FBÜ
FENERBAHÇE ÜNİVERSİTESİ

COMP 102 – Bilişim Sistemleri

Dr. Vecdi Emre Levent

Ders Planı

Hafta 5: Temel Bilgisayar Güvenliği

- Güvenlik
- Gizlilik
- Şifreleme
- İnternet Ağı Güvenliği

Bilgisayar ve Veri Güvenliği

Bilgi ve veri güvenliği;

- Bilginin ‘’izinsiz’’ veya ‘’yetkisiz’’ bir biçimde erişimi, kullanımı, değişrilmesi, ifşa edilmesi, ortadan kaldırılması, el değişrmesi ve hasar verilmesini ‘’önlemek’’ olarak tanımlanır.

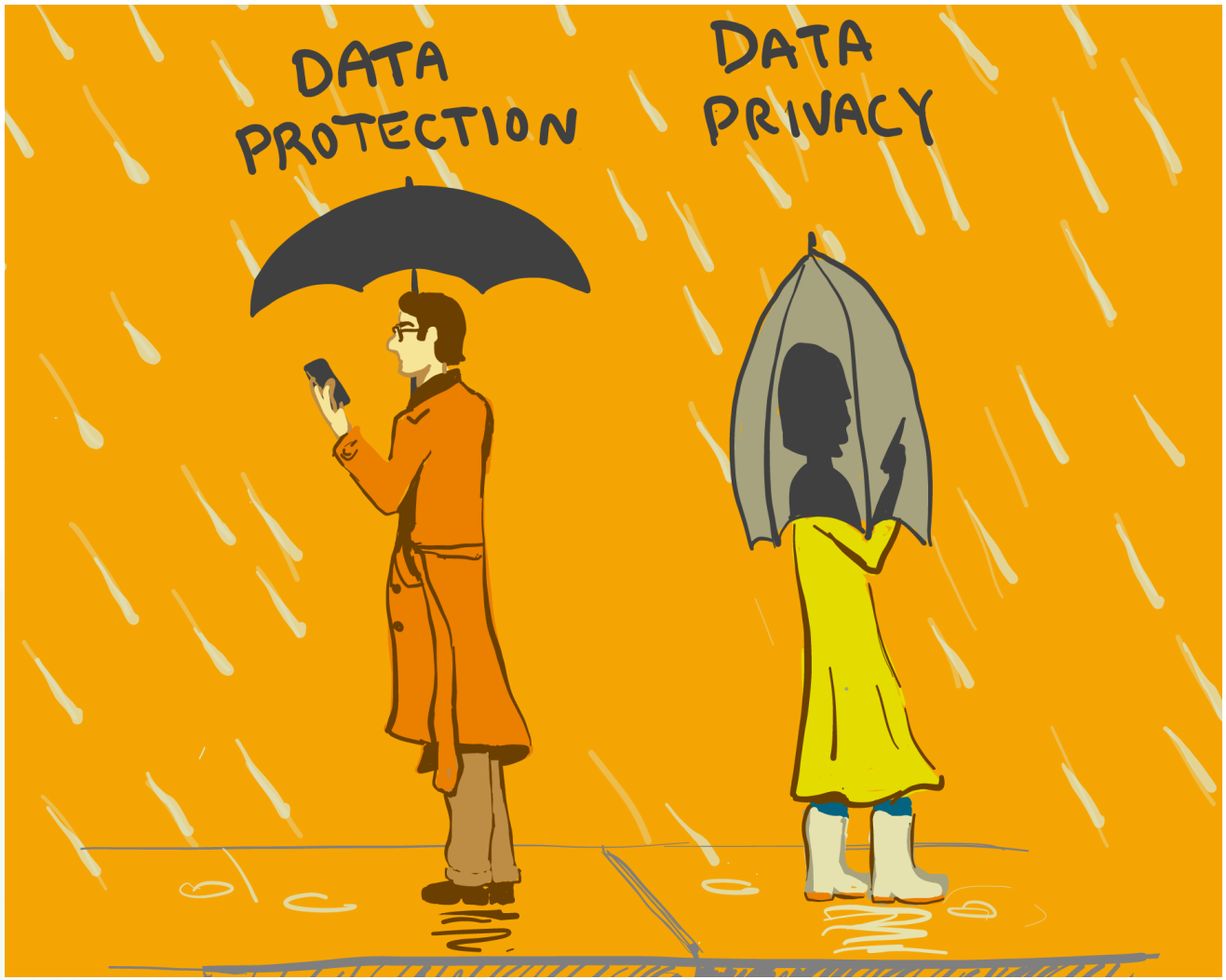
- Disk, iletişim ağı, yedekleme ünitesi ya da başka bir yerde tutulan verilerin, programların ve her türlü bilginin korunmasını ifade eder.

Veri Güvenliğinin Üç Temel Boyutu

Veri güvenliğinin 3 temel boyutu bulunmaktadır. Bu boyutlardan herhangi biri zarar görürse güvenlik zafiye olur.

- **Gizlilik**: Bilginin yetkisiz kişilerin eline geçmeme ve yetkisiz erişime karşı korunmasıdır.
- **Bütünlük**: Bilginin yetkisiz kişiler tarandan değiştirilmemesidir.
- **Erişilebilirlik:** Bilginin yetkili kişilerce ihyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

Veri Güvenliğinin Üç Temel Boyutu



Veri Güvenliğini Tehdit Eden Kaynaklar

- Teknik saldırılar (kötü amaçlı yazılımlar)
- Kötü niyetli kişi saldırıları (hacker)
- Sistem hataları (donanım arızaları ve kullanıcı hataları)
- Yangın, su baskını, terör gibi dış etkenler

Veri Güvenliğinin Tehdit Edilme Sebepleri

- Para hırsızlığı
- Yazılıma zarar verilmesi
- Bilgi çalınması
- Bilgiye zarar verilmesi
- Servislerin izinsiz kullanılması
- Zarar vermeden güvenlik ihlali
- Sistemlerin kısmen veya tamamen devre dışı kalması

Bilgi Güvenliği Oluşturmanın Yolları

- Dikkat ve farkındalık
- Belirli periyotlarla bilgileri yedekleme ve yedeklenen bilgileri güvenli alanlarda tutma
- En az 20 karakterden oluşan şifreler kullanma ve bunları belirli periyotlarda güncelleme
- Güvenliği sağlamada anti-virüs, anti-spam, anti-casus ve güvenlik duvarı gibi çözümlerin kullanılması ve bunların güncel tutulması
- Yeni güvenlik yaklaşımlarının takip edilip uygulanması
- Bilinmeyen veya anlaşılmayan hususlar konusunda şüpheci olunması ve uzmanlardan destek alınması

Bilgi Güvenliği Oluşturmanın Yolları

- Kullanılmayan bilgilerin sistemlerden kaldırılması sadece ihtiyaç duyulan bilgilerin elektronik ortamlarda barındırılması, ihtiyaç olmayan yazılımların bile sistemlere yüklenilmemesi
- Elektronik ortamları kolaylıkla takip edilebilir ve izlenebilir ortamlar olduğunun herzaman akılda tutulması
- Konu ile ilgili olarak kullanıcıların bilgilerini arttırmaları
- Sahip olunan bilgi varlıklarının gerektiği gibi korunması veya paylaşılmaması ve başkalarının bilgilerini izinsiz kullanmama ve sistemlerine izinsiz girilmemesi gerektiği ve bunun da suç olduğunun hatırlanması

Saldırı Yöntemleri

Saldırı Kavramı

Kurum ve şahısların sahip oldukları;

- Tüm değer ve bilgilere izinsiz erişmek
- Zarar vermek
- Maddi/manevi kazanç sağlamak

için bilişim sistemleri kullanılarak yapılan her türlü hareket dijital saldırı olarak tanımlanabilir.

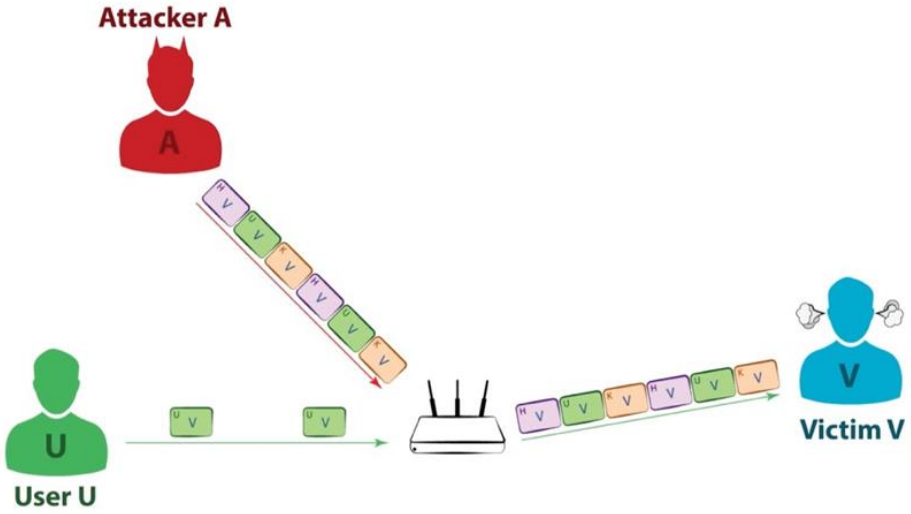
Saldırı Türleri

İzinsiz Erişim:

Bu saldırı türünde, saldırgan bilgiye (yazılım, donanım ve veri) yetkisi olmadığı halde erişebilmesidir.

Aynı bilgiye yetkili kullanıcılar da olağan şekilde erişebilirler, yani bilginin kendisinde bir bozulma yoktur.

Bununla birlikte o bilgiye erişmesi beklenmeyen kişilerin bunu yapabilmesi, saldırı olarak nitelendirilir (örn: ağ koklama)



Saldırı Türleri

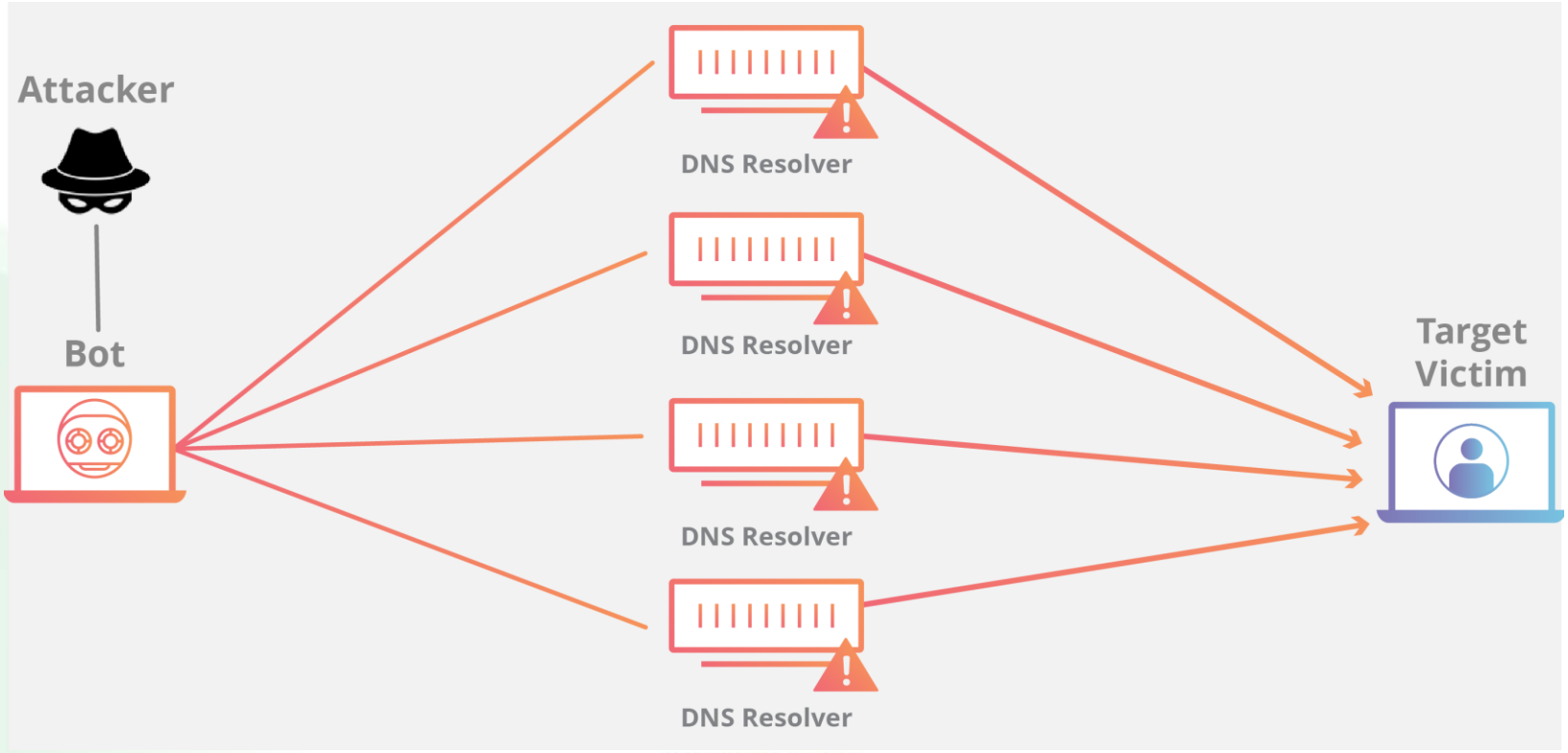
Engelleme veya Zarar Verme:

Bu saldırı türünde, bilgiye erişim engellenir.

Bilgi ya kaybolmuştur/silinmiştir; ya kaybolmamıştır, ama ulaşılamaz durumdadır; veya kaybolmamıştır ve ulaşılabilir durumdadır, ama yetkili kullanıcılar tarafından kullanılamaz durumdadır
(örn: donanımın kırılması, veya DoS veya DDoS gibi erişim reddi saldırıları).

Saldırı Türleri

Engelleme veya Zarar Verme:



Saldırı Türleri

Değişiklik Yapma:

Bu saldırı türü, bilginin yetkili kullanıcıya ulaşmadan önce saldırganın amaçları doğrultusunda bilgide değişiklik yapmasını içerir.

Program kodları, veri veya aktarılmakta olan veri üzerinde yapılması mümkündür (örn: virüsler ve truva atları).

Saldırı Türleri

Üretim:

Bu saldırı türü, gerçekte olmaması gereken verinin üretilmesini içerir.

Üretilen veri, daha önceki gerçek bir verinin taklidi olabileceği gibi, gerçeğe uygun tamamen yeni bir veri şeklinde olabilir (örn: sahte veri, ya da veri taklidi).

Saldırgan Grupları

Amatörler:

Bu grupta yer alan saldırganlar, aslında sıradan bilgisayar kullanıcılarından başkası değildir.

Bu tür saldırılarda genelde saldırının oluş şekli sistemdeki bir açıklığı fark edip yararlanma şeklinde olur.

- Örneğin, bir Unix sistem üzerindeki bir kullanıcının erişim izinlerinin uygun olduğunu gördüğü dosyayı silmesi gibi.
- Bir başka kullanıcının sistem üzerinde kendine bir dosya sınırlaması olmadığını fark edip yüzlerce MB boyutundaki bir dosyayı sisteme indirmesi gibi.

Amatörlerin genel olarak saldırılarını planlamadıkları söylenebilir.

Saldırgan Grupları

Kırıcılar (Cracker):

- Çoğunlukla yanlış bir biçimde “hacker” olarak adlandırılan bu grubun doğru isimlendirmesi “cracker” olup, saldırılarını amatörlere göre biraz daha planlı ve programlı yapan kişilerden oluşur.
- Saldırının çok belirli bir amacı olmayıp, merak etme, yapılabildiğini gösterme, ya da sırf yapmış olmak için yapma gibi amaçlar olabilir.
- Açıkları tesadüfen fark edebildikleri gibi, aslında yaptıkları plan ve program sistemin açıklarını bulmaya yönelik bir uğraştır.
- Bilgisayar sistemlerini “kırmak” için uğraştıklarından dolayı bu grubu “kırıcılar” olarak adlandırmak da mümkündür.

Saldırgan Grupları

Profesyonel suçlular:

- Bu gruptaki saldırganlar, yukarıdaki iki grubun aksine, güvenlik kavramlarını ve amaçlarını anlayan ve bozmaya yönelik organize eylemler içinde bulunan kişilerdir.
- Birden fazla kişilerden oluşan ekipler kurarak güvenliği bozmaya yönelik saldırılar gerçekleştirebilirler.
- Nitelik açısından en tehlikeli grubu oluşturdukları söylenebilir, çünkü bu kişiler yaptıkları iş karşılığında para kazanırlar.
- Saldırıların hedefleri önceden belirlidir, planlı ve organize şekilde saldırıda bulunurlar.

Kötü Amaçlı Yazılımlar (Maleware)

Bilginiz veya izniniz olmadan bir bilgisayara sızmak ve muhtemelen zarar vermek için tasarlanmış kod parçalarıdır.

- Virüs (Virus),
- Casus (Spyware),
- Korku (Scareware),
- Reklam (Adware),
- Truva atı (Trojan horse),
- Solucan (Worm),
- Rootkit ve diğer tiplerde istenmeyen yazılımlar bu kapsamdadır.

Bilgisayar Virüsleri

- Kullanıcının bilgisi haricinde bilgisayarda çalışan bir koddur.
- Dosyalara veya makro gibi kodlara bulaşırlar.
- Çalıştırıldığında bilgisayara bulaşmaktadır.
- Virüsler kendilerini bilgisayarda başka bölümlere kopyalayabilirler.
- Virüs bulaşan dosyalara diğer bilgisayarlar tarafından ulaşıldığında virüs diğer sistemlere de bulaşabilir.
- Her türlü zararlı yazılıma yanlış bir algılama ile virüs denilmektedir.

Virüsler Nasıl Çalışır?

- Temel virüsler genelde yeterli bilgisi olmayan bilgisayar kullanıcıları tarafından farkında olmadan paylaşılır veya gönderilir.

- Solucanlar gibi daha karmaşık olan virüsler, bir e-posta paylaşma uygulaması gibi diğer yazılımları denetleyerek kendilerini otomatik olarak çoğaltabilir ve diğer bilgisayarlara gönderebilir.

- Truva atı adı verilen belirli virüsler, faydalı bir program gibi görünerek kullanıcıların aldanıp onları karşıdan yüklemelerine yol açabilir.

Virüslerin Belirtileri

- Bilgisayarın normalden daha yavaş çalışması
- Normal olmayan hata mesajları
- Antivirüs programlarının çalışmaması
- Bilgisayarın sık sık kilitlenmesi
- Sabit diskin sürekli kullanımda olması

Virüslerin Belirtileri

- Disk sürücüleri veya uygulamaların doğru çalışamaması
- Simgelerin kaybolması veya yanlış görünmesi
- Veri dosyalarının artan sayıda bozuk çıkması
- Otomatik olarak oluşturulmuş klasörler ve dosyalar

Casus Yazılımlar

Spy + Software = Spyware

- Spyware farkında olmadan bir web sitesinden download edilebilen veya herhangi bir üçüncü parti yazılım ile birlikte yüklenebilen kötü amaçlı bir yazılım tipidir.

- Genelde, kullanıcının izni olmaksızın kişisel bilgilerini toplar.

fbu.edu.tr

Casus Yazılımlar

- Herhangi bir kullanıcı etkileşimi olmaksızın bilgisayar ayarlarını değiştirebilmektedirler.
- Çoğunlukla web reklamları ile bütünleştirilmiştir.
- En belirgin bulgusu, tarayıcı açılış sayfasının değiştirilmesidir.

Spyware Belirtileri

- Web tarayıcının açılış sayfasının sürekli değişmesi
- Her arama yapılmasında özel bir web sitesinin açılması
- Aşırı derecede popup penceresi görüntülenmesi
- Kendiliğinden çalışan yazılımlar
- Firewall ve/veya antivirüs programlarının kapanması
- ADSL kotanızın beklenenden çok fazla kullanılmış olması

Korku Yazılımları (Scareware)

- Yeni bir saldırı türüdür.
- Amacı sizi korkutarak para kazanmaktır.
- Genelde bilgisayarınız pek çok virüs tarafından ele geçirildiğini ve temizlenebilmesi için belirli bir yazılıma lisans ücreti ödemeniz gerektiğini söylenir.

Korku Yazılımları (Scareware)

Reklam Yazılımları (Adware)

Advertisement + Software = Adware

- Reklam amaçlı yazılımlardır.
- Bu reklamlar genelde popup (açılır pencere) şeklindedir.
- Bilgisayara zarardan çok kullanıcıya kullanım sıkıntısı veririler.
- Genelde bilgisayara casus yazılımlarla birlikte bulaşırlar.

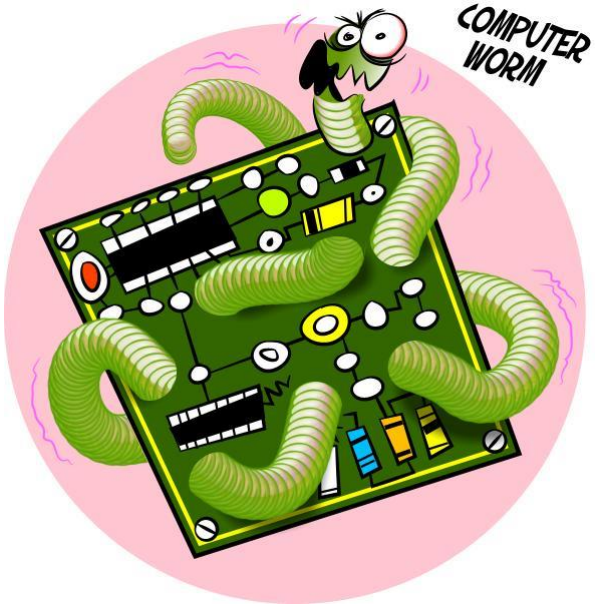
Truva Atları (Trojan)

- Görüntüde istenilen fonksiyonları çalıştıran, ancak arka planda kötü amaçlı fonksiyonları da gerçekleştiren yazılımlardır.
- Bunlar teknik olarak virüs değillerdir ve farkında saldırgan istediğinde arka planda kolayca kötü amaçlı yazılımı kurabilirler.

- Truva atları, ücretsiz olarak yüklediğiniz yazılımlarla bir arada da gelebilir.
- Crack kullanarak kurulan yazılımlarda sık karşılaşılır.

Solucanlar (Worms)

- Solucanlar, uygulamalar ve işletim sistemindeki güvenlik açıklıklarından ve arka kapılardan yararlanır.
- Solucanlar çalışmak için kullanıcıya gereksinim duymazlar.
- Daha çok ağ paylaşımları ve toplu e-mailler ile yayılırlar.



En Ünlü Solucanlar

- ILOVEYOU, bir e-mail eklentisi olarak dağıtılmış ve 5.5 milyar dolarlık bir zarara neden olmuştur.
- Code Red 359,000 siteyi etkilemiştir.
- SQL Slammer tüm interneti bir süreliğine yavaşlatmıştır
- Blaster ise bilgisayarınızı tekrar tekrar yeniden başlatabilir.

Rootkit (Sinsi Yazılımlar)

- Rootkit bilgisayara bulaşan, çalışan işlemler arasında kendini gizleyen, kötü niyetli kişilere, uzaktan bilgisayarınızın tam hakimiyetini sağlayan tespit edilmesi oldukça zor olan bilgisayar programıdır.

- Virüsler gibi amacı sisteminizi yavaşlatmak ve yayılmak değildir. Bilgisayarınızın kontrolünü ele geçirmeyi hedeflemektedir.

- Siz farkında olmadan örneğin internete bağlıyken bilgisayarınız Rootkit yazılımlarla kontrol edilebilir, yine siz farkında olmadan Kötü niyetli sitelere girilebilir, bilgisayarınız siber saldırılarda kullanılabilir.

- Pek çoğu işletim sisteminin çekirdeğine kendini yerleştirdiği için, antivirüsler tarafından tespit edilmesi oldukça zordur.

Zombi Bilgisayarlar (Botnet)

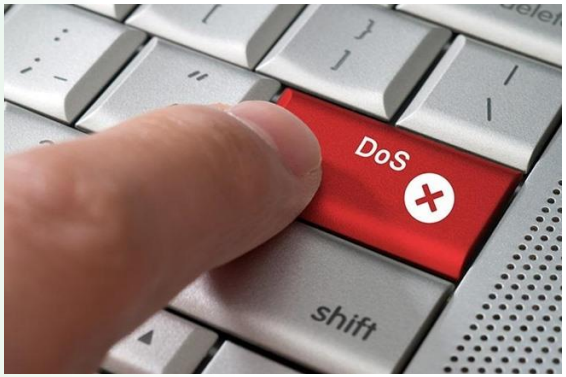
- Kötü amaçlı yazılımlar tarafından ele geçirilmiş sistemlerdir. (Genellikle “truva atları” tarafından)
- Bu sistemler bir kısır döngü içerisinde sürekli olarak zararlı yazılım yayarlar ve kullanıcıları bunun farkında değildir.
- Zombi Bilgisayarlar (Botnet)

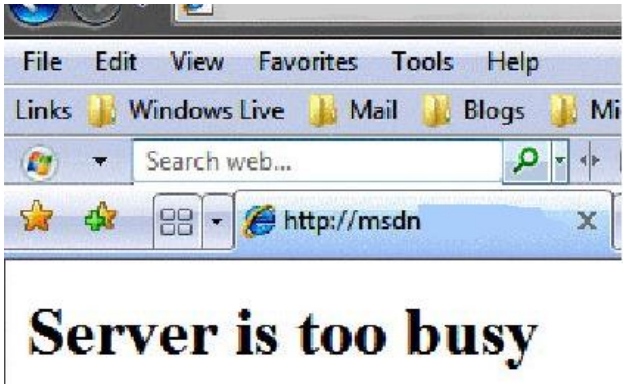
Yerel Ağ Saldırıları

- Yerel ağda bulunan kullanıcıların, sahip oldukları hakları kötü niyetli kullanması sonucu oluşmaktadır
- Amaç genelde diğer çalışanların e-postalarını okumak, yöneticilerin şifrelerini yakalamak, kuruma veya farklı bir çalışana ait bilgilerin incelenmesi olmaktadır
- Paket yakalamak, oturum yakalamak, oturumlara müdahale etmek en sık kullanılan saldırılardır

Hizmet Aksatma Saldırıları

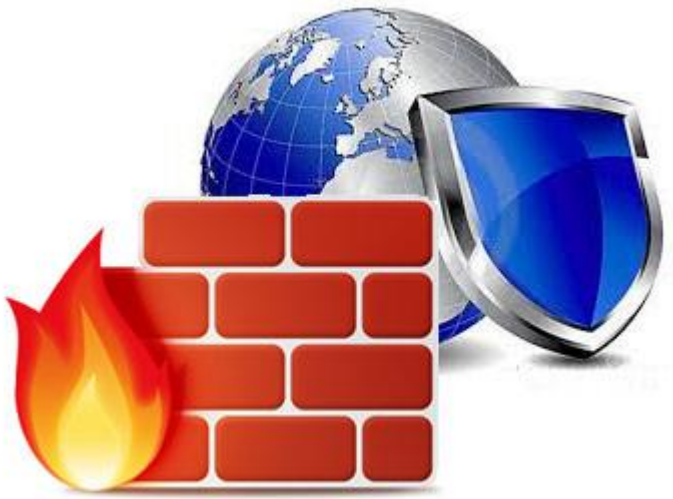
- Protokol, işletim sistemi veya uygulamada bulunan zayıflıkların sonucunda, sunucunun servis veremez hale getirilmesidir
- Hedef bir sunucu, servis, uygulama veya ağın devre dışı bırakılması olabilir
- Tek merkezli yada çok merkezli olarak yapılabilir





Korunma Yöntemleri

- Güvenlik yazılımları
- Yazılım güncellemeleri
- Kimlik doğrulaması
- Verilerin yedeklemesi
- Verilerin erişim izinleri
- Verilerin şifrelenmesi
- Verilerin güvenli şekilde silinmesi
- Bilinçli kullanıcı davranışları



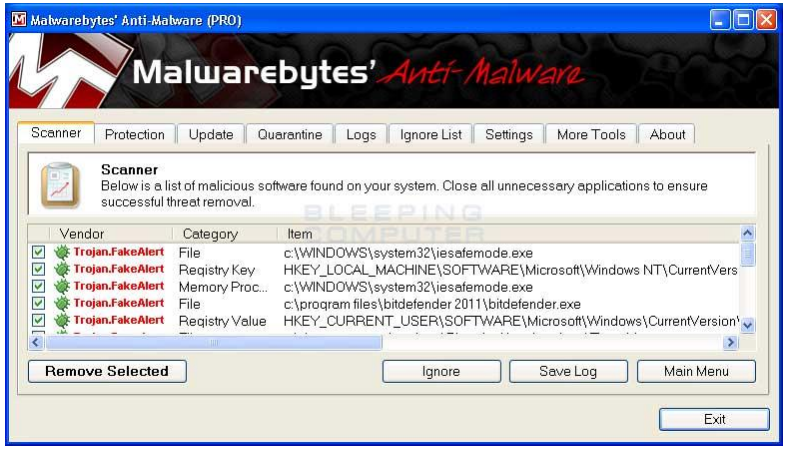
Güvenlik Yazılımları

- **Güvenlik yazılımları çeşitli şekillerde sisteminizi korurlar**
  - Antivirüs, antispyware; zararlı yazılım engelleme ve temizleme
  - Firewall; ağ paketlerinin erişim izinlerini denetlenmesi
  - Denetim merkezleri; güvenlik yazılımlarının etkinliğinin kontrolü
  - Her bilgisayar, bir anti virüs yazılımına sahip olmalıdır ve virüs veritabanı sürekli güncellenmelidir
  - Windows XP, Vista, 7, 8 ve 10 sürümleri yerleşik güvenlik duvarı, antispyware yazılımı ve denetim merkezleri sunmaktadır

Güvenlik Yazılımları

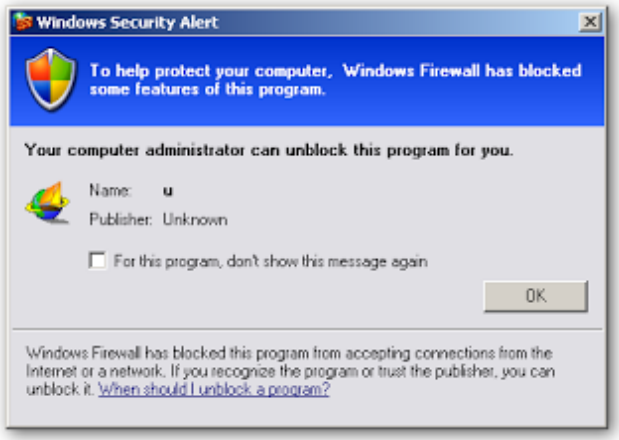
Zararlı Yazılımların Tespit Edilmesi

- Eğer bir sistem zararlı bir yazılım tarafından etkilenirse, en basit bulgu sistemin cevap verme süresinin gecikmesi olacaktır.
- Sistem istenmeyen veya yanlış davranışlar sergileyebilir.
- CPU ve bellek kaynakları doğrudan veya arka planda kullanılır.
- Tutarsız davranışlar karşısında sistem mutlaka güvenlik yazılımları ile taranmalıdır.



Güvenlik Duvarı (Firewall)

- Güvenlik duvarları, bilgisayarın veya ağların, ağ ve internet ortamı ile iletişimini takip eden ve tanımlı kurallara göre bu trafiği yöneten yazılımlardır
- İzin verilenler dışındaki tüm portlar kapatılır, açık olan portlar üzerindeki paket trafiği ise sıkı kurallar tarafından denetlenir
- Windows XP, Vista, 7,8 ve 10 üzerinde yerleşik güvenlik duvarı bulundurur



Kimlik Doğrulaması ve Şifreler

- Kimlik doğrulamasında en yaygın yöntem belirli bir kullanıcı adına bağlı olarak veya kullanıcı adı olmaksızın şifre girilmesidir.

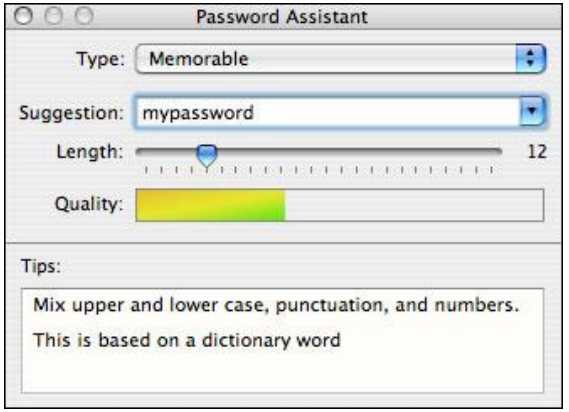
- Bu sistemin işe yaraması için, güçlü bir şifrenin oluşturulması ve bu şifrenin iyi korunması zorunludur.

- Dünyada aşılması ‘’imkansız’’ bir şifre yoktur; ancak aşılması imkansıza yakın derecede zor olan şifreler vardır.

- Ardışık veya klavye dizilimi çok kolay şifreleri asla kullanmayınız. Şifresi 123456 veya qwerty olan milyonlarca kullanıcı bulunmaktadır.

Şifre Oluştururken Dikkat Edilmesi Gerekenler

- Şifrelerinizde kesinlikle kişisel bilgilerinizi kullanmayın
- Sizi az da olsa tanıyan bir kişinin bile tahmin edemeyeceği şifrelerler üretin; hatta mümkünse anlamlı bir dizilimi olmamalıdır
- Mümkün olduğu kadar harf, rakam ve diğer sembolleri bir arada kullanın; klavyedeki #$½|<} gibi karakterleri araya alın
- Şifrelerinizi çok kısa tutmayın; en az 8 basamaklı şifreler kullanın

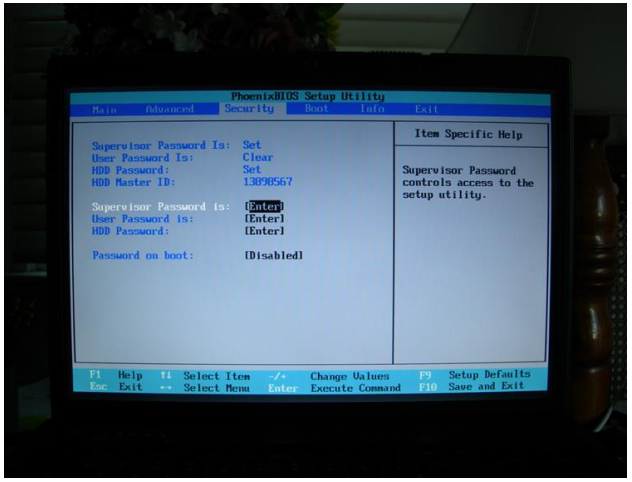


Şifreleri Korumak

- Şifrenizi anlık mesajlaşma yazılımlarından göndermeyin
- Şifrelerinizi düzenli aralıklarla değiştirmeyi unutmayın
- Her yere aynı şifreyi kullanmayın; daha az güvenli bir siteye üye olduğunuz zaman, sakın mail adresinizin şifresini girmeyin
- Bilgisayarınızda bir metin dosyasında veya şifresiz bir Word belgesinde şifrelerinizi kaydetmeyin
- Mümkünse şifrelerinizi bilgisayar ortamında depolamayın

BIOS Şifreleri

- Bilgisayara koyabileceğiniz ilk şifreler BIOS şifreleridir
- Çoğu BIOS yazılımında, BIOS ayarlarını değiştirebilmek ve bilgisayarı açmak için 2 ayrı şifre belirlenebilmektedir
- Bu şifreler fiziksel erişim imkanı bulunan kişiler için anlamlıdır
- BIOS şifreleri herhangi bir ağ veya internet güvenliği sunmaz
- Ayrıca yetkisiz kişi sistem kasasını açabilecek durumda olursa, BIOS şifrelerini geçersiz kılması son derece kolaydır



FENERBAHÇE ÜNİVERSİTESİ

FBÜ

FENERBAHÇE ÜNİVERSİTESİ

fbu.edu.tr