PBAC/Politika-temelli erişim mimarisinde "kararı veren" bileşen hangisidir?

- ○ IdP – Kimliği doğrulayan sağlayıcıdır; karar üretmez, yalnızca kimlik bilgisini sunar.
- ○ PIP – Politika bilgilerini sağlar; veriyi besler fakat tek başına karar vermez.
- ○ PAP – Politikaları yönetir ve yayınlar; icra ya da karar mekanizması değildir.
- ● PDP – Politika kurallarını değerlendirip sonuç üretir; kararı belirleyen bileşendir.
- ○ PEP – Kararı uygular; istekleri engeller veya geçirir, değerlendirme yapmaz.

2. MULTIPLE CHOICE • 2 mins • 1 pt

OAuth 2.0 ile OpenID Connect (OIDC) arasındaki ilişkiyi doğru ifade eden seçenek hangisidir?

- ● OAuth yetkilendirme çerçevesidir; OIDC ise onun üzerine eklenen kimlik katmanıdır.
- ○ OIDC çoğunlukla mobil ve web uygulamalarında çalışsa da tek platformla sınırlı değildir.
- ○ Her iki teknoloji de yetkilendirme akışlarında farklı belirteç türlerini amaçlar, SAML değildir.
- ○ OAuth kimlik katmanı değildir; temel hedefi kaynaklara yetkili erişimi temsil etmektir.
- ○ OAuth tarayıcı çerezleriyle sınırlı kalmaz; çeşitli aktarım ve belirteç yapıları kullanır.

3. MULTIPLE CHOICE • 2 mins • 1 pt

OIDC'de "ID Token" ve "Access Token" için doğru eşleştirme hangisidir?

- ○ ID Token, süre bilgisini taşıyabilir; Access Token, anahtar kümesiyle bire bir aynı değildir.
- ○ ID Token, SAML ile karıştırılmamalıdır; Access Token bir relaystate değeri de değildir.
- ○ ID Token API yetkisi değildir; Access Token kimliği doğrudan ifade etmez genellikle.
- ○ ID Token yenileme izni değildir; Access Token kullanıcı parolası gibi gizli bilgi değildir.
- ● ID Token kimliği ifade eder; Access Token API erişim yetkisini temsil eder net olarak.

4. MULTIPLE CHOICE • 2 mins • 1 pt

SAML'de SP-başlatmalı akış için daha doğru ifade hangisidir?

- ○ Mesajlar yalnızca arka kanal değildir; farklı bağlamlarda önyüz yönlendirmeleri de görülür.
- ● SP, kullanıcıyı IdP'ye yönlendirir ve dönüşte ACS üzerinde katı doğrulama yapılır.
- ○ RelayState tamamen yok sayılmaz; durumu taşımak için pratik biçimde kullanılabilir.
- ○ İmzalama zorunluluğu yoktur demek doğru değildir; güvenlik için yaygın biçimde kullanılır.
- ○ IdP'nin tek taraflı seçim yapması tipik değildir; akış SP tarafından tetiklenir genelde.

5. MULTIPLE CHOICE • 2 mins • 1 pt

"Erişim reddi" loglamasında asgari veri alanlarını en iyi özetleyen seçenek hangisidir?

- ○ IP ve tarayıcı ayrıntıları faydalı olabilir; tek başına yeterli bir bağlam sunmazlar.
- ○ Sadece kullanıcı adı ile zaman damgası, denetim için çoğu durumda eksik kalacaktır.
- ● Kim, neye, hangi işlemi, hangi politikaya göre ve neden reddedildi — özlü çerçeve.
- ○ Kimlik sağlayıcı ismi ile token süresi tek başına neden bilgisini kapsamaz genelde.
- ○ Yalnızca politika adı ya da HTTP kodu, olayın sebebini açıklamakta

DAC (Discretionary Access Control) için en doğru tanım hangisidir?

- [x] Kaynak sahibi nesne izinlerini belirler ve devredebilir; sahip-merkezli esnek bir modeldir.
- [ ] Yalnızca rollere bağlanan izinlerden ibaret değildir; yetki devri önemli bir özelliktir.
- [ ] Ağ katmanı kurallarıyla karıştırılmamalıdır; dosya ve nesne düzeyi kontrol vurgulanır.
- [ ] Sistem etiketleriyle katı zorunluluk içeren yaklaşım değildir; yönetim kuralı farklıdır.
- [ ] Salt bağlamsal nitelik ifadelerine dayanmaz; sahiplik ilişkisi temel rol oynar burada.

7. MULTIPLE CHOICE • 2 mins • 1 pt

MAC (Mandatory Access Control) modelinde aşağıdakilerden hangisi esastır?

- [ ] Kullanıcıların nesne izinlerini dilediğince değiştirmesi beklenmez; bu yaklaşım farklıdır.
- [x] Özne ve nesneler etiketlenir; sistem politikası kararları zorunlu ve değiştirilemez kılar.
- [ ] Roller üzerinden atama yapılması tek ilke değildir; etiket mantığı belirleyici konumdadır.
- [ ] Zaman ve konuma dayalı bağlamlar kullanılabilir; temel prensip etiket bütünlüğüdür.
- [ ] Sadece kullanıcı nitelikleriyle sınırlı değildir; güvenlik seviyeleri ana eksendir burada.

8. MULTIPLE CHOICE • 2 mins • 1 pt

RBAC ve ABAC arasındaki farkı en doğru özetleyen seçenek hangisidir?

- [ ] Her ikisi de yalnızca kaynak tarafındaki ACL listeleri değildir; kavramlar daha geneldir.
- [ ] RBAC yalnız kullanıcı etiketlerine bakmaz; ABAC tek başına IP adresiyle sınırlı değildir.
- [x] RBAC'ta izinler rollere, roller kullanıcılara verilir; ABAC nitelik temelli politika değerlendirir.
- [ ] İki model tamamen aynı değildir; tasarım ve ifade gücü bakımından ayrışırlar net olarak.
- [ ] ABAC sadece kimlik doğrulamada çalışmaz; karar aşamasında nitelikleri değerlendirir.

9. MULTIPLE CHOICE • 2 mins • 1 pt

Politika değerlendirmesinde tercih edilen temel güvenlik ilkesi hangisidir?

- [ ] Varsayılan izin anlayışı risklidir; sonradan denetleme tek başına yeterli olmayacaktır.
- [ ] Permit-overrides her senaryoda ideal değildir; bağlam ve politika yapısı önemlidir.
- [ ] Kararı yalnızca PEP tarafında üretmek doğru değildir; görev ayrımı yaklaşımı esastır.
- [ ] IdP çerezi içine tüm kararları gömmek tasarımsal açıdan uygun görülmemektedir.
- [x] Deny-by-default esastır; açıkça tanımlanmayan istekler güvenlik için reddedilir.

10. MULTIPLE CHOICE • 2 mins • 1 pt

RuBAC (Rule-Based Access Control) hakkında doğru ifade hangisidir?

- [ ] Sadece rollere dayalı değildir; kuralların değerlendirilmesi temel mekanizmadır burada.
- [ ] ABAC'tan farkı yalnızca nitelik kullanımı değildir; ifade tarzı kurallar etrafında örülür.
- [ ] ACL satır eşleşmesine indirgenmez; değerlendirme motoru kural koşullarını uygular.
- [x] Önceden tanımlı kurallar çalıştırılır; zaman veya ağ gibi çevresel koşullar dâhil edilebilir.
- [ ] Sadece veritabanı satır düzeyine özgü değildir; geniş kapsamlı bir modelleme sunabilir.