TEHDİTLER, GÜVENLİK AÇIKLARI VE SALDIRILAR

Ankara Üniversitesi

Bölüm Tanıtımı

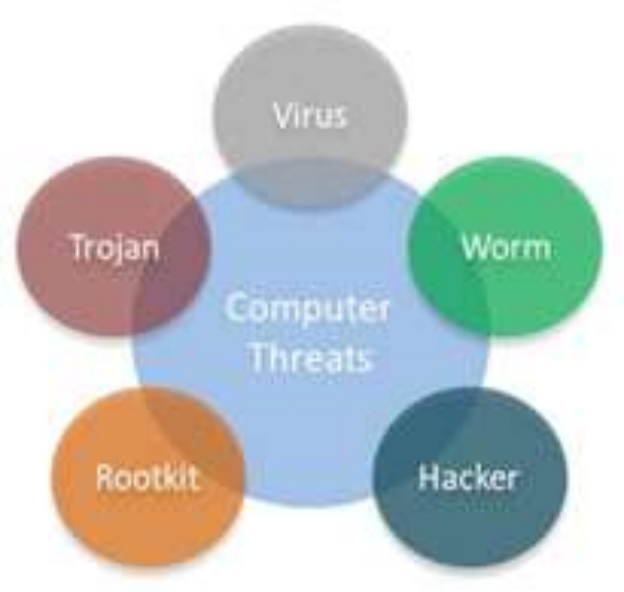
- Bu bölümde
  - siber tehditler
  - güvenlik riskleri
  - güvenlik açıkları
  - saldırılar

ayrıntılı olarak ele alınmıştır.

- Ayrıca her bir saldırı türü için öneriler, önlemler ve farkındalık konuları da tartışılacaktır.

1.Tehditler

- Tehdit, verilere zarar vermek, bozmak veya çalmak için bilgisayar ağlarına, başka bir kişinin veya kuruluşun ağına yetkisiz erişim sağlayan kötü niyetli bir aktördür.



Virüsler

- Bilgisayar virüsü, kullanıcının izni veya bilgisi dışında bilgisayarın çalışma şeklini değiştiren ve kendisini diğer dosyalarda gizlemeye çalışan bir tür bilgisayar programıdır.
- Bu programlar tek başlarına çalışabilseler de genellikle bilgisayardaki diğer programların içine yuvalanarak çalışırlar. Virüsler, çalışmayı başardıktan sonra kendilerini diğer dosyalara kopyalamaya çalışırlar. Virüslerin aktif olabilmeleri için "çalıştırılmaları" gerekir.
- Bulaşıcı dosyalar başlangıçta yalnızca "program" dosyalarıydı, bu nedenle genellikle ".exe, .com, .pif" uzantılarına sahiptirler.
- Bununla birlikte, yazılım teknolojilerinin ilerlemesi, "yürütülebilir" dosya türlerinin artması ve işletim sistemlerinin gelişmesiyle birlikte, potansiyel olarak tehlikeli dosya türleri de artmıştır.

Bilgisayar Solucanları

- Solucanlar, daha karmaşık bir yapıya sahip kötü amaçlı yazılımlardır. Genellikle e-posta ekleri, çeşitli web siteleri ve ağ üzerinden paylaşılan dosyalar kullanılarak yayılırlar.
- Solucanlar bir sistemi ele geçirdiklerinde, kullanıcının başka bir işlem yapmasına gerek kalmadan, kullanıcının veri kaynaklarını (e-posta adres listesi gibi) kullanarak kaynak dosyalarını hızlı bir şekilde diğer kullanıcılara ulaştırmaya çalışırlar ve bu sayede kendilerini çok sayıda çoğaltabilirler.
- Virüslere benzer işlevleri vardır, ancak programlara bulaşmak için kullanıcı tarafından çalıştırılan programlar değildirler.
- Solucanlara karşı korunmak için ideal çözüm, bilgisayarı işletim sistemlerinin en son sürümü ile kurmak, güncellemeleri takip edip gerçekleştirmek ve kişisel bir güvenlik duvarı kullanarak dış saldırılara karşı kapıları kapatmaktır.

Truva Atları

- Truva atı adı verilen kötü amaçlı yazılımlar, kullanıcılara yararlı bir program olarak kendilerini sunar ve indirilmelerine neden olur. Truva atları, yararlı gibi görünen ancak aslında yararlı olmayan kötü amaçlı yazılımlardır. Eklendikleri program dosyasının çalıştırılması ve kopyalarının kullanıcılar tarafından dağıtılması sonucunda aktif hale gelirler.
- Truva atları temel olarak iki farklı dosya içerir:
  - Kullanıcıya gönderilen dosya
  - Sistemde çalıştırılan dosya
- Saldırganlar, kurbanın sisteminden şifreler, kredi kartı bilgileri ve diğer önemli belgeler gibi kişisel bilgileri alabilir.
- Truva atı kötü amaçlı yazılımı çok çeşitli olduğundan, yalnızca derinlemesine bir savunma stratejisi kullanılarak önlenebilir. Ayrıca sistemlerin güvenlik açıklarını azaltmak için kullanıcıların sadece işletim sistemlerini değil, kullandıkları tüm yazılımları düzenli olarak güncellemeleri gerekiyor.

Rootkitler

- Rootkit, bilgisayar korsanlarının kurban cihaza girmesine ve onu kontrol etmesine izin vermek için oluşturulmuş bir tür kötü amaçlı yazılımdır.
- Rootkit'lerin çoğu işletim sistemlerini ve yazılımları etkiler.
- Rootkit'ler varlıklarını gizleme konusunda uzmandırlar ve gizli kaldıkları sürece aktif kalırlar.
- Rootkit'in gerçekte hangi dosyaları değiştirdiğini, hangi modülün çekirdeğe yüklendiğini, hangi ağ servisini dinleyeceğini ve uygun komutla harekete geçeceğini belirlemek zordur.

Bilgisayar Korsanları ve Avcılar

- Bilgisayar korsanları ve avcılar arasındaki temel fark, bilgisayar korsanlarının kendi çıkarları için başkalarını feda etmeleridir.
- Bu çevrimiçi bilgisayar korsanları ve avcılar, bilgisayarlara kötü amaçlı dosyalar göndermek ve güvenliği tehlikeye atmak için genellikle kimlik avı dolandırıcılıkları, spam ve diğer teknikleri kullanır.
- Bazen çalışanlar ve kullanıcılar, güvenli bilgisayar uygulamalarını takip etmeyerek ve uygulamayarak kuruluşları için tehdit oluşturmaktadır.
- Bu nedenle, çalışanların siber güvenlik bilgisi eksikliği, bir kuruluşun ağ güvenliği için en büyük risklerden birini oluşturabilir.
- Bilgisayar korsanları, güvenlik duvarı ile koruma yoksa doğrudan bilgisayara ve özel bilgilere erişmeye çalışabilir. Bu nedenle, bu tür kötü niyetli faaliyetlere kurban gitmemek için kaliteli güvenlik duvarı çözümleri ve antivirüs koruması kullanılmalıdır.

2. Riskler

- Dijital çağın ihtiyaçları doğrultusunda kurum ve kuruluşlar verilerini farklı veri merkezlerinde ve bulut ortamlarında dağıtık bir yapıda barındırmaktadır.
- Siber saldırganlar da bilgisayar tabanlı sistemlerden daha fazla fayda sağlamak için saldırı yöntemlerini geliştiriyorlar.
- Veri hırsızlığından fidye yazılım saldırılarına kadar geniş bir yelpazede değerlendirilen bu faaliyetlerin tamamına "Siber Risk" adı verilmektedir.
- En yaygın olarak bilinen siber risk türleri aşağıdakilerdir:
  - Spyware (casus yazılım)
  - Scareware (korkuluk)
  - Joke programs (şaka programları)
  - Ransomware (fidye yazılımları)
  - Hacking tools (bilgisayar korsanlığı araçları)
  - Remote access (uzaktan erişim)

Casus Yazılımlar

- Bilgisayar kullanıcısının izni olmadan veri toplayan yazılımlardır.
- Casus yazılımlar, kullanıcının klavyede bastığı tuşları kaydetme, görüntülenen web sayfalarını takip etme, internette yapılan aramaları izleme gibi işlemler yaparak kişisel bilgilerin gizliliğini ihlal ederler.
- Casus yazılımlar, açıkça kullanıcıya yasa dışı ve doğrudan zarar verecek şekilde tasarlanmadığı ve kullanıcının rızası ile bilgisayara yüklendiği için genellikle virüslerden ayrılır. Ayrıca, virüsler gibi, casus yazılımlar da hiçbir şekilde kendisini bir bilgisayardan diğerine kopyalamaz.
- Bu casus yazılımlardan korunmak için ara sitelerden dosya indirmemek, güvenilmeyen kaynakları cihazlara bağlamamak ve bilinmeyen e-postaları açmamak gibi güvenlik önlemlerinin alınması gerekmektedir.

Korkuluk

- Rogueware olarak da bilinen malware sınıfında yer alan kötü amaçlı bilgisayar yazılımlarına verilen isimdir. Genellikle gerçekçi olmayan senaryolarla kullanıcıları korkutur ve onları yazılımı satın almaya teşvik eder
- Scareware yazılımlarının asıl amacı sahibine para kazandırmaktır. Bir web sitesine giriş yaptığınızda bilgisayarda virüs olmamasına rağmen "bilgisayarınızda x tehdit algılandı" şeklinde bir açılır pencere çıkar.
- Buradaki asıl amaç kullanıcıları korkutmak ve bu korkuyla yazılımı satın almaya zorlamaktır
- Eğer bilgisayarda Scareware yazılımı kurulu ise hemen paniğe kapılmaya gerek yoktur. Çünkü genellikle Scareware yazılımları bilgisayarın Program Ekle/Kaldır menüsüne giriş yapılarak bulunup silinebilmektedir.

Şaka Programları

- Bir şaka programı, genellikle hiçbir kötü amacı olmayan yaygın bir programdır. Bu programların temel amacı kullanıcıyı kızdırmak veya eğlendirmektir .
- Bununla birlikte, bazı kurbanlar paniğe kapılabilir ve yanlışlıkla sürücü biçimlendirme veya dosya silme gibi verilerin zarar görmesine neden olabilecek faaliyetlerde bulunabilir.
- Bazen, bu programlar fare veya yazıcı gibi bazı aygıtları geçici olarak devre dışı bırakabilir.
- Şaka programları çoğu zaman masum gibi görünse de bazen bir kurum veya kuruluş için maliyetli olabiliyor.

Fidye Yazılımı

- Fidye yazılımı, önemli dosyalara, belgelere, uygulamalara, işletim sistemlerine, ağlara veya sunuculara erişilemez hale getiren en büyük siber risk türlerinden biridir.
- Fidye yazılımı bilgisayara bulaştıktan sonra, siber suçlulardan genellikle kripto para cinsinden bir fidye ödemeleri istenir. Karşılığında veri sözü veriliyor.
- Sahte bir ek veya bağlantı ile insanları kandırıyorlar. Kötü amaçlı dosyalar genellikle sıradan belgeler (sipariş onayları, makbuzlar, faturalar, bildirimler) kılığına girer ve saygın bir şirket veya kurum tarafından gönderilmiş gibi görünür.

Bilgisayar korsanlığı araçları

- Bilgisayar korsanlığı aracı, bilgisayar korsanına yardımcı olmak için tasarlanmış bir program veya yardımcı programdır
- Bilgisayar korsanlığı araçları, sistemlere sızmak için tasarlanmış farklı yeteneklere sahiptir. Örneğin Hacktool:Win32/Keygen, en iyi bilinen bilgisayar korsanlığı araçlarından biridir ve çeşitli yazılımlar için sahte aktivasyon anahtarları veya lisansları oluşturabilen sahte bir aracın kod adıdır.
- Birçok bilgisayar korsanlığı aracı, solucanlar, virüsler ve Truva atları eklemek için bir bilgisayara yetkisiz erişim elde etmek için yaygın olarak kullanılır.

Uzaktan erişim

- Uzaktan erişim, bulunduğunuz yerden bağımsız olarak bilgisayarınızı internet üzerinden bağlayıp yönetmenizi sağlayan, özel protokoller üzerinden çalışan bir uygulamadır.
- Uzaktan saldırıların ana nedenleri, verileri yasa dışı olarak görüntülemek veya çalmak; virüsleri veya diğer kötü amaçlı yazılımları başka bir bilgisayara, ağa veya sisteme sokmak; ve hedeflenen bilgisayara veya ağa zarar verir.
- Uzaktan erişim saldırılarına karşı korunmak için daha eski ve daha az güvenli protokollere sahip VPN'lerden kaçınılmalıdır.
- Aynı zamanda, herhangi bir cihazın uzaktan yönetilebilmesi için en az iki güvenlik katmanı uygulanmalı ve koruma için antivirüs ve kötü amaçlı yazılımdan koruma programları kurulmalı ve güncellenmelidir.

3. Güvenlik Açıkları

- Güvenlik açığı, bir ürün veya sistemdeki, bir saldırganın söz konusu ürün veya sistemin bütünlüğünü, kullanılabilirliğini veya gizliliğini tehlikeye atmasına izin verebilecek bir zayıflıktır. Güvenlik açığı türleri aşağıda listelenmiştir:
  - Yazılım açıkları
  - Güvenlik duvarı açıkları
  - TP/IP güvenlik açıkları
  - Kablosuz ağ güvenlik açıkları
  - İşletim sistemi güvenlik açıkları
  - Web sunucusu güvenlik açıkları

3. Güvenlik Açıkları

1.Yazılım açıkları

- Yazılım güvenlik açıkları, uygulamalarda hatalar veya hatalar olduğunda ortaya çıkar. Saldırganlar, hatalı yazılımları sisteme saldırmak için bu kusurları kullanma fırsatı olarak görürler. Yazılım güvenlik açıklarından kaynaklanan saldırılara arabellek taşması ve yarış koşulları örnek olarak verilebilir.

2.Güvenlik duvarı açıkları

- Güvenlik duvarları, ağları saldırılardan koruyan yazılım ve donanım sistemleridir. Güvenlik duvarı güvenlik duvarı, güvenlik duvarının koruması beklenen güvenilir ağa saldırmak için kullanılabilen güvenlik duvarı tasarımı, uygulaması veya yapılandırması sırasında yapılan bir hata, zayıflık veya geçersiz varsayımdır.

3. Güvenlik Açıkları

- **3. TCP/IP güvenlik açıkları**
- Bu güvenlik açıkları, bir ağın çeşitli katmanlarına aittir. Bu protokoller, güvenli olmayan bir ağda istenen özelliklerden yoksun olabilir. ARP saldırıları ve Parçalanma saldırıları, TCP/IP zafiyetlerinden kaynaklanan saldırılara örnek olarak verilebilir.

- **4. Kablosuz ağ güvenlik açıkları**
- Kablosuz LAN'lar, kablolu LAN'ları rahatsız eden benzer protokol tabanlı saldırılara sahiptir. Güvenli olmayan kablosuz erişim noktaları, bir saldırgana kişisel veya şirket ağında bir yol sundukları için tehdit oluşturabilir. Bu güvenlik açıklarına örnek olarak SSID sorunları ve WEP sorunları verilebilir.

3. Güvenlik Açıkları

- **5. İşletim sistemi güvenlik açıkları**
- Windows, macOS ve Unix gibi işletim sistemlerindeki güvenlik açıklarıdır. Üzerinde çalışan uygulamaların güvenliği, işletim sisteminin güvenliğine bağlıdır. Sistem yöneticisinin en ufak bir ihmali, işletim sistemlerini savunmasız hale getirebilir.

- **6. Web sunucusu güvenlik açıkları**
- Bu güvenlik açıkları, tasarım ve mühendislik hatalarından veya yanlış uygulamadan kaynaklanır. Web Sunucusu güvenlik açıklarının neden olduğu saldırılara örnek olarak koklama ve yanıltma saldırıları verilebilir.

Güvenlik Açığı Tarama

- Saldırıların birçoğu, hedeflenen sistemlerin güvenlik açıklarından faydalanarak gerçekleştirilmektedir. Bu yüzden, bilgi güvenliği profesyonelleri tarafından sıklıkla kullanılan bir kavram olan "vulnerability scanning" ile güvenlik açıklarının belirlenmesi büyük önem taşımaktadır.

- Vulnerability scanning, bilgisayar sistemlerindeki güvenlik açıklarını belirlemek ve bunları önlemek için kullanılan bir tekniktir. Bu teknik, güvenlik açıklarını tespit etmek için bir dizi test ve analiz yöntemi kullanır. Bu testler, ağ taramaları, sistem ve uygulama açıklarını tespit etmek için manuel ve otomatik testler gibi çeşitli yöntemleri içerir.

Güvenlik Açığı Taraması Nasıl Yapılır?

- Güvenlik açığı taraması yapmak, sisteminizdeki veya ağınızdaki olası güvenlik zayıflıklarını belirlemede önemli bir adımdır. Güvenlik açığı taraması gerçekleştirmek için temel adımlar şunlardır:
- **Taramanın kapsamını belirleyin:** Hangi sistemlerin veya ağ bölümlerinin taranacağını belirleyin.
- **Bir güvenlik açığı tarayıcısı seçin:** Birçok ticari ve açık kaynaklı güvenlik açığı tarayıcısı mevcuttur, gereksinimlerinize ve bütçenize uygun olanı seçin.
- **Tarayıcıyı yapılandırın:** Tarama sıklığı, gerçekleştirilecek tarama türü ve tarama derinliği dahil olmak üzere tarayıcıyı ihtiyaçlarınıza göre yapılandırın.

Güvenlik Açığı Taraması Nasıl Yapılır?

- Güvenlik açığı taraması gerçekleştirmek için temel adımlar şunlardır:
- **Taramayı çalıştırın:** Taramayı başlatın ve tamamlanmasını bekleyin. Bu, sisteminizin veya ağınızın boyutuna ve karmaşıklığına bağlı olarak birkaç dakikadan birkaç saate kadar sürebilir.
- **Sonuçları analiz edin:** Tarama tamamlandığında, güvenlik açıklarını belirlemek için sonuçları analiz edin, bunları önem derecesine göre sınıflandırın ve düzeltme için öncelik sırasına koyun.
- **Güvenlik açıklarını giderin:** Belirlenen güvenlik açıklarını düzeltmek için yazılım yamaları uygulayarak, ayarları yeniden yapılandırarak veya ek güvenlik önlemleri uygulayarak gerekli adımları atın.
- **Taramayı tekrarlayın:** Sisteminizin güvenli ve güncel kalmasını sağlamak için düzenli güvenlik açığı taramaları gerçekleştirin.

Güvenlik Açığı Tarama Araçları

1. Netsparker

- Netsparker, web uygulamalarındaki güvenlik açıklarını belirlemek için tasarlanmış bir web uygulaması güvenlik tarayıcısıdır.
- Web sitelerini SQL enjeksiyonu, siteler arası komut dosyası çalıştırma ve diğer güvenlik açıkları için tarayabilen güçlü bir araçtır.
- Netsparker'ın temel özelliklerinden biri, web uygulamalarını doğru ve verimli bir şekilde tarayabilmesidir. İmza tabanlı algılamaya dayanan diğer web uygulaması tarayıcılarının aksine Netsparker, uygulamanın kaynak kodunu ve davranışını analiz ederek güvenlik açıklarını algılayabilen ileri teknoloji kullanır.

Güvenlik Açığı Tarama Araçları

2. Acunetix

- Acunetix, güvenlik uzmanları tarafından web uygulamalarındaki potansiyel güvenlik tehditlerini tespit etmek ve azaltmak için kullanılan bir web güvenlik açığı tarayıcısıdır.
- İlk olarak 2005 yılında Malta merkezli bir şirket olan Acunetix Ltd tarafından piyasaya sürüldü ve o zamandan beri siber güvenlik endüstrisinde popüler bir araç haline geldi.
- Acunetix, hassas verilere yetkisiz erişim elde etmek veya SQL enjeksiyonu, siteler arası komut dosyası çalıştırma (XSS) ve arabellek taşması saldırıları gibi saldırıları başlatmak için saldırganlar tarafından istismar edilebilecek potansiyel güvenlik açıklarını belirlemeye yardımcı olur.
- Acunetix'in en önemli avantajlarından biri hızı ve doğruluğudur.

Güvenlik Açığı Tarama Araçları

3. Intruder

- Sızma testi aracı olarak da bilinen davetsiz misafir aracı, harici bir kaynaktan gelen bir saldırıyı simüle ederek bir bilgisayar sisteminin, ağının veya uygulamasının güvenliğini test etmek için tasarlanmış bir yazılım programıdır.
- Bu aracın amacı, güvenlik önlemlerindeki zayıflıkları belirlemek ve bunları iyileştirmek için öneriler sunmaktır.
- Bu araçlar, kaba kuvvet saldırıları, hizmet reddi saldırıları ve SQL enjeksiyon saldırıları dahil olmak üzere çeşitli saldırı türlerini simüle eder.
- Davetsiz misafir araçları, tipik olarak, herhangi bir zayıflığı veya güvenlik açığını belirlemek amacıyla bir hedef sisteme veya uygulamaya bir dizi istek göndererek çalışır.

Güvenlik Açığı Tarama Araçları

4. SolarWinds

- SUNBURST veya Soorigate olarak da bilinen SolarWinds saldırı aracı, SolarWinds Orion ağ izleme yazılımını hedeflemek için tasarlanmış oldukça gelişmiş bir kötü amaçlı yazılım parçasıydı.
- Kötü amaçlı yazılım, yüklendikten sonra bir süre uykuda kalacak ve tespit edilmesini zorlaştıracak şekilde tasarlandı. Ancak etkinleştirildiğinde, kurbanın ağı hakkında bilgi toplamaya ve saldırganın komuta ve kontrol sunucusuna geri göndermeye başlar.
- SolarWinds saldırısı, çok sayıda aşama ve teknik içeren, son derece sofistike ve iyi koordine edilmiş bir operasyondu.
- SolarWinds aynı zamanda Ağ Yapılandırma Yöneticisi ile ağ güvenlik açığı tespiti sağlar. Ağ yapılandırmalarını izlemek, yönetmek ve korumak için işlevlere sahiptir.

Güvenlik Açığı Tarama Araçları

5. OpenVas

- Açık Güvenlik Açığı Değerlendirme Sisteminin kısaltması olan OpenVAS, bir ağdaki güvenlik açıklarını tespit etmeye yardımcı olan ücretsiz ve açık kaynaklı bir güvenlik açığı tarayıcısıdır.
- OpenVAS, güvenlik açıklarını tanımlayıp bildirerek ağlarını güvende tutmak için güvenlik uzmanları ve sistem yöneticileri tarafından yaygın olarak kullanılır.
- OpenVAS, güvenlik açıklarını tanımlamaya ve sınıflandırmaya yardımcı olan NVT (Ağ Güvenlik Açığı Testleri) ve NASL (Nessus Attack Scripting Language- Nessus Attack Komut Dosyası Dili) gibi çeşitli tarama motorları içerir.
- OpenVAS'ın ana özelliklerinden biri, kapsamlı güvenlik açığı değerlendirmeleri yapabilmesidir.

Güvenlik Açığı Tarama Araçları

6. Nexpose Community

- Nexpose, tehdit tespiti ve müdahalesi için çözümler sunan bir siber güvenlik şirketi olan Rapid7 tarafından sunulan bir güvenlik açığı yönetimi çözümüdür.
- Nexpose topluluğu, kuruluşlarının BT altyapısındaki güvenlik açıklarını belirlemek ve öncelik sırasına koymak için Nexpose kullanan bir grup güvenlik uzmanıdır.
- Nexpose topluluğunun bir parçası olmanın en önemli avantajlarından biri Rapid7 Security Exchange'e erişimdir. Bu platform, kullanıcılara geniş bir güvenlik açığı kontrolleri kitaplığına, yararlanma modüllerine ve diğer güvenlikle ilgili içeriğe erişim sağlar.

Güvenlik Açığı Tarama Araçları

7. Nikto

- Nikto, web sunucularındaki güvenlik açıklarını tespit etmek ve tespit etmek için kullanılabilen açık kaynaklı bir web sunucusu tarayıcısıdır.
- Nikto, Unix, Linux ve Windows platformlarında çalışacak şekilde tasarlanmıştır.
- Web sunucularını, sunucu yanlış yapılandırmaları, güvenli olmayan dosyalar ve eski yazılım sürümleri dahil olmak üzere 6700'den fazla güvenlik açığı için tarayabilir.
- Nikto'nun kullanıcı dostu arayüzü, taramaları yapılandırmayı ve çalıştırmayı kolaylaştırır.
- Ayrıca, düzeltme önerileri de dahil olmak üzere bulunan güvenlik açıklarına ilişkin ayrıntılı raporlar sunar.

Güvenlik Açığı Tarama Araçları

8. Microsoft Baseline Security Analyzer (MBSA)

- Kullanıcıların ve BT uzmanlarının Windows tabanlı sistemlerdeki güvenlik açıklarını ve yanlış yapılandırmaları belirlemesine yardımcı olan ücretsiz bir araçtır.
- MBSA, hem yerel hem de uzak bilgisayarları taramak için tasarlanmıştır ve kullanıcılara, tarama sırasında belirlenen güvenlik sorunlarını ayrıntılı olarak açıklayan raporlar sağlar.
- MBSA'nın birincil işlevi, Windows tabanlı sistemleri taramak ve güvenlik açıklarını ve yanlış yapılandırmaları kontrol etmektir. Bunu, sistemin güvenlik ayarlarını ve yapılandırmalarını analiz ederek ve bunları Microsoft tarafından sağlanan önerilen en iyi güvenlik uygulamaları veritabanıyla karşılaştırarak yapar.

Güvenlik Açığı Tarama Araçları

9. Wireshark

- Wireshark, kullanıcıların ağ trafiğini yakalamasına ve analiz etmesine olanak tanıyan bir ağ protokolü analizcisidir.
- Wireshark, diğerleri arasında TCP/IP, HTTP, DNS ve FTP dahil olmak üzere çok çeşitli ağ protokollerini destekler.
- Wireshark, ağ trafiğini yakalamak için rastgele modda bir ağ arabirim kartı (NIC) kullanır.
- Paketler yakalandıktan sonra, Wireshark paketleri analiz eder ve verileri çeşitli biçimlerde görüntüler.

Güvenlik Açığı Tarama Araçları

10. Apptrana

- Güvenlik açıklarını algılayan ve raporlayan otomatik bir web uygulaması güvenlik açığı tarayıcısıdır.
- Bildirilen güvenlik açığının kanıtını sağlamak ve yanlış pozitifleri ortadan kaldırmak için tasarlanmıştır.
- Ek Manuel Sızma testleri ve raporları aynı panoda yayınlanır. Duraklatma ve devam ettirme özelliği vardır.

Özet

- Siber tehditler, güvenlik riskleri, güvenlik açıkları incelenmiştir.
- Siber tehditler kapsamında virüsler, truva atları, solucanlar, rootkit'ler ve hacker'lar hakkında bilgi verilmiştir.
- Casus yazılım, korku yazılım, şaka programları ve fidye yazılım gibi bilinen tehditler açıklanmıştır.
- Güvenlik açıkları ve bu açıkları tespit etmek için en çok kullanılan zafiyet tarama araçlarından bahsedilmiştir.