BGA SECURITY SIZMA TESTLERİ KONTROL LİSTESİ

BGA Security Sızma Testleri Kontrol Listesi

Her an yeni bir güvenlik zafiyetinin yayınlandığı siber dünyada kurumları tehditlere karşı korumak amacıyla geliştirilen yöntemlerden biri sızma testleridir.

Sızma testleri, kurumların anlık güvenlik açısından resimlerinin çekilmesi ve önerilerin sunulmasından ibaret olmasına rağmen çoğu kurum sızma testi aldık artık güvendeyiz şeklinde yaklaşımlar sergilemektedir.

Sızma testlerini gerçekleştirmek üzere bu yola giren çoğu kişinin bir zaman sonra karşılaşacağı temel maddelerden birisi meslek körlüğüdür. Her saat aynı işle uğraşan kişiler uğraştığı konuda ne kadar uzmanlaşırsa uzmanlaşsın bir müddet sonra farklı zamanlarda aynı sistemi incelediğinde farklı güvenlik zafiyetleri tespit edememeye başlayacaktır.

Sızma testi yapan firmaların karşı karşıya kalacağı en kötü durum hizmet verdiği firmanın güvenlik problemi yaşamasıdır. Çoğu firma maliyet ve benzeri nedenlerden dolayı sızma testi yaptırırken kapsamı dar tutmakta ve kendilerince önemli, kritik sunucuları teste tabi tutturmaktadır. Oysaki siber saldırganlar için önemli veya önemsiz sistem yoktur. Sisteme giriş için kullanılacak bir yol gereklidir ve genellikle kötü niyetli kişilerin sistemlere girerken kullandıkları yol kurum açısından en değersiz, göz önünde olmayan sistemlerdir.

Sızma testlerini gerçekleştirirken dikkat edilmesi gereken diğer önemli bir hususta sızma testi gerçekleştirecek kişi veya firmaların sızma testinde hangi noktalara baktığının somut olarak ortaya konmasıdır. Tamamen kişisel güven esasına dayalı olarak yürüyen bu sistem (sızma testinde neleri kontrol ettiği kişinin aklındadır, yazılı değildir) sonucunda aynı firmaya farklı sızma testi uzmanları tarafından gerçekleştirilen denetimlerin sonuç raporları oldukça farklı çıkabilmektedir.

BGA Security olarak 2013 yılında 13 farklı başlıkta yaklaşık 400 farklı maddeden oluşan **"Sızma Testi Kontrol Listesi"** hazırladık. Kontrol listemizde uzmanlarımızın tecrübelerinden faydalanarak aşağıdaki maddeleri ve gereklilik listelerini ortaya çıkardık.

Sızma testinde kişisel uzmanlık önemli fakat yapılan işlerin kişiden bağımsız olarak tekrar edilebilmesi, hangi test maddelerinin başarıyla sonuçlandığının, hangi test maddelerinin başarısız olduğunun ortaya konması (böylece kurumun sadece eksik yanları değil, güçlü yanları da ortaya çıkmaktadır.)

Halihazırda dokümanımızda hangi test adımının hangi araçlar kullanılarak nasıl gerçekleştirileceği de adım adım yazılıdır.

NOT: Yakın zamanda detaylı Wiki sayfası olarak yayınlanacaktır.

Kontrol Listesi

DNS GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ ve AÇIKLAMASI
PT-01	DNS	DNS portlarının (UDP/53, TCP/53) kontrol edilmesi (IP/Subnet)
PT-02	DNS	DNS sunucu yazılım/platform bilgilerinin belirlenmesi
PT-03	DNS	DNS yazılımında bulunan güvenlik zafiyetlerinin belirlenmesi
PT-04	DNS	DNS Zone transferine açık olup olmadığının belirlenmesi
PT-05	DNS	DNS sunucuda kayıtlı alan alt adlarının belirlenmesi (brute force)
PT-06	DNS	Genele açık DNS hizmeti (R DNS) verilip verilmediğinin belirlenmesi
PT-07	DNS	DNS sunucunun "." isteklerine cevap durumunun belirlenmesi
PT-08	DNS	Alt domain keşfi için brute force denemelerinin gerçekleştirilmesi.
PT-09	DNS	Arama motorları kullanarak alt domain keşfi
PT-10	DNS	DNS cache poisoninge açık olup olmadığının belirlenmesi
PT-11	DNS	DNS cache snooping etkilenme durumunun belirlenmesi
PT-12	DNS	TXT,HINFO ve NSEC kayıtlarından bilgi ifşası kontrolü
PT-13	DNS	DNS sunucuya yönelik tam kapsamlı Nessus taraması
PT-14	DNS	DNSSEC ve EDNS0 desteği olup olmadığının tespiti (DoS icin)

E-POSTA GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ ve AÇIKLAMASI
PT-15	MAIL	SMTP Versiyon Belirleme/Fingerprinting (25, 465, 587)
PT-16	MAIL	E-posta sistemine yönelik zafiyetlerin kontrolü
PT-18	MAIL	Belirli e-posta adreslerinin sistemde olup olmadığının belirlenmesi
PT-19	MAIL	MX kaydı olmayan alan adlarından e-posta kabul kontrolü
PT-20	MAIL	Firma içinden geliyormuş gibi e-posta gönderim testi
PT-21	MAIL	MTA mail geçirme (Open Relay) Testleri
PT-22	MAIL	Çeşitli zararlı yazılım içeren pdf/exe/ofis belgelerinin e-posta ile gönderilerek AV atlatma testleri
PT-23	MAIL	Eposta filtreleme sistemlerini şifreli veri gönderilerek atlatma testleri
PT-24	MAIL	SPF kaydı olmayan adreslerden mail kabul etme kontrolü
PT-25	MAIL	SMTP üzerinden iç ağ ve Dmz ip yapılandırması IP keşif çalışması
PT-26	MAIL	SMTP kimlik doğrulama testleri
PT-27	MAIL	EXPN ve VRFY desteği kontrolü, sistem kullanıcısı tespiti
PT-28	MAIL	POP ve IMAP servislerine yönelik brute force denemeleri
PT-29	MAIL	E-posta harici başka servislerin açık olup olmadığının testleri
PT-30	MAIL	İşletim sistemine yönelik güvenlik zafiyet taraması
PT-31	MAIL	E-posta DoS testi amaçlı büyük boyutlu dosyaların gönderilmesi
PT-32	MAIL	Tek kaynaktan yüklü sayıda e-posta gönderimi [DOS]

PT-33	MAIL	Zip bomb gönderilerek Antivirus yazılımının kontrolü [DoS]
PT-34	MAIL	Kurum IP adreslerinin kara listele kontrolü
PT-35	MAIL	SMTP ve POP/IMAP Portları için Heartbleed açıklık kontrolü

YEREL AĞ GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-35	LAN	Nmap ile Ayaktaki(up) sistemlerin belirlenmesi
PT-36	LAN	Canlı olarak belirlenen (Up) sistemlerin Nessus ile taranması
PT-37	LAN	Nmap ile Full Port Taramanın gerçekleştirilmesi (Farklı portlarda çalışan uygulamaların belirlenmesi)
PT-38	LAN	Yerel ağ uygulama ve servis sürüm bilgilerinin haritasının çıkartılması
PT-39	LAN	Belirlenen servis sürümlerinde güvenlik zafiyeti aranması (exploit-db.com)
PT-40	LAN	Nmap ile SYN proxy arkasındaki sistemlere port tarama
PT-41	LAN	Nmap ile kimlik doğrulama gerektirmeyen telnet servislerinin tespiti
PT-42	LAN	Genele açık Dosya Paylaşımlarının - SMB üzerinden kontrolü
PT-43	LAN	Genele açık Dosya Paylaşımlarının - NFS üzerinden kontrolü
PT-44	LAN	Tüm iç ağda Anonim FTP hesaplarının bulunması ve incelenmesi
PT-45	LAN	Kimlik doğrulama gerektiren top 10 servisin bulunması
PT-46	LAN	Yerel ağda kullanılan yazılım ve donanımların tespiti
PT-47	LAN	İlgili uygulamalara ait ön tanımlı hesap bilgilerinin denenmesi
PT-48	LAN	Kimlik doğrulama gerektiren servislere yönelik parola bulma denemeleri
PT-49	LAN	MITM(Man in The Middle) Testleri
PT-50	LAN	MITM-ARP Cache poisoning testleri
PT-51	LAN	MITM-DHCP Spoofing testleri
PT-52	LAN	MITM-ICMP Redirect testleri
PT-53	LAN	Local Admin parolası aynı olan sistemlerin bulunması (Pass The Hash)
PT-54	LAN	Tüm network için ms08-067 taraması(nmap)
PT-55	LAN	Tomcat,Jboss,Sun GlassFish gibi servislerin tespiti
PT-56	LAN	Belirlenen kritik açık port ve servislerin manuel incelenmesi
PT-57	LAN	Belirlenen SNMP açık sistemlerden bilgi toplanması
PT-58	LAN	IP spoofing, mac spoofing testleri (NAC Testleri)
PT-59	LAN	Mac flooding kullanarak DoS testi denemesi
PT-60	LAN	Yerel ağda kullanılan ip aralığının belirlenmesi (pasif)
PT-61	LAN	İç ağdaki web arabirimlerine ait ekran görüntüsünün alınması
PT-EK	LAN	LAN-DMZ, DMZ-LAN, wifi-LAN arası yetkisiz geçiş testleri
PT-EK	LAN	NAC çözümü atlatma testleri
PT-62	LAN	Vlan Hopping testleri

INTERNET ÜZERİNDEN GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-63	INTRNT	Whois ile IP bloklarının bulunması
PT-64	INTRNT	Tam kapsamlı Port Tarama
PT-65	INTRNT	Syncookie/SynProxy koruma tespiti
PT-66	INTRNT	Kimlik doğrulama isteyen ağ servislerinin belirlenmesi
PT-67	INTRNT	Shodan,Bing, Robtex üzerinden bilgi toplama
PT-68	INTRNT	DNS ve Google aracılığı ile UP olan makinelerin belirlenmesi
PT-69	INTRNT	ShodanHQ arama motoru kullanarak firmaya ait subnetlerin incelenmesi
PT-70	INTRNT	VPN servislerinin tespiti ve zaafiyet denetimi
PT-71	INTRNT	Aktif IDS/IPS tespiti
PT-72	INTRNT	Kuruma ait anahtar kelimelerin pastebin sitesinde arattırılması
PT-73	INTRNT	Kuruma ait ağ cihazlarının belirlenmesi (Traceroute)

WEB UYGULAMA GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-74	WEB	İlgili domainlere ait whois kayıtlarının incelenmesi
PT-75	WEB	Aynı IP adresi üzerindeki web sitelerinin belirlenmesi
PT-76	WEB	Google üzerinden subdomain arama
PT-77	WEB	Web, uygulama ve veritabanı sunucularının sistem bileşenleri hakkındaki kritik bilgiler (sunucu adı ve sürümü, kullanılan program sürümü v.b.) belirleme.
PT-78	WEB	Uygulamada oluşan hatalar ve uygulama sunucusu ön tanımlı hata mesajları kullanıcıya detaylı olarak belirlenmesi.
PT-79	WEB	Dosya, dizin listeleme testleri.
PT-80	WEB	Arama motorları üzerinden bilgi toplama
PT-81	WEB	Robots.txt dosyası kullanarak hassas dizinlerin belirlenmesi.
PT-82	WEB	Hedef sistem Windows mu, Unix tabanli mi?
PT-83	WEB	Dosya, dizinlerin bulunmasına yönelik brute force denemeleri.
PT-84	WEB	Bilinen web yazılımlarına ait imza taraması
PT-85	WEB	İç IP adres yapısı hakkında bilgi toplama
PT-86	WEB	SSL/TLS versiyon, algoritma ve sertifika geçerlilik testleri
PT-87	WEB	Hedef uygulamada kullanılan yönetim panelinin belirlenmesi
PT-88	WEB	Dosya uzantısı yönetimi testleri
PT-89	WEB	Yedek, kopya, test veya eski sürümlerden kalma sayfa ve uygulamaların belirlenmesi
PT-90	WEB	ASP.NET ViewState güvenlik kontrolleri
PT-91	WEB	Web arka kapı kontrol testleri
PT-92	WEB	Sunucu tarafından desteklenen metodların ve XST belirlenmesi
PT-93	WEB	Hassas bilgilerin HTTPS üzerinden aktarımı kontrolü

PT-94	WEB	Hedef uygulama üzerinde kullanıcı adı belirleme/doğrulama çalışmaları
PT-95	WEB	Hedef uygulama üzerinde tanımlı kullanıcıların belirlenmesi -
PT-96	WEB	Hedef uygulama üzerinde yetkili kullanıcılara yönelik brute force parola denemeleri
PT-97	WEB	Kimlik doğrulama aşamasını atlatma denemeleri
PT-98	WEB	Parola hatırlatma ve parola sıfırlama özelliklerinin testleri
PT-99	WEB	Browser ön bellek yönetimi ve “Log out” fonksiyonlarının testleri
PT-100	WEB	CAPTCHA güvenlik testleri
PT-101	WEB	Captcha atlatma ve replay testleri
PT-102	WEB	Captcha resim boyutlarıyla oynayarak DoS testi
PT-103	WEB	Oturum yönetimi zayıflıkları, oturum yönetimi bypass testleri
PT-104	WEB	Ovturum sabitleme (session fixation) testleri
PT-105	WEB	Oturum değerleri tahmin saldırıları
PT-106	WEB	CSRF(Cross site request forgery) testleri
PT-107	WEB	Oturum bilgisi zaman aşımı kontrol testleri
PT-108	WEB	Oturum bilgisini içeren çerezlerin domain/ yol bilgileri sızıntısı
PT-109	WEB	Hassas formlarda AUTOCOMPLETE ozelligi kontrolu
PT-110	WEB	Cookie'lere ait Secure ve HttpOnly özelliklerinin kontrolu
PT-111	WEB	Parola güncelleme için eski parolanın sorulması kontrolü (CSRF)
PT-112	WEB	Parola unutma fonksiyonu zayıflık testleri
PT-113	WEB	Dizin atlatma/gezme(Directory Treversal) testleri -
PT-114	WEB	Yetkilendirme atlatma, yetkilendirme geçiş testleri
PT-115	WEB	Yetki yükseltimi testleri
PT-116	WEB	Yansıtılan(Reflected) XSS testleri
PT-117	WEB	Depolanmış(Stored) XSS testleri
PT-118	WEB	DOM tabanlı XSS testleri
PT-119	WEB	XSF (Flash XSS) testleri
PT-120	WEB	SQL enjeksiyonu testleri(Error Based)
PT-121	WEB	SQL enjeksiyonu testleri(Boolean Based)
PT-122	WEB	SQL enjeksiyonu testleri(Blind (Time Based))
PT-123	WEB	Local/Remote File Inclusion
PT-124	WEB	Open Redirection
PT-125	WEB	LDAP enjeksiyonu testleri
PT-126	WEB	Xpath enjeksiyonu testleri
PT-127	WEB	Kod enjeksiyonu testleri(Blind / Nomal)
PT-128	WEB	İşletim sistemi komut enjeksiyonu testleri
PT-129	WEB	Bellek taşması (buffer overflow) testleri
PT-130	WEB	Http response splitting testleri
PT-131	WEB	Clickjacking testleri
PT-132	WEB	SQL wildcard üzerinden DoS testleri Hesap kitleme politikasının testi
PT-133	WEB	Buffer overflow DoS testleri
PT-134	WEB	Oturum boyutu arttırma DoS testleri -

PT-135	WEB	http GET Flood DoS testleri
PT-136	WEB	Slowloris HTTP GET/POST atağının denenmesi
PT-137	WEB	site:domain.com.tr "SQL syntax"
PT-138	WEB	site:domain.com.tr inurl:admin inurl:login inurl:vpn
PT-139	WEB	Firma domainine ait .asp uzantılı web sayfalarının bulunması
PT-140	WEB	Firma domainine ait .php uzantılı web sayfalarının bulunması
PT-141	WEB	Firma domainine ait .aspx uzantılı web sayfalarının bulunması
PT-142	WEB	Firma domainine ait .jsp uzantılı web sayfalarının bulunması
PT-143	WEB	Firma domainine ait .cgi uzantılı web sayfalarının bulunması
PT-144	WEB	Arama motorlarından error, warning gibi ifadelerin arattırılması
PT-145	WEB	login, yonetim, signup gibi login barındıracak sayfaların Google üzerinden bulunması
PT-146	WEB	Nikto kullanarak statik güvenlik testlerinin yapılması
PT-147	WEB	Excel, word içerikli dosyaların belirlenmesi
PT-148	WEB	Parola, şifre, password gibi kelime gruplarının ilgili domaine özel arattırılması
PT-149	WEB	İlgili web sayfasına ait girdi alan web sayfalarının bulunması
PT-150	WEB	Dirbuster, Wfuzz kullanarak alt sayfaların bulunması
PT-151	WEB	Hata mekanizmasının test edilerek ek bilgi çıkartılmaya çalışılması
PT-152	WEB	Kullanılan web sunucu ve platform bilgilerinin bulunması
PT-153	WEB	Manuel testlerde Firefox eklentileri kullanma
PT-154	WEB	IE uyumlu uygulamaları Firefox üzerinden test etme
PT-155	WEB	Parolaların veritabanında açık olarak tutulup tutulmadığının testleri
PT-156	WEB	Flash dosyaları statik analiz testleri
PT-156	WEB	Parola resetleme, parola hatırlat fonksiyonlarının test edilmesi
PT-156	WEB	XML Enjeksiyon Testleri
PT-156	WEB	XXE Enjeksiyon Testleri
PT-156	WEB	SSI Enjeksiyonu Testleri
PT-156	WEB	SMTP/IMAP Üzerinden Komut Çalıştırma Açıklığı
PT-156	WEB	HPP -HTTP Parameter pollution Kontrolü
PT-156	WEB	Kullanılan HTTP Metodlarının Tespiti
PT-156	WEB	Eski, Arşiv Dosyalar Üzerinden Bilgi İfşası Açıklığı
PT-156	WEB	Hesap Kitleme Mekanizması Testleri
PT-156	WEB	WAF/IPS Tespiti ve Keşif Çalışması
PT-156	WEB	HTTP Strict Transport Security Testi
PT-156	WEB	Kullanıcı Kayıt Prosedürlerinin Test Edilmesi
PT-156	WEB	Öntanımlı Hesap Bilgilerinin Test Edilmesi
PT-156	WEB	Oturum Sabitleme(Session fixation) Güvenlik Testleri
PT-156	WEB	Dosya Yükleme Fonksiyonlarının Testi

SOSYAL MÜHENDİSLİK GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-157	SOS. MUH.	Çalışanlarına ait e-posta adreslerinin bulunması (Arama motorları)
PT-158	SOS. MUH.	LinkedIn üzerinden çalışanlarının e-posta adreslerinin belirlenmesi
PT-159	SOS. MUH.	Kurum alan adlarına ait sorumluların belirlenmesi (registrars)
PT-160	SOS. MUH.	Internete hizmet veren webmail/VPN servislerin belirlenmesi
PT-161	SOS. MUH.	Kuruma ait alan adlarının password reset denemesi (whois)
PT-162	SOS. MUH.	Kurumun kullandığı e-posta, spam GW sistemlerinin belirlenmesi
PT-163	SOS. MUH.	LinkedIN üzerinden çalışanlara ait ad/soyad/görev bilgilerinin elde edilmesi
PT-164	SOS. MUH.	Google üzerinden çalışanlara ait e-posta formatının belirlenmesi
PT-165	SOS. MUH.	Kurumun dışa açık kimlik doğrulama gerektiren hizmetlerinin belirlenmesi
PT-166	SOS. MUH.	Kurumun web sitelerine benzer isimde sitelerin belirlenmesi
PT-167	SOS. MUH.	FOCA aracı kullanarak hedef kuruma ait meta bilgilerinin ortaya çıkartılması
PT-168	SOS. MUH.	Internet uzerindeki servislerde bulunabilecek, firma binasi ve cevresindeki geolocation bilgisini iceren iceriklerin tespiti (twitter, foursquare vb.)
PT-169	SOS. MUH.	Elde edilen bilgiler kullanilarak sahte icerikli eposta gonderimi Telefon ile bilgi toplama, sosyal muhendislikten yararlanma denemeleri
PT-170	SOS. MUH.	Call center'lara yonelik sosyal muhendislik testleri
PT-171	SOS. MUH.	Whois kayıtlarına göre sosyal müh. Denemesi (Nic.tr)

KABLOSUZ AĞ GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-173	WI-FI	Hedef sisteme ait kablosuz ağların(SSID) bulunması
PT-174	WI-FI	Gizli durumdaki kablosuz ağların(Hidden SSID) bulunması
PT-175	WI-FI	Kablosuz ağa bağlı sistemlere yönelik bilgi toplama(mac vs.)
PT-176	WI-FI	Kablosuz ağda kullanılan şifreleme yöntemlerinin belirlenmesi
PT-177	WI-FI	Kablosuz ağa bağlı mobil cihazların bulunması
PT-178	WI-FI	MAC adresinden cihaz tipi belirlenmesi
PT-179	WI-FI	Kullanılan IP adres aralığını belirleme
PT-180	WI-FI	AP cihazına yönetim arabirimine yönelik güvenlik testleri
PT-181	WI-FI	AP cihazı ip adresinin bulunması
PT-182	WI-FI	AP cihazına yönelik kimlik doğrulama(open/shared) denetimleri
PT-183	WI-FI	Ağa bağlı istemcilerin IP adreslerini ve işletim sistemlerini belirleme
PT-184	WI-FI	MAC adres filtreme belirleme
PT-185	WI-FI	MAC adres filtreleme özelliğinin atlatma
PT-186	WI-FI	Hotspot atlatma testleri – DNS Tünelleme

PT-187	WI-FI	Ağa bağlı istemcilere yönelik MITM testleri
PT-188	WI-FI	Ağa bağlı istemcilerin sistemlerini ele geçirme testleri(fake upgrade)
PT-189	WI-FI	WEP/WPA/WPA2 Parola Kırma Testleri
PT-190	WI-FI	Sahte Access Point Kurulumu ve Yayını
PT-191	WI-FI	Firmaya ait hotspot ortaminin simule edilerek, buraya baglanan kullanicilardan bilgi toplanmasi
PT-192	WI-FI	Ağa bağlı istemcilerden WEP/WPA anahtarı alma denemeleri
PT-193	WI-FI	Ağa bağlı kablosuz istemcilere De-authentication saldırıları gerçekleştirme
PT-194	WI-FI	Ağa bağlı kablosuz istemcilere De-asssicate saldırıları gerçekleştirme
PT-195	WI-FI	Access Point'e sahte bağlantı istekleri göndererek bağlantı limitlerinin zorlanması
PT-196	WI-FI	Wireless AP'lerde bulunan bilinen zaafiyetlerin tespiti
PT-197	WI-FI	Nipper kullarak yapılandırma güvenlik testleri
PT-198	WI-FI	SNMP servisi zaafiyetleri kontrolu

VERİTABANI GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-199	DB	Ön tanımlı veritabanı kullanıcı hesapları kontrolü
PT-200	DB	Veritabanı oracle SID tahmini
PT-201	DB	Veritabani surum tespiti ve zaafiyet analizi
PT-202	DB	Oracle listener tespiti ve zaafiyetleri
PT-203	DB	Öntanımlı/Zayif veritabani yonetici sifrelerinin tespiti
PT-204	DB	Mysql Authentication Atlatma Testleri
PT-205	DB	Ele geçirilen veritabanı parola/hashlerinin kırılması
PT-206	DB	Microsoft SQL üzerinden işletim sistemi ele geçirme
PT-207	DB	Veritabanı yönetim arabirimleri kimlik doğrulama testleri

GÜVENLİK SİSTEMLERİ TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-208	NETSEC	Hedef sistem önünde WAF çalışıp çalışmadığı belirleme
PT-209	NETSEC	Hedef sistem önünde IPS çalışıp çalışmadığı belirleme
PT-210	NETSEC	IPS/WAF statefull calisip calismadiginin testi (Inline IPS/WAF)
PT-211	NETSEC	Dışardan WAF'i SSL ile atlatma testleri
PT-212	NETSEC	IPS'I SSL üzerinden atlatma testleri
PT-213	NETSEC	İçerden Guvenlik duvarı atlatma calismalari – ultrasurf
PT-214	NETSEC	İçerden içerik filtreleme, Firewall IPS atlatma testleri FIREWALL meterpreter_reverse_Https
PT-215	NETSEC	İçerden Dışarı Doğru Yapılan Testler (Tünelleme)
PT-216	NETSEC	SSH Tünelleme denemeleri

PT-217	NETSEC	DNS Tünelleme denemeleri
PT-218	NETSEC	HTTP Tünelleme denemeleri
PT-219	NETSEC	Güvenlik duvarının FIN, ACK, PUSH gibi oturum kurulmamış TCP bayraklı paketlere cevap vermesi
PT-220	NETSEC	TTL değerleri kullanarak aradaki cihazların(koruma amaclı L3) belirlenmesi
PT-221	NETSEC	Rate limiting uygulamasının belirlenmesi
PT-222	NETSEC	Rate limiting sonucuna göre istenilen ip adresinin engelletirilmeye çalışılması
PT-223	NETSEC	SSL inceleme yapılıp yapılmadığının belirlenmesi
PT-224	NETSEC	Parçalanmış paketlerle IPS/WAF atlatma denemesi
PT-225	NETSEC	Encoding(Web için) yöntemleriyle atlatma denemesi
PT-226	NETSEC	Hackvertor.co.uk üzerinden encoding testleri
PT-227	NETSEC	Yeni nesil güvenlik duvarı ve DLP testleri
PT-228	NETSEC	Spam gw testleri metload exe pdf vs gönderilmesi
PT-229	NETSEC	Içerik filtreleme atlatma testleri –ultrasurf.
PT-230	NETSEC	Vpn testleri

ATM SİSTEMLERİ GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-231	ATM	WMI üzerinden Meterpreter yükleme denemesi
PT-232	ATM	WCE ve mimikatz ile hashdump alınarak ve parola bilgileri alınarak inceleme yapılır
PT-233	ATM	Kurulu AV atlatmak icin encoding teknikleri kullanilir.
PT-234	ATM	Paylaşım var mı yok mu kontrol edilip paylaşımlardaki bilgiler incelenir.
PT-235	ATM	Açılışta okunan dosyalar incelenir ve hassas bilgi olup o lmadığı kontrol edilir.
PT-236	ATM	USB takıp autorun kontrolü yapılır
PT-237	ATM	Makine reboot edilerek Backtrack ile acılıp hash bilgileri alınır
PT-238	ATM	Varolan kisitlamalarin, USB uzerinden yuklenen dosyalarla asilip asilamadiginin kontrolu

DoS/DDOS PERFORMANS TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-239	DDOS	TCP Tabanlı DoS/DDoS Testleri (SYN/FIN(ACK)
PT-240	DDOS	TCP Connection Flood Testleri
PT-241	DDOS	UDP Flood DDoS Testleri
PT-242	DDOS	ICMP Flood DDoS Testleri
PT-243	DDOS	Bant Genişliği Taşırma DoS Testleri

PT-244	DDOS	Botnet Simulasyonu Testleri
PT-245	DDOS	HTTP GET/POST Flood Dos/DDoS Testleri
PT-245	DDOS	HTTP Slowloris DoS Testleri
PT-246	DDOS	SSL Connection Flood Testleri
PT-247	DDOS	DNS Flood DoS/DDoS Testleri
PT-248	DDOS	Rate Lmiting DoS Testleri
PT-249	DDOS	Kullanılan Yazılım/sistemlere özel DoS testleri

VOIP SİSTEMLERİ GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-250	VOIP	VoIP Sistemler Hakkında Bilgi Toplamak
PT-251	VOIP	VoIP Sistemlere Yönelik Denial of Service (DoS) Testleri
PT-252	VOIP	Kimlik Doğrulama Bilgilerini Ele Geçirme
PT-253	VOIP	Arama Sahteciliği (Caller ID spoofing) Testleri
PT-254	VOIP	Ortadaki Adam (MITM) Testleri
PT-255	VOIP	VoIP Sistemlere Yönelik İstismar (Exploitation) Çalışması

MOBİL UYGULAMA GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-256	MOBİL	Dosya sisteminde okunabilir hassas veri barındırma testleri
PT-257	MOBİL	Araya girme ve veri değiştirme testleri
PT-258	MOBİL	Test amaçlı bırakılmış hesap bilgilerinin kontrolü
PT-259	MOBİL	Yetersiz kimlik doğrulama(sunucu/istemci) testleri
PT-260	MOBİL	Mobil uygulama sunucu tarafı testleri (web)
PT-261	MOBİL	Mobil uygulama ikili dosya çözümleme ve kod denetimi testleri
PT-262	MOBİL	İstemci tarafı kontrol atlatma testleri (IP, User-Agent v.b)
PT-263	MOBİL	SSL sertifika pinning özelliği testler
PT-264	MOBİL	Hassas verilerin açık kanallardan iletişimi testleri

WINDOWS SİSTEM GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-265	WINDOWS	Windows güvenlik yama eksikliği kontrolü
PT-266	WINDOWS	Windows yetki arttırımı denemeleri
PT-267	WINDOWS	Disk üzerindeki paylaşım alanlarında hassas veri arama
PT-268	WINDOWS	Bellek üzerinden parola HASH değerlerinin elde edilmesi
PT-269	WINDOWS	Bellek üzerinden parola açık değerlerinin elde edilmesi
PT-270	WINDOWS	Sistem açılışında BİOS koruması ve disk şifreleme kontrolü
PT-271	WINDOWS	Offline olarak disk üzerinden parola hash değerlerinin alınması

PT-272	WINDOWS	Açılış dosyalarının bulunduğu ortak alanın incelenmesi
PT-273	WINDOWS	W2K8 Group Policy ortak parola kullanımı kontrolü
PT-274	WINDOWS	MBSA kullanarak yerel sistem güvenlik testleri
PT-275	WINDOWS	Encoding kullanarak Antivirüs atlatma testleri
PT-276	WINDOWS	Sisteme psexec üzerinden ajan yazılım yükleme testleri

LINUX/UNIX SİSTEM GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-277	LINUX	Linux kernel hak yükseltme (priv.esc) denemesi
PT-278	LINUX	SSH üzerinden brute force denmesi
PT-279	LINUX	Sudo kullanarak root yetkilerine geçiş denemeleri
PT-280	LINUX	777 izinli dosyaların bulunması
PT-281	LINUX	Hassas bilgi barındıran dosyaların bulunması
PT-282	LINUX	Linux parola güvenlik testleri
PT-283	LINUX	History dosyalarının araştırılması(.bash/.mysql)
PT-284	LINUX	Çalışan proseslerden hassas veri ifşası testi(lsof, ps)
PT-285	LINUX	SSH anahtar dosyalarının izin kontrolü ve ifşası
PT-286	LINUX	Fork bomb DoS testi
PT-287	LINUX	Yapılandırma dosyalarında hassas veri arama

SIZMA TESTİ İLERLEME ADIMLARI KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-288	POSTXPL	Girilen sistemden ulaşılabilen diğer ağların keşfi
PT-289	POSTXPL	Uzaktan VPN kullanarak pivoting testleri
PT-290	POSTXPL	Elde edilen parola ve hash değerlerinin tüm sistemlerde denenmesi
PT-291	POSTXPL	Girilen sistemin domaine üye olup olmadığının belirlenmesi
PT-292	POSTXPL	Domaine adminin giriş yaptığı üye sistemlerin belirlenmesi
PT-293	POSTXPL	Hak yükseltme/Domain admin olma denemeleri
PT-294	POSTXPL	Girilen sistemlerde kullanılan exploitlerin silinmesi

AĞ CİHAZLARI GÜVENLİK TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ VE AÇIKLAMASI
PT-295	NETW	Kimlik doğrulama servislerine yönelik ön tanımlı parola testleri
PT-296	NETW	SNMP üzerinden hassas veri ifşası
PT-297	NETW	SNMP community name denemeleri
PT-298	NETW	Cihazda çalışan yazılım sürümüne ait çıkmış güvenlik zafiyetlerinin araştırılması
PT-299	NETW	Elde edilen parola hash değerlerinin kırılması

PAROLA KIRMA TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ
PT-300	PASSWD	Hash/Şifreleme tipinin Belirlenmesi
PT-301	PASSWD	LM HASH kullaniminin aktif olup olmadiginin kontrolu
PT-302	PASSWD	Bilinen sözlükler kullanarak parola denemeleri
PT-303	PASSWD	Internet üzerinden hash arattırılması
PT-304	PASSWD	Kaba kuvvet parola (brute force) testleri
PT-305	PASSWD	GPU kullanarak parola kırma testleri
PT-306	PASSWD	İsteğe göre sözlük listesi oluşturma
PT-307	PASSWD	Bulut bilişim hizmetleri kullanarak parola kırma testleri

DNS SUNUCU SIZMA TESTLERİ KONTROL LİSTESİ

KOD	KATEGORİ	KONTROL İSMİ
PT-01	DNS	DNS için ilgili portların (UDP/53, TCP/53) kontrol edilmesi (Tüm Subnetin kontrolü)
PT-02	DNS	DNS sunucu yazılım sürüm bilgilerinin belirlenmesi
PT-03	DNS	DNS sunucu yazılımında bulunan güvenlik zafiyetlerinin belirlenmesi
PT-04	DNS	DNS Zone transferine açık olup olmadığının belirlenmesi
PT-05	DNS	DNS sunucuda kayıtlı alan adlarının belirlenmesi
PT-06	DNS	Genele açık DNS hizmeti (recursive DNS) verilip verilmediğinin belirlenmesi
PT-07	DNS	DNS sunucunun "." isteklerine cevap vermediğinin belirlenmesi
PT-08	DNS	Alt domain keşfi için brute force denemelerinin gerçekleştirilmesi.
PT-09	DNS	Arama motorları kullanarak alt domain keşfi
PT-10	DNS	DNS cache poisoninge açık olup olmadığının belirlenmesi
PT-11	DNS	DNS cahce snooping saldırılarından etkilenip etkilenmediğinin belirlenmesi
PT-12	DNS	TXT,HINFO ve NSEC kayıtlarından bilgi ifşası kontrolü
PT-13	DNS	DNS sunucuya yönelik tam kapsamlı Nessus taraması
PT-14	DNS	DNSSEC hizmeti sunulup sunulmadığının bilgisi

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu" , "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.