Certified in Hacking and Defending the Cloud Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Cloud altyapılarının hızla yaygınlaşması ve kurumların hibrit cloud mimarilerine yönelmesi, yanlış yapılandırmaların ve erişim hatalarının ciddi güvenlik risklerine dönüşmesine neden olmaktadır. **Certified in Hacking and Defending the Cloud** eğitimi; AWS, Microsoft Azure ve Google Cloud Platform ortamlarında ortaya çıkabilecek güvenlik açıklarını, yanlış yapılandırmaları ve saldırı yüzeylerini hem saldırgan hem de savunma perspektifinden ele alan kapsamlı bir programdır.

Dört günlük bu eğitim, katılımcıları gerçek dünya saldırganlarının düşünce yapısıyla tanıştırır ve gelişmiş laboratuvar ortamlarında çok sayıda saldırı tekniğini uygulama fırsatı sunar. Eğitim süresince 25'ten fazla farklı saldırı senaryosu incelenir; yaklaşık **38 laboratuvar** ve **10 demonstrasyon** ile teorik bilgiler uygulamaya dönüştürülür.

Program, yalnızca saldırı tekniklerini öğretmekle kalmaz. Aynı zamanda cloud ortamlarında zafiyetlerin nasıl tespit edileceği, nasıl giderileceği, cloud-native ve açık kaynak araçlarla nasıl izleneceği ve güvenlik olaylarına nasıl yanıt verileceği üzerinde de durur.

Katılımcılar; sanal makineler, storage bucket'ları, serverless fonksiyonlar, container servisleri, kimlik ve erişim yönetimi altyapıları gibi cloud bileşenlerinin oluşturduğu saldırı yüzeylerini değerlendirmeyi öğrenir. Ayrıca AWS, Azure ve GCP'de IAM, metadata servisleri, storage yapılandırmaları ve servis bazlı erişim kontrollerinin güvenlik üzerindeki etkilerini incelerler.

Program sonunda katılımcıların cloud dağıtımlarındaki karmaşık güvenlik açıklarını daha güvenli biçimde tespit edebilmeleri, bu açıklara karşı uygun savunma kontrolleri oluşturabilmeleri ve cloud ortamlarını sürekli gözlemleyebilecek bir güvenlik yaklaşımı geliştirebilmeleri hedeflenir.

Önkoşullar

Katılımcıların eğitimden maksimum fayda sağlayabilmeleri için:

- Temel veya orta seviyede siber güvenlik bilgisine sahip olmaları,
- Tercihen en az 1,5 yıllık güvenlik deneyimine sahip olmaları,
- Yaygın command-line komutlarıyla çalışabilmeleri

önerilir.

Certified in Hacking and Defending the Cloud Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Kimler Katılmalı

Bu eğitim özellikle:

- Cloud yöneticileri ve cloud architect'ler,
- Penetration tester'lar ve red team uzmanları,
- Blue team, CSIRT ve SOC analistleri,
- Incident responder'lar,
- Cloud developer ve engineer'lar,
- Security ve IT yöneticileri,
- Teknik takım liderleri

için uygundur.

Cloud güvenliğinde teknik veya yönetsel sorumluluğu bulunan ve AWS, Azure ya da GCP ortamlarında daha ileri düzey güvenlik bilgisi edinmek isteyen profesyoneller de programdan faydalanabilir.

Neler Öğreneceksiniz

Eğitim sonunda katılımcılar:

- Gelişmiş tehdit aktörlerinin cloud ortamlarına nasıl yaklaştığını anlayabilir.
- AWS, Azure ve GCP'deki karmaşık güvenlik açıklarını ve yanlış yapılandırmaları belirleyebilir.
- Gerçek saldırgan davranışlarını temel alan penetration test senaryoları tasarlayabilir.
- VM, bucket, CaaS ve serverless servislerin oluşturduğu saldırı yüzeylerini değerlendirebilir.
- Açık servisler üzerinden cloud ortamına erişim sağlayan saldırı tekniklerini anlayabilir.
- Post-exploitation sürecinde sistemleri enumerate etmeyi ve veri sızıntısı yollarını değerlendirebilir.
- AWS, Azure ve GCP için uygun savunma yöntemlerini karşılaştırabilir.
- Patching, asset inventory ve least privilege gibi kontrolleri cloud savunma stratejilerine dahil edebilir.
- Cloud aktivitelerini izlemek için cloud-native ve açık kaynak araçlardan yararlanabilir.
- Cloud ortamlarında audit ve benchmark süreçlerini uygulayabilir.
- Yeni zafiyetleri ve saldırı tekniklerini gerçekçi laboratuvar senaryoları üzerinde değerlendirebilir.

Eğitim Yaklaşımı

Program **Defense by Offense** yaklaşımını benimser. Eğitim içeriği yalnızca teorik açıklamalara değil, gerçek pentest çalışmaları ve araştırma çıktılarında gözlemlenen saldırı yöntemlerine dayanır.

Eğitimin yaklaşık %60'ı uygulamalı laboratuvar çalışmalarından oluşur.

Katılımcılar:

- Gerçekçi cloud ortamlarını saldırı ve savunma perspektifinden analiz eder,
- AWS, Azure ve GCP üzerinde farklı exploitation senaryoları uygular,
- Güvenlik açıklarını doğrular ve remediation yaklaşımlarını inceler,
- Capture the Flag (CTF) senaryosunda öğrendikleri teknikleri test eder,
- Gerçek vakaların etkilerini eğitmenle birlikte değerlendirir.

Certified in Hacking and Defending the Cloud Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Eğitim İçeriği

Modül 1: Cloud Computing'e Giriş

Bu modül, cloud güvenliğinin temelini oluşturan kavramları açıklar.

- Cloud computing'e giriş
- Cloud security'nin önemi
- Shared Responsibility Model
- Geleneksel güvenlik modeli ile cloud güvenliğinin karşılaştırılması
- Cloud metadata API'lerinin saldırgan açısından önemi

Modül 2: Cloud Asset Enumeration

Cloud varlıklarının dışarıdan nasıl keşfedilebileceği incelenir.

- Cloud ortamlarında DNS'in önemi
- DNS tabanlı enumeration
- Cloud asset keşfinde OSINT teknikleri
- Cloud provider API'leri üzerinden username enumeration

Modül 3: Cloud Servislerinin Saldırı Yüzeyi

Farklı cloud servis modellerinin oluşturduğu güvenlik riskleri değerlendirilir.

- IaaS saldırı yüzeyi
- FaaS saldırı yüzeyi
- PaaS saldırı yüzeyi
- CaaS saldırı yüzeyi

Modül 4: Cloud Storage Güvenliği

AWS, Azure ve GCP storage servislerinin yanlış yapılandırmalarına odaklanılır.

- AWS S3'e giriş
- AWS S3 misconfiguration örnekleri
- GCP Storage'a giriş
- Azure Storage'a giriş
- Azure Shared Access Signature (SAS) URL yanlış yapılandırmaları

Modül 5: Azure ve Microsoft Entra ID Saldırıları

Azure servisleri ve kimlik altyapısı ayrıntılı olarak incelenir.

- Azure ve Microsoft Entra ID'ye giriş
- App Service, Function App ve Storage saldırıları
- Azure Database güvenliği
- Automation Account
- Azure Key Vault
- Microsoft Entra ID authentication yöntemleri
- Authentication riskleri
- Managed User Identity saldırıları

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- MFA ve Conditional Access kontrollerinin atlatılmasına yönelik risk senaryoları
- Dynamic Membership Policy kötüye kullanımı
- Azure Identity Protection ile kullanıcı davranışlarının izlenmesi

Modül 6: AWS Güvenliği ve Saldırı Teknikleri

AWS'nin gelişmiş güvenlik özellikleri ve yaygın zafiyet senaryoları ele alınır.

- AWS IAM ve policy yapıları
- AWS policy evaluation
- AWS Cognito
- IAM misconfiguration'ları
- Elastic Beanstalk
- AWS Cross-Account yanlış yapılandırmaları
- Pacu ile role enumeration
- EC2 instance attribute kötüye kullanımı
- Resource-based policy yanlış yapılandırmaları
- Lambda ve API Gateway exploitation senaryoları
- AWS ECR ve ECS
- Docker image'larından hassas bilgi elde edilmesi
- AWS Organizations
- IAM Access Analyzer

Modül 7: Google Cloud Platform Güvenliği

GCP kimlik, compute, storage ve application servisleri güvenlik perspektifinden değerlendirilir.

- GCP'ye giriş
- IAM Role ve Service Account yapıları
- Service Account file ile authentication
- Access token ile authentication
- Compute Engine
- Cloud Storage
- App Engine
- Identity-Aware Proxy (IAP)
- Firestore ve Firebase
- Cloud Functions
- Pub/Sub
- Cloud Run
- IAM Impersonation
- Secret Manager
- Container Registry

Modül 8: AWS, Azure ve GCP Misconfiguration'larının Hardened Ortamda Yeniden Değerlendirilmesi

Önceki modüllerde ele alınan kritik yanlış yapılandırmaların düzeltilmesi ve doğrulanması üzerinde durulur.

Aşağıdaki başlıklara yönelik remediation kontrolleri test edilir:

- Microsoft Entra ID

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Azure MFA
- Azure Key Vault
- Elastic Beanstalk
- AWS IAM
- ECS ve ECR
- AWS Cognito
- GCP IAM
- GCP IAP

Modül 9: Backdooring ve Erişimin Sürdürülmesi

Cloud ortamlarında saldırganların kalıcılık oluşturma yöntemleri ve bu davranışların savunma açısından nasıl tespit edilebileceği incelenir.

Modül 10: AWS, Azure ve GCP IAM Yapılarının Karşılaştırılması

Üç büyük cloud sağlayıcısının kimlik ve erişim yönetimi yaklaşımları karşılaştırılır.

- AWS IAM yapısı
- Azure / Microsoft Entra ID yaklaşımı
- GCP IAM yapısı
- Temel farklılıklar
- Yaygın IAM hataları
- Erişim kontrolündeki kritik riskler

Modül 11: Open-Source ve Cloud-Native Araçlarla Cloud Defense

Cloud savunması dört temel aşamada ele alınır: identification, protection, detection ve response.

- Cloud asset identification
- Hybrid account asset inventory
- Açık kaynak araçlarla AWS multi-account inventory
- Cloud asset protection
- Least Privilege prensibi
- EC2, IAM ve RDS üzerinde least privilege örnekleri
- Budget mekanizmalarıyla finansal koruma
- Metadata API koruması
- Linux firewall ile metadata API koruma demonstrasyonu
- Cloud-native araçlarla aktivite monitoring
- Hybrid cloud monitoring stratejisi
- Malicious activity'ye karşı automated response
- AWS Config ve AWS Step üzerinden saldırılara yanıt

Modül 12: Cloud Auditing ve Benchmarking

Cloud ortamlarında güvenlik denetimi ve benchmark yaklaşımı incelenir.

- Audit hazırlığı
- Araçlarla automated auditing
- Uygulamalı audit egzersizi
- Golden Image audit
- Docker Image audit

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

- Uygulamalı image audit çalışmaları
- Cloud ortamları için ilgili benchmark'lar
- CIS benchmark yaklaşımı

Öne Çıkan Üç Kazanım

Program özellikle üç temel yetkinliğe odaklanır:

1. Açık servislerden yararlanarak cloud ortamına giriş yapılmasına yönelik exploitation tekniklerinin anlaşılması
2. Post-exploitation aşamasında enumeration ve exfiltration senaryolarının değerlendirilmesi
3. AWS, Azure ve GCP ortamlarında uygun savunma yöntemlerinin uygulanması

Sınav ve Değerlendirme

Sınav, APMG'nin gözetimli sınav platformu üzerinden gerçekleştirilir.

Sınav Formatı

- 60 soru
- Her soru için 4 seçenek ve 1 doğru cevap
- Dört temel soru kategorisi:
  - Azure
  - AWS
  - GCP
  - Genel cloud güvenliği
- Süre: 60 dakika
- Kapalı kitap
- Başarı barajı: %50