Pentesting Fundamentals

Task 1 What is Penetration Testing? (Sızma Testi Nedir?)

Etik bilgisayar korsanlığının teknik uygulamalı yönlerini öğretmeden önce, bir sızma testi uzmanının iş sorumluluklarının neler olduğu ve pentest (bir müşteri uygulaması veya sistemindeki güvenlik açıklarını bulma) gerçekleştirirken hangi süreçlerin izlendiği hakkında daha fazla bilgi sahibi olmanız gerekir.

Siber güvenliğin önemi ve geçerliliği her geçen gün artıyor ve hayatın her alanında karşımıza çıkabiliyor. Haber başlıkları ekranlarımızı dolduruyor, bir başka hack veya veri sızıntısını bildiriyor.

Siber güvenlik, e-postalarınızı korumak için güçlü bir şifre politikası veya hem cihazları hem de verileri zararlardan koruması gereken işletmeler ve diğer kuruluşlar da dahil olmak üzere modern dünyadaki tüm insanları ilgilendirir.

Sızma testi veya pentest, bu varlıkları ve bilgi parçalarını korumak için güvenlik savunmalarını test etmeye ve analiz etmeye yönelik etik odaklı bir girişimdir. Sızma testi, kötü niyetli birinin kullanacağı araçların, tekniklerin ve metodolojilerin aynısını kullanmayı içerir ve bir denetime benzer.

Bir siber güvenlik sektörü dergisi olan Security Magazine'e göre, her gün 2.200'den fazla siber saldırı gerçekleşiyor - her 39 saniyede 1 saldırı.

Task 2 Penetration Testing Ethics (Sızma Testi Etiği)

Sızma testi bir yana, siber güvenlikte yasallık ve etik savaşı her zaman tartışmalıdır. "Hacking" ve "hacker" gibi etiketler, özellikle popüler kültürde, birkaç çürük elma sayesinde genellikle olumsuz çağrışımlara sahiptir. Bir bilgisayar sistemine yasal olarak erişim sağlama fikrini kavramak zordur - sonuçta bunu tam olarak yasal yapan nedir?

Sızma testinin bir bilgisayar sisteminin güvenliğinin ve savunmasının sistem sahipleri tarafından kararlaştırılan yetkili bir denetimi olduğunu hatırlayın. Sızmanın yasallığı bu anlamda oldukça nettir; bu anlaşmanın dışında kalan her şey yetkisiz kabul edilir.

Bir sızma testi başlamadan önce, sızma testi uzmanı ile sistem sahibi arasında resmi bir tartışma gerçekleşir. Test edilecek çeşitli araçlar, teknikler ve sistemler üzerinde anlaşmaya varılır. Bu tartışma sızma testi anlaşmasının kapsamını oluşturur ve sızma testinin izleyeceği yolu belirler.

Sızma testi hizmetleri sağlayan şirketler yasal çerçevelere ve sektör akreditasyonuna tabidir. Örneğin, Ulusal Siber Güvenlik Merkezi (NCSC) Birleşik Krallık'ta CHECK akreditasyon programına sahiptir. Bu kontrol, yalnızca "[CHECK] onaylı şirketlerin kamu sektörü ve CNI sistemleri ve ağlarının yetkili sızma testlerini yapabileceği" anlamına gelir. (NCSC).

Etik, doğru ve yanlış arasındaki ahlaki tartışmadır; bir eylem yasal olsa da, bireyin doğru ve yanlış inanç sistemine aykırı olabilir.

Sızma testi uzmanları genellikle bir sızma testi sırasında ahlaki açıdan sorgulanabilir kararlarla karşı karşıya kalırlar. Örneğin, bir veritabanına erişim elde ediyor ve potansiyel olarak hassas verilerle karşılaşıyorlar. Ya da bir kuruluşun insan güvenliğini test etmek için bir çalışana kimlik avı saldırısı gerçekleştiriyor olabilirler. Bu eylem ilk aşamalarda kararlaştırılmışsa, etik açıdan sorgulanabilir olsa da yasaldır.

Hackerlar üç şapkaya ayrılır ve eylemlerinin arkasındaki etik ve motivasyonları hangi şapka kategorisine yerleştirileceklerini belirler. Bu üç şapkayı aşağıdaki tabloda ele alalım:

Şapka Kategorisi:	**Açıklama**:	**Örneği**:
Beyaz Şapkalı:	Bu hackerlar "iyi insanlar" olarak kabul edilir. Yasalar dahilinde kalırlar ve becerilerini başkalarına fayda sağlamak için kullanırlar.	Örneğin, bir şirket üzerinde yetkili bir görev gerçekleştiren bir sızma testi uzmanı.
Gri Şapkalılar:	Bu kişiler becerilerini genellikle başkalarına fayda sağlamak için kullanırlar; ancak yasalara veya	Örneğin, bir dolandırıcılık sitesini kapatan biri.

	etik standartlara her zaman saygı duymazlar/uymazlar.	
Siyah Şapkalı:	Bu kişiler suçludur ve genellikle kuruluşlara zarar vermeye veya başkalarının zararına bir tür mali fayda elde etmeye çalışırlar.	Örneğin, fidye yazılımı yazarları cihazlara kötü amaçlı kod bulaştırır ve verileri fidye için tutar.

Angajman Kuralları (ROE)

ROE, bir sızma testi görevinin ilk aşamalarında oluşturulan bir belgedir. Bu belge üç ana bölümden oluşur (aşağıdaki tabloda açıklanmıştır) ve sonuçta görevin nasıl yürütüleceğine karar vermekten sorumludur. SANS enstitüsü bu belgenin harika bir örneğine sahiptir ve buradan çevrimiçi olarak görüntüleyebilirsiniz.

Bölüm:	**Açıklaması**:
izin:	Belgenin bu bölümü, gerçekleştirilecek angajman için açık bir izin vermektedir. Bu izin, bireyleri ve kuruluşları yürüttükleri faaliyetler açısından yasal olarak korumak için gereklidir.
Test Kapsamı:	Belgenin bu bölümünde, görevin uygulanması gereken belirli hedefler açıklanacaktır. Örneğin, sızma testi tüm ağa değil, yalnızca belirli sunuculara veya uygulamalara uygulanabilir.
Kurallar:	Kurallar bölümü, angajman sırasında izin verilen teknikleri tam olarak tanımlayacaktır. Örneğin, kurallar kimlik avı saldırıları gibi tekniklerin yasak olduğunu, ancak MITM (Man-in-the-Middle) saldırılarının serbest olduğunu özellikle belirtebilir.

soru⇒ Bir kuruluşta güvenlik denetimi yapmak için size izin verildi; ne tür bir hacker olurdunuz?

cevap ⇒ white hat

soru ⇒ Bir kuruluşa saldırır ve verilerini çalarsanız, ne tür bir hacker olursunuz?

cevap ⇒ black hat

soru ⇒ Bir sızma testi görevinin nasıl yürütülmesi gerektiğini tanımlayan belge hangisidir?

cevap ⇒ Rules of Engagement

Task 3 Penetration Testing Methodologies (Sızma Testi Metodolojileri)

Sızma testlerinin çok çeşitli amaçları ve kapsam dahilindeki hedefleri olabilir. Bu nedenle, hiçbir sızma testi aynı değildir ve bir sızma test uzmanının bu teste nasıl yaklaşması gerektiğine dair tek bir durum yoktur.

Bir sızma testi uzmanının bir görev sırasında attığı adımlar metodoloji olarak bilinir. Pratik bir metodoloji, atılan adımların eldeki durumla ilgili olduğu akıllı bir metodolojidir. Örneğin, bir web uygulamasının güvenliğini test etmek için kullanacağınız bir metodolojiye sahip olmak, bir ağın güvenliğini test etmeniz gerektiğinde pratik değildir.

Bazı farklı endüstri standardı metodolojileri tartışmadan önce, hepsinin aşağıdaki aşamalardan oluşan genel bir temaya sahip olduğunu belirtmeliyiz:

Sahne:	**Tanımı**:
Bilgi Toplama:	Bu aşama, bir hedef/kuruluş hakkında mümkün olduğunca çok kamuya açık bilgi toplamayı içerir, örneğin OSINT ve araştırma. Not: Bu, herhangi bir sistemin taranmasını içermez
Numaralandırma/ Tarama:	Bu aşama, sistemler üzerinde çalışan uygulama ve hizmetlerin keşfedilmesini içerir. Örneğin, potansiyel olarak savunmasız olabilecek bir web sunucusunun bulunması.
İstismar:	Bu aşama, bir sistem veya uygulamada keşfedilen güvenlik açıklarından yararlanmayı içerir. Bu aşama, genel istismarların kullanılmasını veya uygulama mantığının istismar edilmesini içerebilir.
Ayrıcalık Yükseltme:	Bir sistemi veya uygulamayı başarılı bir şekilde istismar ettikten sonra (dayanak noktası olarak bilinir), bu aşama bir sisteme erişiminizi genişletme girişimidir. Yatay ve dikey olarak yetki artırımı yapabilirsiniz; burada yatay olarak aynı izin grubundaki başka bir hesaba (yani başka bir kullanıcıya), dikey olarak ise başka bir izin grubuna (yani bir yöneticiye) erişebilirsiniz.
Sömürü sonrası:	Bu aşama birkaç alt aşamadan oluşmaktadır. 1. Başka hangi ana bilgisayarlar hedeflenebilir (pivotlama) 2. Artık ayrıcalıklı bir kullanıcı olduğumuza göre ana bilgisayardan hangi ek bilgileri toplayabiliriz? 3. İzlerinizi örtmek 4. Raporlama

OSSTMM

Açık Kaynak Güvenlik Test Metodolojisi Kılavuzu, sistemler, yazılımlar, uygulamalar, iletişim ve siber güvenliğin insani yönü için ayrıntılı bir test stratejileri çerçevesi sunar.

Metodoloji öncelikle bu sistemlerin, uygulamaların nasıl iletişim kurduğuna odaklanır, bu nedenle bir metodoloji içerir:

Telekomünikasyon (telefonlar, VoIP, vb.)

Kablolu Ağlar

Kablosuz iletişim

Avantajlar:	**Dezavantajlar:**
Çeşitli test stratejilerini derinlemesine ele alır.	Çerçevenin anlaşılması zordur, çok ayrıntılıdır ve benzersiz tanımlar kullanma eğilimindedir.
Belirli hedefler için test stratejileri içerir (örn. telekomünikasyon ve ağ)	Kasıtlı olarak boş bırakılmıştır.
Çerçeve, kuruluşun ihtiyaçlarına bağlı olarak esnektir	Kasıtlı olarak boş bırakılmıştır.
Çerçeve, sistemler ve uygulamalar için bir standart oluşturmayı amaçlamaktadır, bu da bir sızma testi senaryosunda evrensel bir metodolojinin kullanılabileceği anlamına gelir.	Kasıtlı olarak boş bırakılmıştır.

OWASP

"Open Web Application Security Project" çerçevesi, yalnızca web uygulamalarının ve hizmetlerinin güvenliğini test etmek için kullanılan, topluluk odaklı ve sık sık güncellenen bir çerçevedir.

Vakıf düzenli olarak bir web uygulamasının sahip olabileceği ilk on güvenlik açığını, test yaklaşımını ve düzeltme yöntemlerini belirten raporlar yazmaktadır.

Avantajlar:	**Dezavantajlar**:
Alması ve anlaması kolay.	Bir web uygulamasının ne tür bir güvenlik açığına sahip olduğu net olmayabilir (genellikle örtüşebilirler).
Aktif olarak sürdürülür ve sık sık güncellenir.	OWASP, herhangi bir özel yazılım geliştirme yaşam döngüsü için öneride bulunmamaktadır.

Testten raporlamaya ve düzeltmeye kadar bir görevin tüm aşamalarını kapsar.	Çerçeve, CHECK gibi herhangi bir akreditasyona sahip değildir.
Web uygulamaları ve hizmetleri konusunda uzmanlaşmıştır.	Kasıtlı olarak boş bırakılmıştır.

NIST Siber Güvenlik Çerçevesi 1.1

NIST Siber Güvenlik Çerçevesi, bir kuruluşun siber güvenlik standartlarını geliştirmek ve siber tehdit riskini yönetmek için kullanılan popüler bir çerçevedir. Bu çerçeve, popülerliği ve ayrıntıları nedeniyle biraz onurlu bir sözdür.

Çerçeve, kritik altyapılardan (enerji santralleri vb.) ticari kuruluşlara kadar tüm kuruluşlar için güvenlik kontrolleri ve başarı ölçütleri hakkında kılavuz ilkeler sunmaktadır. Bir sızma testi uzmanının izlemesi gereken metodoloji için standart bir kılavuza ilişkin sınırlı bir bölüm bulunmaktadır.

Avantajlar	Dezavantajlar
NIST Çerçevesinin 2020 yılına kadar Amerikan kuruluşlarının %50'si tarafından kullanılacağı tahmin edilmektedir.	NIST'in birçok çerçeve yinelemesi vardır, bu nedenle hangisinin kuruluşunuz için geçerli olduğuna karar vermek zor olabilir.
Çerçeve, kuruluşların siber tehditlerin yarattığı tehlikeyi azaltmalarına yardımcı olacak standartları belirleme konusunda son derece ayrıntılıdır.	NIST çerçevesi zayıf denetim politikalarına sahiptir, bu da bir ihlalin nasıl gerçekleştiğini belirlemeyi zorlaştırır.
Çerçeve çok sık güncellenmektedir.	Çerçeve, kuruluşlar için hızla daha popüler hale gelen bulut bilişimi dikkate almamaktadır.
NIST, bu çerçeveyi kullanan kuruluşlar için akreditasyon sağlamaktadır.	Kasıtlı olarak boş bırakılmıştır.
NIST çerçevesi diğer çerçevelerle birlikte uygulanmak üzere tasarlanmıştır.	Kasıtlı olarak boş bırakılmıştır.

NCSC CAF

Siber Değerlendirme Çerçevesi (CAF), çeşitli siber tehditlerin riskini ve bir kuruluşun bunlara karşı savunmasını değerlendirmek için kullanılan on dört ilkeden oluşan kapsamlı bir çerçevedir.

Çerçeve, kritik altyapı, bankacılık ve benzerleri gibi "hayati önem taşıyan hizmetler ve faaliyetler" gerçekleştirdiği düşünülen kuruluşlar için geçerlidir. Çerçeve temel olarak aşağıdaki konulara odaklanmakta ve bunları değerlendirmektedir:

Veri güvenliği

Sistem güvenliği

Kimlik ve erişim kontrolü

Esneklik

İzleme

Müdahale ve kurtarma planlaması

Avantajlar	Dezavantajlar
Bu çerçeve bir devlet siber güvenlik kurumu tarafından desteklenmektedir.	Çerçeve sektörde henüz yeni olduğundan, kuruluşların buna uygun hale gelmek için gerekli değişiklikleri yapmak için fazla zamanları olmadı.
Bu çerçeve akreditasyon sağlar.	Çerçeve, ilkelere ve fikirlere dayanır ve diğer bazı çerçeveler gibi kurallara sahip olmak kadar doğrudan değildir.
Bu çerçeve, güvenlikten müdahaleye kadar uzanan on dört ilkeyi kapsamaktadır.	Kasıtlı olarak boş bırakılmıştır.

soru ⇒ Sızma testinin hangi aşaması kamuya açık bilgilerin kullanılmasını içerir?

cevap ⇒ **Information Gathering**

soru ⇒ Telekomünikasyon pentestingi için bir çerçeve kullanmak isteseydiniz, hangi çerçeveyi kullanırdınız? Not: Burada tam adı değil kısaltmayı arıyoruz.

cevap ⇒ **OSSTMM**

soru ⇒ Web uygulamalarının test edilmesine odaklanan çerçeve hangisidir?

cevap ⇒ **OWASP**

Task 4 Black box, White box, Grey box Penetration Testing (Kara kutu, Beyaz kutu, Gri kutu Sızma Testi)

Bir uygulama veya hizmeti test ederken üç temel kapsam vardır. Hedefinize ilişkin anlayışınız, sızma testi görevinizde gerçekleştireceğiniz test düzeyini belirleyecektir. Bu görevde, bu üç farklı test kapsamını ele alacağız.

Black-Box Testi

Bu test süreci, test uzmanına uygulamanın veya hizmetin iç işleyişi hakkında herhangi bir bilgi verilmediği üst düzey bir süreçtir.

Test uzmanı, uygulamanın veya yazılım parçasının işlevselliğini ve etkileşimini test eden normal bir kullanıcı gibi hareket eder. Bu test, arayüzle, yani düğmelerle etkileşime girmeyi ve amaçlanan sonucun döndürülüp döndürülmediğini test etmeyi içerebilir. Bu tür bir test için programlama bilgisi veya programın anlaşılması gerekmez.

Black-Box testi, hedefin saldırı yüzeyini anlamak için bilgi toplama ve numaralandırma aşamasında harcanan süreyi önemli ölçüde artırır.

Gri Kutu Testi

Bu test süreci, sızma testi gibi işlemler için en popüler olanıdır. Hem kara kutu hem de beyaz kutu test süreçlerinin bir kombinasyonudur. Test uzmanı, uygulamanın veya yazılım parçasının dahili bileşenleri hakkında sınırlı bilgiye sahip olacaktır. Yine de, uygulama ile sanki bir kara kutu senaryosuymuş gibi etkileşime girecek ve ardından uygulama hakkındaki bilgilerini kullanarak sorunları buldukça çözmeye çalışacaktır.

Gri Kutu testi ile verilen sınırlı bilgi zaman kazandırır ve genellikle son derece iyi sertleştirilmiş saldırı yüzeyleri için seçilir.

Gri Kutu testi ile verilen sınırlı bilgi zaman kazandırır ve genellikle son derece iyi sertleştirilmiş saldırı yüzeyleri için seçilir.

White-Box Testi

Bu test süreci genellikle programlama ve uygulama mantığını bilen bir yazılım geliştirici tarafından yapılan düşük seviyeli bir süreçtir. Test uzmanı, uygulamanın veya yazılım parçasının dahili bileşenlerini test edecek ve örneğin belirli işlevlerin doğru şekilde ve makul bir süre içinde çalışmasını sağlayacaktır.

soru⇒ Sizden bir uygulamayı test etmeniz isteniyor ancak kaynak koduna erişim izni verilmiyor - bu nasıl bir test sürecidir?

cevap ⇒ **Black Box**

soru⇒ Sizden bir web sitesini test etmeniz isteniyor ve size kaynak koduna erişim izni veriliyor - bu nasıl bir test sürecidir?

cevap⇒ **White Box**

Task 5 Practical: ACME Penetration Test (Pratik: ACME Sızma Testi)

ACME bir görev için size başvurdu. Altyapıları üzerinde bir sızma testinin aşamalarını gerçekleştirmenizi istiyorlar. Siteyi görüntüleyin (bu görevdeki yeşil düğmeye tıklayarak) ve bu alıştırmayı tamamlamak için yönlendirmeli talimatları izleyin.

soru ⇒ ACME'nin altyapısına karşı sızma testi çalışmasını tamamlayın.

cevap ⇒ **THM{PENTEST_COMPLETE}**