**Sızma Testi Sözleşmesi**

Sızma testi talep eden ilgili kurum ve/veya kuruluş, Siber Olaylara Müdahale (SOME) Birimi tarafından sızma testi talep eden ilgili kurum ve/veya kuruluşa verilecek saldırı simülasyonu hizmetleri kapsamında iş bu sözleşmeyi imzalamayı kabul ve taahhüt eder. Sözleşmenin konusunu oluşturan saldırı simülasyonu, kötü amaçlı bir saldırganın sistemlere verebileceği zararın ilgili kurum ve/veya kuruluş tarafından görülerek gerekli tedbirlerin alınabilmesi için yapılmaktadır.

* Siber Olaylara Müdahale (SOME) Birimi tarafından ilgili kurum veya kuruluşa verilecek hizmetin ön hazırlıkları sırasında, saldırı simülasyonları öncesi ve saldırı simülasyonları esnasında üçüncü kişileri haberdar etmek, gerekmesi hâlinde yazılı ve/veya sözlü her türlü izni almak ve diğer idari prosedürlerin yerine getirilmesinden, testi talep eden kurum veya kuruluş sorumludur. Bu yükümlülüklerin yerine getirilmemesi nedeniyle doğabilecek doğrudan ve/veya dolaylı zararlardan kurum veya kuruluş sorumluluğu olmayacaktır. İlgili kurum veya kuruluş, bu anlaşmazlık, talep ve zararlardan tabii tutacaktır.
* Testi talep eden ilgili kurum veya kuruluş, Siber Olaylara Müdahale (SOME) Biriminin ağır kusuru ile sebep olduğu durumlar hariç olmak üzere saldırı simülasyonları sırasında ilgili kurum veya kuruluşun DoS, DDoS ve/veya test sistemlerinin zarar görmesi ve bunun hizmet aksaklığına sebep olması durumunda kurumun sorumlu olmayacağını kabul eder.
* Testi talep eden ilgili kurum veya kuruluş, saldırı simülasyonları sırasında oluşabilecek hizmet aksaklığı, sistem yüklenmeleri gibi olumsuz durumlardan kurumun hiçbir şekilde sorumlu olmayacağını kabul eder.
* Web uygulama ve mobil uygulama sızma testlerinin, test ortamı yerine canlı ortamda test edilmek istenmesi hâlinde doğabilecek başta veri kayıpları/değişikliği olmak üzere zararlardan, kurum veya kuruluş sorumlu değildir.
* Testi talep eden ilgili kurum veya kuruluş test süresince test ortamında herhangi bir değişiklik yapmayacağını kabul eder. Talep edilen test canlı ortamda ise acil bir durum olmadıkça canlı ortamda majör bir değişiklik yapmayacağını kabul eder.
* İşbu Sözleşme, ilgili kurum ve/veya kuruluşun yetkili kişileri tarafından imza edilmekle geçerli ve bağlayıcıdır.

|  |  |
| --- | --- |
| TALEP EDEN KURUM / KURULUŞ | KABUL EDEN |
| Tarih:  Yetkili Onayı  (En Yetkili Merci Kaşe&İmza) | Tarih:  ...................  Müdürlüğü/Başkanlığı |

**Kapsam Belirleme**

Penetrasyon testi yapılacak olan firma ile şirket arasında yapılan anlaşmaya göre belirlenmektedir. Testin gerçekleştirileceği kurum yetkileri ile teste tabi tutulacak sistemlerin tipi ve sayısı belirlenir.

**Web Uygulama Güvenliği Testi**

Web uygulama güvenliği testi sisteme zarar vermeyecek şekilde kötü niyetli hackerın yapabildiği/yapabileceği bütün ihtimalleri göz önüne alarak saldırı aşamasıdır.

**Bilgi Toplama**

Pentest istenilen şirket hakkında bilgi toplanılıp pentest çalışmasına yön verecektir. Bu istek üzerine googleda x.com adında herhangi bir sosyal medya hesabı varsa sosyal medya hesaplarını incelenmeli. İşe yarayacağı düşünülüp ilerleyen adımlarda ssh, ftp gibi açık portlara yönelik veya admin panelinden giriş yapabilmek için brute force saldırısı için wordlist oluşturulmalı. Daha sonrasında şirket ile ilgili olumlu veya olumsuz yorumları arşivlenip ileride sosyal mühendislik saldırısı sebebiyle faydası dokunacaktır.

Google chrome uygulması olan wappalyzer uygulaması ile sistem hakkında bilgi topladım. Bu bilgiler arasında Cloudflare bulunmakta. Nmap sonucu bize vermeyecektir bu sebepten web uygulama açıklarına yönelinmeli. Dnsenum aracı ile subdomain ve ip bloklarını topladım. Ips olduğunu görünce ip ban yememek için online araçlar kullandım. Shodan.io, online nmap sayesinde hem hedef sisteme kendimi deşifre etmiyeceğim hemde hemde ip ban yemekten kurtulacağım.

Dirb, dirbuster, gobuster, dirsearch gibi çeşitli araçları kullanarak sistemde dizin keşfi yapılıp, işe yarayacak dizin aranmalı. (robots.txt, upload.php, login.php vb.)

**Zafiyet Tarama**

Wappalyzer sonucunda sistemin php diliyle yazıldığını görülmekte ve dizin taraması sonucu admin.php isimli bir dizin keşfedildi. Bu dizine gidilerek username ve password' a ''Or'='Or'' gibi çeşitli payloadlar kullanılarak giriş yapılması sağlanır. Hedef sistemin php diliyle yazıldığı bilinmekte. Örneğin;

<http://x.com/index.php?=1> olan sitenin sondaki rakamının yanına tek tırnak işareti (') konularak sql hatası alınması sağlanılır. <http://x.com/index.php?=1'> gibi hata veriliyor ise açık bulunmaktadır.

Karakter girilebilecek yerlere <script>alert(HACKED)</script> gibi payload yazılarak xss zafiyeti denenmeli.

Nmap port taraması yapılarak sisteme ait açık portları öğrenilmeli ve açık portlar hakkında bilgi toplanılmalıdır. (ftp,ssh username, ftp içindeki dosyalar vb.) nmap -Pn -sC -sV x.com-ip

**İstismar Etme**

Bulunan admin paneline yaptığımız bypass işlemi ile sunucuya girildi daha sonrasında uygun bir alana php reverse Shell yüklenip netcat ile bağlantı kurulmalı. Hedef sistemde sql açığı tespit edildi ve bunun üzerine sqlmap aracı ile database çekilebilir ve OSshell ile sistemde bağlantı kurulabilir. Dizin taraması sonucu upload.php dizini bulduk ve buraya php reverse Shell yükleyip netcatten bağlantı kurulmalı.

Xss açığı tespit etmiştik ve xss keylogger payloadları kullanılarak siteye giriş yapan kullanıcıların verileri ele geçirilebilir veya psikolojik baskıyı artırabilmek adına pop-up oluşturulabilir.

Nmap port taraması sonucu 21. Port açık görünmektedir. Nmap çıktısında 21. Portun altında Anonymous yani gizli kullanıcı ile giriş yapılabilceğini belirtmekte. ftp -p ip yazarak ve kullanıcı adına anonymous diyip şifreyi boş bırakırsak sisteme erişim sağlanabilirlik kazanılabilir. Nmap çıktısında ftp anonymous kullanıcısı bulunmamakta ve username görülmekte bunun üzerine hydra aracı ile ftp brute attack saldırısı ile ftp ye ait parolaya saldırı yapılmalıdır. ( hydra -l username -P wordlist.txt X.X.X.X ftp) Şifre bulunduktan sonrasında şirkete ait veriler çekilebilir ve reverse Shell yüklenip sisteme erişim sağlanılabilir.

Nmap port taraması sonucu 22. Port açık görünmektedir. Nmap çıktısında ssh’a ait username bulunmakta ve ssh ile sisteme bağlantı kurabilmek için hydra programı yardımıyla brute force attack saldırısı ile şifre denemesi yapılabilir. ( hydra -l username -P wordlist.txt X.X.X.X ssh) Tespit edilen şifre ile ssh [username@x.x.x.x](mailto:username@x.x.x.x) şeklinde sisteme erişim sağlanılır. Brute force saldırısından şifreyi bulunamadı fakat id\_rsa isimli bir dosya bulundu. Bu dosyayı indirip bulunduğumuz dizinde chmod 600 id\_rsa yazıp yetkilendiriyoruz. Ssh –i id\_rsa [username@x.x.x.x](mailto:username@x.x.x.x) yazarak sisteme erişim sağlanacaktır.

Nmap port taraması sonucu 23. Port açık görünmektedir. Terminale msfconsole yazarak metasploit programına geçilip versiyon bilgisine göre uygun auxilary aranmalı. Bulunan uygun auxiliary ile googledan sistem hakkında bilgi topladığımız olabilecek şifre listesini auxiliary’e yüklenip brute force attack saldırısı yapılıp şifre tespit edilmeli. Tespit edilen şifre ile terminale telnet x.x.x.x yazılarak hedef sisteme erişim sağlanılır.

Nmap port taraması sonucu 139. Port açık görünmektedir. Sisteme erişim sağlayabilmek için ilk önce terminale smbmap –H x.x.x.x yazılarak smb portundaki dizinler keşfedilir. Keşfedilen dizinler incelenmeli smbclient –l username [\\\\\x.x.x.x\\dizin](file://\x.x.x.x\\dizin) şeklinde çalıştırılıp sisteme giriş yapılır ve dosya indirme yükleme işlemleri yapılabilir.

Nmap port taraması sonucu 3306. Port açık görünmektedir. Sisteme erişim sağlayabilmek için terminale mysql –h hostname -u username@localhost yazarak sistemden data çekilebilir.

Hedef sisteme ait mail adreslerine sosyal mühendislik yöntemleri ile sunuculara karşı oltalama

**Yetki Yükseltme**

Netcat ve ssh ile bağlantı kurduğumuz yerlerde sudo –l komutunu çalıştarak root olabilmemiz için hangi dizinde çalıştığını görüntülenir. Görüntülenen dizini <https://gtfobins.github.io/> sitesinde aratarak sudo kısmındaki exploiti terminale yapıştırarak sistemde root olabiliriz veya githubtan exploit aratarakta bu işlemi gerçekleştirebiliriz, fakat sudo –l komutu çalışmadı (şifre ister şifreyi bilmiyorsak) o zaman cat /etc/passwd komutunu terminale yazarak hangi kullanıcının hangi dizinde çalıştığını görüntülenip root dizinini <https://gtfobins.github.io/> aratarak exploit arayıp root olmak için uğraşılır. Gtfobins sitesinden ulaşamadıysak githubtan exploit aranarak sistemde root olunabilir.

**Diğer Ağlara Sızma**

Domain’e ait ip adresini kopyalayarak dnsenum aracı ile subdomain ve ip blockları toplanır zafiyet tarama ve istismar etme konularındaki işlemler uygulanır. Domaine ait ip adresini site:x.x.x.x şeklinde google’ye yazılarak aynı ip adresine ait farklı sunucular çekilir(config çekme). Zafiyet tarama ve istismar etme konularındaki işlemler uygulanır.

**E-posta Servisi Testleri**

Müşteri Kurum’un e-posta servislerinde şu testler gerçekleştirilecektir.

* E-posta sunucularının topolojik konumu incelenecektir.
* Virüs tarayıcı ağ geçitlerinin sürüm bilgisi elde edilmeye çalışılacak bu sürümlerin bilinen açıkları araştırılacaktır.
* Sunucular üzerindeki yönlendirme (relaying) zafiyetlerini incelemek için bir dizi e-posta gönderilecektir.
* Sunucular üzerinde e-posta dışında bir servisin çalışıp çalışmadığı incelenecektir.
* E-posta sunucu üzerinde kimlik doğrulamanın aktif olup olmadığı incelenecektir.
* E-posta sunucu üzerinde POP3, IMAP gibi istemci servislerinin erişime açık olup olmadığı kontrol edilecektir.
* E-posta sunucular güvenlik taramasına tabi tutulacaktır.
* Sistemlerde kullanılan e-posta içerik kontrolcüleri, anti-virüs ağ geçitleri, spam filtrelerinin kullandığı kütüphanelerde var olabilecek muhtemel açıklıklar incelenecektir.
* E-posta servisini veren yazılımların bilinen diğer açıklıkları araştırılacaktır.
* E-posta servislerinin gönderilen e-postaların boyutlarını sınırlayıp sınırlamadığını kontrol etmek amacı ile boyutu büyük e-postalar gönderilecektir.
* Muhtemel olarak kullanılan e-posta listesi yazılımlarının açıklıkları tespit edilmeye çalışılacaktır.

**Kablosuz Ağ Sızma Testleri**

Müşteri kurumun sistemlerinde kablosuz ağlar ile ilgili şu testler gerçekleştirilecektir.

* Kurumda kullanılan kablosuz ağ cihazlarının genel mimari içindeki yeri incelenecektir.
* İstemcilerin kablosuz ağ yapılandırmaları incelenecektir.
* Kurumda bulunan kablosuz ağlar taranarak özellikleri keşfedilmeye çalışılacaktır
* Kablosuz ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenecektir.
* Kablosuz ağlarda kullanılan şifreleme ayarları incelenecektir.
* WEP ve WPA/WPA2 şifreleme kullanılan ağlarda kablosuz ağ şifresi ele geçirilmeye çalışılacaktır.
* İstemciler üzerinden kablosuz ağ taraması yapılarak, kurum etrafında bulunan diğer kablosuz ağlar keşfedilmeye çalışılacaktır.
* İstemciler üzerinden kablosuz ağ kullanılarak kurum dışına bağlantı yapılıp yapılamayacağı incelenecektir.

**Sosyal Mühendislik Testleri**

Müşteri Kurum’da çalışanların bilgi güvenliği farkındalıklarının sınanması amacıyla

aşağıdaki sosyal mühendislik saldırıları gerçekleştirilecektir.

* Sosyal ağlar, arama motorları, Müşteri Kurum web siteleri kullanılarak Müşteri Kurum ve çalışanları hakkında bilgi elde edilmeye çalışılacaktır.
* Müşteri Kurum içinden veya dışından yapılacak telefon görüşmeleri ile hassas bilgilere ulaşılmaya çalışılacaktır.
* Müşteri Kurum içinden veya dışından yapılacak telefon görüşmeleri ile hassas bilgilere ulaşılmaya çalışılacaktır.
* Müşteri Kurum’a sızabilmek için hazırlanan özel materyallerin kullanıcılar tarafından çalıştırılması amacıyla ortamlar hazırlanacaktır.
* E-mail yoluyla phishing (oltalama) ve backdoor ile kuruma sosyal mühendislik uygulanacaktır.

**Raporlama**

Raporlama penetrasyon testinin (pentest in) son ve en önemli aşamasıdır. Bu aşamada pentest esnasında bulunan açıklıklar ve çözüm önerileri, açıklıkların olası etkileri, açıklığın nasıl ele geçirilebileceği, açıklıkların dağılım grafikleri, uygulanan saldırı yöntemleri gibi detaylar hizmeti alan kuruma sunulmaktadır. Bulunan açıklar beş şekilde değerlendirilmelidir. Bunlar acil, kritik, yüksek, orta ve düşük.

**Yönetimsel Test Raporu**

* Belirlenen açıklar acil, kritik, yüksek, orta ve düşük şeklinde katogorilere ayrılacaktır.
* Belirlenen açıklar hakkında koruma altına alınması ile ilgili yüzelsel önerilerde bulunulacaktır.
* Sistemde belirlenen açıkların genel bakış açısı ile değerlendirilebilmesi için istatiksel bilgiler yazıyla ve grafikle sunulacaktır.

**Müşteri Test Raporu**

* kaBelirlenen açıkların güvenlik riskleri tagorilere ayrıştırılarak sunum halinde paylaşılacaktır.
* Sunumda kurumun bilgi güvenliği kapsamında güçlü ve zayıf yönleri anlatılacaktır.
* Bulunan açıklar bulguları ile anlatılıp, açığı kapatmak için detaylı öneride bulunulacaktır.
* Test sonucunda kurumun önerilere uyup uymadığı ile ilgili kontrol testi yapılacaktır ve bu test kurumun hazır olduğu dönemde uygulanacaktır.
* Bu kontrol testi sonucunda kurumun önerileri doğru algılandığından ve gerekli çalışmaların gerçekleştirildiğinden emin olunacaktır.

**Kaynakça**

**btyon:https://www.btyon.com.tr/pentest-penetrasyon-testi-nedir.php**

**Sağlık Bakanlığı:** [**https://bilgiguvenligi.saglik.gov.tr/**](https://bilgiguvenligi.saglik.gov.tr/)

**Tübitak bilgem: SIZMA TESTLERİ VE GÜVENLİK DENETLEMELERİ İŞ TANIMLAMA DOKÜMANI ŞABLONU SÜRÜM:1.1 30 Mart 2011**