Mobil Cihaz Güvenliği

Burada seçtiğiniz bir maddenin alt başlıklarını gerçekleyip rapor hazırlayın 10 maddelik güvenlik sorularını cevaplayın süreniz 30 dakika.

1. Mobil Tehditleri Tanıma Uygulamaları

1.1. Mobil Zararlı Yazılım Tespiti Simülasyonu

Amaç:
Bir uygulamanın zararlı olup olmadığını tespit etmek.

Uygulama Adımları:
1. Bilgisayarınızda ya da telefonunuzda herhangi bir .apk dosyasını bulun veya indirin.
2. https://www.virustotal.com/ adresine girin ve bu dosyayı yükleyin.
3. Oluşan analiz raporunu inceleyin. Kaç farklı güvenlik motorunun bu dosyayı zararlı olarak işaretlediğini not alın.
4. Sonuçları kısa bir şekilde yorumlayın.

Teslim: Raporun ekran görüntüsü ve kısa yorumu.

1.2. Sahte Uygulama Analizi

Amaç:
Sahte veya klon uygulamaları tespit etmek.

Uygulama Adımları:
1. Google Play Store'da popüler bir uygulama ismini aratın (örneğin "WhatsApp").
2. Karşınıza çıkan uygulamalar içinde orijinaliyle aynı veya benzer isimli olanları belirleyin.
3. İndirilen sayısı, kullanıcı yorumları ve yayıncı bilgilerini karşılaştırarak hangisinin sahte olabileceğini analiz edin.
4. Sahte olduğunu düşündüğünüz bir uygulamanın ekran görüntüsünü ve kısa analizini ekleyin.

1.3. Cihaz İşletim Sistemi ve Güvenlik Güncellemesi Kontrolü

Uygulama Adımları:
1. Kendi akıllı telefonunuzdan "Ayarlar > Hakkında > Yazılım Bilgisi" bölümüne girin.
2. Mevcut işletim sistemi versiyonunu ve en son güvenlik yaması tarihini not alın.
3. Kullandığınız cihazın güncel olup olmadığını üretici sitesinden veya "Ayarlar > Yazılım Güncelleme" bölümünden kontrol edin.

Teslim: Ekran görüntüsü ve kısaca güncel olup olmadığına dair yorumunuz.

iOS Güvenlik Ayarları

iPhone kullanan öğrenciler için öneriler:
- Güçlü parola, Face ID veya Touch ID kullanımının aktif olduğunu gösteren ekran görüntüsü.
- iCloud yedeklemesinin açık olup olmadığını kontrol edin.
- Uygulama izinleri ve konum izni ayarlarını gözden geçirin.
- Siri ve bildirimlerin ekran kilitliyken kısıtlandığından emin olun.

2. Android Güvenlik Ayarları ve Testleri

2.1. Bilinmeyen Kaynaklardan Uygulama Kurulumu Ayarı

Uygulama Adımları:
1. "Ayarlar > Güvenlik > Bilinmeyen Kaynaklar" menüsüne gidin.
2. Bu ayarın kapalı olduğundan emin olun. Açık ise kapatın.
3. Neden kapalı olması gerektiğiyle ilgili kısa bir not yazın.

Teslim: Ayar ekranının ekran görüntüsü ve kısa açıklama.

2.2. Uygulama İzinleri Kontrolü

Uygulama Adımları:
1. Telefonunuzda yüklü herhangi bir uygulamanın ayarlar menüsüne girin.
2. "İzinler" sekmesinde, uygulamanın hangi izinleri istediğini kontrol edin.
3. Gerekli olmadığını düşündüğünüz izinleri kapatın ve neden kapattığınızı kısaca not edin.

Teslim: Öncesi ve sonrası ekran görüntüleri, hangi izinleri neden kapattığınızın açıklaması.

2.3. Erişilebilirlik İzinleri ve Riskleri

Uygulama Adımları:
1. "Ayarlar > Erişilebilirlik" menüsünden hangi uygulamaların erişilebilirlik izni aldığını kontrol edin.
2. Tanımadığınız veya gereksiz gördüğünüz uygulamaların bu iznini devre dışı bırakın.

Teslim: Ekran görüntüsü ve yaptığınız değişikliklerin kısa açıklaması.

2.4. Biometrik Kilit ve Yedek Şifre/PIN Tanımlama

Uygulama Adımları:
1. "Ayarlar > Güvenlik > Parmak İzi" veya "Yüz Tanıma" bölümüne girin.
2. Bir parmak izi veya yüz tanıma ekleyin ve yedek olarak güçlü bir şifre/PIN belirleyin.

Teslim: Ekran görüntüsü veya uygulamanın etkinleştirildiğine dair kanıt.

3.Ekstra (İsteğe Bağlı) – TryHackMe Mobile Malware Analysis Uygulama Simülasyonu

TryHackMe platformunda, sanal laboratuvar ortamında bir Android APK dosyasını analiz ederek mobil zararlı yazılım tespiti pratiği yapmak.

Uygulama Adımları:

1. **TryHackMe'ye Kayıt Ol ve Giriş Yap**
   https://tryhackme.com/ adresinden ücretsiz hesap açılır ve giriş yapılır.
2. **"Mobile Malware Analysis" Odasına Katıl**
   Üstteki arama kutusuna "Mobile Malware Analysis" yazılır veya https://tryhackme.com/room/mma linkiyle doğrudan odaya girilir.
   "Join Room" butonu ile katılım sağlanır.
3. **Sanal Makineyi (AttackBox) Başlat**
   Odadaki yönergeleri takip ederek "Start Machine" veya "AttackBox" tuşu ile laboratuvar ortamı başlatılır.
   Makine başlatıldığında, masaüstünde analiz edilecek bir APK dosyası bulunur.
4. **MobSF ile APK Dosyasını Analiz Et**
   Sanal makinede MobSF arayüzü açılır (kısayol veya tarayıcı üzerinden).
   Masaüstündeki örnek .apk dosyası MobSF'ye yüklenir.
   Analiz tamamlanınca çıkan raporda şunlar incelenir:
   - Paket adı
   - Tehlikeli izinler (permissions)
   - Şüpheli aktiviteler ve servisler
   - Hardcoded bağlantılar, şifreli/metin veriler
   - Kod ve davranış analizleri
5. **VirusTotal Analizi**
   APK dosyasının hash (SHA-1) değeri alınır (MobSF raporundan veya PowerShell'de Get-FileHash komutuyla).
   VirusTotal.com sitesine bu hash girilerek zararlı tespiti yapılır.
   Virüs raporunda en çok hangi antivirüslerin zararlı olarak işaretlediği, hangi isimle tespit edildiği ve topluluk yorumları incelenir.
6. **Sonuçların Raporlanması**
   – Analiz edilen APK'nın adı, paket adı, izinleri ve davranışları özetlenir.
   – MobSF ve VirusTotal'dan alınan önemli ekran görüntüleri eklenir.
   – "Bu uygulama neden zararlı?", "Hangi izinler kritik?", "En çok hangi antivirüs yakaladı?" gibi sorular maddeler halinde cevaplanır.

10 Maddelik Güvenlik Kontrol Listesi

- Aşağıdaki maddelerin her biri için cihazınızı kontrol edin ve “Evet/Hayır” olarak belirtin. Eksikse nasıl düzelteceğinizi yazın.

1. Cihazın işletim sistemi güncel mi?
2. Güçlü parola veya biyometrik kilit var mı?
3. Bilinmeyen kaynaklardan uygulama yükleme kapalı mı?
4. Gereksiz uygulamalar silindi mi?
5. Önemli uygulamalarda iki faktörlü kimlik doğrulama (2FA) açık mı?
6. Uygulama izinleri kontrol edildi mi?
7. Wi-Fi ve Bluetooth kullanılmadığında kapalı mı?
8. Otomatik/manuel yedekleme açık mı?
9. “Cihazımı Bul” gibi özellikler etkin mi?
10. Parola yöneticisi kullanılıyor mu?

Teslim: Her madde için kısa değerlendirme.