalma.
- Bire-bir İkna : Telefon vs ile kullanıcıyla iletişime geçerek kişisel bilgilerin alınması
- Güven kazanarak bilgi edinmek : Bir başkası yerine geçerek, karşısındakinden bilgiler alma.



Sosyal Mühendislik – Oltalama Nasıl İşler?

Oltalama yöntemleri yıllarla birlikte değişmedi: Psikolojik bir kanca ile kurbanlar yemlenir, böylelikle sahte bir forma ya da uygulamaya yönlendirilir.

3 adımda oltalama :

1. Hedef Seçilir - Uygun bir kurban seçilir, kurban ile ilgili bilgiler toplanır.

2. Sosyal Mühendislik Uygulanır - Bilgileri çalmak ya da zararlı yazılım (malware) yüklemek için uygun bir senaryo hazırlanır, kurbanların yemi yutması beklenir.

3.Teknik Mühendislik - Sahte web siteleri oluşturulur, güvenlik tedbirleri atlatılarak kurbanların bilgisi çalınır.

Oltalama - Adım 1 - Hedef Seçilir

Uygun bir hedef seçilir, hedef ile ilgili bilgiler toplanır.

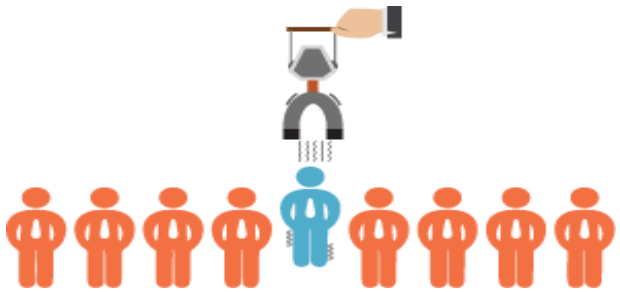
Hedef nasıl seçilir?

- Siber Suçlulardan satın alınan kullanıcı bilgileri arasından,
- Zayıf şifreye sahip sitelerden çalınan bilgilerden,
- Sosyal Medya'dan toplanır,
- Spam Mail listesinden rastgele seçilir.

Hedef olmamak benim elimde mi?

Oltalama - Adım 2 – Sosyal Mühendislik

Bilgileri çalmak ya da zararlı yazılım (malware) yüklemek için uygun bir senaryo hazırlanır, kurbanların yemi yutması beklenir.



Sosyal Mühendislik Hangi Şekillerde Karşımıza Çıkabilir?

- Doğrulamak için bilgilerinizi giriniz.
- Kargo teslimi için bilgilerinizi onaylayın.
- Tatil kazandınız, bilgilerinizi girin.
- Fatura ödeme için Kredi Kartı bilgilerinizi girin,
- Kredi kartı aidat iadesi için bilgilerinizi girin,
- İş başvurusu için bilgilerinizi girin,
- HGS ödemek için bilgilerinizi girin,
- Sitemizi ziyaret eden bir milyonuncu kişisin, hediye kazandın,
- Adınız yasa dışı bir suça karıştı, yardım edelim.

Başımıza geldiğinde engellemek elimizde mi?

Oltalama - Adım 3 – Teknik Mühendislik

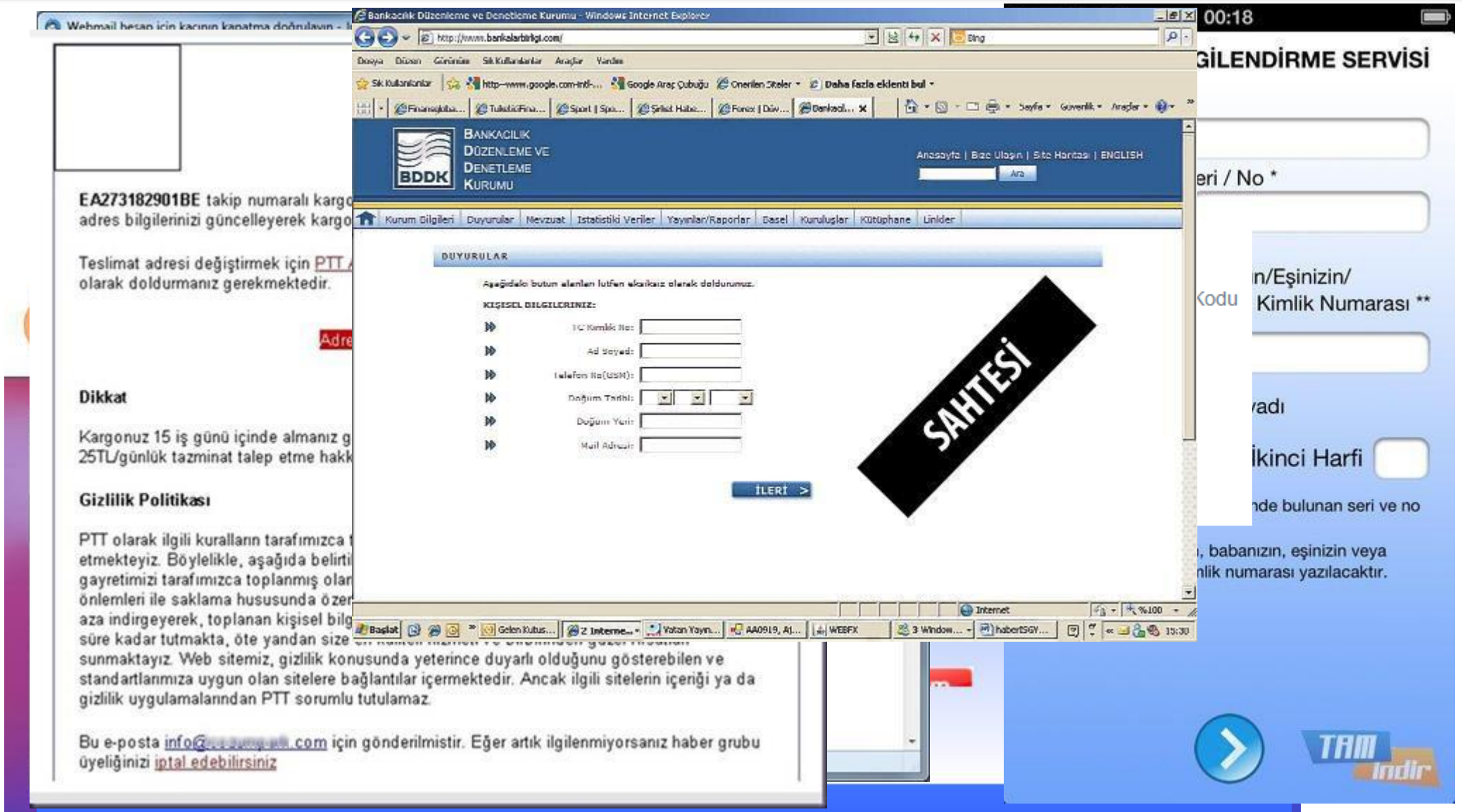
Sahte web siteleri oluşturulur, güvenlik tedbirleri atlatılarak kurbanlara ulaşılmaya çalışılır.

Hangi Yöntemler Karşımıza Çıkabilir?

- Gerçek bir site ele geçirilir, kullanıcıların girmesi beklenir,
- Yanıltıcı bir URL oluşturulur,
- Yanıltıcı bir Domain oluşturulur,
- Yanıltıcı https sertifikası oluşturulur,
- E-posta ekine çalıştırılabilir kod konulur,
- E-posta ekine Zararlı Makro içeren doküman konulur.

Başımıza geldiğinde engellemek elimizde mi?

Oltalama Yerel Örnekler



Sosyal Mühendislik Neden Etkilidir?

Sosyal Mühendislik Tanımı : Psikolojik yanıltmalar ile insanlara istemedikleri eylemleri yaptırmak ve bilgilerini ifşa etmesini sağlamak.

Kendinizi «Özgür İradenizle» istemediğiniz bir işi yapar bulursanız üzülmeyin.

Hacker'ların bu davranışınız için bazı psikolojik prensipleri kullandıklarını unutmayın..

Robert Cialdini – İkna Psikolojisi
Influence: The Psychology of Persuasion

Sosyal Mühendislik İkna Psikolojisi - Sonuç

- Kurallar sadece dijital market için kullanılmıyor.
- Uyanık olun.
- Kolay ikna olmayın, şüpheci olun.
- Üzerinize oynanmak istenen oyunu bilirseniz daha zor kandırılırsınız.

Bölüm 4:

SANAL SİBER GÜVENLİK ORTAMI LABORATUVAR VE KURULUMLARI

Sanallaştırma (Virtualization)

Birden fazla işletim sisteminin aynı fiziksel ekipman kaynaklarını paylaşarak çalışmasını if ade eder.

Türleri;

- Sunuc u Sana ll aştır m a (Server Virt ualization)
- Depolama Sanallaştırma (Storage Virtualization)
- Ağ Sanallaştırma (Network Virt ua lization)
- Masaüstü ve Dizüstü Sanallaştırma (Desktop & Laptop Virtualization)
- Uygulama Sanallaştırma (Application Virtualization)

Sanallaştırma Yazılımları

- VMware {VMware)
- VirtualBox {Oracle)
- Hyper-V (Microsoft)
- XenServer (Citrix)
- Xen Project
- OpenVZ

https://customerconnect.vmware.com/en/downloads/info/slug/desktop_end_user_computing/vmware_workstation_player/17_0

VirtualBox

https://www.virtualbox.org/wiki/Downloads

Microsoft
Hyper-V

Laboratuvar Ortamı

Sanallaştırma yazılımı ile oluşturulan sanal makinaların oluşturduğu ortamdır. Bir Siber Güvenlik Sanal Laboratuvar ortamında bulunabilen sistemler;

Linux İşletim Sistemleri (Dağıtımları)

- **Kali,** Debian, Fedora, Ubuntu, Suse,vb.. Zafiyet Çatı Sistemleri (Vulnerable)
  - **Metasploitable, Holynix,Kioprtx, Hack2net, vb..**

Microsoft işletim Sistemleri

- Windows7·8·10, 2008·l012-20J6vb..

Veritabanı Sistemleri

- **MySQL, Ms SQL. Orade, Postgresql , Nosql , vb..**

Ağ ve Güvenlik Sist emleri

- **Firem ll(Checkpoin, t Pfsense)l,PS/IOS(Suricata,Snort), Roter(C.isco, Juniper),GNS3, vb..**

Kurumsal Uygulama Sunucu Mimarileri

- **Shat(p' 01nt,,Weblogic, SAP,Apac.hc to mc,.ı vb..**

Unix i şletim Sistemleri

- **FreeBSO, Open&SO,Sofarlş,vb..**

İstemci Uygulamaları

- **Java, POF, Flash, Browser(Tar.ıyıcılar), vb..**

içerik Yönetim Sistemleri

- **Wordpress, Joomla, Oıupal, vb..**

Antivirüs Sisteml eri

- **Kaspcrsky,Symantee,Bitdefcınder, McAfco, vb..**

Ağ Hizmetleri

- **ONS,Eposta,FTP,We-b-www,VPN,vb..**

Kurulumlar

- Sanall aştırma Yazılımı
  - **VMware** Workstation Player {VMware)

    veya
  - VirtualBox {Oracle)
- **Kali** Linux Dağıtımı
- Metasploitable2

MacOS için Fusion
Amd içind e.. Kali?

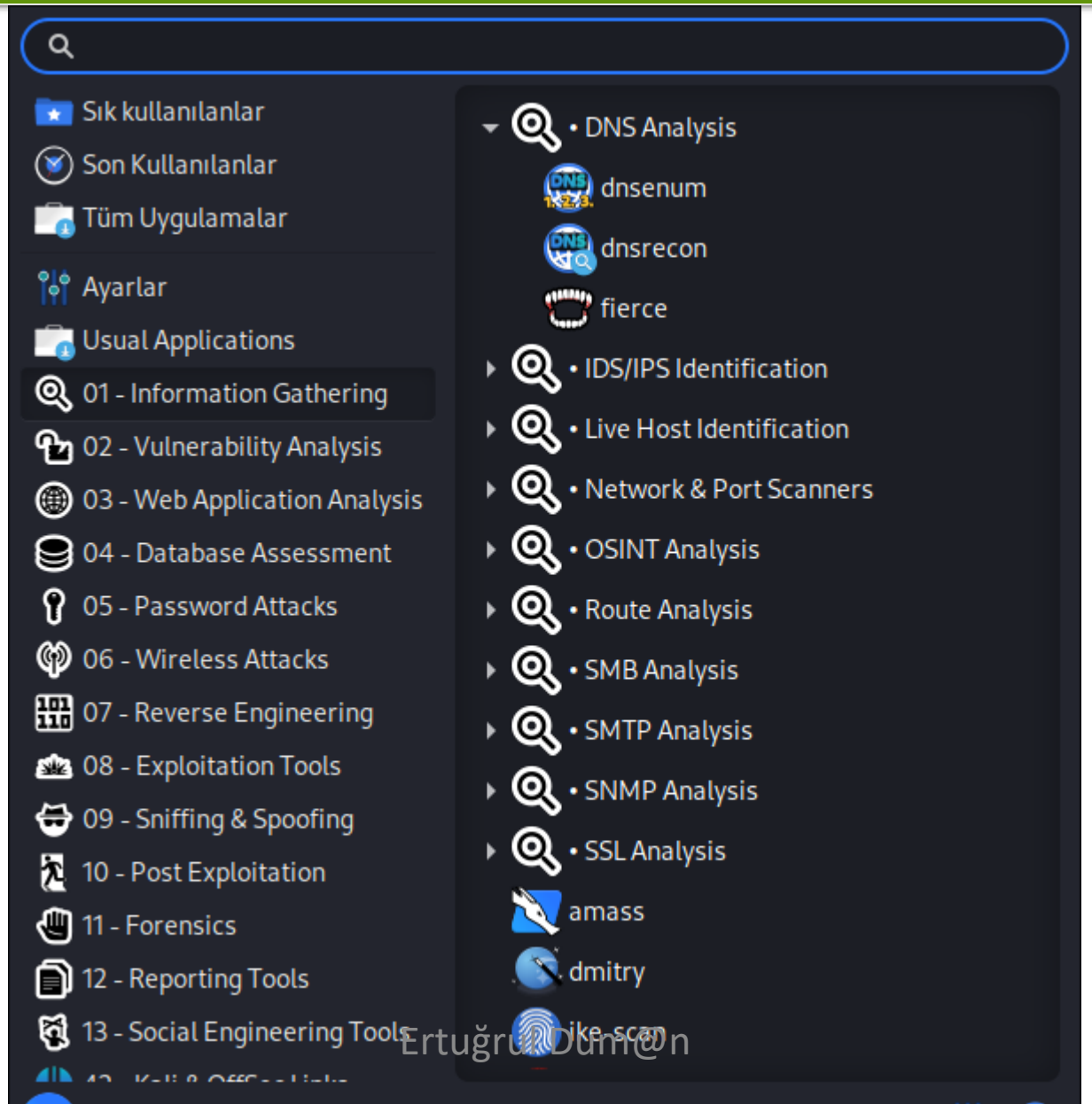
Bölüm 5:
Siber Saldırı / Sızma Testi Bilgi Toplama Araçları

Sızma Testlerinde Bilgi Toplama

- Bilindiği üzere sızma testi yapıldığında hedefe istenildiği yerden yaklaşmak her zaman mümkün olmamaktadır. Hedef sistemin durumunu göz önüne alındığında bir çok karmaşık yapı ile karşılaşılabilmekte ve sızma testi yapan kişiler için bazen anlamlandırması zor durumları ve şartları karşısına çıkarabilmektedir.

- Sızma testlerinde karmaşalardan sıyrılmak ve zor durumları aydınlandırabilmek için **sistem hakkında bilgi sahibi olmak kritik bir faktördür**. Sistem hakkında yeterli bilgi sahibi olunmadığı takdirde test işlemi oldukça fazla uzadığı gibi, sonuçları da çok sağlıklı olamayacaktır. Fazla bilgi sahibi olmanın bir zararı olmayacağı gibi aksine faydası olacaktır.

Bilgi Toplama Kali-Linux



Sızma Testlerinde Bilgi Toplama

- Kısacası bir Sızma testi işleminde hedef sistem hakkında edinilen bilgiler size gideceğiniz yolun nasıl bir yol olabileceği hakkında önemli görüşler bildirir. Çoğu Hackerın katıldığı gibi bir hedefe sızma işlemi sırasında bilgi toplama aşaması aslında işin yüzden 90'dan fazlasını oluşturduğunu söylemek yanlış olmaz.

- Sızma testi sırasında bilgi toplamayı çeşitlendirebiliriz. Bunlar **Aktif ve Pasif** bilgi toplama yöntemleridir.

PASİF Bilgi Toplama

- Herkese açık bilgilerin taranmasına verilen bilgi toplama yöntemidir. Hedefin kendisi hakkında bir bilgi toplandığından haberi olmaz. Direkt olarak hedefe bir bağlantı gerçekleştirilmez. Pasif bilgi toplama için kullanılan araçlardan bazıları ve özellikleri şunlardır.

  - theHarvester
  - Netcraft
  - Maltego
  - Whois
  - Nslookup
  - Google Dorking
  - Shodan
  - TinfoLeak

PASİF Bilgi Toplama

theHarvester

Email, subdomains, hostsları bulmak için kullanılan python ile yazılmış bir tooldur. Kali Linux'a kurulu bir şekilde gelmektedir. Oltalama saldırıları yapmak için önemli bilgiler verebilir. Pasif bilgi toplama yaptığı gibi, aktif bilgi toplama yaptığını da unutmamak lazım.

https://github.com/laramies/theHarvester.git adresinden indirilebilir.

Netcraft

Netcraft bir web sitenin web sunucusunu, işletim sistemlerini, arka planda çalışan yazılımları öğrenmek için kullanılan bir web sitesidir. Hızlı bir şekilde sonuç verdiği için tercih edilmektedir.

PASİF Bilgi Toplama

Maltego

İnternetteki çeşitli yerlerden aranan kişi yada web sitesinin verilerini toplayarak grafiksel olarak sonuçlarını döndürebilen bir uygulamadır. Hedef kişinin Facebook, Twitter, İnstagram vb. sosyal medya hesaplarına keşif yapabildiği gibi e-posta adresi için de aramalar yapabilir. Kolay ve anlaşılabilir grafiği sayesinde tercih edilen araçlardan biridir.

Whois

Hedef web sitenin alan adını sorgulayarak tuttuğu kayıtları bulmamızı sağlar. Bu kayıtlar adres, e-posta, telefon numarası olabilir.

PASİF Bilgi Toplama

Nslookup

nslookup, bir Internet sunucusu yöneticisinin veya herhangi bir bilgisayar kullanıcısının bir ana bilgisayar adı girmesini sağlayan bir programın adıdır ve karşılık gelen IP adresini öğrenir . DNS sorgusu yaparak bilgileri toplayarak kullanıcının alan adlarını veya IP adreslerini bulmaya yarayan bir araçtır.

Google Dorking

Bilgi toplama aşamasında hazır araçlar yada yazılımlar çoğu şeyi yapsa dahi Google araması da çoğu zaman yapılır. Kullanılan programların hata yada güncelleştirme sorunlarında kaynaklı olarak Google araması yapmak güvenilir bir seçenektir.

PASİF Bilgi Toplama

Shodan

Herkese açık bir şekilde gösterilen IOT cihazlarını bulmaya yarayan bir arama motorudur. Google'a göre içeriğindeki veriyi detaylıca gösterir ve kullanıcıyı kısıtlayan sonuçlar döndürmez.

TinfoLeak

Twitter hesapları üzerinden bilgi edilerek istihbarat toplanmasına yarayan uygulamadır. Aranan kişinin detaylıca bilgilerini toplayabilir.

https://github.com/vaguileradiaz/tinfoleak adresinden indirilebilir.

AKTİF Bilgi Toplama

- Pasif bilgi toplamanın aksine hedef ile doğrudan iletişime geçilir. Hedefin kendisi hakkında bir bilgi toplandığından haberi olabilir. Aktif bilgi toplama için kullanılan araçlardan bazıları ve özellikleri şunlardır.

  - Sandmap
  - Yasuo
  - dirb
  - Dmitry
  - Devploit v3.6
  - TrackerJacker
  - BruteX

AKTİF Bilgi Toplama

Sandmap

Çok sık tercih edilen nmap toolunu kullanarak ağ ve sistemleri keşfetmek için kullanılan bir araçtır. Nmap'e göre kullanılıcı arayüzü sağlayarak daha kolay bir deneyim sunar. Nmap Scripting Engine (NSE) desteği ile kullanabildiği gibi, TOR desteği de mevcuttur.

https://github.com/trimstray/sandmap adresinden indirilebilir.

Yasuo

Ruby dili geliştirilmiş third part yazılımları tarayan ve üzerlerindeki açıkları yakalamaya çalışan uygulamadır.

https://github.com/0xsauby/yasuo adresinden kurulabilir.

AKTİF Bilgi Toplama

dirb

web sitelerin görütüleyebileceğimiz uzantılarını bulmaya yaran uygulamadır. Bulunan uzantılar hakkında sonuçlarıda döndürebilir. Kali Linux'a kurulu olarak gelir ve çok sık tercih edilen tool'dur.

DMitry

Subdomain, email adresleri , açık port taraması , whois sorgusu gibi çeşitli bilgileri elde etmek için kullanılır.

Devploit v3.6

Python ile geliştirilmiş bilgi toplama araçlarından biridir. HTTP başlıklarına, port, GeoIP, Subnet bilgilerine bakmak için kullanılabilir.

https://github.com/joker25000/Devploit adresinden indirilebilir

AKTİF Bilgi Toplama

TrackerJacker

Linux ve MacOS'ta desteklenen bağlantı gerçekleştirmeden Wifi ağının haritasını çıkarmaya yarayan araçtır. Wifi ağına bağlı tüm cihazları görüntüleyebildiği gibi bant genişliği hakkında bilgi de verebilir. https://github.com/calebmadrigal/trackerjacker adresinden indirilebilir.

BruteX

https://github.com/1N3/BruteX.git adresinden indirilebilir. ***Nmap, Hydra & DNS*** enum gibi araçları içerir. ***BruteX'i diğer bilgi toplama araçlarından farklı kılan Brute Force(Kaba Kuvvet) saldırısı yapılmasına olanak sağlamasıdır.*** SSH, FTP vb. protokolleri açarak buna olanak sağlar.

Bölüm 6:
Tarama, Zafiyet Tespiti ve Parola Kırma Araçları

Tarama, Zafiyet Tespiti

Parola Kırma Araçları

- Ağ, sunucu veya web uygulamalarındaki açıkları tespit edebilmek için bildiğiniz üzere yardımcı pentest araçları kullanılmaktadır.
- Tüm bu araçlar herhangi bir ağ uygulamasındaki bilinmeyen zafiyetlerin tespitini sağlamaktadır.
- Eski zamanlarda sistem taramaları ve açıklıklarının tanımlanması oldukça zor ve manuel işlemler gerektirmekteydi.
- Ancak günümüzde bu pentest araçları sayesinde oldukça kolay bir şekilde taramalarımızı gerçekleştirebilmekteyiz.

Tarama, Zafiyet Tespiti
Parola Kırma Araçları

- Tarama ve Zafiyet Tespiti İçin Kullanılan Araçlardan Bazıları;
  - Metasploit
  - NMAP
  - Wireshark
  - Aircrack-NG
  - Nessus
  - Social Engineering Toolkit
  - W3AF (Web Application Attack and Audit Framework)
  - Burp Suite
  - BeEF
  - SQLmap

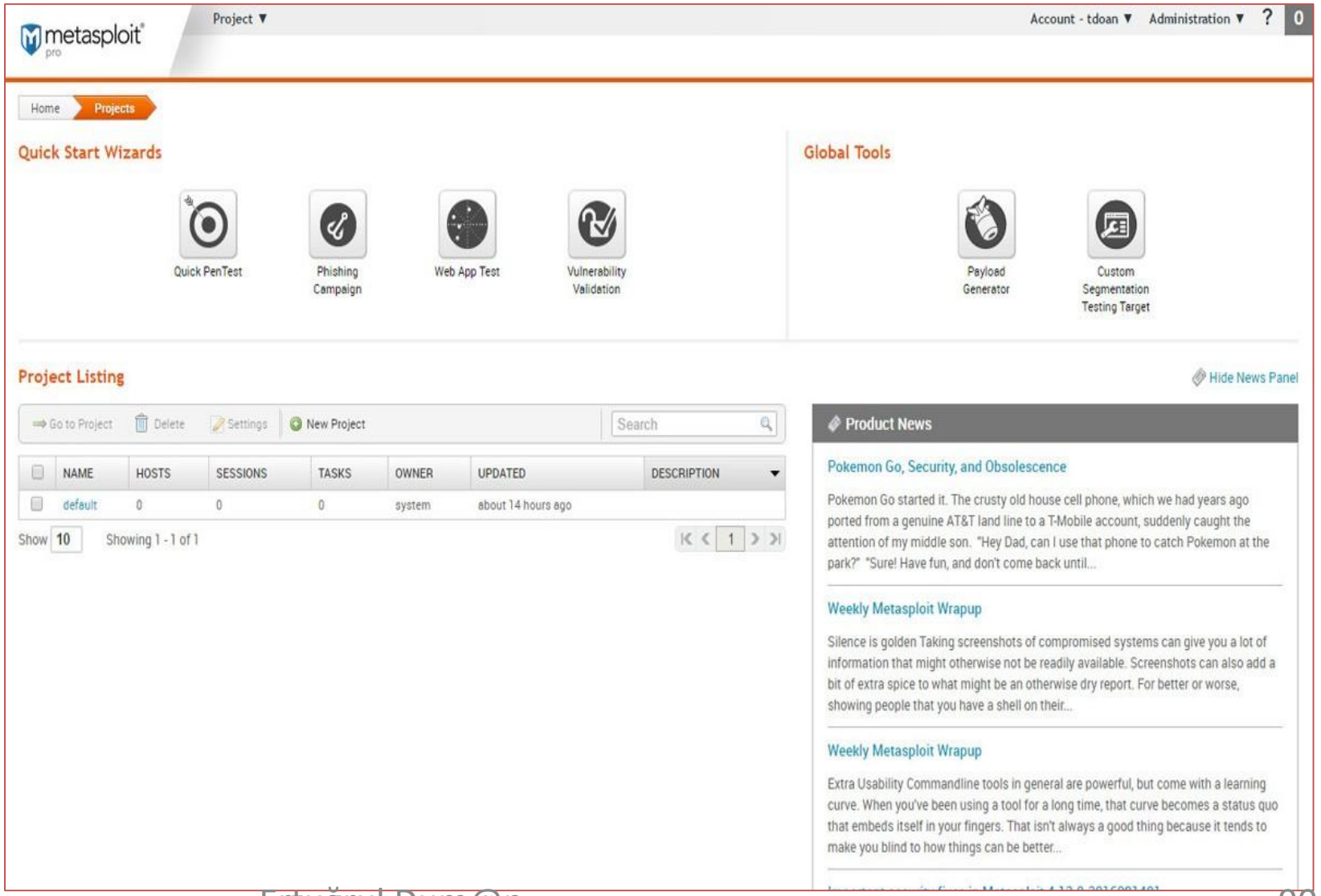
1. Metasploit

Rapid7 Metasploit; saldırgan gibi davranmanıza yardımcı olan penetrasyon testi çözümüdür.

Çeşitli zafiyetleri keşfeder, güvenlik değerlendirmeleri yapar ve savunma tekniği formüle eder.

Ayrıca, Metasploit aracını çevrimiçi tabanlı uygulamalar, ağlar ve diğer farklı sunucularda kullanabilirsiniz.

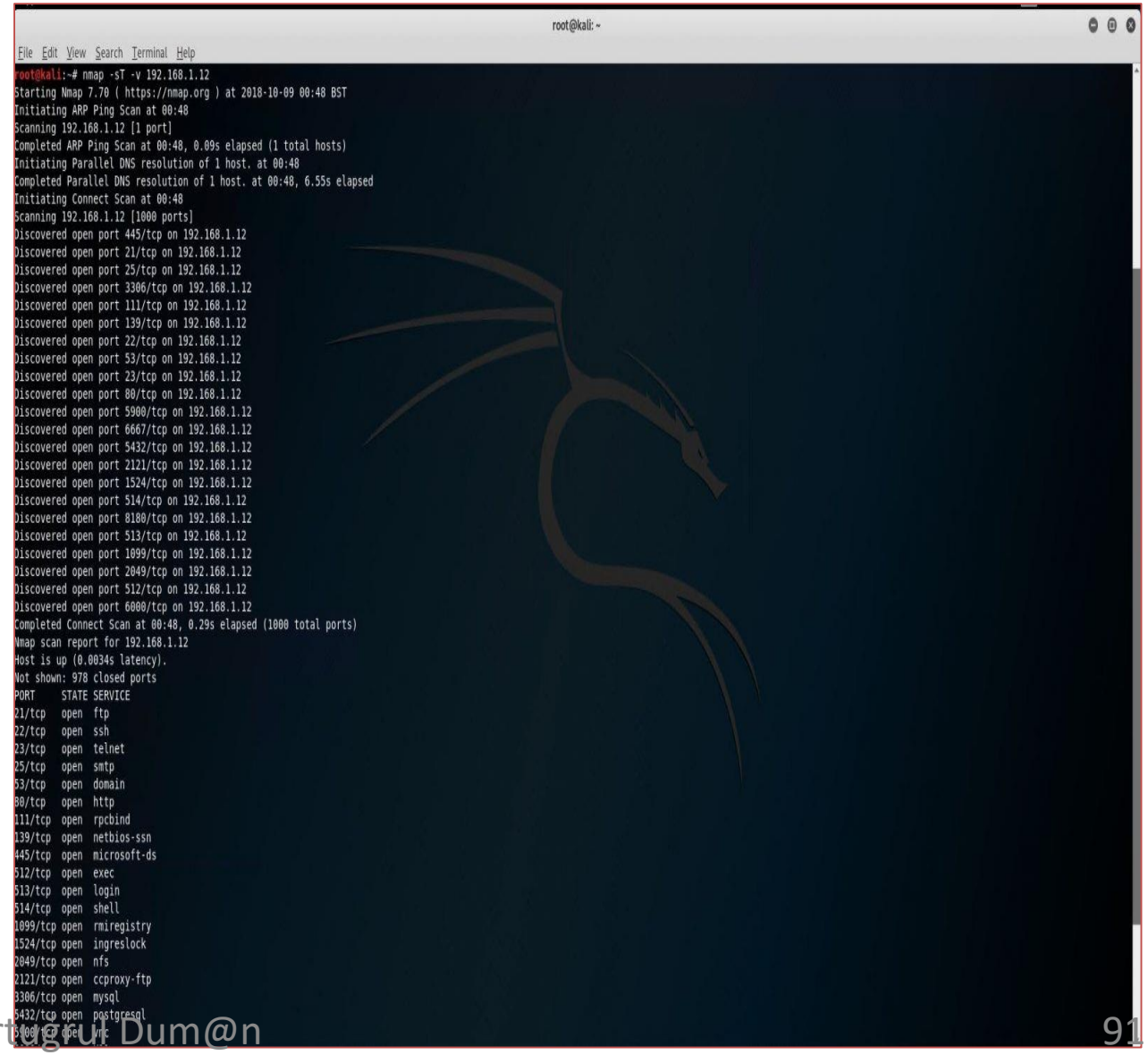
[Metasploit Linki]



2. NMAP

Nmap, ağ tarama ve zafiyet tespiti için kullanılan açık kaynaklı bir araçtır. İsmini Network Mapper'in kısaltmasından almaktadır. Ağ yöneticileri nmap'i sistemlerinde hangi cihazların çalıştığını belirlemek, mevcut ana makineleri ve sundukları hizmetleri keşfetmek, açık bağlantı noktaları bulmak ve güvenlik risklerini taramak için kullanırlar. Nmap, yüz binlerce cihazı ve alt ağı kapsayan geniş ağların yanı sıra tek ana bilgisayarı izlemek için kullanılabilir.

Nmap sistem bağlantı noktalarına ham paketler göndererek bilgi toplar. Yanıtları dinler ve bağlantı noktalarının örneğin bir güvenlik duvarı tarafından açık, kapalı veya filtrelenmiş olup olmadığını belirler. Nmap üzerinde bulunan modüller sayesinde port taraması, servis keşfi, versiyon ve işletim sistemi tespiti gerçekleştirebilir. **Nmap Linki**

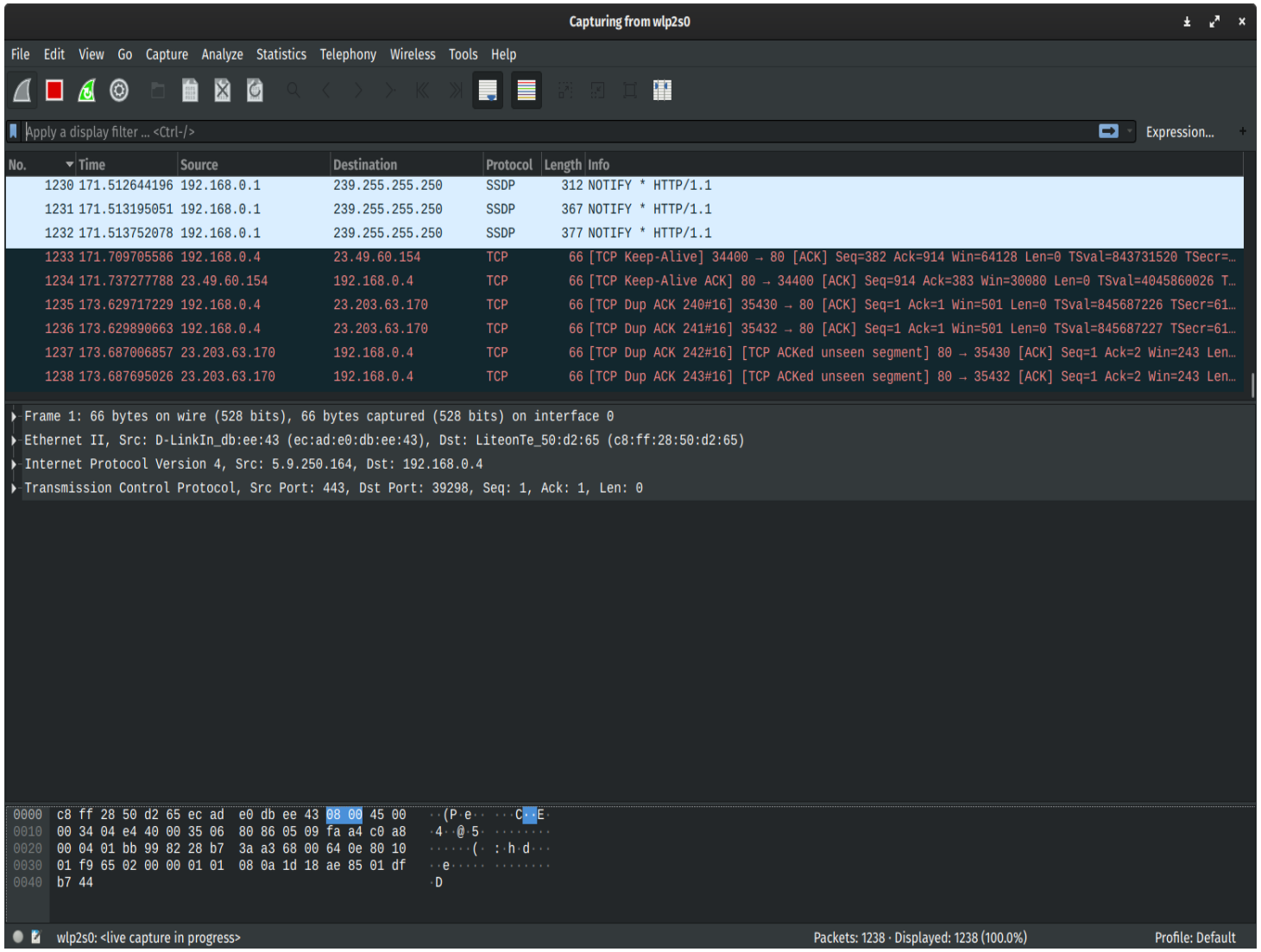


3. Wireshark

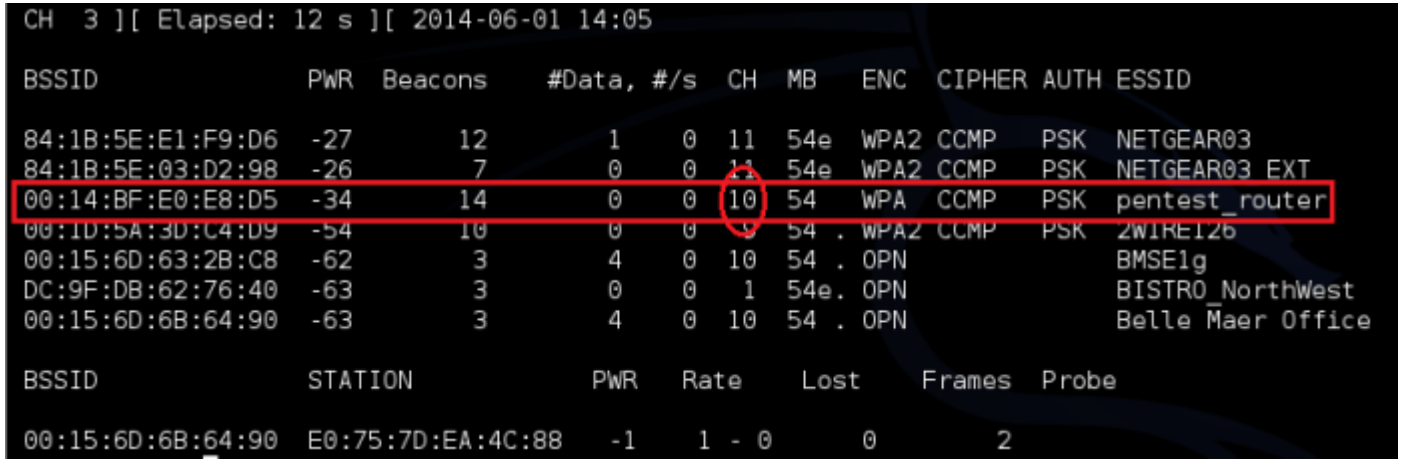
Wireshark; network trafiğinin, bir grafik arayüz üzerinden izlenmesini sağlayan, pek çok zaman hayat kurtarancı öneme sahip bir programdır.

Uygulamanın kurulu olduğu bilgisayar üzerinden anlık network trafiği izlenebileceği gibi, Wireshark daha önce kaydedilmiş dosyaların incelenmesi amacı ile de kullanılabilir.

Wireshark Linki



4. Aircrack-NG

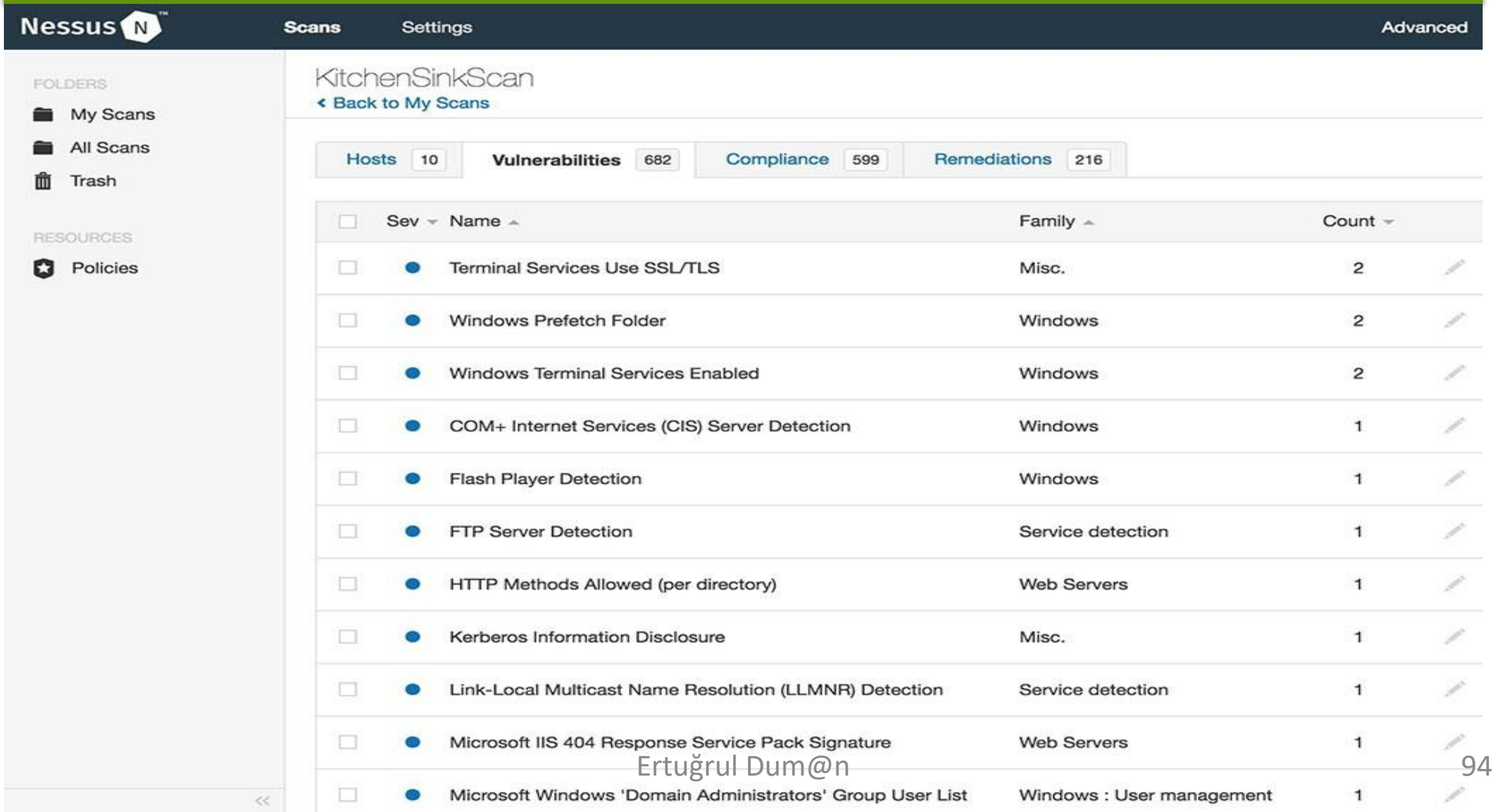


Aircrack-ng; algılayıcı, paket sezici, 802.11 telsiz LAN için WEP ve WPA/WPA2-PSK çözücü ve analiz aracından oluşan ağ yazılım takımıdır.

802.11a, 802.11b ve 802.11g trafiği sezebilen bir araçtır. Yani kısacası Wireless Hacking Tools olarak adlandırabiliriz.

Aircrack-ng Linki

5.Nessus


Nessus
Scans
Settings
Advanced
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
KitchenSinkScan
Back to My Scans
Hosts 10
Vulnerabilities 682
Compliance 599
Remediations 216
Sev
Name
Family
Count
Terminal Services Use SSL/TLS
Misc.
2
Windows Prefetch Folder
Windows
2
Windows Terminal Services Enabled
Windows
2
COM+ Internet Services (CIS) Server Detection
Windows
1
Flash Player Detection
Windows
1
FTP Server Detection
Service detection
1
HTTP Methods Allowed (per directory)
Web Servers
1
Kerberos Information Disclosure
Misc.
1
Link-Local Multicast Name Resolution (LLMNR) Detection
Service detection
1
Microsoft IIS 404 Response Service Pack Signature
Web Servers
1
Microsoft Windows 'Domain Administrators' Group User List
Windows : User management
1

5.Nessus

Nessus, dünyada birçok kullanıcısı bulunan güvenlik zafiyeti tarama programıdır. Nessus Professional, Nessus Manager, Nessus Home ve Nessus Cloud sürümleri mevcuttur. Fiziksel, sanal ve bulut ortamlarında güvenlik zafiyetlerinin ve zararlı yazılımların tespitini sağlar.

Bilişim altyapılarının güvenlik açısından denetlenmesi ve güvenlik seviyelerinin tespit edilerek açıklıklarının kapatılması gibi çalışmaları kapsayan penetrasyon/sızma testi hizmeti kurumların gerçekleşecek siber saldırılara karşı hazırlıklı ve dayanıklı olmalarını sağlar. Böylelikle penetrasyon testi yapan güvenlikçiler, hacker gibi düşünüp sisteme sızma ve ele geçirme senaryolarını uygulayarak ve saldırganların deneyebileceği tüm yöntemleri deneyerek gerçek bir saldırı ile karşılaşıldığında sistemin açıklık barındıran noktalarının onarılmış ve güvenliği sıkılaştırılmış olmasını sağlamaktadırlar.

Penetrasyon testlerinde lisanslı veya açık-kaynak kodlu araçlar kullanılmakta, otomatize tarama araçlarının yanı sıra kuruma özel manuel testler de uygulanarak mümkün olduğunca tüm zafiyetler tespit edilip düzeltilmeye çalışılmaktadır.

İç ağ penetrasyon testlerinde kullanılan en önemli araçlardan biri olan Nessus, siber suçlular tarafından kullanılan çeşitli saldırı tekniklerini simüle eden kod parçalarından oluşan pluginleri veritabanında barındırır ve tarama yapılacak cihazlarda uygulayarak sahip oldukları açıklıkları ortaya çıkarır. [Nessus Linki]

6.Social Engineering Toolkit

Social Engineering Toolkit, sosyal mühendislik saldırılarının İsviçre çakısı olarak adlandırabileceğimiz bir yapıdır.

İçerisinde web sitesi saldırısı, “phishing” saldırıları, zararlı medya yaratıcısı, “payload” ve “listener” yaratıcısı, çoklu e-posta saldırısı gibi bir sürü modül bulundurur.

Bu yapı Kali Linux ile gelen varsayılan programlar arasındadır.

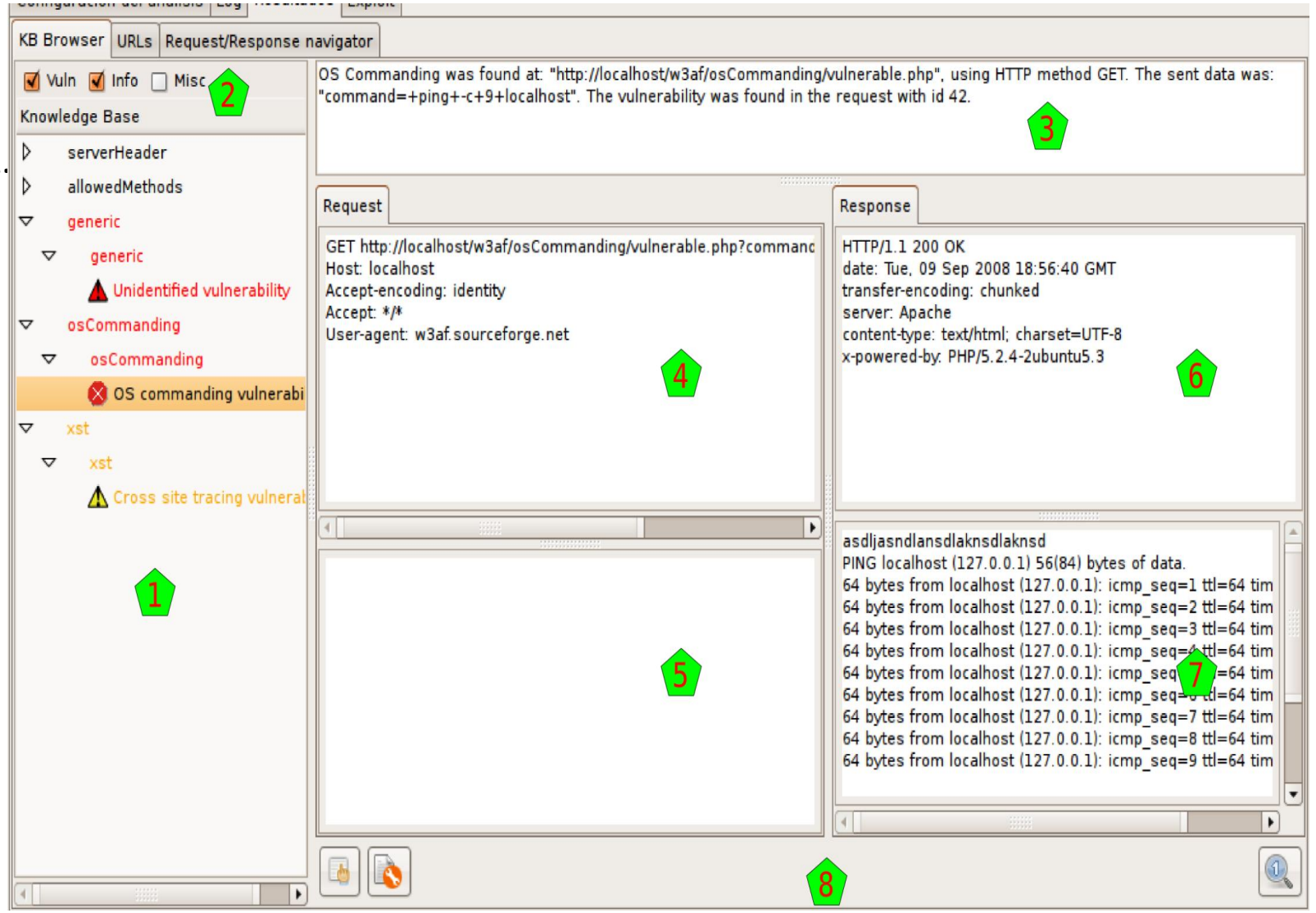
[Social Engineering Toolkit Linki]

7. W3AF (Web Application Attack and Audit Framework)

W3AF; web uygulamaları için kullanılan saldırı ve denetim programıdır. W3AF ile web site analiz ve zafiyet taraması yapabiliriz. Program arayüz ile birlikte kullanılabilmektedir.
W3af ile sayısız zafiyet tarama özelliği vardır bulabildiği zafiyet türleri;

- SQL injection detection
- SSI detection
- XSS detection
- Local file include detection
- Buffer Overflow detection
- Remote file include detection
- Format String bugs direction
- Response splitting detection
- OS Commanding detection
- File upload inside webror

[W3AF Linki]



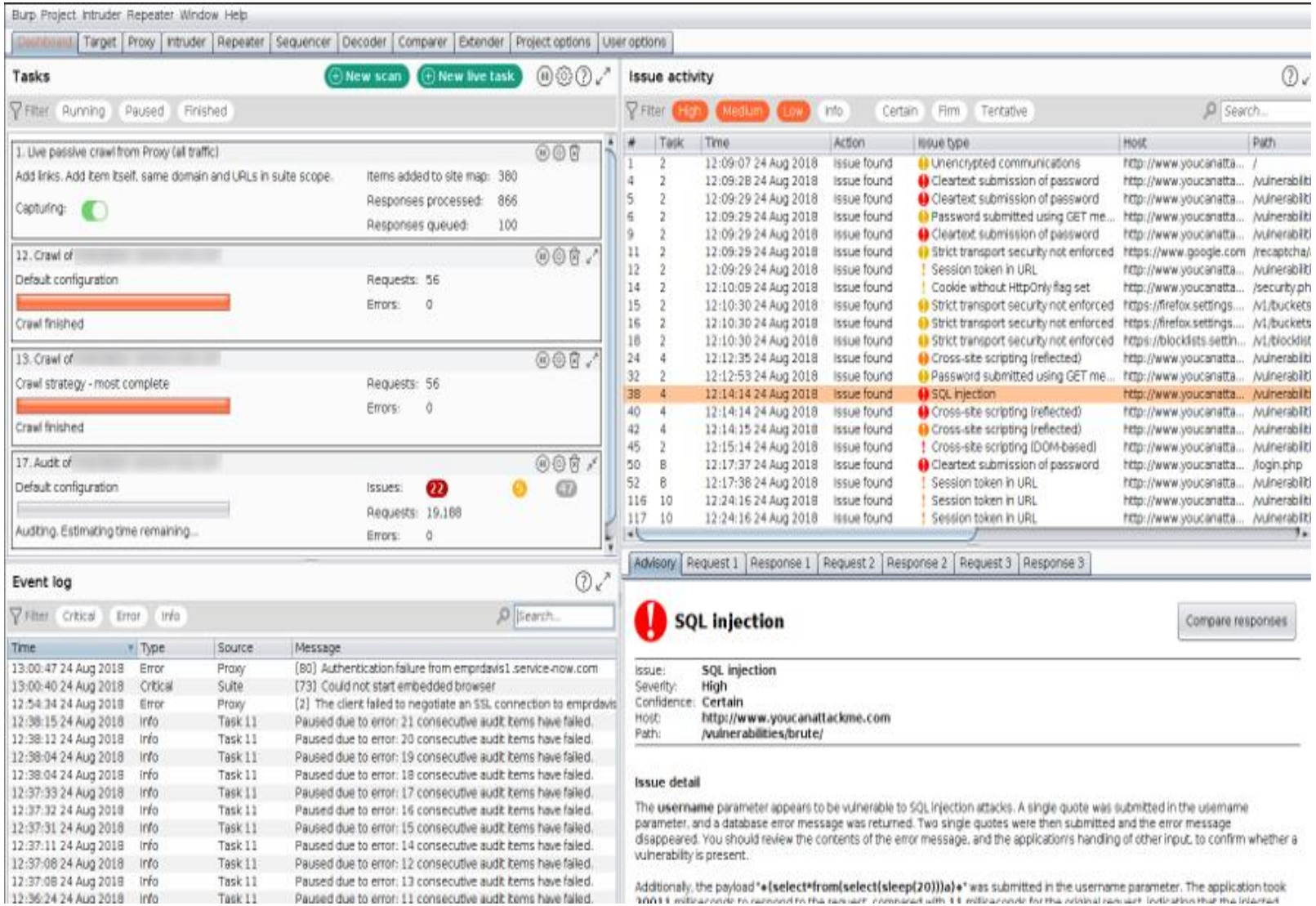
8. Burp Suite

Burp Suite, web uygulaması güvenlik testi için kapsamlı bir platformdur. Web uygulamalarının detaylı sayımı ve analizi için kullanılabilir.

Burp, HTTP/S isteklerini kolayca engelleyebilir ve kullanıcı ile web sayfaları arasında aracı görevi görebilir.

Kullanıcı web'de gezinirken gerekli ayrıntılar web sitesinden alınır. Bu bilgiler, bir web uygulamasının güvenliği hakkında fikir sahibi olmamızı sağlar.

[Burp Suite Linki]



8. BeEF

BeEF, The Browser Exploitation Framework'in kısaltmasıdır. Web tarayıcısına odaklanan bir penetrasyon test aracıdır.

Mobil istemciler de dahil olmak üzere müşterilere yönelik web tabanlı saldırılarla ilgili endişeler arttıkça, BeEF, profesyonel penetrasyon test cihazının istemci taraflı saldırı vektörlerini kullanarak gerçek bir hedef güvenlik ortamını değerlendirebilmesini sağlar.

BeEF, bir veya daha fazla web tarayıcısını kendine bağlayarak ve bunları yönlendirilmiş komut modüllerini başlatmak ve tarayıcı bağlamında sisteme karşı daha fazla saldırı başlatmak için ana sunucu olarak kullanacaktır.

[BeEF Linki]

10. SQLMap

Sqlmap, açık kaynak kodlu sql injection açıkları tespit ve istismar etme aracıdır.

Kendisine sağlanan hedef web uygulamasının kullandığı veri tabanı sistemine gönderdiği çeşitli sorgular/komutlar ile sistem üzerindeki sql injection tipini tespit eder.

Yine kendisine sağlanan parametrelere göre çeşitli bilgileri hedef veri tabanından alır.

Sqlmap Linki

Bölüm 7:
Kriptografi Steganografi

Acaba Nedir? *(Dersin özeti)*

w5bEn3JlbmNplGhhesSxciBvb
GRlxJ91bm RhlMO2xJ9yZXRtZ
W4gZ8O2csO8bmVjZWt0aXlu
VGhllEJlZGRoYQ==

Terimler ve Kavramlar

Kriptografi: Gizli yazışma sanatı anlamına gelmektedir.

Yunancada *gizli* anlamına gelen **kripto/kryptos** ve *yazılmış* bir şey yazmak anlamına gelen **grafi/graphein** kelimelerinden oluşur.

Kriptoloji: Kriptografi biliminin çalışma disiplinine Kriptoloji denir.

(Kriptoloji: Şifre Bilimidir.)

Terimler ve Kavramlar

- **Kriptografi:** Veriyi yalnızca okuması istenen şahısların okuyabileceği bir şekilde saklamak ve göndermek amacıyla kullanılan teknikler bütünüdür.

- **Kripto algoritması:** Verinin matematiksel yöntemler kullanılarak kodlanması ve okunamayacak hale getirilmesidir.

Terimler ve Kavramlar

- **Kript oanaliz :** Bir şifreleme sistemini veya sadece şifreli mesajı inceleyerek, şifreli mesajın açık halini elde etmeye çalışan kriptoloji disiplinidir.

- **Encoding :** Verinin başka bir forma dönüştürülmesidir. (şifreleme yapılmamaktadır.) ***base64*** gibi.

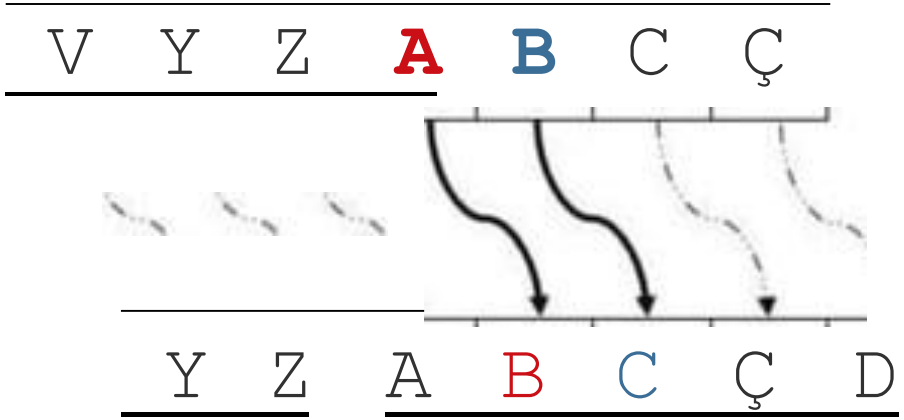
- **Stenografi :** Verinin başka veri içerisinde saklanmasıdır. (Bilgi şifr elenm ez, gizlenir.)
  - Stenografi alfabesi ile yazılması şeklinde kullanılır.

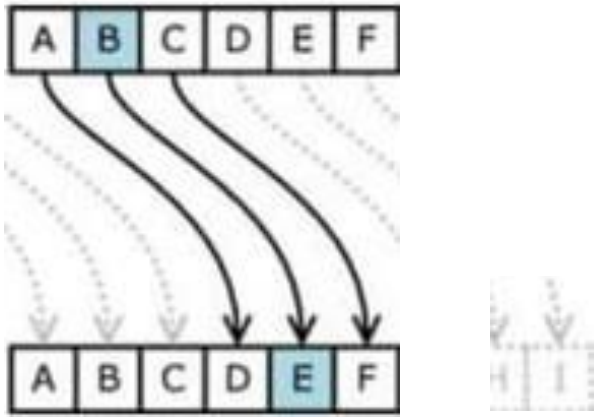
Atbash şifrelemesi

A	B	C	D	E	F	G	H	1	J	K	L	M
Z	y	X	W	V	U	T	S	R	Q	P	O	N

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	L	K	J		H	G	F	E	D	C	B	A

Sezar Şifresi (Çevrimsel Alfabe)





- Kaba kuvvet (brute-force) saldırısıyla çok kolay çözülür.
- Çünkü, Şifreleme/Şifre çözme yöntemi gizli değildir.
- Sadece 25 farklı deneme yeterlidir. (Anahtar uzayı 25 elemanlıdır.)
- Düz metin (plaintext) ve formatı gizli değildir.
- Harf değiştirme şifrelemelerinde toplam 26! farklı şifre tablosu vardır.

Scytale Cipher (Sarmal Şifrelemesi)

Çok Alfabeli {Polyalphab etic} Şifreleme

Çok alfabeli şifre leme(po lyalpha betic Cipher): J467 yılında Leon Battista Alberti tarafmdan bulunmuştur. Yerdeğiştirmeye dayalı bir şifrelemedir. Bunların en bilineni vigenere şifresidir.

Örnek (Türk alfabesine göre):

Düz Metin	: S A L D I R I	Ş A F A K T A
Anahtar	: L İ M O N L İ	M O N L İ M O
Şifreli Metin	: F İ A S V E S	Ğ O Ş L U H O

Base64

- Verinin başka bir forma dönüştürülmesidir.
  (Encoding) Şifreleme yapılmamaktadır.
- ASCII karakter lerini kul lananortamlarda iletilmesine ve saklanmasına olanak tanıyan bir kodlama şemasıdır.

Base64 Encod Ing Table

Value	Char	Value	Cher	Value	Cher	Value	Char
0	A	16	O	32	9	48	w
1	B	17	R	39	h	49	x
2	C	18	S	34	1	50	y
3	D	19	T	35	i	51	z
4	E	20	U	35	k	52	0
5	F	21	V	37	1	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	1	24	y	[illegible]	o	[illegible]	4
9	J	25	Z	41	p	57	5
10	K	28	●	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	●	60	8
13	N	29	d	45	1	61	9
14	O	30	o	46	u	62	●
15	p	31	1	47	v	63	I

Steganografi

Orijinal Resim

Gizlenmiş Resim

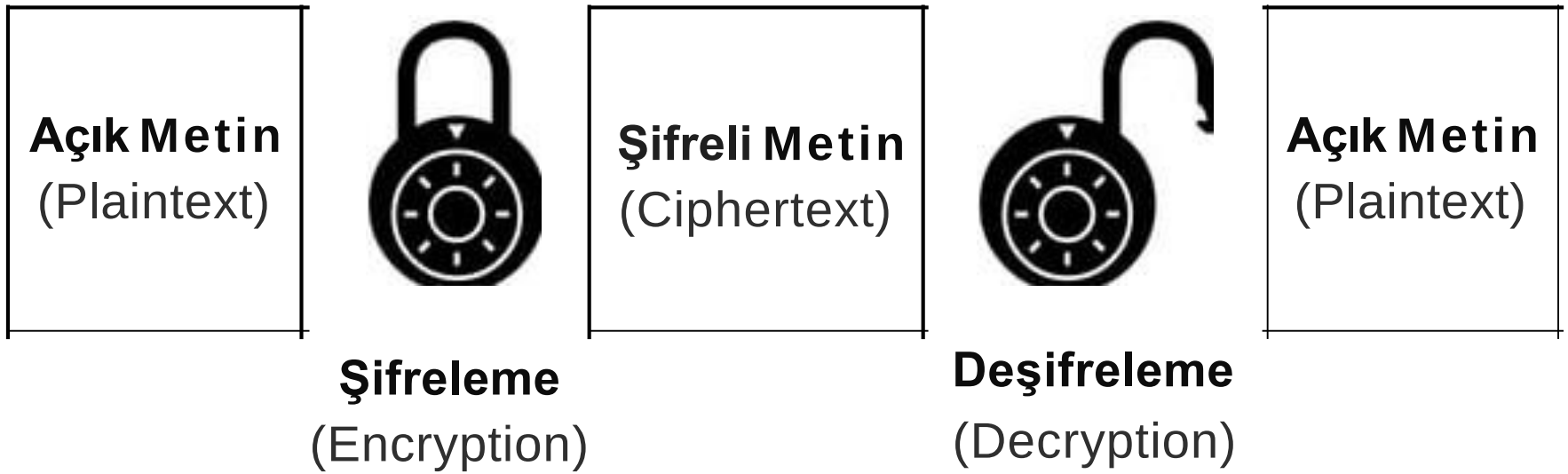
http://stylesuxx.github.io/steganography/

Terimler ve Kavramlar

- **Açık** Metin(clear text): Şifrelenmemiş, bir insanın okuyabileceği yazı veya verilerdir.
- **Şifreli** Metin(ciphered text): Bir kripto algoritması kullanılarak herkesin okuyamayacağı bir şekilde kodlanmış bilgiye denir.
- **Şifreleme:** Açık metinden şifreli metne geçme işlemidir.
- **Şifre Çözme**: Şifreli metinden açık metne geçme işlemidir.

Şifreleme -> Deşifreleme

(Encryption -> Decryption)



Terimler ve Kavramlar

- **Simetrik Şifreleme:** Hem şifreleme hem de deşifreleme için aynı anahtarı kullanan kripto sistemleridir.

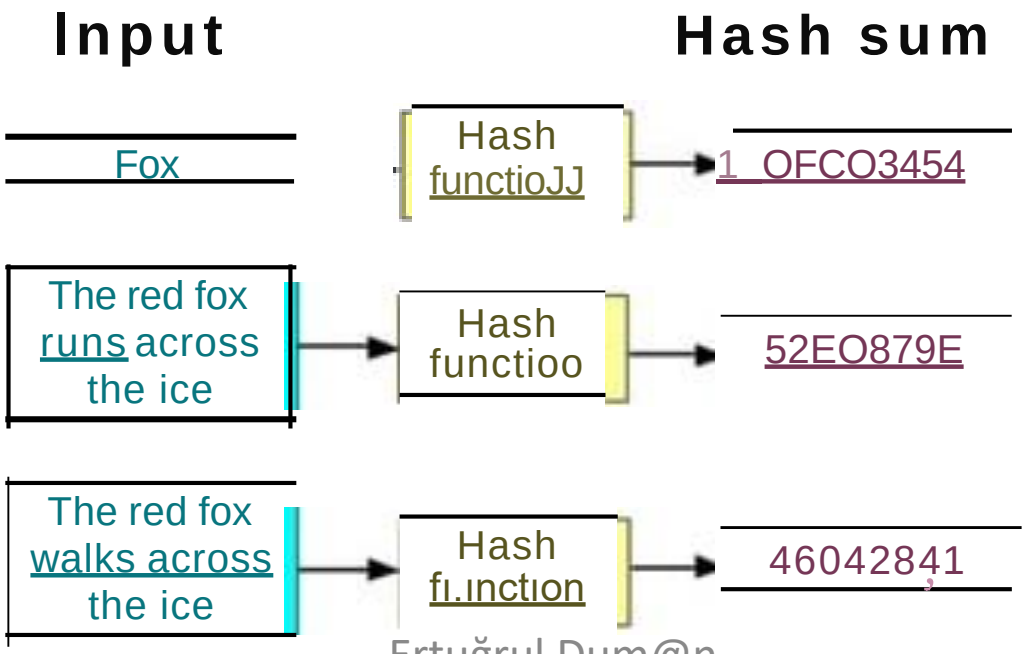
- **Asimetrik Şifreleme:** Kişiye genel ve özel anahtarı ile şifrelenip gönderilir, kişi kendi özel anahtarı ile deşifre eder.

Kriptografik Sistemler

- Anahtarsız Şifreleme (Keyless Encryption)
  - M DS, SHA-1, RIPEMD-1 60, ..
- Simetrik (Gizli) Anahtarlı Şifreleme (Private Encryp tion)
  - Blok Şifre Sistemleri (AES, DES, iDEA, camellia..)
  - Akan Şifre Sistemleri (RC4(Wep), AS/l(Gsm),AS/2..)
- Asimetrik (Açık) Anahtarlı Şifreleme (Public Encryption)
  - İmzalam a Algoritmaları (DSA, ECDSA, RSA..)
  - Anahtar Paylaşım Algoritmaları (RSA, DH, Eliptik..)

Hash (Özet Fonksiyon}

Hash fonksiyonu, değişken uzunluklu veri kümelerini, sabit uzunluklu veri kümelerine haritalayan algoritma veya alt programdır.



MD5

MD5 (Message-Digest Algorithm 5),

- Bir şifreleme yöntemi değil, bir hash fonksiyonudur.
- Herhangi bir uzunlukta verilen mesajı (veya dosyayı) alıp fazla uzun olmayan bir harf ve sayı dizisine çevirir.
- (Kısaca, Girilen verinin boyutundan bağımsız olarak, 128-bit özet değeri üretir.)

Hash ve Salting (Özet+Tuzlama)

	Kullanıcı 1	Kullanıcı 2	Kullanıcı 1	Kullanıcı 2
Password	bob	bob	bob	bob
Salt	-	-	et52ed	ye5sf8
Hash	f4c31aa	f4c31aa	lvn49sa	z32i6t0

Acaba Nedir? *(Dersin özeti)*- CEVAP

w5bEn3JlbmNp/GhhesSxciBvbGR1xJ91bm
Rh/MO2xJ9yZXRtZW4gZ8O2csO8bmVjZWt0aX/u
VGh/lEJlZGRoYQ==

Base 64 - Encode

Öğrenci hazır olduğunda öğretmen görünecektir.
The Buddha

Bölüm 8:

Bilgisayar Ağları(Network) ve Sunucu Sistemleri

Bölüm 9:
İşletim Sistemleri
Linux (Kali Linux)

Bölüm 10:

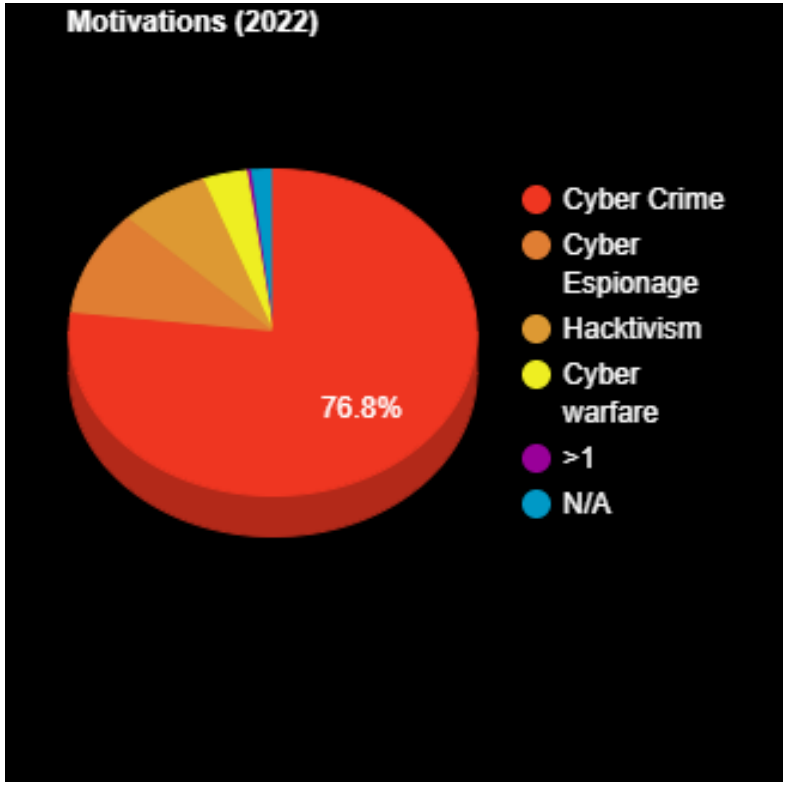
Kablosuz Ağ Güvenliği (Saldırı-Savunma)

Bölüm 11:
Siber Suç ve Siber Suçlular

Siber Saldırılar Altında Yatan Motivasyon

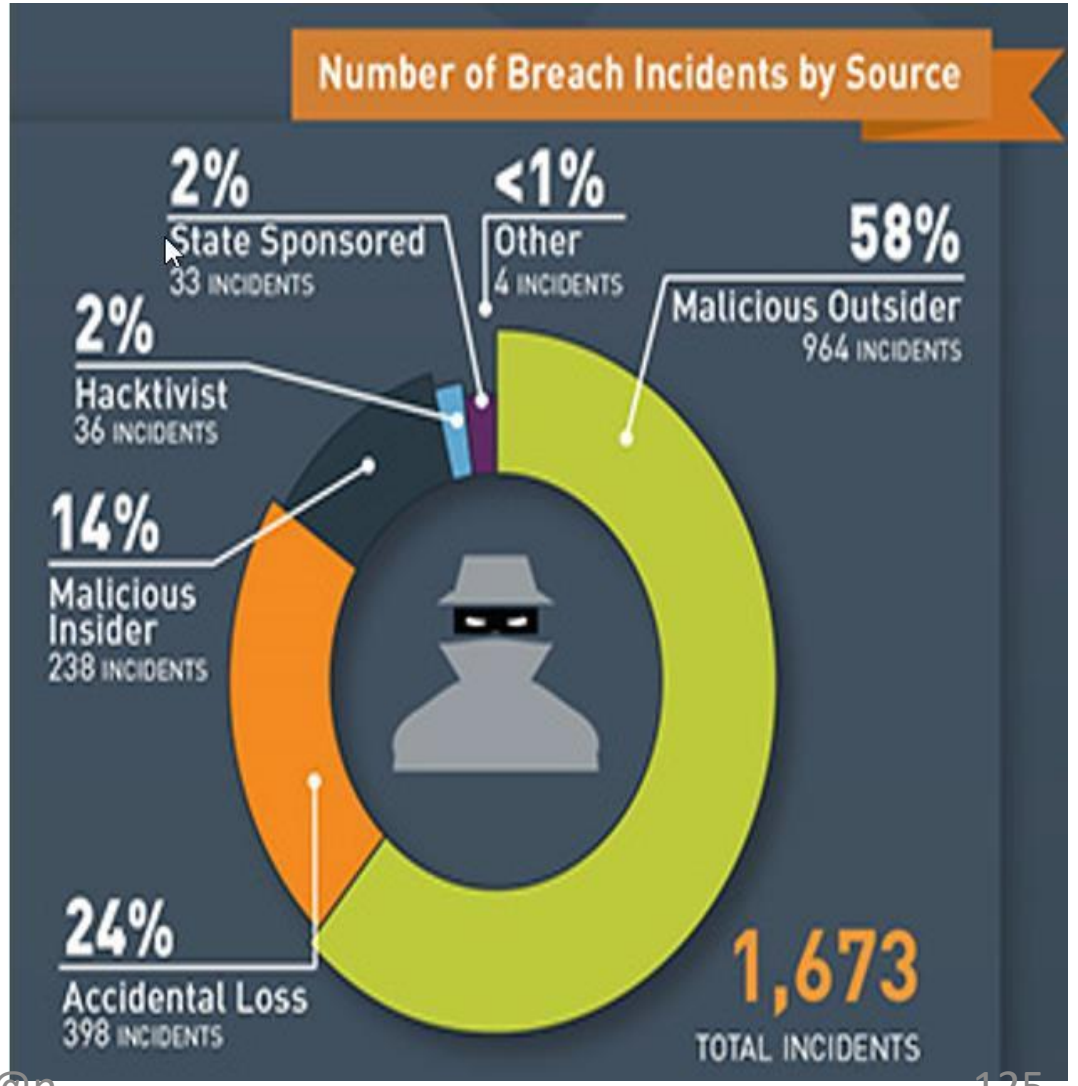
- Siber saldırıların büyük bir çoğunluğu parasal kazanç amaçlı yapılıyor. Kişilerin bilgilerine ulaşmak ve ülkeler arası mücadele amaçlı yapanlara da rastlanıyor.

- Saldırgan profilleri ve temel motivasyonları (Saldırıyı gerçekleştirmedeki amaçları) :
  - ***Siber suçlular****:* kolay ve çok para kazanma fırsatı
  - ***Hacktivist:*** İdeolojik bir amaca hizmet
  - ***Hacker grupları:*** Ünlü olma, adını duyurma
  - ***Egemen devletler:*** Ulusal güvenlik ve ulusal çıkarlar
  - ***Suç örgütleri:*** Belli şahısların becerilerini veya karşılarına çıkan fırsatları değerlendirip para kazanmak

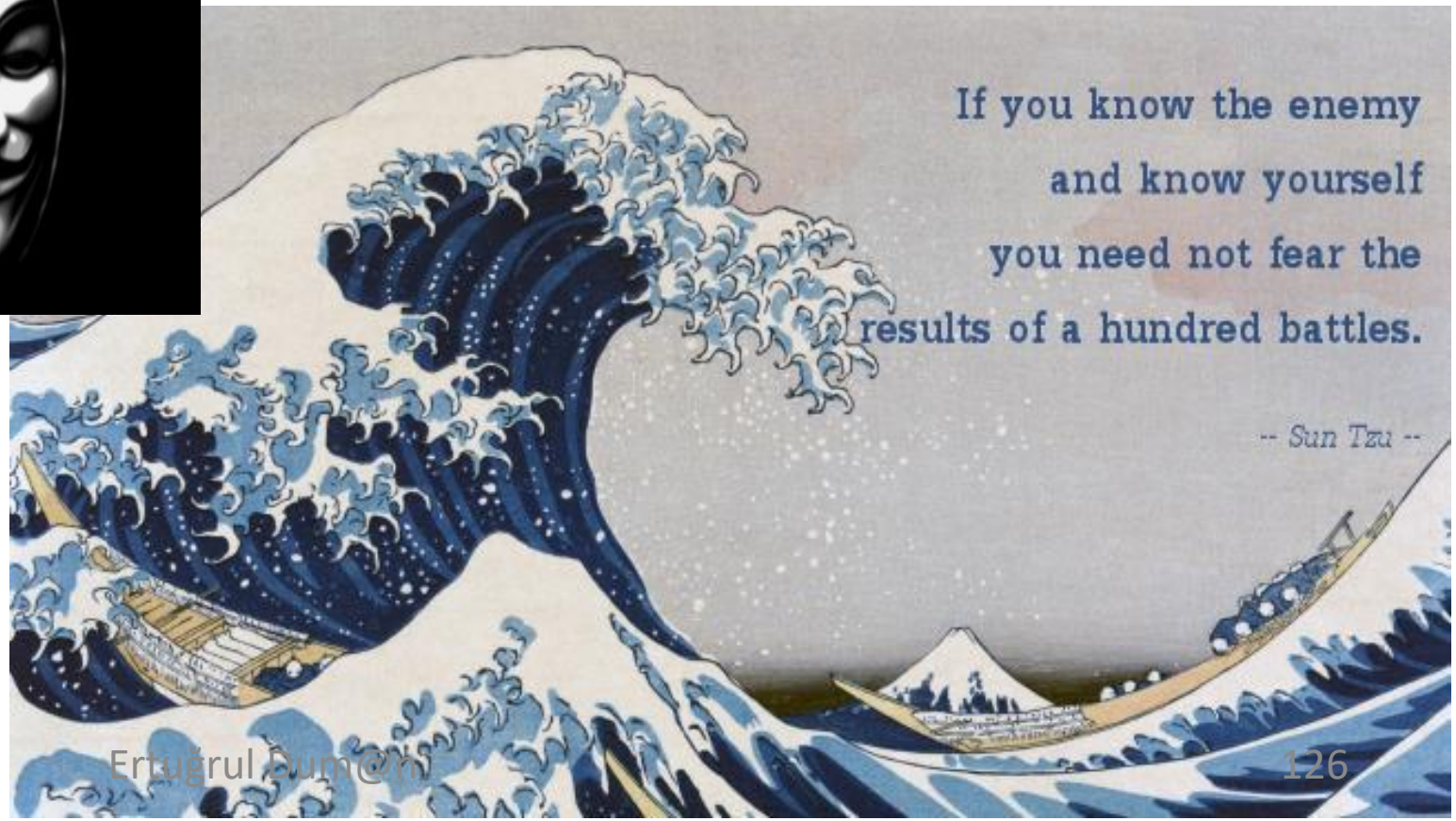


Veri Sızıntısı Saldırılarının Kaynakları

- Dış saldırılar : %58 (Hacker)
- İç Saldırılar : %14 (Çalışanlar, 3. Partiler, vb.)
- Kaza ile yaşanan kayıplar : %24



Düşmanımızı Tanıyalım

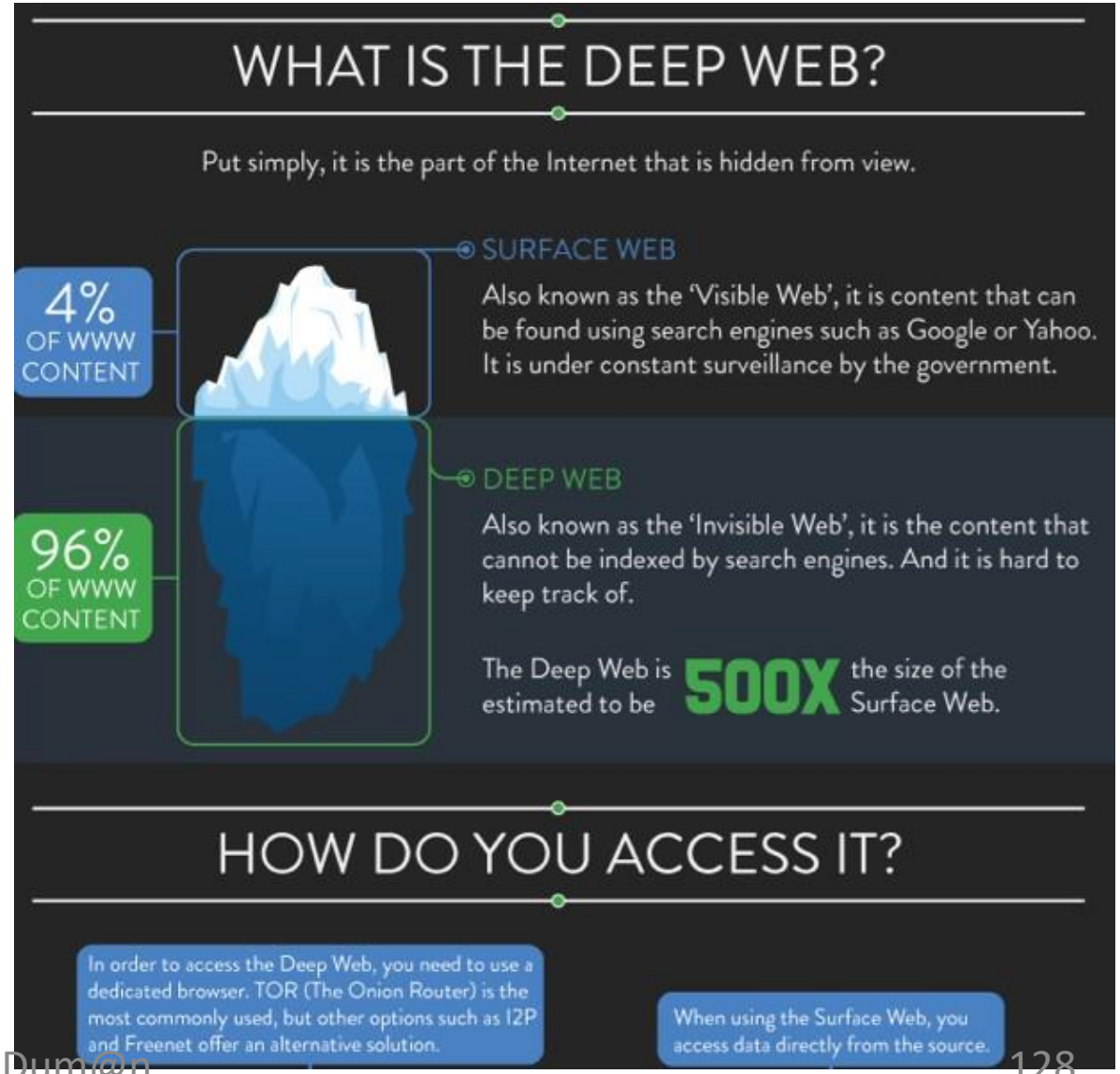


Deep Web


Surface Web
Deep Web
Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription-only information
Some organization-specific repositories
Dark Web
TOR
Political protest
Drug trafficking and other illegal activities
96% of content on the Web (estimated)

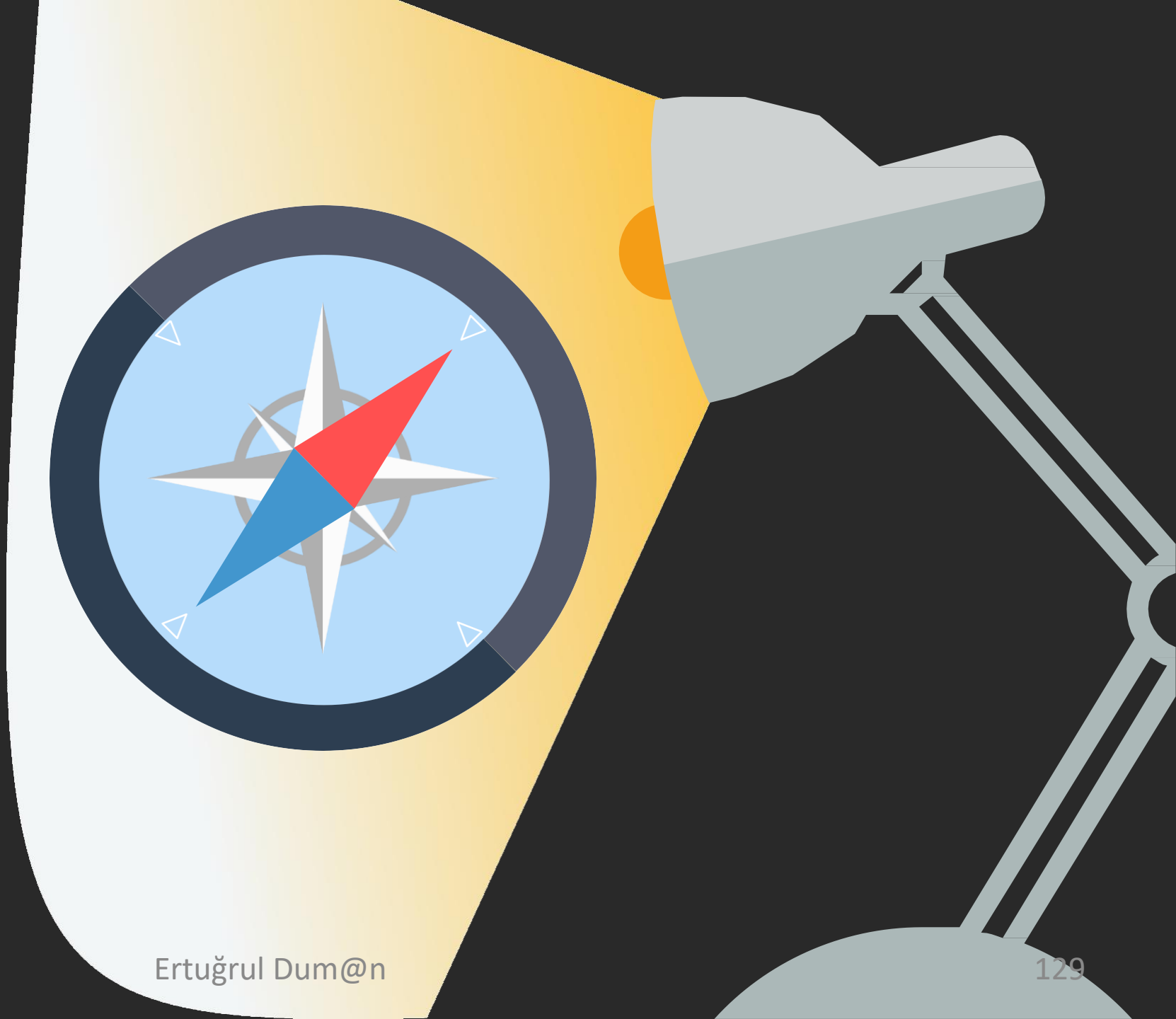
Deep Web

- Arama motorlarının (**Google, Yandex, Bing, Yahoo)** internet arama sistemlerinin ulaşamayacağı internet siteleri ve içerikleri..
- Devlet kurumlarının, özel şirketlerin ve kişisel kullanıcıların, tüm kullanıcılara açık olmayan arama motorları tarafından i**ndexlenmeyen** verilerin ve sitelerin bütününün bulunduğu yer..
- Public erişim istenmeyen ya da illegal bilgilerin bulunduğu alandır.
- Kendi içinde katmanları vardır.

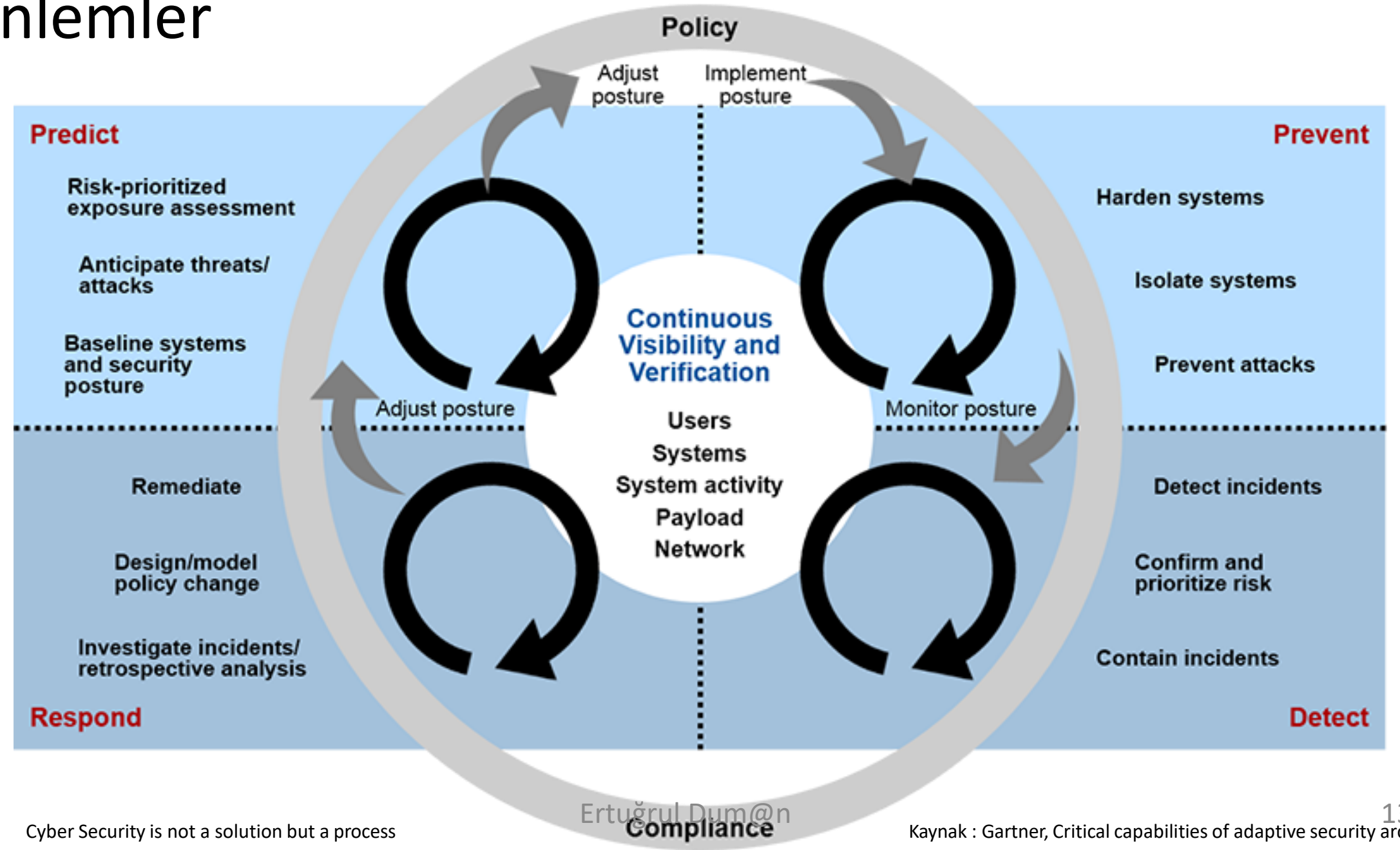


Bölüm 12:

Standartlar Ve Uyum



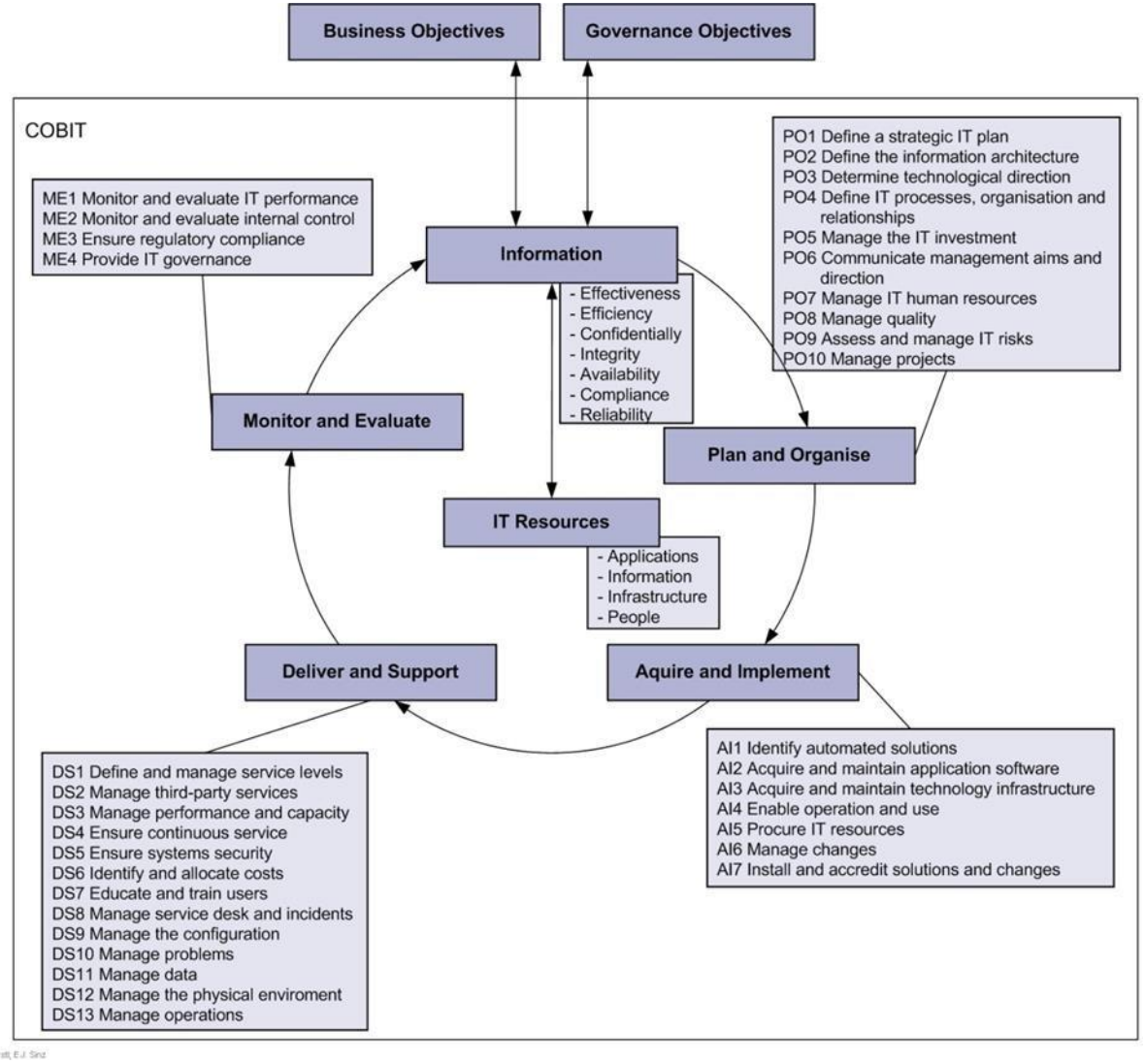
Önlemler



Cyber Security is not a solution but a process

Kaynak : Gartner, Critical capabilities of adaptive security architecture

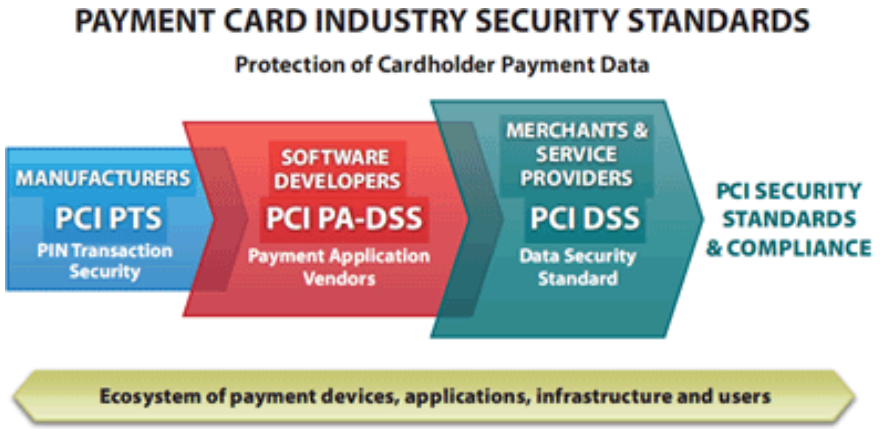
CobIT



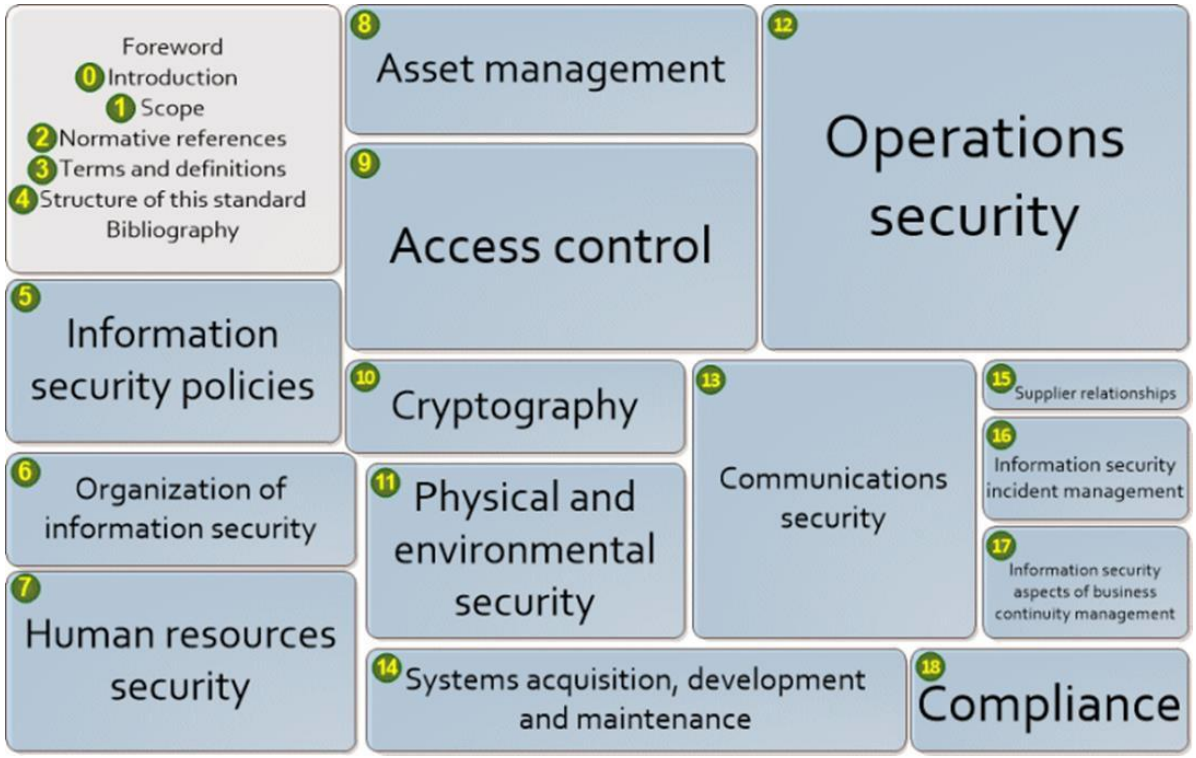
PCI

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel



ISO 27001



ISO 22301

Table of contents

ISO 31000:2009

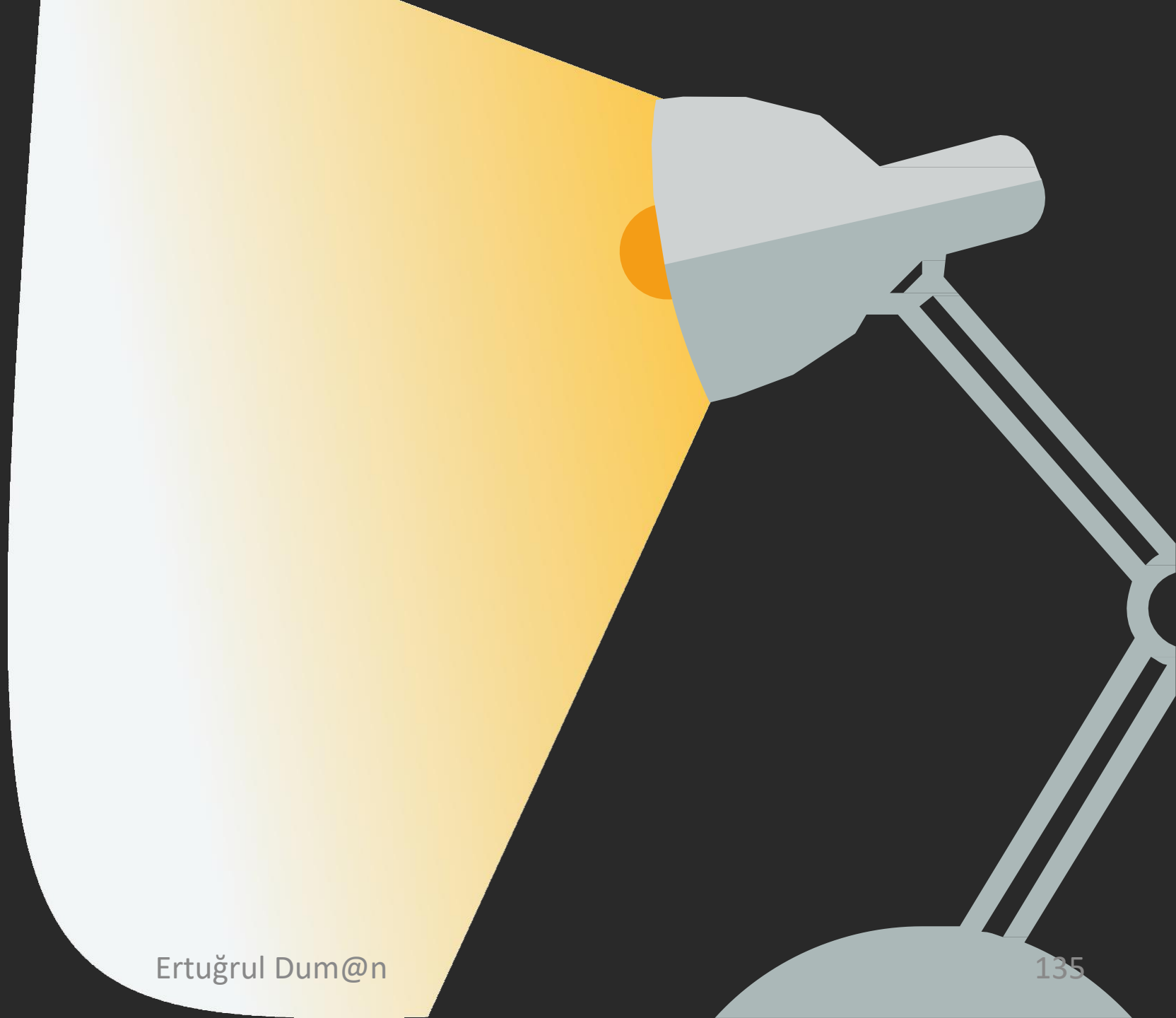
Table of contents

ISO 38500:2015

Table of contents

Bölüm 13:
Siber Güvenliğin Hukuki Boyutu ve Bilişim Hukuku

Bölüm 13:
Adli Bilişim



Bölüm 15:
Web Güvenliği Saldırı ve Savunma Yöntem -Araçları (Temiz Kod)

Bölüm 16:
Öngörüler & Öneriler

2019 - 2023 Siber Tehdit Öngörüleri

1.Ransomware (Fidye Yazılımları) iş dünyası ve organizasyonlara en tehlikeli tehdit olarak karşımıza çıkacak.

2. Siber suçluların odağı sanal paralar olacak. **Cryptocurrencies**

3.Rusya, Çin ve İran **APT grupları,** batı organizasyonları için üzerindeki baskılarını arttıracaklar.

4. İşletmeler için bulut güvenliği en yüksek önceliğe sahip olacak (**Cloud security)**

5.Siber suçlularla mücadele için ortak uluslararası çaba gösterilecek (**International effort)**

6. Siber suçluların öncelikli hedefi **IoT devices** olacak.

7. Mobil Tehdit artarak devam edecek. (Banking Trojan/Mobile Ransomware)

8.Siber dünya kullanılarak birilerine ve özellikle çocuklara baskı kurma olayları daha fazla görülecek (**Cyberbullying)**

9. Siber Sigorta tekliflerinde patlama olacak (**Cyber-Insurance)**

10. Pek çok kurum, **GDPR (** Genel Veri Koruma Tüzüğü**)** uyumluluğunu zamanında tamamlayamayacak.

11. Yapay Zeka odaklı saldırı araçları (yazılımlar) hızla artacak

Bilgi Güvenliği İpuçları

Siber Güvenlik bir süreçtir

Her süreçte olduğu gibi bir akış, sürecin sahibi, kuralları, yöntemleri ve uygulayıcıları olmalıdır. Ortaya çıkaracak olduğunuz ürünü bir servis mantığında kurgulayıp Siber Güvenlik konularında ekip içinde bir lider seçmeli ve tüm paydaşların bu liderin öncülüğünde organize olmasını sağlamalısınız.

Uyum ve Regülasyon Konuları Göz önünde bulundurulmalı

Projeye göre uyulması gereken kanun ve regülasyonlar bilinmeli ve takip edilmeli. Müşterinin kişisel bilgilerinin saklanması ve kullanılması konusunda sınırlar ve yöntemler sıkı takip edilmeli, bu konuda bir sorumlu kişi atanmalıdır. Uyulmadığı takdirde ciddi cezalar ve itibar kaybına sebep olabilecek tüm riskli alanlar tespit edilmelidir.

Özelleştirilmiş, Görev Bazlı Güvenlik Eğitimleri Düzenlenmeli

Ekip içinde herkesin siber güvenlik konusunda farkındalığının gerekli olmasının yanı sıra, görevlerine göre özelleştirilmiş güvenlik eğitimleri alınmalıdır. Geliştiricilerin, teknik ekibin kendi sorumlulukları ile ilgili güncel Siber Güvenlik bilgilerine sahip olmaları gereklidir.

Siber Saldırı Yöntemleri hakkında bilgi sahibi olunmalı

Kötü amaçlı kişilerin kullanmış oldukları çok farklı saldırı yöntemleri bulunmaktadır. Ancak bunlar içerisinde en çok kullanılanlarının bilinmesinde fayda vardır. 80/20 kuralını hatırlayın !

Güvenlik ürünün bir parçası olmalı

Çözümünüze her eklediğiniz parçanın güvenli olmasını sağlamak için çaba göstermek yerine, baştan güvenli çözümler tasarlamak (“security by design”) en doğrusudur. Kolay bir iş olmasa da, maliyeti bulunsa da en doğru yöntem budur.

Bilgi Güvenliği İpuçları

Güvenli Yazılım Kodu Geliştirme Standartlarına Uyulmalı

Kod geliştirirken basit bir takım önlemlerle büyük güvenlik açıklarının önüne geçilmesi mümkündür. Neler mi yapılabilir ? Yazılımın güvenlik standartlarına uygun geliştirilip geliştirilmediği ortaya çıkaran ücretli/ücretsiz ürünler bulunmaktadır.

Güvenlik Testleri Yazılım Geliştirme Sürecinin bir parçası olmalı

Yazılıma entegre edilmiş güvenlik özellikleri test edilmeli, belirli sayıdaki başarısız oturum açma denemelerinden sonra kullanıcı kilitlenmesi, işlem sınırlaması gibi yazılımın güvenliği ile ilgili kavramlar göz önünde bulundurularak, yazılım geliştirildikçe güvenlik testleri de gerçekleştirilmeli, fonksiyonel testlerin yanında güvenlik testleri de yer almalıdır.

Sızma testleri yaptırılmalı

Güvenlik kuralları göz önüne alarak geliştirilmiş, tüm güvenlik testlerinden geçmiş bir yazılım bile üretime alındığında çok farklı saldırı yöntemleri ile sızma testlerine tabi tutulmalı. Unutmamalı ki bir hacker gözü ile yapılan sızma testleri, her zaman farklı açıkların varlığını bize göstermektedir.

Güvenlik Sektöründeki gelişmeler, haberler takip edilmeli

Gün geçmiyor ki daha önceden keşfedilmemiş bir açıklık tespit edilmesin, bu açıklıktan etkilenen kişi, firma, sektör, ülkeler ifşa olmasın. Özellikle tespit edilen açıklıklar sonrası çıkan yamalar takip edilmeli ve soruna sebep olmadan girişimlerinizde uygulanmalı.

İTİBAR OLUŞTURMAK 20 YIL ALIR, MAHVETMEK 5 DAKİKA. EĞER BUNU KABUL EDER VE DÜŞÜNÜRSENİZ, YAPTIKLARINIZI **DAHA FARKLI** YAPMAYA BAŞLARSINIZ.

Warren Buffett, Berkshire Hathaway

Ödev / Proje / Araştırma Konuları

Siber Güvenlik @2023