1. MULTIPLE CHOICE • 2 mins • 1 pt

Preview Edit

"Çok Katmanlı Savunma" (Defense in Depth) stratejisinin temel amacı nedir?

- [x] Saldırganın tek bir savunma hattını aşsa bile başka engellerle karşılaşmasını sağlamaktır.
- [ ] Sadece ağ çevresinde güçlü bir güvenlik duvarı oluşturmaktır.
- [ ] Güvenlik testlerini yalnızca otomasyon araçları ile gerçekleştirmektir.
- [ ] Sistemdeki en zayıf halkayı bularak sadece orayı güçlendirmektir.
- [ ] Tüm güvenlik önlemlerini sadece uygulama katmanında toplamaktır.

2. MULTIPLE CHOICE • 2 mins • 1 pt

"Tehdit Modellemesi" sürecinin temel kazanımlarından (T1) biri nedir?

- [x] Saldırı yüzeyini çıkartmak ve en az 5 tehdit vektörü belirlemektir.
- [ ] Güvenlik kurallarını otomasyon (IaC) ile hızlıca dağıtmaktır.
- [ ] Tüm sistemi hemen şifrelemek için bir algoritma seçmektir.
- [ ] Yalnızca antivirüs yazılımının güncel olup olmadığını kontrol etmektir.
- [ ] Başarısız giriş denemeleri için FSM (Sonlu Durum Makinesi) çizmektir.

3. MULTIPLE CHOICE • 2 mins • 1 pt

Parola özeti (hash) veya OTP gibi gizli verileri kıyaslarken "constant-time karşılaştırma" (sabit zamanlı kıyaslama) tekniği neden kullanılır?

- [ ] Parola kırma işlemini hızlandırmak ve sunucu üzerindeki işlem yükünü azaltmak için.
- [ ] Başarısız denemeleri sayarak kaba kuvvet (brute-force) saldırılarını yavaşlatmak için.
- [x] Girdi içeriğine göre (doğru/yanlış) farklı süre yaratan zaman yan kanalı sızıntısını önlemek için.
- [ ] Kullanıcıların daha karmaşık veya daha uzun parolalar seçmesini zorunlu kılmak için.
- [ ] Tüm parola karşılaştırmalarını tek bir merkezi sunucuda verimli bir şekilde toplamak için.

4. MULTIPLE CHOICE • 2 mins • 1 pt

"Canonicalization" (Kanonikleştirme) ilkesinin temel amacı nedir?

- [ ] Kullanıcı başına düşen istek sayısını belirli bir zaman aralığında sınırlamaktır.
- [ ] Başarısız olan dış servis çağrılarında (örn. AV API) sistemi hızlıca başarısızlığa uğratmaktır.
- [ ] Sunucudan dönen hata mesajlarını her zaman aynı ve genel (generic) tutmaktır.
- [x] Girdiyi (örn. dosya yolu) doğrulamadan önce normalize ederek (örn. '../') path traversal gibi saldırıları önlemektir.
- [ ] Bir işlemin (örn. ödeme) tekrar tekrar çalıştırılsa bile tek bir sonuç üretmesini sağlamaktır.

5. MULTIPLE CHOICE • 2 mins • 1 pt

"5 dakika içinde 8'den fazla başarısız ve ardından 1 başarılı giriş denemesi" gibi bir deseni tespit eden kural, hangi kural yaklaşımına örnektir?

- [ ] Yalnızca İmza Tabanlı (Signature-based) Tespit.
- [x] Durum Takibi ve Korelasyon (Stateful Correlation) Tabanlı Tespit.
- [ ] Yalnızca Zafiyet Tarama (Vulnerability Scanning) Sonucu.
- [ ] Makine Öğrenmesi (Machine Learning) Sınıflandırması.
- [ ] İstatistiksel Anomali (Statistical Anomaly) Tabanlı Tespit.

Saldırı tespit kurallarını değerlendirmek için kullanılan "Precision" (İsabet Oranı) metriği neyi ölçer?

- [x] Üretilen toplam uyarıların (alarmların) yüzde kaçının gerçekten doğru (gerçek pozitif) olduğunu.
- [ ] Meydana gelen gerçek saldırıların (gerçek pozitif) yüzde kaçının başarıyla yakalandığını.
- [ ] Kuralın ne kadar hızlı çalıştığını ve sistemi ne kadar yavaşlattığını.
- [ ] Güvenlik ekibinin bir uyarıya ne kadar sürede müdahale ettiğini (MTTR).
- [ ] MITRE ATT&CK çerçevesindeki toplam tekniklerin yüzde kaçının kapsandığını.

7. MULTIPLE CHOICE • 2 mins • 1 pt

Ağ savunma politikalarından "segmentasyon" (bölümlendirme) neden önemlidir?

- [ ] Ağ trafiğini analiz etmeden önce tüm paketleri şifrelemek için.
- [x] Saldırganın ağa girse bile (örn. bir kullanıcı bilgisayarı) sunuculara yayılmasını, yani yanal hareketini kısıtlamak için.
- [ ] Ağdaki tüm cihazların aynı IP bloğunda ve aynı VLAN'da olmasını sağlamak için.
- [ ] Tüm ağ kurallarını tek bir merkezi güvenlik duvarında (firewall) toplamak için.
- [ ] Sadece dışarıdan (internet) gelen trafiği engellemek (ingress filtering) için.

8. MULTIPLE CHOICE • 2 mins • 1 pt

"Altyapı Olarak Kod" (IaC) veya "Politika Olarak Kod" (PaC) yaklaşımının temel amacı nedir?

- [ ] Ağdaki tüm güvenlik açıklarını otomatik olarak bulup yamamak.
- [ ] Sadece Pardus işletim sisteminde çalışan özel güvenlik duvarı betikleri yazmak.
- [ ] Ağdaki tüm trafiği analiz için merkezi bir log sunucusuna göndermek.
- [ ] Güvenlik kurallarını (örn. firewall kuralları) her sunucuya tek tek manuel olarak girmek.
- [x] Ağ politikalarını (örn. ACL, güvenlik grupları) otomasyon araçlarıyla (örn. Ansible, Terraform) tekrarlanabilir ve denetlenebilir hâle getirmek.

9. MULTIPLE CHOICE • 2 mins • 1 pt

Sızdırılmış parola listelerinin denendiği "Kimlik Doldurma" (Credential Stuffing) saldırılarına karşı en etkili önlemlerden ikisi hangileridir?

- [ ] Tüm kullanıcılar için aynı ve varsayılan (default) bir parola belirlemek.
- [ ] Oturum (session) token ömrünü süresiz (hiç bitmeyen) olarak ayarlamak.
- [ ] HTTP güvenlik başlıklarını (örn. HSTS) kullanmak ve sunucu sürüm bilgisini kaldırmak.
- [x] Başarısız girişler için oran sınırlaması (rate-limit) ve Çok Faktörlü Kimlik Doğrulama (MFA) uygulamak.
- [ ] Kullanıcı parolalarını veritabanında şifrelemeden, düz metin (plaintext) olarak saklamak.

10. MULTIPLE CHOICE • 2 mins • 1 pt

"Oturum Sabitleme" (Session Fixation) veya "Token Çalma" (Token Theft) saldırılarına karşı oturum (session) yönetiminde alınması gereken temel önlem nedir?

- [ ] Başarılı girişlerde kullanıcıyı her zaman ana sayfaya yönlendirmek.
- [x] Kullanıcı giriş yaptığında (kimlik doğruladığında) oturum kimliğini (Session ID) yenilemek (değiştirmek).
- [ ] Kullanıcıdan her sayfa geçişinde parolasını tekrar girmesini istemek.
- [ ] OAuth2/OIDC akışlarını tamamen devre dışı bırakıp sadece basit parola kullanmak.