ÖN BİLGİ

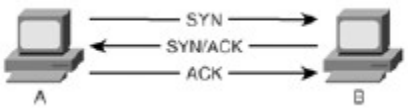
Bir makale internetten bulunup şu adreste yedeklenmiştir.

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Gazi%20Universitesi%20Tezi.pdf

Bu belge ise yedeklenen bu makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Port tarama tekniklerinin daha iyi anlasılabilmesi için iki host arasındaki TCP baglantısının nasıl kuruldugunun bilinmesi önemlidir

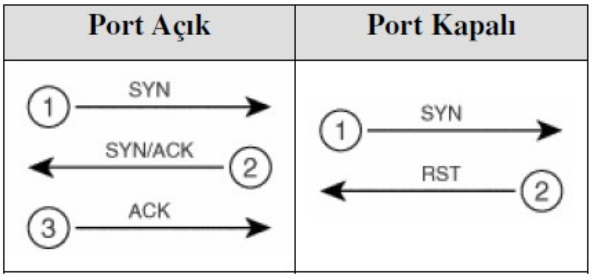


A bilgisayarı B bilgisayarı ile baglantı kurmak istediginde, B bilgisayarına SYN paketi ve baslangıç sıra numarası (ISN) gönderir. B bilgisayarı kabul paketi (SYN/ACK) ile sıra numarasını bir artırarak (ISN+1) A bilgisayarına gönderir. Daha sonra A bilgisayarı B bilgisayarına kabul (ACK) paketi göndererek TCP baglantısının iki bilgisayar arasında kurulmasını saglar. ACK paketinin sıra numarası B bilgisayarının sıra numarasıdır (ISN+1). TCP baglantısında sıra numaralarında tutarsızlık yasandıgında reset (RST) paketi gönderilerek baglantı kesilir.

Port tarama teknikleri, TCP_Connect, TCP Syn, TCP Null, TCP Fin, TCP_Ack, Xmas-Tree, Dumb, UDP Tarama olmak üzere sekiz gruba ayrılarak asagıda detaylı sekilde açıklanmıstır.

a)

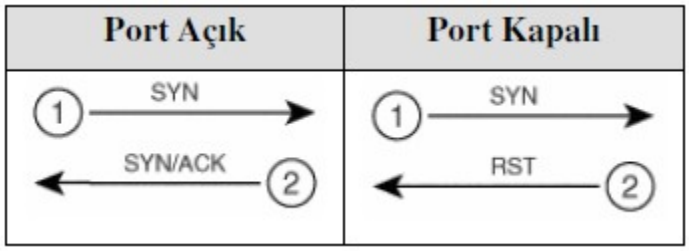
TCP_Connect tekniginde, hedef porta baglanmak için SYN paketi gönderilir, bu pakete karsılık SYN/ACK paketi gelirse ACK paketi göndererek porta baglanılır, yani portun açık oldugu onaylanır. Eger SYN paketine RST cevabı gelirse portun kapalı oldugu varsayılır. Bu tarama türünün dezavantajı açılan tüm oturumların hedefteki güvenlik sistemleri (STS, GD, vb.) tarafından tespit edilerek kayıtlarının tutulmasıdır.



Sekil 4.7. TCP_Connect tarama

b)

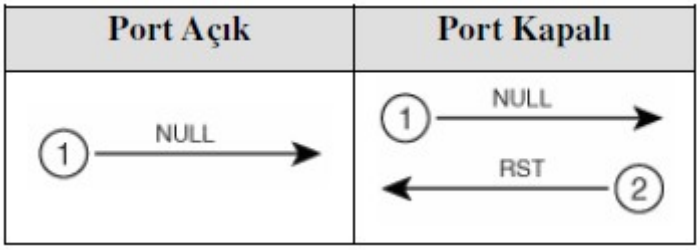
SYN Port Taraması, yarı açık olarak da tanınan SYN tarama TCP oturumunu tamamen açmaz, SYN paketinin karsılıgında SYN/ACK paketi geldiginde portun açık oldugunu rapor eder ve RST paketi göndererek oturumu kapatır, port kapalı ise hedef RST cevabı gönderir. Bu tür taramada güvenlik duvarları tarafından farkedilme ihtimali düsük, atak tespit sistemleri (IDS) tarafından farkedilme olasılıgı yüksektir.



Sekil 4.8. SYN tarama

c)

NULL Tarama, normal TCP haberlesmesinden farklı olarak hiçbir bayrak biti isaretlenmez. RFC 793'e göre eger gelen TCP segmentinde isaretli bir bayrak biti yoksa alıcı TCP segmentinin haberlesmesini keserek gönderene RST paketi yollar. Asagıdaki sekilde görülecegi gibi bayrak biti isaretlenmeyen bir paket gönderildiginde, eger hedefteki port açıksa paketi yok sayarak cevap vermez, ancak port kapalı ise gönderene RST paketi yollayarak cevap verir.



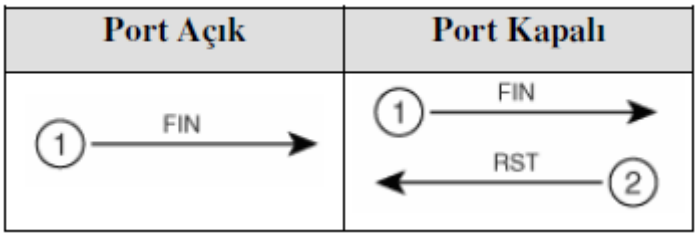
Sekil 4.9. NULL tarama

Bu tarama tekniginin kullanılacagı ortamlar RFC 793 ile uyumlu olmalıdır. Örnegin, Windows isletim sisteminin çalıstıgı ortamlar bu RFC ile uyumlu degildir. Bu sebepten Windows yüklü bilgisayarlarda bu arama yöntemi kullanılamamaktadır. Windows isletim sistemi yüklü olan bilgisayarlar bayrak seti isaretlenmemis bir TCP paketi aldıgında, RFC 793 ile uyumlu olmadıgı için göndericiye RST paketi yollayarak cevap verir. UNIX tabanlı sistemler RFC 793

ile uyumlu oldugundan port taramalarında bu yöntem kullanılabilir. Bu yöntemde gelen TCP paketine hiçbir cevap verilmemesiyle portların açık oldugu belirlendiginden ters tarama sonuçlu port tarama sistemi olarak sınıflandırılır. Güvenlik duvarları ve atak tespit sistemleri tarafından bu tarama yönteminin algılanması zordur.

d)

FIN Tarama, bir diger ters tarama sonuçlu port tarama yöntemidir. NULL taramaya benzer, fakat bu yöntemde FIN biti isaretlenmis TCP paketi hedefe gönderilir. FIN biti TCP oturumunun bittigini belirten bir alandır. RFC 793 ile uyumlu olan ortamlarda geçerlidir.



Sekil 4.10. FIN tarama

e)

ACK Tarama, yöntemi güvenlik duvarlarının erisim kontrol listelerini geçerek tarama hedefteki hostların portları üzerinde tarama yapılmasını saglar. Stateful veya basit paket filtreleme güvenlik duvarları, dısarıdan gelen SYN paketlerini bloke edebilir ancak ACK paketinin geçisine izin verirler. Bu tarama yönteminde ACK paketine rastgele üretilmis sıra numaraları verilir. Hedeften cevap gelmez veya ICMP port ulasılamaz mesajı gelirse port filtrelenen bir porttur. Eger port güvenlik duvarları tarafından filtrelenmemisse RST paketi üretilerek kaynaga gönderilir. RST paketlerine bakılarak portların güvenlik duvarları tarafından filtrelenip filtrelenemedigi ögrenilebilir.

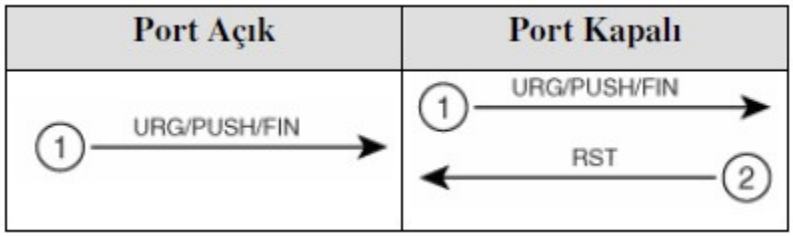
f)

Xmas-Tree Tarama, Noel agacı anlamına gelen ters amaçlı tarama tipinde asagıda belirtilen bayrakların isaretlendigi paket gönderilir. İsaretlenen bayraklar asagıda gösterilmistir.

URG Verinin acil oldugunu ve derhal isleme alınması gerektigini belirtir.

PUSH Tampona veri gönderilmesini belirtir

FIN TCP oturumu bittigini belirtir



Sekil 4.11. Xmas-Tree tarama

Bu tarama yönteminde yukarıda gösterilen bayrakların isaretlendigi paket hedef hosta gönderildiginde RFC793'e göre hedeften hiç bir cevap gelmezse port açık, RST paketi döndürülürse portun kapalı oldugu anlasılır.

g)

Dumb Tarama tarama teknigi. hedefteki hostlara ait portların zombie diye tabir edilen üçüncü bir bilgisayar tarafından taranmasına dayanır. SYN tarama yöntemindeki gibi hedefteki hosta SYN paketi gönderilir. Eger port açıksa hedefteki host SYN/ACK paketi döndürür, port kapalı ise hedefteki host RST paketi göndererek oturumu kapatır. Dumb taramada yukarıda anlatılan tüm islemler zombie hostlar üzerinde yapılır.

Bu bilgisayarlar modem arama yazılımları (war dialer) adı verilen yazılımlarla kolayca tespit edilebilir.

h)

UDP tarama, yönteminde hedefteki host'a UDP tipinde bir paket gönderilir. Eger port kapalı ise hedefteki bilgisayardan ICMP port ulasılamaz mesajı döndürülür herhangi bir mesaj döndürülmediginde ise uzak sistemdeki host üzerindeki portun açık oldugu anlasılır.

ı)

Uygulama ve zafiyet eslestirilmesi: Port tarama islemi sonucunda sızma testi yapılacak ag üzerinde çalısan hostlara ait açık portların bir listesi çıkartılır.

Uygulamaların tespit edilmesinde en çok kullanılan yöntem reklâm bandı korsanlıgı (banner grabbing) adı verilen yöntemdir. Uzaktaki uygulamalara baglanarak programların çıktıların gözlemlenmesi, reklâm bandı korsanlıgı olarak adlandırılır

Bu yöntem hedef sistemler üzerinde izin verilen servisler (Telnet, FTP, HTTP, SNMP, vb.) kullanılırken giris veya hosgeldin mesajlarının analiz edilmesine dayanmaktadır.

Açık portların hangi uygulamalar tarafından kullanıldıgının tespit edilmesinden sonra ilgili uygulamalara ait o ana kadar duyurulan zayıflıkların ne olduguna dair arastırmalar yapılır.

(Page 177-181)

2)

Zafiyetlerin kullanımı sızma testlerinin en önemli asamasıdır. Bilgi sistemleri üzerinde bulunan yazılımlara ait güvenlik açıklarının kullanılmasını saglayan küçük programlar istismar kodları (exploit) olarak adlandırılmaktadır. İstismar kodları zafiyetlerin genel veya özel kullanımı için farklı programlama dillerinde (C, C++, Perl, Lisp, Python, vb.) uzman yazılımcılar veya usta saldırganlar tarafından gelistirilmektedir.

(Page 183)

3)

Shellcode : İstismar kodlarının çalıştırılacağı platforma özel ikili kodlar. (e.g. CMD
komutları, Terminal komutları)

NOP : İşlevi olmayan veya bellek adresinin öğrenilebilmesi için bellek dolduran bitlere denir. “Not Operation”ın kısaltılmışıdır.

Encoder : Çalıştırılacak shellcode’u değiştiren ve IDS’ler tarafından yakalanmasını önleyen yazılımlara denir.

(Page 184)

4)

İstismar kodlarının gelistirilme asamaları aşağıda gösterilmistir.

Parametreler, son kullanıcı seviyesinde islem gören seçeneklerin (uzak hedefin seçilmesi, ofset seçimi, derinlemesine çalıstırma, hata giderme, vb.) belirlenmesini saglar. Ag baglantı isleyici, isim çözümlemesi, soket baglantılarının kurulması, hataların islenmesi gibi çesitli ağ yordamlarını içermektedir. İstek karsılayıcı, istismar kodlarını tetikleyen betiklerdir (script). İsleyici yordamı istismar kodunun büyük bir kısmını kapsayan shellcode operasyonlarının yapıldıgı asamadır.

(Page 184-185)

5)

İstismar kodlarının yazılabilmesi, test edilebilmesi amacıyla ticari ve açık kaynak kodlu çerçeve yazılımlar gelistirilmistir. Bunlardan en popüler üçü Metasploit Framework, Core Impact ve Canvas'tır.

(Page 185)

6)

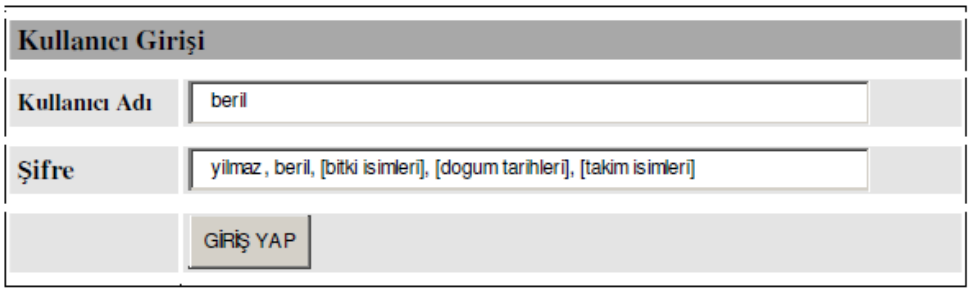
Sızma asamasında çerçeve yazılımların yanında elle (manüel) yapılan istismarlar da çok önemlidir. Özellikle web uygulamalarında sıkça rastlanan ve kodlama esnasında güvenligin ihmal edilmesinden kaynaklanan SQL enjeksiyonu, siteler arası kod çalıstırma, parametre manipüle edilmesi, uzak dosya yükleme gibi zafiyetlerin tespit edilmesinde elle yapılan yöntemlerin kullanılması gerekmektedir.

Elle yapılan yöntemde bilinçli olarak, uygulamalar üzerinde hataların meydana getirilerek, meydana gelen hatalardan sistem hakkında bilgiler alınması ve alınan bilgilerin yardımıyla sistemlere yetkisiz erisim yapılması hedeflenmektedir. Web uygulamaları üzerinde mevcut sayfalarla oynanarak, uygulamanın kaynak kodlarından yararlanılması, uygulamaya ait formlarla, baslık bilgileriyle, çerezlerle oynanması sonucunda istenilen hatalar olusturulabilir.

(Page 185-186)

7)

Brute Force
Kaba kuvvet sızma testlerinde, normal ve ters olmak üzere iki farklı yöntem uygulanmaktadır [204]. Normal yöntemde, tek kullanıcı ismine ait sifrenin bulunması için Sekil 5.4'de gösterildigi gibi birçok parola, deneme yanılma yöntemiyle tahmin edilmeye çalısılmaktadır..



Şekil 5.4

Ters yöntemde Sekil 5.5'de gösterildigi gibi tek parolaya ait birçok kullanıcı ismi deneme yanılma yöntemine tabi tutularak tahmin edilmeye çalısılmaktadır. Milyonlarca kullanıcı hesabına sahip sistemlerde, birden çok kullanıcının aynı parolaya sahip olma olasılıgı yüksek oldugundan ters kaba kuvvet sızma testlerinin basarı olasılıgı daha yüksektir.

(Page 201)

8)

Yetersiz Kimlik Doğrulama Yöntemi
Çogu web uygulaması, görünen dizinler dısında görünmeyen (yönetim, sistem, kullanıcılar, vb.) baska dizinler ve yönetici fonksiyonları içermektedir. Gizli olan

dizinlere web sitesinin herhangi bir yerinden link verilmemekte ancak söz konusu dizine standart bir web tarayıcısı ile erisebilmek mümkündür. Uygulamayı gelistiren yazılımcılar, web sayfasına herhangi bir link olusturulmadıgı ve herhangi bir kullanıcının da bu web sitesini görmesini beklemedigi için söz konusu sayfaya kimlik dogrulama fonksiyonu eklemeyi çogu zaman ihmal etmektedirler. Herhangi bir saldırgan basit bir sekilde bu web sayfasını ziyaret edecek olursa, web sitesine tüm yönetici yetkileri ile erisme yetkisi kazanacaktır.

(Page 201)

9)

Şifre Kurtarma Denetimi
Sızma testleriyle sifre kurtarma mekanizmalarının saglamlıgının kontrolü yapılmaktadır. Sifre kurtarma islemi sırasında kullanıcının kimligini onaylamak için gereken bilgi tahmin edilebiliyorsa veya bu bilgi isteme islemi atlatılabiliyorsa ilgili web sitesinin zayıf bir parola kurtarma mekanizmasına sahip oldugu anlasılır.

Sifre imaları kullanıcıya sifre hatırlatmak için kullanılır ve bazı ipuçlarını içerirler. Kullanılan sifre imaları web sitelerinde kaba kuvvet kullanılarak sifrelerin bulunması açısından zafiyet olusturmaktadır. Gizli soru ve cevap yönteminde de kullanıcı tarafından daha önce belirlenen sorunun cevabının dogru olarak verilmesi beklenir. Örnegin, kullanıcının sifresi “£iR@0” gizli sorusu “Oturdugunuz Sehir” olabilir. Sifre çok saglam olmasına rağmen gizli soru bir o kadar kolaydır. Gizli sorudan elde edilen bu bilgi, sayesinde sifrenin tahmin edilme olasılıgı çok yükselir.

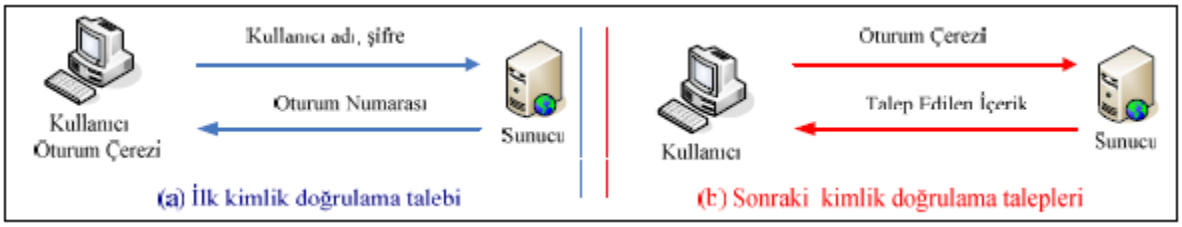
Sifrenin saglam bir sifre olması, sifre güvenligi için önemli bir sart olmasına ragmen sifre güvenligini saglamamaktadır. Sifrelerin geri elde edilmesinde kullanılan yöntemler, sifrelerin güvenliginin saglanması açısından çok büyük önem tasımaktadır.

(Page 202)

10)

Çerezler
Oturum numaraları genellikle tarayıcılar tarafından, çerezler içerisinde kalıcı ve geçici olmak üzere iki farklı yöntemle saklanmaktadır. Geçici depolamada, oturum numarasını içeren çerezleri, tarayıcı kapandıgında süresi doldugundan

silinirler. Kullanıcı web siteleri yetkilendirme ekranlarında yer alan “Beni Hatırla” seçenegini aktif hale getirirse, oturum numaraları kullanıcı bilgisayarları üzerinde kalıcı olarak depolanmaktadır. Kalıcı çerezler isletim sistemi ve tarayıcıların tipine baglı olarak kullanıcı bilgisayarlarında farklı yerlerde (Netscape tarayıcısı, C:\program files\netscape\users\username\cookies.txt, Internet Explorer C:\Documents and Setting\username\Cookies) saklanırlar [206]. Oturum çerezleri sayesinde web sitelerine bir sonraki baglantılar kullanıcı adı ve sifre istenmeden aşağıdaki şekilde gösterildigi gibi otomatik olarak yapılır.



Oturum numarası kullanarak yetkilendirme yönteminde, zayıf algoritmaların kullanılması, kaba kuvvet saldırılarını engelleyecek önlemlerin alınmaması (hesap kilitleme, dogrulama resimleri, vb.), sunucu bilgisayarlarca oturum numaralarının sifresiz gönderilmesi, oturum numaralarını içeren çerezlerin çalınması gibi birçok tehdit vardır. Oturum numaraları çerezler dısında, gizli form alanı veya URL içerisinde depolanmaktadır.

(Page 205)

11)

Oturum bilgisi, muhtemel bir ağ dinleyicisi veya siteler arası kod çalıstırma (XSS) saldırısı ile elde edilebilir.

(Page 206)

12)

[221 – 224 Sayfaları arasında MS SQL için Sql Injection adımları anlatılıyor (Açığın Tespit Edilmesi başlığı itibariyel...). İstersen oku.]

13)

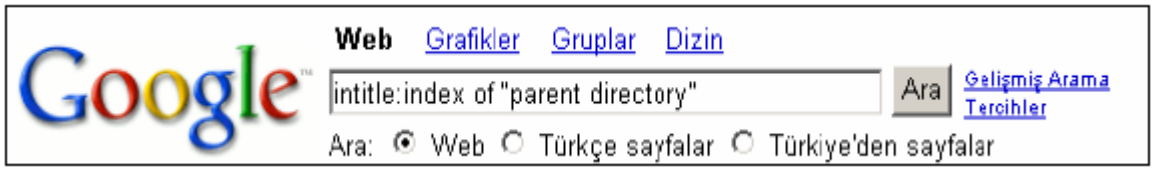
Blind Sql Injection
Veritabanı hata mesajlarının gelistiriciler tarafından son kullanıcıya gösterilmedigi durumlarda yapılan SQL injection saldırısına Blind SQL Injection denir. Normal SQL Injection saldırısında parametreye sadece tırnak işareti koyarak sitenin SQL açığına sahip olup olmadığı anlaşılabiliyordu. Çünkü site tırnağı alınca hata üretiyordu ve bu SQL Injection zafiyeti var anlamına geliyordu. Fakat Blind SQL Injection saldırısı bu hata mesajlarının görüntülenmediği koşullarda yapılan saldırıyı ifade etmektedir. Blind SQL ile SQL Injection zafiyeti sitede var mı yok mu yu WHERE koşulunu iptal ederek anlayabiliriz. Eğer sayfa içeriği bir kayıt gösteriyorken birden fazla kayıt gösterirse sayfa SQL Injection açığına sahiptir deriz.

(Page 225)

14)

Dizin Listeleme Zafiyeti
Dizin listeleme (directory indexing), baslangıç sayfası (homepage) olmayan bir web sitesinin, talep edilen dizin içerisinde yer alan dosyalarının tamamının listelenerek HTML formatında kullanıcıya aktarılmasıdır. Web sunucusu; yapılandırma ayarlarına baglı olarak ziyaretçiden gelen istek dogrultusunda dokümanın bulundugu kök dizininde varsayılan dosyayı (default.asp, default.jsp, index.asp, index.html, vb.) arar ve bu dosyayı HTML formatında kullanıcıya gönderir. Eger varsayılan baslangıç dosyası bulunamazsa, web sunucusu web kök dizini içerisinde yer alan dosya ve klasörlerin (“ls” veya “dir” komutunun web kök dizininde çalıstırılmasına esdegerdir) listelemesini içeren sonuçları kullanıcıya gönderir. Web sunucusundaki hatalı yapılandırmalar ve zafiyetler dizin listelenmesini saglayan nedenlerin basında gelmektedir.

Dizin listeleme zafiyetine sahip siteleri Google hacking ile bulabiliriz:



(Page 229-230)

Aşağıdaki resimleri okumayı unutma!

Çizelge 4.6. Sızma testlerinde kullanılabilecek Windows komutları

Komut	Açıklama
Net Use	Parametreleriyle kullanıldığında bilgisayarı paylaştırılmış kaynağa bağlar, bağlantısını keser veya bilgisayar bağlantıları ile ilgili bilgileri ekranda görüntüler. Bu komut vasıtasıyla kalıcı ağ bağlantıları denetlenebilir. Ayrıca, parametresiz kullanıldığında, ağ bağlantılarının bir listesini alır.
Net View	Parametreleriyle kullanıldığında belirtilen bilgisayar tarafından paylaştırılan etki alanlarının, bilgisayarların veya kaynakların listesini görüntüler. Parametresiz kullanıldığında, Net View komutu geçerli etki alanınızdaki bilgisayarların bir listesini görüntüler.
Net Accounts	Kullanıcı hesapları ve veritabanını güncelleştirerek tüm kullanıcı hesapları için parola ve oturum açma gereksinimlerini değiştirir.
Net Config	Çalışmakta olan yapılandırılabilir hizmetleri görüntüler, bir sunucu hizmeti veya iş istasyonu hizmeti ayarlarını görüntüler veya değiştirir. Parametresiz kullanıldığında, yapılandırılabilir hizmetlerin bir listesini görüntüler.
Net Group	Etki alanlarındaki genel grupları ekler, görüntüler veya değiştirir.
Net Share	Paylaştırılmış kaynakları yönetir. Parametresiz kullanıldığında Net Share, yerel bilgisayarda paylaşılan tüm kaynaklar hakkındaki bilgileri görüntüler.
Net Localgroup	Bilgisayarlara yerel grupları ekler, görüntüler veya değiştirir. Parametresiz kullanıldığında, sunucunun adını ve bilgisayar üzerindeki yerel grup adlarını görüntüler.
Net User	Kullanıcı hesapları ekler, değiştirir veya kullanıcı hesabı bilgilerini görüntüler.
Nslookup	Etki Alanı Ad Sistemi (DNS) altyapısını sorgulamak için kullanılabilecek olan bilgileri görüntüler.
Nltest	Etki alanındaki birincil ve ikincil etki alanı sunucuları ile etki alanındaki bilgisayarlar ve o anda oturum açmış kullanıcıların listesini verir.
Arp	IP adresleri ve IP adreslerinin çözümlenmiş Ethernet veya Token Ring fiziksel adreslerini saklamak için kullanılan bir veya birden fazla tablo içeren Adres Çözümleme İletişim Kuralı (ARP) önbelleğindeki girdileri görüntüler ve değiştirir.
AT	Belirtilen saat ve tarihte bilgisayarda çalıştırılacak komut ve programların zamanlamasını yapar. Parametresiz kullanıldığında, AT komutu zamanlanmış komutları listeler.
Cacls	Paylaşım verilen dosyalardaki isteğe bağlı erişim denetimi listelerini (DACL) görüntüler veya değiştirir.
Cipher	NTFS birimlerinde klasör ve dosya şifrelemesini görüntüler veya değiştirir. Parametresiz kullanıldığında, cipher geçerli klasörün ve içerdiği dosyaların şifreleme durumunu görüntüler.
DsQuery	Belirtilen kritere göre Aktif Dizini sorgular.
Finger	Kullanıcı veya kullanıcılar hakkında bilgiler görüntüler.
GetMac	Yerel olarak veya bir ağ içinde, her bilgisayardaki tüm ağ kartları için ortam erişim denetimi (MAC) adresini ve her adresle ilişkili ağ iletişim kurallarının listesini verir.
IpConfig	Bilgisayar üzerinde geçerli olan tüm TCP/IP ağ yapılandırması ayarlarını görüntüler. Dinamik Ana Bilgisayar Yapılandırma İletişim Kuralı (DHCP) ve Etki Alanı Ad Sistemi (DNS) ayarlarını yeniler. Parametresiz kullanıldığında tüm bağdaştırıcılar için IPv6 adresleri veya IPv4 adresi, alt ağ maskesi ve varsayılan ağ geçidi görüntülenir.
NetStat	Aktif TCP bağlantılarını, bilgisayarın bağlı olduğu bağlantı noktalarını, Ethernet istatistiklerini, IP yönlendirme tablosunu, IP, ICMP, TCP ve UDP iletişim kuralları için IPv4 istatistikleri ile IPv6, ICMPv6, IPv6 üzerinden TCP ve IPv6 iletişim kuralları üzerinden UDP için IPv6 istatistiklerini görüntüler. Parametre olmadan kullanıldığında aktif TCP bağlantılarını görüntüler.
PathPing	Kaynak ve hedef arasındaki ara atlamalarda ağ gecikmesi ve ağ kaybı konularına ilişkin vererek ağ haritası çıkartılmasını sağlar.
Ping	Internet Denetim İletisi İletişim Kuralı (ICMP) Yankı İsteği iletileri göndererek, başka bir TCP/IP bilgisayara IP düzeyinde erişilebilirliği doğrular. Karşılık olarak gelen Yankı İsteği iletileri, iletim süreleriyle birlikte görüntülenir.
Rexec	Rexec hizmetini (arka plan programı) sağlayan ve bu hizmeti çalıştıran Windows dışı bilgisayarlara bağlanmak için Rexec aracını kullanabilirler. Rexec komutu, uzak bilgisayarda belirtilen komutu çalıştırmadan önce kullanıcı adını doğrular.
Route	Yerel IP yönlendirme tablosundaki girdileri görüntüler ve değiştirir.
RSH	RSH hizmeti veya arka plan programı çalıştıran uzak bilgisayarlarda komut çalıştırır.
TaskList	Yerel veya uzak makinede çalışan geçerli işlemlerin listesini görüntüler.
Telnet	Telnet protokolünü kullanan uzak bilgisayarla iletişim kurulmasını sağlar.
Tftp	Önemsiz Dosya Aktarım İletişim Kuralı (TFTP) hizmeti veya arka planını çalıştıran ve genellikle UNIX ile çalışan bir bilgisayardan dosya alır ve gönderir.
TraceRt	Hedefe, Artan Yaşam Süresi (TTL) alanı değerleriyle, Internet Denetim İletisi Protokolü (ICMP) Yankı İstek veya ICMPv6 iletileri gönderildiğinde izlenen yolu belirleyerek ağ haritalarının çıkartılmasını sağlar.

Çizelge 4.5. Sızma testleriyle elde edilecek bilgiler

Konum/ Yöntem	Toplanabilecek Bilgiler
İnternet (Kurum Dışı)	İletişim Bilgileri (Web, Posta Adresi, Telefon, Faks, E-posta)
	Alan İsimleri
	Dış Dünyaya Açık IP Bloğu
	IP'lerin Sunucularla (Güvenlik Duvarı, Web, DNS, E-posta, vb.) Eşleştirilmesi
	Yazılımların ve İşletim Sistemlerinin Tespiti
	Ağ Geçidinin Belirlenmesi (Yönlendirici)
	Güvenlik Yazılımlarının Tespiti (Güvenlik Duvarı, Atak Tespit Sistemi, vb.)
	Uzaktan Erişim Protokollerinin Keşfedilmesi (VPN, Remote Desktop)
İntranet (Kurum İçi)	Kullanılan Ağ Protokolleri (IP, DHCP, DNS, NAT, vb.)
	Dâhili Alan İsimleri Yapılandırması
	Dâhili Ağ IP Bloklarının Belirlenmesi
	Ağ Topolojisinin Belirlenmesi
	Erişim Kontrol Listeleri Mekanizmalarının Tespiti
	Dâhili Atak Tespit Sisteminin Keşfedilmesi
	Uygulama Platformlarının Belirlenmesi (.Net, Java)
	Veri Tabanlarının Belirlenmesi (Oracle, SQL)
	Sunucu Bilgisayarların Belirlenmesi ve Görevlerinin Tespiti
	Güvenlik Yazılımlarının Tespiti (Güvenlik Duvarı, Atak Tespit Sistemi, vb.)
Sosyal Mühendislik (Kurum İçi-Kurum Dışı)	Telefon Yoluyla Taklit ve İkna
	E-posta Yoluyla Kandırmaca
	Çöplük Karıştırma
	Masaüstü Testleri
	Fiziksel Erişim

Alan adı sorgulamasının yapılmasını sağlayan önemli sitelere http://www.whois.net/, http://ws.arin.net/whois, http://www.ripe.net/, https://www.nic.tr,