T.C.
MİLLÎ EĞİTİM BAKANLIĞI

MEGEP

(MESLEKİ EĞİTİM VE ÖĞRETİM SİSTEMİNİN GÜÇLENDİRİLMESİ PROJESİ)

BİLİŞİM TEKNOLOJİLERİ

AĞ GÜVENLİĞİ (DONANIM)

ANKARA 2008

Milli Eğitim Bakanlığı tarafından geliştirilen modüller;

- Talim ve Terbiye Kurulu Başkanlığının 02.06.2006 tarih ve 269 sayılı Kararı ile onaylanan, Mesleki ve Teknik Eğitim Okul ve Kurumlarında kademeli olarak yaygınlaştırılan 42 alan ve 192 dala ait çerçeve öğretim programlarında amaçlanan mesleki yeterlikleri kazandırmaya yönelik geliştirilmiş öğretim materyalleridir (Ders Notlarıdır).
- Modüller, bireylere mesleki yeterlik kazandırmak ve bireysel öğrenmeye rehberlik etmek amacıyla öğrenme materyali olarak hazırlanmış, denenmek ve geliştirilmek üzere Mesleki ve Teknik Eğitim Okul ve Kurumlarında uygulanmaya başlanmıştır.
- Modüller teknolojik gelişmelere paralel olarak, amaçlanan yeterliği kazandırmak koşulu ile eğitim öğretim sırasında geliştirilebilir ve yapılması önerilen değişiklikler Bakanlıkta ilgili birime bildirilir.
- Örgün ve yaygın eğitim kurumları, işletmeler ve kendi kendine mesleki yeterlik kazanmak isteyen bireyler modüllere internet üzerinden ulaşılabilirler.
- Basılmış modüller, eğitim kurumlarında öğrencilere ücretsiz olarak dağıtılır.
- Modüller hiçbir şekilde ticari amaçla kullanılamaz ve ücret karşılığında satılamaz.

İÇİNDEKİLER

AÇIKLAMALAR

KOD	**481BB0063**
ALAN	**Bilişim Teknolojileri**
DAL/MESLEK	**Ağ İşletmenliği**
MODÜLÜN ADI	**Ağ Güvenliği (Donanım)**
MODÜLÜN TANIMI	Ağın donanımsal elemanlarını kullanarak bir ağ sistemi güvenliğini oluşturmak ve güvenlik tedbirlerini almak için gerekli temel bilgi ve becerilerin kazandırıldığı öğrenme materyalidir.
SÜRE	40/32
ÖN KOŞUL	Ağ Sistemleri ve Yönlendirme modülünü almış olmak
YETERLİK	Donanımsal olarak ağ güvenlik sistemini kurmak
MODÜLÜN AMACI	**Genel Amaç** Bu modül ile gerekli ortam sağlandığında donanımsal olarak ağ güvenliğini sağlayabileceksiniz **Amaçlar** ➢ Güvenlik duvarını kavrayarak güvenlik duvarı cihazları kurabileceksiniz ➢ Veri yedeklemenin önemini kavrayabilecek, yedekleme cihazlarını kullanarak yedek alabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	**Ortam:** Ağla birbirine bağlı bilgisayar laboratuarı. **Donanım:** Belirlenen tehlikelere uygun ağ güvenlik cihazı, firewall cihazı, ağ kabloları, harici hard disk, iş güvenliği ile ilgili ekipmanlar
ÖLÇME VE DEĞERLENDİRME	➢ Her faaliyet sonrasında o faaliyetle ilgili değerlendirme soruları ile kendi kendinizi değerlendireceksiniz. ➢ Modül sonunda uygulanacak ölçme araçları ile modül uygulamalarında kazandığınız bilgi ve beceriler ölçülerek değerlendirilecektir.

GİRİŞ

Sevgili Öğrenci,

Bilgisayar ağları, bilgi alışverişinin çok hızlı bir şekilde gerçekleştiği ve bilgiye kolay ulaşım sağlayan bir bilgi havuzudur. Bu ortamı oluşturan ve önemli verileri içerisinde barındıran ağ güvenliğinin önemi de gün geçtikçe artmaktadır.

Dev bir bilgisayar ağı ve bunun sonucu oluşan internet herkes için vazgeçilmez bir bilgi kaynağıdır. Bütün mesleklerde bilgisayar kullanılması, kişisel bilgisayarların her eve girmesi, internete ulaşmanın çok kolay ve ucuz bir hâle gelmesi istisnasız her bilgisayarın bir bilgisayar ağına bağlı olması anlamına gelmektedir.

Bilişim sistemlerine olan bireysel ve toplumsal bağımlılığımız arttıkça bu sistemlerde meydana gelebilecek arızalara ve saldırılara karşı duyarlılığımız da artmaktadır.

Bilgisayar sistemlerine ve ağlarına yönelik saldırılar ciddi miktarda para, zaman, prestij ve değerli bilgi kaybına neden olabilir. Bu saldırıların hastane bilişim sistemleri gibi doğrudan yaşamı etkileyen sistemlere yönelmesi durumunda kaybedilen insan hayatı da olabilir.

Bilgisayar ağlarının bu denli önemli hâle gelmesi ile birlikte ağ güvenliğini sağlama konusunda bilgi sahibi olma ve işine hâkim olan teknik elemanlara ihtiyaç da artmıştır.

Bu modül sonunda edineceğiniz bilgi ve becerilerle ağ güvenliğini tanıma güvenlik tehditlerini önceden tespit edebilme ve önleme, ağ kullanıcılarına düşen görevleri bilme ve sorunlara çözüm üretebilme yeteneklerini eksiksiz biçimde kazanacaksınız.

Mevcut bilgisayar ağlarını daha verimli hâle getirmek için saldırılara karşı çözüm üretebilecek, karşılaşılan sorunlara önce veya sonra hızlı bir şekilde müdahale edebileceksiniz.

ÖĞRENME FAALİYETİ-1

AMAÇ

Ağ güvenliğini tanıyarak, güvenliği tehdit eden unsurları tanıyacak ve gerekli güvenlik önlemleri seçimini yapabileceksiniz.

ARAŞTIRMA

- Piyasada en çok karşılaşılan dış ve iç güvenlik tehditlerinin hangisi olduğunu öğreniniz.
- Ağ güvenliği için potansiyel riskleri belirleyerek bunların önlemlerinin nasıl alındığını öğreniniz.
- Ağ güvenliğini sağlamak için kullanılan donanım cihazlarını tanıyarak nasıl çalıştıklarını öğreniniz.

1. AĞ GÜVENLİĞİ

Son yıllarda internetin, elektronik işletmelerin oluşması ve internet üzerinden ticaretin gelişmesiyle birlikte ağlar, oluşabilecek saldırılara karşı zayıflık göstermeye başlamıştır. Ve ağların bu zayıflıkları, kritik iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmuştur. Bilgisayar virüsleri, DoS saldırıları, şirket çalışanlarının hataları, bilgisayar ağları üzerinde hâlâ büyük bir tehlike oluşturmaktadır. Fakat bu ağ güvenlik açıklarını önlemek elbette ki mümkündür.

Günümüzde internet, gerek kişisel gerekse iş ilişkileri arasındaki bilgi akışını sağlayan, dünyanın en büyük iletişim aracı hâline gelmiştir. İnternetin tüm dünyada böylesine yaygın kullanımı, güvenlik tehlikelerini de artırmaktadır. Önemli bir bilgi kaybı olabilir, gizlilik ihlal edilebilir (kredi kartı numarasının bulunması gibi) veya saatler hatta günler süren yükleme zamanları ortaya çıkabilir. İnternetteki bu tür güvenlik açıkları, insanları internete karşı güvensizleştirebilir ve web tabanlı şirketlerin sonunu hazırlayabilir. Bu yüzden şirketler, güvenliklerini her geçen gün artırmakta ve yeni tehditlere karşı önlem almak amacıyla yatırımlarını sürdürmektedir.

1.1. Ağ Güvenliği İçin Potansiyel Riskler

Risk, bir olay olduğunda hasarın derecesi ya da olayın olma ihtimali olarak tanımlanabilir.

Ağ açısından riskler; hata, kötü amaç ve virüsler gibi sisteme zarar verme potansiyeli olan olaylardır. Risk analizinin bir parçası olarak tehditlerin ihtimallerini ve firma mülklerine zarar verme potansiyellerini belirlemek gerekmektedir.

Ağ açısından potansiyel riskleri, kısaca verinin çalınması, verinin yok edilmesi ve DoS atakları olarak ele alabiliriz.

1.1.1. Veri Çalma (Data Theft)

Veri çalmanın ne olduğunu anlamak için öncelikle veri güvenliğini bilmek, verinin nasıl çalınabileceği bilgisine sahip olmak, tescilli bilginin çalınma yöntem ve tekniklerini kavrayarak bunlara ne gibi önlemler alacağımızı bilmemiz gerekmektedir.

1.1.1.1. Veri Güvenliği

Kurumların internet veya özel iletişim hatları üzerinden akan verilerinin güvenliğinin sağlanması amacıyla kullanılabilecek teknolojiler şunlardır.

- **Fiziksel güvenlik:** Bilgisayarların fiziksel güvenliğinin gerek şifre gibi unsurlarla gerekse akıllı kart, güvenlik kartı türü araçlarla sağlanması.

- **Kullanıcı doğrulaması (authentication) yöntemleri:** Akıllı kart, tek kullanımlı parola, token ve Public Key Certificate gibi araçlar ve RADIUS gibi merkezi kullanıcı doğrulama sunucularının kullanılması.

- **Şifreleme:** Güvensiz ağlar üzerinden geçen verilerin güvenliği için Virtual Private Network veya şifreleme yapan donanımların kullanılması. Ayrıca web tabanlı güvenli veri transferi için SSL ve Public Key şifrelemenin kullanılması. Donanım tabanlı şifreleme çözümleri de mümkündür.

- **İnkâr edilmezlik ve mesaj bütünlüğü:** Sayısal imza teknolojisi kullanarak bunlar sağlanabilir.

1.1.1.2. Bilginin Ele Geçirilmesi

Herhangi bir bilgisayar ağına gönderilen bilgi, o bilgiyi almaya yetkisi olmayan kişilerce ele geçirilebilir. Bu kişiler iletişimi gizlice gözetleyebilir ya da gönderilen bilgi paketini değiştirebilirler. Bunu birçok metot kullanarak yapabilirler. Örneğin IP spoofing yöntemi. Bilgi iletişiminde, bir alıcının IP numarasını kullanarak sanki o alıcıymış gibi gönderilen bilgileri istediği gibi kullanabilir.

1.1.1.3. Tescilli Bilginin Çalınması

Kimlik onayıyla birleştirilmiş güçlü şifreleme bu tür saldırılarla mücadelede etkilidir. Öncelikle bir ağ ortamında hacker'ların nasıl olup da kullanıcı bilgilerini kullanarak sistemlerden bilgi sızdırabildiğini inceleyelim. Bu iş aslında çok basit bir mantığa

dayanmakta, nasıl mı? Hacker kendisini, kullanıcı bilgisayarından çıkan veriler ile bu verileri bekleyen sunucu bilgisayar arasında (Bu genellikle ana segment'tir.) bulunacak şekilde yerleştirir. Bu işlemi yaparken tabii ki çeşitli yazılımlar hatta yazılımcıklar (Script de denilebilir.) kullanırlar.

Kişiye göre değişse de bu işle uğraşan tüm profesyonel hacker'lar ciddi bir ağ protokolleri bilgisine sahiptir. Kullanıcı ana sisteme giriş yaptığında giriş parolası ve iletilen veri hacker tarafından ele geçirilir. Daha sonra veri değiştirilip asıl yönünde yeniden gönderilebilir. Ancak burada hacker için ele geçirilen en önemli bilgi hiç şüphesiz iletilen verinin içeriğinden önce sisteme giriş parolası olacaktır.

Bu sayede hacker her ne kadar parola sahibinin haklarıyla sınırlı kalsa da sunucu üzerindeki işletim sisteminin açıklarından yararlanarak bir şekilde amacına ulaşabilir. Sistem yöneticileri genellikle bu tür saldırılarla mücadele için bir kara liste özelliği kullanırlar. Belirli bir sayıdaki başarısız giriş denemelerinden (genellikle üç ile beş arasında) sonra, sistem yöneticisi giriş sayacını sıfırlamadan daha ileri gidilmesi engellenir. Fakat görüldüğü gibi burada deneme-yanılma yöntemi uygulanmamaktadır. Sisteme direkt gerçek şifre ile giriş yapılır. (Çünkü ağda açık olarak dolaşan şifre hacker tarafından deşifre edilmişti!) Peki amaç nedir? Amaç, tescilli bilginin ve tüm veri tabanının bir kopyasını çıkararak daha sonra belki de sistemi kullanılamaz hâle getirmektir. Diğer bir deyişle çökertmektir. Kimlik onayıyla birleştirilmiş güçlü şifreleme bu tür saldırılarla mücadelede tam olarak etkili olmasa bile büyük ölçüde caydırıcıdır. Ayrıca başında kimsenin bulunmadığı bir bilgisayar da her zaman hacker için zevk kaynağı olmuştur. Bu özellikle kullanıcıların parolalarını açık bir bilgisayardaki dosyada sakladığında böyledir. Ağda geçirilen kısa bir süre bile hacker'a çalıntı kullanıcı isimleri ve parolaları kullanarak ağa erişmeyi sürdürmesi için yeterli bilgiyi sağlayabilir. Sistem sorumlularına bu aşamada düşen görev, kullanıcı PC'lerine erişimi sınırlamak için her zaman bir tür parola kullanılmasını sağlamak ve asla etkin hâle getirmeden bilgisayarlarını boşta bırakmamalarını bir yazılı bildirge ile tüm şirkete duyurmaktır.

Şekil 1.1: Veri alma ve gönderme

1.1.1.4. Sonuç

Aktif veri depolama ünitelerinizin ve sunucularınızın, internal veya external ağ üzerindeki diğer sistemlerle arasında bir firewall (kaliteli bir anti-virüs programı ile entegre edilmiş) kurulu olması gerektiği ve artık bunun bir zorunluluğa dönüştüğü çok açık bir gerçektir. Bu durumda size şöyle bir soru yöneltebiliriz: Çok gizli dokümanlarınızın yanlış

ellere geçtiğini düşünmek içinizde nasıl bir duygu uyandırır? Sorunun cevabı açık, en kısa sürede tedbirinizi alın ya da bir planlama süreci başlatın, geçen her dakika sizin aleyhinize işliyor olabilir! Bu iş için ayıracağınız bütçenin boşa gitmeyeceğinden emin olabilirsiniz

1.1.2. Veri Yoketme (Destruction of Data)

Veri yok etmeyi anlayabilmek için öncelikle verinin nasıl kaybolduğunu anlamak gerekir.

Bireysel açıdan bakıldığında, sistemdeki en kıymetli şey veridir. Çünkü enerji, donanım ve yazılım, yalnızca maddi imkânlarla yerine konabilir. Kullanıcı ayarları da daha kabul edilebilir bir çabayla yerine konabilir. Hâlbuki kişisel çabayla ortaya çıkartılmış ürünler, daha da ötesinde başkalarının çabaları sayesinde toplanmış veriler (mesela edinilen e-posta mesajları, derlenmiş kaynaklar vb.) maddi imkânlarla yerine konamayacaktır. Alınacak önlem veri yedeklemedir ve ilerleyen bölümlerde ayrıntılı olarak ele alınacaktır.

Günümüzde gerek kişiler gerekse kurum ve işletmeler verilerini büyük oranda bilgisayar sistemlerinde işlemekte ve saklamaktadır. Bu veriler bilgisayar sistemlerinde genel hatlarıyla,

- **Manyetik:**Hard diskler, disketler, teyp yedekleme kartuşları,
- **Optik:** CD ve DVD,
- **Elektronik:** Flash bellekler, bellek kartları,

tabanlı ortamlarda depolanmaktadır.

Depolanan bu verilerin normal yollarla erişilemez hâle gelmesi veri kaybı olarak değerlendirilmektedir. Veri kaybı nedenleri ve türleri ise genel hatlarıyla,

- Veri depolama ortamında verilerin dosyalar şeklinde düzenli bir şekilde yerleştirilmesine ve ihtiyaç duyulduğunda erişilmesine yarayan mantıksal düzenlemelerin (dosya sistemi) silinmesi veya hasar görmesi,

- Veri depolama ortamındaki yapının yeniden oluşturulması (formatlama) veya dosyaların silinmesi,

- Ham veya belirli formatlara sahip dosyalarda (veri tabanı dosyaları, belgeler) dâhili bozulmalar olması,

- Veri depolama ortamının fiziksel olarak bozulması ya da hasar görmesi

şeklinde özetlenebilir.

1.1.3. Servis Reddetme (Denial of Service, DoS Attack)

1.1.3.1. DoS Attack Nedir?

Bir tür bilgisayar ağı saldırısı olarak bilinen DoS saldırılarında bilgisayar korsanları, istedikleri Web sitesini çalışmaz hâle getirebilmektedir.

Korsanlar bu saldırıları, kişisel bilgisayarları kullanarak yapmakta ve özellikle büyük web siteleri bu tür saldırılar nedeniyle büyük zararlar görebilmektedir.

Bilgisayar korsanlarının eski taktiklerinden biri olan DoS saldırıları tekrar gündeme taşınmış durumdadır. Bir Web sitesinin hizmet verememesine neden olan DoS saldırısında korsanlar, bireysel ve kurumsal kullanıcılarının bilgisayarlarından yararlanmaktadır.

1.1.3.2. Sistem Nasıl İşliyor?

Bilgisayar korsanı, hiçbir şeyden habersiz olan bilgisayar kullanıcılarına bir program yüklemekte, bu şekilde binlerce kullanıcıyı izleyerek sistemlerine zarar verebilmektedir.

Bilgisayar korsanının belirlediği bir güne kadar bu programlar sessiz sedasız bir kenarda beklemektedir. Bu programların yüklendiği makinelere zombi makineler denmiştir. O gün geldiğinde, bütün bilgisayarlar aynı anda, önceden belirlenmiş bir Web sitesine, giriş talebi göndermeye başlamaktadır.

Bu tür talep gönderen bilgisayar sayısı on binleri bulduğunda, doğal olarak karşı tarafın sunucusu yanıt veremez duruma gelir. Sonuçta da Web sitesi çöker, işlem yapamaz ve site sahipleri maddi zarara uğrar.

Saldırıda kullanılan programcıkların yüklendiği bilgisayarlar ve kurumsal ağlar, ciddi bir bant genişliği darboğazı yaşamaktadır, çünkü bu saldırılar, büyük miktarda veri gönderimi yapılmasını gerektirmektedir.

Saldırılara karşı korunma yolu, bilgisayar ve ağ güvenliği sağlayan çözümlerin kurulmasından ve doğru şekilde konfigüre edilmesinden geçmektedir.

1.2. Ağlar İçin Güvenlik Tehditleri

Günümüzde kurumsal ağlarda güvenlik kavramı, büyük bir değişim geçirmektedir. İnternetin yaygınlaşmaya başladığı günlerde, sadece dış dünyadan (ağ dışından) gelebileceği varsayılan belirgin tehditlere karşı önlem almakla eş değer kabul edilen ağ güvenliği, günümüzde hem iç hem de dış tehditlere karşı önlemler almaya, hatta önlem almaktan öte, ağ davranışını aktif biçimde gözleyerek beklenmeyen aktiviteleri engelleme ve böylelikle henüz belirgin biçimde bilinmeyen tehditleri dahi etkisiz kılmaya varan bir gelişme göstermiştir.

İnternetin genişlemesi ile beraber ağ uygulaması da beklenmedik şekilde genişlemiştir. Bu gelişmeyle birlikte ağ kurulup işletmeye alındıktan sonra ağ yönetimi ve ağ güvenliği büyük önem kazanmıştır. Çünkü internete bağlı ağ sistemleri arasında dolaşan hiçbir veri gerekli önlemler alınmadığı takdirde güvenli değildir. Ağın güvenilir biçimde çalıştırılması anahtar sözcük konumuna gelmiştir. Çünkü ağın günümüz teknolojisi ile kurulup çalıştırılmasıyla iş bitmemekte esas iş ağ performansının ve güvenilirliğinin sağlanmasında bitmektedir.

1.2.1. Dış Tehditler

Bilgisayarları ağlarla birbirine bağlamak, teknolojinin de bununla doğru orantılı olarak gelişmesine yol açmıştır. Bu kültürel değişikliklerle daha yüksek güvenliğe olan ihtiyaç da artmıştır. Eskiden bir bilgisayar suçlusu sistemlere tek bir noktadan saldırı yapabilmekte ve bu da sistem yöneticilerine bir siteyi koruma avantajını sunmaktaydı.

Günümüzün istemci - sunucu ortamında ağ yöneticileri çok farklı bir savaşın içindedirler. Ağlarındaki her erişim noktasından saldırılara açıklar. İnternet çok sayıda sistemin birbirine bağlanmasını sağlayarak kendine özgü problemleri de beraberinde getirmiştir.

1.2.1.1. Servis Reddetme (DoS)

DoS yani açılımı Denial of Sevice olan bu saldırı çeşidi bir hizmet aksatma yöntemidir. Bir kişinin bir sisteme düzenli veya arka arkaya yaptığı saldırılar sonucunda hedef sistemin kimseye hizmet veremez hâle gelmesi veya o sisteme ait tüm kaynakların tüketimini amaçlayan bir saldırı çeşididir. Birçok yöntemle hizmet aksatma saldırıları gerçekleştirilebilir.

Genellikle kullanılan yöntemler üç sınıf altında toplanabilir:

- Bant Genişliğine Yönelik Ataklar
- Protokol Atakları
- Mantıksal Ataklar

1.2.1.1.1. DoS Ataklarının Türleri

- **Service overloading:** Bu atak tipi belirli host ve servisleri düşürmek için kullanılır. Atak yapan kişi özel port ve host'a bir çok ICMP paketi gönderir. Bu olay network monitör ile kolayca anlaşılır

- **Message flooding:** Service overloading'den farkı sistemin normal çalışmasını engellemez. Yine aynı şekilde gönderilen paketler bu sefer normal olarak algılanır. Örnek Nis server'ında flood yapılırsa (Unix network) Nis bunu şifre isteği gibi görür ve saldırganın host'a hükmetmesi sağlanır.

- **Clogging:** Saldırganın SYN gönderip ACK alıp ondan sonra da gelen ACK'ya cevap vermeyip sürekli SYN göndermesinden oluşur. Bu durum defalarca kez tekrarlanırsa server artık cevap veremez hâle gelir. Bu paketler sahte IP ile gönderildiğinden sistem bunu anlayamaz ve hizmeti keser. Anlasa ne olur? Anlasa aynı IP' den gelen o kadar isteğe cevap vermez. Kurtuluş yolu bunları tarayan firewall'lardır.

1.2.1.1.2. DoS Atakları İçin Kullanılan Programlar

- **Ping of death:** Bir saldırgan hedef aldığı bir makineye büyük ping paketleri gönderir. Birçok işletim sistemi, gelen bu maksimum derecede paketleri anlayamaz, cevap veremez duruma gelir ve işletim sistemi ya ağdan düşer ya da çöker.

- **SSPing:** SSPing bir DoS aracıdır. SSPing programı hedef sisteme yüksek miktarda ICMP veri paketleri gönderir. İşletim sistemi bu aldığı data paketlerini birbirinden ayırmaya çalışır. Sonuç olarak bir hafıza taşması yaşar ve hizmet vermeyi durdurur.

- **Land exploit:** Land Exploit bir DoS atak programıdır. TCP SYN paketiyle hedef sisteme saldırıdır. Saldırı aynı port numarasına sürekli olarak yapılır. Land Expoit aynı kaynak ve hedef portları kullanarak SYN paketleri gönderir.

Bir çok makine bu kadar yüklenmeyi kaldıramayacağı için Buffer overflow yaşar ve hiçbir bağlantıyı kabul edemeyecek duruma gelir.

- **Smurf:** Smurf broadcast adreslere ICMP paketleri gönderen bir DoS Saldırı programıdır. Saldırgan ICMP echo istekleri yapan kaynak adresi değiştirerek ip broadcast'a gönderir. Bu broadcast network üzerindeki her makinenin bu istekleri almasını ve her makinenin bu sahte ipli adrese cevap vermesini sağlar. Bu sayede yüksek seviyede network trafiği yaşanır. Sonuç olarak bir DoS saldırısı gerçekleşmiş olur.

Bir TCP bağlantısının başında istekte bulunan uygulama SYN paketi gönderir. Buna cevaben alıcı site SYN-ACK paketi göndererek isteği aldığını teyit eder. Herhangi bir sebeple SYN-ACK paketi gidemezse alıcı site bunları biriktirir ve periyodik olarak göndermeye çalışır.

Zombiler de kullanılarak, kurban siteye dönüş adresi kullanımda olmayan bir IP numarası olan çok fazla sayıda SYN paketi gönderilirse hedef sistem SYN-ACK paketlerini geri gönderemez ve biriktirir. Sonuçta bu birikim kuyrukların dolup taşmasına sebep olur ve hedef sistem normal kullanıcılarına hizmet verememeye başlar.

- **WinNuke:** WinNuke programı hedef sistemin 139 nu.lı portuna "out of band" adı verilen verileri gönderir. Hedef bunları tanımlayamaz ve sistem kilitlenir.

Kullanımı: WNUKE4 -c XXX.com 10000 0 450
(hedefe 10,000 adet 450 byte lık icmp paketleri gönderir.)
WNUKE4 -n XXX.com 0 1024-2024 6667-6668 UNPORT

- **Jolt2:** Jolt2 kendisini farklı segmentte bulunuyormuş izlenimi vererek NT/2000 makinelere DoS atak yapabilen bir programdır. İllegal paketler göndererek hedefin işlemcisini %100 çalıştırıp kilitlenmesine yol açar.

  c: \> jolt2 1.2.3.4 -p 80 4.5.6.7

Komut satırında görülen, 1.2.3.4 ip numarası saldırganın spoof edilmiş adresidir. Hedef adresin 4.5.6.7 80 numaralı portuna saldırı yapar. CPU kaynaklarının tamamını harcar ve sistemi aksatır.

- **Bubonic.c:** Bubonic.c Windows 2000 makineleri üzerinde DoS exploitlerinden faydalanarak çalışan bir programdır. Hedefe düzenli olarak TCP paketlerini gönderir.

  c: \> bubonic 12.23.23.2 10.0.0.1 100

- **Targa:** Targa 8 farklı modül içinde saldırı yapabilen bir Denial of Service programıdır.

DoS (nuke) saldırı türleri aşağıdaki gibidir.

- **NUKE:** Nuke, sisteminizi kilitleyen, göçerten, internet erişimini kesen ve bu gibi zararlar veren saldırılara Nuke (nükleer bombanın kısaltması gibi) adı verilir. Nuke, siz internete bağlıyken ISS nizce size verilen bir ip numarası yardımı ile bir başka kişinin özel programlar yardımı ile bilgisayarınıza paketler göndermesi ve bu paketlerin bilgisayarınıza zarar vermesidir.

- **OOB Nuke:** (Out of band Nuke) Sadece Windows NT ve 95'te bir bug olan OOB nuke, işletim sistemi Windows olan bir makinenin 139. portuna (Netbios session port) MSG_OOB tipi bir bağlantı (connection) yapılmasıyla gerçekleşir. Eğer 95 kullanıyorsanız sisteminizin mavi ekran vererek internet bağlantısının kopmasına, NT kullanıyorsanız sistemin durmasına yol açar.

- **Land:** Bilgisayarı kendi kendine senkronize ettirerek, arka planda internet meselelerini yürüten Winsock adlı programın sonsuz döngüye girmesini sağlar. Böylece farenizi bile hareket ettiremezsiniz. Kaynak IP (Source), Kaynak Port ve Hedef IP (Destination IP) IP, Hedef Port'un aynı olduğu bir IP paketi, Land saldırısının gerçekleşmesini sağlar.

- **Teardrop, Boink, Nestea:** İnternet üzerinde gelen giden veri, parçalar hâlinde taşınır, daha sonra işletim sistemi tarafından birleştirilen paket parçacıkları veriyi oluşturur (fragmentation). Çoğu sistemin duyarlı olduğu bu saldırı tipleri,

bilgisayarınızın bozuk olarak bölünmüş 2 paketi birleştirmeye çalışması ile gerçekleşir. Boink, teardrop saldırısının ters olarak çalışan hâlidir. Nestea, teardrop saldırısının küçük değişimlere uğramış hâlidir ve teardrop ve boink saldırılarına karşı patch edilmiş Linux sistemlerinde etkilidir.

- **Brkill:** Eğer Windows yüklü bir bilgisayara, bağlantının sonlanması ile oluşan PSH ACK tipi bir TCP paketi gönderirseniz Windows size o anki son bağlantı seri numarasını gönderir. Buradan yola çıkarak hedef makinedeki herhangi bir bağlantıyı zorla kesmeniz mümkün olur.

- **ICMP Nuke:** Bilgisayarlar çoğu zaman aralarındaki bağlantının sağlamlığını birbirlerine ICMP paketleri göndererek anlarlar. Bu saldırı var olan bir bağlantının arasına sanki hata varmış gibi ICMP_UNREACH paketi göndererek oluşur.

- **Jolt/SSPing:** Windows 95 ve NT'nin yüksek boyuttaki bölünmüş ICMP paketlerini tekrar birleştirememesinden kaynaklanan bir saldırı tipidir. 65535+5 byte'lık bir ICMP paketi göndermek bu saldırıyı gerçekleştirir.

- **SMURF:** Networkler'de "broadcast address" olarak tanımlanan ve kendine gelen mesajları bütün network'e yönlendiren makineler vardır. Eğer birisi başka biri adına o makineye ping çekerse, ağ üzerindeki bütün çalışan makineler hedef olarak belirlenen makineye ping çeker. Smurf, bu işlemi yüzlerce broadcast makineye tek bir kaynak IP adresinden ping çekerek saldırı hâline çevirir. Bir anda bilgisayarlarınıza on binlerce bilgisayarın ping çektiğini düşünürsek değil sizin şirketinizin bağlantısı, maalesef Turnet (Türkiye internet omurgası) çıkış gücü bile buna cevap vermeye yetmez ve bağlantılarınız kopar.

- **Suffer:** Suffer saldırısı bilgisayarınıza sanki binlerce farklı bilgisayardan bağlantı isteği geliyormuş gibi SYN paketleri gönderir. Bu saldırının sonunda Windows yeni bağlantılar için yeterli hafıza ayıramaz ve kalan hafızayı da bitirir. Bazı firewall türleri de böyle bir durum karşısında binlerce soru kutucuğu açarak makinenin kilitlenmesine sebep olur.

1.2.1.2. Dağıtık Servis Reddetme (DDoS)

Bir saldırgan daha önceden tasarladığı birçok makine üzerinden hedef bilgisayara saldırı yaparak hedef sistemin kimseye hizmet veremez hâle gelmesini amaçlayan bir saldırı çeşididir. Koordineli olarak yapılan bu işlem hem saldırının boyutunu artırır hem de saldırıyı yapan kişinin gizlenmesini sağlar. Bu işlemleri yapan araçlara Zombi denir.

Bu saldırı çeşidinde saldırganı bulmak zorlaşır. Çünkü saldırının merkezinde bulunan saldırgan aslında saldırıya katılmaz. Sadece diğer ip numaralarını yönlendirir. Eğer saldırı bir tek ip adresinden yapılırsa bir Firewall bunu rahatlıkla engelleyebilir. Fakat saldırının daha yüksek sayıdaki IP adresinden gelmesi Firewall'un devre dışı kalmasını sağlar(Log taşması firewall servislerini durdurur.).İşte bu özelliği onu DoS saldırısından ayıran en önemli özelliğidir.

1.2.1.2.1. DDoS Atakları İçin Kullanılan Programlar

- Trinoo
- TFN
- Stacheldraht
- Shaft
- TFN2K
- Mstream

1.2.1.2.2. DDoS Saldırı Yöntemi

Tüm DDoS programları iki safhada çalışır.

- **Mass-intrusion Phase:** Bu safhada DoS saldırısı yapacak olan sistemlere ulaşılır ve saldırıyı gerçekleştirecek olan programlar yüklenir. Bunlar birincil kurbanlardır.

- **DDoS Attack Phase:** Bu safhada hedef sitelere saldırı yapılır bunun için de birincil kurbanlar kullanılarak hedefe yüklenilir.

Bu safhalarda kullanılan programlar şunlardır:

- **Trinoo:** Trinoo DDoS yöntemini kullanan ilk programdır.
  Kullandığı TCP Portları:
  Attacker to master: 27665/tcp
  Master to daemon: 27444/udp
  Daemon to master: 31335/udp

- **TFN2K:** Zombilerin yüklendiği makineler listening modda çalışır. Her an karşıdan gelecek komutlara hazırdır.
  Running the server
  #td
  Running the client
  #tn -h 23.4.56.4 -c8 -i 56.3.4.5
  (bu komut 23.4.56.4 numaralı IP'den 56.3.4.5 numaralı IP'ye saldırı başlatır.)

- **Stacheldraht:** TFN ve Trinoo gibi çalışır fakat modüllerine paketleri kriptolu gönderebilir.
  Kullandığı portlar TCP ve ICMP
  Client to Handler: 16660 TCP
  Handler to and from agents: 65000 ICMP

1.2.1.3. Sömürücüler (Exploits)

Exploit'in kelime anlamı "kötüye kullanma, sömürme" demektir. Yani sisteminizin normal bir özelliğinin bir açığını yakalayarak, bunu kötüye kullanabilir, sisteminizdeki, bilgilere ulaşabilirler. Exploit'ler genelde sistem tabanlı olarak çalışırlar yani Unix'e ait bir exploit Windows için çalışmaz. Bugüne kadar bulunan yaklaşık olarak 1000'in üzerinde exploit var. Ve bunların hepsinin nasıl çalıştığını anlatmamız güvenlik sebeplerinden dolayı mümkün değildir. Aşağıda çok popüler olan bir kaç tanesinden bahsedilecektir.

Windows Null Session Exploit: Windows işletim sistemi, dışarıdaki kullanıcılara network üzerinde hiç bir hakka sahip olmadan oturum, kullanıcı ve paylaşım bilgilerini (session, user ve share) verir. Ve ne kadar ilginçtir ki, bu exploit, Windows Network API'sinde belgelenmiş ve feature (özellik) olarak gösterilmiştir. Kötü niyetli birisi bu exploit'i kullanarak sistem hakkında çok kritik bilgilere sahip olabilir.

PHF Exploit: Bu exploit oldukça eski olmasına rağmen hâlen karşılaşabileceğiniz bir güvenlik açığıdır. Phf cgi yardımı ile sistemdeki dosyalara admin olarak erişebilirsiniz.

Yukarıdaki örnek Unix işletim sistemi ya da türevini kullanan bir makineden kullanıcı bilgilerinin ve şifrelerinin bulunduğu passwd dosyasını görmenizi sağlar.

ASP Exploit: Active server page (ASP) özelliği kullanan Web sunuculardа URL'nin sonuna bir nokta (.) ya da ::şDATA yazarak ASP'nin içeriğini (source code) görebilirsiniz. Eğer ASP'nin içerisinde herhangi bir şifre varsa bu exploit çok tehlikeli olabilir.

http://www.aspkullananserver.com/
default.asp. ya da
http://www.aspkullananserver.com/
default.asp::şDATA

Sendmail Exploit: Eski "send mail" sürümlerinde bir kaç basit hile ile sistemin şifrelerinin tutulduğu dosyayı çekmeniz mümkündür. Ayrıca sistem kullanıcıları hakkında bilgi almak (EXPN) ya da bir kullanıcı isminin o sunucuda olup olmadığını da öğrenmek mümkündür (VRFY).

telnet mail.server.com:25

ICQ Tabanlı Exploitler: Son derece zayıf bir mimariye sahip olan ICQ sistemi, kolayca taklit edilebilen hatta gerçek "spoofing" bile yapmanıza gerek kalmayan bir sistemdir. ICQ kullanıcıları kolayca mesaj bombasına tutulabilir, şifreleri değiştirilebilir, onaya gerek kalmadan listenize alabilir, IP'si kullanıcı istemese bile görülebilir ya da ICQ chat yaparken mesaj taşması (flooding) yapılabilir.

1.2.2. İç Tehditler

Olası saldırıların nereden geleceği sorusuna kesin bir yanıt vermek zorlaşırken, ağların temel hizmet alıcısı durumundaki kullanıcılar, saldırıların hedefi konumundan hem hedef hem de kaynak olma konumuna doğru kayıyor. Ağ güvenliğine yönelik saldırıların kaynakları konusunda yapılan araştırmalar, iç tehditlerin giderek dış tehditler boyutuna geldiğini gösteriyor. Ağın içi, artık sadece korunan bir yer değil, aynı zamanda kendisine karşı tedbir alınan bir yer olarak algılanmalıdır.

Kurum içerisinde kullanılan tüm bilgisayarların istenen güvenlik seviyesinde olmasının sağlanması başlı başına bir yönetim yükü getiren, ciddiyetle planlanması gereken bir faaliyettir. Gerekli güvenlik seviyesinde bulunmayan bir bilgisayarın ağa serbestçe bağlanması, tüm ağ üzerinde zararlı sonuçlar doğurabilecek bir saldırı için mükemmel bir fırsattır. Bu tür bir saldırı, söz konusu bilgisayarı kullanan kişi farkına bile varmadan hızla yayılabilir ve basit önlemlerle engellenebilecek iş kayıplarına sebep olabilir.

İç tehditlerin firma çalışanlarından ve kötü amaçlı kullanıcılardan kaynaklanan yönlerini kısaca açıklayalım:

1.2.2.1. Firma Casusluğu (Corporate Espionage)

Firmanız hangi ağ çözümünü uygularsa uygulasın güvenlik son derece önemlidir. Bilgisayar güvenliği bilgi, donanım ve yazılım gibi firmanın kaynaklarını koruyacak şekilde dizayn edilir. Firma casusluğunu, çalışanlardan kaynaklı servis kullanımının engellenmesi ve sistemin zarara uğratılması olarak adlandırabiliriz.

1.2.2.1.1. Servis Kullanımını Engelleme

Bir kullanıcı veya firma, internet güvenliğinin aşıldığı bir durumda çeşitli tehditlerle karşılaşabilir. Bu tehditlerin sonuçları kullanıcının iş alanına bağlıdır. Örneğin bazı kullanıcılar servislerin tutarlılığı ve hızı konusunda endişelenirken diğerleri bilgisayarlarındaki gizli bilgilerin gizliliği konusunda endişe duyabilirler.

Güvenlik problemlerinin iki ana sınıfı rahatsızlık verici saldırılar ve kötü amaçlı saldırılardır. Rahatsızlık verici saldırılar işinizi yapmanızı engelleyen saldırılardır. Bu tip bir saldırı bilgisayarınızın yavaşlamasına veya çökmesine yol açabilir. Genelde rahatsızlık verici saldırılarda kalıcı hasar veya kayıp amaçlanmaz. Eğer bir saldırgan ağınıza erişim sağlarsa, dosyaları silebilir, kişisel verilerinizi okuyup değişiklik yapabilir veya makinenize virüs bulaştırabilir.

1.2.2.1.2. Şirket Çalışanları

Çoğu güvenlik uzmanları, güvenlik açıklıklarını, ağı veya bilgisayarı kullanan şirket çalışanlarının başlattıklarını iddia etmektedirler. Şirket çalışanları, çoğunlukla ya şakayla ya kötü niyetle ya da yanlışlıkla kendi şirketlerinin ağına veya önemli bilgilere zarar verirler. Şirketler genelde şubelerine de ağlarına erişim hakkı verirler ve şubede çalışan insanlar da,

aynı şekilde güvenlik açıklarına yol açabilirler. Bu yüzden, şirket güvenliğini sürekli kontrol etmek zorundadır.

Örneğin, bazı çalışanlar, ağa bağlanmak için kullandıkları şifreyi, basit, crackerlar tarafından tahmin edilebilir şekilde seçerlerse, bu bir güvenlik açığı oluşturur. Veya yalnızca merkezde bir güvenlik duvarı ile korunan ve bu merkeze özel kiralık devre ile bağlı bulunan bir şubede, herhangi bir kullanıcının telefon hattı ile internete bağlanması da bir güvenlik açığı oluşturabilir.

Bazı çalışanlar da yanlışlıkla internetten ya da floppy diskten bir belge yüklerken bilgisayara virüs bulaştırabilirler ve kendi bilgisayarına bulaştırdığı virüsün farkına varmadan ağ içindeki diğer bilgisayarlarla bilgi alışverişi ile, bu virüsü tüm ağa yayabilirler. Bu da ağ için bir tehlike oluşturur. Bu soruna karşı alınabilecek önlem, tüm bilgisayarlara virüs koruma programı yüklemek ve bir belge yüklerken ekrana uyarı mesajları gelmesini sağlamaktır.

Ayrıca bazı çalışanlar, ki bu kişiler genellikle kovulmuş ya da şirket içinde aşağılanmış kişilerdir, kendi ağ yetkilerini kullanarak ve bilerek tüm ağa virüs bulaştırabilir ya da önemli bilgileri yok edebilir.

Snoops denilen bazı çalışanlar da vardır ki, bir casus gibilerdir. Diğer çalışanlarla arasındaki rekabet nedeniyle, erişim yetkisine sahip olmadığı birtakım gizli bilgilere ulaşmaya çalışırlar. Mesajlara ya da maaş bilgilerine erişmek masum olabilir ancak önemli ve gizli finansal bilgilere ulaşmak, o şirket için büyük tehlike oluşturabilir.

Güvenlik, dâhili ağlarda da önemli bir konudur. Firma çalışanları bazen veri hırsızlığı yapabilir ya da sisteme virüs bulaştırabilir.

Extranet firma dışındaki kullanıcıların erişimine izin veren bir intranet`tir. Bu erişim dâhili ağla küresel internet arasında güvenli haberleşme için belirli harici kullanıcılara ve belirli bilgilere erişilecek şekilde ayarlanır. Örneğin bir firma iş ortaklarıyla ürün bilgilerini paylaşmak isteyebilir. Veya müşterilerin sipariş verebilmesi için, malların teslimatında ve ödemeleri elektronik olarak işleme tabi tutmak için elektronik doküman değişimi (Electronic Document Interchange - EDI) kullanabilir.

Extranet`ler tipik olarak bir firmanın aşağıdaki kategorilerde bilgi paylaşmasını sağlar:

- Satış ve müşteri hizmetleri
- Ürün geliştirme ve pazarlama
- Eleman alımı

Önemli bilgilerin, mesela kredi kartı detaylarının, geniş bir ağda depolandığını varsayalım. Bu tip veriye yetkisiz personel tarafından erişilmemesi önemlidir. Birisi başkasının kredi kartı bilgileri ile kendisine bir şeyler satın alabilir.

Üst yönetim firma için uygun güvenlik politikalarının geliştirilmesi ve yürütülmesinden sorumludur. Ve bireysel kullanıcılar da bu politikalara uymaktan

sorumludurlar. Ayrıca kullanıcılar kişisel bilgilerinin güvende olduğundan herhangi mevcut bir güvenlik mekanizması kullanarak emin olmalıdır.

Bilgisayar ve ağ servisleri sağlayıcıları yönettikleri sistemlerin ve sağladıkları servislerin güvenliğinden sorumludurlar. Ayrıca bütün kullanıcıların güvenlik politikalarından haberdar olduğundan emin olmalılar. Bu politikaları belirli aralıklarla gözden geçirmeli ve yapılan değişikliklerden kullanıcıları haberdar etmelidirler.

Eğer bir sistemin harici kullanıcıları varsa, doğru bilgilerin paylaşıldığından sistemin sahibi sorumludur. Üretici firmalar ve sistem geliştiriciler sağladıkları sistemlerin güvenli olduğundan emin olmalıdırlar. Ayrıca güvenlik kontrollerinin uygulanmasında kullanıcılar ve servis sağlayıcılar ile haberleşmelidirler.

Kurumsal ağınızın yeterli performansa, güvenilirliğe ve yüksek erişilebilirliğe sahip olması kurumsal ağ bağlantılarında artan internet kullanımının doğal sonuçlarından biri olan ağ tıkanıklıkları sonucu kritik uygulamalarda performans sorunları yaşanabilir.

Ortaya çıkabilecek bağlantı hataları, ağ geçidi çökmeleri, ağ bağlantı gecikmeleri ve diğer performans düşüklükleri neticesinde firmalar büyük ekonomik kayıplar yaşayabilirler.

İnternet ve intranet hatlarının gereğinden fazla istemci ve sunucu tarafından kullanılması sonucu, trafik miktarına göre bağlantı kopuklukları, zayıf ‘response’ zamanları ve yavaş internet kullanımı sorunları ile karşı karşıya gelmek normaldir.

Bu gibi durumlarda, sınırlı bant genişliği üzerinde mevcut hattı aktif olarak paylaştırmaya yönelik bir yönetime gidilmelidir.

Eğer yerel ağınız bünyesinde yoğun trafik yaşanıyorsa, birçok kaynağınız (halka açık popüler bir Web sunucusu gibi) negatif yönde etkilenebilir.

Bir uygulama için bir sunucuya güvenmek, zayıf ‘response’ zamanlarına hatta bağlantı kopukluklarına yol açabilir. Sunucu yük dengelemesi bir uygulama sunucusunun işlevini birçok sunucu üzerine dağıtarak ölçeklenebilir bir çözüm sağlar. Bu yolla ayrıca, sunucular üzerindeki performanslar da artırılmış olur.

Performansın yettiği durumlarda dahi, ağ geçidi seviyesinde meydana gelebilecek bir hatayı tolere edebilecek güvenli bir ağ altyapı sistemi oluşturulmalıdır. Günümüzde artık çoğu kurum, ağ geçidinde yaşayacakları anlık erişim sorunları yüzünden dahi büyük mali kayıplar yaşayacaklarından emin olarak yüksek erişilebilirliği destekleyen ağ güvenlik ürünlerini tercih etmektedir.

Yüksek erişilebilirliği destekleyen ürünler hem yazılım, hem donanım bazında yedeklemeli sistemler ile yüzde yüze yakın seviyelerde erişilebilirliği garanti ederler. Bir sorun meydana geldiği zaman, yüksek erişilebilirliği sağlayan bileşenler ağınızın güvenli olmasını sağlamalı ve son kullanıcıya tamamen transparan şekilde devam ettirilmelidir. Gerçek etkili çözümler sunacak ağ yöneticileri, iç ve dış kullanıcılarına daimi güvenilir servisler sağlamalıdır.

Kullanıcı bazında güvenlik politikalarını ağ seviyesinde uygulamak kurumsal ağ konseptinin genişlemesi, birçok ağ için kullanıcı, uygulamalar ve IP adres kullanımı sayılarında aşırı artışlara yol açmıştır. Bu tür dinamik ağ ortamlarında emniyetli ağ politikalarının uygulanması, kullanıcı bazında güvenlik politikalarının oluşturulmasıyla sağlanır. Bu politikalar çerçevesinde, ağ kullanıcıları için kişisel erişim denetimleri, tanılama prosedürleri ve şifreleme parametreleri belirlenir. Yüksek miktarda kullanıcı bilgisi içeren bu uygulamalarla uğraşmak ağ ve güvenlik yöneticileri için bazen kolay olmayabilir.

Kullanıcı seviyesinde güvenlik bilgilerini ölçeklenebilir şekilde merkezi bir yerde depolamak için LDAP protokolü kullanmak en uygun çözümdür. LDAP sayesinde, bütün kullanıcı bilgileriniz, tek bir veri tabanında tutulup diğer ağ uygulamaları tarafından paylaşılır. Bununla birlikte ağ ve güvenlik yönetimleri paralel çalışarak güvenlik ile ilgili zaman harcatıcı rutin prosedürlerin aşılması sağlanır.

Güvenlik denetimlerini en üst düzeyde tutmak için kullanıcı seviyesinde uygulanan güvenlik politikaları kayıtlarının tutulması ve bunların denetlenmesi gerekir. Kişisel güvenlik politikalarının uygulandığı ortamlarda DHCP protokolünün kullanılması etkili bir yol değildir. Bunun sebebi IP adres atamalarının dinamik olarak yapılmasıdır.

1.2.2.2. Kötü Amaçlı Kullanıcılar (Rebellious Users)

İnsanlığın değişik milletler ve toplumlardan meydana geldiğini hepimiz biliyoruz. Bu insan toplulukları içerisinde yaptıkları çalışmalarla diğer insanlara faydalı olan kişiler bulunduğu gibi, çevresindeki insanları rahatsız eden insanlar da vardır.

Bilgisayar programı yazan firmaların ya da kişilerin çoğunluğu insanların, şirketlerin vb. kuruluşların işlerini kolaylaştırıcı programlar, doğan yeni ihtiyaçlar doğrultusunda bu yazılımlarını da yenileyerek geliştirirler.

Bunların yanında topluma zarar vermeyi alışkanlık hâline getirenler de bozucu programlar yazarak piyasaya gizlice sürmektedir. İşte bu işi yapanlara kötü amaçlı kullanıcılar diyoruz.

Kötü amaçlı kullanıcılar yapmış oldukları bu saldırılarla çok değişik suçlar işleyebilirler. Bu suçları işlerken çok değişik yöntemler de kullanabilirler.

Kötü amaçlı saldırılar genelde bir firma ya da kullanıcıya kayıp ya da hasar vermeye yöneliktir. Eğer internete doğru güvenlik önlemlerini almadan bağlanırsanız bilgi sistemlerinizi risk altına aldığınızı bilmelisiniz. Ağınıza bir web sunucusu kurduğunuzda potansiyel olarak tüm internetin yerel ağınıza erişebileceği bir pencereye açıyorsunuz. Sitenizin çoğu ziyaretçisi web sunucunuzu amaçlandığı şekilde kullanacaktır. Fakat bazıları ağınızdaki özel bilgilere erişmeye çalışacak hatta dâhili ağınıza erişim için sistemde güvenlik açığı arayacaktır. Sistem güvenliğinizi kimlerin aşmaya çalışabileceğinden her zaman haberdar olmalısınız. Hacker`lar üniversite ortamındaki öğrencilerden rakiplere veya profesyonel hacker`lar ve endüstriyel casusluk ajanlarına kadar farklılık gösterebilir.

1.2.2.2.1. Kullanılan Yöntemler ve Suç Sahası

Bilgisayar suçları sabotaj, intikam, vandalizm, hırsızlık, gizlice dinleme, veri sahtekârlığı veya veri bilgisayar sitemine girmeden önce, girerken ya da girdikten sonra değişiklik yapmayı içerir. Bilgisayarlar kredi kartı sahtekârlığı, kalpazanlık, zimmete geçirme ve gizli dokümanların çalınmasında kullanılabilir. 2.8MB`lık bilgi içeren bir diskin fiziksel olarak çalınması veri hırsızlığı olarak düşünülür. Sınırlı erişimi olan bir kullanıcı hesabına login olup yakalanmak veya neler yapıldığını açıklayan bir mesaj formunda maksatlı olarak kanıt bırakmak veri sahtekârlığına örneklerdir.

Diğer bir tipte suç da elektronik para transferleri veya zimmete geçirme ile ilgilidir. Bilgisayar Sahtekârlığı ve Kötüye Kullanımı Kanunu (Computer Fraud and Abuse Act) ile mahkûm edilen ilk kişi internete solucanı (worm) sunmuştur. Bu solucanlar bilgisayar ortamında serbestçe gezinip virüslere benzer şekilde programlara saldırmıştır. Bunu bazıları vandalizm (yıkıcılık) olarak görmektedir. Solucan çoğalarak 6200 bilgisayarı etkilemiştir.

Bilgisayarlar suç eylemlerinde 3 farklı rol oynayabilir. Birincisi, bilgisayarlar bir saldırının hedefi olabilir. Örneğin, bir hacker bilgisayardan bilgi çalmaya çalışabilir veya bilgisayara ya da bilgisayar ağına zarar vermeye çalışabilir. Bu tip davranışlara örnek olarak web sitelerinin değiştirilmesi ve bilgisayarlara virüs bulaştırılması sayılabilir.

İkinci olarak, bilgisayarlar geleneksel bir saldırının gerçekleştirilmesinde, örneğin çocuk pornosunun yaratılması ve transfer edilmesinde, bir araç olarak kullanılabilir.

Bilgisayarın kullanabileceği suçlar listesini aşağıdaki gibi sıralayabiliriz:

- Uyuşturucu ticareti
- Kanunsuz 'telemarketing'
- Sahtekârlık, özellikle sahte faturalar
- Entellektüel mülk hırsızlığı
- 'Gerçek yüz' veya ID hırsızlığı ve yanlış temsil
- Casusluk, en konvansiyonel terörizm ve suç
- Elektronik izleme
- Çocuk pornografisi
- Tarih sahtekârlıkları
- Çete suçları, özellikle silah ihlalleri
- Organize suç
- Silahlı soygun simülasyonu
- Kopyalama suçları
- DoS (servis kullanımı engelleme) saldırıları
- Şantaj
- Web sitesi değiştirme (otomatik)
- Endüstriyel ve ulusal

Üçüncü olarak, bilgisayarlar saldırı için 'incidental' (tesadüfi) olabilir fakat bu kanun güçleri için önemlidir. Örneğin, çoğu uyuşturucu kaçakçısı kayıtlarını bilgisayarlarda depolamaktadır ki bu da kağıt üzerindeki kayıtlara oranla forensic (adli) ve kanıt

işlemlerinde zorluk çıkarır. Ek olarak tek bir bilgisayar 3 şekilde de kullanılabilir. Örneğin, bir hacker bilgisayarını kullanarak internet servis sağlayıcısına (hedef) yetkisiz olarak erişebilir ve bu erişimi kullanarak ISS`nin disk sürücüsünde bulunan (incidental) özel bir yazılımı kanunsuz olarak dağıtmada (araç) kullanabilir.

Bilgisayar suçu konusunda endişelenmesi gereken firmalar sadece internet servis sağlayıcılar ve büyük finans kuruluşları değildir. Hacker'lar bireyleri direkt olarak veya ISS'leri üzerinden kişisel ve finans bilgilerinin bütünlüğüne ve gizliliğine saldırarak etkileyebilir.

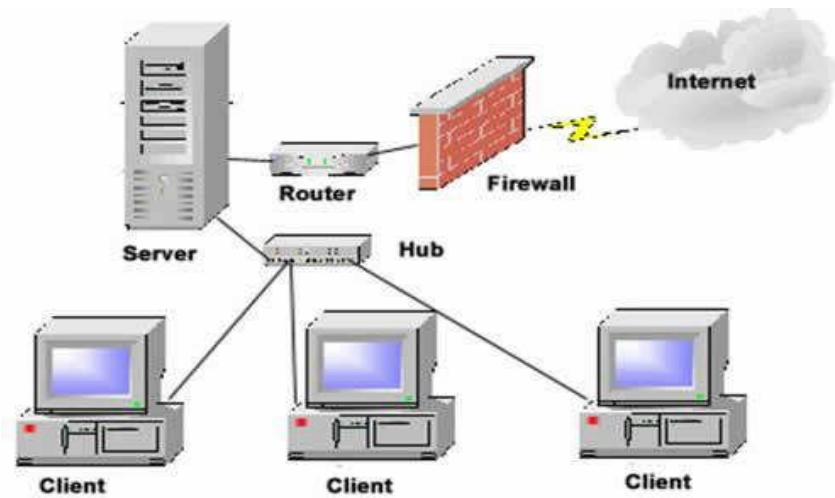
1.3. Güvenlik Duvarı (Firewall) Cihazı

1.3.1. Güvenlik Duvarı Nedir?

Güvenlik duvarı, bir sistemin özel bölümlerini halka açık (public) bölümlerden ayıran, kullanıcıların ancak kendilerine tanınan haklar düzeyinde sistemden yararlanmasını sağlayan çözümlerdir.

Güvenlik duvarı belirli bir makineyi denetlemek için o makine üzerine (host-based) kurulabileceği gibi, bir bilgisayar ağını denetlemek için de kurulabilir. Bu bölümde ağ güvenliğini sağlamak üzere kullanılan ağ güvenlik duvarı çözümleri üzerinde durulmuştur. Ağ güvenlik duvarı, içeride birbirlerine güvenen, az korumalı makinelerin olduğu bir kurum ağı ile dış ağlar (internet) arasına yerleştirilir ve aradaki fiziksel bağlantı yalnızca güvenlik duvarı tarafından sağlanır (Şekil 1.3.1). Güvenlik duvarları salt dış saldırılara karşı sistemi korumakla kalmaz, performans artırıcı ve izin politikası uygulayıcı amaçlar için de kullanılır.

Yukarıda belirtilen sorunları çözmek için bir antivirüs sunucusu veya web adresi denetleyicisi sunucusu ile ortak olarak çalışabilirler. Ağ güvenlik duvarı, yazılım veya donanımla yazılımın entegre olduğu çözümler şeklinde olabilir.



Şekil 1.2: Tipik bir güvenlik duvarı

Ağ güvenliği sağlanırken ister kurumsal ister kişisel bazda olsun ilk önce saldırı tespiti yapılmalıdır. Daha sonra bu tespite göre uygun program ve donanım seçilmelidir. Bilgisayar içindeki bilgiler kişiler için çok önemli olduğundan bunlardan gelebilecek bir saldırı sonucunda bilgilerin yok olması veya istenmeyen kişilerin eline geçmesi mümkün olacaktır. Bu da kişi ya da kuruluşların büyük zararlara uğramasına sebep olacaktır. Bu yüzden ağ güvenliği sağlanırken yukarda açıklanmış olan ağ güvenliği sağlama yöntemleri eksiksiz bir biçimde uygulanmalıdır.

Servis kullanımı engelleme (DoS) internetteki istemci ve sunucular için en ciddi tehditlerden biridir. Aynı zamanda engellenmesi en zor güvenlik tehdididir. Bir servis kullanımı engelleme saldırısı kurbanın normalde erişebildiği bir servise erişebilmesini engelleyen kötü amaçlı bir saldırıdır. Bir saldırganın bunu gerçekleştirebilmesi için pek çok farklı yol vardır.

Bunun için özel ağ ile internet arasına bir Firewall konulması gerekmektedir (Şekil 1.2). Bu sistem ile ağ güvenliği tam olarak sağlanır ve erişim hakları düzenlenir. Bu sistem kurulurken şu noktalara dikkat edilmelidir. Kurulmadan önce ne tür bilgilerin koruncağı, ne derecede bir güvenlik uygulanacağı ve kullanılacak güvenlik algoritmaları önceden belirlenmelidir. Firewall'ın sistem üzerinde etkili kullanılması için ağ ortamı ile internet arasındaki tüm trafiğin Firewall üzerinden geçilmelidir.

Özel ağ kaynaklarına erişimi kısıtlayarak güvenlik politikalarını uygulayan ağ yapılarında kullanılan, yazılım veya donanım çözümleridir.

Kapı kilidine benzetilebilir. Bir odayı sadece anahtarı olan kişilerin açabileceği gibi, ağdaki bir alana da sadece şifresi aracılığıyla erişim hakkına sahip olan kullanıcı girebilir.

Firewall dış dünya ile ağ arasındaki koruyucu bir katmandır. İzinli girişler arasındaki bilgi alış-verişini herhangi bir gecikmeye maruz bırakmadan yapar. Ayrıca, ağa girmeye çalışan herhangi izinsiz bir materyale karşı filtre görevi yapar, ağa girişe izin vermez. Daha sonra, izinsiz ağa girmeye çalışanları, yöneticiye rapor eder.

Güvenlik duvarı (firewall), internet gibi harici ağlarda ya da ağlardan erişim gerektiren ağlarda uygulanan ana güvenlik mekanizmalarından biridir. Bir güvenlik duvarı firmanın dâhili ağını harici internetten ayıran bileşenlerdir. Güvenlik duvarları spesifik bağlantıların geçmesini ve diğerlerinin bloklaşmasını sağlar ve genelde dâhili ağın internete bağlandığı sınırda uygulanır.

1.3.1.1. Güvenlik Duvarı Bileşenleri

Güvenlik duvarı bileşenleri aşağıdakilerin kombinasyonu olabilir:

- Paket-filtreleme router`ları (packet-filterin routers)
- Devre ağ-geçitleri (circuit gateways)
- Uygulama ağ-geçitleri (application gateways)

Çeşitli organizasyonlar güvenli bilgisayar işlemleri için standartlar geliştirmiştir. Örneğin Amerikan Savunma Bakanlığı Orange Book adı verilen yayınlarında çeşitli güvenlik seviyeleri tanımlamaktadır. Orange Book bilgisayar sistemini içerdiği bileşenlere göre sınıflandırmaktadır. Örneğin, C2 güvenlik seviyesi kullanıcıların komutları çalıştırmasında kimlik tanılama seviyeleri kullanır ve denetlemenin kullanılmasını belirler (Avrupa Birliğinin ITSEC Standartlar Katalogu sistemleri Orange Book`takine benzer şekilde sınıflandırır).

Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) açık sistemler standartlarını ve birlikte çalışabilirliği geliştirmekten sorumludur. Gizli veriler için standartlar geliştirdi ve kriptolama standartları geliştiren Ulusal Güvenlik Kurumu (NSA) ile birlikte çalışmıştır.

IETF (Internet Engineering Task Force) internet standartları dâhil kısa-dönem mühendislik konularından sorumludur.

1.3.1.2. Firewall Oluştururken Dikkat Edilmesi Gereken Hususlar

Ağ güvenlik duvarı (network firewall), kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları çözmek üzere tasarlanan çözümlerdir. Bu çözümler yazılım veya donanımla yazılımın entegrasyonu şeklinde olabilir. Güvenlik duvarı çözümü açık sistemler üzerinde bedava dağıtılan modüllerle sağlanabileceği gibi, fiyatları sundukları servislerle orantılı olarak artan ticari ürünlerle de sağlanabilir. Bu bildiride bu tür çözümlerin tanımları yapılmış ve güvenlik duvarı çözümü seçerken dikkat edilmesi gerekenler belirtilmiştir.

1.3.1.3. Sorunlar

İnternet bağlantısında bir kurumun karşılaşabileceği sorunlar aşağıdaki gibidir:

- Dış dünyadan kurum ağına (içeriye) yapılacak saldırılar
- İnternette dolaşırken kullanıcı bilgisayarına, bilgisayardan da sisteme virüs bulaşması
- Mesh, edonkey, overnet gibi programlarla dosya paylaşımının yapılması ve bant genişliğinin (internet veriyolu kapasitesinin) maksadı dışında kullanılması
- İnternette özellikle vakit kaybettirici bazı sitelere ulaşımın kurum içerisinde, kurum zamanında (mesai saatlerinde) yapılması
- İçeriden yetkisiz kişilerin dışarıya bilgi göndermesi
- Yetkisiz kullanıcıların internette gezinmesi

1.3.2. Güvenlik Duvarı Yapısı ve Çalışması

Güvenlik duvarı (Firewall), yerel ağlar üzerindeki kaynakları diğer networkler üzerinden gelecek saldırılara karşı koruyan, iç ve dış ağlar arası ağ trafiğini tanımlanan kurallara göre denetleyen bir ağ geçidi çözümüdür. Kullanıcılarına internet erişimi hakkı vermiş olan bir kurum, yerel ağındaki kaynakları korumak ve dış ağlardaki kaynaklara

kullanıcılarının erişim hakkını belirlemek için yazılım veya donanım bazlı güvenlik duvarları kullanırlar.

Temel olarak, bir yönlendirici programı ile beraber çalışan bir firewall, network üzerinde kendisine gelen paketlerin gitmelerine gereken yerlere (üzerinde tanımlanan kurallar doğrultusunda) gidip gidemeyeceğine karar verir. Bir firewall ayrıca, kullanıcıların istek paketlerini ağa gitmeden önce karşılayacağı bir proxy sunucusuna sahiptir veya bir proxy ile beraber çalışır. Firewall'lar genel olarak, özellikle network'teki diğer makinelerden farklı bir makinenin üstüne kuruludurlar. Bunun sebebi, dışarıdan gelen isteklerin direkt olarak lokal network kaynaklarına ulaşmasını engellemektir.

Güvenlik duvarları'nın birçok denetleme metotları vardır. En basit perdeleme metotlarından biri, daha önceden belirlenmiş domain'lerden ve IP adreslerinden (izin verilen servislerin) paketlerini kabul edip diğer istekleri reddetmektir. Mobil kullanıcılar güvenlik duvarları aracılığı ile, özel ağlara güvenli bağlanma prosedürleri ve tanılama metotları kullanarak uzaktan erişim hizmetini kullanabilirler.

Güvenlik Duvarı (Firewall) urunu üreten birçok firma vardır. Genel firewall özellikleri arasında log tutma, raporlama, atak sınırları aşıldığında otomatik alarm verme ve grafik ara yüzü ile yönetilebilme sayılabilir.

1.3.3. Güvenlik Duvarı Çeşitleri

1.3.3.1. Packet-Filtering Firewall

Bu yöntem Firewall oluşturmanın en kolay yoludur. Paketlerin başlık alanı içindeki bilgilere bakılarak istenmeyen paketler karşı tarafa geçmez. OSI modelinde 3 katman olan network katmanında çalışır.

1.3.3.2. Circuit-Level Gateway

OSI modelinde 4 katmanı olan session katmanı düzeyinde çalışır. Bu sistemde oturum bir kez kabul edilip kurulduktan sonra, her paket için denetim yapılmaz. Paketler kurulan sanal devre üzerinden geçer.

1.3.3.3. Application-Level Gateway

En sık koruma yapan Firewall tekniğidir. OSI modelinde uygulama katmanı düzeyinde çalışır. Bu nedenle tam denetim yapma imkânı sunar.Bu tür düzenlemede oturum kurulduktan sonra bile paketlerin sınaması yapılmaktadır. Bundan dolayı beklenmedik saldırılara karşı korumayı güçlendirir.

1.3.3.4. Cisco Güvenlik Duvarı Çeşitleri

Cisco üç tip güvenlik duvarı çözümü sunmaktadır:

- **Güvenlik Duvarı Donanımları (Dedicated Firewall Appliances):** Dinamik filtreleme yapan özel güvenlik duvarı cihazlarıdır. Cisco PIX ailesi örnek olarak verilebilir.

- **Entegre Cisco IOS Güvenlik Duvarları (Entegrated Cisco IOS Firewalls):** Yönlendirme cihazına yazılım temelli güvenlik duvarı yeteneklerinin ilave edilmesine dayanır. Yönlendirici işlemci ve hafızası yönlendirme ve güvenlik duvarı fonksiyonları için paylaşılır. Güvenlik duvarı koruması için seçilebilecek en ucuz yöntemdir.

- **Entegre Güvenlik Duvarı Servis Modülleri (Firewall Services Modules):** Cisco Catalyst 6500 Serisi Anahtarlara veya Cisco 7500 Serisi İnternet Yönlendiricilere takılabilen güvenlik duvarı modülleridir. FWSM cihaz üzerindeki herhangi bir portun güvenlik duvarı portu olarak kullanılmasına izin verir.

Bir güvenlik duvarı çözümünde verilebilecek servislere örnek olarak aşağıdakiler sayılabilir:

- **NAT (Network Address Translation):** Çağda internete çıkamayacak özel IP şemaları (10.0.0.0/8, 192.168.0.0/16 vb) tanımlanır ve dış bağlantılarda NAT sunucusunun reel IP'si kullanılarak iç ağ konusunda saldırganın bilgi sağlaması engellenir. Güvenlik için artıları olmakla beraber, NAT çoğunlukla adres yönetimi için kullanılmaktadır.

- **Paket Filtreleme:** En basit güvenlik duvarıdır. Router, modem gibi cihazlarla birlikte gelir. Erişim listelerinin (access list) kullandıkları yöntemdir. Bu yöntemle güvenlik duvarından geçen her üçüncü seviye (IP, IPX ..vb) paketine bakılır ve ancak belli şartlara uyarsa bu paketin geçişine izin verilir. Paket filtreleme, güvenlik duvarının her fiziksel bağlantısı üzerinde ayrı ayrı ve yöne bağlı (dışarıya çıkış, içeriye giriş) olarak uygulanabilir. Uygulamaların bağlantı için kullandıkları portlar (icq, imesh .vb. portları) baz alınarak hangi ağların veya kişilerin ne zaman bu uygulamalarla bağlantı kurabileceği belirlenebilir. Paket filtrelemede birim zamanda tek bir pakete bakıldığı ve önceki paketler hakkında bir bilgiye sahip olunmadığı için bu yöntemin çeşitli zayıflıkları bulunmaktadır.

- **Dinamik (Stateful) Filtreleme:** Paket filtrelemeden farkı, paketin sırf protokolüne bakarak karar verilmesi yerine, güvenlik duvarının bir bağlantıyı hangi tarafın başlattığını takip etmesi ve çift yönlü paket geçişlerine buna göre karar vermesidir. Her bağlantı için durum bilgisi tablolarda tutulduğu için paket filtrelemedeki zayıflıklar bulunmamaktadır. Dezavantajı ise dinamik filtrelemenin çok daha fazla işlemci gücüne ve belleğe ihtiyaç duymasıdır.

Özellikle bağlantı(connection) sayısı arttıkça işlem ihtiyacı da artacaktır[2]. Paket filtreleme yerine dinamik filtreleme tercih edilmelidir.

- **DMZ (Silahtan Arındırılmış Bölge):** Dış dünyaya hizmet verecek sunucular buraya yerleştirilmektedir. Özellikle iç ağda NAT uygulaması yapılıyorsa dış dünyaya hizmet veren cihazlar reel IP'lerle burada konumlandırılacaklardır.

- **Proxy:** Proxy bir bağlantı uygulamasında araya giren ve bağlantıyı istemci (client) için kendisi gerçekleştiren bir servistir. Proxy'nin kullanımı, uygulama temelli (application-level) güvenlik duvarı olarak da adlandırılabilir. Bu tür bir uygulama aynı zamanda şu amaçlar için kullanılabilir:

  - Kimlerin bu servisleri kullanacağını belirlemek
  - Performans amaçlı olarak özellikle aynı istekleri bir defaya indirgeyerek bağlantı sayısını azaltmak ve bant genişliğinin daha etkin kullanılmasını sağlamak

- **Anti-Virus çözümleri:** HTTP, FTP ve SMTP trafiğini üzerinden geçirerek virüs taramasını yapmayı ve kullanıcıya gelmeden önce virüslerden temizlemeyi hedefleyen sistemlerdir.

- **İçerik Filtreleme (content filtering):** Çeşitli yazılımlarla ulaşılmak istenen web sayfalarını, gelen e-posta'ları filtrelemeye yarayan sistemlerdir.

- **VPN:** Ortak kullanıma açık veri ağları (public data network) üzerinden kurum ağına bağlantıların daha güvenilir olması için VPN kullanılmaktadır. İletilen bilgilerin şifrelenerek gönderilmesi esas olarak alınır. Public/Private anahtar kullanımı ile sağlanır.

- **Saldırı Tespiti (ID):** Şüpheli olayları ve saldırıları tespit etmeyi hedefleyen bir servistir. Saldırı tespit sistemleri(IDS), şüpheli durumlarda e-posta veya çağrı cihazı gibi yöntemlerle sistem yöneticisini haberdar edebilmektedir.

- **Loglama ve Raporlama:** Kayıtlama (log) ve etkinlik raporları birçok güvenlik duvarı tarafından sağlanmaktadır. Bu kayıtlar çok detaylı ve çok fazla veri içerebilmektedir. Bazı güvenlik duvarları bu logların incelenmesini kolaylaştırmak için çeşitli analiz ve raporlama servisleri sunmaktadır. Kayıtlar sistemlerin zayıflıklarının ve saldırıların belirlenmesinde işe yaramaktadır.

1.3.4. Güvenlik Duvarı Ayarları

1.3.4.1. Yazılım Çözümleri

Güvenlik duvarı çözümü yazılım veya donanımla yazılımın entegre olduğu sistemler şeklinde olabilmektedir. Bu tür çözümlerin birbirine çeşitli artıları ve eksileri bulunmaktadır.

İşletim sistemi üzerinde çalışan çözümlerin artıları aşağıdaki gibidir:

- Çok detaylı raporlamalar alınabilir.
- Önce detaylara kadar kullanıcıları ayrıştırmak ve takip etmek mümkündür.

Bu tür sistemlerin üzerinde çalıştığı işletim sisteminin açıkları en büyük eksiğidir. Burada şu da belirtilmelidir ki bu işletim sistemleri genelde öz (core) olarak kurulduklarından üzerlerindeki servisler kısıtlıdır. Güvenlik duvarları da üzerlerinde çalıştıkları işletim sistemlerinin bazı açıklarını kapatırlar. İşletim sistemi üzerinde çalışan sistemlerin eksileri olarak aşağıdakileri belirtmek mümkündür:

- **Bakım Problemleri:** Güvenlik duvarının üzerinde çalıştığı işletim sisteminin de ayrıca bakımı gerekecektir.
- **Kurulum:** İşletim sisteminin doğru kurulması gereklidir. Gerekmeyen servislerin kaldırılması ve bazı yamaların (patch) uygulanması gerekmektedir. Kurulum süresi, kutu çözümlerine göre daha uzun sürmektedir.
- **İşletim Sisteminin Güvenliği:** Güvenlik duvarının üzerinde kurulduğu işletim sisteminin öncelikle güvenliği sağlanmalıdır. İşletim sistemini seçerken Multi Router Traffic Grapher (MRTG), SNMP protokolü ile toplanan verileri grafiksel olarak görüntüleyen bir programdır. Sistemle birlikte gelen güvenlik açıkları ve zayıflıkları araştırılmalı ve çeşitli ayarlamalarla güvenliğin sağlanabileceği sistemler seçilmelidir.

1.3.4.2. Donanım Çözümleri

Kutu çözümleri kullanıldıkları yerin özelliğine göre ikiye ayrılabilir:

- **Küçük kutu çözümleri:** Bunların üzerinde genellikle Ev/Küçük işletmeler (Home/Small Bussiness) çözümleri çalışır ve bu sınıftaki ürünlerin üzerindeki yazılımlar işlev ve genişletilebilirlik açısından kısıtlı sürümlerdir. Genellikle donanımsal genişletilebilirlikleri yoktur.
- **Performans kutuları:** Bunların üzerinde (100+ kullanıcı) kurumsal sürümler çalışır ve bunlar işletim sistemi üzerinde çalışan sürümlerle aynıdır. Ana fark, bu donanımların söz konusu yazılım için ayarlanmış (tune edilmiş) özerk (proprietary) donanımlar olmasıdır. Bu nedenle aynı koşullardaki işletim sistemi tabanlı versiyonlardan daha performanslı çalışmaktadırlar.

Kutu çözümlerin artıları aşağıdaki gibidir:

- Uygulama için özel geliştirilmiş entegre devrelere (ASIC) sahip olduklarından daha yüksek performans elde edilebilmektedir.
- Genelde en kötü saldırılarda dahi cihazı kapatıp açınca yeniden çalışmaya devam ederler.

- Versiyon yükseltmeleri (upgrade) diğer sistemlere göre daha çabuk yapılır.
- Hizmet dışı kalma süreleri (downtime) azdır.
- İşletim sistemleri bilinmediğinden (Genelde UNIX türevleridir) ve az kullanıldığından açıkları fazla bilinmez.
- Kutu çözümlerin eksileri aşağıdaki gibidir:
- Yazılabilecek kurallar cihazın versiyonu ve kapasitesi ile sınırlıdır.
- Küçük kutu çözümlerinin donanımsal genişletilebilirlik özellikleri yoktur.
- Daha güçlü bir cihaz için büyük olasılıkla bir üst versiyonun alınması gerekecektir. Performans kutularında ise işlemci ve bellek terfileri zor ve pahalıdır.
- Raporlamaları genelde çok sınırlıdır.
- Özellikle küçük kutu çözümlerinde, değişik saldırılara karşı yeni çözümler çok çabuk çıkmaz.
- Versiyon yükseltmeleri (upgrade) mutlaka açma kapamayı gerektirir.
- Performans kutuları işletim sistemi üzerinde çalışan çözümlerden daha pahalıya mal olabilmektedir.

1.3.5. Güvenlik Duvarı Üreticileri

Günümüzdeki Firewall'lar da sadece port kapamak amaçlı kullanılmıyor. Yeni nesil Firewallar da UTM (Unified Threat Management) kısaca açıklaması (firewall,antivirus, antispam, ids/ips, vpn,router,gibi özellikleri olan) tümleşik cihazlardır. Her ne kadar bir dönem bilinen Firewall markaları UTM cihazların hantal ve başarısız olduğunu iddia etse de günümüzde tüm Firewall üreticileri UTM cihazlarını üretmektedir. Kısaca şu an bilinen Firewall (UTM) cihazlarından ve markalarından bahsedelim.

Fortinet, Netscreen, Juniper, Symantec, Cisco ASA serisi Bu cihazlar üzerinde port protokol bazında kısıtlama yapabilir. Web filtrelemesi (terör,şiddet,silah gibi kategorilerine göre yasaklama yapabilir.), dosya indirme gibi işlemleri durdurabilir. İyi kurulmuş bir firewall bilgisayarınızı bir daktiloya çevirebilir.)

UTM cihazının ilkleri Juniper Networks Fortinet (Juniper networks'ten ayrılan ortakların kurduğu bir firma) Netscreen firması Juniper Networks'ü satın almıştır.

UTM cihaz üretmeye başlayanlar Cisco ASA Serisi Symantec Panda’ dır.

Firewall ve UTM Özelliği ayrı olanlar Checkpoint Cisco Sonicwall Watcguard Isa server ve bilmediğimiz bir çok marka vardır.

Firewall'lar işletim sistemi olarak genelde Linux kullanıyor Bu işletim sistemleri cihazlardaki flaşa gömülü olarak gelmektedir. Box cihazlar normal PC firewall'a göre daha hızlı çalışır. Çünkü özel üretilmiş işlemci mimarisi kullanır. Bu da Policylerin daha hızlı çalışmasını sağlar.

KOBİ'ler için tasarlanan 5GT serisi ülkemiz koşulları için oldukça idealdir. Ekonomikliği ve işlevselliği kurum güvenliğine önemli katkılar yapmaktadır.

Netscreen Firewall cihazları en alt modelden en üst modele aynı arayüze ve temel yazılıma sahiptir. Hazır gelen özellikleri ile bir kurumun güvenlik ihtiyaçlarını oldukça karşılamaktadır. İhtiyaca göre gateway antivirüs, spyware, web taraması, VPN tünelleme yapabilen

Netscreen Firewall cihazları dâhili ADSL modemli modelleri ile KOBİ'ler için ideal cihazlardır. Netscreen Firewall cihazlarının genel ve model özellikleri aşağıda belirtilmiştir.

 **Şekil 1.3: Netscreen Firewall Cihazları**	Statefull and Deep Inspection Firewall (Application Level) Hazır Deep inspection paketleri ile Server ve Client için saldırı önleme. SurfControl ile Entegre Web Filtreleme (Ayrıca Surf control kurmanıza gerek yok) Surfcontrol ve Websense Web Filtreleme desteği Trend Micro ile Entegre Antivirüs. Enterprise seviyede VPN Çözümleri. Bant Genişliği Yönetimi ASIC Teknolojisi Dial Backup ile hattın yedeklenmesi. Dual Untrust özelliği ile yedekli internet erişimi. Kaspersky Antivirus ile spyware taraması. Antispam koruması.
Netscreen 500	Sınırsız Kullanıcı , 1500 VPN Tüneli
Netscreen ISG 2000	Sınırsız Kullanıcı , 10000 VPN Tüneli
Netscreen 5200/5400	Sınırsız Kullanıcı , 25000 VPN Tüneli

Tablo 1.1: Netscreen Firewall Modelleri ve Özellikleri

Şekil 1.4: Netscreen-5GT Firewall Cihazı

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ Firewall cihazını router ile yerel ağ arasına kurunuz.	➢ Bağlantıların sağlam olmasına dikkat ediniz.
➢ Router'a bağlanan fxp0, LAN'a bağlanan fxp1 olarak tanıtınız.	➢ Bu intel marka Ethernet kartlarında böyledir. Farklı da olabilir.
➢ fxp0'a 212.152.10.5 nu.lı IP'yi, atayınız.	➢ Farklı bir ip de atayabilirsiniz.
➢ fxp1'e ise 192.168.0.1 nu.lı IP'yi atayınız.	Farklı bir ip de atayabilirsiniz.
➢ Sistemi cvsup ile stable hâle getiriniz.	➢ Bu işlemi ağ ayarlarını tamamladıktan sonra yapınız.
➢ /etc/sysctl.conf dosyasına net.inet.ip.forwarding=1 satırını ekleyiniz.	➢ Bu işlem Ethernet kartları arasında paket geçişine izin vermek içindir.
➢ /etc/rc.conf dosyasına giriniz.	➢ Açılış scriptlerinde düzenlemeler yapmamız içindir.
➢ firewall_enable="YES" firewall_type="open" gateway_enable="YES" ayarlarını yapınız.	➢ Bu ayarları dikkatli yapınız.
➢ tcp_drop_synfin="YES" portmap_enable="NO" ayarlarını yapınız.	➢ Bu ayarları dikkatli yapınız.
➢ inetd_enable="NO" usbd_enable="NO" ayarlarını yapınız.	➢ Bu ayarları dikkatli yapınız.
➢ Bu şekilde standart bir ayarlama yapılmış oldu ve firewall cihazı kuruldu.	➢ Daha sonra geniş bir ayarlama yapabilirsiniz.

ÖLÇME VE DEĞERLENDİRME

OBJEKTİF TEST (ÖLÇME SORULARI)

Aşağıdaki cümlelerde bazı kelimelerin yerleri boş bırakılmıştır. Boş bırakılan yerlere doğru kelimeleri yazınız. Sorulara verdiğiniz cevapları modül sonunda verilen doğru cevaplarla karşılaştırarak kendinizi kontrol ediniz.

1. ……., bir olay olduğunda hasarın derecesi ya da olayın olma ihtimali olarak tanımlanabilir

2. Herhangi bir bilgisayar ağına gönderilen ……., o bilgiyi almaya yetkisi olmayan kişilerce ele geçirilebilir.

3. Bilgi iletişiminde, bir alıcının ……. numarasını kullanarak sanki o alıcıymış gibi gönderilen bilgileri istediği gibi kullanabilir.

4. Kullanıcı ana sisteme giriş yaptığında giriş parolası ve iletilen veri …… tarafından ele geçirilir.

5. Bireysel açıdan bakıldığında, sistemdeki en kıymetli şey ……...

6. Bir tür bilgisayar ağı saldırısı olarak bilinen …….. saldırıların da bilgisayar korsanları, istedikleri Web sitesini çalışmaz hâle getirebiliyor.

7. DoS yani açılımı Denial of Sevice olan bu saldırı çeşidi bir …….. yöntemidir.

8. …….: Bu atak tipi belirli host ve servisleri düşürmek için kullanılır.

9. …….: Service Overloading'den farkı sistemin normal çalışmasını engellemez.

10. ……...Saldırganın SYN gönderip ACK alıp ondan sonra da gelen ACK' ya cevap vermeyip sürekli SYN göndermesinden oluşur.

11. Bir saldırgan hedef aldığı bir makineye büyük …….. gönderir.

12. …… programı hedef sisteme yüksek miktarda ICMP veri paketleri gönderir

13. …… aynı kaynak ve hedef portları kullanarak SYN paketleri gönderir.

14. WinNuke programı hedef sistemin 139 nu.lı portuna "……..."denilen verileri gönderir.

15. Koordineli olarak yapılan bu işlem hem saldırının boyutunu artırır hem de saldırıyı yapan kişinin gizlenmesini sağlar. Bu işlemleri yapan araçlara …….. denir.

16. …… DDoS yöntemini kullanan ilk programdır.

17. Exploit'ler: …….'in kelime anlamı "kötüye kullanma, sömürme" demektir.

18. Exploit'ler genelde …….. olarak çalışırlar yani Unix'e ait bir exploit Windows için çalışmaz.

19. ……, çoğunlukla ya şakayla, ya kötü niyetle ya da yanlışlıkla kendi şirketlerinin ağına veya önemli bilgilere zarar verirler.

20. Topluma zarar vermeyi alışkanlık hâline getirenler de bozucu programlar yazarak piyasaya gizlice sürmektedir. İşte bu işi yapanlara ……. kullanıcılar diyoruz.

21. Bilgisayar suçları sabotaj, intikam, vandalizm, hırsızlık, gizlice dinleme, veri sahtekârlığı veya veri bilgisayar sitemine girmeden önce, girerken ya da girdikten sonra …….. yapmayı içerir.

22. Bir hacker bilgisayarını kullanarak …… sağlayıcısına (hedef) yetkisiz olarak erişebilir.

23. Hacker'lar bireyleri direkt olarak veya ……. üzerinden kişisel ve finans bilgilerinin bütünlüğüne ve gizliliğine saldırarak etkileyebilir.

24. ……, bir sistemin özel bölümlerini halka açık (public) bölümlerden ayıran, kullanıcıların ancak kendilerine tanınan haklar düzeyinde sistemden yararlanmasını sağlayan çözümlerdir.

25. Ağ güvenliği sağlanırken ister kurumsal ister kişisel bazda olsun ilk önce …… yapılmalıdır.

DOĞRU / YANLIŞ TESTİ

Aşağıdaki soruların cevaplarını doğru ve yanlış olarak değerlendiriniz. Sorulara verdiğiniz cevapları modül sonunda verilen doğru cevaplarla karşılaştırarak kendinizi kontrol ediniz.

SORULAR		DOĞRU	YANLIŞ
26	Packet-Filtering FirewallOSI modelinde 3 katman olan network katmanında çalışır.		
27	Circuit-Level Gateway sisteminde oturum bir kez kabul edilip kurulduktan sonra, her paket için denetim yapılır.		
28	Application-Level GatewayEn sık koruma yapan Firewall tekniğidir. OSI modelinde uygulama katmanı düzeyinde çalışır.		
29	Güvenlik için artıları olmakla beraber, NAT çoğunlukla adres yönetimi için kullanılmamaktadır.		
30	Saldırı Tespiti (ID): Şüpheli olayları ve saldırıları tespit etmeyi hedefleyen bir servistir.		
31	Küçük kutu çözümleri üzerinde genellikle Ev ve Küçük işletmeler (Home/Small Bussiness) çözümler çalışır.		
32	Kutu çözümlerinde versiyon yükseltmeleri (upgrade) diğer sistemlere göre daha yavaş yapılır.		
33	Küçük kutu çözümlerinin donanımsal genişletilebilirlik özellikleri yoktur.		
34	Özellikle küçük kutu çözümlerinde, değişik saldırılara karşı yeni çözümler çok çabuk çıkar.		

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları geri dönerek tekrar inceleyiniz. Tüm sorulara doğru cevap verdiyseniz diğer modüle geçiniz.

ÖĞRENME FAALİYETİ–2

AMAÇ

Yedeklemeyi tanıyarak, ağınızın olası tehlikelere karşı güvenliğini sağlayacaksınız.

ARAŞTIRMA

- Size en yakın bilgisayar laboratuvarına giderek, hangi tür yedekleme işlemlerinin yapıldığını öğreniniz.
- Yedekleme işleminin nasıl yapıldığını öğrenerek hangi yöntemin seçildiğini ve neden seçildiğini öğreniniz.

2. YEDEKLEME

2.1. Yedekleme

Yedekleme, en genel anlamıyla, bir bilgisayar sistemini işlevsel kılan temel birimlerin, üzerinde çalışan yazılımların ve depolanan verilerin, arıza, hata, hasar durumlarında çalışmaların kesintiye uğramasını veya verilerin geri dönülemez biçimde kaybolmasını engellemek amacıyla birden fazla kopya hâlinde bulundurulmasını sağlayan işlemler bütünüdür.

Sabit diskte bulunan programların bir kopyasının disk, hard disk, disket vb. alınmasıdır. Yedekleme işlemini yapmak için disk, hard disk, disket vb.lerine ihtiyaç vardır. Yedekleme için arj, zip, backup programları kullanılabilir. Genellikle az kullanılan veriler sıkıştırılarak disketlere kopyalanır. Ayrıca çok önemli dosyalarında disketlere kopyalarının alınması kullanıcının dosyaların bozulmasına karşı önlem alması bakımından önemlidir.

Dosyalar, sabit disk üzerine yazılıp silindikçe tek bir dosya fiziksel olarak bir kaç parçaya bölünmüş olabilir. Bu da dosyayı okuma hızını yavaşlatır. Çünkü okuma kafası dosyanın tümü üzerinde çalışırken farklı noktalara gidip gelmek zorunda kalacaktır. Okuma hızını artırmak ve parçalanan dosyaları birleştirmek için birleştirme (DEFRAG) yapılır. Programlar-Donatılar-Sistem Araçları- Disk Birleştiricisi çalıştırılır.

Disk üzerinde zaman zaman farklı nedenlerden dolayı bazı dosyalar bozulabilir. Özellikle bir dosya üzerinde çalışırken bilgisayarın düğmeden kapatılması, elektrik voltajındaki değişikler vb. buna neden olabilir.

Bu bozuk programların bir kısmı kurtarılabilir. Bunun için Programlar-Donatılar-Sistem Araçları-ScanDisk komutu kullanılır.

2.1.1. Yedekleme Nedir?

- Sabit Disk
- Yedek Sabit Disk
- RAID Sabit Disk
- Disket
- CD-R / CD-RW
- DVD-R / DVD-RW / DVD+R / DVD+RW
- Zip Disk / LS Disk
- Harici Sabit Disk
- USB Bellek
- Teyp Sürücü
- Ağa Bağlı Depolama

Yukarıdaki yedekleme donanımlarından herhangi biri veya birkaçını kullanarak bilgisayarınızdaki bilgilerin periyodik zamanlarda birer kopyasının alınmasına yedekleme denir. Bu işlem için günümüzde en çok CD ve disketler kullanılmaktadır.

Periyodik zamanlarda (genelde haftada bir) bilgilerin disketlere yedek alınması gerekmektedir. Daha sonra ayda bir bu yedek alınan disketler, disketlerdeki bozulmaları önlemek için formatlanmalı (biçimlendirilmeli) ve daha sonra yeniden yedekleme işlemi yapılmalıdır. Disketler kesinlikle manyetik ortamlarda ve güneşte bırakılmamalıdır.

2.1.2. Yedeklemenin Önemi

Yedekleme bilgi yatırımımızı korumanın bir yoludur. Bilgilerimizin çeşitli kopyalarına sahip olursak, herhangi bir kopyanın bozulması bizim için problem teşkil etmez (en fazla yedeklerimizden yüklememizi gerektirir).

Bilgileriniz değerlidir. Onları tekrar meydana getirmek; zaman, para veya en azından kişisel keder ve gözyaşına mal olabilir. Şayet bu bilgiler bazı deneylerin sonucu ise onları tekrar meydana getirmek mümkün olmayabilir. Bilgileriniz bir yatırım olduğuna göre, onları korumalı ve kaybetmemek için bazı adımlar atmalısınız.

2.1.3. Yedekleme Çeşitleri

Yazılımlar, farklı yöntemlerle yedekleme yapılmasına imkân verir. Yaygın üç çeşit yedeklemeyi şöyle sıralayabiliriz:

2.1.3.1. Tam (Full) Yedek

Bu yöntem, seçilen kaynağın tüm içeriğini yedekler. En güvenilir yöntemdir, ancak zaman ve kapasite ihtiyacı yüksektir. Diğer yöntemler uygulanmadan önce, en az bir kez tam yedek alınmalıdır.

2.1.3.2. Adımlı (Incremental) Yedek

Bu tip yedeklemede, sadece son yedekten bu yana yedeklenmemiş olduğu tespit edilen Archive (arşiv) attribute dosyalar yedeklenir. Kurtarma sırasında önce tam yedek, sonra sırayla tüm adımlı yedekler kurtarılmalıdır. Bu nedenle güvenirlik düşer.

2.1.3.3. Fark (Differential) Yedeği

Bu tip yedeklemede, son tam yedekten bu yana yedeklenmemiş olduğu tespit edilen dosyalar yedeklenir. Kurtarma sırasında önce tam yedek, sonra son fark yedeği kurtarılmalıdır. Güvenirlik orta düzeydedir. Bazı yedekleme yazılımları, istek üzerine yapılan yedekleme işlemleri dışında, ayarları kaydedilen bir yedekleme işlemini istenen aralıklarla tekrar edecek özellikler de taşır.

2.2. Sunucu Yedekleme (Server NT Backup)

Yedekleme işlemlerini, komut isteminde veya ntbackup komutu ile birlikte çeşitli parametreler kullanarak toplu iş dosyasından gerçekleştirebilirsiniz.

- **Söz Dizimi**

ntbackup backup [systemstate] "@DosyaAdı.bks" /J{"İşAdı"} [/P {"HavuzAdı"}] [/G {"GUIDAdı"}] [/T { "TeypAdı"}] [/N {"OrtamAdı"}] [/F {"DosyaAdı"}] [/D {"AyarAçıklaması"}] [/DS {"SunucuAdı"}] [/IS {"SunucuAdı"}] [/A] [/V:{yes | no}] [/R:{yes | no}] [/L:{f | s | n}] [/M {YedeklemeTürü}] [/RS:{yes | no}] [/HC:{on | off}]

- **Parametreler**

  - **Systemstate** => Sistem Durumu verisini yedeklemek istediğinizi belirtir. Bu seçeneği belirttiğinizde, yedekleme türü olarak normal veya kopya seçimi zorlanır.

  - **@DosyaAdı.bks** => Bu yedekleme işleminde kullanılacak yedekleme seçim dosyasının (.bks dosyası) adını belirtir.

  - Yedekleme seçim dosyasının adından önce (**@**) karakteri konmalıdır. Bir yedekleme seçim dosyası, yedekleme için seçtiğiniz dosya ve klasörlerdeki bilgileri içerir. Dosyayı, yedeklemenin grafik kullanıcı arabirimi (GUI) sürümünü kullanarak oluşturmalısınız.

- **/J {"İşAdı"}** => Yedekleme raporunda kullanılacak iş adını belirtir. İş adı genellikle geçerli yedekleme işinde yedeklediğiniz dosya ve klasörleri tanımlar.

- **/P {"HavuzAdı"}** => Ortam kullanmak istediğiniz ortam havuzunu belirtir. Bu genellikle Yedekleme ortam havuzunun 4mm DDS gibi bir alt havuzudur. Bunu seçerseniz, /A, /G, /F veya /T komut satırı seçeneklerini kullanamazsınız.

- **/G {"GUIDAdı"}** => Bu teybin üstüne yazar veya ekler. Bu anahtarı /P ile bağlantılı olarak kullanmayınız.

- **/T {"TeypAdı"}** => Bu teybin üstüne yazar veya ekler. Bu anahtarı /P ile bağlantılı olarak kullanmayınız.

- **/N {"OrtamAdı"}** => Yeni teyp adını belirtir. /A'yı bu anahtarla kullanmamalısınız.

- **/F {"DosyaAdı"}** => Mantıksal disk yolu ve dosya adı. Aşağıdaki anahtarları bu anahtarla birlikte kullanmamalısınız: /P /G /T.

- **/D {"AyarAçıklaması"}** => Her yedekleme kümesi için bir etiket belirtir.
-
- **/DS {"SunucuAdı"}** => Belirtilen Microsoft Exchange Server için dizin hizmet dosyasını yedekler.

- **/IS {"SunucuAdı"}** => Belirtilen Microsoft Exchange Server için Bilgi Deposu dosyasını yedekler.

- **/A** => Bir ekleme işlemi gerçekleştirir. Bu anahtarla bağlantılı olarak ya /G ya da /T kullanılmalıdır. Bu anahtarı /P ile bağlantılı olarak kullanmayınız.

- **/V:{yes | no}** => Dosyalar teybe kopyalanırken ortaya çıkmış olabilecek disk hatalarını denetler. Bu seçenek yedekleme süresini önemli ölçüde artırabilir.

- **/R:{yes | no}** => Bu teybe erişimi sahip veya Administrators grubu üyeleriyle sınırlar.

- **/L:{f | s | n}** => Günlük dosyası türünü belirtir: f=tam, s=özet, n=hiçbiri (Günlük dosyası oluşturulmaz).

- **/M {YedeklemeTürü}** => Yedekleme türünü belirtir. Aşağıdakilerden biri olmalıdır: normal, kopya, farklar, artımlı veya günlük.

- **/RS:{yes | no}** => Uzak Depolama Birimi içinde bulunan aktarılmış veri dosyalarını yedekler. Uzak Depolama Birimi yer tutucu dosyalarını içeren yerel Çıkarılabilir Depolama Birimi veritabanını yedeklemek için /RS komut satırı seçeneği gerekli değildir. %systemroot% klasörünü yedeklediğinizde, Yedekleme programı Çıkarılabilir Depolama Birimi veritabanını da otomatik olarak yedekler.

- **/HC:{on | off}** => Kullanılabiliyorsa, teyp sürücüsünde donanım sıkıştırması kullanır.

- **/M {YedeklemeTürü}** =>Yedekleme türünü belirtir. Aşağıdakilerden biri olmalıdır: normal, kopya, farklar, artımlı veya günlük.

- **/?** => Komut isteminde yardımı görüntüler.

➢ **Açıklamalar**

Dosyaları komut satırından ntbackup komutunu kullanarak geri yükleyemezsiniz.

Aşağıdaki komut satırı seçenekleri, bir komut satırı seçeneği ile değiştirilmedikleri sürece, Yedekleme grafik kullanıcı arabirimi (GUI) sürümünü kullanarak ayarlamış olduğunuz değeri varsayılan değer olarak alır: /V /R /L /M /RS /HC. Örneğin, Yedekleme programının Seçenekler iletişim kutusunda donanım sıkıştırması etkin durumda ise, /HC komut satırında belirtilmediği sürece, bu donanım sıkıştırması kullanılacaktır. Ancak komut satırında /HC:off ifadesi belirtilirse, Seçenek iletişim kutusu ayarı geçersiz sayılır ve sıkıştırma kullanılmaz.

Bilgisayarınızda Windows Media Services çalışıyorsa ve bu hizmetlerle ilgili dosyaları yedeklemek istiyorsanız, Windows Media Services çevrimiçi belgelerinde " Windows Media Services ile Yedekleme Çalıştırma" konusuna bakın. Windows Media Services ile bağlantılı dosyaları yedeklemeden veya geri yüklemeden önce Windows Media Services çevrimiçi belgelerinde belirtilen işlemleri izlemeniz gerekir.

Yalnızca yerel bilgisayardaki Sistem Durumu verilerini yedekleyebilirsiniz. Uzak bilgisayardaki Sistem Durumu verilerini yedekleyemezsiniz.

Ortamı yönetmek için Çıkarılabilir Bellek veya verileri depolamak için uzak depolama birimi kullanıyorsanız, aşağıdaki klasörlerde bulunan dosyaları düzenli olarak yedeklemeniz gerekir:

- Sistemkökdizini\System32\Ntmsdata
- Sistemkökdizini\System32\Remotestorage

Böylece, tüm Çıkarılabilir Depolama Birimi ve Uzak Depolama Birimi verileri geri yüklenebilecektir.

- **Minimum Sistem Gereksinimleri**

Microsoft Windows NT Server 4.0 yüklemek için gerekli minimum sistem gereksinimleri (intel tabanlı bilgisayarlar için) şunlardır:

- 386DX ya da daha yukarı bir prosesor,
- Minimum 90 MB boş hard disk alanı,
- Minimum 16 MB bellek,

Bunların yanı sıra bir disket sürücü, CDROM'dan yükleme yapılacak ise bir CDROM sürücü ve minimum VGA ya da daha yüksek çözünürlükte bir ekran gerekmektedir.

- **File Sisteminin Seçilmesi**

Microsoft Windows NT server yüklemeye başlamadan önce hangi file sistemi seçeceğimizi önceden bilmemiz gereklidir. Windows NT işletim sisteminin desteklediği file sistemler şunlardır.

- File Allocation Table (FAT)
- The Windows NT file system (NTFS)

FAT (File Allocation Table) MS-DOS ve OS/2 işletim sistemlerinin kullandığı file sistemidir. Sistemi MS-DOS modunda kullanabilmek için diskin bir bölümünün FAT file sistem olması gereklidir.

NTFS (Windows NT File Sistem) yalnızca Windows NT tarafından desteklenen bir file sistemdir. Eğer bilgisayar başka bir işletim sistemi altında açılmış ise NTFS disk biçimine ulaşmak olanaksızdır.

FAT file sistemi, her türlü erişime izin verir. Çok geniş bir kullanım alanına sahiptir. FAT file sisteminde user bazında güvenlik sağlanamıyor. NTFS lokal güvenlik sağlayan tek file sistem. Burada Windows NT server kurulması aşamasında NTFS file sistemi seçilecektir.

- **Domain Serverlerin Rolleri**

Bir organizasyon içersinde (örneğin bir fakültede) bir Microsoft Windows NT Server kurulmadan önce o birimdeki network'un konfigürasyon planının çıkarılması önemlidir.

Bir Windows NT Server 3 tip server'dan biri olabilir.

- Primary Domain Controller
- Backup Domain Controller
- Stand Alone Server

- **Primary Domain Controller (PDC)**

Her bir domain için, bir bilgisayar Primary Domain Controller olarak seçilir. Bu PDC master bilgisayar oluyor. Account listeleri, güvenlik işlemleri gibi temel işlerin yürüdüğü bilgisayar. Account bilgilerindeki değişimler Primary Domain Controller da yer alıyor.

- **Backup Domain Controller (BDC)**

Primary Domain Controller (PDC) peryodik olarak her güncellemede bilgileri Backup Domain Controller üzerine yükler. Eğer PDC kapalı ise, ya da arıza varsa işleri BDC yürütür.

- **Stand Alone Server**

PDC ve BDC dışında kalan sunucu makineler ise sadece server olarak adlandırılırlar. Bu sunucular print ya da file ya da diğer uygulamalar için server olarak kullanılabilir. Ancak hiç bir zaman kullanıcı aktiviteleri (account) üzerindeki uygulamalar için kullanılamazlar.

2.2.1. Kurulumu

- Windows NT server aşağıdaki 3 metottan biri ile kurulabilir.
- CD-ROM kullanarak
- Network üzerinden
- Disketten (Bu metodun kullanımı pratik olmadığından artık kullanılmamaktadır.)

2.2.1.1.CD-ROM Kullanarak Kurmak

Bu metot en çok tercih edilen yoldur. Bu metot için; Bir CD-ROM sürücü olması gereklidir. CD-ROM'a ulaşılmadan önce 3 adet Setup disketi kullanılarak boot edilmesi gereklidir. RISC temelli sistemlere Windows NT server yalnızca bu yolla kurulabilir.

2.2.1.2. Network Üzerinden Kurmak

Network boot disketi ile sistem açılır. Bu şekilde açınca bizden user id ve password girmemiz istenir.

Userid: install
password: install, şeklinde girebiliriz.

Net use f: \\netserver\mssoft2 komutu; ntserver isimli makinedeki mssoft2 isimli paylaşılan diski bilgisayarımıza f diski olarak monte eder (bağlantılanır).

Winnt /b /S : \\ntserver\mssoft2\nts40\I386 şeklinde başlatılır.

Setup programı (WINNT.EXE) aşağıdaki adımlardan geçerek uygulanır.

Setup programı WINNT.EXE ile başlatılırken aşağıdaki parametreler kullanılabilir.

/O veya /OX : Sadece boot disketleri yaratılır.

/B : Disket kullanmadan kurma

/X : Bu parametre kullanılırsa 3 setup boot disketi yaratılmaz ve WIN_NTLS geçici dizininin tamamen oluşturulmuş olduğu farz edilir. Bununla birlikte kuruluşu tamamlamak için 3 diskete ihtiyaç vardır.

/S : Bu parametre ile Windows NT kaynak dosyalarının yerinin belirtilmesine olanak sağlar.

/F : Bu parametre ile setup boot disklerine dosyalar kopyalanırken sağlama(verify) işlemi yapılmaz.

/C : Bu parametre ile disk üzerinde boş alan miktarı check (kontrol) edilmez.

2.2.1.3. NT İşletim Sisteminin CD Yardımı ile Kurulması

MS-DOS kurulma disketlerinin yardımı ile disk formatlanarak MS-DOS modunda açılır.

CD-ROM tanıtma disketi ile CD-ROM sisteme tanıtılır. Sistem kapatılıp yeniden açılır. CD-ROM üzerinde I386 dizinine geçilir.

Bu dizinde bulunan WINNT.EXE dosyası yardımı ile Windows NT işletim sisteminin kuruluşu başlatılır.

WINNT /B komutu girilerek CDROM dan Windows NT kuruluşuna başlanır.
Bu komut girildikten sonra karşımıza çıkan ekran;Windows NT Server Setup

Setup needs to know where the the Windows NT files are located. Enter the path where Windows NT files are to be found.

(Setup, Windows NT dosyalarının yerleştirileceği yeri bilmek zorundadır. Windows NT dosyalarının bulunacağı yolu belirtiniz.)

E: \NT\SERVER\I386
Bu durumda Enter tuşuna basarak bir sonraki kuruluş aşamasında karşımıza çıkan ekran şudur:

Windows NT Server Setup
Please wait while setup copies files to your hard disk.
(Setup dosyaları hard diskinize kopyalıyor lütfen bekleyin)

Bu aşamada dosyalar hard disk üzerine temporary olarak WIN_NT.LS dizinine kopyalanıyor. Sonra da doğru kopyalanıp kopyalanmadığı kontrol ediliyor. Kopyalama işlemi bittikten sonra karşımıza alttaki ekran görüntüsü gelecektir.

Windows NT Server Setup
The MS-DOS based portion of setup is complete.
(Setup'ın MS-DOS tabanlı kısmı tamamlanmıştır)

The setup will now restart your computer. After your computer restarts, Windows NT setup will continue.
(Şimdi Setup bilgisayarınızı yeniden açacaktır. Bilgisayar yeniden açıldıktan sonra Setup işlemi devam edecektir.)

If there is a floppy disk in drive A; remove it now
(Eğer A disk sürücüsünde bir disket varsa onu şimdi çıkarınız)

Press Enter to restart your computer and continue Windows NT setup.
(Bilgisayarı yeniden açmak ve Windows NT yükleme işlemine devam etmek için ENTER tuşuna basınız)

2.2.2. Ayarları

Disketi sürücüden çıkarıp Enter tuşuna bastıktan sonra sistem yeniden açılacak ve karşımıza alttaki ekran görüntüsü gelecektir.

Windows NT Server SetupThe setup program for the Microsoft Windows NT operating system version 4.0 prepares Windows NT to run on your computer.

To learn more about Windows NT setup before continuing, Press F1
(Windows NT hakkında daha fazla bilgi edinebilmek için F1 tuşuna basınız)

To set up windows NT, Now press ENTER
(Windows Setup için Enter tuşuna basınız)

To repair a damaged Windows NT version 4.0 installation, Press R.
(Var olan bir hasarlı Windows NT version 4.0 yüklemek için R tuşuna basınız)

To quit setup without installing Windows NT, Press F3.
(Setuptan işletim sistemini yüklemeden çıkmak için F3 e basınız)

Enter tuşuna bastığımızda karşımıza ;
Setup has recognized the following mass storage devices in your computer
(Setup aşağıdaki cihazları bulmuştur).

IDE CD-ROM (ATAPI 1.2)/PCI IDE Controller

Adaptec AHA - 294X/AHA -394X/AIC - 78xx SCSI Controller yazıları ile başlayan ekran görüntüsü gelecektir. Bu ekran görüntüsünü de ENTER tuşu ile geçince karşımıza

Windows NT Server Microsoft Licence Agreement
(Windows NT Server Microsoft Lisans antlaşması) çıkacaktır.

Bu yazıların (isterseniz okuyup) pagedown tuşu ile sonuna kadar gitmeniz gerekmektedir. Son sayfaya geldiğinizde sistem sizden F8 (I Agree) şeklinde onaylamanızı bekleyecektir.

Bundan sonraki aşamada karşımıza gelen ekran ise;
Setup has determined that your computer contains the following hardware and software components.
(Setup bilgisayarınızın aşağıdaki donanım ve yazılım bileşenlerini kullanır)

Computer Standart PC
Display Autodetect
Keyboard XT, AT, or Enhenced Keyboard
Keyboard Layout US
Pointing Device Microsoft Serial Mouse

Bu seçeneklerden sadece Keyboard Layout (Kullandığımız klavye türü) seçeneğini Turkish Q olarak değiştiriyoruz.

No changes : The above list matches with my computer
(Değişiklik yok: Yukardaki liste benim bilgisayarıma uymaktadır) seçeneğinin üstüne gelip ENTER tuşuna basıyoruz.

Daha sonraki aşamada karşımıza gelen ekrandan ;
The list below shows existing partitions and spaces avaliable for creating new partitions.
(Aşağıdaki listeden, var olan disklerden NT yüklemek istediğinizi seçiniz)

Use the up and down arrows to choose the item
(Yukarı ve aşağı ok tuşlarını kullanınız)

(Bundan sonraki 3 kuruluş aşaması ise)

Gathering Information about your computer
(Bilgisayarınız hakkında bilgilerin elde edilmesi)

Installing Windows NT networking
(Network ile ilgili bilgilerin eklenmesi)

Finishing setup
(Setup işleminin bitirilmesi)

Bu adımları sıra ile geçip, Setup Wizard yardımı ile kurulum ve ayarlama işlemlerini tamamlıyoruz.

2.2.3. Yedek Alma

Aşağıda **ntbackup** komutunu nasıl kullanabileceğinizi gösteren dört örnek verilmektedir.

2.2.3.1. Normal Bir Yedekleme Yapma

Aşağıdaki örnek, \\iggy-multi\c$ uzak paylaşımını "İsim 1" adlı bir normal yedekleme ile yedekler. Bu örnek, Yedekleme ortam havuzundan bir teyp alır ve teybi "Komut Satırı Yedekleme 1" olarak adlandırır. Yedekleme işinin açıklaması "Komut Satırı İşlevselliği" olacaktır. Yedekleme işi bitince yedekleme doğrulanır, erişim sahip/yönetici ile sınırlı olmaz, günlüğe alma düzeyi yalnızca özet'e ayarlanır, Uzak Depolama Birimi verileri yedeklenmez ve donanım sıkıştırması etkinleştirilir.

ntbackup backup \\iggy-multi\c$ /m normal /j "İsim 1" /p "Backup" /n "Komut Satırı Yedekleme 1" /d "Komut Satırı İşlevselliği" /v:yes /r:no /l:s /rs:no /hc:on

2.2.3.2. Kopya Yedeklemesi Yapma

Aşağıdaki örnek, D:\ yerel sürücüsünü "İsim 2" adlı kopya yedekleme ile yedekler. Yedeklenen dosya ve klasörler "Komut Satırı Yedekleme 1" adlı teybe eklenir. Diğer tüm seçenekler Yedekleme programında belirtilen ayarları varsayılan ayarlar olarak alacaktır.

ntbackup backup d:\ /j "İşim 2" /a /t "Komut Satırı Yedekleme 1" /m copy

2.2.3.3. Belirtilen Yedekleme Türünü Kullanarak Yedekleme Yapma

Aşağıdaki örnek, Yedekleme programında belirtilen yedekleme türünü kullanarak bir yedekleme gerçekleştirir. Yedeklenecek dosyaları seçmek için, C:\Program Files\Windows NT\ntbackup\data\ dizininde bulunan Commandline.bks adlı yedekleme seçimi dosyasını kullanır. Yedekleme işi "İsim 3" olarak adlandırılacak ve "Komut Satırı Yedekleme 1" adlı teybi "Komut Satırı Yedekleme 2" ile değiştirecektir.

Ntbackupbackup "@C:\Program Files\Windows NT\ntbackup\data\commandline.bks" /j "İsim 3" /t "Komut Satırı Yedekleme 1" /n "Komut Satırı Yedekleme 2"

Bir dosya için komut satırından yedekleme yapmak için;

Aşağıdaki örnekler komut satırından bir dosyaya yedeklemenin nasıl gerçekleştirileceğini göstermektedir. Üç örnek, yedekleme türü, doğrulama ayarı, oturum açma düzeyi, donanım sıkıştırması ve diğer kısıtlamalar için yedekleme programının varsayılan değerlerini kullanmaktadır. İlk örnek \\iggy-multi\d$ dosyasının D:\Backup.bkf dosyasına nasıl yedekleneceğini, ikinci örnek ise aynı yedeklemenin aynı dosyaya nasıl ekleneceğini göstermektedir. Üçüncü örnek aynı yedekleme ile dosyanın üzerine nasıl

yazılacağını göstermektedir. Her üç örnekte, sürücü harfi yerine tam bir UNC adı kullanılabilir (başka bir deyişle kullanıcı, d:\backup.bkf yerine yedekleme hedefi olarak \\iggy-multi\d$\backup.bkf dosyasını belirtebilir).

ntbackup backup \\iggy-multi\d$ /j "Komut Satırı Yedekleme 4" /f "D:\backup.bkf"

ntbackup backup \\iggy-multi\d$ /j "Komut Satırı Yedekleme 5" /f "D:\backup.bkf" /a

ntbackup backup \\iggy-multi\d$ /j "Komut Satırı Yedekleme 6" /f "D:\backup.bkf"

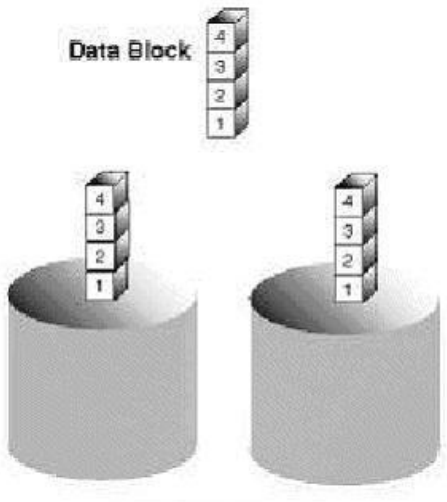
2.3. Aynalama (Mirroring)-Şeritleme (Striping)

RAID, "Redundant Array of Independent Disks" (bağımsız disklerin artıklı dizisi) anlamına geliyor. Kelimelerinin baş harflerinden oluşuyor. RAID dizesinde, iki veya daha fazla diski tek üniteye bağlayarak, disklerin tek başlarına yapamadığı şeyleri yapmanıza olanak sağlar. Uyguladığınız RAID konfigürasyonunu çeşidine göre, RAID dizesi ile daha fazla performans, daha fazla veri güvenliği veya her ikisini de elde edebileceksiniz. RAID'in esas amacı, bir dize içerisinde bulunan ana hard diskin çeşitli yöntemlerle yedeği alınarak, diğer hard disklerin bozuk olduğu zaman, sistemin çalışmama süresini en aza indirgemektir. Burada söylediklerimiz, birazdan anlatacağımız kavramlar için temel oluşturuyor. RAID için farklı konfigürasyon seçenekleri bulunuyor. Ancak biz burada RAID 0 (Şeritleme-Striping) ve RAID 1 (Aynalama-Mirroring)' den bahsedeceğiz.

RAID 0 (Striping): RAID 0 konfigürasyonunda, RAID kontrolcüsüne en az iki disk bağlayarak bir dizi oluşturuyorsunuz. Disk dizisi kullanırken, aynı türden bağlanmış diskler üzerine veriler yazılırken ardışık bloklara bölünerek diskler üzerine dağıtılarak yazdırılıyor. Bu ciddi bir performans artışı sağlıyor desek yeridir. Bunu daha anlaşılabilir bir şekilde anlatalım. Elimizde yazılması gereken 8 kelimelik bir cümle var. Dört elimizin olduğunu varsayalım. Bir elin bir kelimeyi yazması bir dakika aldığını varsayarsak; kelime sayısını el sayısına göre paylaştırıp yazdırırsak, tek elin 8 dakikada yaptığı işi, dört elimizle 2 dakikada yapmış olacağız.

RAID 1 (Mirroring): Evet diğer RAID sistemimiz ise RAID 1, diğer adıyla disk "aynalama". "Aynalama" teriminden tahmin edeceğiniz üzere şu anlam ortaya çıkıyor : 2 veya daha fazla diskiniz var ve bu disklerin birisindeki bilgiler, diğerine eş zamanlı olarak kayıt ediliyor. %100 veri güvenliği amaç edinilmiş. Aniden hard diskimizdeki bilgiler yok olduğunu düşünürsek bilgilerin aynalandığı diskten dosyaları tekrar yeni ana diskinize kopyalayarak olayı çözümleyebiliyorsunuz.

RAID 1 (Mirroring) ile bilgi blokları iki diske birden yazılırlar. Burada en az iki disk kullanılabilir. Böylece birbirinin kopyası olan diskler oluşur. Kapasite tek bir disk kapasitesidir. Farklı disk kapasitedeki disklerde en küçük kapasiteli disk referans alınacaktır. Herhangi bir disk arızası durumunda ikinci disk görevi üstlenerek sistemin çalışmasını sağlıyor. Böylece iş akışı durmamış oluyor. Arızalı disk sistem çalışırken çıkartılıp yerine sağlam disk takılır, sistem konfigürasyonu eski hâline getirilir. Disk okuma hızı artarken yazma hızı yavaşlamaktadır. Disk güvenliğinin en üst seviyede olduğu durumlarda kullanılır.



Şekil 2.1: RAID 1 (Mirroring-Aynalama) Çalışma Sistemi

2.3.1. Destekleyen Ana Kartlar

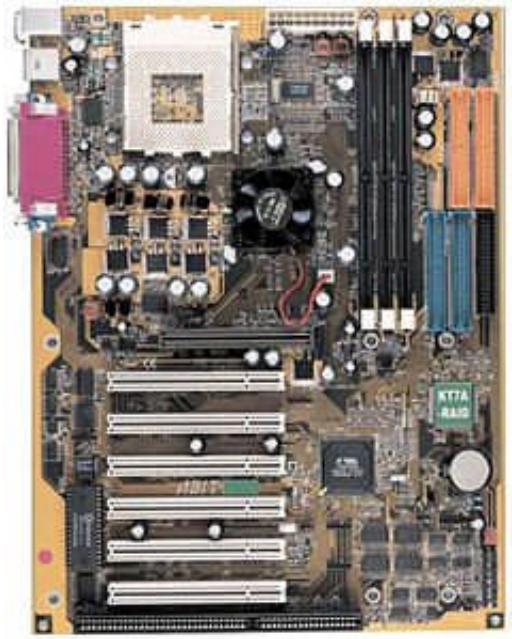
Esas RAID'in SCSI RAID olduğunu söyleyebiliriz. SCSI RAID ile performansın yanı sıra, güvenliği maksimum dereceye ulaştıran çok kompleks yapıda olan bir sistemdir. Fakat, IDE Disk'lerin fiyatlarının oldukça ucuzlaması, çok pahalı olan SCSI RAID kartlarındaki bazı kompleks yapıdaki sistemlerin kısıtlanması ile, IDE RAID kartları uygun bir fiyatla ortaya çıkmıştır, hatta, yeni ana kartların bir kısmında, IDE RAID kontrolcüsü entegre olarak piyasaya sürülmüştür. Sonuç olarak, karşımızda performans ve güvenlik konusunda yarar sağlayan IDE RAID kontrol kartlarını ve IDE RAID'li ana kartlara ulaşmamız oldukça kolaydır.

Ülkemizde, Abit'in HTP370 RAID kontrolcüsü kartından başka PCI IDE RAID kontrol kartı pek bulunamamaktadır. Kendisi üzerinde RAID kontrolcüsü taşıyan ana kartlar ise piyasada pek fazla değil. Ama Abit'in RAID kontrolcüsü taşıyan kartları pek fazladır. GigaByte'ın ve Asus'un henüz RAID kontrolcüsü taşıyan kartları yeni yeni piyasaya girdi.

Aşağıda aynalama ve şeritleme yöntemlerini destekleyen, ABIT KT7A-RAID ana kart ve bileşenleri kullanılarak yedekleme yapılmıştır.

Esas RADI'in SCSI RAID olduğunu kabul edebiliriz. SCSI RAID ile performansın yanı sıra güvenliği maksimum dereceye ulaştıran çok kompleks yapıda olan sistemlerin olduğunu söyleyebiliriz. Fakat, IDE Disk'lerin fiyatlarının oldukça ucuzlaması, "çok pahalı" olan SCSI RAID kartlarındaki bazı kompleks yapıdaki sistemlerin kısıtlanması ile, IDE RAID kartlarının uygun bir fiyatla ortaya çıktığını, hatta ve hatta, yeni ana kartların bir kısmında, IDE RAID kontrolcüsünün entegre olarak üretilmektedir. Sonuç olarak,

karşımızda performans ve güvenlik konusunda yarar sağlayan IDE RAID kontrol kartlarını ve IDE RAID'li ana kartlara ulaşmamız oldukça kolaydır.



- KT133A Chipset
- 100/133 MHz FSB ile çalışan tüm Duron/T-Bird işlemcilere destek
- 6 PCI / 1 ISA / 1 AGP 4X
- VIA 686B köprüsü ile ATA/100 desteği
- HPT370 RAID kontrolcüsü ile ATA/100 **RAID desteği**
- Topkam 4 IDE Portu
- SoftMENU-III
- 3 DIMM slotu ile max. 1,5 GB SDRAM desteği.
- 3 Kademeli Güç Sistemi
- 4 USB Portu

Şekil 2.2: ABIT KT7A-RAID Destekli Anakart

2.3.2. Bağlantısı

Öncelikle kafanızda hangi RAID sistemini kuracağımızı belirlemeliyiz. Eğer şeritleme (RAID 0) yapacaksanız, disklerin kapasiteleri ve modelleri aynı olacak diye bir kaide yoktur. Kapasiteleri ve modelleri farklı olabilir. Fakat bizim önerimiz, birbirine yakın özelliklerde, aynı kapasitedeki disklerden kullanmanız olacaktır şeritleme yöntemi için aynı model ve kapasite tabii ki tercih sebebidir. Örneğin, sisteminizde 7200 devir dönen ve 2 MB tampon belleğe sahip bir disk var. Şeritleme yapacaksanız, bunun yanına aynı kapasitede 5400 devir bir disk takmanız mantıklı değildir. Yine 7200 devir, 2 MB tampon belleğe sahip, tercihen aynı kapasiteye sahip bir disk takmanız yararınıza olacaktır. Şeritleme yaparken, kapasiteden önce, diskin devir dönüş hızı değerleri ile tampon belleği kapasitelerinin aynı olmasına özen gösteriniz. Mesela, 7200 rpm'lik bir disk'in yanına aynı kapasitede 5400 rpm disk yakıp şeritleme yaptığınızda, performans hiç de istediğiniz gibi olmayabilir. Aynalama (RAID 1) modunda ise, kaynak olacak olan disk'in boyutu, yedekleme işlemi yapacak olan disk'ten daha küçük olmalıdır. Yani, yedekleme işlemci yapacak olan ikinci disk'in boyutu, birinci disk'ten daha büyük olmalıdır. Yeni bir sistem kuracaksanız ve aynalama yapmaya niyetli iseniz, aynı model ve kapasiteye sahip iki disk almanız gerekmektedir.

Diskleri temin ettikten sonra, ana kartınızın üzerinde IDE RAID kontrolcüsü entegre olarak gelmiş ise, bir şey yapmanıza gerek yoktur. Eğer ana kartınızda böyle bir kontrolcü yok ise, PCI yuvasına takılan IDE RAID kontrolcülerinden almalısınız.

- **İşlemler**

Yukarıdaki gibi uyumlu bir sistem oluşturduktan sonra RAID ana karta entegre olarak HPT370 RAID kontrolcüsünü 1.03b BIOS'u ve sürücüleri kullanacağız. İşlemci olarak ise Duron 600 işlemciyi kullandık. Şimdi şeritleme (RAID 0) sistemini kuralım, 2 tane 7200 devir ve 2 MB tampon belleğe sahip 20 GB'lık Quantum Fireball AS disklerimizi şeritleme metodu ile sisteme bağlıyoruz.

Eğer 2 disk ile şeritleme yapacaksanız, iki diskinizi de RAID kontrolcüsünün farklı portlarına Master olarak bağlayacaksınız. Biliyorsunuz, ATA/66 standardı ile birlikte kabloların artık disklere takılacak yönü standartlaştı. Disk'lerin üzerinde Jumper'lar ile artık oynamıyoruz. Bir kerelik olsun, Jumper'ımızı "Cable Select" konumuna getiriyoruz. Böylece, diski bağladığımız kablonun ucu, hard disk'in bağlı olduğu kanalda efendi veya köle olmasını belirliyor. ATA/100 kablomuzun (ATA/66 kablosu ile aynı) mavi ucu, kontrolcünün IDE portlarına takılacak. Eğer diskin efendi (master) olması isteniyorsa, kablonun siyah ucuna; köle (slave) olması isteniyorsa kablonun gri ucuna diski takmak gerekiyor.

Bu noktalara dikkat ettikten sonra, eğer iki disk ile şeritleme yapacaksanız, iki disk'i de farklı kanallar Master olarak bağlayacaksınız. Eğer iki disk ile aynalama yapacaksanız, bu disklerin de ayrı kanallara master olarak bağlanması gerekmektedir.

Hangi yapılar için, disklerin bağlantı durumunun nasıl olması gerektiğini öğrendik. Şimdi ise, kontrol kartlarımızın BIOS'una girerek bu işlemlerin yazılımını yüklememiz gerekmektedir.

2.3.3. Yazılımını Yükleme

Sürücüleri genelde işletim sistemini kurduktan sonra güncelleyebiliriz ama BIOS ayarlarını önce yapmamız gerekmektedir. Her RAID kontrolcüsünün bir BIOS'u var, Tıpkı ana kartın BIOS'u gibi; BIOS'a girip RAID yapılandırmalarını yapıyoruz ve birkaç ayarlama yapıyoruz. Tıpkı ana kartların nasıl BIOS güncellemesi çıkıyor ise, IDE RAID kontrolcülerinin de BIOS güncellemeleri çıkıyor ve var olan hatalar düzeltiliyor. Bazen bu hatalar ciddi düzeyde olabiliyor. Mesela, eski BIOS'da yer alan bir hata, şeritlediğiniz diskleri işlevsizleştirebiliyordu. Bundan dolayı, en son BIOS sürümünü yüklemek gerekiyor. Eğer ana kartınızın üzerinde entegre bir RAID kartı var ise, ana kartınızın en son BIOS'unu yüklemeniz yeterli. Bu sayede, RAID kontrolcüsünün BIOS'u da güncellenmiş olacaktır. PCI RAID kontrolcüsü kullanıyor iseniz, hangi marka o kartı üretmiş ise onun internet sitesine gitmek gerekmektedir.

Örneğin; HighPoint'in HTP370 RAID kontrolcüsünü taşıyan kartlar için generic BIOS sürümleri mevcut: http://www.highpoint-tech.com/370drivers.htm. Promise, hem RAID

kontrolcüsü üreten, hem de bu kontrolcüleri taşıyan kartları üreten bir firma. Bu kartlardan sahipseniz, http://support.promise.com/Support/ adresine gidiyorsunuz.

Şekil 2.3: HighPoint HTP370 RAID Generic BIOS

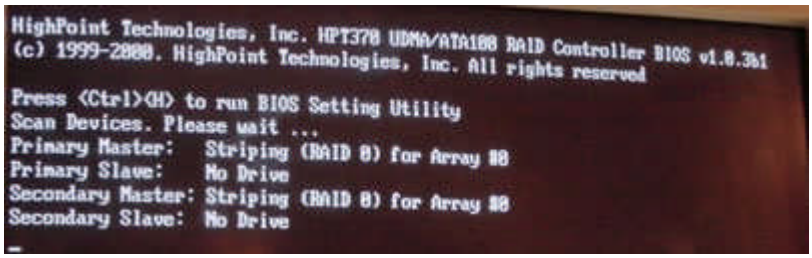
PCI RAID kartlarının BIOS'u güncelleme işlemi pek de zor değildir. Bir sistem disketiyle, bilgisayarı açınız. Komut satırına, güncelleme programının ismini yazınız. Seçenekler arasından "Flash BIOS" ifadesini seçip dosya ismini giriniz. Dikkat etmeniz gereken, her üreticinin farklı bir güncelleme sistemi içermesidir. Dolayısıyla, çektiğiniz dosya arasında olan readme (beni oku) dosyalarında söylenenleri adım adım yapmak, kartınızı bozmamanız açısından mantıklı olacaktır.

Daha sonra, kartın sürücülerini yüklemeniz gerekir. Ses kartının sürücüsünü nasıl yüklüyorsanız, RAID kontrolcüsünün sürücülerini de yüklemeniz gerekmektedir. İlgili adresler yukarıda verilmiştir. İlerde bize lazım olacaktır. Eğer, Windows 2000 veya NT 4.0 gibi bir işletim sistemi kuracaksanız, bu sürücüler önceden lazımdır. Yok eğer Win98 & ME kuracağım derseniz ister önce kurun ister sonra, fark etmeyecektir.

2.3.3.1. Test Sistemi Destekleyen Ana Kartlar

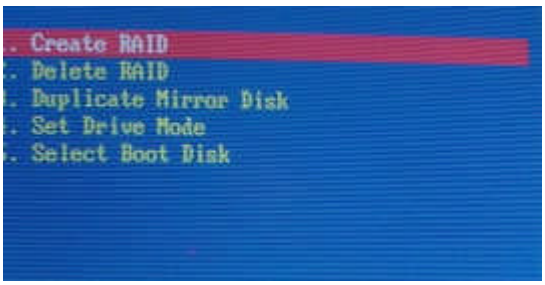
- Abit KT7A-RAID Ana kart
- Duron 600 MHz işlemci
- 2 x 20 GB Quantum FireBall AS ATA/100 Hard Disk
- 128 MB Kingston PC133 SDRAM
- Leadtek Geforce2 MX
- Samsung SD-608 (8X) DVD-ROM

Bilgisayarınızı açtıktan sonra, BIOS Post Ekranından sonra, IDE RAID kontrol kartının BIOS ekranı görünür ve burada kartın BIOS'una girebilmek için Ctrl + H tuş kombinasyonu kullanılır.



Şekil 2.4: RAID BIOS' a Giriş

Kartın BIOS ekranı geldiğinde, pek de yabancı gözükmeyen bir ekran ile karşılaşırsınız.

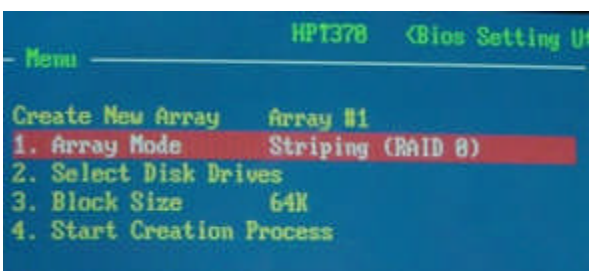


Şekil 2.5: RAID BIOS' da Create Ayarı

(Ana menüdeki Create RAID bölümü ile işiniz olacaktır.)

BIOS ekranında 5 tane seçenek karşınıza gelir. Birinci seçenek ile RAID dizimizi yaratabiliriz, ikinci ayar ile daha önceden var olan RAID dizimizi silebiliriz, kontrolcü üzerine bağlı olan IDE aygıtların çalışma modunu seçebilirsiniz (Mesela diskiniz ATA/100 standardında ise, burada ayar UDMA 5 olarak belirir; bu ayarı değiştirebilirsiniz). Ve son olarak, eğer kontrolcünün üzerine birden fazla disk takılı ise, bunlardan hangisinin birincil disk olarak kullanılacağını belirlersiniz. Bizim burada yoğunlaşacağımız seçenek birincisidir.

Birinci seçenek olan, Create RAID (RAID Yarat) seçeneğine girdiğimizde, birkaç oynamamız gereken ayar çıkar. Bunlardan birincisi: Array Mode. Yani hangi RAID sistemini kuracağımızı buradan belirleriz.



Şekil 2.6: RAID BIOS' da Array Mode Ayarı

RAID dizimizi hangi mod ile yaratacağımızı buradan belirleriz.

Örneğin iki diskimizi şeritleme yapacağız. İlk başta birinci seçenek olan Array Mode seçeneğinin üzerine gelerek Enter'a basıyoruz ve gelen menüden RAID 0 (Striping) seçeneğini seçeriz. Burada, hangi RAID sistemini kullanacağımızı belirtiriz.

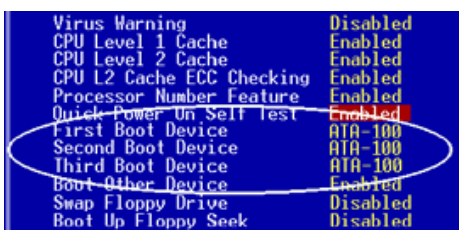
Bir sonraki aşamada, Select Disk Drives seçeneğine geliriz. Bu seçenekle, yukarıda belirttiğimiz şeritleme metodunda hangi disklerin kullanılacağını seçeriz. Bu seçeneğin üzerine gelip Enter'a basar ve aşağıda belirecek çubuk yardımı ile belirlediğimiz RAID sisteminde kullanılacak diskleri belirleriz.

Üçüncü seçenekte ise Block Size yani cluster boyutunu belirleriz. Bu rakamın 64 KB olması uygun olacaktır. Block Size, hard diskinize ait bir mantıksal birimdir. Cluster'lar bilgilerin saklandığı en küçük birimdir. Mesela, Cluster boyutunu siz 64 KB olarak belirlerseniz, diskinize kopyalayacağınız en küçük dosya boyutu 64 KB olarak kalacaktır. Mesela, 1 KB'lik dosya kopyaladıysanız, bu diskte 64 KB yer kaplayacaktır. Cluster boyutu ne kadar büyük ise performans o kadar iyi demektir.

Örnek vererek anlatalım; Siz 100 parçalık bir dokümanın içinden mi bir dosyayı daha kolay bulursunuz, yoksa 20 parçalık bir dokümanın içinden mi? 20 parçalık dokümanın içinde, aradığınız dosyayı bulmak daha kolay olur. Cluster boyutunu ne kadar küçültürseniz, Sabit Diskiniz istediğiniz dosyayı bulmak için biraz daha fazla çaba harcayacaktır. Bu da performans düşüşü demek olur. Ancak, sıralı okuma ve yazmada normale oranla oldukça hızlı çalışabilirsiniz Bu işin dezavantajı ise; Eğer küçük dosyalar ile çok fazla uğraşıyorsanız, bu sizin için kapasiteden kaybetmeniz anlamına gelir. Video Editing gibi işlemlerle uğraşanlar için bu miktarın 32 veya 64 KB olması tavsiyemizdir.

En son seçenek ise, "Start Creation Process"tir. Bu seçenek ile seçtiğimiz ayarlara göre RAID dizimiz oluşturulur. Daha sonra BIOS'umuzdan çıkarak bilgisayarı yeniden başlatırız.

Diskimizi şimdi biçimlendirmemiz gerekmektedir. 2 adet 20 GB'lık diskimizi şeritledikten, RAID ayarlarını yaptıktan ve RAID dizemizi yarattıktan sonra. FDISK ile diskimizi biçimlendirmeye çalıştığımızda, tek parça 40 GB'lık dev bir parça göreceksiniz. Sonra "format c:" komutunu verdiğinizde ise, sabit diskiniz formatlanmaya başlanacak. Bu arada, BIOS'dan birincil boot aygıtı olarak ATA100 RAID' i seçmeyi unutmayınız. Eğer PCI RAID kontrol kartına sahipseniz, birincil boot aygıtı olarak SCSI'yi seçin.



Şekil 2.7: RAID BIOS' da Array Mode Alt Ayarları

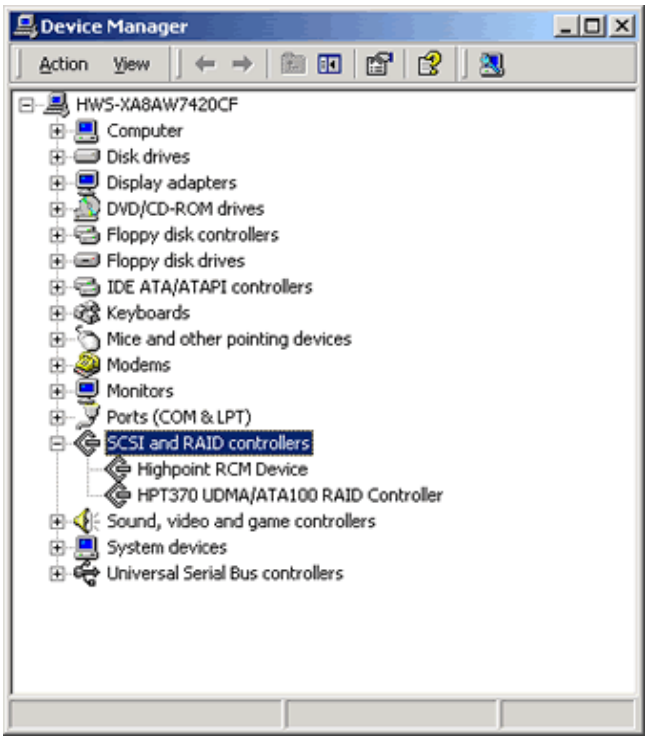
BIOS'umuzda aynalama (RAID 1 = Mirroring) yapacak arkadaşlara has birkaç özellik bulunmaktadır. Bu ayarlardan birincisi, ana menüde olan "Duplicate Mirror Disks" ayarıdır. Bu ayar ile var olan bir disk'in, hiçbir şekilde biçimlendirilmeden başka bir diske yedeğinin alınmasını sağlar ve bir "aynalama" sistemi kurulur. Bu menüye girdiğiniz zaman karşınıza, üç seçenek gelecektir. Select Source Disk - Selecet Target Disk - Start Duplication.

Birinci seçenek ile kopyalanmasını istediğiniz kaynak disk'i seçiniz. İkinci seçenek ile, bu dosyaların kopyalanacağı, yani "ayna" olacak diski seçiniz. Üçüncü seçenek ile ise bu kopyalama işlemlerini başlatıyorsunuz. Bu işlem yaklaşık 30 dakika kadar sürecektir. Daha sonra bu menüden çıkıp işlemlerinize devam edebilirsiniz. Sizden şöyle bir soru gelebilir: Ben sıfırdan bir RAID 1 (aynalama) sistemi kurmak istemiyorum. 15 GB bilgim var ve ben bu bilgileri yedekleyemem. Eğer aynalama sistemi kurarken disk'ten bilgiler silinecekse, bu işi hiç yapmayalım. Bilgilerimize zarar vermeden, ikinci bir disk'i, ana diskimin aynası olarak nasıl konfigüre edebilirim". İşte bunu "Duplicate Mirror Disks" menüsünden yapacaksınız.

Bu arada, "Create Array" menüsünden, "Array Mode" yani hangi RAID dizesi oluşturulacağının sorulduğu menüden, Span (JBOD) seçeneği dikkatinizi çekecektir ve bunun ne olduğunu soracaksınız. "Span "modu ile, belirlediğiniz disklerden bir havuz oluşacak. Yani sistemde takılı olan iki tane 20 GB'lık diski "Span" yap dediğinizde, tıpkı RAID 0 (şeritleme) metodunda olduğu gibi diskinizi 40 GB göreceksiniz. Burada "Span" modu, herhangi bir performans ya da güvenlik bakımından getirdiği bir özelliği olmayan, sadece belirlediğiniz disklerden bir "havuz" oluşturan bir sistemdir.

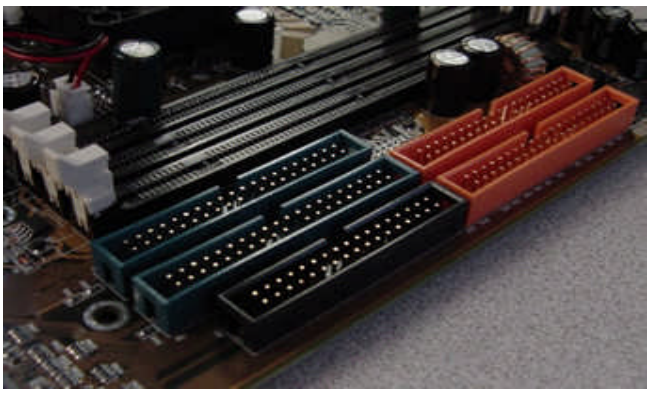
Bu adımları takip ettiğiniz takdirde bir sorun olmaz. Windows 2000 veya NT 4.0 işletim sistemlerini kurarken bir sorun çıkabilir. NT tabanlı işletim sistemleri (NT 4.0 ve Win2K) üçüncü parti IDE kontrolcüleri üzerine takılı olan disklerden kurulum yapamaz. Bunun için, bu iki işletim sistemini de kurarken, alt tarafta şöyle bir mesaj görünür : "3. parti SCSI veya IDE kontrolcüleri üzerindeki disklerden kurulum yaparak F6 tuşuna basınız." Kurulumun başında F6 tuşuna basınız ve kurulumun ilerleyen bölümlerinde sizden IDE veya SCSI kontrol kartının disketini isteyecektir. Uygun olan disk ve disket sürücülerini seçerek işlemi tamamlayınız.

Şimdi yeni sürücülerin kurulması gerekmektedir. Windows 9x & ME kurarken bu sürücülere ihtiyaç yoktur. İşletim sisteminin kurulumu bittikten sonra, Bilgisayarım - Denetim Masası - Sistem Yöneticisi - Aygıt Yöneticisi bölümünden, bilinmeyen aygıtlar bölümüne baktığınızda, Mass Storage Controller adlı bir aygıt göreceksiniz. Bu aygıt'ın üzerine gelip, özelliklerine gidip, "Sürücüleri Güncelle" butonuna tıklayarak, internetten indirdiğiniz yeni sürücülerin yerini gösterdiğinizde ve aygıt yöneticisine baktığınızda, aşağıdaki resim gibi bir görüntü elde edersiniz. Bu şekilde sürücü kurulumu bitmiş olur.



Şekil 2.8: RAID kontrol kartı sürücü yükleme ayarları

Aynalama (Mirroring) sistemi ile elimize gerçekten çok sağlam bir güvenlik sistemi geçmiş olur. Disk bozulma kaygısı olmadan işlemlere devam edebilirsiniz. Ama bu güvenlik için bir diskinizi feda etmiş olursunuz. Çoğu kişi sırf bu konu yüzünden aynalama metodu yerine, performans için şeritleme metodunu uygulayabilir. Şimdi 2 disk şeritlendiğinde; performans kazancının ne olacağı düşünülebilir. Bu iş için 2 x 20 GB Quantum Fireball AS 7200 rpm ATA/100 disk alıp ve Abit KT7A-RAID üzerine bu diskleri Striping (şeritleme) metodu ile ayarlayınız.



Şekil 2.9: Abit KT7A Entegre RAID kontrol kartı Yuvası

Entegre RAID kontrolcüsüne sahip kartlarda fazladan 2 IDE portu bulunur.

Cluster boyutu, yukarıda tavsiye edildiği gibi 64 KB olarak belirlenmiştir. Dosya sistemi olarak FAT32 kullanılmıştır ve Windows 2000 Professionel İşletim sistemi yüklenilmiştir. Daha önce aynı sistemde, yine HPT 370 RAID kontrolcüsüe takılı olan tek Quantum Fireball AS diski, aynı şartlarda test edilmiştir. Daha sonra şeritleme yapılan sistem ile sonuçlar karşılaştırılmıştır.

İlk başta performans sonuçlarına bakılarak yorum yapılabilir:

Öncelikle, sistemin genel performansını artırmak için şeritleme yöntemi çok mantıklıdır. Özellikle, görüntü ve resim işleme gibi Sabit Disk'inizi oldukça kasan uygulamalarda farkı ciddi olarak hissetmeniz mümkündür. Görüntü işlemeyle uğraşan bir çok kişi, IDE Sabit Disk'i üzerinde büyük video'ları işlerken sorun yaşamaktan şikâyet etmektedir. İki tane 7200 devir, 2 MB tampon belleğe sahip ve ATA/100 özelliğinde disk alıp bunlar şeritlendiğinde, bu sorunların altından kalkılabileceğini bilmek gerekir. En azından darboğaz olan disk hızını en aza indirebilmek mümkündür.

Hızı önemsemeyen ama verilerini güvene almak isteyen kullanıcılar için ise RAID 1 (Mirroring - Aynalama) konfigürasyonu oldukça mantıklı olacaktır. Bu sayede, veri kaybetme korkusu olmadan işlere devam etmek oldukça rahatlık verici bir olaydır. Siz hiçbir şey yapmadan, diğer taraftan bilgilerinizin yedeklerinin alınması ve birinci diske bir şey olduğunda, aynalama yaptığınız disk ile çalışmalarınıza devam etmek oldukça önemlidir.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ 2 tane hard diski bilgisayarın kasasına bağlayınız.	➢ Disklerin birbirine uyumlu olmasına dikkat edebilirsiniz. Devir hızları ve kapasiteleri gibi.
➢ Jumper'leri "Cable Select" konumuna getiriniz.	➢ ATA66 standartlarında kablo uçlarına dikkat etmeyebilirsiniz.
➢ Şeritleme yapmak için disklerin iki ucunu da farklı kanallara master olarak bağlayınız.	➢ Diski master olarak tanıtmak için kablonun siyah ucuna takabilirsiniz.
➢ Ctrl + H tuşlarına basarak kartın BIOS' una giriniz.	➢ Her RAID kartının farklı BIOS'u olduğunu unutmayınız.
➢ Create RAID (RAID Yarat) seçeneğine giriniz.	➢ Enter tuşuyla ilerleyebilirsiniz.
➢ Array Mode seçeneğinin üzerine gelerek Enter'a basınız.	➢ Bu ayarda ayrıca aynalama ve diğer yöntemleri de seçebilirsiniz.
➢ Gelen menüden RAID 0 (Striping) seçeneğini seçiniz.	
➢ Select Disk Drives seçeneğine gelerek hangi diskleri kulanacağınızı belirleyiniz.	➢ 1.diskte işlem yapılacağını 2. diskte ise aynısının kopyalanacağını unutmayınız.
➢ Block Size cluster boyutunu 64 KB olarak belirleyiniz.	➢ Boyut ne kadar büyük olursa verim o kadar hızlı olacaktır.
➢ Start Creation Process" seçeneğinde enter' e basarak RAID dizesini oluşturunuz.	➢ Artık diskler yedekleme işlemi için hazırlanmış olacaktır.
➢ BIOS' tan 1. aygıt olarak RAID' i seçiniz.	➢ Bilgisayar açılmaya başladığında 1. aygıtı görecektir.
➢ BIOS'tan çıkarak bilgisayarı yeniden başlatınız.	➢ Herhangi bir eksik ayar yapılmadığından emin olunuz.
➢ "format c:" komutunu kullanarak diskleri tek bir diskmiş gibi formatlayınız.	➢ Bu işlemde iki disk tek bir diskmiş gibi görünür örneğin 2 tane 20GB'lik hard disk 40 GB görünecektir.
➢ Şimdi ise 1. diskte yaptığınız her bir işlem ve değişiklik ikinci diskte de olacak ve her iki diske de yedeği alınmış olacaktır.	➢ Siz herhangi bir kopyalama ve değişiklik yaptığınızda her iki diske de kopyalanacaktır.

ÖLÇME VE DEĞERLENDİRME

OBEJKTİF TEST (ÖLÇME SORULARI)

Aşağıdaki soruları dikkatlice okuyarak uygun şıkkı işaretleyiniz.

1. Aşağıdakilerden hangisi yedekleme için kullanılan programlardan biri değildir?
A) Arj B) Word C) Zip D) Backup

2. Okuma hızını artırmak ve parçalanan dosyaları birleştirmek için yapılan işleme ne denir?
A) Defrag B) Scan disk C) Format D) Setup

3. Bozuk programların bir kısmının kurtarılabildiği işlem hangisidir?
A) Format B) Kopyalama C) Kesme D) Scan disk

4. Aşağıdakilerden hangisi bir yedekleme donanımı değildir ?
A) Hard disk B) CD-ROM C) Flash disk D) Disket

5. Periyodik zamanlarda bilgilerin disketlere yedek alınmasına ne denir.?
A) Yedekleme B) Filtreleme C) Biçimlendirme D) Kaydetme

6. Genelde disketlerdeki bozulmaları önlemek için yapılan işleme ne denir?
A) Silme B) Kaydetme C) Filtreleme D)Formatlama

7. Aşağıdakilerden hangisi veri kayıplarında etkili değildir ?
A) Donanım B) Yazılım C) İnsan D) Zaman

8. Aşağıdakilerden hangisi yedekleme çeşidi değildir ?
A)Tam yedek B) Toplam yedeği C) Adımlı yedek D) Fark Yedeği

9. Diğer yöntemler uygulanmadan önce, en az bir kez yapılan yedekleme çeşidi hangisidir?
A) Fark Yedeği B) Tam Yedek C) Adımlı yedek D)Hiçbiri

10. Sadece son yedekten bu yana yedeklenmemiş olduğu tespit edilen Archive (arşiv) dosyaları hangi yedeklemede yapılır?
A) Adımlı Yedek B) Tam yedek
C) Fark Yedeği D) Hepsi

11. Aşağıdakilerden hangisi Server NT Backup parametrelerinden biri eğildir ?
A) systemstate B) @DosyaAdı.bks
C) /Ö D) /J

12. Yedekleme türünü hangi parametreyle belirleriz?
A) /A B) /V C) /M D) /R

13. MS-DOS ve OS/2 işletim sistemlerinin kullandığı file (Dosya) sistemi hangisidir?
A) NTFS B) FAT C) COM D) LPT

14. Eğer PDC kapalı ise, ya da arıza varsa işleri hangi Kontrolcü yürütür?
A) BDC B) PDC C) SAS D) NT

15. Server NT hangi metotla kurulamaz?
A) CD-ROM ile B) Yazıcı ile
C) Network ile D) Disket ile

16. Setup programı WINNT.EXE ile başlatılırken aşağıdaki parametrelerden hangisi kullanılmaz?
A) /O B) /B C) /X D) Hepsi

17. Disket kullanmadan Server NT kurmak için hangi parametre kullanılır?
A) /B B) /S C) /F D) /C

18. Server NT' yi CD-ROM kullanarak kurarken hangi dizin kullanılır.
A) PROGRAM B) SYSTEM C) WINDOWS D) I386

19. NT Server kurarken karşımıza gelen Keyboard Layout ayarı ne içindir?
A) Fare türü B) Klavye türü C) Ekran türü D) Ses türü

20. "Redundant Array of Independent Disks" (bağımsız disklerin artıklı dizisi) anlamına gelen kısaltma nedir?
A) RAID B) RAED C) BDAD D) RAYT

21. RAID 1 ile hangi işlem yapılır ?
A) Şeritleme B) Kulonlama C) Aynalama D) Tarama

22. Aynalama (Mirroring) yapmak için kaç diske ihtiyaç vardır?
A) 1 B) 4 C) 3 D) 2

23. PCI RAID kartlarının BIOS'unu güncellerken hangi seçeneği kullanırız?
A) FlashBios B) SetupBios C) Readme D) Hiçbiri

24. RAID oluşturma seçeneği hangisidir?
A) Array Mode B) Delete RAID C) Create RAID D) Open Mode

25. Aynalama (Mirroring) hangi seçenekle yapılır?
A) Blok Size B) Array Mode C) S.D. Drivers D) S.C. Process

26. RAID kontrol kartı sürücü yükleme ayarlarını hangi seçenekten yaparız?

A) Control Panel B) Device Panel
C) Contol Unit D) Device Manager

27. Belirlediğiniz disklerden bir havuz oluşturmak için hangi seçeneği kullanırız?

A) Span (JBOD) B) Master
C) Slave D) Reboot

DOĞRU / YANLIŞ TESTİ

Aşağıdaki soruların cevaplarını doğru ve yanlış olarak değerlendiriniz. Sorulara verdiğiniz cevapları modül sonunda verilen doğru cevaplarla karşılaştırarak kendinizi kontrol ediniz.

SORULAR		DOĞRU	YANLIŞ
28	Komut satırında /HC:off ifadesi belirtilirse, seçenek iletişim kutusu ayarı geçersiz sayılır ve sıkıştırma kullanılmaz.		
29	Yalnızca yerel bilgisayardaki Sistem Durumu verilerini yedekleyebilirsiniz.		
30	Uzak bilgisayardaki Sistem Durumu verilerini yedekleyebilirsiniz.		
31	CDROM'dan yükleme yapılacak ise bir CDROM sürücü ve minimum VGA ya da daha yüksek çözünürlükte bir ekran gerekmez.		
32	FAT file sistemi, her türlü erişime izin verir. Çok geniş bir kullanım alanına sahiptir.		
33	FAT file sisteminde user bazında güvenlik sağlanır.		
34	NT server kurulması aşamasında NTFS file sistemi seçilmesi gerekmektedir.		

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konulara geri dönerek tekrar inceleyiniz. Tüm sorulara doğru cevap verdiyseniz diğer öğrenme faaliyetine geçiniz.

MODÜL DEĞERLENDİRME

PERFORMANS TESTİ (YETERLİK ÖLÇME)

Modül ile kazandığınız yeterlik, aşağıdaki işlem basamaklarına göre değerlendirilecektir.

DEĞERLENDİRME ÖLÇÜTLERİ	Evet	Hayır
1. Ağ Güvenliği (Donanım) kavramını tanıdınız mı?		
2. Ağ Güvenliği için Potansiyel Riskleri öğrendiniz mi?		
3. Veri Çalma (data theft) yöntemlerini öğrendiniz mi?		
4. Veri Yok Etme (destruction of data) türlerini öğrendiniz mi?		
5. Servis Reddetme (Denial of Service, DoS Attack) yöntemlerini öğrendiniz mi?		
6. Ağlar için Güvenlik Tehditlerini öğrendiniz mi?		
7. Dış Tehditleri tanıdınız mı?		
8. Servis Reddetme (DoS) yöntemini tanıdınız mı?		
9. Dağıtık Servis Reddetme (DDoS) yöntemini tanıdınız mı?		
10. Sömürücüler (Exploits)' i öğrendiniz mi?		
11. İç Tehditleri tanıdınız mı?		
12. Firma Casusluğu (Corporate Espionage)' nu öğrendiniz mi?		
13. Kötü Amaçlı Kullanıcılar (Rebellious users)'ı tanıdınız mı?		
14. Güvenlik Duvarı (Firewall) Cihazını tanıdınız mı?		
15. Güvenlik Duvarı tanımını kavradınız mı?		
16. Güvenlik Duvarının Yapısı ve Çalışmasını öğrendiniz mi?		
17. Güvenlik Duvarının Çeşitlerini öğrendiniz mi?		
18. Güvenlik Duvarının Ayarlarını öğrendiniz mi?		
19. Güvenlik Duvarının Üreticilerini tanıdınız mı?		
20. Yedeklemenin ne olduğunu öğrendiniz mi?		
21. Yedeklemenin önemini öğrendiniz mi?		
22. Yedeklemenin Çeşitlerini öğrendiniz mi?		
23. Sunucu Yedekleme (Server NT Backup)'yi öğrendiniz mi?		
24. Server NT Backup Kurulumunu yapabildiniz mi?		
25. Server NT Backup Ayarlarını yapabildiniz mi?		
26. Server NT Backup ile yedek aldınız mı?		
27. Aynalama (Mirroring) nedir tanıdınız mı?		
28. Aynalamayı Destekleyen Anakartları öğrendiniz mi?		
29. Aynalamanın Bağlantısını yapabildiniz mi?		
30. Aynalamanın Yazılımını Yükleyebildiniz mi?		

DEĞERLENDİRME

Yaptığınız değerlendirme sonucunda eksikleriniz varsa öğrenme faaliyetlerini tekrarlayınız.

Modülü tamamladınız, tebrik ederiz. Öğretmeniniz size çeşitli ölçme araçları uygulayacaktır, öğretmeninizle iletişime geçiniz.

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1 CEVAP ANAHTARI

SORU	CEVAP	SORU	CEVAP
1	Risk	18	sistem tabanlı
2	bilgi	19	Şirket çalışanları
3	IP	20	kötü amaçlı
4	hacker	21	değişiklik
5	veridir.	22	Internet servis
6	DoS	23	ISS
7	hizmet aksatma	24	Güvenlik duvarı
8	Service Overloading	25	saldırı tespiti
9	Message flooding	26	Doğru
10	Clogging	27	Yanlış
11	ping paketleri	28	Doğru
12	SSPing	29	Yanlış
13	Land Expoit	30	Doğru
14	out of band	31	Doğru
15	Zombi	32	Yanlış
16	Trinoo	33	Doğru
17	Exploit	34	Yanlış

ÖĞRENME FAALİYETİ-2 CEVAP ANAHTARI

SORU	CEVAP	SORU	CEVAP
1	B	18	D
2	A	19	B
3	D	20	A
4	B	21	C
5	A	22	D
6	D	23	A
7	D	24	C
8	B	25	B
9	B	26	D
10	A	27	A
11	C	28	Doğru
12	C	29	Doğru
13	B	30	Yanlış
14	A	31	Yanlış
15	B	32	Doğru
16	D	33	Yanlış
17	A	34	Doğru

KAYNAKÇA

- ÇÖLKESEN Rıfat, **Bilgisayar Haberleşmesi ve Ağ Teknolojileri**, Papatya Yayıncılık, Ekim 2000.
- ÇÖLKESEN Dr.Rıfat, **Bilgisayar Haberleşmesi ve Ağ Teknolojileri**, ISBN:975-6797-00-2, 2002.
- DERFLER Frank J, **Network Sistemleri ve Bilgisayar Bağlantı Klavuzu**, Sistem Yayıncılık, Şubat 1998.
- TANENBAUM Andrev S., **Computer Networks (3. Edition)**, Prentice-Hall,1996.
- UTKU Selim, **Internetworking & TCP/IP**, Armada Yayıncılık 2000.
- http://www.asistbilisim.com \Ağ_Guvenligi.htm
- www.bilgisayardershanesi.com
- http://www.bilisimsurasi.org.tr/ e-turkiye/docs/guvenlik07042004.doc,2002
- http://www.forumex.net/showthread.php?p=294905
- http://www.microsoft.com/turkiye/girisimci/themes/sgc/checklist/articles/zararli.mspx
- http://www.olympos.org/article/articleview/128/1/10/internet_guvenligi___bolum_2
- http://www.olympos.org/article/articleview/1351/1/10/voip_security
- http://www.pcnet.com.tr/
- http://silifke.meb.gov.tr/egitim/Windows%20NT/NT_yedekleme.htm
- http://www.tepum.com.tr/secura_guvenlik_duvari.htm
- http://www.veritim.com.tr/security.htm