T.C.
TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ REKTÖRLÜĞÜ
Bilgi İşlem Daire Başkanlığı

Konu : Teklife Davet

Üniversimiz Kurumsal Bilgi Sistemlerinin Güvenliğini Artırmaya Yönelik **(Sızma Testi Hizmet Alımı) İşi**, 4734 Sayılı Kamu İhale Kanunu'nun 22. Maddesinin (d) fıkrası uyarınca (**DOĞRUDAN TEMİN USULÜ**) alınacaktır. İlgilendiğiniz takdirde **K.D.V. hariç** fiyat teklifi göndermenizi rica ederim.

Salih AÇIK
Şube Müdürü
e-imzalıdır

Son Başvuru Tarih ve Saati	:	**06/07/2026 – 10:30**
Teklif Başvuru Yeri	:	Rektörlük Binası Bilgi İşlem Daire Başkanlığı 1. kat 313 nolu oda - Taşlıçiftlik Kampüsü TOKAT
Teslimat Yeri	:	TOGÜ- Bilgi İşlem Daire Başkanlığı
Teklif Türü	:	İşin Tamamı

İHTİYAÇ LİSTESİ

S.N.	MAL/İŞİN ADI, CİNSİ VE ÖZELLİĞİ	MİKTARI	KDV HARİÇ BİRİM FİYAT	KDV HARİÇ TUTAR
1	**" SIZMA TESTİ HİZMET ALIMI "**	**1 Adet**		
			KDV HARİÇ TOPLAM	

Ek: Teknik Şartname (15 Sayfa)

Yukarıda cinsi ve miktarı yazılı Hizmet Alımının TAMAMI KDV HARİÇ (RAKAMLA)₺……..……(YAZI İLE)…….……. TL karşılığında vermeyi / yapmayı taahhüt ederim.

Teslimat Süresi : ……..
KDV Oranı : ……..
Diğer Açıklamalar:

FİRMA KAŞE
ADI SOYADI İMZA

NOT:

1- Talep edilen malzeme/hizmet alımına ilişkin ödeme, Maliye Bakanlığı'nın ödenekleri serbest bırakma oran ve ilkeleri doğrultusunda malzemelerin muayene kabul ve teslim alınmasından sonra yapılacaktır.
2- Teklifler kapalı zarf içerisinde elden teslim edilebilir veya posta, kargo, faks yoluyla da gönderilebilir.
3- Teklif isteme yazımızda mal/malzeme/iş verilecek TOPLAM FİYAT üzerinden değerlendirmeye alınacaktır.
4- Şartlı teklifler ve Türk Lirası haricinde verilen teklifler değerlendirmeye alınmayacaktır.
5-Teslimat süresi değerlendirmede tercih nedeni olabilecektir.
6- Malzemelerin nakliyesi, kargo vb. giderler yüklenici firmaya ait olup, bunlar için ayrıca ücret talep edilmeyecektir.

Taşlıçiftlik Kampusü – TOKAT
Telefon (0 356) 252 16 10 Faks: (0 356) 252 16 35
e- posta: bidbsatinalma@gop.edu.tr web: www.gop.edu.tr
Bilgi İçin: Veysel GÜRSES / VHKİ. / Dahili No: 1618

TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ SIZMA TESTİ HİZMETİ (PENETRASYON) TEKNİK ŞARTNAMESİ - 2026

1. İŞİN KONUSU

Bu şartname **Tokat Gaziosmanpaşa Üniversitesi Bilgi İşlem Daire Başkanlığı** kurumsal bilgi sistemlerinin güvenliğini artırmaya yönelik, mevcut bilgi güvenliği alt yapısının analizi, raporlanması ve iyileştirilmesi çalışmalarını içermektedir. Sızma testinin hedefi kuruluşun sahip olduğu bilgi işlem altyapısının temel bileşenlerini oluşturan sunucular, aktif ağ cihazları, uygulama sunucuları, veri tabanları gibi standart ekipman ve yazılımlar ile kuruluşa özel geliştirilmiş, iş uygulamalarına yetkisiz erişim elde edilmesine veya hassas bilgilere ulaşılmasına neden olabilecek güvenlik açıklarının istismar edilmeden önce tespit edilmesi, risk düzeylerinin belirlenmesi hizmetidir.

2. TANIMLAR

İş bu teknik şartnamede kullanılan kelime ve deyimler, içinde geçtiği metin farklı bir anlam vermedikçe aşağıda tarif edildiği gibi anlaşılacaktır.

2.1. İDARE: Tokat Gaziosmanpaşa Üniversitesi
2.2. İŞ GÜNÜ: Resmî tatiller haricinde haftanın pazartesi, salı, çarşamba, perşembe, cuma günleridir.
2.3. SİSTEM: Tokat Gaziosmanpaşa Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından geliştirilen uygulamalar ve kurumun yerel ağı.
2.4. TARAFLAR: İDARE ve YÜKLENİCİ 'yi belirtir.
2.5. YÜKLENİCİ: İhaleyi kazanan, İDARE ile sözleşme yaptıktan sonra ihale konusu işi yapmaya yetkili ve aynı zamanda idari ve teknik açıdan sorumlu firma.
2.6. Sızma Testi Hizmeti Kapsam Listesi: İçerisinde sızma testi yapılacak olan web uygulamalarının ve alt ağların listelerinin olduğu dokümandır.

3. KISALTMALAR

3.1. DNS : Domain Name System
3.2. FTP : File Transfer Protocol
3.3. http : Hyper Text Transfer Protocol
3.4. HTTPS : Secure Hyper Text Transfer Protocol
3.5. ICMP : Internet Control Message Protocol
3.6. IP : Internet Protocol
3.7. LPT : Licensed Penetration Tester
3.8. NETBIOS : Network Basic Input/Output System
3.9. RPC : Remote Procedure Call
3.10. SNMP : Simple Network Management Protocol
3.11. TSE : Türk Standartları Enstitüsü

3.12. URL : Uniform Resource Locator
3.13. SIEM : Security Information and Event Management
3.14. ISO : International Organization and Standardization

4. KAPSAM

4.1. İdarenin bilişim sistemlerinde oluşabilecek güvenlik açıklıklarını veya zafiyetlerini azaltacak gerekli güvenlik taraması testlerinin yürütülmesi,
4.2. Şartnamede yer alan IP, uygulama, servis vb. tüm bileşenler,
4.3. Test ve denetim hizmetlerinin sağlaması gereken testlerin kapsamı aşağıda belirtilmiştir.
4.3.1. İç ağda yer alan bileşenlerde bulunabilecek zafiyetlerin taranması
4.3.2. Dış ağa açık bileşenlerde bulunabilecek zafiyetlerin taranması
4.3.3. Dışa açık web uygulamalarının sızma testleri
4.3.4. Veri tabanı yapılandırma testleri
4.3.5. Kuruma özel geliştirilmiş yazılımlar
4.3.6. DNS servisi testleri
4.3.7. E-posta servisi testleri
4.3.8. Sosyal mühendislik testleri
4.3.9. Güvenlik duvarı testleri
4.3.10. URL ve içerik filtreleme testleri
4.3.11. Ağ ve Sistem Altyapısı

5. GENEL ŞARTLAR

5.1. Yüklenici firma, yapılan testler ve rapor işlemlerinde kullanacak bütün yazılım, lisans ve cihazları kendisi temin etmelidir.
5.2. Yüklenici firma, bu teknik şartname kapsamındaki Projenin eksiksiz olarak tamamlanmasından mesuldür.
5.3. Yüklenici firma, bu projenin takibi için en az 3 (üç) kişiyi görevlendirecektir.
5.4. YÜKLENİCİ personeli, sistem üzerinde yapacağı her türlü iş, işlem ve müdahaleyi İDARE personeli eşliğinde/izniyle **kurum bünyesinde** yapacaktır.
5.5. Tüm Güvenlik test raporları, test hizmetlerinin tamamlanmasından sonra, en geç 15 (onbeş) iş günü içerisinde İDARE'ye teslim edilecektir.
5.6. Yüklenici, test ve değerlendirme çalışması sonucunda Detaylı Teknik Test Sonuç Raporu ile Yönetici Test Sonuç Raporu'nu hazırlayarak İdare'ye sunacaktır. Teknik rapor yeterince açık ve sözlü açıklamaya gerek bırakmayacak biçimde net olacaktır.
5.7. Denetim ve analiz sırasında ortaya çıkan kritik güvenlik konularının karşılıklı olarak görüşülerek hızlıca giderilmesi için çözüm önerileri sunulacaktır. Bu açıklıkların bildirimi için raporlama süreci beklenmeyecektir.
5.8. YÜKLENİCİ, Kuruluşumuz bilişim sistemlerinin İDARE'nin Bilgi Güvenliğini artırmaya yönelik tüm açıklıkları, zafiyetleri ve iyileştirilmesi gereken alanları tespit etmekten ve bunların kapatılması ve iyileştirilmesi amacıyla önerilerle birlikte

raporlanmasından sorumludur.

5.9. Dış ağ erişim noktaları ve iç ağ topolojisi idare tarafından yüklenici firmaya verilecektir. Bu verilen topolojiye göre ayrıntılı bütün iç ve dış IP numaraları için en az Layer 3 katmanında tarama yapılıp bütün açık port ve network topoloji haritası çıkartılacak bu haritaya göre uygun test altyapısı hazırlanıp bu topoloji üzerinden temel metodolojiye karar verilecektir.

5.10. Yapılacak testler en az 4 ana kısım üzerinden yürüyecektir. Bunlar iç ağdan yapılacak testler, dış ağdan yapılacak testler, servis testleri ve varsa diğer testler şeklinde kategorize edilecektir.

5.11. Dış ağdan yapılacak testler için farklı erişim noktalarından İdareye ait ve internet üzerinden erişilebilen sistemler test edilecektir.

5.12. Servis testlerinde ise idare bünyesinde çalışmakta bulunan sunucu servislerinin güvenlik açıkları test edilecektir.

5.13. Farklı test kategorilerindeki açıklar ve çözüm önerileri ayrı olarak raporlandırılacaktır.

5.14. İDARE'nin talep etmesi durumunda sözleşme sürecinde alınan tedbirler nedeniyle güvenlikten etkilenen veya envantere eklenen web ve mobil uygulamalar için ek ücret talep edilmeksizin kapsamın %10'u kadar uygulama, test edilmesi için Sızma Testi Hizmeti Kapsam Listesi(EK-1)'ne eklenebilecektir.

5.15. YÜKLENİCİ Proje kapsamında hazırlayacağı ve İDARE'ye sunacağı bütün dokümanları Türkçe olarak hazırlayacaktır. Teknik detaylar için İngilizce terimler kullanıldığı durumlarda parantez içinde Türkçesi yazılacaktır.

6. SIZMA TESTİNİN GİZLİLİĞİ VE YÜKLENİCİNİN SORUMLULUKLARI

6.1. İş bu şartname ile tanımlanan tüm yükümlülükleri yerine getirecektir.

6.2. Yüklenici yaptığı testler esnasında kuruluş çalışanlarının kişisel bilgilerine ulaşması durumunda, bu bilgileri kuruluş ile paylaşmamalı, sızma testi sonuç raporuna eklememeli ve bir kopyasını kendisine almamalıdır. Sızma test raporunda kullanıcı adı ve parolaları maskelenmelidir.

6.3. Testler yasadışı araçları veya yöntemleri içermemelidir. Testler esnasında kuruluş ile sözleşmede veya teknik şartnamede belirlenmiş olan kapsam dışına kuruluşun yazılı izni olmadan çıkılmamalıdır.

6.4. Bu şartnamede tanımlanan ve Yüklenici tarafından gerçekleştirilecek güvenlik denetimleri, sonuçları ve ilgili çalışmalar kapsamında elde edilen her türlü bilgi, Yüklenici tarafından gizli tutulacak ve elde edilen hiçbir matbu/elektronik belge kopyalanarak çoğaltılmayacaktır ve üçüncü taraflar ile paylaşmayacaktır. Sadece yüklenicinin içeriklere erişim sağlandığını gösterebilmesi için gerekiyorsa örnek olarak birkaç kayıt delil sağlamak amacıyla kopyalanabilecektir.

6.5. Yüklenici yasal olarak faaliyetlerine son vermesi durumunda, kendisinde bulunan sızma testi sonuç raporlarını geri dönülemez şekilde imha etmelidir.

6.6. İş başlangıcında İDARE tarafından yükleniciye verilen bilgi, dokümanlar ve iş sonunda Yüklenici tarafından hazırlanan raporlar, çıktılar, ekran görüntüleri vb. yükleniciye tesliminden sonra Yüklenici tarafından kesinlikle depolanmayacak ve 3. taraflarla

paylaşılmayacaktır. İşlerle ilgili tüm bilgiler (network topolojileri, kullanılan protokol bilgileri, güvenlik zafiyetleri, raporlar, vb.) aksi yazılı olarak belirtilmedikçe 'GİZLİ' olarak kabul edilecektir.

6.7. Raporlar özellikle sunumlarda kullanılmamalı ve örnek mahiyetinde diğer kuruluşlara gösterilmemelidir.

6.8. Yüklenici, hangi personelinin hangi testlerde görev aldığını dair kayıtları tutmalı ve en az 2 (iki) yıl süre ile bu kayıtları saklamalıdır.

6.9. Yüklenici ve Personel Yetkinlikleri

6.9.1. Yüklenici aşağıdaki belge veya sertifikaları karşılamalıdır:

a. Yüklenicinin A veya B TİPİ TSE SIZMA TESTİ FİRMA belgesine sahip olması,
b. Yüklenici bünyesinde TSE Sızma testi sertifikalı ve/veya kayıtlı personel/personellerin bulunması ve bu personellerin görevlendirilmesi.
c. Yüklenicinin ISO 27001:2022 sertifikasına sahip olması
d. Yüklenicinin Sanayi ve Teknoloji Bakanlığı Milli Teknoloji Genel Müdürlüğü Sızma Testi Yetki Belgesine sahip olması
e. Yüklenicinin Sanayi ve Teknoloji Bakanlığı Milli Teknoloji Genel Müdürlüğü Kamu Bilişim Yetki Belgesine sahip olması

7. ZAFİYET VE SIZMA TESTİ ÇALIŞMALARI

7.1. İdarenin Bilişim altyapısı güvenliği hem internet hem de yerel alan ağı (intranet) üzerinden denetlenecektir.

7.2. İdarenin domain ve subnetlerinde güvenlik açıkları ve bunların yarattığı riskler tespit edilecek, gerekli iyileştirmelere yönelik çözüm önerileri raporlanacaktır.

7.3. Yapılan analizler sonucunda güvenlik açığı tespit edilirse İdarenin iş akışında ne tür riskler oluşturacağı tespit edilecektir. Sonuçlar gizli bir rapor ile İdare'ye sunulacak ve bu açıklara karşı güvenliği arttırmak için iyileştirici çözüm önerileri de belirtilecektir.

7.4. Güvenlik Denetiminin sonucunda hazırlanan rapor İdareye bir toplantı ile sunulacaktır. Denetim ve analiz sırasında ortaya çıkan güvenlik konularının karşılıklı olarak görüşülerek hızlıca giderilmesi için çözüm önerileri sunulacaktır.

7.5. Yüklenici, denetim testleri sırasında İdare'nin internet hizmetlerinin kesintiye uğramamasını sağlamalıdır. Çalışmalar esnasında internet hizmetlerinin kesilmesi gerekli ise, çalışmalar Kurumun resmi mesai saatleri dışında İdarenin izni ile yapılabilecektir.

7.6. İdarenin bilişim mimarisinde bulunan ve şartname kapsamında belirtilen aktif cihazların, sunucuların ve yazılımlarının güvenlik açısından analizi yapılacaktır.

7.7. Sızma testi tek aşamalı olacaktır. Sızma testinin aşaması raporların sunumu ile bitecektir.

7.8. Çalışmalar neticesinde hazırlanacak raporun dili Türkçe olacaktır. Raporlarda tespit edilen zafiyetlerle ilgili yeterli seviyede detay bilgi verilecek, zafiyetin giderilmesi konusunda yapılması gerekli düzenlemelere ilişkin öneriler net biçimde yer alacaktır. Raporda yer alacak önerilerin uygulanması durumunda ortaya çıkacak olası etkiler belirtilecektir.

7.9. Yüklenicinin raporda belirteceği bütün bulgular elle kontrol edilmiş ve zafiyetin gerçekliği teyit edilmiş olmalıdır.

8. SIZMA TESTİ SÜRECİ

8.1. YÜKLENİCİ, sistemlerin güvenlik seviyesinin analizi için, kurum bünyesinde aşağıdaki çalışmaları gerçekleştirecektir.

8.2. İç Ağdan Gerçekleştirilecek Temel Sızma Testleri

8.2.1. Yerel ağda bulunan bütün ip bloklarında yer alan bilgisayarlar, sunucu ve cihazlarda tespit edilen açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma, bilgi kaçırma ve sistemlerine giriş testleri gerçekleştirilecektir.

8.2.2. Kurum bünyesinde iç ağda bulunan sunucular ve cihazlar üzerinde çalışmakta olan servislere ait kullanıcı adı ve şifreler tahmin edilerek sunuculara erişilmeye çalışılacaktır. Bu işlem için gelişmiş kullanıcı adı ve şifre tahmin etme programları kullanılacaktır.

8.2.3. Yerel ağ için zafiyet taraması yapılacaktır.

8.2.4. Kurum yerel ağında araya girme teknikleri ile hassas bilgiler elde edilmeye çalışılacaktır.

8.2.5. Elde edilen bilgiler ışığında kullanıcı bilgisayarları, sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırıları gerçekleştirilecektir.

8.2.6. Ele geçirilen sunucu ve kullanıcı bilgisayarları üzerinden daha kritik bilgilere ulaşılmaya çalışılacaktır.

8.3. Dış ağdan Gerçekleştirilecek Temel Sızma Testleri

8.3.1. İdareye ait internet erişimi için Ek-1 de yer alan dış IP adresleri için testler yapılacaktır.

8.3.2. İdareye ait dışarıya açık Ek-1 de yer alan normal web uygulamaları için sızma testi araçları ile otomatik testler yapılacaktır.

8.3.3. İdareye ait dışarıya açık Ek-1 de yer alan kritik web uygulamaları için sızma testi araçları ile otomatik testler, detaylı analizler için de elle taramalar yapılacaktır.

8.3.4. İdareye ait dışarıya kapalı Ek-1 de yer alan normal web uygulamaları için sızma testi araçları ile otomatik testler yapılacaktır.

8.3.5. İdareye ait dışarıya kapalı Ek-1 de yer alan kritik web uygulamaları için sızma testi araçları ile otomatik testler, detaylı analizler için de elle taramalar yapılacaktır.

8.3.6. İnternet güvenliği testlerinde Whitebox, Graybox, Blackbox metotlarından uygun olanı İdare ile birlikte belirlenip uygulanacaktır.

8.3.7. Zafiyet tespit edilmesi durumunda sadece tespit edilen bulgu raporlanıp test bitirilmeyecek, benzer ürünler için de tespit edilen bulguya yönelik taramalar devam edecektir.

8.3.8. İnternet güvenliği testleri kapsamında, İdare'nin domain ve alt alan adlarında, internet üzerinden erişilebilen IP adres aralığında çalışan sunucular için güvenlik zafiyeti taraması yapılacaktır.

8.3.9. Erişilen sunucular üzerindeki işletim sistemleri, sürümleri ve yamaları belirlenecektir.
8.3.10. Kullanılan güvenlik cihazları ve güvenlik uygulamaları tespit edilecektir.
8.3.11. Dışarıya hizmet veren DNS, web, e-posta, FTP vb. sunucuların kontrolü yapılacaktır.
8.3.12. SMTP, SNMP HTTPS, TELNET, ICMP, RPC, NETBIOS sık kullanılan servislere dışarıdan erişim testleri yapılacaktır.
8.3.13. İdare IP bloğunda bulunan zafiyetler sömürülerek hedef sistemlere erişilmeye çalışılacaktır.
8.3.14. İdare IP bloğundaki servislere kaba kuvvet saldırıları ile erişim elde edilmeye çalışılacaktır.
8.3.15. İdare'nin web sitesi ve dış IP adresleri siber istihbarat ürünü ile incelenerek skorlanacaktır.
8.3.16. Sızma testleri kapsamında minimum Aktif Cihazlar, Bilişim Güvenlik Sistemleri ve Sunucu Altyapısı testleri, DNS Servisleri testleri, Etki Alanı Sunucusu testleri, E-posta Sunucusu testleri, Veri tabanı Sistemleri testleri, Web Uygulamaları testleri, Sosyal Mühendislik testleri yapılacaktır. Birinci aşamada dışarıdan testler tamamlanacaktır.
8.3.17. Güvenlik Denetimi, İdare'nin merkez yerel ağ (LAN) sistemleri üzerinden ve Internet üzerinden gerçekleştirilecektir.
8.3.18. Internet'e açık çalışan sunucular üzerinde çalışan web uygulamalarının güvenliği denetlenecektir.
8.3.19. Sunucular ile ilgili açık portlar, kullanılan uygulamalar ve uygulamaların olası güvenlik açıkları kontrol edilecektir (VM, MIS, Mail, AD, DB vb. tüm sunucular).
8.3.20. İdarenin belirleyeceği ve Ek-1 de geçen aktif network cihazlarında güvenlik açıklarına karşı tarama yapılacaktır.
8.3.21. Merkezdeki omurga aktif network cihazlarının ve firewall cihazlarının konfigürasyon kontrolleri yapılacaktır.
8.3.22. Web sayfasının dışarıdan erişimlerde güvenlik açıklarının olup olmadığının kontrolü yapılacaktır.
8.3.23. İdare bünyesinde çalışan tüm web uygulamaları belirlenecektir.
8.3.24. Web sitesinin haritası çıkarılacak, uygulama girdi noktaları tespit edilecek ve kullanılan yönetim paneli belirlenecektir.
8.3.25. Hedef web sitesi, web sunucusu ve web servisi için kullanılan yazılım sürüm bilgileri belirlenecek, web yazılımlarına ait imza taraması yapılacak, hata mesajları incelenecektir.
8.3.26. Uygulamanın kullandığı veri tabanına sızılmaya çalışılacaktır.

8.3.27. SSL/TLS varsa versiyon, algoritma ve sertifika geçerlilik testleri yapılacaktır.
8.3.28. Hassas bilgilerin şifreli / şifresiz kanallardan aktarılıp aktarılmadığı kontrol edilecektir.
8.3.29. Hedef site üzerinde varsa tanımlı kullanıcılar belirlenecek, kullanıcı adı belirleme/doğrulama çalışmaları, kimlik doğrulama aşamasını atlatma denemeleri yapılarak, parola hatırlatma ve parola sıfırlama özellikleri test edilerek yetkili

kullanıcılara yönelik brute force parola denemeleri yapılacaktır.

8.3.30. Oturum yönetimi zayıflıkları, oturum yönetimi bypass testleri ve detaylı cookie güvenlik testleri gerçekleştirilecektir.

8.3.31. Oturum Sabitleme (Session Fixation) testleri, oturum değerleri tahmin saldırıları, CSRF (Cross Side Request Forgery) testleri, dizin atlatma/gezme (Directory Traversal) testleri, yetkilendirme atlatma/yetkilendirme geçiş testleri ve yetki yükseltimi testleri yapılacaktır.

8.3.32. Uygulamanın işleyişinin belirlenmesini takiben uygulamanın işleyişine yönelik teknik olmayan iş mantığı atakları yapılacaktır.

8.3.33. Yansıtılan/depolanmış/DOM tabanlı XSS testleri yapılacaktır.

8.3.34. SQL enjeksiyon / kod enjeksiyon testleri yapılacaktır.

8.3.35. İşletim sistemi komut enjeksiyon testleri, bellek taşması (buffer overflow) testleri, HTTP Response Splitting testleri ve hesap kilitleme politikasının testleri gerçekleştirilecektir.

8.3.36. Web servisi bilgi toplama çalışmaları, WSDL testleri, XML yapı testleri ve genel Ajax testleri yapılacaktır.

8.3.37. Web uygulama güvenlik duvarı keşif testleri ve network IPS keşif testleri tamamlandıktan sonra IPS / web uygulama güvenlik duvarı atlatma testleri gerçekleştirilecektir.

8.3.38. Yapılan analizlerin sonucunda Güvenlik Denetim Raporu hazırlanarak, bulunan güvenlik açıklarının ne gibi risklere sebep olduğu belirtilecektir. Raporda, bulunan açıklara karşı alınacak önlemler ile güvenliği arttırmak için gerekli iyileştirici öneriler yer alacak, sistemde tespit edilen güvenlik açıklarının taşıdıkları riskler itibariyle öncelikleri ve giderilmesi için yapılması gereken işlemler detaylı ve anlaşılır bir şekilde tarif edilecektir.

8.3.39. Raporlar bir toplantı ile sunulacak, teker teker açıklar üzerinden geçilecek, çözümü kimin yapacağı not alınacak ve rapor ilgili kişilere göre bölünerek ayrı ayrı tekrar verilecektir.

8.3.40. İdare bünyesinde dış IP üzerinden iç IP yönlendirilmesi yapılan sunucu sistemleri ve cihazlar üzerindeki açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma testlerinin gerçekleştirilecektir.

8.3.41. Üniversite bünyesinde dış IP üzerinden iç IP yönlendirilmesi yapılan sunucu üzerinde çalışmakta olan servislere ait kullanıcı adı ve şifreleri tahmin edilerek sunuculara erişilmeye çalışılacaktır. Bu işlem için gelişmiş kullanıcı adı ve şifre tahmin etme programları kullanılacaktır.

8.3.42. Bu sunucular ve cihazlar için dış erişim noktası üzerinden zafiyet taraması yapılacaktır.

8.3.43. Elde edilen bilgiler ışığında kullanıcı bilgisayarları, sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırıları gerçekleştirilecektir.

8.3.44. Ele geçirilen sunucu ve kullanıcı bilgisayarları üzerinden daha kritik bilgilere ulaşılmaya çalışılacaktır.

8.4. İletişim Altyapısı ve Aktif Cihazlar Sızma Testleri

8.4.1. Kurumda kullanılan ağ cihazlarının genel mimari içindeki yeri incelenecektir.
8.4.2. Tüm ağ cihazları açıklık bulma araçları ile taratılacaktır.
8.4.3. Tespit edilen açıkların uygulanabilirlikleri sınanacaktır.
8.4.4. Ağlarda MAC adresi tabanlı filtrelemenin olup olmadığı incelenecektir.
8.4.5. Aktif cihaz üzerindeki port güvenliği, VLAN ve trunk yapısı incelenecektir.
8.4.6. Ağ topolojisi ve segmentasyonu incelenerek kullanıcı-sunucu ağları arasında erişim kontrolünün olup olmadığı denetlenecektir.
8.4.7. Aktif cihaz üzerinde çalışan servisler incelenecektir.
8.4.8. Kullanılan servislerin servis dışı bırakılmayla sonuçlanabilecek saldırılara karşı (ARP zehirlemesi, CDP DoS, DHCP DoS, SNMP DoS vb.) durumu incelenecektir.
8.4.9. Cihazlar üzerinde açık olan Telnet, HTTP, FTP, SNMP, TFTP, SSH servislerine sözlük saldırısı veya kaba güç kullanılarak erişim sağlanmaya çalışılacaktır.
8.4.10. Erişim sağlanan cihazlar üzerinden alınan bilgilerle diğer cihazlara erişilmeye çalışılacaktır.
8.4.11. Aktif cihazlar için uzak/yerel erişim kontrolü, yönetim, kayıt ve kimlik doğrulama mekanizmaları incelenecektir.
8.4.12. Cihazların merkezi şekilde yönetilmesini ve gözetlenmesini sağlayan yönetim sistemlerinin varlığı araştırılıp, bu sistemlere sızma girişimlerinde bulunulacaktır.
8.4.13. Cihazlarda ortak parolanın kullanılıp kullanılmadığı test edilecektir.
8.4.14. Kurum çalışanları için kullanılan içerik filtreleme sistemleri atlatılmaya çalışılacaktır.
8.4.15. Kurum içinden dışarı tünel kurulmasıyla, kurum dışından kurum içine yetkisiz bağlantı gerçekleştirilmeye çalışılacaktır.
8.4.16. Kurumda kullanılan ağ cihazlarının genel mimarı içindeki yeri incelenecektir.
8.4.17. Cihazların tespiti yapılacaktır.
8.4.18. Tespit edilen cihazların marka, model ve sürüm belirlenecektir.
8.4.19. İş gereksinimlerine göre cihazın kullanım şeklinin değerlendirilmesi yapılacaktır.
8.4.20. Ön tanımlı parola ve ayarların kontrolü yapılacaktır.
8.4.21. Üretici yamaları ve uygulanması incelenecektir.
8.4.22. Ele geçirme saldırıları yapılacaktır.
8.4.23. Aktif cihaz üzerinde çalışan servisler incelenecektir.
8.4.24. MTM (Man In The Middle) kontrolleri yapılacaktır.

8.5. DNS Servisleri Güvenlik Testleri

8.5.1. DNS sunucuların topolojik incelenmesi yapılacaktır.
8.5.2. DNS Sunucusunun alan yapılandırmasında yer alan kayıtların ortaya çıkartılması
8.5.3. Sunucu üzerinden alan transferi (zone transfer) yapılmaya çalışılacaktır.
8.5.4. NXT ve NSEC kaynak kayıtları üzerinden bilgiler elde edilmeye çalışılacaktır.
8.5.5. Pasif sorgularla bilgi toplanacaktır.

8.5.6. DNS sunucular için ön bellek zehirlemesi kontrolü yapılacaktır.
8.5.7. DNS sunucular üzerindeki kaynak kayıt girdileri kontrolü yapılacaktır.
8.5.8. DNS sunucuların sürüm bilgisi incelenecektir.
8.5.9. Kurum dışı alan adı sorgularının kontrolü yapılacaktır.
8.5.10. Sunucular üzerinde DNS dışında bir servisin çalışıp çalışmadığının kontrolü yapılacaktır.
8.5.11. Güvenlik Duvarında DNS sunucular için izin verilen ayarların kontrolü yapılacaktır.
8.5.12. DNS sunucuların zafiyet taraması yapılacaktır.
8.5.13. DNS servisini veren yazılımın açıklıkları araştırılacaktır.
8.5.14. DNS sunucuların topolojik konumu incelenecektir.
8.5.15. Netcraft, Google, Whois sorguları yapılarak Kurum ağında yer alan sunucular tespit edilmeye çalışılacaktır.
8.5.16. DNS sunucular üzerindeki ters kaynak kayıt girdileri incelenecektir.
8.5.17. Elde edilen açıklar ve çözüm önerileri Servis Testi raporunda belirtilecektir.

8.6. Etki alanı ve Kullanıcı Bilgisayarları Güvenlik Testleri

8.6.1. Kullanıcı bilgisayarlarının açılış ayarlarındaki eksiklikler tespit edilip, yerel yönetici hakları elde edilmeye çalışılacaktır.
8.6.2. Yerel yöneticilerin kullanımındaki zafiyetler ile hak yükseltme saldırıları gerçekleştirilecektir.
8.6.3. Etki alanındaki şifre politikası ve şifre saklama politikasındaki zafiyetler tespit edilip, kullanıcı hesaplarının şifreleri ele geçirilmeye çalışılacaktır.
8.6.4. Yama yönetimindeki zafiyetler ve desteği kaldırılmış eski sistemler tespit edilip, uzaktan kod çalıştırma ve hak yükseltme saldırıları gerçekleştirilecektir.
8.6.5. Yetkisiz erişime imkân tanıyan dosya paylaşımları tespit edilerek, bu paylaşımlar ve paylaşımlardaki hassas veriler yoluyla hak yükseltme saldırıları gerçekleştirilecektir.
8.6.6. Hak yükseltme saldırıları ile etki alanı kullanıcılarının hesapları ele geçirilmeye çalışılacaktır.
8.6.7. Etki alanında yönetici haklarına sahip kullanıcı hesapları ve kullanıcı hesabı gruplarının kullanımındaki zafiyetler kullanılarak hak yükseltme saldırıları gerçekleştirilecektir.
8.6.8. Elde edilen şifre ve haklar ile hassas bilgilerin bulunduğu sunucu ve kullanıcı bilgisayarlarına erişim sağlanmasına çalışılacaktır.
8.6.9. Etki alanında güvenlik politikaları kontrol edilecektir.
8.6.10. Etki alanındaki yetkili kullanıcıların ayrıcalıkları ve kullanım şekilleri kontrolleri sağlanacaktır.
8.6.11. Yama yönetimi politikaları kontrol edilecektir.
8.6.12. Virüs koruma politikaları kontrol edilecektir.
8.6.13. Hassas bilgi içeren ve yetkisiz erişime olanak sağlayan paylaşım kontrolleri yapılacaktır.
8.6.14. Taşınabilir aygıtların kullanımı ile ilgili güvenlik ayarları
8.6.15. Yerel kullanıcı hesabı ve kullanıcı grupları kontrolleri yapılacaktır.
8.6.16. Bilgisayarların fiziksel saldırılara karşı güvenilirliği

8.7. E-posta Servisleri Güvenlik Testleri

9.7.1.E-posta sunucularının topolojik konumu incelenecektir.
9.7.2. Virüs tarayıcı ağ geçitlerinin sürüm bilgileri elde edilmeye çalışılarak bu sürümlerin bilinen açıklıkları araştırılacaktır.
9.7.3. Anti-spam ağ geçitlerinin kurum dışı sahte e-postalara karşı davranışı incelenecektir.
9.7.5.E-posta sunucusu üzerinde kimlik doğrulamanın aktif olup olmadığını incelenecektir.
9.7.6.E-posta sunucuları güvenlik taramasına tabi tutulacaktır.
9.7.7.Sistemlerde kullanılan e-posta içerik kontrolcüleri, anti-virüs ağ geçitleri, spam filtrelerinin kullanıldığı kütüphanelerde var olabilecek muhtemel açıklıklar incelenecektir.
9.7.8.E-posta servisini veren yazılımların bilinen diğer açıklıkları araştırılacaktır.
9.7.9. Eposta sunucular üzerinde başka servislerin tespiti kontrol edilecektir.
9.7.10. Eposta sunucusu üzerinde ilgili servislerin kontrolleri (IMAP, POP3) yapılacaktır.
9.7.11. Zafiyet taraması yapılacaktır.
9.7.12. İzin verilen eposta boyutu kontrolü yapılacaktır.
9.7.13. Eposta liste uygulamalarının zafiyet taramaları yapılacaktır.

8.8. Veri tabanı Sistemleri Güvenlik Testleri

8.8.1. Sistemdeki veri tabanı uygulamaları ve bu uygulamaları üzerinde barındıran işletim sistemleri tespit edilerek, tespit edilen bu sistemlere erişimin açık olup olmadığı denetlenir ve erişimin açık olması halinde çeşitli tarama araçlarıyla veri tabanı sürümü, üretici adı gibi bilgiler ele geçirilmeye çalışılacaktır.
8.8.2. Elde edilen veri tabanı sistem bilgileri kullanılarak, bu sistemlere yönelik kullanıcı adı ve parola deneme saldırıları yapılacaktır. Bu saldırılar sırasında, ön tanımlı kullanıcı adı ve parolaların denenmesinin yanında, kuruma özel olabilecek ve tahmin edilebilir kullanıcı adı ve parolalar da denenecektir.
8.8.3. Veri tabanı kullanıcı adı ve parola saldırılarının başarısız olması durumunda, işletim sistemi seviyesinden erişim denemeleri yapılacaktır. Windows, Linux ve diğer ortamlar üzerinden sistem kullanıcıları ile veri tabanı uygulamasına bağlanılmaya çalışılacaktır.
8.8.4. Parola deneme saldırılarının başarılı olması durumunda tespit edilen erişim bilgileriyle sistemlere bağlanılacaktır. Bağlanılan sistemlerde hangi hassas verilerin bulunduğu, kullanıcı adı, parola ve parolalara ait karmaşıklaştırılmış özet verilerinin bulunup bulunmadığı denetlenecektir.
8.8.5. Görüntülenebilen kullanıcı adı ve parola özet bilgileri çeşitli araçlarla tespit edilmeye çalışılarak zayıf olarak belirlenmiş parolalar tespit edilecektir.
8.8.6. Erişilebilen sistemlerde yama bilgisi kontrol edilir. Bilinen açıklıkları içeren ve gerekli güncellemeleri yapılmamış sistemlerde hak yükselme gibi saldırılarla erişim sağlanan kullanıcının hakları genişletilmeye çalışılacaktır.
8.8.7. Erişilebilen sistemlerden diğer erişilemeyen sistemlere tanımlanmış bağlantılar varsa bu bağlantılar kullanılarak diğer veri tabanı uygulamalarına geçilmeye çalışılacaktır.
8.8.8. Hassas verileri ihtiva eden sistemlere erişilmesi halinde yetki seviyesi arttırılmaya

çalışılır. Erişim bilgisi elde edilecek sistemlerin sayısı arttıkça, her sistem için yukarda bahsi geçen adımlar tekrarlanır ve mevcut tüm veri tabanlarının güvenliği bu şekilde kontrol edilecektir.

8.8.9. Veri tabanı sunucusunun topolojik konumu incelenecektir.
8.8.10. Yamaları kontrol edilecektir.
8.8.11. Veri tabanı için önemli olan işletim sistemi dosyalarının erişim izinlerinin incelenecektir.
8.8.12. Veri tabanı sunucusunun güvenlik ayarları kontrol edilecektir.
8.8.13. Veri tabanı sunucusunun parola politikası, kullanıcı hesapları güvenlik ayarları kontrol edilecektir.
8.8.14. Veri tabanı sunucusunda, güvenlik açısından önemli olan paketler, nesneler, roller, tablo ve hakların kontrolü sağlanacaktır.
8.8.15. Veri tabanı sunucusunda, denetleme mekanizmasının kontrolü sağlanacaktır.
8.8.16. Veri tabanı sunucusunun yedekleme ve kurtarma mekanizması kontrol edilecektir.
8.8.17. Veri tabanının kurulumu ile birlikte gelen ve kullanıcılar için atanan varsayılan değerlerin kontrolünü yapılacaktır.
8.8.18. Uzaktan erişimin güvenlik kontrolleri yapılacaktır.

8.9. Web Uygulamaları Güvenlik Testleri

Aşağıdaki maddeler kontrol edilecektir.

8.9.1. Veri Kontrolleri
- 8.9.1.1. Girdi denetimi
- 8.9.1.2. Çıktı denetimi
- 8.9.1.3. Değiştirilen içeriğin tespiti
- 8.9.1.4. HTML etiketlerinin filtrelenmesi
- 8.9.1.5. SQL injection
- 8.9.1.6. Sunucu taraflı girdi denetimi
- 8.9.1.7. URL yönlendirmeler
- 8.9.1.8. Diğer injection
- 8.9.1.9. XSS
- 8.9.1.10. HTTP yanıt bölme
- 8.9.1.11. HTTP başlık değiştirme
- 8.9.1.12. HTTP form değiştirme
- 8.9.1.13. Bellek taşma

8.9.2. Oturum Yönetimi
- 8.9.2.1. Giriş sonrası oturum bilgisi yenileme, oturum sabitleme
- 8.9.2.2. Çerezlerin içeriği
- 8.9.2.3. Oturum sonlandırma
- 8.9.2.4. Oturum bilgisinin URL içinde taşınması
- 8.9.2.5. Oturum çalma (Session riding)
- 8.9.2.6. CSRF
- 8.9.2.7. Çerez değiştirme

8.9.3. Kimlik yönetimi, doğrulama ve iş mantığı
- 8.9.3.1. Yetki artırımı
- 8.9.3.2. Yetki dışı işlem

8.9.3.3. Şifre politikaları
8.9.3.4. Bilinen hesap/şifre bileşenlerinin denenmesi
8.9.3.5. Basit kimlik doğrulama kullanımı
8.9.3.6. Kimlik doğrulamanın atlatılması
8.9.3.7. Çıkış işlevi
8.9.3.8. Path traversal
8.9.3.9. Bypass authorization
8.9.3.10. Privilege escalation
8.9.3.11. Uygulama mantığı kontrolleri
8.9.3.12. Kaba-kuvvet kullanarak parola tespit testleri
8.9.3.13. Yetkilendirme mekanizmasını devre dışı bırakma testleri

8.9.4. Web Servis Testleri
8.9.4.1. Web servislerin tespiti
8.9.4.2. Web servisi detay tarama
8.9.4.3. REST
8.9.4.4. SOAP
8.9.4.5. Ajax
8.9.4.6. Bilgi Sızdırma ve Ayar Yönetim
8.9.4.7. Yardım sayfaları
8.9.4.8. SSL kullanımı
8.9.4.9. HTML comment
8.9.4.10. Sunucu bilgisi
8.9.4.11. Ayrıntılı hata mesajları
8.9.4.12. Dosya uzantıları
8.9.4.13. Yedek dosyalar
8.9.4.14. Yönetici ara yüzü
8.9.4.15. Desteklenen HTTP metotları ve XST açıklığı
8.9.4.16. Sitenin SSL sertifikasının geçerlilik testi
8.9.4.17. Metadata kontrolleri
8.9.4.18. Diğer sistemlerle iletişim ve veri aktarımı güvenliği testleri
8.9.4.19. Veri tabanı servisleri denetimi
8.9.4.20. Veri tabanı yetkisiz erişim denetimleri,
8.9.4.21. Uygulama sunucusu servisleri denetimi,
8.9.4.22. Komut enjeksiyonu (OS, SQL, SSI, XPATH vb. komutları) testleri,

8.9.5. Hizmet Dışı Bırakma
8.9.5.1. Güvenlik resmi (Captcha) kullanımı
8.9.5.2. Web Server hizmet dışı bırakma saldırısı
8.9.5.3. İstemci talebine uyarınca bellekte nesne oluşturmak (User specified object allocation)
8.9.5.4. Fazla veri döndüren işlemler

9. TEKNİK HUSUSLAR

9.1. Sızma testini yapacak Yüklenici; iş bu şartnamede işin kapsamında belirtilen her proje için tanımlanan işleri (bundan sonra tümü "iş" olarak ifade edilecektir) gerçekleştirecek

ve iş sonunda Sızma ve Zafiyet Testi raporlarını hazırlayarak İdareye sunacaktır.

9.2. Sızma testini yapacak Yüklenici; iş bu şartnamede işin kapsamında belirtilen her proje için tanımlanan işleri ve çalışacak personeli Proje Planında belirtecek ve yazılı/e-posta ile İdareye bildirecektir. İdarenin yazılı bildirimi veya e-posta cevabı olmadan iş kapsamında herhangi bir çalışma yapılamaz, İdare'nin onay vermediği kişi/kişiler çalıştırılamaz veya mevcut kişi/kişiler değiştirilemez.

9.3. Test yapılacak sunucu bilgileri İdare tarafından verilecektir.

9.4. Sızma ve zafiyet testi yapılacak olan sunucular için, işin yapılmasında ihtiyaç duyulan bilgi ve dokümanlar (network topolojisi, kullanılan IP bilgileri, proje iç işleyiş bilgileri vb.) İdare tarafından Yükleniciye verilecektir.

9.5. İdare, Sızma testlerinde, whitebox, blackbox, graybox yöntemlerinden bir veya birkaçının kullanılmasını isteyebilecektir.

9.6. İş kapsamında yapılacak olan Sızma ve Zafiyet testlerinin hedefi olacak bilgi sistemleri üzerinde oluşabilecek olası hizmet kesintileri ve/veya sistemlere verilebilecek zararlar, testler yapılmadan en az 2 (iki) gün önce İdareye yazılı/e-posta olarak bildirilecektir. İdarenin onayı ile ilgili çalışmalar yapılacaktır. Yapılacak olan tüm çalışmalar planlı olacaktır.

9.7. İş kapsamında yapılacak olan Sızma ve Zafiyet testlerinde sistem kesintilerini en aza indirgeyebilmek için kullanılan tarama araçlarında "health check" seçeceği aktif edilerek taramalar yapılacaktır.

9.8. İş sonucunda hazırlanacak olan ilgili raporlarda;

Tespit edilen güvenlik zafiyetleri, ekran çıktıları ve/veya video görüntüleri,
Bu zafiyetlerin sebep olabileceği zararlar/sonuçlan ve zafiyete ilişkin referans bilgileri, Güvenlik zafiyetlerini gidermek için yapılması gerekenler,

detaylı şekilde açıklanacaktır.

9.9. İş sonucunda oluşturulan raporlar hem basılı hem de elektronik ortamda Microsoft Word ve Pdf formatında İdare'ye sunulacaktır.

9.10. İş sonucunda üretilmiş olan raporların tüm telif hakları İdareye ait olacaktır. Raporlar, İdareye özelleştirilmiş, İdare logolu ve Yüklenici logolu olarak iki ayrı formda sunulacaktır.

9.11. İş kapsamında Yüklenici tarafından yapılacak işlerin tamamı ya da bir kısmında İdare'nin belirleyeceği İdare personeli/personelleri gözlemci olarak bulunabileceklerdir.

9.12. İş kapsamında hazırlanan sızma ve zafiyet test' raporunda projeler için tespit edilen zafiyetler raporlanacaktır.

9.13. İş kapsamında hazırlanan sızma ve zafiyet testi raporunda tespit edilen güvenlik zafiyetleri kritiklik seviyelerine (kritik, yüksek, orta, düşük) göre gruplandırılacak ve sınıflandırmanın nasıl yapıldığı ilgili raporda açıklanacaktır.

9.14. İş kapsamında hazırlanan sızma ve zafiyet testi raporunda, tespit edilen bir güvenlik zafiyeti, söz konusu zafiyeti bulunduran sistemler bazında gruplandırılmalıdır.

9.15. İş kapsamında hazırlanan sızma ve zafiyet testi raporunda, tespit edilen her güvenlik

zafiyeti için alınması gereken önlem/önlemler Yüklenici tarafından belirlenmeli ve raporlanmalıdır.

9.16. İş kapsamında yapılacak olan sızma ve zafiyet testlerinde İdare iç ağının (intranet) ve/veya sistem salonlarının kullanılması, gerekliği durumda işi yapacak olan Yüklenici personeli, ilgili lokasyona İdare izni ile girecek ve işini Bilgi İşlem Dairesi Başkanlığı personelinin refakati ile yapacaktır.

9.17. İş kapsamında kullanılacak olan tarama yazılımları, uygulama sunucu yazılımları vb. yazılımlar ve lisansları Yüklenici tarafından temin edilecektir. İdare lisanslama ile ilgili herhangi bir yükümlülüğe girmeyecektir. Tüm lisans sorumluluğu Yükleniciye aittir.

9.18. Kapsama dahil edilecek sistemler için yapılacak olan envanter çalışması sonrası Küçük, Orta, Büyük seviyeleri arasından proje büyüklüğü belirlenecektir. Ayrıca projede bulunan uygulamalara göre yöntemler arasından uygun sızma analiz yöntemleri belirlenecektir.

9.19. İş kapsamındaki sistemler üzerinde Yüklenici tarafından yapılacak sızma ve zafiyet testleri, projenin topolojisine göre hem internet hem intranet üzerinden yapılacaktır. Yüklenici bu iş için ilave ücret talep etmeyecektir.

9.20. İş kapsamında yapılacak olan sızma ve zafiyet testlerinde kullanılması gerekebilecek olan test kullanıcı hesapları ve özel kullanıcı bilgileri (credentials) İdare tarafından Yüklenicinin kullanımına verilebilecektir. Söz konusu bilgilerin uygulama bazlı olarak verilip/verilmeyeceğine İdare karar verecektir.

9.21. İş kapsamında hazırlanan raporların tümünde yönetici özeti bulunmalıdır.

9.22. İş kapsamında hazırlanan raporlar, tespit edilen açıklar kullanılarak gerçekleştirilen bir atak bulunması durumunda ekran görüntülerini ve/veya video çekimlerini içermelidir.

9.23. İş kapsamında yapılan çalışmaları, hazırlanan raporları, tespit edilen açıkları ve bu açıkları giderme yöntemlerini görüşmek üzere yapılacak tüm toplantılara İdarenin talep etmesi halinde Yüklenici katılım sağlayacaktır. Yüklenici bu işler için ayrıca ücret talep etmeyecektir.

10. DİĞER HUSUSLAR

10.1. Sızma testini yapacak Yükleniciden istenen sertifikalar, bu sözleşme kapsamında tek bir personelde toplanamaz.

10.2. Sızma testini yapacak Yüklenici bu özelliklere sahip personellerinin sözleşme aşamasında çalıştığını gösteren SGK bildirgelerini, özgeçmişini, sertifikalarını ve diplomalarını sözleşme aşamasında kuruma sunacaktır.

10.3. Tüm proje bilgileri elektronik formatta belgelenerek İdare'ye teslim edilecektir.

10.4. Belgeler şifreli bir şekilde teslim edilecek, şifre ayrı olarak gönderilecektir.

10.5. Belgeler teslim edildikten sonra detaylı bir toplantı ile tüm maddeler anlatılacaktır.

Sızma Testi Hizmeti Kapsam Listesi(EK-1)

Sunucu Sayısı	100 adet
İç IP Adresleri Sayısı	**4000 adet**
Domain adı	gop.edu.tr
Çalışma Lokasyonu	Tokat Gaziosmanpaşa Üniversitesi Taşlıçiftlik Kampüsü
Dış IP Adresleri	**193.140.180.0/24 193.140.182.0/24**
Sosyal Mühendislik (e-posta ile)	3800 adet e-posta adresi için uygulanacaktır.
Web Sunucu Sayısı	10 adet
Web Uygulama Sayısı	12 adet
URL Adresleri	12 adet adres uygulama aşamasında verilecektir.
Active Directory Sayısı	1 adet
DNS Sayısı	2 adet
Mail Sunucu	1 adet
DHCP Sunucu	1 adet

Engin TÜRK
Öğretim Görevlisi

Şakire YÜCE
Tekniker

Mustafa KAPLAN
Mühendis