ISTANBUL UNIVERSITY ENGINEERING FACULTY **YEAR : 2002 (345-358)**
JOURNAL OF ELECTRICAL & ELECTRONICS VOLUME : 2
NUMBER : 1

GÜVENLÝK DUVARLARINDA TEST YÖNTEMÝ GELÝÞTÝRÝLMESÝ: TASARIM & UYGULAMA

DEVELOPING TESTING METHODOLOGY OF FIREWALLS: DESIGNING & APPLICATION

Serkan KURT[1] Ýbrahim SOÐUKPINAR[2]

[1,2]Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliði Bölümü Gebze, Kocaeli, Türkiye

[1]e-posta: serkan.kurt@vestelnet.com [2] e-posta: ispinar@bilmuh.gyte.edu.tr

ABSTRACT

Firewalls are hardware and software systems that protect a corporate network from attacks coming from the outside internet. There are several firewalls available in the market.Altough some firewalls are stronger then others with respect to some security or functionality aspects, they may be weaker in others. Therefore it becomes necessary to find testing methodology that will ease the process of firewall comparison. Performance, operating system, hardware and software building, ,etc., properties are important to develop testing methodology.

Key Words:

ÖZET

Güvenlik Duvarlarlarý að güvenliðinde kullanýlan ve en yaygýn olan yazýlým veya donanýmdýr. Piyasada bilinen Güvenlik Duvarý tipleri oldukça fazladýr. Bu Güvenlik Duvarlarý tasarým açýsýndan birbirlerinden farklýlýklar göstermekte ve uygulama alanlarýna gore tercih nedeni olmaktadýrlar. Bazý Güvenlik Duvarlarý içerdikleri fonksiyonellik bakýmýndan diðerlerinden üstün gözükselerde zayýflýklarý olabilir. Dolayýsýyla bir test yöntemi geliþtirilip gerçekten de göründüðü kadar güvenli olup olmadýðý araþtýrýlmalýdýr. Test yöntemi geliþtirilirken, performans, iþletim sistemi, donanýmsal yapý, yazýlým, sistemin yapýsý, vs. gibi. belirli hususlar dikkate alýnmalýdýr.

Anahtar Kelimeler:

1. GÝRÝÞ

Bilgisayar Aðlarý kavramý ortaya çýkmasýyla birlikte Að güvenliði konusuda beraberinde gelmiºtir. Çünkü ºu anda internet üzerinde bankacýlýk iþlemlerinin yapýlýyor olmasý bile güvenlik konusunun önemini bir kez daha belirtmektedir.

Güvenlik Duvarlarlarý að güvenliðinde kullanýlan ve en yaygýn olan yazýlýmlardýr. Piyasada bilinen Güvenlik Duvar tipleri oldukça fazladýr. Bu Güvenlik Duvarlarý tasarým açýsýndan birbirlerinden farklýlýklar göstermekte ve uygulama alanlarýna gore tercih nedeni olmaktadýrlar. Bazý Güvenlik Duvarlarý içerdikleri fonksiyonellik bakýmýndan diðerlerinden üstün gözükselerde zayýflýklarý olabilir. Dolayýsýyla bir test yöntemi geliþtirilip gerçekten göründüðü kadar güvenli olup olmadýðý araþtýrýlmalýdýr.

Bu makalede Ýnternet Güvenlik Duvarlarý ile ilgili olarak test yönteminin geliºtirilmesi ve yapýlan testlerin amacý anlatýlmýþtýr ve test yönteminin geliþtirilmesi konusu anlatýmý sýrasýnda öncelikle konuyla iliþkili olan **Güvenlik** ve **Güvenlik Duvarý** kavramlarý ele alýnmýþtýr.

Daha önce de bu konuda yapýlan yapýlan bir araþtýrmada [4] farklý bir test yöntemi geliºtirilmiºtir ve elde edilen sonuçlar bir tabloda sunulmuþtur. Konu daha ayrýntýlý olarak sonraki bölümlerde ele alýnmýþtýr.

1.1 Güvenlik Kavramý:

Günümüz iþdünyasý, bilgi paylaþýmýnýn hýzlý ve ayný zamanda güvenilir olmasý gerekliliðinin farkýndadýr. Kurumlar, bu tür ihtiyaçlarýný Ýnternet üzerinden gerçekleþtirebilmekte ancak beraberinde güvenlik açýklarýndan dolayý bu konuda çekingen davranmaktadýrlar. Kurum veritabanýna eriþen bir saldýrgan bu bilgileri kullanarak kurumun piyasada ki prestij ve finansal geleceðini çok rahatlýkla tehdit edebilir.

Her kurum kendisine uygun bir güvenlik politikasý oluþturmalý ve yapý mutlaka belirli testlerden sonra hayata geçirilmelidir. Bunun için að yapýsý her yönüyle incelenmeli ve ihtiyaçlar doðrultusunda en uygun güvenlik politikasý belirlenmekte, uygun tasarým yapýlýp, kuruluþ gerçekleþtirilmelidir. Gerekli test sonuçlarý incelenir ve sistem devreye alýnýr. [3,4,7]

1.2 Güvenlik Duvarý Tanýmý

Ýnternette güvenlik ile ilgili konular arasýnda adý sýk sýk geçen Güvenlik Duvarý (Firewall) kavramý esas olarak yazýlým ile oluþturulup, internet üzerinden bir sisteme giriºleri kýsýtlayan/yasaklayan ve genellikle bir internet gateway servisi (ana internet baðlantýsýný saðlayan servis - að geçidi) olarak çalýþan bir bilgisayar üzerinde bulunan güvenlik sistemine verilen genel addýr. Ýnternet üzerinden baðlanan kiºilerin, bir sisteme giriºini kýsýtlayan/yasaklayan ve genellikle bir internet gateway servisi (ana internet baðlantýsýný saðlayan servis) olarak çalýþan bir bilgisayar ve üzerindeki yazýlýma verilen genel addýr. [1,2,9]

1.3 Kurumsal Güvenlik

Kurumsal Internet Baðlantýlarý'ndaki en önemli unsur þirketinizi dünyaya açtýðýnýz zaman Internet üzerinden gelebilecek olan saldýrýlar ve bunularýn sonucunda uðrayabileceðiniz maddi ve manevi hasarlardýr.

Að güvenliðinde aþaðýda belirtilen konularýn incelenmesi gerekmektedir:

- [a] ifreleme
- Onaylama
- Güvenlik Duvarý
- Paket Filtreleme
- NAT Sistemi
- Proxy
- Virüs Koruma
- Güvenlik Denetimi
- Saldýrý Tespiti
- Diðer

Internet ortamýnýn çok hýzlý geliþmesi sonucunda her geçen gün donaným ve yazýlým bazýnda yeni güvenlik açýklarý bulunmaktadýr.

1.4 Performans Kavramý:

Performans iº yapabilme kabiliyetidir. Bu birim zamanda yapabileceði iþ miktarý gibi de tanýmlanabilir. Performans denince akla ilk gelen kavramlardan bir tanesi de hýz kavramýdýr. Zira performans ve hýz kavramlarý bir bütündür.

1.5 Performans Kavramýnýn Kurumsal Að Ýçerisindeki Yeri

Kurumsal að içerisinde veri alýþveriþindeki hýz, birim zamanda yapýlabilecek iþ miktarý ile doðru orantýlýdýr. Ayrýca birim zamanda

gönderilebilecek veri miktarýda performans açýsýndan önemlidir.

Örneðin bir bilgisayar üzerinde kullanýcý için gerekli olmayan servislerin kapatýlmasý mevcut bilgisayarýn performansýný artýracaktýr.

1.6 Saldýrý türleri

Genellikle çok karþýlaþýlan saldýrý türleri aþaðýda özetlenmiþtir.[10]

Probe,Scan,Scam: Bir sistemdeki açýk ve kullanýlan portlarýn taranmasý ve bu portlardan hizmetlere yönelik saldýrýlarý türüdür.

Prank: Kullanýcý hesaplarýnýn yanlýþ oluþturulmasý sonucu oluþan açýklardan

yapýlan saldýrý türleridir.

Email spoofing: Baþka bir kullanýcý adýna e-posta gönderilmesi...

Email bombardment: Bir e-posta adresine genelde farklý adresten çok sayýda e-postagönderilmesi

Sendmail attack: Smtp portuna yönelik saldýrýlardýr...

Break-in: Verilen hizmetlerin devre dý ý býrakýlmasýna yönelik saldýrý türüdür.

Intruder gained root access: Saldýrganýn normal kullanýcý olarak girdi i sistemde süper kullanýcý yetkisini kazanmasý.

Intruder installed trojan horse program: Saldýrganýn girdi i sisteme genelde daha sonra tekrar rahat girebilmesi ya da uzaktan yönetim için ajan program yerle tirimesi.

Intruder installed packed sniffer: Saldýrgan tarafýndan hedef makinaya yönelik paket dinleyici yerle tirilerek yapýlan saldýrý türüdür. Bu þekilde bir yerel að korumasýz bir konak üzerinden saldýrýlara açýk hale gelebilir.

NIS attack: Að kullanýcý yönetim sistemine yönelik saldýrý türüdür.

NFS attack: Að dosya yapýsýna yönelik saldýrý türüdür. Genellikle að eriþimini devre dýþý býrakmada kullanýlýr.

Telnet attack: Uzaktan eriþim protokolünün açýklarýndan faydalanýlarak yapýlan saldýrý türüdür.

Rlogin or rsh attack: Uzaktan eriþimde kullanýlan servislerin açýklarýna yönelik yapýlan saldýrý türüdür.

Cracked password: Kolay tahmin edilebilir parolalarýn tahmini ya da þifreli hallerine gore sözlük saldýrýsý yapma türüdür.

Anoymous FTP abuse: Anonim eriþiim izni verilen dosya aktarým sunucularýna yönelik saldýrýlardýr.

IP spoofing: IP adres yanýltmasýyla yapýlan saldýrý türüdür.

Configuration error: Çok kullanýlan programdaki kullanýcýlardan kaynaklanan konfigürasyon hatalarýndan do an açýklýklardýr.

Misuse of hosts resources: Konak kaynaklarýnýn yanlý kullanýmý sonucu ortaya çýkan açýklýklar.

- Worm,Virus Konaklarda kullanýcýlardan habersiz çalýþan zararlý programlar[3]

2. Test Kavramýnýn Ýncelenmesi ve Güvenlik Duvarlarýnda Testin Gerekliliði

Testin amacý; mevcut Güvenlik Duvarý Sisteminin amacýna uygun bir þekilde çalýþýr olduðundan emin olmak ve tanýmlanan kurallarýn istenilen þekil de olup olmadýðýndan emin olmaktýr. Ayryca performans artýrýmý için yapýlabilecekleri analiz etmektir. Burada bahsedilen Güvenlik Duvarý sistem testi, sadece Güvenlik Duvarýný deðil Güvenlik Duvarý ile birlikte çalýþan sisteminde bir bütün olarak gözden geçirilmesidir.

Güvenlik Duvarý Sisteminin testi, sistem iþleyiþinin istenilen þekilde iþleyip iþlemediðini ve performansýndan emin olmaktýr.

Hata mesajlarý anlaþýlýr ve çözüm getiren açýklamalar içermelidir. Donanýmsal veya yazýlýmsal olarak her tipteki hata analiz eidilebilir olmalýdýr. Çünkü bir hata olduðunun sistem tarafýndan bildirilmesi hataným kaynaðýnýn bildirilmemesi veya bilinmeyen bir hata mesajý alýnmasý istenilen bir durum deðildir. Testin bir amacý'da bilinmeyen yani öncesinde analiz edilmeyen bir hata durumunu araþtýrmak olmalýdýr.

Güvenlik açýðýnýn en önemli nedeni mevcut sistem yapýlandýrmasýnýn hatalý

yapýlandýrýlmasýndandýr. Bir Güvenlik Duvarý sistemi oluþturulduðunda mutlaka gerekli testlerden geçirilip yapýdan emin olunmalýdýr.

2.1 Güvenlik Duvarlarý Testi Konulu Yapýlan çalýþmalar

Ýlk olarak bahsedeceðimiz makale çevirisi Khalid Al-Twai ve Ýbrahim A. Al-Kaltham tarafýndan yapýlan ve konusu "Evaluation and Testin of Internet Firewalls" olan yani "Ýnternet Güvenlik Duvarlarýnýn Deðerlindirilmesi ve Testi" konulu bir araþtýrmasýdýr. Araþtýrmanýn amacý internet güvenlik duvarlarýnýn deðerlendirilmesi ve piyasada iyi bilinen iki güvenlik duvarýnýnda ele alýnarak test yöntemlerinin anlatýmýna yer verilmesidir. [4]

Anlatýmda bazý mevcut Güvenlik Duvarý ürünlerini açýklanmýþ 1) Trusted Information Systems Inc. Tarafýndan geliþtirilen TIS Güvenlik Duvarý aracý 2) D.Koblas tarafýndan geliºtirilen socks kütüphaneleri.

Bu ürünlerin ikisi de kamu etki alanlý güvenlik duvarlarýdýr.
Bunlarýn tanýmýna kýsaca bir göz atarsak;

TIS intenet Güvenlik Duvarý Aracý (FWTK)

TIS intenet Güvenlik Duvarý aracý Amerikan savunma bakanlýðý tarafýndan organize edilen bir çalýþmada hazýrlanan software modullerinden ve konfigurasyon kýlavuzlarýndan oluþur. Toolkit öðeleri beraber çalýþacak þekilde tasarlanmýþtýr. Fakat tek baþýna veya diðer Güvenlik Duvarý öðeleriyle birlikte de kullanýlabilir. Güvenlik Duvarý yazýlýmý Unix sistemlerde Berkeley soket arayüzüyle birlikte TCP/IP yi kullanýr

Socks Güvenlik Duvarý

Socks paketi bir internet soket servisidir. 3 bölümden oluºur: 1)client library rutinleri, 2)daemon, 3)Güvenlik Duvarý host üzerinden uygun ve güvenli bir network baðlantýsýný saðlayacak bir protokol.

Test Ortamlarý olarak; test yataðý tek bir güvenlik duvarýnýn belli bir zamandaki performansýný deðerlendirmek üzere tasarlanmýþ Bu bölümde güvenlik duvarlarýnýn deðerlendirilmesi ve kýyaslanmasýyla ilgili 3 farklý test yataðý kullanýlmýþ Bu üç test yataðýnýn avantaj ve dezavantajlarýný gösterilerek bunlar denenecek olan güvenlik duvarlarýnýn çalýþtýðý hostlar ve network analizi ya da hack simülasyon araçlarýnýn çalýþtýðý hostlar arasýnda kurulacak baðlantý saðlamak için omurga mimarisi oluþturmada kullanýlmýþ Daha sonra testlerin sonuçlarý incelenerek tablo oluºturulmuº.

Yapýlan çalýþmada bazý güvenlik deðerlendirme araçlarýnýn yardýmýyla bazý Güvenlik Duvarý ürünleri deðerlendirilmiþ Bazý test metotlarý geliþtirilip iki Güvenlik Duvarý karþýlaþtýrýlmasý için kullanýlmýþ SOCKS ve TIS\FWTK. Bununla birlikte herbir Güvenlik Duvarý un farklý bir ortama ihtiyaç duyduðu ortaya çýkmaktadýr. Örneðin bir uygulama düzeyi Güvenlik Duvarý olan FWTK, birleþik güvenlik ortamýndan daha çok akademik olarak tanýmlanabilecek, daha fazla güvenlik ve daha az esneklik ortamý sunar. Diðer taraftan, aygýt düzeyi bir Güvenlik Duvarý olan SOCKS, birleþik güvenlik ortamlarýndan daha çok akademik görünen Daha fazla esneklik ve daha az güvenliðin olduðu bir ortam sunar. Bu deneyde iki Güvenlik duvarýnýn otomatik deðerlendirilmesini yapmak için SATAN güvenlik analiz aracýný kullanýlmýþ SATAN bu proje baþladýðýnda çok yaygýndý. Fakat þu anda SATAN ýn kontrol ettiði birçok güvenlik açýðý güncel yazýlýmlarla düzeltilmiþtir. Yeni yazýlýmda da yeterince korunmayan alanlar bulunabilir.

Bir diðer akademik çalýþma da H.Joseph Wen (School of Management, New Jersey Institude of Technology, Newark, USA) ve Jyh-Horng Micheal Tarn (Information Systems, Department of Business, Chowan College, Murfreesboro, USA) tarafýndan yapýlan Internet Güvenliði: Güvenlik Duvarý Seçimindeki Hususlar (A Case Study of Firewall Selection) konulu çalýþmadýr[2]. Bu çalýþmada da yine Güvenlik Duvarý mimarileri incelenmiþ ve güvenlik duvarý seçiminde dikkat edilmesi gereken hususlar anlatýlmýþtýr. Genel olarak paket filtreleme, kullanýcý onaylama (User Authentication), Uyarý Denetimi gibi özellikler incelenmiº.

Tablo 1. Konfigurasyon ve çalýþtýrma kýyaslamasý

Karþýlaþtýrma Faktörleri	**SOCKS v5**	**TIS FWTK 2.0**
Yükleme öncesi konfigurasyon	Çok opsiyonlu,otomatik	Manuel(host sistem hakkýnda bilgi gerektiriyor)
Yükleme	Otomatik	Otomatik (Fakat tek öðeler ayrý ayrý deðerlendirilmeli)
Programlar	Tek program	Ayrýk küçük programlar
Etkilenen makinalar	Sunucu ve bütün dahili/harici client workstationlar	Yalnýzca sunucu
Desteklenen mimariler	Tekli ve çoklu hostlar	Tekli ve çoklu hostlar
Host Güvenliði	Geliºtirilmemiº	Geliºtirilmiº
Clientler	Aþaðýdakilerden biri kullanýlarak Sock uyumlu yapýlmalýdýr 1) Statik 2) Dinamik	Özel bir iºlem gerekmiyor
Authenticate opsiyonlarý	Herhangi bir authenticate opsiyonu	Herhangi bir authenticate opsiyonu
Eriþim kontrol opsiyonlarý	Aþaðýdakileri tanýmlayan kurallar tarafýndan; 1) Kaynak ve varýþ host adresleri 2) Kaynak ve varýþýn servis portu 3) Kullanýcý adý/ password 4) Arayüz adresi	Bireysel servisler tarafýndan; 1) Kaynak host 2) Kullanýcý adý/password 3) Güçlü authenticate 4) DNS kontrolü
Arayüz algýlama	Network arayüzlerini algýlar	Arayüzleri algýlamaz
Etki Alaný Servisleri	Kontrol edilmez	IP adres spoofing etkisine karþý kontrol edilebilir
TCP tabanlý Servisler	SOCK uyumlu hale getirilerek kullanýlabilir	1) FWTK að geçidi Poxy leri þunlarý kapsar: ftp, http, rlogin,telnet, X11 and plug-gw 2) Netacl diðer TCP tabanlý servisleri kontrol etmede kullanýlýr.
UDP tabanlý servisler	Uygulanamaz	UDP servisler kullanýlamaz. Bir çok UDP tabanlý hizmet sunucular forward etme görevini yerine getirecek ºekilde ayarlandýktan sonra kullanlýlabilir.

Karþýlaþtýrma Faktörleri	**SOCKS v5**	**TIS FWTK 2.0**
Güvenlik Duvarý türü	Devre düzeyi	Uygulama düzeyi
Güvenlik duvarýnýn baþlatýlmasý, restlenmesi ve durdurulmasý	SOCKs komutlarýný kullanarak basitçe	Ýstenen servisleri seçebilmek için inetd.conf un deðiþtirilmesini ve inetd daemon unun resetlenmesini gerektirir.
Clientlar	Sock uyumlu uygulamalarý kullanmak zorundalar	Diðer tarafa baðlanmadan önce FWTK sunucuya baðlanmak zorundalar.
Þeffalýk	Kullanýcýlar için %100 þeffaf hale getirilebilir	FWTK sunucuya baðlanmasý gereken kullanýcýlar için þeffaf deðildir.
Inbound baðlantýlar	Yalnýzca socks sunucu ve clientlardan	Socks sunucu ve clientlar da olabilen herhengibir TCP/IP wokstationdan
Diðer Güvenlik Duvarýyla baðlantý	Socks clientlar FWTK sunucu aracýlýðýyla baðlanabilirler	FWTK clientlar Socks sunucu aracýlýðýyla baðlanamazlar
Güvenlik Duvarý host eriºilebilirliði	Güvenlik Duvarý hosta eriþmeye imkan tanýmaz.	Farklý yollarla izin verilebilir veya engellenebilir.
Ýzin verilen servisler	Herhangi sock uyumlu uygulama ve servis	Yalnýzca FWTK sunucu kontrolunde çalýþan FWTK proxy servisleri ya da standart servisler

Tablo 2. SOCKS ve FWTK kullanýmý kýyaslamasý

Artýlar	Eksiler
ª effaf	Devre düzeyi: Kontroller yalnýzca baðlantý zamanýnda yapýlabilir.
Socks clientlar Sock olmayan diðer TCP/IP tabanlý güvenlik duvarý aracýlýðýyla baðlanabilirler	Yalnýzca socks sunucu ve clientlardan gelen baðlantýlar kabul edilir.
Authenticate ve ºifreleme	VarýþSocks Güvenlik Duvarý adresi local socks sunucu tarafýndan bilinmeli ve konfigurasyon dosyasýnda bulunmalýdýr.
Kaynak/VarýþHost/Port kombinasyonlarýyla eriºim kontrolü	Locak socks Güvenlik Duvarý adresi kendi clientlarý tarafýndan bilinmeli ve herbirinin konfigurasyon dosyasýnda bulunmalýdýr.
Arayüz algýlama	Yalnýzca Sock uyumlu uygulama ve servisler Güvenlik Duvarý dan geçebilir.
Güvenlik Duvarý hosta baðlantý yapýlamaz(Güvenlik duvarýnýn türü devre düzeyi olduðu için bu avantaj olarak kabul edilir)	Çalýþtýðý hostun güvenliði artýrýlamaz.
	UDP desteðinin olmamasý

3. Güvenlik Duvarlarında Test Yönteminin Geliştirilmesi ve Güvenlik Duvarý Testleri

Bazý Güvenlik Duvarlarý paket filtreleme tekniði kullanýrlar[9] ve bu filtreleme deðişken yeteneklerde de kullanýlabilir. Bu yüzden Güvenlik Duvarýnýn test edilip deðerlendirilmesi gerekmektedir. Güvenlik Duvarlarýn testi ve deðerlendirmesi organizasyon için doðru, uygun ve fonksiyonellik olarak tatmin edicilik için yardýmcý olur.

Yaptýðýmýz inceleme sýrasýnda ki Güvenlik Duvarlarý günümüzde ki en çok tercih edilenler arasýndan seçilerek incelenmiştir. Ayrýca Güvenlik Duvarýlarýn seçiminde;

- . Desteklediði Platformlar
- . Güncelleme mekanizmasý
- . Kontrol mekanizmasý
- . WEB site Ýzleme
- . Güvenlik Politikasý
- . Virüs Tarama
- . Veritabanýerişimi
- . Að Adresi Dönüştürme (NAT)
- . Kriptolama
- . GUI tabanlý yönetim
- . Uyarý mekanizmasý

gibi konulara dikkat edilir.

3. 1 Güvenlik Duvarý Testleri [7,9]

3.1.1 Donanýmsal (Yapýsal) Test

Donanýmsal test, mimari yapýnýn incelenmesi ve analiz edilmesidir. Güvenlik Duvar'larýn mimari içinde ki yerinin güvenlik ve performans açýsýndan yeterliliðinin testidir. Çünkü bir mimaride Güvenlik Duvarý að üzerinde bulunduðu yer itibariyle üzerinden geçen að trafiði, onun performansýný ve güvenlik içeriðini etkileyecektir.

3.1.2 Yazýlým Testi

Güvenlik Duvarý yazýlýmýnýn hangi proðramlama dilinde yazýlý olduðu ve bununla birlikte yazýlýmýn artý ve eksilerinin incelenmesi.

3.1.3 Güvenlik Testi

Güvenlik testinin amacý; konfigurasyonu yapýlan güvenlik duvarýnýn internet ortamýnda iyi bilinen yüzlerce atak formlarýna karşý güvenilirliðini test etmektir. Bu tür testler için gerek internet ortamýnda gerekse firmalar tarafýndan programlar satýlmakta ve desteði verilmektedir.

3.1.4 Performans Testi

Performans testi, güvenlik duvarýnýn data trafiðinde paket/zaman başarým oraný testidir. Data trafiðinde ki iletişim sýrasýnda gelen ve giden datalarý check etme süresi, bellek durumu, datanýn yogunluguna gore başarýmý göz önünde tutulurGüvenlik duvarlarý kendi aralarýnda da yapýlarýna göre elbette ki farklý performanslar gösterir. Bir yazýlým güvenlik duvarý ile donaným güvenlik duvarý arasýnda bu durum daha açýkca görülür. Ayrýca performans testinde limit deðerlere (Veya sýnýr deðerler) yakýn deðerlerde olan trafik akýşýnda güvenlik duvarýnýn göstereceði performans, oluşabilecek hatalarýn test edilmesi gerekmektedir.

3.1.5 Yönetimsel Test

Güvenlik Duvarý konfigurasyonunun yönetimsel testidir. Güvenlik Duvarlarýnýn yönetilebilirliði ve kurulum kolaylýðýnýn testidir. Arayüzeylerin anlaşýlýrlýðý, konfigurasyon sýrasýnda oluşabilecek hatalar, uyarýlar önemlidir. Her konuda olduðu gibi burda da anlaşýlýrlýk önemlidir. Kişi önceden yaptýðý konfigurasyonu kolaylýkla analiz edebilmelidir.

3.1.6 Kullanýşlýlýk Testi

Kullanýlýşlýk Testi; kurulum kolaylýðý, konfigurasyon, yönetim, dokumante işlemi, yardým menüsü ve raporlama özelliðinin test edilmesidir. Bu konu hakkýnda uzman kişinin görüşü bakýmýndan ele alýnýr. Bu konu altýnda AltaVista Güvenlik Duvarý 97 ile Check Point Güvenlik Duvarý incelenirse;

3.1.6.1 AltaVista Güvenlik Duvarý 97

AltaVista Güvenlik Duvarý 97; özel network'lerle internet arasýnda veya güvenli kalmasý gereken TCP/IP uygulamalarý arasýnda güvenli baðlantý saðlayan, kolay yönetilebilen, ileri raporlama ve alarm özelliklerine sahip bir güvenlik yazýlýmýdýr. Saðladýðý olanaklar açýsýndan aşağýdaki özelliklere sahiptir.

Avantajlar ;
Servisler açýsýndan güvenilir uygulamalara sahiptir (FTP, Telnet, WWW, Mail, News, RealAudio ve Finger)

- Kurulumu kolaydýr (Adým adým instolasyon)
- Yönetimi kolaydýr (Güvenlik Duvarý loglarý uzaktan izlenebilir, servisler Start/Stop edilebilir, gerçek zaman monitoring, gerçek zaman raporlama, istatistik ve alarm analizleri, çok sayýda güvenlik duvarý yönetimi uzaktan yapýlabilir).
- Altavista Güvenlik Duvarý 97; Dual-DNS sunucu olarak konfigüre edilebilir (Grafic User Interface tabanlý konfigürasyon kullanýlarak, name servislerin; internal servis veya external servis olduðu anlaþýlabilir).
- Alarm özellikleri açýsýndan ileri çözümler sunmaktadýr (Yeþil, sarý, turuncu ve kýrmýzý renkleri üzerinde çeþitli alarm tipleri tanýmlanarak, herhangi bir kötü niyetli giriþimin durumu ekranda izlenebilir. Sistem yöneticisine mail gönderilmesi saðlanabilir).
- Altavista Güvenlik Duvarý 97; Uniform Resource Location (URL) bloklamaya izin verir
- (URL'nin bloklama yaptýðý www servisleri þunlardýr: HTTP, Gopher, FTP, SSL)
- Konfigurasyonu ve kontrolü en kolay güvenlik duvarlarýndan biridir(GUI olanaklarý ile)
- Altavista Güvenlik Duvarý 97; hem Windows NT hem de UNIX iþletim sistemleri üzerinde çalýþabilmektedir. Ancak en iyi performansý, DIGITAL UNIX iþletim sistemi üzerinde çalýþýrken göstermektedir (IP paket filtreleme, Enhanced www proxy, generic UDP proxy ve DMZ desteði; Altavista Güvenlik Duvarý 97'nin windows NT iþletim sistemi üzerinde çalýþtýrýlmasý durumunda verilmemektedir)

Dezavantajlar ;

- Altavista Güvenlik Duvarý 97; çok büyük netwokler için elverişli deðildir (Kim olduklarýna bakýlmaksýzýn, Güvenlik Duvarý dýþýndaki her baðlantýya benzer davranýr; sistem yöneticilerine özel ayrýcalýklar tanýnmaz)
- 2 LAN arabirimi kullanmaktadýr (Tüm diðer Güvenlik Duvarlarý en az 3 LAN arabirimi kullanmaktadýr)

3.1.6.2 Checkpoint Güvenlik Duvarý

Check Point Güvenlik Duvarý-1; internet, intranet/extranet ve uzaktan eriþim saðlayan kullanýcýlar için, çok güçlü authentication, kodlama ve network address translation (NAT) yetenekleriyle güvenlik hizmetleri sunan bir yazýlýmdýr. Saðladýðý olanaklar açýsýndan aþaðýdaki özelliklere sahiptir.

Avantajlar ;

- Grafiksel olarak log görüntüleme olanaklarýný sunmaktadýr (Güvenlik Duvarýna yapýlan tüm baðlantý giriþimlerinin ve geçerli olan baðlantýlarýn izlenmesi olanaklýdýr).
- "Inspection Module" yardýmý ile veri, tüm paket katmanlarýnda incelenebilir. Bu modülle; paketin IP adresi, port numarasý bilgileri elde edilebilir, bir baðlantý gerekirse reddedilir.
- Merkezi yönetim olanaklarýyla; network'ler, kullanýcýlar, sunucular için güvenlikle ilgili parametreler güncelleþtirilebilir, baðlantý isteklerine iliþkin loglar analiz edilebilir, görüntülenebilir, print edilebilir.
- Her kullanýcý için; FTP, TELNET, HTTP, RLOGIN servislerinin kullanýmýna yönelik sýnýrlama getirilebilir. Ancak özel konfigürasyonlarla, sistem yöneticilerine bazý ayrýcalýklar tanýnabilir.
- "Network Address Translation" özelliði ile, geçersiz veya gizli IP adreslerinin internal olarak kullanýlmasý saðlanabilir. Bu özellikle, internet'e tek bir IP adresinden ulaþýlab ilir(Dinamik olarak bir port numarasý geçersiz IP adreslerini, geçerli bir tek IP numarasýna çevirir); böylece internal olarak binlerce IP adresi kullanýlabilir. Host veya sunucular IP adresleri yerine, isimleriyle temsil edilebilir; bu özellik de güvenliði artýran unsurlardan bir tanesidir.
- FTP, SMTP ve HTTP uygulamalarýna iliþkin virüs taramasý yapýlabilir (Dosya ve mail)
- Güvenlik Duvarý gruplarýnýn tek bir baþlýk altýnda konfigure edilmesi olanaðýný sunmaktadýr. Grafic User Interface (GUI) kullanýlarak, Güvenlik Duvarý gruplarýna ve paket filtreleme yapan yönlendiricilere

iliºkin kurallar enterprise'da install edilebilir.

- Virtual Path Network (VPN) kullanýlarak, internal veya internet üzerinde güvenli haberleþme yapýlabilir.
- HTTP, URL ve içerik tabanlý filtreleme, güvenlik alanýnda en önde gelen konulardandýr. Ýçerik tabanlý filtreleme; Java ve ActiveX programlarýnýn yerel aða girmesine engel olmak amacýyla kullanýlmaktadýr.

Dezavantajlar ;

- DIGITAL UNIX iºletim sistemini desteklememektedir.

Sonuç olarak;
Altavista Güvenlik Duvarý 97; hem Windows NT hem de UNIX iºletim sistemleri üzerinde çalýþabilmektedir. Ancak en iyi performansý, DIGITAL UNIX iºletim sistemi üzerinde çalýþýrken göstermektedir (IP paket filtreleme, Enhanced www proxy, generic UDP proxy ve DMZ desteði; Altavista Güvenlik Duvarý 97'nin windows NT iºletim sistemi üzerinde çalýþtýrýlmasý durumunda verilmemektedir)
CheckPoint Güvenlik Duvarý-1; Windows 3.51, Windows 4.0 ve UNIX (Sunos, Solaris ve HP-UX) iºletim sistemlerini desteklemekte, ancak DIGITAL UNIX iºletim sistemini desteklememektedir

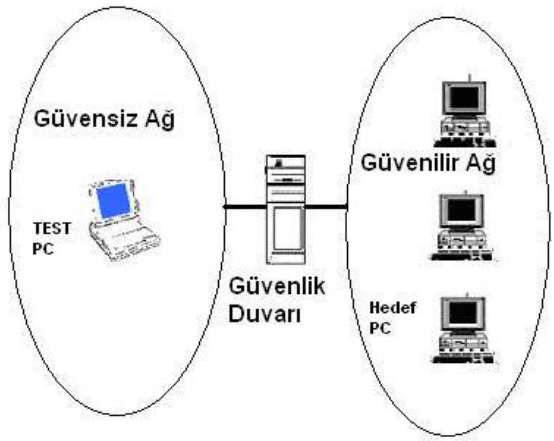
4 Güvenlik Duvar Test Ýþlemleri

Testi yapacak olan PC'yi aslýnda saldýrý yapan hacker PC olarak ta tanýmlayabiliriz. Bu PC si ilgili ºekil 1 ve ºekil 2'de de görüleceði gibi yerel að üzerinde belirlenen konumlarda bilinen tüm saldýrý teknikleriyle hedef network'e saldýrýr.

Test PC si genel olarak aþaðýda belirtilen genel að yapýlarý içerisinde olarak gerekli test iºlemlerini yapar.

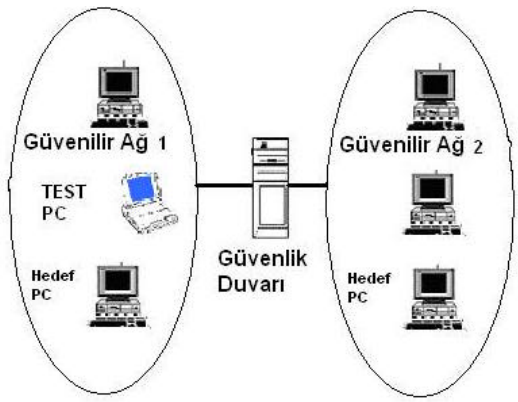
Mevcut korunmasýný istediðimiz aðý güvenli að, internetide güvensiz að olarak tanýmlarýz.
Aþaðýda ki þekilde Test PC si güvensiz að üzerinden Güvenilir aða atak yapmaktadýr.

Örneðin bir port taramasý yapabilir. Böylelikle açýk, kapalý portlar test edilmiþolur.



Þekil 1. Test Bilgisayarýnýn Güvensiz Að Üzerinden Güvenlik Duvarýna Baðlantýsý

Aþaðýda ki þekilde ise mevcut güvenilir birden fazla networkün olduðu bir aðda her iki güvenilir að arasýnda ki bir güvenlik duvarý üzerinden hedef PC ye atak yapýlarak test yapýlmaktadýr.



Þekil 2. Test Bilgisayarýnýn Güvenilir Ýki Að arasýnda Güvenlik Duvarýna Baðlantýsý

4.1 Test Yöntemi

Test yöntemimiz önceki test yöntemlerine bazý yönlerden benzerlik taþýmasýna raðmen genel olarak test yönteminin geliþtirilmesi açýsýndan yeni analizler içermektedir. Bir test yönteminin nasýl olmasý gerektiði ile ilgili anlatýmlara öncelikle yer verilmiºtir. Daha sonra da güvenlik duvarý öncelikle tek baþýna ele alýnmakta ve incelenmekte, bununla beraber güvenlik duvarý tarafýndan korunan sistemin de bir bütün olarak ele alýnmasýyla test yöntemi uygulanmakta.

Yazýlan bir programla güvenlik duvarý test edilmekte ve analizler yapýlmakta. Ayrýca uzman

kişiler tarafından da tüm sistemin incelenmesi gerektiğinin önemi belirtilmektedir.

Yazılan proğram öncelikle güvenlik duvarı üzerinde ki açık portları taramakta ve bu portlardan gelebilecek saldırılara karşı kullanıcıyı bilgilendirmekte ve öneri sunmaktadır.

Güvenlik duvarına yüksek miktarda data gönderilerek tanımlanan kuralların (rule) işlevi engellenmeye çalışılmıştır. Bu sayede güvenlik duvarının performans testi yapılmaktadır.

4.2 Test Programının Yapısı

Programın amacı bir güvenlik duvarının ve beraberinde tüm sistemide ele alarak güvenlik testini yapmaktır. Program tasarlanırken amaç, tamamiyle yeni bir hack programı yazmak değil, bilinen en popüler hack programları da araştırılıp bunların içerisinden en iyi ve etkili olanlarının analiz edilip VisualBasic 6.0 yazılan bir test programına dahil edilmesidir. Ayrıca bu programla Güvenlik Duvarı üzerinde tanımlanan kurallar (rule) test edilmektedir.

Programda özellikle port tarama programlarına ilk başta yer verilmekte ve genel testler de bunlarla yapılmakta. Mevcut açık portlar belirlenmekte ve bu portlardan gelebilecek saldırı türleri hakkında bilgilendirme yapmaktadır. Portun açık olmasının ne gibi riskler taşıdığı ve sonuç olarak öneriler sunmaktadır.

Ayrıca Güvenlik Duvarına proğram tarafından yüksek miktarda veri gönderilerek meşgul edilmekte ve kural (rule) tanımlamalarını sağlıklı çalışmasıı önle nerek oluşabilecek hata ve açıklar analiz edilmeye çalışılmakta.

Ayrıca test programı sadece Güvenlik Duvarını değil Güvenlik Duvarının olduğu tüm sistemi ele alınarak tasarlanmıştır.

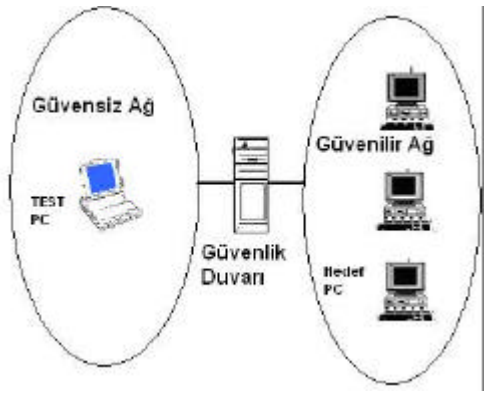
4.3 Test Yönteminin Uygulanması

Test yönteminin uygulanması için öncelikle test ortamı incelenir. Çünkü güvenlik duvarının sistem içinde ki yeride çok önemlidir. Sistemin genel olarak yapısı incelenirken donanımsl ve yazılımsal olarak incelenmelidir. Çünkü güvenlik duvarının izin verdiği bir erişimden bilgisayarınızda ki backdoor dan zarar verilebilir ya da sistem açıklarından zarar verilebilir.

Mevcut korunmasını istediğimiz ağı güvenli ağ, dışınetworküde güvensiz ağ olarak tanımlarız.

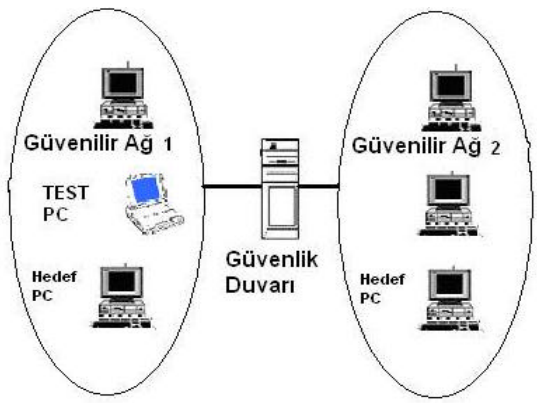
Aşağıdaki şekil -3 de Test PC si güvensiz ağ üzerinden Güvenilir ağa atak yapmaktadır.

Örneğin bir port taraması yapabilir. Böylelikle açık ve kapalı portlar test edilmişolur.



Şekil-3 Test Bilgisayarının Güvensiz Ağ Üzerinden Güvenilir Ağda ki Hedef PC'yi Güvenlik Duvarı Üzerinden Testi

Şekil-4 de ise mevcut güvenilir birden fazla networkün olduğu bir ağda her iki güvenilir ağ arasında ki bir güvenlik duvarı üzerinden hedef PC ye atak yapılarak test yapılmaktadır.



Şekil-4 Test Bilgisayarının Güvenilir Ağ-1 Üzerinden Güvenilir Ağ-2 de ki Hedef PC'yi Güvenlik Duvarı Üzerinden Testi

Daha sonra da güvenlik duvarı öncelikle tek başına ele alınmakta ve incelenmekte, bununla beraber güvenlik duvarı tarafından korunan

sistemin de bir bütün olarak ele alýnmasýyla test yöntemi uygulanmaktadýr.

Yazýlan programla güvenlik duvarý test edilmekte ve analizler yapýlmakta. Ayrýca uzman kiþiler tarafýndan da tüm sistemin incelenmesi gerektiðinin önemi belirtilmektedir. Yazýlan program öncelikle güvenlik duvarý üzerinde ki açýk portlarý taramakta ve bu portlardan gelebilecek saldýrýlara karþý kullanýcýyý bilgilendirmekte ve öneri sunmaktadýr.

Güvenlik duvarýna yüksek miktarda data gönderilerek tanýmlanan kurallarýn (rule) iþlevi engellenmeye çalýþýlmýþtýr. Bu sayede güvenlik duvarýnýn performans testi yapýlmaktadýr. Ayrýca Güvenlik Duvarý konfigurasyonunu yapan sistem yöneticiside sonuçta tanýmladýðý kurallarýn (rule) istenilen þekilde olup olmadýðýný test etmesi gerekmektedir. Çünkü Güvenlik Duvarý hatalý konfigürasyonunuz sonucu istenilen þekilde hizmet edemeyebilir. Sorumlulukda burada tamamiyle konfigurasyonu yapan sistem yöneticisine aittir.

Programda özellikle port tarama programlarýna ilk baþta yer verilmekte ve genel testler de bunlarla yapýlmakta. Mevcut açýk portlar belirlenmekte ve bu portlardan gelebilecek saldýrý türleri hakkýnda bilgilendirme yapmaktadýr. Portun açýk olmasýnýn ne gibi riskler taþýdýðý ve sonuç olarak öneriler sunmaktadýr. Örneðin eðer güvenlik duvarý üzerinden yerel aða port 25 yani SMTP portu açýk hale getirilmiþse bu port 25 den gelecek tüm saldýrýlara yerel að açýk demektir. Bu yüzden port 25 açýk olsa bile mail sunucu dýþýnda ki tüm sunucularýn SMTP Servisleri stop edilmelive güvenlik duvarýnda da sadece IP olarak mail sunucular için bu port açýk olmalýdýr. Proðram böyle bir açýk bulursa bu gibi ayrýntýlý öneriler sunmaktadýr.

Ayrýca Güvenlik Duvarýna proðram tarafýndan yüksek miktarda veri gönderilerek meþgul edilmekte ve kural (rule) tanýmlamalarýn saðlýklý çalýþmasý önlenerek oluþabilecek hata ve açýklar analiz edilmeye çalýþýlmakta.

Ayrýca test programý sadece Güvenlik Duvarýný deðil Güvenlik Duvarýnýn olduðu tüm sistemi ele alýnarak tasarlanmýþtýr.

4.4 Yerel Aðýn Tanýnmasý

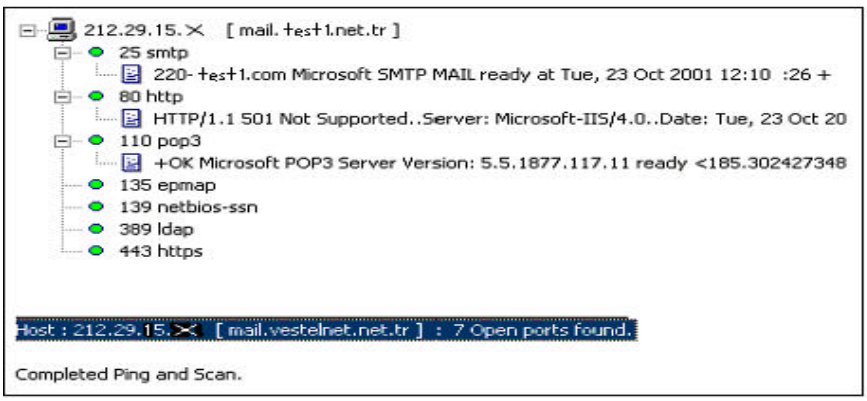
Yerel Aðýn tanýnmasý sunucu ve istemcilerin iþletim sistemleri ve donanýmlarýnýn bilinmesi, ki bu bir þirket için herzaman bilinmesi gerekli olan bir konudur ve bunun için bir durum listesi oluþturulmaludýr. Yerel aðda bulunan güvenlik duvarý tipi, anahtar, hub, yönlendiricilerinde bilinmesi gereklidir. Örneðin bir yönlendirici de güvenlik duvarý olarak yerel aðý koruyabilir.

4.5 Port Tarama ve Sonuçlarý

Port tarama program üzerinde bulunan port tarama butonuna basýldýðýnda karþýmýza birden fazla port tarama proðramlarý çýkar. Bunlar sonuçta ayný iþi yapmalarýna karþýn yazýlýmlarý ve analiz ayrýntýlarý farklýdýr. Yani kimi basit bir tarama yaparken diðeri daha ayrýntýlý bir inceleme yapmaktadýr. Biz Zorlu Holding bünyesinde bulunan Vestelnet Online Communications and Information Inc. 'nin iki güvenli að arasýnda bulunan CheckPoint Güvenlik duvarýnýn testini yaptýðýmýzda;

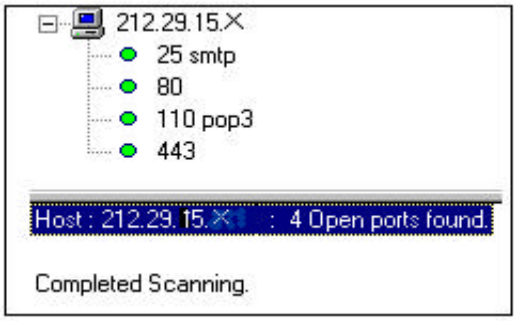
Önemli Not: IP'ler ve Host isimlerigüvenlik amacýyla tam olarak yazýlmamýþtýr.

Verilen bir posta sunucunun ip'sini yerel aðýmýzdan port taramasý yapýlmýþtýr.



þekil-5 Bir Posta Sunucusunun Güvenilir Að Üzerinden Port Taramasý Sonuçlarý

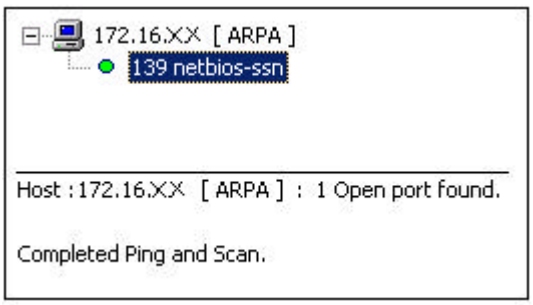
şekil-6 da Dial-up bir bağlantý kurarak port taramasýný güvensiz aðdan güvenli aða doðru yaptýðýmýzda bazý portlarýn daha kapalý olduðunu gözlemleyebiliriz.



şekil-6 Bir Posta Sunucusuna Güvensiz Að Üzerinden Yapýlan Port Taramasý Sonuçlarý

Görüldüðü üzere hiçbir açýk port bulunmamaktadýr. Yani hertürlü eriþim engellenmiþtir. Bu içerden gelebilecek bir saldýrýyý önlemektedir.
Açýk portlardan sunucunun bir posta sunucu olduðu görülmektedir.

Güvenlik duvarýnýn kendisine port taramasý uygulandýðýnda ise;



şekil-7 Güvenlik Duvarýna Yapýlan Port Taramasý Sonuçlarý

Sadece bir tek portu açýk olarak görüyoruz. Çünkü biz aslýnda güvenlik duvarýna deðil onun kurulu olduðu sunucuyu test edebiliyoruz burada. Güvenlik duvarý o sunucuda bir yazýlýmdan ibarettir.

4.6 Güvenlik Duvarýnda tanýmlanan kurallarýn testi

Sistem Yöneticisi kural (rule) tanýmlarken hata yapabilir. Bu yüzden güvenlik duvarýnda ki arayüzlerin kullaným kolaylýðý önemlidir. Sistem yöneticisi bir IP'ye hak tanýmlarken örneðin IP yazýmýnda hata yapabilir veya önceden tanýmlamýþ olduðu bir kural artýk kullanýlmýyor olabilir. Bu gibi durumlarda sistem yöneticisi peryodik kontroller yapmayý ihmal etmemelidir.

4.7 Mevcut Aðýn Meþgul Edilmesi ve Performansýnýn Deðerlendirilmesi

Güvenlik duvarý sonuçta gelen isteklere cevap verme kapasitesi sýnýrlýdýr. Biz program vasýtasýyla yüksek miktarda veri göndererek güvenlik duvarýný sürekli meþgul ettik ve veri gönderme iþi birden fazla bilgisayar tarafýndan yapýldý. Çünkü bir güvenlik duvarýný sadece bir tek PC'den meþgul etmeye çalýþmak yetersiz olacaktý. Belirli bir veri gönderdiðimizde güvenlik duvarýný kullanna diðer PC'lerin veri alýþveriþleri yavaþlamýþ ve mevcut aðda rahatsýz edici bir yavaþlama oluþturduk Bu sýrada güvenlik duvarýnýn gelen isteklere cevap verme süresi, cevap verebilme yeteneði bize onun performansýný göstermektedir.

Örneðin deneme amaçlý olarak Windows NT Sunucu üzerine kurulu bir PC'ye CheckPoint Güvenlik Duvarý kurduk ve bu PC'ye test proðramýmýz ile yüksek miktarda veri gönderdik.

Güvenlik duvarý olan PC bir süre sonra aðda mevcut diðer PC'lere ping dahi atamaz duruma geldi.

Normal þartlarda ping komutuna

Reply from 212.29.65.X: bytes=32 time=20ms TTL=125
gibi yanýt alýnýr. Ancak að meþgul edildiginde;

Reply from 172.16.7.182: bytes=65500 time=550ms TTL=128
Request timed out.
Reply from 172.16.7.182: bytes=65500 time=240ms TTL=128
Request timed out
Request timed out

gibi yanýt alýnýr. Yani Sunucunun að iletiþimi engellenmiþ olur.

4.8 Analiz Sonuçlarýnýn incelenmesi

Sonuç olarak güvenlik duvarýnýn testi, sistemimizin güvenliðinden emin olamýza yarar. Yani sayýsal bir iþlemin saðlamasý gibi. Proðramda manuel olarak yapmamýz gereken

bazý testlerde kullanýcý için kolaylaþtýrýlmýþtýr.Yasaklanan bazý sitelerin gerçekten gelip gelmediði gibi engellemeler otomatik olarak gözlemlenebilmektedir.
Port tarama ve Aðýn meþgul edilerek kurallarýn test edilmesi bu çalýþmanýn temelini oluþturmaktadýr. Yerel aðda bulunan açýk portlarla güvensiz aða karþý açýlan portlarýn farklý olduðunuda yaptýðýmýz testte gördük. Ancak bu sistem yöneticisi ve þirketin sistem güvenliðinden sorumlu kiþilerin bilgisi dahilinde olan birþeydir. Sistem yöneticisi sonuçta içerden gelebilecek saldýrýlara karþý da önlem almak zorundadýr. Ýstatistiklere göre þirket içinden yapýlan saldýrý oraný þirket dýþýndan yapýlan saldýrý oranýndan yüksektir.

5. Sonuç ve Öneriler

Bir aðda yeterli güvenliði saðlamak için basit þifrelerden kompleks güvenlik duvarlarýna kadar deðiþen güvenlik seviyeleri vardýr. Güvenlik seviyesi artýrýldýkça, aða baðlý kaynaklarýnda güvenliði de o derece artýrýlmýþ olur. Tabi bu arada maliyette artmaktadýr. Ýyi bir güvenlik sistemi kolaylýkla ayarlanmalý ve yönetilebilmelidir.

Mevcut aðý korumanýn en iyi yolu bir güvenlik duvarý kullanmaktýr. Güvenlik duvarý, üzerinden geçen að trafiðini analiz eder ve raporlar.

Güvenlik duvarýnýn performansý da að yapýsý için önemlidir. Çünkü performans þirketlerin hýzla geliþen haberleþme teknolojisi içerisinde ihtiyaç duyulan en önemli kavramlar içerisinde yer alýr.

Güvenlik duvarýnýn konfigurasyonu uzmanlýk isteyen bir konudur. Konfigurasyon arayüzeyinin de kolay anlaþýlýr ve yönetilebilir olmasý gereklidir. Hatalý bir konfigurasyon tüm aðý riske atar ve þirket güvenliðini maddi ve manevi yönden zarara uðratabilir.

Bu gibi durumlar göz önüne alýnarak bir güvenlik testi yapýlmasý gerekmektedir. Özellikle güvenlik duvarýnýn ve performansýnýn test edilmesi önem taþýr. Bu manuel olarak da yapýlabileceði gibi mevcut geliþtirilmiþ proðramlar da kullanýlabilir.

Test yöntemi hazýrlanacaðý zaman sadece güvenlik duvarý deðil að yapýsý bütünüyle ele alýnmalýdýr. Güvenlik duvarýnýn að içerisinde konum ve iþlevi önemlidir. Gereksiz kural tanýmlamalarýndan kaçýnmalý, performans verimi sürekli göz önünde tutulmalýdýr.

Test yöntemi oluþturulurken bölüm 3'te verilen güvenlik duvarý seçim özellikleri de da dikkate alýnarak yöntem geliþtirilmelidir. Test yöntemi için geliþtirdiðimiz proðram yukarýda belirtilen konular çerçevesinde yapýlmýþ ve sonuç olarak sistem yöneticisini bilgilendirme ve yönlendirme amacýyla tasarlanmýþtýr. Özellikle performans kavramýna dikkat çekilmiþ ve konunun önemi belirtilmiþtir. Sadece yazýlýmsal testin deðil gözlemsel testinde gerekliliði anlatýlmýþtýr. Mevcut yapýlan çalýþmalardan daha genel bir test yapýsýna sahiptir.

Geliþtirilen test yönteminin her ortama uygulanabilir olmasý önemli bir avantajdýr.

KAYNAKLAR:

[1] Dr. Rýfat ÇÖLKESEN, Prof. Dr. Bülent ÖRENCÝK, "Bilgisayar Haberleþmesi ve Að Teknolojileri", Haziran 1999

[2] H.Joseph Wen and Jhy-Horng Micheal Tarn, "Internet Security:a case of firewall selection" ,Information Management & Computer Security, 6/4 [1998] 178/184

[3] Dennis Steinauer, Stuart Katzke and ShirleyRadack, "Basic Intrusion Protection The First Line of Defense", IT Pro, January | February 1999

[4] Khalid Al- Tawil and Ibrahim A.Al-Kaltham, "Evaluation and Testing of Internet Firewalls", International Journal of Network Management, 1999, 9, pp:135-149.

[5] Cheswick / Bellovin, "Firewalls and Internet Security", Addison-Wesley, 1994

[7] Firewall Mailing List Archieves- http://www.netsys.com/firewalls/

[8] Testing Methodologies http://www.netsys.com/firewalls/firewalls-9508/0066.html)

[9] Reto E.Haeni, "Firewall Penetration Testing", January 1997

[10] Chris Brenton, " Mastering Network Security", SYBEX Inc. 1999.

Yrd. Doç. Dr. Ýbrahim Soðukpýnar. 1982'de Ý.T.Ü. Elektronik ve Haberleþme Mühendisliði Bölümü'nden Lisans, 1985'de Ý.T.Ü. Kontrol ve Bilgisayar Mühendisliði Bölümü'nden Yüksek Lisans, 1995'de Ý.T.Ü. Bilgisayar Mühendisliði Bölümü'nden Doktora derecelerini aldý. Halen Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliði Bölümünde Yrd.Doçent olarak görevini sürdürmektedir.

Serkan Kurt. 17.06.1976 Kýrýkkale doðumlu. 1995'de öðrenime baþladýðý Ýstanbul Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Bölümünden 1999'da mezun oldu. Þubat 2000'de Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliði bölümünde yüksek lisansa baþladý. Eðitimi devam etmektedir. Araþtýrma konularý: Güvenlik Duvarlarýnda Tercih Kriterleri, Güvenlik Duvarlarýnda Test Yönteminin Geliþtirilmesi, Güvenlik Duvarlarýnda Tasarým Yöntemi. Vestelnet Online Communications and Information Inc. 'de sistem mühendisi olarak çalýþmaktadýr.