

Temel Kavramlar

Bilgisayar Teknolojileri Bölümü
Siber Güvenlik ve Bilgi Güvenliđi



Öğr. Gör. Halil ARSLAN

Temel Kavramlar?

- Türk Ceza Kanunu, Onuncu Bölüm, Bilişim Alanında Suçlar Kısımında (**5237 Sayılı Kanun**);
 - **Madde 243** ve **Madde 244** de açıkça belirtildiği gibi;
 - Bilişim sistemine girme (243)
 - Sistemi engelleme, bozma, verileri yok etme veya değiştirme (244)
 - SUÇ tur ve cezası vardır.
 - İki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.



Temel Kavramlar?

- **Türk Ceza Kanunu Madde 243** (Bilişim sistemine girme)
 - 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.
 - Yukarıdaki fıkra tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.
 - Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Temel Kavramlar?

- **Türk Ceza Kanunu Madde 244** (Sistemi engelleme, bozma, verileri yok etme veya değiştirme)
 - Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.
 - 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.
 - 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.
 - 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.

Temel Kavramlar?

- Bilgi
- Güvenlik
- Bilgi Güvenliği
- Siber
- Siber Güvenlik
- Etik
- Hack
- Hacker
- Hacking
- Etik Hacker
- Etik Hacking
- Saldırı
- Savunma
- İnternet
- Zafiyet
- Tehdit
- Kriptoloji
- Şifre
- Adli Bilişim
- Network
- Server
- Linux
- Kali Linux
- Pentest
- Metasploitable
- Exploit
- Payload
- Extranet
- Owasp
- CIA
- CEH
- IDS/IPS
- SIEM
- CVE
- OSINT
- IoT
- SQLI
- Malware
- DoS/DdoS
- Metasploit
- Intranet

Temel 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.
- **Etik:** Ahlâk ile ilgili (meslek ahlakı), karakter/kültür olarak doğru tutum ve davranış

Temel Kavramlar?

- **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 değiştirmek)
- **Etik Hacker:** Bilgi ve yeteneğini etik kurallar çerçevesinde kullanan (hacker) kişilerdir.
- **Etik Hacking:** Sistemin açık ve tehlikeli yönlerini ortaya çıkarmak için yapılan erişim veya ele geçirme işlemi. (Sızma Testi)

Temel Kavramlar?

- **Tehdit:** Bir sistem veya kuruluştaki zarara neden olabilecek istenmeyen bir olayın potansiyel nedeni.
- **Zafiyet: (Vulnerability):** Saldırgana fırsat verebilecek, yazılım-donanım hatası veya prosedürler (açıklık-güvenlik boşluğu)
- **Şifre:** Gizliliği olan şeylerin açılması, kullanılması veya iletilmesi için gerekli olan işaretler (harf, rakam, sembol, vb.) bütünüdür.
deneme => 8F10D078B2799206CFE914B32CC6A5E9 (md5)
- **Parola:** Gizlilik ortamında tanıma veya iletişim için gerekli anahtar (kelime) ifadedir. (Gizli)
pArola123

Temel 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 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 Kavramlar?

- **Linux:** Unix işletim sistemine fıkırsel 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 5 devamı niteliğindedir.



Temel 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 Kavramlar?

- **Metasploitable:** Pentestler gerçekleştirmek için güvenlik açıkları hakkında bilgi sağlayan, sızma testleri amacıyla içerisinde çeşitli araçlar (exploit, payload, auxiliary, encoder) olan bir (framework yapısı) zafiyetler barındıran bilgisayar güvenlik projesidir.
- **Exploit:** Sistemler ve servisler üzerinde yer alan güvenlik açığının kullanılmasını sağlayan araçlara denilmektedir.
- **Payload:** Hedef sistem veya servis üzerinde çalıştırılması istenen kodlara denir. (Exploit işleminin ardından)

Faydalı Kaynaklar

Faydalı Kaynaklar



- **BTK Akademi**
- -> **Eğitimler** -> **Sistem Dünyası** -> **Siber Güvenlik**
- <https://www.btkakademi.gov.tr/portal/catalog?categoryId=1003>

The image displays four course cards from BTK Akademi, each featuring a BTK Akademi logo and a green "Temel Seviye" (Basic Level) badge. The cards are arranged horizontally. A large, dark blue curved arrow points from the right side of the cards towards the URL above.

- Siber Güvenliğe Giriş** (Introduction to Cyber Security)
- Bilgi Güvenliğine Giriş** (Introduction to Information Security)
- Kali Linux**
- Adli Bilişime Giriş** (Introduction to Forensic Computing)