

Siber Güvenlik Dersi Sözlük Oluşturma Etkinliği

KELİME

Açık Anahtar Altyapısı (Pkı)

DEFINITION

Asimetrik Şifreleme Ve Dijital Sertifika Uygulamalarını Kullanarak Dijital Ortamda Güvenli İşlemler Gerçekleştirme Olanağı Tanıyan Altyapıdır.

Adli Bilişim

Bilişim Suçları Davalarında, Olay Yerine Suça Konu Olan Dijital Delillerin Zarar Göremeyecek Ve Değiştirilemeyecek Şekilde Toplanması, Toplanan Verilerin Mahkeme Süresince Olayın Aydınlatılması Adına Kullanılabilmesi Gibi Süreçleri İçeren Bilim Dalıdır

Adli İnceleme

Bir Siber Güvenlik Olayının Nasıl Meydana Geldiğini Veya Kimler Tarafından Gerçekleştirildiğini Belirlemek İçin Dijital Kanıtların Toplanması Ve Çeşitli İşlemlerden Geçme Süresidir.

Adware (Zararlı Reklam)

Bilgisayarınızda Reklamları Otomatik Gösteren Yazılımdır. Bir Uygulamayı Kullandığınızda Bilgisayarınızda Otomatik Olarak Reklamlar Bir Anda Ekranda Belirir.

Aes (Advanced Encryption) Gelişmiş Şifreleme Standardı

128 İle 256 Bit Anahtar Boyutlarını Kullanan Simetrik Bir Şifreleme Algoritmasıdır.

Ağ Bağlantısı

Bilgisayarların Birbirlerine Bağlanması Sonucunda Ortaya Çıkan Ortamağdenir. Günlük Ve Kişisel Yaşam İçerisinde Nasıl Ki Bir Dosyanın Transferine Veya Değiştirilmesine İhtiyaç Duyuyorsak, Kurumla Da Verilerin Değiştirilmesi Ve Transfer Edilmesi Gibi İhti

Ağ Geçidi

Bir Ağdan Başka Bir Ağa Geçilmesini Sağlayan Cihazdır.

Ağ Güvenliği

Ağ Güvenliği, Ağ Trafikini De Kapsayan Dijital Varlıkları Korurken, İzinsiz Ağ Saldırılarını İzlemek, Önlemek Ve Bunlara Yanıt Vermek İçin Tasarlanmış Araçları, Taktikleri Ve Güvenlik Politikalarını Tanımlayan Bir Terimdir. Ağ Güvenliği, Donanım Ve Yazılım

Ağ Trafik Analizi

Ağ Üzerindeki Gelen Ve Giden Trafik Ve Bu Trafik Üzerinde Taşınan Paketlerin Analiz Edilmesi Sürecidir.

Ağ Trafik Analizi

Ağ Üzerinde Gelen Ve Giden Trafik Ve Bu Trafik Üzerinde Taşınan Paketlerin Analiz Edilmesi Durumudur.

KELİME

Aktivite İzlenmesi (Accounting)

DEFINITION

Herhangi Bir Kullanıcının Ne Yaptığı, Kullanıcı Hareketleri, Kullanıcı Veri Bağlantıları Ve Kullanıcı Sistem Kayıtlarının İzlenebilmesi Amacıyla Yapılan İşlemdir.

Alan Adı

Çok Detaya İnmeden, İnternetteki Kimliğinizdir Diyebiliriz

Alan Adı (Domain)

Alan Adı, Bir Web Sitesinin İnternet'Teki Adı Ve Adresidir. Bu Adres Olmadan Bir İnternet Kullanıcısı Web Sitesine Sadece İp Adresiyle Ulaşabilir.

Alan Adı Sistemi

266 Karaktere Kadar Uzaya Bilen Alan Adı İsimlerini İp Ye Çevirmek İçin Kullanılan Hiyerarşik Veritabanıdır.

Alan Adı(Domain)

İnternetteki Kimliğinizdir.

Alarm Durumu

Kurum İçinde Meydana Gelen Herhangi Bir Kesinti Kritik Seviyeye Ulaştığında Ve Kesintiyi Giderecek Çözüm Bulunmadığında Yaşanan Durumdur.

Anahtar Risk Göstergesi

Önemli Riskleri Tahmin Etme Olasılığı Oldukça Yüksek Risk Göstergesi Olarak İfade Edilir.

Anonymizing Proxy

Kullanıcının Web Aktivitesini Gizlemesini Sağlar. Genellikle Web Güvenlik Filtrelerini Atlamak İçin Kullanılır.

Anti Virüs

Bilgisayar, Telefon Başta Olmak Üzere İşletim Sistemi Olan Neredeyse Her Sistemde Kullanılabilen Bir Güvenlik Çözümüdür.

Anti-Malware

Bilgisayar Virüsleri, Solucanlar, Trojanlar Zararlı Tarayıcı Eklentileri, Adware Ve Spyware Dahil Olmak Üzere Birçok Malware Tehdidini Tespit Etmek Veya Ortadan Kaldırmak İçin Yaygın Olarak Kullanılan Teknolojisidir.

Anti-Malwawre

Bilgisayar Virüsleri, Solucanlar, Trojanlar Zararlı Tarayıcı Eklentileri, Adware Ve Spyware Dahil Olmak Üzere Birçok Malware Tehdidini Tespit Etmek Veya Ortadan Kaldırmak İçin Yaygın Olarak Kullanılan Teknolojisidir.

KELİME

Antivirüs

DEFINITION

Antivirüs Bilgisayarları Virüs Adı Verilen Zararlı Yazılımlara Karşı Koruyan Programdır. Antivirüs, Virüsleri Tarayabilir, Temizleyebilir, Karantinaya Alabilir Ve Engellebilir.

Arka Kapı

Bir Sisteme Dışardan Sıza Bilmesi İçin Sistemde Açık Oluşturulması Amacıyla Kullanılan Sanal Bir Ajandır.

Asimetrik Şifreleme

Şifre Ve Deşifre İşlemleri İçin Farklı Anahtarların Kullanıldığı Bir Şifreleme Tekniğidir.

Authentication (Kimlik)

Gönderici Ve Alıcının Kullanıcı Ve Bilgisayarları Doğrularak Veri Trafiğinin Gerçekten Geldiğini Söylediği Kökenden Geldiğini Kanıtlayan Bir Süreçtir.

Availability (Kullanılabilirlik)

Bilgi Sistemlerinin Ve Hizmetlerin Her Zaman Kullanılabilirliğini Sağlamak. (Kaynak Ders Kaydı)

Backdoor (Arka Kapı)

Backdoor, Bir Sisteme Dışarıdan Sızılabilmesi İçin O Sistemde Açık Oluşturma İşlemidir. Genellikle Bazı Portları Açarak Kendi Üreticisinin Ve/Veya Başka Bir Yazılımın Sisteme Sızmasını Sağlayan Yazılımlardır.

Bakteri

Bağımsız, Kendi Kendine Çoğalabilen, Bir Bilgisayarda Birçok Türünü Kendi Kendine Yaratabilen Bir Programdır; Çoğalan Türlerini Çalıştırırken, Daha Fazla Disk Alanı Ve İşletim Zamanı İşgal Ederler.

Bellek

Bilgisayardaçeşitli Programların Çalıştırıldığı, Geçici Veya Kalıcı Bilgilerin Bulunacağı Hafıza Alanlarıdır.

Beyaz Şapkalı Hacker

Beyaz Şapkalılar Her Türlü Programı, Siteyi Veya Bilgisayarı Güvenlik Açıklarından Yararlanarak Kırabiliyor Ancak Kırıldığı Sistemin Açıklarını Sistem Yöneticisine Bildirerek, O Açıkların Kapatılması Ve Zararlı Kişilerden Korunmasını Sağlıyorlar.

Bilgi Güvenliği

Bilgi Güvenliği, Bilgilerin İzinsiz Kullanımından, İzinsiz İfşa Edilmesinden, İzinsiz Yok Edilmesinden, İzinsiz Değiştirilmesinden, Bilgilere Hasar Verilmesinden Koruma, Veya Bilgilere Yapılacak Olan İzinsiz Erişimleri Engelleme İşlemi.

KELİME

Bilişim Sistemleri

DEFINITION

Bilgi Ve İletişim Teknolojileri Vasıtasıyla Sağlanan Her Türlü Hizmetin, İşlemin Ve Verinin Sunumunda Yer Alan Sistemleri

Bot / Botnet

Siber Suçluların Birçok Bilgisayarın Uzaktan Kontrolünü Tamamen Ele Geçirmesine İzin Veren, Güvenliği İhlal Eden Ve Suçlunun Tüm Ağı Uzaktan Yönetebildiği Bir Tür Yazılım Uygulaması Veya Komut Dosyasıdır.

Botnet

Hacker Tarafından Uzaktan Kontrol Edilen Virüslü Bilgisayardır.

Breach (İhlal)

Bir Bilgisayardaki Veya Cihazdaki Güvenlik Açığından Yararlanarak, Dosyalara Ve Ağa Erişim Sağlamaktır.

Browser Hijacking (Tarayıcı Ele Geçirme)

Browser Hijacking, Bazı Web Siteleri Tarafından, Sayfalarının Ziyaret Sayısını Arttırmak, Kendi Web Sitelerindeki Reklamların Yüksek Görüntülenme Rakamlarına Ulaşmasını Sağlamak Amacıyla Web Tarayıcınıza Yerleştirilen, Başlangıç Sayfalarını Ve Arama Sayfa

Brute Force Attack

Kaba Kuvvet Saldırısı: Hackerların Herhangi Bir Kullanıcı Hesabına Erişmek İçin Deneme Yanılma Yöntemi Kullanmasına Denir.

Buffer Overflow

Bir Program Geçici Bir Depolama Alanında Tutabileceğinden Daha Fazla Veri Depolamaya Çalıştığında Oluşur. Tahsis Edilen Bellek Alanının Dışında Yazmak Verileri Bozabilir Ve Programı Çökertebilir. Statik Ve Dinamik İfadeye Hizmet Veren Web Uygulamalarında

Bulut (Cloud)

Dünyanın Herhangi Bir Yerinden, Dosya Vb. Hizmetlerinize İnternet Üzerinden Erişmemizi Sağlayan Büyük Depolama Özelliğine Sahip Bir Teknolojidir.

Bulut Bilişim

Bulut Bilişim Tüm Uygulama, Program Ve Verilerin Sanal Bir Sunucuda Yani Bulutta Depolanmasıdır. İnternete Bağlı Olunan Herhangi Bir Ortamda Cihazlar Aracılığıyla Bu Bilgilere Kolayca Erişim Sağlanabilir.

Bulut(Cloud)

Dünyanın Herhangi Bir Yerinden, Dosya Ya Da Hizmetlerinize İnternet Üzerinden Erişmemizi Sağlayanbüyük Depolama Özelliklerine Sahip Bir Teknolojidir.

KELİME

DEFINITION

Bütünlük

Bilgilerin Kasti, Yetkisiz Veya Kazaya Bağlı Değişikliklerden Korunma Prensidir.

Byod (Kendi Cihazını Getir)

Çalışanların Kişisel Cihazlarının İş Dünyasında Kullanılmasını Sağlayan Bir Şirket Güvenlik Politikasını İfade Eder. Bir Byod Politikası, Kişisel Bir Telefonun Veya Dizüstü Bilgisayarın Kurumsal Ağ Üzerinden Bağlanıp Bağlanamayacağına Dair Sınırlamalar Ve

Captcha

Captcha (İnsan Ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi), Sorgulama-Yanıt Doğrulaması Olarak Bilinen Bir Güvenlik Önlemidir. Captcha Spam Ve Şifre Çözme Koruması Sağlanmasına Yardımcı Olur.

Casus Yazılım

Bir Diğer Virüs Çeşidi Olan Casus Yazılım, Sistem Ve Kullanıcı Faaliyetlerini Gizlice İzler. Örneğin Casus Yazılımı Yöneten Hacker, Ekran Görüntünüzü Alabilir, Klavyede Yazdıklarınızı Kayıt Ederek Kullanıcı Hesaplarınıza Erişebilir.

Casus Yazılım (Spyware)

Casus Yazılım Genellikle Kullanıcının Onayı Ve Bilgisi Olmadan Bir Bilgisayardan Veri Toplayarak Bu Verileri Üçüncü Şahıslara İletmek İçin Tasarlanan Yazılım Olarak Tanımlanır. Genellikle Parolalar, Pın'ler Ve Kredi Kartı Numaraları Gibi Gizli Verilerin T

Catfishing

Somut Kişi Veya Kişileri Kandırmak İçin Sahte Sosyal Medya Hesapları Kullanılarak Yapılan Siber Güvenlik Suçu.

Chipset

Chipset Ya Da Yonga Seti, Bilgisayarın Anakartı Üzerindeki Temel Ve Bütünleşik Arabirimleri Yöneten Ve Bunlar Arasındaki Veri Akışını Sağlayan Bir Çeşit İşlemcidir.

Cia Triad Modeli

Kurum İçerisinde Bilgi Güvenliği Politikalarına Rehberlik Etmek İçin Tasarlanmış Bir Modeldir. Confidentiality (Gizlilik) , Integrity (Bütünlük) Availability (Kullanılabilirlik) Gibi 3 Kavramı Kapsar.

Clickbait

Clickbait, Dikkat Çekmek Ve Kullanıcıları Bu Bağlantıyı İzlemeye Ve Bağlantılı Çevrimiçi İçeriği Okumaya, Görüntülemeye Veya Dinlemeye İkna Etmek İçin Tasarlanmış Köprü Metni Veya Küçük Resim Bağlantısı Kullanan Bir Yanıltıcı Reklam Biçimi.

KELİME

Clickjacking

DEFINITION

İnternet Kullanıcılarının Farkında Olmadan, İstenmediği Bir Bağlantıya Veya Düğmeye Tıklamaya Zorlayan Bir Saldırıdır.

Command Execution Exploits

Komut Çalıştırma Zayıflıkları

Compromise

Network'E Yapılan Saldırı Ve Güvenliği Aşma Durumlarında Güvenlik Sistemi Tarafından Kullanılan Prosedürlere Denir.

Computer Emergency Response Team (Cert)

Bilgisayar Ve Network Güvenliği Konularında Öncelikli Olarak Servis Sağlayan, Sistem Yöneticilerinden Oluşan Bir Resmi Bir Organizasyondur.

Confidentiality (Gizlilik)

Verinin Mahremiyetinin Korunmasıdır.

Cookie (Çerez)

Cookie'Ler Web Sitelerinde Dolaşırken Bilgilerin, Şifrelerin Kaydedildiği, O Web Sitesine Tekrar Girildiğinde Bilgilerin Hatırlanarak Giriş Yapıldığı Dosyalardır.

Cookie (Çerez)

Cookie'Ler Web Sitelerinde Dolaşırken Bilgilerin, Şifrelerin Kaydedildiği, O Web Sitesine Tekrar Girildiğinde Bilgilerin Hatırlanarak Giriş Yapıldığı Dosyalardır.

Cracker

Programların Kodunu Değiştirerek Kırmaya İşlemi Gerçekleştiren Kişilere Cracker Denir.

Cryptology

Şifrebilim

Cyber Threat Intelligence (Cti)

Siber Tehdit İstihbaratı Olarak Dilimize Çevirilir. Hacker Forumlarında, Arama Motorlarında Ve Diğer Kaynaklarda Bir Kurumla İlgili Bilgi Toplama Süreçlerinin Tamamını İçerir. Güvenlik Analistlerinin Yaptığı İş Olan Siber Tehdit İstihbaratı İle, Ortak Çal

Çevreleme Politikası

Bir Olay Tespit Edildiğinde Ve Doğrulandığında Etkilerin Minimum Düzeye İndirilmesi İçin Atılan Adımları İçeren Polikadır.

Çevrimiçi Kimlik

Bir İnternet Kullanıcısının, Çevrimiçi Topluluklarda Ve Web Sitelerinde Kullandığı Sosyal Kimlik.

KELİME

Çok Faktörleri Kimlik Doğrulaması

DEFINITION

Çift Aşamalı Güvenlik Seviyesi Olarak Kullanıma Sunulan Yöntemdir.

Dark Web

Google, Yandex Ve Yahoo Gibi Bilindik Arama Motorlarının İndekslemediği, Onion Ağında Bulunan İnternet Siteleridir. Buradaki Web Sitelerine Ancak Tor Tarayıcısı İle Giriş Yapılabilmektedir.

Data Encryption Standart (Des)

National Institute Of Standars And Technology (Uluslararası Teknoloji Ve Standartları Enstitüsü) Tarafından Geliştirilmiş Gizli Ve Kilit Şifreleme Standartıdır.

Data Privacy

Network Verilerinin Gizlice Elde Edilmesi Ya Da Kurcalanmasına Karşı Oluşturulmuş Savunma İşlemidir. Bazı Durumlarda Gre Veya Layer 2 Tunneling Protocol (L2Tp) De Olduğu Gibi Tunneling Teknolojisi Kullanılarak Data Ayrılır, Bu Da Etkili Veri Gizliliğini Sa

Ddos Saldırısı

Genellikle İnterneti Ya Da Belirli Bir Siteyi Êrişilmez Hâle Getirmekte Kullanılır. Botnet Olarak Bilinen (Bot Kelimesi Robotun Kısaltması, Net İse Ağ Anlamına Geliyor) Binlerce Bilgisayarın Ayna Anda Bir Servisi Kullanmak İstemesiyle, Talep Yoğunluğu Olu

Debian

Birçok Linux Dağıtımının Kaynak Olarak Komutların Kullanıldığı Ve Orta Seviyedeki Her Linux Kullanıcısının Kullanabileceği Bir Linux Dağıtımıdır.

Deepfake

Deepfakes, Mevcut Bir Görüntü Veya Videoda Yer Alan Bir Kişinin Yapay Sinir Ağları Kullanarak Bir Başka Kişinin Görüntüsü İle Değiştirildiği Bir Medya Türüdür.

Denial Of Service Attacks (Hizmeti Engelleme Saldırısı)

Truva Atlarının Dayandığı Temel Düşünce Kurbanın Bilgisayarındaki İnternet Trafiğini Bir Web Sitesine Ulaşmasını Veya Dosya İndirmesini Engelleyecek Şekilde Arttırmaktır. Hizmeti Engelleme Saldırısı Truva Atlarının Bir Başka Versiyonu Mail-Bombası Truva A

Deşifreleme(Decryption)

Şifrelenmiş Olan Bilgilerin Eski Haline Getirilmesi.

Dış Tehdit

Dışardan Yapılan Saldırıları İle Sunucuya Erişip, Yazılımın Kaynak Kodları Veya Sunucuda Bulunan Veri Tabanına Ulaşmak Veya Şirket İçi Önemli Bilgilerinin Çalınması, Dış Tehdit Olarak Adlandırılabilir

KELİME

Diffie Hellman

DEFINITION

Şifreleme Tabanlı Yönetim Sistemlerinde, İzin Verilen İki Kullanıcı Ya Da Network Cihazının Güvensiz Bir Ortamda Yine Bu Şifreleri Kullanarak Güvenli Bir Şekilde Data Alış-Verişi Yapmasıdır.

Dmz

Yerel Alan Ağlarının (Lan) Güvenliğini Sağlamak için Bir Güvenlik Duvarı Yapılandırması.

Dmz Demilitarized Zone

Savunmasız Bölge Olarak İfade Edilebilir. Güvenlik Duvarı Tarafından Daha Az Korunan, Daha Fazla Erişime İzin Verilen Bölgedir.

Dns Hijacking

Dns Hijacking Saldırısında Saldırgan Bilgisayarın Ayarlarını Dns'i Görmezden Gelecek Şekilde Değiştirir Veya Kendisi Tarafından Kontrol Edilen Bir Dns Sunucusu Kullanır. Saldırganlar İletişimi Sahte Sitelere Yönlendirir. Kullanıcılar Genellikle Giriş Bilg

Doğrulayıcı

Kullanıcın Kimliğini Sisteme Doğrulatma Biçimidir. Yüz Tarama Ya Da Şifre Olabilir.

Dos/Ddos

Denial Of Service --- Hizmet Reddi Distributed Denial Of Service --- Dağıtılmış Hizmet Reddi dağıtılmış Ağ Saldırıları isimleriyle bilinir. Bu Tür Saldırıları, Bir Şirketin Web Sitesini Sağlayan Altyapı Gibi, Herhangi Bir Ağ Kaynağı İçin Geçerli Olan Belirli Ka

Dosya Aktarımı

İnternete Bağlı Bilgisayarlar Arasında Dosya Transferi Yapmak İçin Kullanılan Bir İnternet Protokolüdür.

Driver

Bilgisayar Kullanıcılarının Tümünün Bilmesi Gereken En Temel Terimlerden Biri Olan Driver Türkçesiyle sürücüdür. Bilgisayarımızın Üzerinde Yer Alan Donanımların Tümünü Bir Ana Karta Bağlıdır. Bu Ana Kart Üzerindeki Donanımların K

E- Mail Malware

E- Mail Aracılığıyla Yayılan Bir Zararlı Yazılımdır. Virüslerin Yayılması İçin Kullanıcının Ekteki Linke Tıklaması Gerekir.

Eap

(Genişletilebilir Kimlik Doğrulama Protokolü) İki Cihaza Kimlik Doğrulama izni Veren bir Standart.

Eap: (Genişletilebilir Kimlik Doğrulama Protokolü)

İki Cihaza Kimlik Doğrulama izni Veren bir Standart.

KELİME

DEFINITION

Eaves - Dropping

Özel Konuşmaların Gizlice Dinlenmesidir.

Edr

Endpoint Detection & Response-Uç Nokta Tespiti Ve Yanıtı. Bu Araç Sınıfı, Ana Bilgisayarlara Yüklenen Uç Nokta Aracılarını Ve Bunları Yönetmek İçin Altyapıyı İçerir.

Ekran Kazıyıcı

Özel Veya Kişisel Bilgileri Yakalamak İçin Görsel Bir Ekranı Gönderilen Bilgileri Günlüğe Kaydeden Bir Virüs Veya Fiziksel Cihaz.

En Düşük Erişim Hakkı İlkesi

Bir Görevi Tamamlamak İçin Gereken Erişim Hakkını Sağlamak Amacıyla Kullanılan Kontrollerdir.

Encryption

Verinin İletim Sırasında Bilinçli Olarak Şifrelenmesi Ve Kimse Tarafından Okunmadan Alıcıya Ulaştırılması Ve Ardından Yeniden Şifrenin Çözülmesi İşlemidir.

Entegre

Birbiriyle Bağlantılı Olarak Olan,Tümleşme.

Erişebilirlik

Erişilebilirlik, Yetkili Tarafların Gerektiğinde Bilgilere Erişebilmelerini Sağlar. Veriler, Yalnızca Doğru Kişiler Doğru Zamanda Erişebiliyorsa Değer Taşır. Ddos Saldırıları, Donanım Hataları, Programlama Hataları, İnsan Hataları Gibi Güvenlik Olayları N

Erişim

Belirli Bir Adresteki Verilere Okuma Veya Yazma İşlemi Gerçekleştirebilecek Şekilde Ulaşılma İşlemidir.

Erişim Kontrolü

Erişimkontrolü, Binanıza, Belirli Odalara Veya Bölgelere Girmek İçin İzin Vermenizi Ve İzin Vermemenizi Sağlayan Bir Güvenlik Tekniğidir.

Etki Analizi

Siber Olayların Veya Tehditlerin Maliyetleri Baz Alınarak Bilgi Kaynaklarının Kurum Açısından Kritiklik Seviyelerinin Tespit Edilmesi Amacıyla Gerçekleştirilen Çalışmalardır.

Exploit(Sömürme)

İşletim Sistemleri Ve Bazı Programların Açıklarını Bulup Bu Açıkları Kötüye Kullanma Yöntemine "Exploit" Deniliyor. Exploit'ler İle Sistem Şifreleri Görülebilir, Sistemler Hakkında Bilgiler Elde Edilebilir. Exploitler Sistemin Olağan Olarak Çalışmasına

KELİME

Fidye Yazılım

DEFINITION

Bir Cihazı Kilitleyebilen Veya Sahibinden Para Çekmek İçin İçeriklerini Şifreleyebilen Kötü Amaçlı Yazılımlardır.

Fidye Yazılımı (Ransomware)

Sisteme Giriş Yapabildiği Takdirde Üst Seviye Şifreleme Mekanizmalarını Kullanarak Mevcut Verileri Şifreleme İşlemine Dayanır. Verilerini Geri İsteyen Kurum Ve Firmalardan Belli Bir Miktarda Fidye Talep Ederek Çözücü Parolayı Verme Sistemi İle Çalışmaktadır

Fidye Yazılımı(Ransomware)

Bir Cihazın Verilerini Sanal Olarak Ele Geçirir Ve Karşılığında Fidye İster. Daha Detaylı Anlatmamız Gerekirse; Bilgisayarınızdaki Tüm Verileri Şifreler, Bu Veriler Şifre Anahtarı Olmadan Şifresiz Hâllerine Döndürülemez. Yazılım Bu Şifreyi Hacker'ın Belir

Firewall

Güvenlik Duvarı Yazılımı, Bir Kural Kümesi Temelinde Ağa Gelen Giden Paket Trafiğini Kontrol Eden Donanım Tabanlı Ağ Güvenliği Sistemidir. Birçok Farklı Filtreleme Özelliği İle Bilgisayarve Ağın Gelen Ve Giden Paketler Olmak Üzere İnternettrafiğini Kontro

Frame

Bir Web Tarayıcısı Bağlamında, Bir Çerçeve, İçeriği Bağımsız Olarak Yükleyebilen, Kabından Bağımsız Olarak İçerik Görüntüleyen Bir Web Sayfasının Veya Tarayıcı Penceresinin Bir Parçasıdır.

Gelişmiş Kalıcı Tehdit- (Apt)

Gelişmiş, Gizli, Sürekli Saldırı Teknikleri Kullanılarak Sisteme Erişen Ve Orada Bilgi Toplamak, Sızdırmak, Yıkıcı Sonuçlar Yaratmaya Yetecek Kadar Uzun Süreli Olan Saldırılardır.

Geniş Alan Ağı

Birden Fazla Cihazın Birbiri İle Bağlanmasına Ve İletişim Kurmasını Sağlayan Fiziksel Veya Mantıksal Büyük Ağıdır. Yerel Alan Ağlarınınbirbirine Bağlanmasını Sağlayan Çok Geniş Ağlardır. En Meşhur Geniş Olan Alan Ağı İnternettir

Giriş Kontrolü (Access Control)

Ağ Üzerindeki Herhangi Bir Bilgi Kaynağına Erişim Konusunda Yetkilendirilmiş Kişiler, Programlar, İşlemler Veya Ağ İçindeki Diğer Sistemler İçin Konulan Sınırlamadır. Bu Sınırlamalar Verilerin Korunması İçin Yapılır.

Gizlilik

Gizlilik, Verilerin Yetkisiz Tarafra İfşasını Önlemekle İlgilidir. Ayrıca, Verilerin Paylaşılması Ve Gizli Tutulması İle İlgili Yetkili Tarafların Kimliğini Gizli Tutmaya Çalışmak Anlamına Da Gelir. Çoğunlukla Gizliliğin Kötü Olması, Doğru Şekilde Şifre

KELİME

DEFINITION

Gizlilik (Confidentiality)

Verinin Mahremiyetinin Korunmasını Sağlar. Verinin Korunumunu Sağlamak İçin Belirli Kategorilere Ayrılabilir. Bu Sayede Her Verinin Erişimi Verinin Gizliliğine Göre Sınıflandırılır Ve Gizliliğe Göre Tedbir Alınır.

Gölge Parola

Linux Sistemlerde Kullanıcı Hesap Bilgileri, /Etc/Passwd Dosyasında Tutulur. Eğer Şifreleme Olarak "Gölge Parola" (Shadowing) Seçilmişse Şifreler Ayrı Olarak /Etc/Shadow Dosyasında Tutulur. Gölge Parola, Sonradan Linux Sistemlere Eklenmiş Bir Özelliştir.

Görüntü Şifreleme

Görüntü Şifreleme bir Kameranın Bulunduğu Konum İle Yakaladığı Görüntülerin Uzaktan İzlendiği, Kaydedildiği Ve Saklandığı Yer Arasında, Bir Siber Suçlunun Ağa Girip Gizli Video Ve Verilere Erişme Olasılığı Daima Bulunmaktadır. Görüntü Şifreleme, Ağ Üzerind

Gri Şapkalı Hacker

Şahsi Veya Kurumsal Bilgisayarlara Ve Ağlara İlegal Yöntemlerle Giriş Yapıp Buldukları Güvenlik Açıklarını, Sorunları Giderirler. Ya Da Buradan Elde Ettikleri Verileri İyi Bir Amaç Uğruna Kullanırlar. Niyetleri İyi Ancak Kullandıkları Yöntem Legal Değild

Güvenli İşletim Sistemi (Os)

Şifreleme Ve Şifre Çözmenin Yanı Sıra Uygulamaların Değiştirilmediğini Veya Sahte Olduğunu Doğrulamak Amacıyla Ayrı Bir İşletim Sistemi (Os) Kullanmak, Kameranın Ana İşletim Sisteminin İş Yükünü Azaltır. Güvenli Bir İşletim Sistemine Erişmek İçin Ayrı Bir

Güvenli Jtag

Jtag Portları; Aygıtları Programlamak, Test Etmek Ve Hata Ayıklamak Amacıyla Kullanılan Donanım Arayüzleridir. Bununla Birlikte, Siber Suçlular Tarafından Ele Geçirilerek Bir Cihazın Düşük Düzeyde Kontrolünü Kazanmak Ve Belki De Ürün Yazılımını Kötü Amaç

Güvenlik

Toplum Yaşamında Yasal Düzenin Aksamadan Yürütülmesi, Kişilerin Korkusuzca Yaşayabilmesi Durumudur.

Güvenlik Açığı

Bilgisayar Güvenliğinde Güvenlik Açığı, Saldırgan Gibi Bir Tehdit Aktörü Tarafından Bilgisayar Sistemi İçindeki Ayrıcalık Sınırlarını Aşmak İçin Yararlanılabilen Bir Zayıflıktır.

Güvenlik Açıkları

Güvenlik Açıkları Saldırganların Sisteme Sızmasını Sağlayan Zayıf Noktalar Veya Saldırganların Sistemlere Zarar Verip, Güvenliğini Azaltan Açıklar Da Denilebilir.

KELİME

Güvenlik Duvarı

DEFINITION

Ağa Bağlı Sistemleri Kendi Dışındaki Etmenlerden Korumak Üzere Kullanılan Yazılım, Donanım Ya Da Her İkisinin Birleşimi Yapılar. İzin Verilmeyen Erişimi Önler. Bunun İçin Belirli Kural Yapıları Konularak, Güvenlik Duvarının Bunlara Uyması Sağlanabilir. At

Güvenlik Duvarı (Firewall)

Yetkisiz Erişimi Engellemek İçin Tasarlanmış Bir Bilgisayar Sistemi Veya Ağın Bir Parçası

Hacker

Aslında Sistem Yapısını İhlal Eden Herkese Verilen Ad. Bir Cihazı Üretildiğinden Farklı Şekilde Çalıştırabiliyorsanız, Siz De Bir Hacker'Sınız. Ancak Güvenlik Anlamında Beyaz Şapkalı Ve Siyah Şapkalı Olarak İkiye Ayrılıyor. Tıpkı Yüzüklerin Efendisi'Nde O

Hackivist

Hackivism Eylemleri Sergileyen İnternet Korsanlarıhaktivistdenir.

Hacktivizm

Politik Bir Gündemi Veya Sosyal Değişimi Teşvik Etmek İçin Bir Sivil İtaatsizlik Biçimi Olarak Bilgisayar Korsanlığı Gibi Bilgisayar Temelli Tekniklerin Kullanılmasıdır.

Harmanlanmış Tehdit Metodu

-Farklı Güvenlik Açıklarına Karşı Saldırıların Bir Kombinasyonu Kullanarak Gerçekleştirilen Bir Tehdit Metodudur.-Özellikleri: Solucan, Truva Atı, Gibi Çeşitli Malware- Kurbanı Ele Geçirme Yöntemi: Phishing Gibi Bir Çok Farklı Metod Kullanılır.

Harmanlanmış Tehdit Metodu

Farklı Güvenlik Açıklarına Karşı Saldırıların Bir Kombinasyonu Kullanarak Gerçekleştirilen Bir Tehdit Metodudur.

Hash

Hashdeğeri, Dosyaların Kendilerine Özel Parmak Veya Dil İzleridir.Hashdeğerine Göre Dosyada Değişiklik Yapılıp Yapılmadığını, Dosyanın Düzgün Bir Şekilde Bilgisayarınıza İnip İnmediğikontrol edilebilir.

Hedef Kitle

Pazarlaması Yapılacak Olan Ürünün Kim Tarafından Ve Ne Amaçla Alınacağı Yönünden Yapılan İstatistiki Bilgileri Oluşturmaktadır.

Hedef Odaklı Oltalama(Spear Phishing)

Hedefe Odaklı Bir Oltalama Yöntemi Kullanılır, Belirli Bir Sektöre Ait Çalışanlar Veya Belirli Bir Grubu Hedef Alan Bu Atak Sofistike Tekniklerin Kullanıldığı Bir Saldırı Çeşididir.

KELİME

Host(Network)

DEFINITION

Ağ Ana Bilgisayarı, Bir Bilgisayar Ağına Bağlı Bir Bilgisayar Veya Başka Bir Aygittir. Ana Bilgisayar, Kullanıcılara Veya Ağdaki Diğer Ana Bilgisayarlara Bilgi Kaynakları, Hizmetler Ve Uygulamalar Sunan Bir Sunucu Olarak Çalışabilir. Ana Bilgisayarlara En

Hotspot

Hotspot, Çoğunlukla Halka Açık Ya Da Kurumsal Alanlarda Kullanılan İnternet Hizmetidir.

Html

Html Hyper Text Markup Language Kelimelerinin Kısaltılması Şeklinde Olan Metin İşaretleme Dilidir. Web Sitelerin Oluşturulmasında Kullanılan Bir Programlama Dilidir, Bu Dilin Çalışabilmesi İçin Chrome, Firefox, Safari, Edge, Opera Gibi Tarayıcılar Tarafın

Https

Özellikle İnternet Üzerinde Geniş Dağıtım Yapan Bilgisayar Ağı Üzerinde Güvenli İletişim İçin Bir İletişim Protokolü.

Https (Hypertext Transfer Protocol Secure)

Özellikle İnternet Üzerinde Geniş Dağıtım Yapan Bilgisayar Ağı Üzerinde Güvenli İletişim İçin Bir İletişim Protokolü.

Id Numarası

Id; Kullanıcı Adı Demek, Herhangi Bir Yerde, Forumlarda, Oyunlarda, Kullanıcı Gerektiren Programlarda, E-Posta Servislerinde Kullanılır.

Idor (Insecure Direct Object Reference)

Türkçeye "Güveniz Doğrudan Nesne Referansı" Olarak Çevirilmiştir. Bir Web Uygulama Güvenliği Zafiyetidir Ve Access Controll Adımında Ortaya Çıkmaktadır. Saldırganın , Web Uygulamasına Gönderdiği İsteği Başka Bir Nesne Referansı İle Gönderiyormuş Gibi Mani

Incident Response (Olay Müdahalesi)

Oluşan Bir Siber Saldırı Sonrasında Kurumun Hasarı Gidermesi Ve Açığı Kapatması İşlemidir. Olay Müdahalesini Genelde Computer Securirty Incident Response Team (Csirt) Yapmaktadır.

Incognito Mode (Gizli Mod)

İnternet Tarayıcılarıyla Sunulan, Gizlilik Özelliğidir.

Information Security

Bilginin Güvenliğidir. Özellikle Kurumsal Bilgi Cıa Triad Modeli İle Korunmalıdır.

Integrity (Bütünlük)

Verinin Tüm Yaşam Döngüsü Boyunca Tutarlılığını Ve Güvenilirliğini Korumayı İçerir.

KELİME

DEFINITION

Intrude

İzinsiz Girmek. Intruder : İzinsiz Giren Kişi.

Intrusion Detection System

Bir Bilgisayar Ya Da Bağlı Kaynaklara İzinsiz Erişim Hâline Uyarı Veren Ve Programlandıkları Diğer Eylemleri Gerçekleştiren Sisteme Denir.

Intrusion

İzinsiz Giriştespit Sistemi (Ids), Tüm Gelen Ve Giden Ağ Faaliyetlerini Denetler Ve Bir Sisteme Girmeye Ya Da Bir Sistemi Ele Geçirmeye Çalışan Birinden Bir Ağ Ya Da Sistem Saldırısını Gösterebilecek Şüpheli Kalıpları Tanımlar.

İot(Internet Of Things)- Nesnelerin İnterneti

Nesnelerin İnterneti, Fiziksel Nesnelerin Birbirleriyle Veya Daha Büyük Sistemlerle Bağlantılı Olduğu İletişim Ağıdır. Nesnelerin Tekil Anahtar İle İşaretlenerek İnternet Altyapısı Üzerinden Birlikte Çalışabilmesi Ve Bu Sayede Küçük Parçaların Toplamından

İp Adresi

İp Adresi, Uzun Adı "İnternet Protokolü" Olan, İnternet Üzerinden İletişim Kurabilmek Ve Veri Alışverişinde Bulunabilmek İçin Kullanılan Ağ Kimliğidir. İnternete Bağlı Olan Her Cihazın Bir Kimliği Olmak Zorundadır. İp Adresleri, İnternet Üzerinden Gönderi

İç (Dahili) Saldırganlar

Organizasyon İçerisinde, Belirli Amaçlar Çerçevesinde Dahilisistemlere Saldırı Düzenleyen Kurumsal Kişilerdir.

İç Tehdit

Şirket İçi Kullanıcılarının,Kullanıcı Hesapları Çalınması,Kötü Niyetli Çalışanların Veriyi Dışarıya Sızdırmak İstemesi, Kızgın Çalışanlar İç Tehdit Örneğidir.

İki Adımlı Kimlikleri Doğrulama

Kullanıcıların Parolanın Yanı Sıra, İkinci Bir Adım İzleyerek Sisteme Giriş Yapmalarını Sağlar. Örneğin İnternet Bankacılığında Olduğu Gibi Telefonunuza Bir Sms Gelir. Böylece Sadece Kullanıcı Adı Ve Parolanız Sisteme Girişte İşe Yaramaz. Telefonunuzdaki

İntegrity(Bütünlük)

Verinin Tüm Yaşam Döngüsü Boyunca Tutarlılığını Ve Güvenilirliğini Korumayı İçerir. (Kaynak: Ders Kaydı)

İşlemci

Bilgisayarın Temel İşlem Birimini Oluşturan, Belirli Mantık Ve Matematik İşlemlerini Elektronik Olarak Yapabilecek Biçimde, Verilen Komutları Yorumlayan Ve Yürüten, Yongalardan Oluşmuş Tümleşik Devre.

KELİME

İşletim Sistemi

DEFINITION

İşletim Sistemi, Bilgisayarda Çalışan, Donanım Kaynaklarını Yöneten Ve Çeşitli Uygulama Yazılımları İçin Yaygın Servisleri Sağlayan Yazılımdır.

Kali Linux

Kali; Linux Tabanlı, Cd'Den Başlatma Seçeneklibacktrackyapımcıları Tarafından 2013 Yılında Oluşturulmuş Olan Bir Güvenlik Kontrol İşletim Sistemidir.

Kamu Bilişim Sistemler

Türkiye Cumhuriyeti Kamu Kurum Ve Kuruluşlarına Ait Olan Ve/Veya Kamu Kurum Ve Kuruluşları Tarafından İşletilen Bilişim Sistemlerini

Katman Anahtarı

Alıcı Ve Gönderici Cihazların İpadreslerine Bağlı Olarak Verileri Filtreleyen Ve Aktaran Bir Cihazdır.

Kayıt Edici (Logger)

Genellikle Bir Zararlı Yazılımla Sisteme Bağlı Giriş Ve Çıkış Cihazlarını Takip Ederler Ve Her Hareketlerini Kaydederek, Sisteme İzinsiz Erişen Kişi Veya Kişilere İletirler. Bu Sayede Yazılan Her Şey Karşı Tarafa Gittiği İçin Kullanıcı Adı Ve Parolalar, K

Kendi Cihazını Getir

Kişilerin İşyerlerinde De Kendi Şahsî Cihazlarını Kullanmasını İfade Ediyor. Ancak Bunun Yaygınlaştığı Günümüzde, Kurumsal Güvenlik Politikaları Değişiyor. Kurumsal Veri Hırsızlığı, Kişisel Cihazlardan Bulaşabilecek Zararlı Yazılım Tehlikesi Gibi Konular

Kerberos Protokolü

Sistemlerde Kimlik Doğrulama İşlemini Biletler Aracılığıyla Sağlayan Bir Protokoldür. Kullanıcı Sistemde Bir İşlem Yapmak İstedğinde Kerberos Protokolü Sayesinde Tgt (Ticket Granting Service)'Den Bir Bilet Alır Ve Bu Bileti İşlem Yapmak İsteddiği Servise

Keylogger

Keylogger, Bir Tür Takip Yazılımıdır. Bu Yazılım, Kullanıcının İzni İle Veya Kullanıcıdan İzinsiz Bilgisayara Yüklendiğinde, Bilgisayarda Anlık Olarak Ekran Görüntüsü Çekilir, Klavyede Basılan Her Tuşun Kaydı Tutulur Vebu Kayıtlar Kişisel Bilgilerinizi Ç

Keylogger (Tuş-Kayıt)

Keylogger, Uzak Bilgisayara Kendi Kurulumunu Gerçekleştirdikten Sonra Genellikle Kendini Hiç Belli Etmeden Çalışmaya Başlar Ve Kaydettiği Verileri Programlandığı Zaman Aralıklarında Hacker 'A İletir. Genellikle Tüm Klavye Hareketlerini Ara Hafızasına Alır

KELİME

Kimlik (Authentication)

DEFINITION

Gönderici Ve Alıcının Kullanıcı Ve Bilgisayarları Doğrularak Veri Trafiğinin Gerçekten Geldiğini Söylediği Kökenden Geldiğini Kanıtlayan Bir Süreçtir.

Kimlik Avı

Şifre Ve Sosyal Güvenlik Numarası Gibi Hassas Bilgilerin Korsanlarca Görevlendirilen Kullanıcılar Tarafından Ele Geçirilmesidir.

Kimlik Denetimi

Herhangi Bir Kişiye Ait Rol Ya Da Kimliğin Doğrulama Mekanizmasıdır.

Kişisel Veri

Tanımlanan Bilen Yaşayan Bir Kişiye Ait Olan Tüm Verilerdir. Bireyin Adı Ve Soyadı, Doğum Tarihi, Doğum Yeri Gibi Kişinin Kesin Teşhisini Sağlayan Bilgiler, Bu Bilgilere Telefon Numarası, Arabasının Plakası, Pasaport Numarası Veya Fiziki, Ailevi, Ekonomik

Klavye Dinleme Sistemi

Klavye Dinleme Sistemi Veya Klavye Yakalama Sistemi, Klavyede Bir Harfe Dokunulduğunda Casus Yazılım Dinler Ve Klavye Harflerini Kaydeder.

Klon Karşıtı Donanım

Klon Karşıtı Donanım İşlevi Bir Yonga Setinin Klonlanmasını Önler. Fikri Mülkiyetin Korunmasına Ek Olarak, Bu İşlev, Üreticinin Etiketine Sahip Bir Yonga Setinin Orijinal Kopya Olmasını Sağlar Ve Parolalar Gibi Hassas Verileri Çalmak Amacıyla Kullanılan K

Kötü Amaçlı Yazılım(Malware)

Bir Bilgisayarda Hasara Yol Açmak İçin Tasarlanmış Her Türlü Kötü Amaçlı Yazılımı Tanımlayan Bir Terim. (Virüs, Worm Vb)

Kripto Hızlandırma

Kameralı Güvenlik Çözümlerine Uygulandığında, Kripto Hızlandırma Genellikle Şifreleme Ve Şifre Çözmeye İlişkin Karmaşık Matematiksel İşlevler Gerçekleştiren Bir Kamera Yonga Seti Bağlamında İfade Edilir. Bu, Yonga Setine Ait Kaynakların Büyük Bir Kısımının

Kriptografi Anahtarı

Şifreleme, Şifre Çözümü Ve Bilgi Onaylamak İçin Kullanılan Dijital Bir Şifredir.

Kriptoloji

Kriptoloji, Şifre Bilimidir.Kendi İçerisinde İki Farklı Branşa Ayrılır Bunlar Kriptografi(Şifreli Yazı Yazma)Ve Kriptoanalizdir(Şifreleri Çözme Ya Da Analiz Etmedir.). Kriptoloji; Askeri Kurumlardan, Kişiler Arası Veya Özel Devlet Kurumları Arasındaki İle

KELİME

Kurumsal Veri

DEFINITION

Kurumların Merkezi Özelliklerini, İç Yapılarını,Süreçlerini Ve Farklı Sosyal Ve Ekonomik Bağlantılarda Kurumsal Aktörler Olarak Davranışlarını Tanımlar. (Kaynak Ders Kaydı)

Local File Inclusion

Web Uygulamalarında Bulunan Bir Güvenlik Açığıdır. Hedef Sistemde Normalde Kullanıcının Görmemesi Gereken Dosyaları Görüp Okuyabilmesine Neden Olan Açık Türüdür.

Loglama

Tüm Kritik Ağlar. Cihazları Kapsayan Bilişim Sistemlerinin Ürettiği Olay Kayıtlarının Belirlenen Kurallara Göre Analiz Edilmesidir.

Mail Server

İnternet E-Posta Sisteminde, Bir Mesaj Aktarım Aracısı Veya Posta Aktarım Aracısı Veya Posta Aktarımı, Smtip Kullanarak Elektronik Posta Mesajlarını Bir Bilgisayardan Diğere Aktaran Yazılımdır.

Malicious Software

Virüsler, Solucanlar, Truva Atları, Casus Yazılımları, Reklamlar, Tehditkar Yazılımlar, Programları İzinsiz, Şifreleyen Yazılımlar, Kötü Niyetli Yazılımların Tümü

Malicious

Kötü Niyetli

Malware

Scumware Olarak Daadlandırılan Malware;Bilgisayarınızın Ayarlarını Değiştirmek, Yazılımlarınızı Ortadan Kaldırmak, Sistem Hatalarına Neden Olmak, Kullanım Alışkanlıklarınızı İncelemek Veya Bilgisayarınızı Saldırlara Karşı Tamamen Açık Hale Getirmek Amacı

Man-İn-The-Middle Attack

Ortadaki Adam Saldırısı

Mantık Bombası (Logic Bomb)

Belirli Bir Zamanda Veya Belirli Bir Durum Oluştığında Çalışan Programlardır. Mantık Bombası, Bilgisayarda Gizli Bir Şekilde Çalışacağı Günü Bekleyebilir Veya Kullanılan Bir Programda Zamanı Geldiğinde Zararlı İşlemleri Yapacak Şekilde Ayarlanabilir.

Meltdown

-Kullanıcı Uygulamaları Ve İşletim Sistemi Arasındaki Temel Soyutlama Mekanizmasını Kırarak Zararlı Bir Uygulamanın Belleğe Erişmesine Ve İşletim Sistemi Veya Diğere Uygulamaların Memory'De İşlediği Gizli Bilgileri Elde Etmeye Olanak Sağlamaktadır.- Uzmanl

KELİME

Mimikatz

DEFINITION

Windows'Daki Kimlik Doğrulama İşlemini Sömürerek Sistemdeki Kullanıcının Parolasını Açık Metin Olarak Elde Eden Bir Araç.

Mirai

Linux Çalıştıran Ağa Bağlı Cihazları, Büyük Ölçekli Ağ Saldırılarındabir Botnet'in Parçası Olarak Kullanılabilecekuzaktan Kontrol Edilen Botlaradönüştürenbir Kötü Amaçlı Yazılımlardır.Öncelikle Ip Kameralarve Ev Yönlendiricileri Gibi Çevrimiçi Tüketici Ci

Mobil Cihaz Yönetimi (Mdm)

Mdm, Mobil Cihaz Yönetimi Yani Mobile Device Management Kelimelerinin Kısaltmasıdır. Kurumsal Verilerin, Mobil Cihaz (Akıllı Telefon, Tablet Gibi) İşletim Sistemleri Üzerinden Bilgi Güvenliğini Sağlamak Amacıyla İdaresidir. Kurum, Kuruluş Ve İşletmeler Bi

Multipartite (Çok Bölümlü Virüs)

Boot Ve Dosya / Program Virüslerinin Melezi Olarak Tanımlanabilir. Program Dosyalarına Bulaşır Ve Program Açıldığında Boot Kayıtlarına Yerleşir. Bilgisayarın Bir Dahaki Açılışında Hafızaya Yerleşir Ve Oradan Diskteki Diğer Programlara Da Yayılır

Nat (Ağ Adres Çevirmeni)

Bir Ağda Kullanılan Ip Adresinin Başka Bir Ağdaki Ip Adresine Dönüştürülmesi

Netflow

Etkin Olan Bir Ağ Anahtarına Giden Veya Gelen Tüm Ip Trafikini Toplamak Ve Kaydetmek Ve Ağ Trafikini İzlemek İçin Yaygın Kullanılan Protokoldür.

Network

İki Veya Daha Fazla Bilgisayarın Kablolulu Veya Kablosuz Bir Şekilde Birbirine Bağlanarak Veri Alışverişinde Bulunmasına Network Denir. Geçmiş 1960'Lı Yıllara Dayanıp Günümüzde Yaygın Biçimde Kullanılmaktadır. Bilinen En Büyük Network İnternettir.

Nmap

Kali Linux İşletim Sisteminde Varsayılan Bir Araç Olarak Gelmektedir. Esasen Port Tarama Aracı Olarak Ortaya Çıksa Da Yapılan Geliştirmeler İle Hedef Sistemde Derinlemesine Tarama Yapabilmekte Ve Açık Keşfine Olanak Tanıyabilmektedir. En Yaygın Kullanılan

Oltalama

Dünyadaki Hack Olaylarının Büyük Bölümü Sosyal Mühendislikle Gerçekleşir. Yani Birisi Sizi kandırarak Bilgilerinizi Alır Ya Da Parolanızı Tahmin Edecek Kadar Bilgi Toplar. Oltalama Da, Sizi Başka Bir Şey Oluyormuş Gibi kandıran Bir Saldırı Türüdür.

KELİME

Oltalama Saldırısı

DEFINITION

Siber Saldırganlar Tarafından Seçilen Kurbanlara Ait Mahrem Bilgilerin, Finansal Verilerin, Banka Hesapları Gibi Benzeri Kritik Verilerin Çalınmasıdır. Rastgele Bir Kurban Seçilebileceği Gibi Bir Kişi Veya Kurum Da Hedef Alınabilir.

Open Source

Açık Kaynak Kod

Ortadaki Adam Saldırısı(Man-İn-The-Middle Attack))

Man-İn-The-Middle Attack, Saldırganın Birbiri İle Doğrudan İletişim Kuran İki Taraf Arasındaki İletişimi Gizlice İlettiği Veya Değiştirdiği Saldırı Türüdür.Wikipedia

Ortadan Kaldırma

Olay Kontrol Altına Alındıktan Ve Gerekli Önlemler Uygulandıktan Sonra Olayın Asıl Nedeni Tespit Edilir Ve Tamamen Ortadan Kaldırılır.

Ölçeklenebilirlik

Sistemin Bir Şirketin İş İhtiyaçlarını Karşılama İçin Büyüme Yeteneğidir.

Pasif Saldırı

Çoğu Saldırı Aktif Saldırı Olma Özelliğini Taşıyor. Yani Hacker Ya Da Virüs Sisteme Girip Bir Değişiklik Yapıyor, Zarar Veriyor. Pasif Saldırı İse Sisteme Girip, Olup Biteni İzlemeye Verilen Ad. Bilgi Hırsızlığı Amacıyla Yapılıyor.

Password Generator

Rastgele Bir Şifre Üreticisi, Rastgele Veya Sözde Rastgele Bir Sayı Üreticisinden Girdi Alan Ve Otomatik Olarak Bir Şifre Üreten Yazılım Programı Veya Donanım Cihazıdır.

Pen Test (Sızma Testi)

Sızma Testi, Güvenlik Açıklarını Bulmak Ve Güvenlik Açıklarını Değerlendirmek Amacıyla Korsan Araç Ve Teknikleri Kullanarak Güvenliği Değerlendirmenin Bir Yoludur.

Penetrasyon(Sızma Testi)

Penetrasyon (Sızma) Testi, Alanında Tecrübeli Ve Siber Güvenlik Üzerine Gelişmiş Bilgilere Sahip Uzmanlar Tarafından, Hackerların Kullandıkları Araç Ve Teknikler Kullanılarak Hedef Kurum Veya Şirkete Yönelik Gerçekleştirilen Siber Güvenlik Analiz Ve Atak

Penetration Test

Bir Bilişim Sisteminin Durumunu Ve Üzerinde Barındırdığı Zafiyetleri Tespit Etme Yaklaşımını İfade Eder.Bilişim Sisteminin Sahibi, Ne Kadar Güvende Olduğunu Ve Alınması Gereken İlave Tedbirleri Tespit Etmek İçin, Sızma Ve Güvenlik Testini Kullanabilir.Söz

KELİME

Phishing

DEFINITION

Oltalama Saldırıları Olarak Da Bilinen Bu Saldırı Türünde Genel Olarak Kurbanların E-Posta Hesaplarına Hediye, İndirim, Ödül gibi Cezbedici Sahte İletiler Gönderilir Ve Kredi Kartı Bilgileri, Kimlik Bilgisigibi Hassas Verilerin Çalınması Amaçlanır. Dolandırıcı

Phreaker

Telefon Ağları Üzerinde Çalışan, Telefon Sistemlerini Hackleyerek Bedava Görüşme Yapmaya Çalışan Kişilerdir.

Polymorphic Virüs

Her Bulaşmada Kendini Değiştirmektedir. Virüs Programları Bu Virüsü Önleyebilmek İçin Tahmin Yürütme Yoluna Dayalı Teknolojiler Kullanırlar. Yani Tehlikeli Sayılabilecek Virüslendendir.

Proxy Sunucu

Kullanıcılar Ve Diğer Sunucular Arasında Aracı Görevi Gören Ve Kullanıcı İsteklerini Doğrulayan Sunucu.

Ransomware

Verilerini Rehin Tutan, Kasıtlı Olarak Bilgisayardaki Dosyalara Erişmeyi Engellenen Kötü Amaçlı Bir Yazılım Biçimidir.

Rastgele Numara Üretici

Bilgisayarlar Çok Öngörülebilir Veriler Oluşturmak Üzere Tasarlanmıştır Ve Bu Nedenle İyi Şifreleme İçin Gerekli Olan Rastgele Sayılar Üretme Konusunda Çok İyi Değildir. Özel Bir Rastgele Sayı Üretici, Bu Görev İçin Özel Bir Mekanizmaya Sahip Olması Dolay

Reconnaissance (Recon)

"Passive Recon" Ve "Active Recon" Olarak İkiye Ayrılır. Türkçe'ye "Pasif Keşif" Ve "Aktif Keşif" Olarak Çevirilebilir. Hedef Sistemle İlgili Bilgi Toplama Süreçlerinin Tamamıdır. Hedefle Temasa Geçildiği Durumlarda Pasif Keşiften Aktif Keşife Geçiş Sağlan

Reklam (Adware)

Browser Ayarlarını Değiştirebilen Bu Virüs Türü Genellikle Karşınıza Bazı Reklamların Çıkmasını Sağlar. Eğer Anlayamadığınız Bir Şekilde Sürekli Reklama Maruz Kalıyorsanız Adware Virüsünden Şüphelenebilirsiniz.

Remote File Injection

Uzaktan Dosya Çalıştırma

Remote File Inclusion

Saldırganın Hedef Site Üzerinde Kendi Dosyasını Yükleyip Okuyabilmesine Olanak Tanıyan Bir Güvenlik Açığıdır.

Restore

Saldırı Ya Da Hata Sonrası Kaybedilen Verileri Kurtarma.

KELİME

Risk

DEFINITION

Siber Saldırı Anında Ortaya Çıkabilecek Olası Zararları Tanımlar.

Rootkit

Bilgisayara Bulaşan, Çalışan İşlemler Arasında Kendini Gizleyen, Kötü Niyetli Kişilere, Uzaktan Bilgisayarınızın Tam Hakimiyetini Sağlayan Tespit Edilmesi Oldukça Zor Olan Bilgisayar Programıdır.

Rootkit(Kök Kullanıcı Takımı)

Benzerlerinden Farklı Olarak Rootkit, İşletim Sisteminden Gizlenen Programları İşaret Eder. Hangi Sistemde Bulunuyorsa Burada Varlığını Gizleyecektir. Kullanım Amacı Bakımından Geçmişte Bilgileri Saklamak İçin Varlığını Sürdürse De Kötü Amaçlı Yazılan Çeş

Saldırı İmzası (Attack Signature)

Ağ Üzerinden Gelen Bilgi Paketlerini Bazı Modellere Göre Dikkatlice İnceleyerek Kötü Niyetli Aktiviteleri Haber Veren Bir Sistemdir.

Saldırı Tespiti Sistemi

Ids Olarak Kısaltılan Bu Sistemler, Bir Bilgisayar Ya Da Bağlı Kaynaklara İzinsiz Erişim Hâline Uyarı Verirler Ve Programlandıkları Diğer Eylemleri Gerçekleştirirler.

Sanal Özel Ağ

Vpn, Virtual Private Network (Sanal Özel Ağ) Teriminin Kısaltılmış Halidir Ve En Temel Anlamıyla İnternete Başka Bir Ip Adresi Üzerinden Bağlanmanızı Sağlayan Hizmettir. Vpn, Bağlantınızı Güvenli Hale Getirir Ve Herhangi Bir Ağa Bağlanırken Sizin Bağlan

Screenlogger(Ekran-Kayıt)

Fare Kullanılırken Ekran Üzerinde Bir Yere Tıkladığınızda Ekran Kaydı yapankötü amaçlı Yazılım Türüdür. Kaydettiği Alan Ya Bir Kısmı Ya Da Ekranın Tamamıdır. Bu Kayıtlar Sabit Bir Yere Gönderilir.<https://www.natro.com>

Secure Shell

Güvenli Veri İletişimi. Uzaktan Komut Çalıştırma Ve İki Ağa Bağlı Bilgisayarlar Arasındaki Diğer Güvenli Ağ Hizmetleri İçin Bir Şifreleme Ağ Protokolü

Sertifika (Certificate)

Güvenilir Bir Otorite Tarafından Özel Açıklama İle Belirli Bir Kalıp Ve İsim Altında Belirlenen Özelliklere Sahip Olunduğunu Bildirir.

Sflow

Yüksek Hızla Veri Transferi Yapan Ağlarda Durum Tanımsız(Stateless) Paket Örnekleme Protokoldür.

KELİME

Siem

DEFINITION

Security Information And Event Management.-Güvenlik Bilgileri Ve Etkinlik Yönetimi. Bir Siem'ın Birincil İşlevi, Çeşitli Veri Kaynaklarındaki Anormallikleri Toplamak, Normalleştirmek, İlişkilendirmek, Toplamak Ve Saptamaktır.

Siem(Security Information And Event Management)

Log Analizine Göre Daha İnce Detaylı Yapılandırma Ve Raporlama Seçenekleri Sunmasıdır.

Sıfıncı Gün Saldırıları

Henüz Siber Güvenlik Dünyası Tarafından Bilinmeyen, Uzmanların Keşfedemediği, Yayınlanmamış Açıklıklara Sıfıncı Gün (Zero Day) Açığı Adı Verilmektedir.

Siber

Bilgisayar Ağlarına Ait Olan", "İnternete Ait Olan", "Sanal Gerçeklik" Manalarına Gelmektedir.

Siber Aktivistler

Dünya Görüşleri Çerçevesinde Kötü Veya Uygunsuz Gördükleri Toplumsal Ya Da Politik Sorunları Dile Getirmek Amacı İle Kamu Ya Da Özel Sektör Siber Uzaylarına Saldırı Düzenleyen Şahıs Ya Da Gruplardır

Siber Casusluk

Sahiplerinin İzni Olmaksızın Gizli Bilgi Edinmek İçin Bilgi Teknolojisini Kullanma.

Siber Caydırıcılık

Sanal Ortamlarda Karşılaşılabilecek Tehdit Ve Tehlikelere Maruz Kalmamak İçin Saldırganlığı Önleme, Engelleme Ve Önlem Alma Girişimleri.

Siber Espiyonaj

Gizli Ve Kritik Bilgileri Siyasi Veya Ekonomik Sebepler Doğrultusunda Ele Geçirmek İçin Yürütülen Faaliyetlerin Bütünüdür.

Siber Korsan

Siber Korsanlık, Bazen Sosyal Medya Ortamlarında Sahte Birsosyal Medya Kampanyasıolarak Karşımıza Çıkarken, Bazen De Güvenilir Bir Yerden Geliyormuş İzlenimi Uyandıran Ve Zararlı Yazılımlar İçeren Bir Bağlantıya Tıklanması Ve Yüklenmesiyle, Bazen İse Sade

Siber Olay

Fiziksel Veya Mantıksal Siber Varlıkların Çeşitli Şekillerde Paydaş Olduğu Olaydır. Bilişim Ve Endüstriyel Kontrol Sistemlerinin Veya Bu Sistemler Tarafından İşlenen Bilgi Veya Herhangi Bir Verinin Gizlilik, Bütünlük Veya Erişilebilirliğinin İhlal Edilmesi

KELİME

Siber Ortam

DEFINITION

Tüm Dünyaya Ve Uzaya Yayılmış Durumda Bulunan Bilişim Sistemlerinden Ve Bunları Birbirine Bağlayan Ağlardan Oluşan Ortamı

Siber Savaş

Belirlenen Hedeflere Bilgisayar Ve Bilişim Teknolojileri Kullanılarak Yapılan Saldırılar Ve Ulusal Güvenliği Etkileyecek Şekilde Yapılan Bt Tabanlı Saldırılardır.

Siber Savunma

Siber Savunma Bilişim Sistemlerine Bağlı Olarak Çalışan Araç, Teçhizat, Sistem Ve Alt Yapılarını Oluşabilecek Siber Tehditlere, Saldırılara Karşı Korumak İçin Alınması Gereken Önlemler Dizisi Olarak Adlandırılabilir.

Siber Silah

Saldırı Yeteneğine Sahip Zararlı Yazılımların Hepsisi.

Siber Suç

Herhangi Bir Suçun Siber Ortamda İşlenme İmkânı Bulması Ve Bu Ortamda Gerçekleşen Fiilin Hukuka Aykırı Olarak Tanımlanabilmesi Durumunda Bu Siber Suç Olarak Sayılmaktadır. Siber Suçlar “Devlet Ve Kamu Düzenine Karşı İşlenen Siber Suçlar”, “Mal Varlığına K

Siber Terörizm

Siber Terörizmbelirli Bir Politik Ve Sosyal Amaca Ulaşabilmek İçin Bilgisayar Veya Bilgisayar Sistemlerinin Bireylere Ve Mallara Karşı Bir Hükümeti Veya Toplumunu Yıldırma, Baskı Altında Tutma Amacıyla Kullanılmasıdır.

Siber Uzay

Tüm Dünyaya Ve Uzaya Yayılmış Durumda Bulunan Bilişim Sistemlerinden Ve Bunları Birbirine Bağlayan Ağlardan Oluşan Veya Bağımsız Bilgi Sistemlerinden Oluşan Sayısal Ortam.

Siber Varlık

Klasik Bilişim Unsurlarının (Bilgisayar, Sunucu, Ağ Cihazları, Vb.) Yansıra, İnternet Bağlantılı Televizyondan, Araçlardaki Arızayı Servise Otomatik Bildiren Bileşenlere Kadar, Tüm Bu Cihazları Ve Yazılım, Donanım Bileşenlerini “Siber Varlık” Tanımı İçine

Side-Channel Attack

Bilgisayarlardan Farkında Olmadan Sızan Bilgilere Dayanan, Cryptanalytsis Teknikler (Kripto Analiz) (Şifreleme Yöntemi) Yardımıyla Gizli Bilgiyi Ortaya Çıkarmayı Amaçlayan Bir Saldırı Türüdür.

KELİME

Sistem Açığı

Sistemin Zayıf Noktası Anlamına Gelir. Sistemlere Girmek İçin Kullanılan Yazılım Ve Donanımlar, Karşıda Sürekli Bir Boşluk Arar. Genellikle Teknik Arıza Olan Durumlarda Ya Da Sistemin Yeni Keşfedilen Açıklara (Sıfırıncı Gün Açıkları - Zero Day Bugs) Karşı

Sistem Açığı (Bug)

Sistemin Zayıf Noktası Anlamına Gelir. Sistemlere Girmek İçin Kullanılan Yazılım Ve Donanımlar, Karşısında Sürekli Bir Boşluk Arar.

Siyah Şapkalı Hacker

Bilgisayar Korsanı Olarak Da Bilinir.Şahsî Bilgisayarlara Veya Çeşitli Kurumve Kuruluşlara Ait Bilgisayarlara Ve Ağlara İzinsiz Olarak Giriş Yapan Kişilerdirler, Sistemleri Kullanılmaz Hale Getirir Veya Gizli Bilgileri Çalarlar. Elektronik Veya Mekanik Ot

Sntp

Basit Ağ Yönetimi Protokolüüp Ağları Üzerinde Aygıtları Yönetmek İçin Bir İnternet Standart Protokol.

Sntp (Basit Ağ Yönetimi Protokolü)

İp Ağları Üzerinde Aygıtları Yönetmek İçin Bir İnternet Standart Protokol.

Soar

Çok Farklı Kaynaklardan Gönderilen Güvenlik Verilerinin Toplanarak Düzenlenmesini Standardizasyonunu Ve Otomasyonunu Sağlamak İçin Ortaya Konmuş Bir Sistemler Bütünüdür.

Software

Değişik Ve Çeşitli Görevler Yapma Amaçlı Tasarlanmış Elektronik Aygıtların Birbirleriyle Haberleşebilmesini Ve Uyumunu Sağlayarak Görevlerini Ya Da Kullanılabilirliklerini Geliştirmeye Yarayan Makine Komutlarıdır.

Solucan

Solucan, Kendini Kopyalayarak Diğer Bilgisayarlara Yayılan Bir Kötü Amaçlı Yazılım Çeşididir, Virüsün Bulaşmış Olduğu Bilgisayarda Bir Tünel Açabilir Ve Başka Birinin Uzaktan Bilgisayarınızın Denetimini Eline Geçirmesini Sağlayabilir.

Solucanı

İletişim Ağları Üzerinden Yayılma Kabiliyetine Sahiptir. Örneğin E-Posta Ekinde Gelir Ve Kopyalarını İletmek Üzere Kişi Listesini Kullanır. Böylece Hızla Yayılır.

Sosyal Medya

Tek Yönlü Bilgi Paylaşımından, Çift Taraflı Ve Eş Zamanlı Bilgi Paylaşımına Ulaşılmasını Sağlayan Medya Sistemidir. Ayrıca Sosyal Medya; Kişilerin İnternet Üzerinde Birbirleriyle Yaptığı Diyaloglar Ve Paylaşımın Bütünüdür.

KELİME

Sosyal Mühendis

DEFINITION

Eylemleri Gerçekleştirmeye Veya Gizli Bilgileri İfşa Etmeye Yönelik Olarak İnsanların Psikolojik Manipülasyonudur.

Sosyal Mühendislik

Sosyal Mühendislik, İnternette İnsanların Zaafiyetlerinden Faydalanarak Çeşitli İkna Ve Kandırma Yöntemleriyle İstenilen Bilgileri Elde Etmeye Çalışmaktır. İnsanların Karar Verme Süreçlerini Değiştirmeye Yönelik Teknikler İçerir.

Sosyal Mühendislik

Bilgi Güvenliği Bağlamında Sosyal Mühendislik, Eylemleri Gerçekleştirmeye Veya Gizli Bilgileri İfşa Etmeye Yönelik Olarak İnsanların Psikolojik Manipülasyonudur.

Spam Mail

Bir Kuruma Ya Da Kişiye Toplu Olarak Yollanan Virüslü Maildir.

Spearphishing

Hedef Odaklı Oltalama Olarak Adlandırılan Bu Saldırıda, Belirli Bir Kuruluş İçindeki Kişileri Hedef Alarak Kritik Bilgileri Paylaşmaları Konusunda Kandırmaya Yönelik E-Postalar Gönderilir.

Spectre

Farklı Uygulamalar Arasındaki İzolasyon Mekanizmasını Kırarak Uygulamaların Diğer Uygulamalardan Bilgi Sızdırmasına Neden

Spoofing

Güvenli Bir Sisteme Yetkisiz Erişim Sağlamak İçin Sahte E-Postaların Gönderilmesidir.

Spyware

Spyware, Bilgisayar Kullanıcısının Kendi Rızası Ve/Veya Bilgisi Dışında Veri Toplayan Casus Yazılımlardır. Daha Genel Veya Farklı Anlamları Da Olan "Malware" Ve "Adware" Gibi Adlar Da "Spyware" Yerine Kullanılabilmektedir.Casus Yazılımlar, Kişisel Bilgi G

Sql Injection

Web Sitesine Sql Kodlarının Enjekte Edilmesiyle Veritabanından Çeşitli Bilgilerin Elde Edilebildiği Açık Türüdür.

Ssh (Secure Shell)

Güvenli Veri İletişimi. Uzaktan Komut Çalıştırma Ve İki Ağa Bağlı Bilgisayarlar Arasındaki Diğer Güvenli Ağ Hizmetleri İçin Bir Şifreleme Ağ Protokolü.

Steganography

Yunanca'Dan Gelmektedir. Fotoğrafların, Videoların Ve Ses Dosyalarının Ardına Mesaj Saklama Tekniğidir.

KELİME

Stukxnet

DEFINITION

Solucan Yazılımdır. Silah Seviyesinde Bir Yazılım Olarak Değerlendirilmesidir. Abd Ve İsrail'In İran Nükleer Çalışmalarını Sekteye Uğratmak İçin Geliştirilmiştir. Silah Olarak Adlandırılması İse Sanal Dünyada Yaşayıp Aktif Hale Geldiğinde Gerçek Dünyada K

Sunucu(Server)

Bir Ağ Üzerinde, Program Veya Bilgiyi, Farklı Kullanıcılara, Sistemlere Paylaştıran, Dağıtan Donanım Veya Yazılıma Verilen İsimdir.

Surface Web

World Wide Web, Milyonlarca İnsanın İnternette Etkileşime Girebilen Bir Platform Olarak Tasarlanmıştır. Web Dünyasında Halka En Açık Olan Alan Surface Web Olarak Tanımlanır. Bu Alan Google, Yahoo, Bing Gibi Arama Motorlarını Kullanarak Yani Özel Bir Taray

Süper Darbe

Bilgisayar Sistemlerindeki Arızalar İle Sistemin Kilitlenmesi Durumunda Güvenlik Kontrollerinin Aşılarak Sistemin Düzeltilmesi İçin Geliştirilmiş Programlardır. Bu Durum Kötüye Kullanıldığında Güvenlik Devre Dışı Bırakılmaktadır.

Şifre

Bilgisayara Veya İçerdiği Bilgiye Erişim İçin Kullanılan Ve Bilgisayar Tarafından Tanınan Özel Karakter Dizisi.

Şifre Çözme(Decryption)

Şifrelenmiş Bilgiyi Tekrar Eski Haline Getirme İşlemidir.

Şifre Koklama>Password Sniffing)

Bilgi Almak İçin Bir Ağdaki Trafiği İzleyerek Bir Şifre Bulmak İçin Kullanılan Bir Yöntem.

Şifreleme

İnternet Gibi Güvenli Olmayan Ortamlarda Gönderilecek Veri Paketlerinin Kodlanması İçin Bir Yöntem.

Şifreleme (Encryption)

Verilerin Çalınmasını Önlemek Amacıyla Yapılan Şifreleme İşlemidir.

Tersine Mühendislik

Mevcut Bir Sistem, Cihaz Veya Nesnenin Üretim Aşamalarını Bulunduracak Şekilde Tasarım Ve İşlevsel Özelliklerinin Tahlil Edilmesinetersine Mühendislik (Reverse Engineering, Re)Denir. Bir Başka Değişle Mühendislik Sırlarının Keşfedilmesidir.Hızlı Yüzey İle

Threat Actor

Siber Saldırı Oluşturan Ya Da Kazaya Sebep Olan Kişi.

KELİME

Tor

DEFINITION

Tor, Teknoloji Severlerin Gizliliğini Korumak Amacıyla Kullanılan Ve Çoklu Şifreleme Katmanlarına Atıf Yapan "The Onion Router"ın Kısaltmasıdır.

Tor Browser

İnternette Anonim Olarak Gezmenizi Sağlayan Tarayıcı.

Tracking Cookie

Cookie Yani Çerezler İnternette Gezdiğiniz Siteler Vb. İle İlgili Veri Barındıran Basit Metin Dosyalarıdır Ve Bilgisayarınızda Çerez (Cookies) Klasöründe Bulunurlar. Pek Çok Site De Ziyaretçileri Hakkında Bilgi Almak İçin Çerezleri Kullanırlar. Örneğin Bi

Truva Atı

Bilgisayar Yazılım Terimi Olarak Truva Atı Zararlı Kod İçeren Yazılım Demektir. Terim Klasik Truva Atı Efsaneinden Türetilmiştir. Kullanıcıya Faydalı Program Gibi Görünen Yazılım Çalıştırıldığında Bilgilerinize Veya Diğer Programlarınıza Zarar Verir.Truv

Tuzak Kapanları(Trap Doors)

Tuzak Kapısı Ya Da Arka Kapı, Bir Sistemin Yazılımını Yapan Kişi Tarafından, Yazılımın İçine Gizli Bir Şekilde Yerleştirilen Bir Virüs Yazılımıdır. Bu Programın Çalıştığı Bilgisayara Virüsü Yerleştiren Kişinin, Uzaktan Erişim Yöntemiyle Sistem Koruyucular

Ulusal Siber Ortam

Kamu Bilişim Sistemleri İle Gerçek Ve Tüzel Kişilere Ait Bilişim Sistemlerinden Oluşan Ortamı

Url Spoofing

Bir Web Sitesine Ait Url'in Tıklandığında Farklı Bir Adrese Yönlendirilerek Hedef Kişinin kandırılması Durumdur.

Uzak Erişim

Bir Bilgisayara Veya Cihaza Uzaktan Bağlanma Yeteneği.

Uzak Erişim (Remote Access)

Bir Bilgisayara Veya Cihaza Uzaktan Bağlanma Yeteneği.

Uzak Erişim (Remote Access)

Bir Bilgisayara Veya Cihaza Uzaktan Bağlanma Yeteneği.

Verbis

Kişisel Verileri İşleyen Gerçek Ve Tüzel Kişilerin, Kişisel Veri İşlemeye Başlamadan Önce Kaydolmaları Gereken Ve İşlemekte Oldukları Kişisel Verilerle İlgili Kategorik Bazda Bilgi Girişi Yapacakları Bir Kayıt Sistemidir.

KELİME

Veri Bütünlüğü (Data Integrity)

DEFINITION

Verinin Ağ İçindeki Aktarımı Sırasında Değişikliğe Uğramadığı Ve Zarar Görmediğini Garanti Etme İşlemidir.

Veri Gizliliği (Data Confidentiality)

Verinin Sadece Veriye Ulaşma Yetkisi Olanlara Gönderilmesinin Garanti Edilmesidir.

Veri Tabanı Sunucu

Veri Tabanı Hizmetleri Vermek İçin Oluşturulan Sunuculardır .

Virüs

Yayılmadan Önce Bilgisayardaki Bilgileri Bozmayı,Silmeyi Veya Değiştirmeyi Amaçlayan Bir Tür Kötü Amaçlı Yazılımdır.

Vm

Vulnerability Management- Güvenlik Açığı Yönetimi, Ancak Aynı Zamanda Bir Diğer Potansiyel Kullanım Olarak Sanal Makine

Vpn

Özel Bir Ağa Bağlanmak İçin Yapılandırılmış Ağ.

Vpn Tüneli

Güvensiz Ağ Ortamında İki Nokta Arasındaki Güvenli (Genellikle Şifreli) Bağlantı.

Vpn- Tüneli

Güvensiz Ağ Ortamında İki Nokta Arasındaki Güvenli (Genellikle Şifreli) Bağlantı.

Vulnerability

Güvenlik Açığı

Wannacry Virüsü

Windows İşletim Sistemi Kullanan Kullanıcıların Bilgisayarlarına Bulaşan Ve Windows İçindeki Bazı Açıklardan Yararlanarak Bilgisayarları Neredeyse Devre Dışı Bırakan Virüs, Kısa Süre İçinde Kontrolü Ele Geçiriyor. Format Atmanın Bile İşe Yaramadığı Wanacr

Web Server

Hosting İşlemini İnternet Protokolü Üzerinden Sunan Sunucudur.

Worm

Bulaşmayı Diğer Bağlı Bilgisayarlara Yaymak İçin Kendini Çoğaltabilecek Kötü Amaçlı Bir Yazılımdır.

KELİME

Xss (Cross Site Scripting)

DEFINITION

Güvenilir Web Sitelerine Zararlı Scriptler Enjekte Edilmesini Sağlayan Bir Saldırı Türüdür.

Yama Ve Güncelleme

Yazılım Üreticileri Bir Açık Bulunması Sonrası Bu Açığı, Tıpkı Kıyafetteki Bir Yırtığı Kapatır Gibi Kapatıyorlar. Bunun İçin Hazırlanan Açık Kapatıcı Programa, Tekstildekine Benzer Şekilde Yama (Patch) Adı Veriliyor. Sistemle İlgili Tüm Yeniliklerin Adı İ

Yazılım

Program Da Denilen, Bir Bilgisayarı Belirli İşlevleri Yerine Getirmek Üzere Yöneten, Bilgisayara Ne Yapacağını Söyleyen, Kodlanmış Komutlar Dizisi.

Yazılım Korsanı

Yazılım Korsanları Bilgisayar Programlarının Kopya Korumalarını Kırarak, Bu Programları İzinsiz Olarak Dağıtımına Olanak Sağlayıp Para Kazanırlar. Piyasaya Korsan Oyun Ve Program Cd'lerini Yazılım Korsanları Çıkarır.

Yedekleme

Bilgi Teknolojisinde, Yedekleme Veya Veri Yedekleme, Başka Bir Yerde Alınan Ve Depolanan Bilgisayar Verilerinin Bir Kopyasıdır, Böylece Veri Kaybı Olayından Sonra Orijinali Geri Yüklemek İçin Kullanılabilir.

Yemleme Tekniği

Yemleme, Yasa Dışı Yollarla Bir Kişinin Şifresini Veya Kredi Kartı Ayrıntılarını Öğrenme. Bir Kişinin Sahipliğindeki Değerleri, Yasadışı Aldatma Yolları İle Ele Geçirme Veya Değerlerine Zarar Verme Eylemi.

Yemleme(Phishing)

Yasadışı Yollarla Kullanıcıların Herhangi Bir Sistem İçin Kullandıkları Kullanıcı Adı, Şifre, Kimlik Bilgileri, Kredi Kartı Ayrıntıları Gibi Bilgilerin Ele Geçirilmesidir.

Yetki (Authorization)

Kullanıcı Ya Da Kullanıcılara Sisteme, Programa Ve Ağa Erişim Hakkının Verilmesidir.

Yetkilendirme

Sistemde Kayıtlı Bulunan Kimliklerin, Yetki Seviyelerinin Belirlenmesi Ve Veriye Ulaşımında Belirli Yetkiler Konulmasıdır.

Yığın E - Posta (Spam Mail)

İstenmeyen E- Postaların Tümüne Bu Ad Veriliyor. Bunlarla En Çok Reklamlar Ve Virüsler Gönderiliyor. Genelde Yasa Dışı Ürünlerin Reklamı Yapılırken, Son Zamanlarda Kimlik Hırsızlığı Sebebiyle Oltalama Saldırılarında Da Sık Kullanılmaya Başlandı.

KELİME

Yığın E-Posta (Spam Mail)

DEFINITION

İstenmeyen E-Postaların Tümüne Bu Ad Veriliyor. Bunlarla En Çok Reklamlar Ve Virüsler Gönderiliyor. Genelde Yasa Dışı (İlaç, Site Vb.) Ürünlerin Reklamı Yapılırken, Son Zamanlarda Kimlik Hırsızlığı Sebebiyle Ortalama Saldırılarında Da Sık Kullanılmaya Baş

Yönlendirici (Router)

Bir Bilgisayar Ağının Uygun Bölümlerine Veri Paketlerini İleten Bir Cihaz.

Yönlendirici (Router)

Bir Bilgisayar Ağının Uygun Bölümlerine Veri Paketlerini İleten Bir Cihaz.

Zafiyet

Bir Sistemin Dizayn Ve Üretiminden Kaynaklanan Hatalar Olabileceği Gibi, Yazılımın Algoritmik Mantık Hatasından Da Kaynaklanabilecek Ve İstismara Açık Noktalarına Denir.Zafiyet, Donanımsal Ve Yazılımsal Nedenlerden Kaynaklı Olabileceği Gibi İnsan Faktör

Zararlı Reklam Yazılımı

Bilgisayarınızda Reklamları Otomatik Gösteren Yazılımdır.

Zararlı Yazılım

Teknoloji İle İlgili Tehditlerin Büyük Bölümü Bu Grup Altında Toplanır. Kullanıcının İzni Olmaksızın Bilgisayara Ya Da Cihaza Sızan Ve Zarar Verme Amacına Yönelik Hareket Eden Yazılımları Kapsar.

Zararlı Yazılımlar (Malware)

En Genel İfade İle Bilgisayar Sistemlerini Kötü Amaçlı Kullanmak İçin Sistem Bilgilerine Erişim Sağlamaya Yarayan Ya Da Bilgisayar Sistemlerine Ciddi Zararlar Veren Kötücül Bilgisayar Programlarıdır

Zero Day

Yeni Ve Daha Önce Karşılaşılmamış Bir Zararlı Yazılıma Düzeltme Yaması Bulunana Kadar Verilen İsim.

Zeroday Güvenlik Açığı

Bir Yazılım Üzerindeki Açığın Fark Edilmesi Ve Bu Açığın Ortaya Çıkmasından Sonra İnternet Korsanlarının Açık Olabilmesi Muhtemel Platformlara Saldırıları Düzenlemesidir.

Zombi

Üçüncü Tarafların Denetimini Ele Geçirdiği Bilgisayarları Tanımlamakta Kullanılan Bir Terimdir.

Zorunlu Erişim Kontrolü

Erişim Haklarını Sistem Belirler Ve Kullanıcı Bunları Değiştirmez. İşletim Sistemi Zorunlu Erişim Kontrollerini Kendi Yürütür