NETFİLTER VE LİNUX TABANLI BİR FİREBOX TASARIMI

Gürkan KARABATAK
Fırat Üni. Enformatik Bölümü
gkarabatak@firat.edu.tr

Yrd.Doç.Dr Hasan H.BALIK
Fırat Üni. Mühendislik Fakültesi
balik@firat.edu.tr

ÖZET

Günümüzde ağ sistemlerinde en yaygın olarak kullanılan açık kaynak kodlu firewall alt sistemi olan Linux-Netfilter, kabuk programlama ve php script dili kullanılarak donanımsal bir firewall tasarlanması amaçlanmıştır. Bu firewall tamamen web uzerinden yonetilebilecek bir yapıdadır ve istenildiği zaman seri port üzerinden konsol bağlantısı yapılarakda kullanılabilmektedir. Bu sayede kullanıcı firewall'u tamamen gorsel web arabirimini ve kolayliklarini kullanarak hızlı, etkin ve kolay bir sekilde sistemine kurup yonetebilecektir.

GİRİŞ

Günümüz teknolojisinin hızla geliştiği bu günlerde bilgisayar ağları ve internet alanındaki uygulamalar hızla artmaktadır. Bununla birlikte bu ağlardaki uygulamalar ve kullanıcıların güvenliği ise önemli bir sorun teşkil etmektedir. Bu sorun günümüzde çeşitli güvenlik duvarı (firewall) yazılım ve donanım araçlarıyla çözülmeye çalışılmaktadır.

Buradaki düşünce, hem kullanıcılara bilgisayarları başından erişebilecekleri hizmetler sunabilmek hem de bu hizmetlerin kesintisiz olmasını sağlamak ve hizmeti aksatıp suistimal edebilecek herhangi bir kötü emelli erişime karşı önlemler alabilmektir. Bu nedenle bu araçların kullanımı bilgisayar ağları ve internet üzerindeki uygulamalarla doğru orantılı olarak artmaktadır.

Bu araçların bu denli önemli olmasından dolayı bu araçların kurulumu ve kullanılması ağ ortamına, kullanıcı sayısına ve verilen hizmetlere göre değişip zorlaşabilmektedir. Çünkü en ufak bir aksama tüm kullanıcıları ve verilen hizmeti büyük ölçüde etkileyecektir. Örneğin bir bankanın Internet üzerinden sunacağı hizmetin kesintiye uğraması hem banka hem de kullanıcılar üzerinde büyük etkiler oluşturacaktır.

Yapılan bu sistem sayesinde kullanıcı linux konsolu kullanmadan sistemi yönetebilecektir ve yapabileceği tüm işlemleri web üzerinden erişerek yapabilecektir. Web erişiminin kesintiye uğraması durumunda ise konsol portu üzerinden seri bağlantı yaparak sistemi yönetebilecektir.

1. Oluşturulacak Sistemin Yapısı:

Firewall sisteminde Genel Ayarlar, Firewall Ayarları, Routing Ayarları ve Bağlantı Takibi kısımları bulunmaktadır.

Genel Ayarlar kısmında bulunan Interface ayarları kısmı ile tüm interfacelere IP adresleri atanabilir ve var olan IP adresleri degistirilebilir. Şifreleme kısmında Web sayfasına erişim için kullanıcı adı ve şifre atanabilir ve Reset kısmından ise Sistem resetleme işlemi yapılabilir.

Firewall Ayarları kısmında Netfilter altsistemi için gerekli kural ve politika işlemleri yapılır. Zincirler için politikalar belirlenip istenilen Iptables kuralları eklenip, kaldırılıp, değiştirilebilir veya listelenerek basit ve hızlı bir şekilde yer değiştirilebilir.

Routing ayarları kısmında Network için gerekli yönlendirme işlemleri yapılabilir. Bu yönlendirme işlemleri network veya host bazında olabilir ve Ağgeçidi işlemleri yapılabilir.

Bağlantı Takibi kısmında ise port ve IP bazlı olarak bağlantı takibi yapılabilir. Firewall üzerinden gerektiğinde seri port kullanılarak seri bağlantı yapılabilir. Bu sayede web erişimi kesilse bile firewall seri bağlantı yoluyla linux konsolu üzerinden yapılandırılabilir.

Sistem herhangi bir Linux dağıtımı ve bilgisayar donanımı üzerine yapılandırılabilir. Sistem Linux-Netfilter-Iptables firewall sistemi, Kabuk programlama, Apache Web sunucusu ve PHP script dili kullanılarak tasarlanmıştır.

2. Linux İşletim Sistemindeki Gerçekleştirmeler:

Bu aşamada yapılan işlemler şu şekildedir.

İlk aşamada Linux işletim sistemi kurulup güvenlik duvarı haline getirilebilmesi için üzerinde ne gibi değişiklikler yapıldığı tespit edildikten sonra web sunucu üzerinde gerekli işlemler yapılmıştır. Bu aşamada Web sunucunun Linux işletim sistemi üzerinde gerektiğinde tam yetkili olarak komutlar çalıştırılabilmesi sağlanmıştır. Yine aynı şekilde gerekli yapılandırma dosyaları da ayarlanmıştır.

3. Web Arabiriminin Tasarlanması:

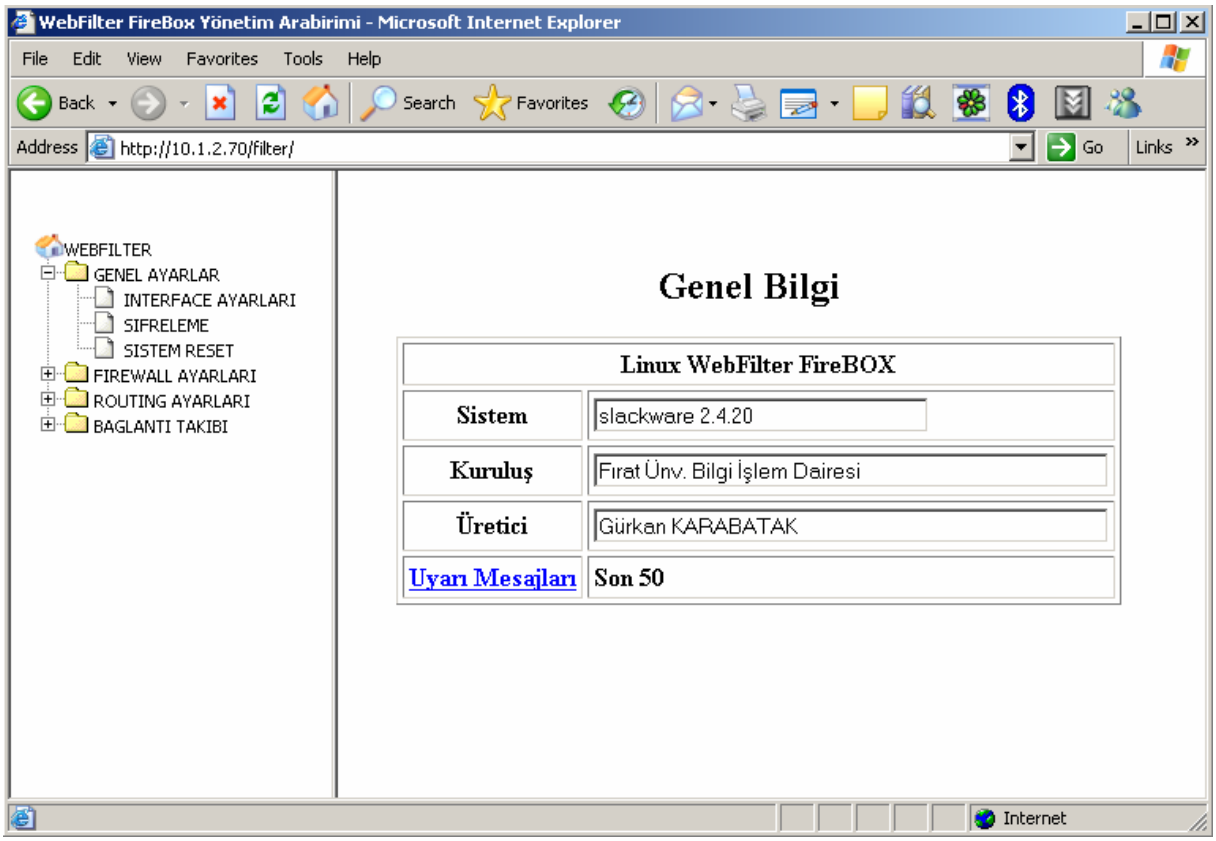
Güvenlik duvarının tamamen donanımsal bir yapı olmasından dolayı web arabirimi Oldukça büyük bir önem arz etmektedir.

a) Genel Ayarlar Modülü: İlk olarak güvenlik duvarının web yönetim kısmındaki bu modül tasarlanmıştır. Bu modülde Güvenlik duvarına web üzerinden bağlanıldıktan sonra. İnterface Ayarları, Şifreleme ve Reset kısımları oluşturulmuştur.

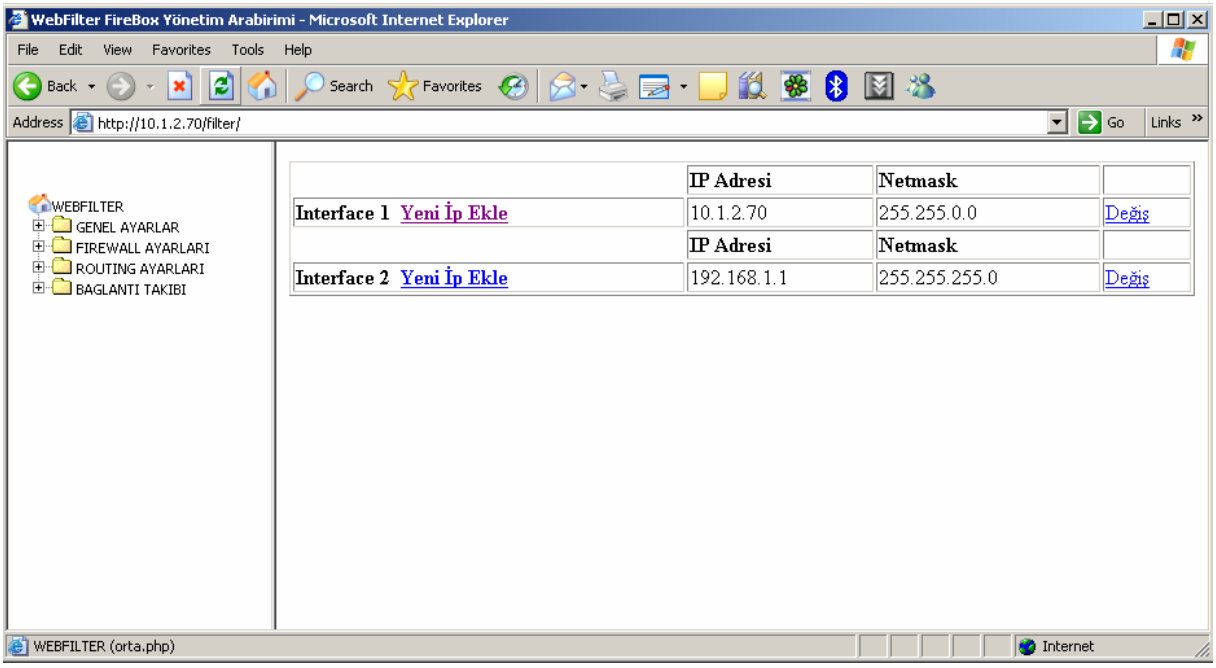
İnterface ayarları için PHP script dili ile Linux üzerinde kabuk programlama yapılmış ve gerekli komutlar kullanılarak web yönetim konsolu üzerinden güvenlik duvarı interfacelerine müdahale edilebilmesi sağlanmıştır. Web üzerinden tüm interfaceler otomatik olarak görüntülenip gerekli ip adresleri değişimlerinin yapılabilmesi sağlanmıştır.

Şifreleme kısmında web yönetim konsolu için kullanılan Apache web sunucu üzerinde ayarlar yapılarak web sayfasının istenildiğinde kullanıcı adı ve şifre verilerek güvenlik sorgulaması yapılması sağlanmıştır. Web sunucu dosyalarının bulunduğu dizinlerde gerekli dosyalar oluşturulması ve Apache konfigürasyon dosyalarında gerekli değişikliklerin yapılabilmesi için gerekli PHP kodları yazılarak işletim sistemi üzerinde bash kabuğu ile gerekli komutların çalıştırılabilmesi sağlanmıştır. Şifreleme işleminin iptalinde de yapılan işlemlerin geri alınması için gerekli kodlar yazılmıştır.

Reset kısmında ise sistemi yönetim konsolu üzerinden resetleyebilmek için gerekli kodlamalar yapılmıştır. Aynı şekilde resetleme işleminden sonra sistemin doğru şekilde açılabilmesi için düzenlemeler yapılması sağlanmıştır.

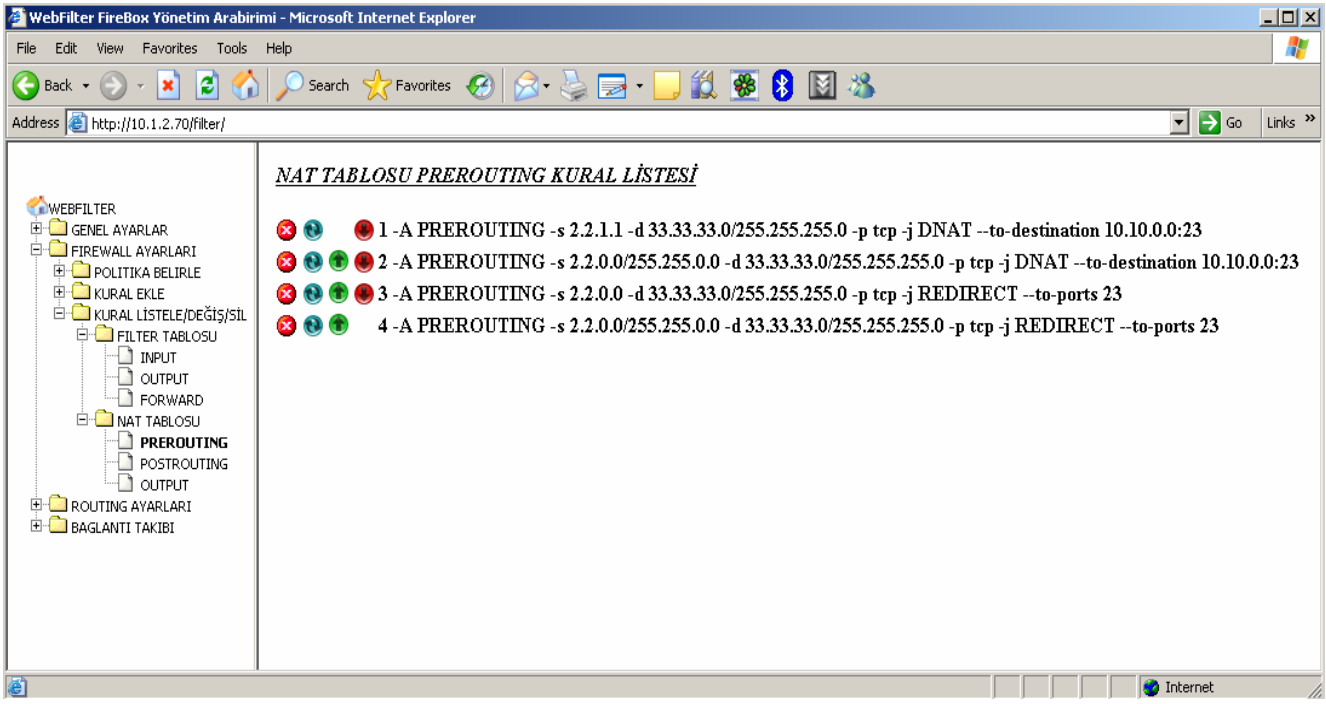


Şekil 3.1: Firewall Web Yönetim Ekranı Genel Görünümü



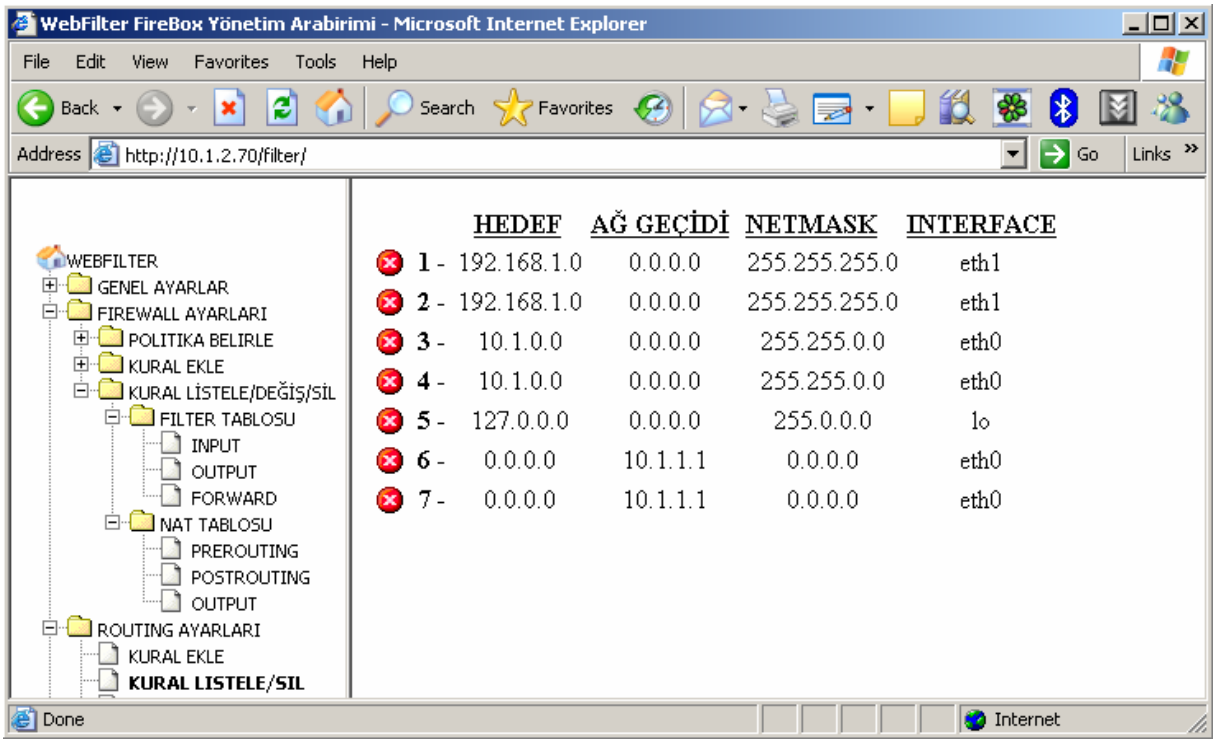
Şekil 3.2: Firewall Genel Ayarlar Ekranı İnterface Bölümü Görünümü

b) Firewall Ayarları Modülü: Bu kısım tamamen web üzerinden Linux işletim sistemine erişip güvenlik duvarı kurallarının oluşturulması sağlanmıştır. Web üzerinden yapılan tanımlamalarla Netfilter güvenlik duvarı alt sisteminin Iptables kural seti oluşturma yapısı kullanılarak bu kuralların sisteme uygulanmasını sağlayacak Dinamik HTML ,PHP ve Kabuk program kodları yazılmıştır. Bu kısımda güvenlik duvarında kullanılabilecek tüm yapılandırma işlemleri (NAT,MASQ,ACCEPT,DROP) için tanımlamalar yapılmıştır. Bu sayede tüm kurallar görülebilir, değiştirilebilir ve silinebilir hale getirilmiştir. Kuralların sıralandırılmasının kolay bir şekilde yapılması sağlanmıştır.



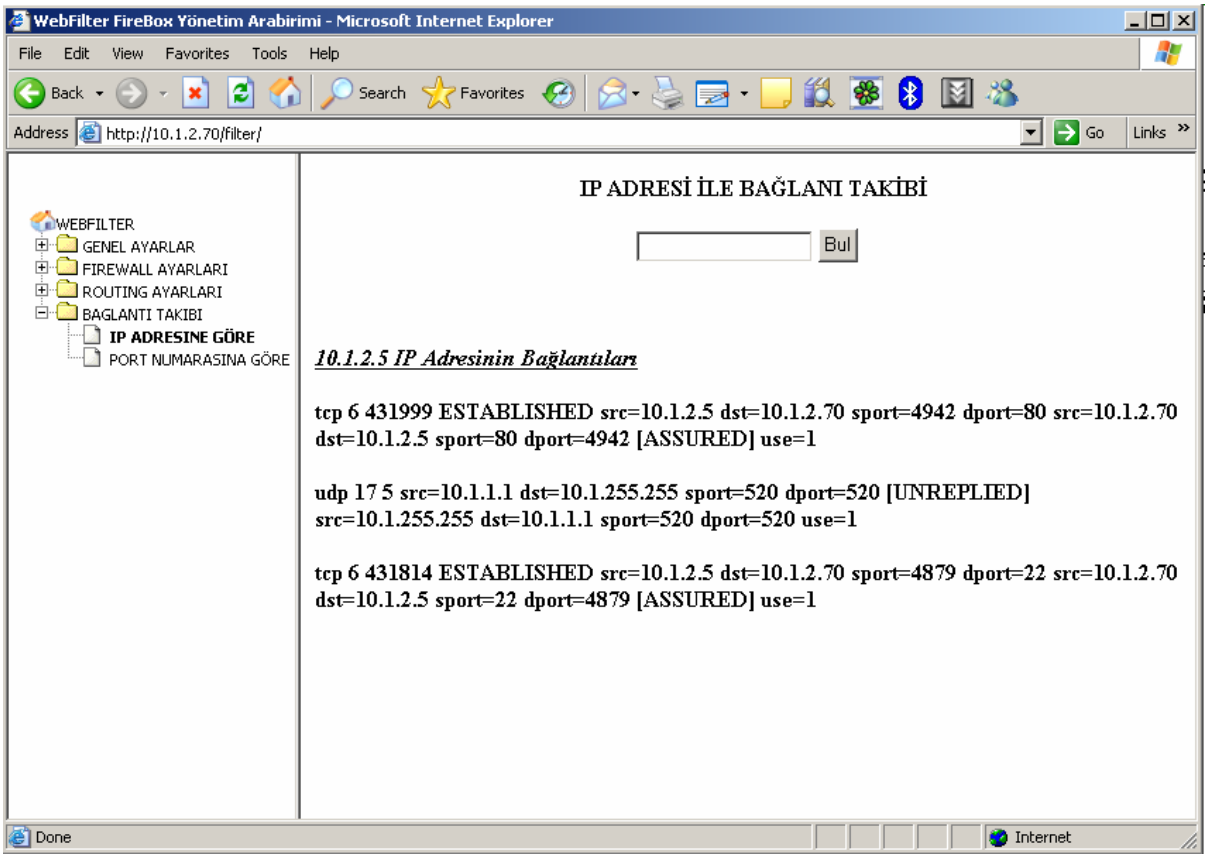
Şekil 3.3: Firewall Ayarları Modülü Kural Listeleme Ekranı

c) Routing Ayarları Modülü: Bu modül tamamen yönlendiricilerin yaptığı işlemleri yapabilecek kabiliyette tanımlanmıştır. Bunun için Linux kernelindeki yönlendirme yapısı kullanılmıştır. Bu sayede güvenlik duvarı ağ üzerinde yönlendirme işlemleri yapabilecek ve yönlendirici yerine kullanılabilecek hale getirilmiştir. Tüm güvenlik duvarlarında yönlendirme yapısı bulunmak zorundadır. Paket filtreleme işlemleri istenilen paketlerin yönlendirilmesi ve istenmeyenlerin engellenmesi mantığı ile çalışmaktadır.



Şekil 3.4: Routing Ayarları Modülü Kural Listeleme Ekranı

d) Bağlantı Takibi Modülü: Bu kısım ise güvenlik duvarının kullanıldığı durumlarda gerekli bağlantı takibi işlemlerinin yapılması sağlanmıştır. Bunun için gerekli düzenli ifade yapıları kullanılıp bağlantı aşamasında port bazlı ve IP bazlı kontrollerin yapılması sağlanmıştır. Bu işlem İşletim sisteminde yönlendirme aşamasında kullanılan contrack (Bağlantı takibi) yapısı kullanılmıştır. Bu yapı WEB'e aktarılarak kullanıcı tarafından gözetlenmesi sağlanmıştır.



Şekil 3.5: Bağlantı Takibi Modülü IP Adresli Takip

4. Konsol Port Bağlantı Modülü:

Bu kısım web yönetim arabiriminden tamamen bağımsızdır. Web yönetim kısmında sorun olduğunda veya TCP bağlantısının yapılamadığı durumlarda işletim sistemine ve güvenlik duvarına Seri port ve null modem kablosu kullanılarak bağlantı yapılabilmektedir. Bu sayede her durumda kullanıcının sisteme müdahale edebilmesi sağlanmıştır. Gerekli yapılandırmalar yukarıda anlatılan ilk yapılandırma dosyası içine yerleştirilmiş ve ilk kurulum esnasında gerekli değişikliklerin sistem üzerinde yapılabilmesi sağlanmıştır.

KAYNAKLAR:

1. Evi Nemeth, “Linux Administration Handbook” , Prentice Hall, Upper Saddle River Nj USA.
2. M.D. Bauer, “Building Secure Servers with Linux”, O'Reilly & Associates, London UK
3. K.G.Beauchamp & G.-S. Poo, “Computer Communications”, International Thomson Computer Press , Boston USA
4. Murat Yıldırımoğlu, “TCP/IP , internetin evrensel dili”, Pusula Yayıncılık Ltd. Şti. İstanbul TURKEY
5. Dr.Rifat Çölkesen & Doç.Dr.Bülent Örencik, “Bilgisayar Haberleşmesi ve Ağ Teknolojileri”, Papata Yayıncılık , İstanbul TURKEY
6. Dr.Rifat Çölkesen, “Network, TCP/IP, UNIX el kitabı”, Papatya Yayıncılık , İstanbul TURKEY