T.C.
MİLLİ EĞİTİM BAKANLIĞI

MEGEP

(MESLEKİ EĞİTİM VE ÖĞRETİM SİSTEMİNİN GÜÇLENDİRİLMESİ PROJESİ)

ENDÜSTRİYEL OTOMASYON TEKNOLOJİLERİ

UZAKTAN ERİŞİM

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	**481BB0088**
ALAN	**Endüstriyel Otomasyon Teknolojisi**
DAL/MESLEK	**Endüstriyel Kontrol Teknisyenliği**
MODÜLÜN ADI	**Uzaktan Erişim**
MODÜLÜN TANIMI	Gerekli ortam sağlandığında internet ortamında güvenlik uygulamalarını doğru olarak yapabilme yeteneğinin kazandırıldığı bir modüldür.
SÜRE	40/32 Saat
ÖN KOŞUL	İnternet Programcılığı Uygulamaları modülünü almış olmak.
YETERLİK	İnternet güvenliği uygulaması yapmak.
MODÜLÜN AMACI	**Genel Amaç** İnternet ortamında güvenlik uygulamalarını doğru olarak yapabileceksiniz. **Amaçlar** 1. Şifreleme programı ve SSH server kurulumunu hatasız olarak yapabileceksiniz. 2. Telnet ve uzaktan kontrol sunucusu kurulumunu hatasız olarak yapabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	**Ortam:** Bilgisayar laboratuvarı **Donanım:** Bilgisayar, hub
ÖLÇME VE DEĞERLENDİRME	Her faaliyetin sonunda ölçme soruları ile öğrenme düzeyinizi ölçeceksiniz. Araştırmalarla, grup çalışmaları ve bireysel çalışmalarla öğretmen rehberliğinde ölçme ve değerlendirmeyi gerçekleştirebileceksiniz.

GİRİŞ

Sevgili Öğrenci,

İnternet Güvenliği modülü ile endüstriyel otomasyon teknolojileri alanında gerekli olan internete bağlı bilgisayarların virüslere, saldırganlara karşı korumaya yönelik bilgi ve teknolojiye ait temel yeterlilikleri kazanacaksınız.

Günlük hayatımızın bir parçası olan interneti daha güvenli bir şekilde kullanabileceksiniz. Ayrıca bilgisayarlara uzaktan erişimin güvenli bir şekilde nasıl yapıldığını kavrayacak ve bu konuyla ilgili işlemleri rahatlıkla uygulayabileceksiniz.

Bu modülü başarılı bir şekilde tamamladığınızda internet haberleşmesiyle ilgili birçok sorununuzu rahatlıkla çözebileceksiniz.

ÖĞRENME FAALİYETİ–1

AMAÇ

Şifreleme programı ve SSH server kurulumunu hatasız olarak yapabileceksiniz.

ARAŞTIRMA

- Bilgisayarlara internet yoluyla saldırı yapılıp sistemin kullanılamaz hale getirilme sebeplerinin neler olduğu konusunda bir araştırma yapınız.

1. ŞİFRELEME

1.1. Şifre Kırma (İzinsiz Kullanım)

İki tip şifre kırma vardır.Her iki tip şifre kırma da suçtur.

Birinci tip şifre kırmada herhangi bir kâr amacı yoktur. Bu tip şifre kırmaya "attention-getting crime" yani “ilgi çekmek amacıyla suç işleme” denir.

İkinci tip şifre kırmanın amacı ise bilgisayara yasa dışı bir şekilde erişim sağlayarak bu işten kazanç sağlanmasıdır.

1.1.1. İlgi Çekmek İçin Suç İşleme (Attention-getting crime)

"Attention-getting crime" bazı insanların eğlence olarak algıladığı bir suçtur. Ve bu insanlar aşağıda sayılan işleri yaparlar.

- Virüslü mailler göderirler.
- Web sitelerini çökertirler.
- İnternet sayfalarındaki bilgileri tahrip ederler.

Ayrıca sunucu sistemlerinin işlevini durdurur ve bilgisayarınızdaki önemli dosyaları silerler. Bunları yaparken herhangi bir kazançları yoktur.

1.1.2. Kazanç İçin Yapılan Şifre Kırma

İnternetteki bir sunucu birçok değişik bilgiye sahiptir. Örneğin bir mail sunucu, kullanıcıların mail adres bilgilerine sahiptir. Başka bir örnek olarak veri tabanı sunucu birçok değişik bilginin kullanımına olanak sağlar.

Bu bilgiler saldırganlar tarafından elde edilip kâr amacıyla satılabilir. Bilgisayara izinsiz giriş dış bilgisayar ağından olabileceği gibi yerel bilgisayar ağından da olabilir. Bu yüzden güvenlik tedbirleri önemlidir.

1.1.3. Olabilecek Zararlara Karşı Temel Tedbirler

Bu bölümde bilgisayara izinsiz giren saldırganların verebileceği zararlar ve bunlara karşı alınacak temel tedbirler anlatılacaktır.

1.1.3.1. Dosyaların Bozulması ve Sistemin Çökmesi

Web sayfasındaki dosyaların bozulması buna tipik bir örnektir. Bozulan dosyalar yeniden yüklenebilir. Fakat bu durum web sayfasının güvenirliğini düşürür.Sistemin çökmesi ise bazı temel dosyaların kullanılamaması anlamına gelir. Bu dosyalara örnek olarak OS(İşletim Sistemi) veri tabanı verilebilir. Temel dosyaların zarar görmesi durumunda sistem tekrar açılamaz. Sistemin yeniden yüklenmesi gerekir. Böyle bir durumda internet servisi uzun süre hizmet veremeyeceği için zarar eder.

1.1.3.2. Virüs

Birçok çeşit virüs vardır. En basit örnek olarak e-mail dosyalarıyla gelen virüslerdir.Virüslerin çeşitli bulaşma yolları vardır:

- İnternetten dosya indirme yoluyla
- Bilgisayarın çevre birimlerinin kullanılması yoluyla: Örneğin floppydisk, CD-Rom

1.1.3.3. DoS Saldırısı

Dos (Servisin Durdurulması) saldırısı nedir?

Dos saldırısı karşı sistemde işlemekte olan servisleri bloke yapmak amacıyla yapılan saldırılardır. DoS saldırısı internet sunucularının durmasına sebep olur. Böyle bir durumda kullanıcılar internet servislerinden yararlanamazlar.

1.1.3.4. Bilgi Sızıntısı

Bilgi Sızıntısının Sebebi

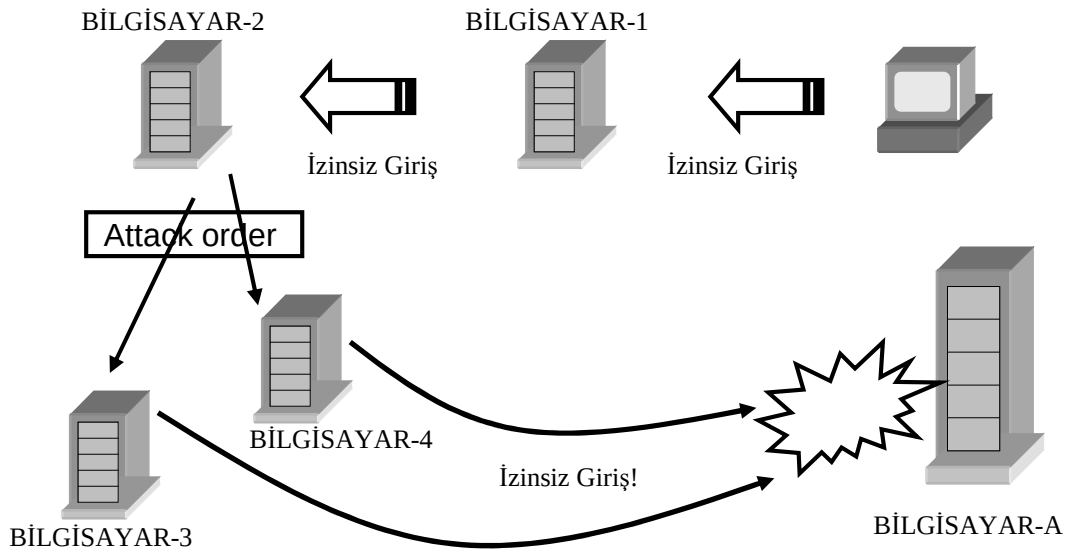
- Yerel ağ içindeki bilgilerin izinsiz kullanılması
- Sistemi veri tabanına izinsiz girme.

Eğer önemli bilgiler izinsiz kullanılıyorsa bunun sonucu çok kötü olabilir.Bilgi sızdırılmasına karşı temel tedbirler şunlardır:

- Bilgisayara izinsiz girişlere karşı korunma
- Bilginin kodlanması
- Bilgisayara şifre verilmesi

1.1.3.5. Tuzak

Genellikle bir okul sunucusunda önemli bilgiler olduğu düşünülmez. Bu yüzden bu tip sunucularda güvenlik tedbirlerine gerek duyulmaz. Bu düşünce şekli çok yanlış ve tehlikelidir. Saldırganlar network ağında yaptıkları suçları gizlemek için güvenlik tedbirlerine dikkat edilmeyen bilgisayarları kullanırlar. Aşağıdaki örneği inceleyecek olursak saldırganların kendilerini nasıl gizlediklerini daha iyi anlayabiliriz.Saldırgan tuzak olarak kullandığı bilgisayarı kullanarak kimliğini saklar.



Şekil.1.1: Tuzak

Saldırgan BİLGİSAYAR-A'ya ulaşmak için ilk olarak BİLGİSAYAR-1'i kullanılır. Daha sonra BİLGİSAYAR-2'ye BİLGİSAYAR-1'i kullanarak ulaşır. Ve sırasıyla BİLGİSAYAR-3 ve BİLGİSAYAR-4'de de ulaşan saldırgan, bu bilgisayarların IP adreslerini kullandığı için kendi IP adresini gizler. Bu şekilde izinsiz olarak kullanılan bilgisayarlara "Tuzak" denir. Saldırganlar ülke içinden de ülke dışından da sunuculara izinsiz girip bu bilgisayarları "Tuzak"olarak kullanabilirler. Bundan dolayı internet üzerindeki sunucularda gerekli güvenlik tedbirlerinin alınması gerekir.

1.2. Şifre Kırmanın Yöntemi

Saldırgan aşağıdaki yöntemi izleyerek bilgisayara izinsiz giriş yapar.

- Basamak bilgisayara ulaşılması

⇩

- Basamak sistem konfigürasyonunun incelenmesi

⇩

- Basamak Sistem kontrolünün ele geçirilmesi

⇩

- Basamak sistemin izinsiz kullanılması

Bu yöntemle bilgisayara giren saldırgan sistemde ne kadar uzun süre kalırsa sisteme vereceği zarar da artar.

1.2.1. Hedef Bilgisayarın Ele Geçirilmesi

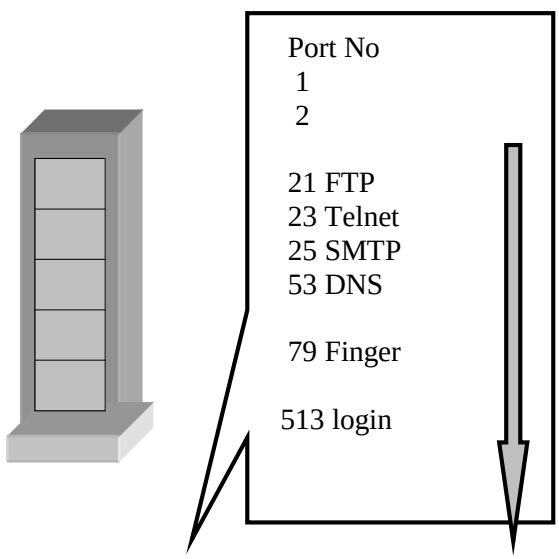
1.2.1.1. Tarama

Tarama genel olarak aşağıdaki şekilde icra edilir.

- **Ping taraması:** Ping komutu bilgisayarın IP adresini kontrol eden bir araçtır. Saldırgan bu şekilde hedef aldığı bilgisayarın internete bağlı olup olmadığını anlar.

- **İsim taraması:** Efektif hostname ve IP adresi internetten elde edilir ve listelenir.

- **Port taraması:** IP adreslerine sahip bilgisayarlara ulaşmak için sunucular (HTTP, SMTP, Telnet gibi) incelenir.



Şekil.1.2: Port taraması

TCP/IP protokolü port taraması için kullanılır. Saldırgan içinde port numaralarının (1ile 1023 arası) bulunduğu TCP/IP paketi hedef bilgisayara gönderir. Eğer saldırgan hedef bilgisayardan gönderdiği paketin cevabını alırsa hedefindeki bilgisayarın hangi portunun açık olduğunu anlar.

1.2.2. Sistem Konfigürasyonunun İncelenmesi

Saldırgan, hedef bilgisayarı bulduktan sonra aşağıdaki yolu takip eder.

Sunucunun OS'sini (Apache gibi) inceler. Hedef bilgisayardaki eksik güvenlik tedbirlerini tespit eder.

Bundan sonra saldırgan gelişigüzel bilgisayara girmeye çalışabilir. Ancak belirli bir alana girebilir. Bu durumda hedef bilgisayar ile ilgili alan bilgisine ihtiyaç vardır. Bu bilgi ise e-mail başlığı gibi yöntemler kullanılarak elde edilebilir.

1.2.3. Buffer Overflow(Geçici Bellek Bilgi Taşması) (Hedef Bilgisayara İzinsiz Giriş)

Bilgisayara izinsiz girmek için bazı yöntemler vardır. Bu yöntemlerin en önemlisi geçici bellekteki bilgi taşmasının kullanılmasıdır.

1.2.3.1. Geçici Bellek Bilgi Taşmasının Genel Hatları

Bu yöntemle saldırgan, kullanıcı adı ve şifreyi kullanmadan sadece komut ve programla bilgisayarı ele geçirebilir.

Bilgi taşmasından kaynaklanan güvenlik boşluğunu gidermek için özel programlar kullanılsa bile saldırgan değişik araçlar kullanarak bilgisayara girebilir. Özellikle bilgisayar internete açık ise bilgisayarın kontrolünün ele geçirilmesi daha kolay olacaktır.

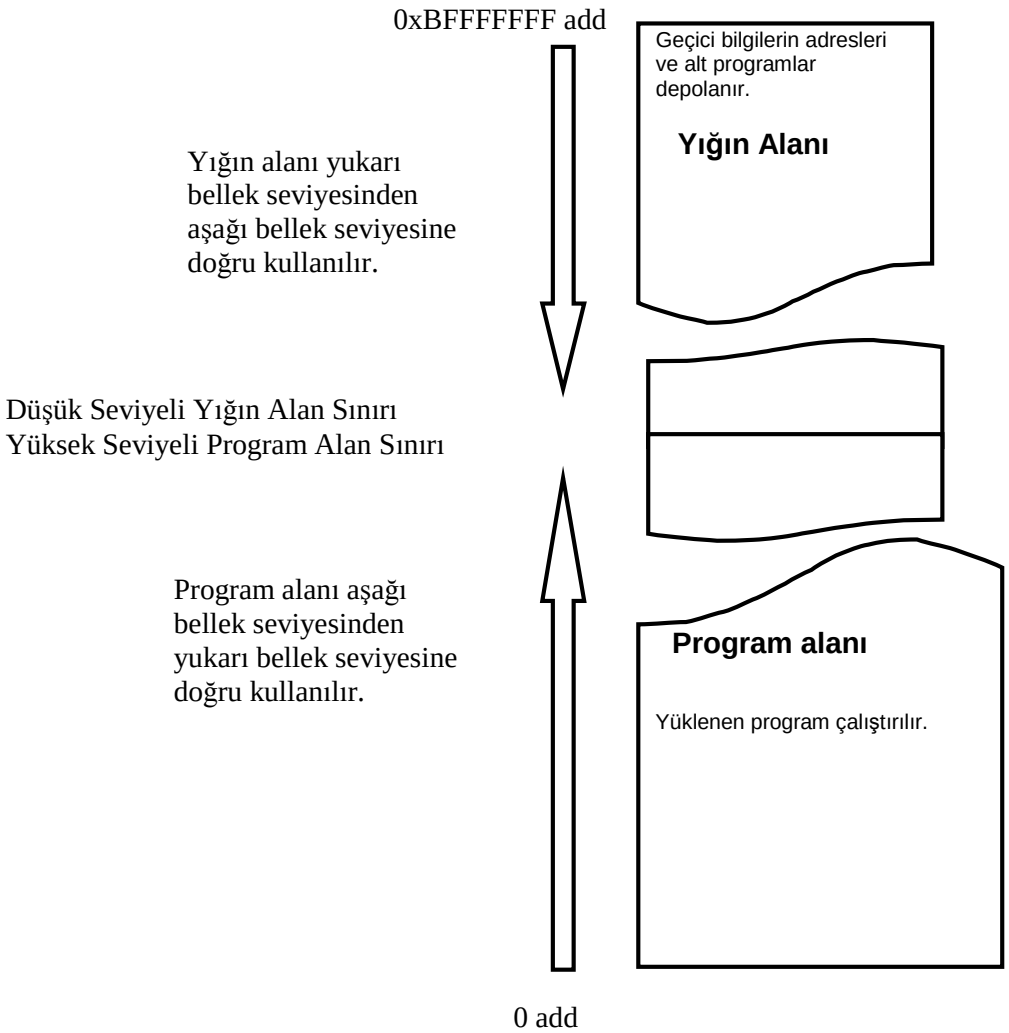
Geçici bellekteki bilgi taşmasından kaynaklanan sorunlar şunlardır:

- Bilgisayar kullanıcısının ilk açılışta güvenlik amacıyla uyguladığı şifre ve kullanıcı adının hiçbir fonksiyonu kalmaz.
- Root yetkisinin kullanılamama olasılığı yüksektir.
- TCP/IP protokolü kullanıldığı için bilgisayara yapılan saldırıyı firewall kullanılarak engellemek çok zordur.
- Bu daemon programının bir hatasıdır.

Bilgi taşmasını önlemek için gereksiz programların yüklenmemesi gerekir. Veya programların son sürümleri kullanılmalıdır.

1.2.3.2. Geçici Bellekteki Bilgi Fazlalığının Oluşması

Bu bölümde bilgi fazlalığı hakkında bilgi verilecektir.



Şekil.1.3: Bellek nasıl kullanılır

CPU belleğe ulaşır, adres bölünür, OS belleği ikiye böler.

- Program alanı
- Yığın alanı

"Buffer" bilgilerin geçici olarak yığın alanında depolandığı bir bellektir. Bilgi fazlalığı yığın alanında bufferın oluşmasına neden olur.

1.2.4.Tapping (Saldırı)

Kullanıcı ID ve şifrenin kullanılamadığı saldırı çeşididir. Bu tip saldırılara "Sniffer". denir. LAN içindeki bilgilerin analiz edilmesi 1995'e kadar çok zordu. Çünkü bu iş için özel donanımlara ve yüksek teknolojiye ihtiyaç vardır.Bugün LAN içindeki bilgileri kolayca toplayacak araçlara sahibiz. Bu araçlar networkte meydana gelecek arızaların giderilmesinde kullanılır.

1.2.5.Saldırının İşareti

Saldırganların kullandığı teknoloji devamlı değiştiği için bunlara karşı alınacak tedbirler de değişim göstermek zorundadır. Eğer LAN' da saldırganın saldırısını erken farkedersek oluşacak zararları minumuma indiririz.Saldırgan sisteme girdikten sonra kendisini gizlemek ister. Bunun için değişik yöntemler kullanır. Örneğin, log dosyasını tahrip eder.

1.3. Saldırı

Saldırı yapmak için değişik teknikler vardır. Burada iki tip DoS saldırı çeşidini öğreneceğiz.

1.3.1. Servisin Durdurulması

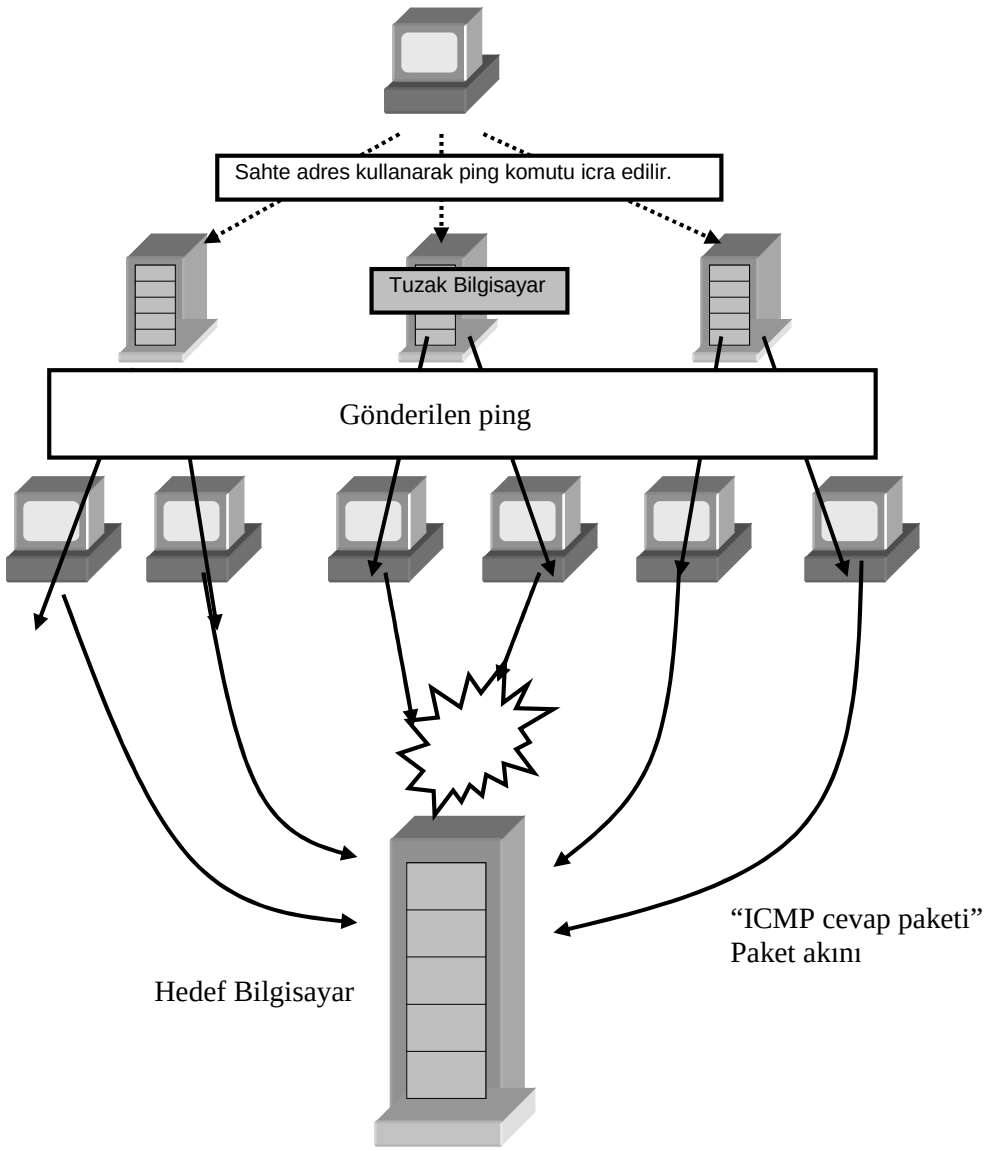
1.3.1.1. Ping Komutu Kullanılarak Yapılan Saldırı

Ping komutu uygulandığı zaman bunun cevabı olarak ICMP paketi gönderilir. Burada Ping komutunu "-b" seçeneğini ile beraber kullanırsak meydana gelecek olayları inceleyelim. Şunu da belirtelim ki "-b" seçeneği root yetkisinde kullanılır

ping –b 192.168.0.255

ICMP paketi alan bilgisayar cevap olarak yine ICMP paketi gönerir.

Ping komutu gönderen bilgisayar birçok cevap paketi alır.



Şekil 1.4: Ping Komutu kullanılarak yapılan saldırı

Kaynak ve hedef için kullanılan IP adres TCP/IP paket içinde tanımlanır. Saldırgan, kaynak için sahte bir IP adres kullanır. Ping komutunu bu sahte adresle icra eder.

⇩

ICMP istek paketini alan bilgisayarlar hedef bilgisayara ICMP cevap paketini gönderir.

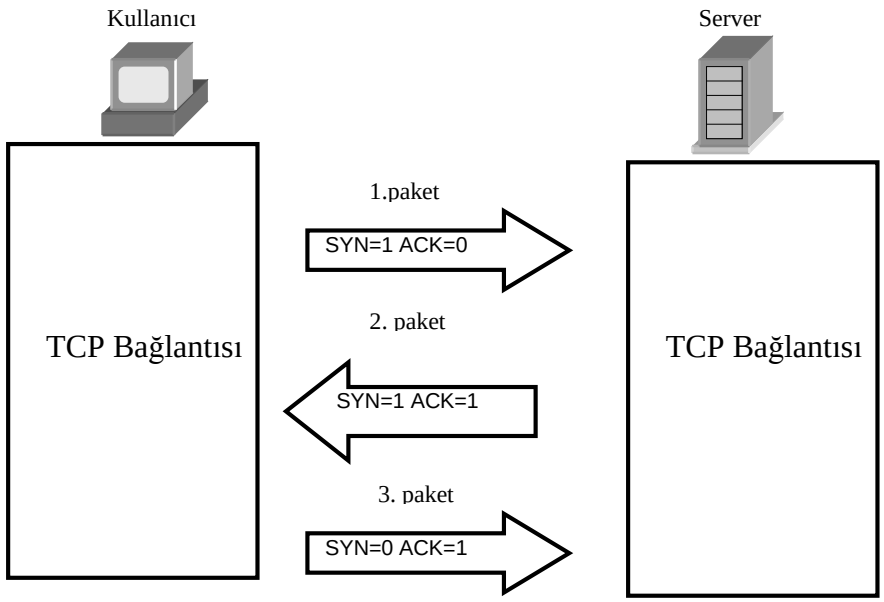
⇩

Sonuç olarak hedef bilgisayara çok miktarda ICMP cevap paketi gönderilir.

Buna ek olarak saldırgan aynı sahte IP adresle icra ettiği ping komutunu tuzak olarak kullandığı bilgisayar üzerinden de gönderir. Böylece hedef bilgisayar daha fazla ICMP cevap paketi alır. Hedef bilgisayarın CPU'su ICMP paketlerine cevap vermekten aşırı şekilde yüklenir ve çabuk bozulur.Bu şekilde yapılan saldırıya Smurf saldırısı veya Pingseli saldırısı denir.

1.3.1.2. SYN Saldırısı

TCP protokolde SYN ve ACK bayrakları kullanılarak bilgisayar arası iletişim sağlanır.



Şekil.1.5: Üç aşamalı haberleşme

Server "SYN" bayrağının 1 olduğu paketi alır.

"SYN" bayrakları sırasıyla işleme alınır. Bunun için bu bayraklar yaklaşık kapasitesi 256MB olan bir bilgi alanına depolanır. "SYN" bayraklarının miktarı 256MB olan bilgi alanının kapasitesini geçerse üçüncü paket alınamaz.

Çünkü bilgi alanının kapasitesi geçildiği için sıradaki birinci paket işleme konulamamıştır. Bilgi alanı artık kullanım dışıdır.

Bilgisayar yeni "SYN" bayrağını alamaz. Bunun manası network iletişiminin kesilip servisin durması demektir. Bu saldırıya "SYN" saldırısı denir.

Bu, "netstat" komutunun bir sonucudur. Komut aşağıdaki şekilde uygulanır.

```
[root@server root]# netstat -a | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address    Foreign Address        State
tcp        0      0  *:x11              *:*                 LISTEN
tcp        0      0 *:ftp               *:*                 LISTEN
tcp        0      0 *:https             *:*                 LISTEN
```

Yukarıdaki mesajlarda şu ana kadar hiçbir sorun yok. Fakat SYN saldırısı başladığı anda ekranda aşağıdaki mesaj görüntülenir.

SYN_RECV

Bu saldırıyı diğer normal paketlerden ayırmak çok zordur. Ayrıca saldırganlar başka bilgisayarlardan da (tuzak bilgisayarlar) SYN paketleri gönderebilirler. Bu saldırıya devam edildikçe sistem çöker ve yeniden reboot yapılsa bile sistem hata verir.

Saldırganın başka bilgisayarları kullanarak yaptığı saldırıya "DDoS (Distributed Denial of Service) denir.

1.3.2. Zararlı E-Posta

1.3.2.1. SPAM Mail

Sunucuya mail göndermek için SMTP (Simple Mail Transfer Protocol) kullanılır. Ve POP3 protokolü ile sunucudan mailler indirilir.

Bu iki protokol arasındaki fark;

POP3 kullanıcı bilgisi doğrulama

SMTP genelde kullanıcı bilgisi doğrulanmaz.

Yani diğer bilgisayarlarla direkt bağlantı kurulup e-mail diğer bilgisayarlara gönderilir.

Yukarıda bahsettiğimiz mekanizmayı değişik amaçlı kullanarak kazanç sağlayan saldırganlar vardır. Hackerlar, kullanıcı bilgisini geçersiz hale getirerek "SPAM”mail ”(zararlı mail) gönderirler. Bu mailleri gönderen kişilere "SPAMER" denir.

SPAMER zararlı mailleri (SPAM) göndermek için mail sunucuyu kullanır. SPAM’ler için kullanılan sunucu çalışamaz duruma gelebilir.

1.3.2.2. Mail Bombası

Mail bombası hedef sistemi çökertmek için sunucudan gönderilir. Kullanıcıya gelen bu maillerin hem sayısı fazladır hem de büyük bilgi alanı işgal ederler. Sonuç olarak disk alanı dolar ve kullanım dışı kalır.

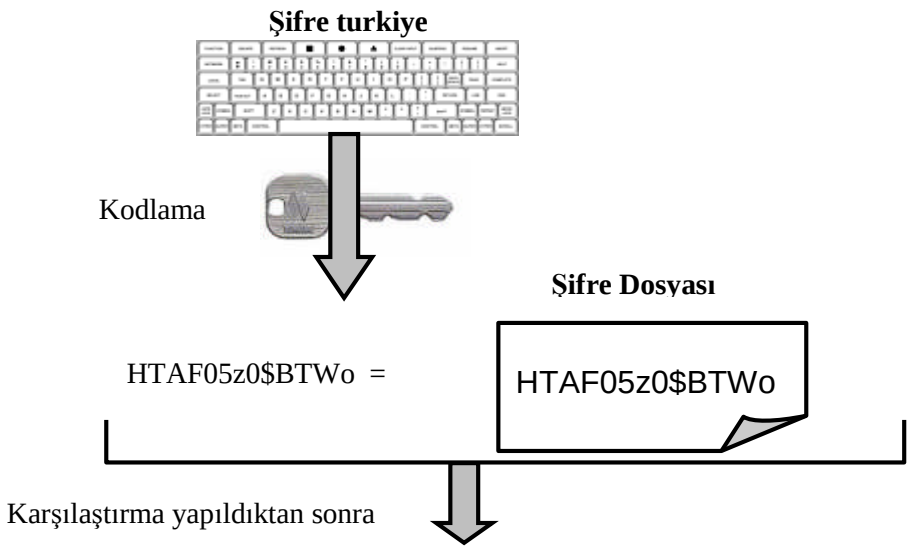
1.4. Şifreleme Algoritmaları

1.4.1.Şifre Mekanizması

Bilgisayara verilen şifreler "hash" fonksiyonu kullanılarak kodlanır. Hash fonksiyonunun özelliğinden dolayı şifre kodu çözülemez.

Örnek olarak “turkiye” olarak verilen bir şifre kodlanır.

Sonra verilen şifre, şifre dosyasındaki kodla karşılaştırılır.



Şekil.1.6: Şifre mekanizması

Örnek : Shell

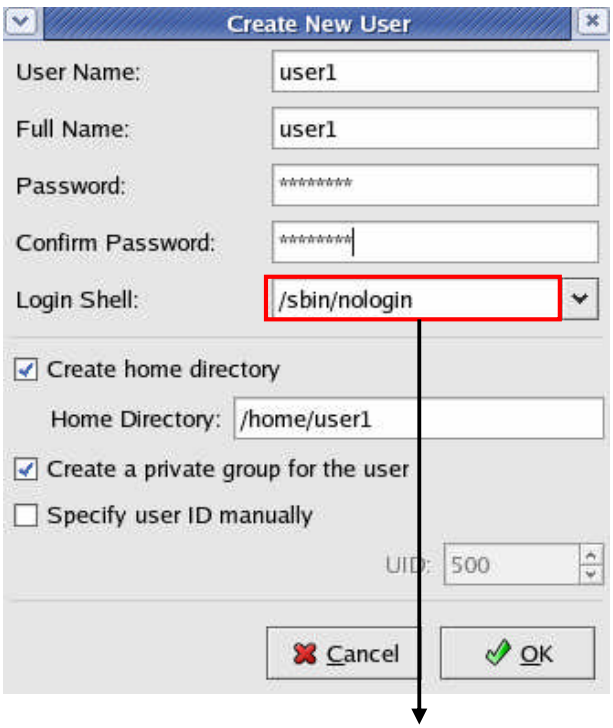
Saldırgan'ın bilgisayara izinsiz girip Shell'i uygulama dışı bırakması çok tehlikeli sonuçlar doğurur. Bundan dolayı POP protokolle sadece e-mail kullanan bilgisayara shell verilmemelidir. Aşağıda Shell'le ilgili alıştırmayı inceleyiniz.

- **Kullanıcı tanımlaması**

Kullanıcı aşağıdaki şekilde tanımlanır.

User (kullanıcı) user

Passwd (şifre) hogehoge



Login shell aşağıdaki şekilde değiştirilir.

Şekil 1.7: Login Shell'in değiştirilmesi

- **Login kontrolü**

Login'e user1 yazılır. Bu halde login'e girilememelidir.

- **Shell'in değiştirilmesi**

Shell editör kullanılarak değiştirilebilir

cat /etc/passwd
Yukarıdaki komutu uyguladıktan sonra aşağıdaki satırı görürüz.
user1:x:503:503:user1::/sbin/nologin

Bu satırdaki parametrelerin anlamları aşağıda verilmiştir.

user1	Kullanıcı adı
x	Kodlanmış şifre
503	Kullanıcı ID numarası
503	Gurup ID numarası
user1	Login dizini
::	Kullanıcı bilgisi (ismin tamamı vb.)
/sbin/nologin	Shell kullanılır.

- Kullanıcının Silinmesi

Bu alıştırma için belirlenen kullanıcılar silinir.

1.4.2. Saldırganların Saldırısına Karşı Tedbirler

1.4.2.1.Paketin Bloke Edilmesi

Örnek: Paketin Bloke Edilmesi

Linux işletim sistemi içinde saldırılara karşı "Proc File System" olarak bilinen savunma fonksiyonları mevcuttur. Bu fonksiyonlar "/proc" dizini altındaki dosyalarda mevcuttur.

"/proc" dizini altındaki savunma dosyalarının özel bir anlamı vardır ve sahip oldukları parametreler kernel'ı çalıştırır.

- **Dosyanın kontrolü**

Aşağıda "Proc File System" ile ilgili alıştırmayı inceleyiniz. Ve "ls" komutunu kullanarak aşağıdaki mesajı kontrol ediniz.

ls /proc/sys/net/ipv4/

Mesaj

```
[root@ie /]# ls /proc/sys/net/ipv4/
conf                                 ipfrag_time
tcp_max_syn_backlog
icmp_echo_ignore_all                 ip_local_port_range     tcp_max_tw_buckets
icmp_echo_ignore_broadcasts          ip_nonlocal_bind        tcp_mem
icmp_ignore_bogus_error_responses    ip_no_pmtu_disc         tcp_orphan_retries
icmp_ratelimit                       neigh                   tcp_reordering
icmp_ratemask                        netfilter               tcp_retrans_collapse
igmp_max_memberships                 route                   tcp_retries1
inet_peer_gc_maxtime                 tcp_abort_on_overflow   tcp_retries2
inet_peer_gc_mintime                 tcp_adv_win_scale       tcp_rfc1337
inet_peer_maxttl                     tcp_app_win             tcp_rmem
inet_peer_minttl                     tcp_dsack               tcp_sack
inet_peer_threshold                  tcp_ecn                 tcp_stdurg
ip_autoconfig                        tcp_fack                tcp_synack_retries
ip_conntrack_max                     tcp_fin_timeout         tcp_syncookies
ip_default_ttl                       tcp_frto                tcp_syn_retries
ip_dynaddr                           tcp_keepalive_intvl     tcp_timestamps
ip_forward                           tcp_keepalive_probes    tcp_tw_recycle
ipfrag_high_thresh                   tcp_keepalive_time      tcp_tw_reuse
ipfrag_low_thresh                    tcp_low_latency         tcp_window_scaling
ipfrag_secret_interval               tcp_max_orphans         tcp_wmem
```

Sistem başlarken parametrelerin ayarlanması için aşağıdaki tanımlamanın yapılması gerekir.

/etc/sysctl.conf

Yukarıdaki tanımlamayı sysctl.conf içinde yaparsak "/" yerine "." kullanılmalıdır. "/proc/sys" için tanımlama yapılmayabilir.

- SYN Cookies

vi /etc/sysctl.conf

Aşağıdaki tanımlamayı yapın.

net.ipv4.tcp_syncookies = 1

Hata!# Controls IP packet forwarding
net.ipv4.ip_forward = 0

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0

# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1

net.ipv4.tcp_syncookies = 1

net.ipv4.icmp_echo_ignore_broadcasts = 1

Yukarıdaki tanımlamayla şu sonuçlar elde edilir.

SYN saldırısının özelliği olarak bilgisayar yarı açık birçok bağlantı isteği alır.

⇩

Bunun bir saldırı olduğuna karar verilir ve kernel SYN Cookies kullanacak şekilde ayarlanır.

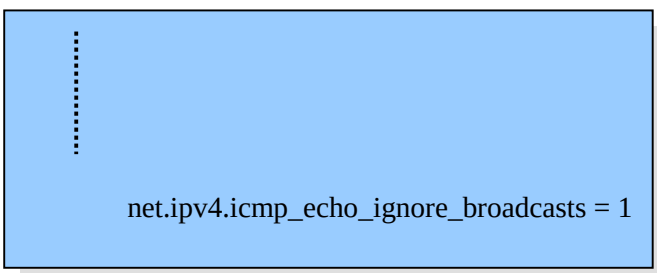
⇩

geçici bellekteki bilgileri hemen işleme konulmaz.

- ICMP Paketi Gönderme

vi /etc/sysctl.conf

Aşağıdaki komutu sysctl.conf. içine yazınız.
net.ipv4.icmp_echo_ignore_broadcasts = 1



IP protokol genellikle üç şekilde kullanılır.

- TCP
- UDP
- ICMP

ICMP protokolü network ağını test etmek için kullanılır (ping ve traceroute komutları gibi) (11. sınıfta bu komutlar işlenmişti).Broadcast adresini kullanan ICMP paketi yukarıdaki ayarlama yapıldıktan sonra işleme alınmaz. Başka bir deyişle “Smurf saldırsı veya ping saldırısı ihtimali azaltılır.

1.4.3. Önemli Güvenlik Tedbiri

Örnek: w komutu

Log olarak kullanılan kullanıcı ismini ve login zamanını öğrenebiliriz.

w

Mesaj

```
[root@ie root]# w
 14:26:46  up 7 min,  2 users,  load average:  0.16, 0.16, 0.09
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU  WHAT
root     :0       -                 2:21pm   ?     0.00s  0.44s  /usr/bin/gnome-root
pts/1    :0.0                       2:26pm  0.00s  0.03s  0.01s  w
```

Bu bölüm önemlidir. Genellikle bir veya daha fazla olmaz. Load average kısmı bir veya daha fazla olursa dışarıdan bilgisayara izinsiz girilmiş olunabilir.

Örnek: gcc İzni

C dilinin kaynak kodlarını sunucuya gönderene "Slapper(worm) denir. Worm sunucudaki kodlarını derler.Bu yüzden “gcc” yüklenen sistemlerde izinin değiştirilmesi tercih edilir.

- “gcc” nin yeri

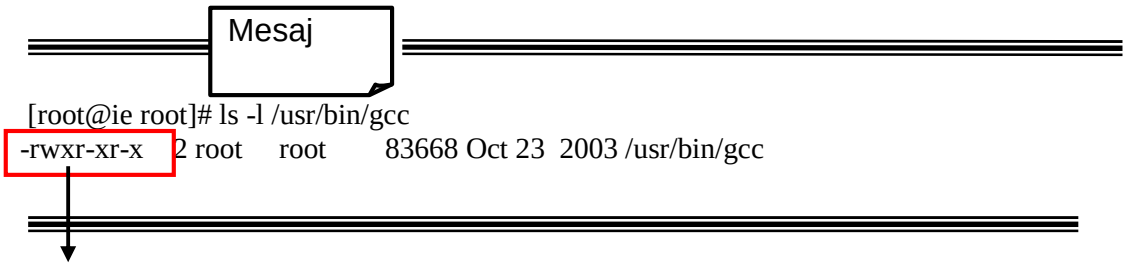
İlk olarak “gcc” nin nerede kayıtlı olduğu bulunur.

```
which gcc
```

Sonuç olarak aşağıdaki dizine ulaşırız.
/usr/bin

- İznin kontrolü

```
ls –l /usr/bin/gcc
```



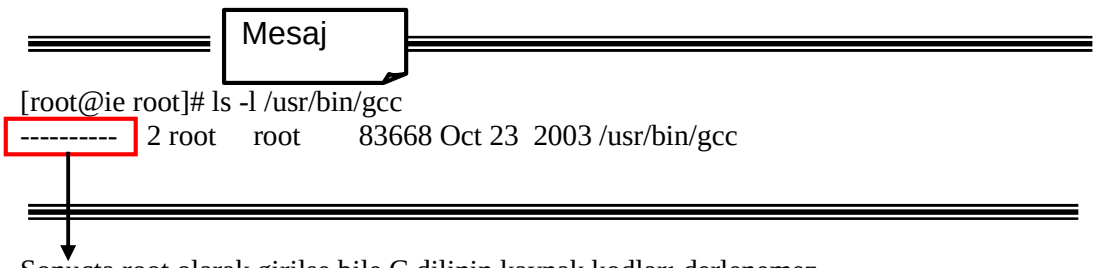
Bu ayarlamayla bütün kullanıcılar C dilinin kaynak kodlarını derleyebilir.

- İzinin Kaldırılması

```
chmod 000 /usr/bin/gcc
```

- İznin Tekrar Kontrolü

```
ls –l /usr/bin/gcc
```



Sonuçta root olarak girilse bile C dilinin kaynak kodları derlenemez.

Örnek: last Komutu

Son olarak bilgisayara giren kullanıcı ekranda görüntülenir. Ayrıca Linux'ın başlama zamanı da görüntülenir.

Mesaj

```
[root@ie root]# last
root     pts/2        :0.0                          Wed Oct 20 14:27   still logged
in
root     pts/1        :0.0                          Wed Oct 20 14:26   still logged
in
root     :0                                         Wed Oct 20 14:21   still logged
in
reboot   system boot  2.4.22-1.2115.np              Wed Oct 20 14:19         (00:19)
root     pts/1        :0.0                         Wed Oct 20 12:43 - 12:44
(00:00)
root     :0                                        Wed Oct 20 12:43 - down
(00:03)
reboot   system boot  2.4.22-1.2115.np              Wed Oct 20 12:42         (00:04)
root     pts/1        :0.0                         Wed Oct 20 09:45 - 10:54
(01:08)
root     :0                                        Wed Oct 20 09:45 - down
(01:09)
user1    :0                                         Wed Oct 20 09:43 - 09:43
(00:00)
```

Zamanın görüntülendiği yer

- Bilgisayara girilen zaman
- Linux başladığı zaman
- Linux'un kapatılma zamanı

Örneğin, yukarıda yazılı zamanlarda bilgisayarı kullandığınızı hatırlamıyorsanız veya bilgisayara çok geç bir zamanda girildiği ekranda gözüküyorsa,

Linux'un izinsiz olarak kullanıldığı ihtimali yüksektir.

ÖRNEK: top Komutu

CPU ve belleğin kontrolü

```
top
```

Mesaj

```
[root@ie root]# top
 14:47:01  up 27 min,  3 users,  load average: 0.24, 0.08, 0.02
79 processes: 78 sleeping, 1 running, 0 zombie, 0 stopped
CPU states:  cpu    user    nice  system    irq  softirq  iowait    idle
           total    0.0%    0.0%    0.0%  33.2%    33.4%   33.3%    0.0%
Mem:   482180k av,  282700k used,  199480k free,       0k shrd,   32180k buff
       49892k active,               207952k inactive
Swap:  979956k av,       0k used,  979956k free                  147148k cached

  PID USER     PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME CPU COMMAND
 2858 root      16   0 12380  12M  7812 S     1.9  2.5   0:05   0 gnome-terminal
 2687 root      15   0 47620  14M  4736 S     1.7  3.0   0:10   0 X
 2942 root      17   0  1096  1096  888 R     0.3  0.2   0:00   0 top
    1 root      16   0   420   420  360 S     0.0  0.0   0:03   0 init
    2 root      15   0     0     0    0 SW    0.0  0.0   0:00   0 keventd
    3 root      15   0     0     0    0 SW    0.0  0.0   0:00   0 kapmd
```

Buffer Overflow'ın (Geçici bellekteki taşma) durumunu belleği kontrol ederek öğrenebiliriz. Yukarıdaki mesaj beş saniye içinde yenilenir.

Örnek :Portun Kontrolü

netstat –a

Mesaj

```
[root@ie root]# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:32770                 *:*                     LISTEN
tcp        0      0 ie.masuda.com:32771     *:*                     LISTEN
tcp        0      0 *:netbios-ssn           *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
tcp        0      0 *:http                  *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
```

Hangi portun açık olduğunu görürüz. Gereksiz bir port açık ise o portu kapatmalıyız. Portları açıp kapamale ilgili uygulamalar diğer modülde anlatılacaktır.

Örnek: Özel Dosya İzni

Program ve komutların kullanılması için Linux'ta kullanıcı(user) ID kullanılır. Bununla beraber SUID (SetUserID) ve SGID (SetGroupID) bayrağı dosya izninde ayarlanır.

Bu durumda user ID (kullanıcı ID) kullanılmaz. Kullanıcı dosyasındaki user ID veya group ID kullanılarak program çalıştırılır. Buna örnek olarak "passwd" komutunu verebiliriz.

Genel kullanıcı "passwd" komutunu çalıştırır.

Root kullanıcı dosyası ("/usr/bin/passwd"). Ve SUID bayrağı set (ayarlanır) edilir.

Yukarıdaki ayarlardan dolayı bu geçici root olarak kullanılır.

Şifre değiştirilir.

"/usr/bin/passwd" bitirilir, ve ID root'tan genel kullanıcıya döner.

Genel kullanıcının geçici olarak root olması ve programın çalıştırılması sorun oluşturur. Başka bir ifadeyle genel kullanıcı root'a girmek için "su-" komutunu kullanmaz. Bundan dolayı genel kullanıcı root olarak dikkate alınmaz.

Bu durumda SUID ve SGID bayraklarının set edilmesi tehlikelidir.

Aşağıdaki alıştırma SUID ile ilgilidir.

- **Dosyanın bulunması**

İlk olarak hangi dosyanın SUID bitinin set edildiği kontrol edilir. Bu bilgiye "find" komutuyla ulaşırız.

find / -perm +4000

Mesaj

```
 [root@ie /]# find / -perm +4000
/usr/X11R6/bin/XFree86
/usr/sbin/usernetctl
/usr/sbin/userhelper
/usr/sbin/userisdnctl
/usr/sbin/suexec
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/rcp
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/at
/usr/bin/sudo
/usr/bin/crontab
/usr/bin/lppasswd
/usr/bin/kon
/usr/bin/newvc
/usr/libexec/openssh/ssh-keysign
/bin/ping
/bin/ping6
/bin/traceroute6
/bin/mount
/bin/umount
/bin/su
/bin/traceroute
/sbin/pam_timestamp_check
/sbin/pwdb_chkpwd
/sbin/unix_chkpwd
```

Yukarıda görülen çıktıdaki "/usr/bin/passwd" daha önce anlatılmıştı.

- **İznin kontrolü**

"/usr/bin/passwd" izin kontrol edilir.

```
ls –l /usr/bin/passwd
```

Mesaj

```
[root@ie /]# ls -l /usr/bin/passwd
-r-s--x--x    1 root     root        18992 Jun  6  2003 /usr/bin/passwd
```

"s" biti kesinlikle eklenir.

- SUID Bitinin Çıkarılması

SUID biti ileride anlatılacak problemden dolayı çıkarılır.

```
chmod –s /usr/bin/passwd
```

- İznin Tekrar Kontrolü

```
ls –l /usr/bin/passwd
```

Mesaj

```
[root@ie /]# ls -l /usr/bin/passwd
-r-x--x--x    1 root     root        18992 Jun  6  2003 /usr/bin/passwd
```

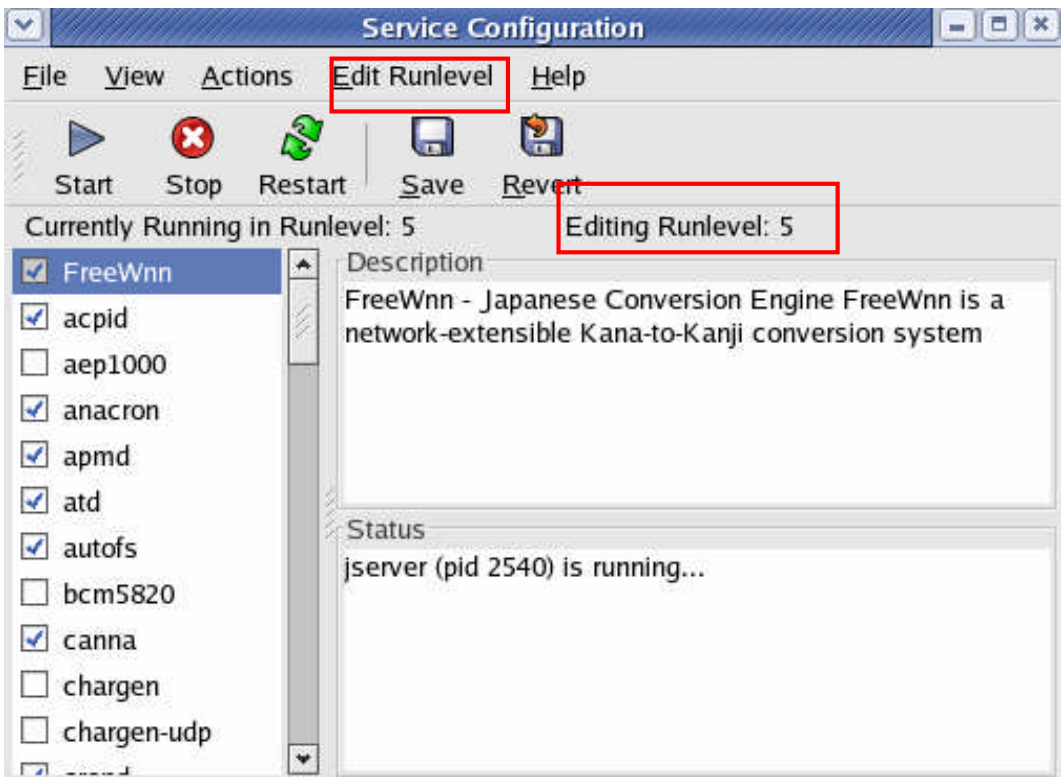
"s" biti kesinlikle silinir.

Örnek: Run Level'ın Ayarlanması

Run level Linux'ın işlem modudur. Yedi çeşit run level modu vardır. Numerik değere göre işlem değişiktir.

Run level	Anlamı
0	Kapatma
1	Tek kullanıcı modu (sadece root için)
2	Birden çok kullanıcı modu (Network kullanılmaz)
3	Normal birden çok kullanıcı modu (text log in)
4	Kullanılmaz
5	Birden çok kullanıcı modu (Grafiksel log in)
6	Sistemin yeniden başlatılması

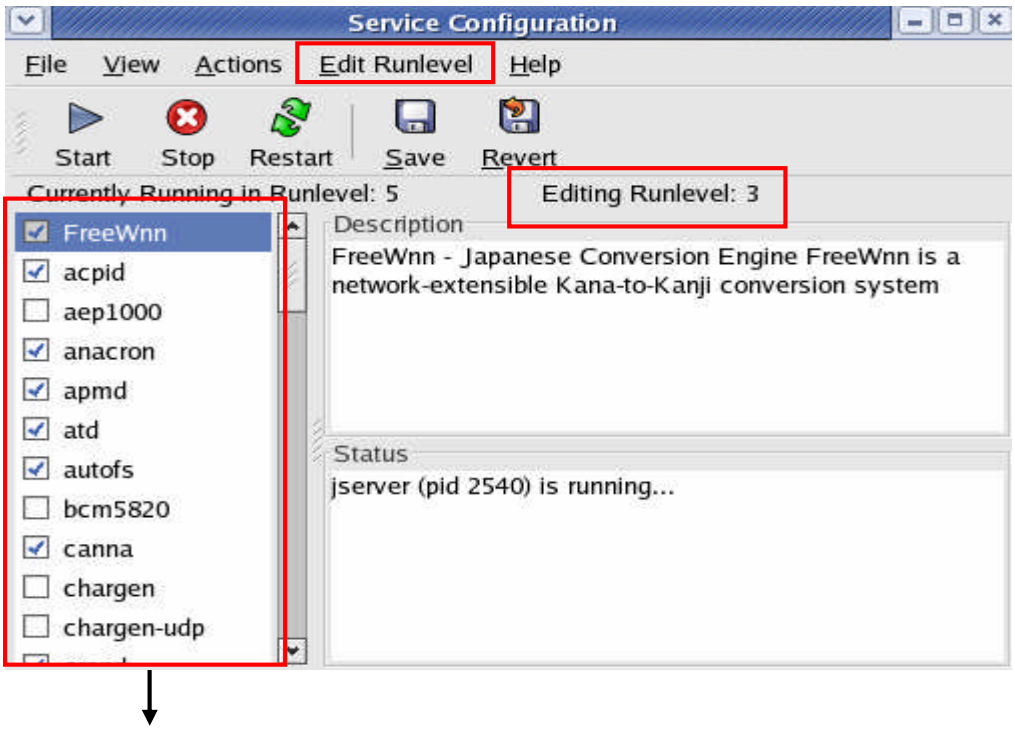
Run level 5



Şekil.1.8:Run Level 5

Text log in ve grafiksel log in (Run level 3 ve 5) beraber kullanıldığı için aynı içerikli set edilmesi gerekir.

Run level3



Şekil.1.9:Run Level 3

Her ikisi için de daemon ayarlaması(set edilmesi) aynı olmalıdır.

Örnek: X daemon'ın Set Edilmesi

X çalışmasa bile sunucu çalışabilir. Bu durum bir güvenlik boşluğuna yol açabilir. Bu bölümde x daemon'ı durdurmayı öğreneceğiz.

- **Konfigürasyon dosyasında değişiklik**

vi /etc/inittab

```
# inittab    Bu dosya INIT işleminin sistemi belirli
        bir run-level'da nasıl ayarlaması gerektiğini anlatır.
#
# Author:       Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
#               Modified for RHS Linux by Marc Ewing and Donnie Barnes
# Run xdm in runlevel 5
# x:5:respawn:/etc/X11/prefdm -nodaemon
```

Bu satır açıklamayla bitirilir.

- **Log in kontrolü**

Bilgisayar yeniden başlatılır ve text log in'e girilir.

- **Xwindow hakkında**

Xwindow'u başlatmak için aşağıdaki komut uygulanır.

```
startx
```

- **CUI'ya dönüş**

CUI'ya dönüş için aşağıdaki komut uygulanır

```
Logout
```

UYGULAMA FAALİYETİ

Aşağıdaki işlem basamaklarına göre uygulama faaliyetini yapınız.

- Güvenlik nedeniyle şifrenin düzenli olarak değiştirilmesi gerekir. “chpasswd” komutuyla Server yöneticisi olarak “chpasswd” komutuyla kullanıcı şifrelerini değiştiriniz.

İşlem Basamakları	Öneriler
➢ root’a giriniz. ➢ Üç kullanıcı belirleyiniz. User (kullanıcı) passwd(şifre) turkey1 tokyo1 turkey2 osaka2 turkey3 nagoya3 ➢ Şifre dosyası oluşturunuz. vi pass.txt turkey1:japan1 turkey2:international turkey3:cooperation ➢ Şifre veriniz. Şifre verilirken komut aşağıdaki şekilde uygulanır. Chpasswd < pass.txt ➢ Şifreleri kontrol ediniz. İlk olarak root’dan çıkılır. Sonra üç kullanıcıya ait şifrelerle bilgisayara girilip girilemeyeceği kontrol edilir. ➢ Kullanıcıları siliniz. Belirlediğimiz üç kullanıcıyı silelim.	➢ İşlem basamaklarının 2.adımında oluşturulacak kullanıcılar işletim sisteminde Uygulamalar – Sunucu Ayarları – Kullanıcılar ve Gruplar sırası takip edilerek oluşturulacaktır. ➢ İşlem basamaklarının 3.adımında oluşturulacak kullanıcılar pass.txt dosyasına yazılacaktır. ➢ Komutları uyguladıktan sonra hata mesajları alırsanız yazdığınız komutları tekrar kontrol edin. Yazım yanlışlıklarına dikkat edin.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki soruları doğru yanlış şeklinde cevaplayınız.

1. last komutu kullanılarak bilgisayara giren kullanıcıların isimleri ve Linux'ın başlama zamanı görüntülenir.

2. Saldırganlar port taraması yaparak bir bilgisayarda hangi portların açık olduğunu bulabilirler.

3. Saldırganlar kendilerini gizlemek için başka bilgisayarlara ulaşıp bu bilgisayarları tuzak olarak kullanırlar.

4. netstat –a | more komutu uygulanarak bilgisayarımızdaki kullanımda olan port numaralarını görebiliriz.

5. Server'a mail göndermek için POP3 protokolü kullanılır.

6. Server'dan mail almak için SMTP protokol kullanılır.

7. chmod 000 /usr/bin/gcc komutuyla gcc'ye kullanım izini verilir.

8. top komutuyla CPU ve belleğin kontrolü yapılır.

9. Efektif hostname ve IP adresi internetten ping taramasıyla elde edilir.

10. Saldırgan, bir bilgisayarın internete bağlı olup olmadığını ping komutuyla öğrenir.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete geri dönerek tekrar inceleyiniz.

ÖĞRENME FAALİYETİ–2

AMAÇ

Telnet ve uzaktan kontrol sunucusu kurulumunu hatasız olarak yapabileceksiniz.

ARAŞTIRMA

- İnternette bilgilerin kodlanarak gönderilmesi ile oluşturulan güvenlik tünelinin hangi amaçlarla kullanıldığı konusunda bir araştırma yapınız.

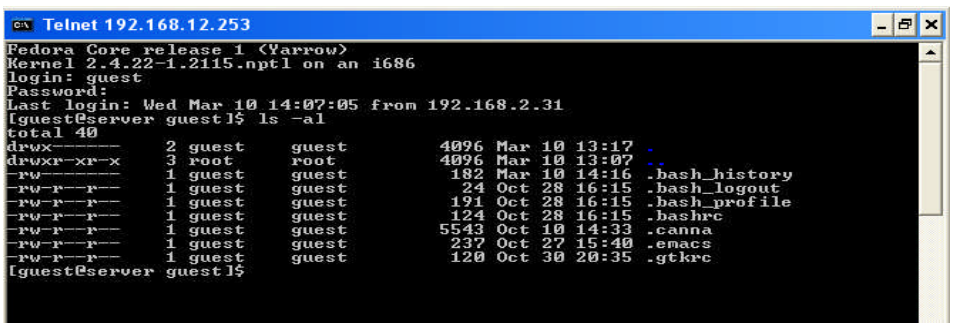
2. TELNET

2.1. HTTP protokolü

Bir web sitesine erişilmek istendiği zaman, erişim isteği web sunucuya gönderilir ve cevap olarak veri sunucu tarafından tarayıcıya geri döndürülür. Browser kullanılırken istek yapıldığında HTTP isimli bir protokol tarafından veri taşınır. Bu protokol veri temelli erişim için bir örnektir.

2.1.1. Telnet hakkında

Telnet, internet ağı üzerindeki çok kullanıcılı bir makineye uzaktaki başka bir makineden bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan programlara verilen genel isimdir. Bağlanılan makineye girebilmek (login), orada bir kullanıcı isminin (user name) ve bağlantının gerçekleşebilmesi için bir telnet erişim programının olması gereklidir. Telnet erişim programları, günümüzdeki işletim sistemlerinin çoğunda birlikte gelmektedir. Çok kullanıcılı işletim sistemleri (UNIX vb.) genellikle kullanıcılara metin tabanlı bir arayüz sunar ve bu sistemlerde tüm işlemler klavye vasıtası ile komut isteminden (command prompt) gerçekleştirilir.



Şekil.2.1: Telnet Login

Telnet programı ile sanal sunucunuza (virtual server) bağlandığınızda, uzaktan UNIX işletim sistemine bağlanmış olursunuz. Bu, UNIX komutları yazabileceğiniz, programları çalıştırabileceğiniz, sanki makinenin karşısında oturuyormuş gibi web sitenizi düzenleyebileceğiniz anlamına gelir.

Telnet güvensiz bir protokoldür. Telnet protokolü kullanıcı adı (username) ve şifrenizi (password) bağlı bulunduğunuz ağda kolaylıkla görebilecek bir format olan PLAIN TEXT (düz metin) düzeninde göndermektedir. Bu kullanıcı isminizin ve şifrenizin ağı dinleyen herhangi biri tarafından kolaylıkla görülebileceği anlamına gelir.

Eğer üzerinde herhangi bir Windows işletim sistemi yüklü bir makineden Telnet ile bağlantı gerçekleştirmek istiyorsanız sırayla şu işlemleri gerçekleştirmelisiniz.

- Başlat (Start) -> Çalıştır (Run) menüsünü çalıştırın.
- Komut satırına "telnet" komutu ile birlikte bağlanmak istediğiniz makinenin ip adresini veya hostname' ni yazarak "ENTER" tuşuna basınız.
- Eğer adresi doğru girdiyseniz bu işlemden sonra karşınıza komut satırı gelecektir.
- Kullanıcı adını (login) ve kullanıcı şifrenizi girdikten sonra artık sunucuya bağlanmış olursunuz.

Artık istediğiniz UNIX komutlarını rahatlıkla çalıştırabilirsiniz.

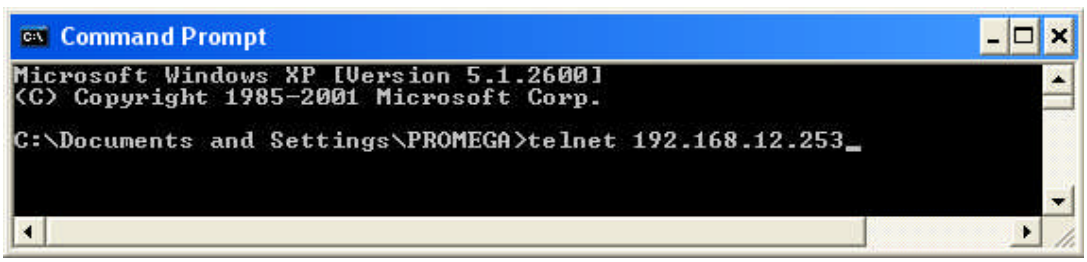
2.1.2. Telnet ile HTTP Protokol

Eğer Telneti kullanırsak, diğer bilgisayarlara character data gönderip alabiliriz. Burada, character data WWW Server'a gönderilmiştir. Ayrıca WWW Server'ın ne reaksiyon gösterdiğini gözlemleyebiliriz.

ÖRNEK: Telnet ile HTTP protokol

- Uygulama server'ına bağlanın.

telnet 192.168.12.253

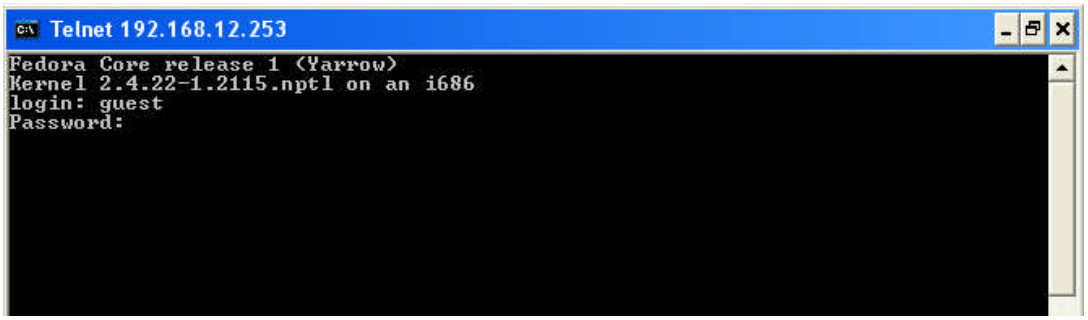


Şekil.2.2: Telnet ile IP Adresin Kullanılması

➢ Server'a Login olunuz.

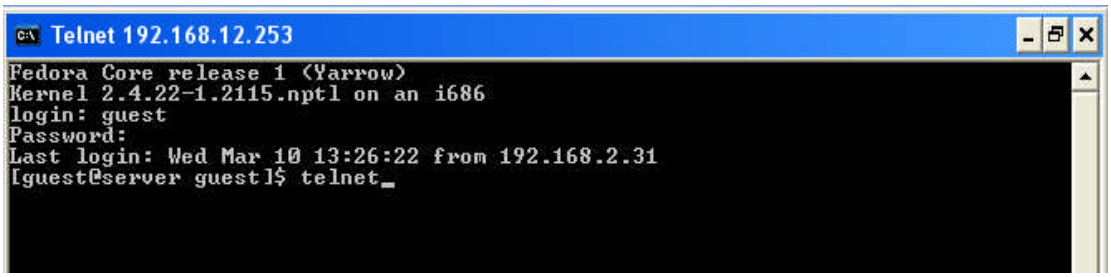
username guest

password guest01



Şekil.2.3:Telnet ile login olunması

➢ "Telnet" daemonı açınız



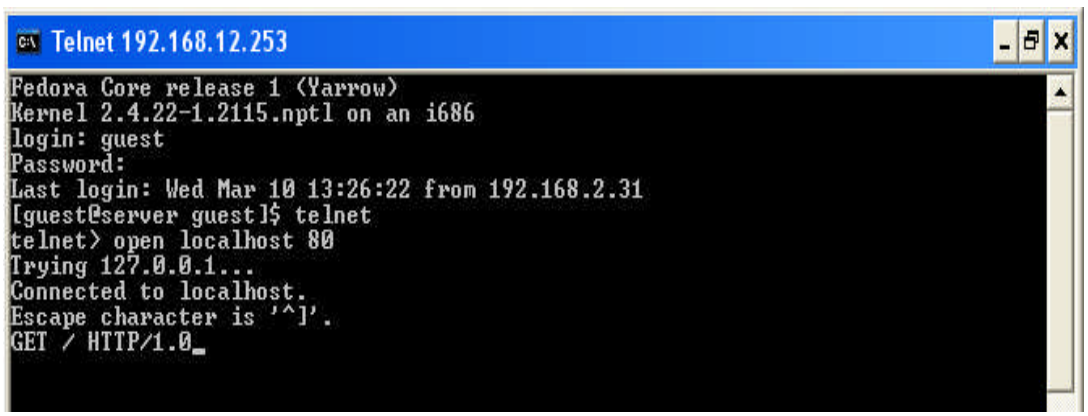
Şekil.2.4:Telnet daemonın açılması

➢ Web sunucuya bağlanınız.

open localhost 80

Burada, localhost ve 192.168.12.253 IP numarası aynı anlamdadır.

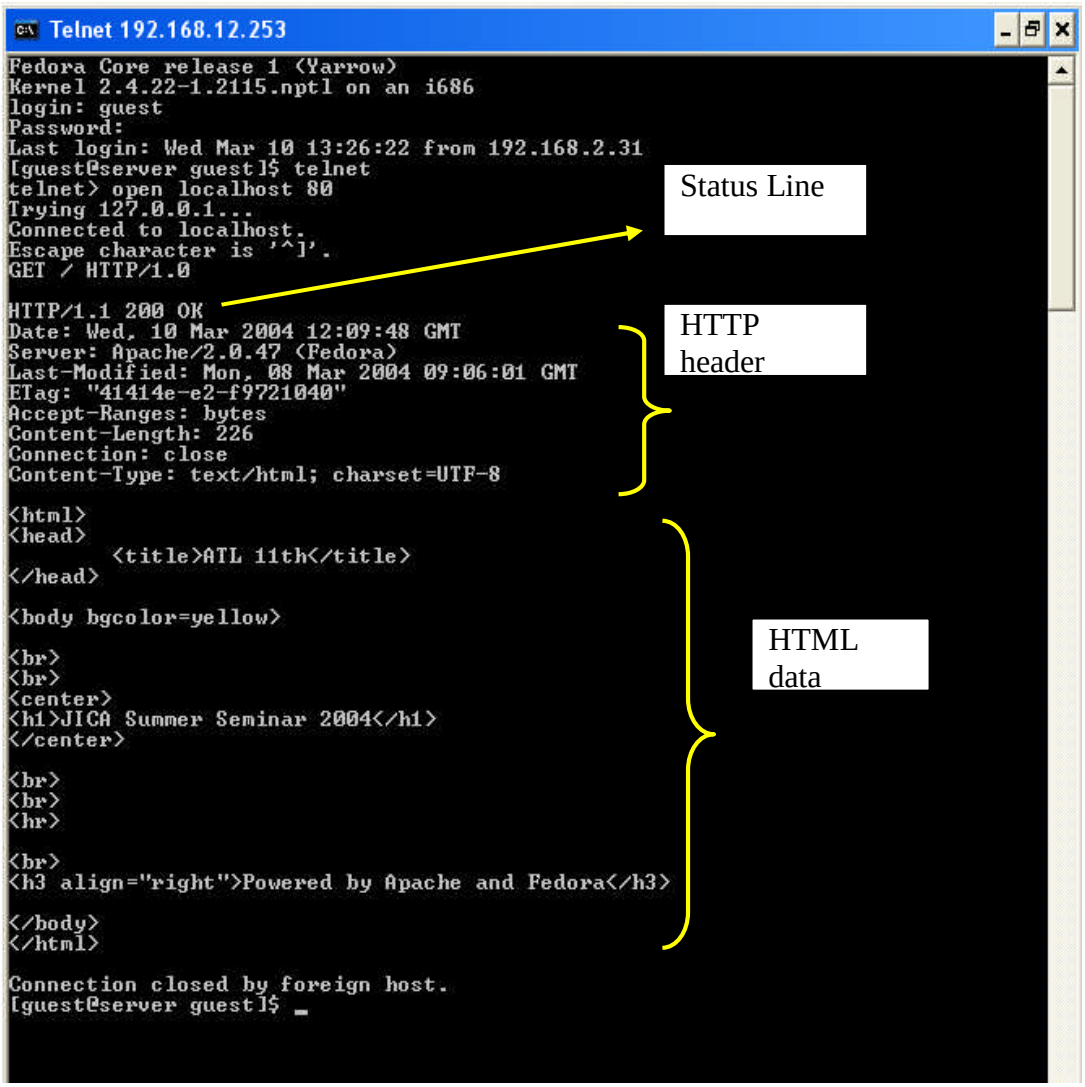
GET / HTTP/1.0



Şekil.2.5:Telnet ile Web Server'a bağlantı

Yazınız ve iki defa **enter** tuşuna basınız. (return)

- Web verisini görebiliriz.



Şekil.2.6:Telnet ile index.html sayfasının görüntülenmesi

İlk önce, istek Telnetten Web Server'a gönderilmiştir ve Web Server gelen isteği içeriğine göre işler. Sonuç Telnete geri gönderilir. Bu HTTP terminolojisinde "yanıt" olarak adlandırılır. Kolay olmasına rağmen HTTP ve Telnet Web Server'ın ilkel bir uygulamasıdır. Böyle bir operasyon modeli Client/Server model (C/S model) olarak adlandırılır. Bu yüzden, HTTP'nin temel mekanizması C/S modeldir denilebilir.

Yukarıdaki şekli incelersek,

<html>'den </html>'e, "Entity" olarak isimlendiririz. Bu bölümde web sayfasında görüntülenecek bilgiler (resimler, metinler, linkler vb.) bulunur.

İsteğin anlamı

"GET"

Okuma sayfasının anlamını gösteren komuttur. Bu komut HTTP içerisinde bir metot olarak kullanılır ve buna isteğin ilk satırında karar verilir. ("/") Okunan dosyanın belirleyici özelliklerinden biridir. Root dizini ifade edilir. Web server'a bir istek geldiği zaman kontrol edeceği ilk yer root dizini altındaki /var/www/html dizinidir.

Örneğin index.html, default.htm vb. "HTTP/1.0"

HTTP protokolünün versiyon numarasıdır. 0.9, 1.0 ve şimdi kullanılmakta olan 1.1 HTTP'nin versiyonlarıdır. 1.0 günümüzde kullanılan 1,1'e göre daha basittir.İstekten sonra bir boş satır vardır. Bu, isteğin sonunu gösterir. Sonraki takip eden bölüm serverdan gelen bir yanıttır.

Yanıtın anlamı

İlk satır, durum satırıdır. Bu işlem sonucunun normal olup olmadığını gösterir. Bunun formatı HTTP sürümünü, durum kodunu ve sonucunu gösteren bir karakter grubudur. Üç karakterden oluşan durum koduna karar verir ve sol taraftaki digitten itibaren ana hatları anlatır. Bir hata oluştuğu zaman, Şekil.2.2'de gösterildiği gibi görüntülenir. Bu numara durum kodudur. HTTP başlığı aşağıdaki satırdan itibaren başlar. Başlık alanının anlamı için Tablo.2.3'e bakınız.Bundan sonra, boş bir satır vardır. Bu satır yanıt bilgisinin sonunu gösterir. Son bölüm HTML datadır. Browser tarafından Web Server'a eriştiğimiz zaman, bu bölüm HTML kodların rolüne göre ekranda gösterilir (Şekil.2.6).

- **logout**

Method	Açıklama
GET	Bilgi server dışından alınır.
HEAD	Hemen hemen GET ile aynı anlamdadır. Bununla birlikte, HTTP başlığı geri gönderilmesine karşın datanın içerikleri geri gönderilmez.
POST	Data istemciden sunucuya iletilir.
OPTIONS	İletişim seçeneği bildirildiği zaman o kullanılır.
PUT	Dosya server üzerinde değiştirilir. Belirtilen dosya varolmadığı zaman, dosya yeniden yapılır.
DELETE	Dosya server üzerinde silinir.
TRACE	Server tarafından alınan istek satırı ve başlık istemciye geri gönderilir.

Tablo.2.1 HTTP Method (Ana bölümler)

Kod değeri	Açıklama
1xx	İşlemlerin geçiş konumları vb. bildirilir.
2xx	Normal bitiş.
3xx	Gerekli bazı uygulamaları gösterir.
4xx	İstemci tarafında problem var.
5xx	Server tarafında problem var.

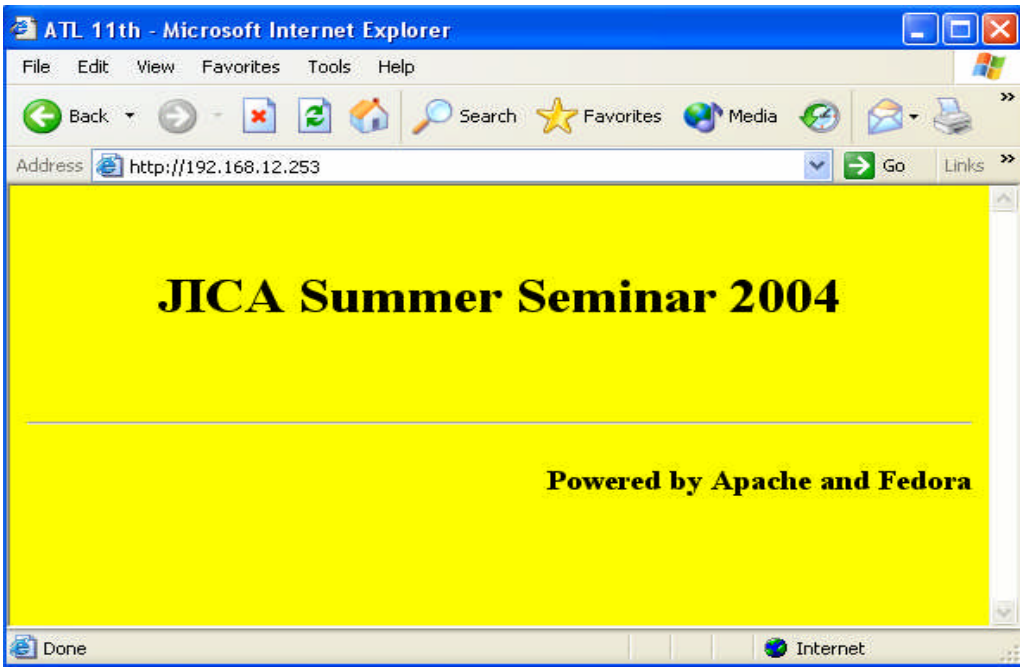
Tablo.2.2 HTTP durum kodu

Başlık ismi	Açıklama
Date	İstek ve yanıt yapıldığı zamanki tarih.
Pragma	cash of data izin verildi mi yoksa izinsiz mi?
Cache-Control	control cash için bilgi.
Connection	Yanıttan sonra TCP iletişiminin devam edip etmediğini gösterir.
Transfer-Encoding	Mesajın içeriğinin çözümleme metodu
Upgrade	HTTP/1.1.'den başka protokollere değiştirir.
Via	Geçen Proxy ve gateway kaydedilir.
Location	Bilginin doğru yeri olarak gösterilir. Bilginin pozisyonu tam ismiyle belirtilir.
Server	Server isminin ve verisyonunun bilgisidir.
WWW-Authenticate	İstenilen kısıtlı bilgiye erişildiği zaman, data yetkili user için geri gönderilir.
Accept-Ranges	Dosyanın bir bölümü server tarafından istenip istenmediği kontrol edilir.
Age	cached data'nın eski olup olmadığına karar verir.
Proxy-Authenticate	WWW kadar doğrular. Proxy, istemci bilgisayara iletir.
Public	Hangi serverın belirtilen istemciyi kabul edebildiğini gösteren metodun listesidir.

Retry-After	Server, servisi yeniden başlatma zamanını belirtir.
Vary	Dil kodu ve karakter kodunun iki veya daha fazla formuna izin verildiği zaman, sunucular arasından hangisinin seçildiği ifade edilir.
Warning	Yanıtın durumuyla ilgili uyarıdır.
Allow	Metodun uygulanabilirliği gösterilir.
Content-Encoding	Sıkıştırma işlemi çözümü entity'e verildiği zaman metod gösterilir.
Content-Length	Entity'nin uzunluğu gösterilir.
Content-Type	Entity'nin datası ve türünü gösterir.
Expires	Entity süresinin dolma tarihi olarak gösterilir.
Last-Modified	Son update tarihi ve zamanının bilgisi.
Content-Language	Entity'nin dili gösterilir.
Content-Location	Entity'nin sunucu üzerinde nereye konulduğunu gösterir.
Content-MD5	İletişim hatalarını bulmak için kullanılır.
Etag	browser'ın cash'i olarak kullanılır.

Tablo.2.3 HTTP başlığı

Şekil.2.7: Hata mesajı



Şekil.2.8: Erişim sonucu

2.2. SSH Server

2.2.1. SSH Server'ın Genel Hatları

2.2.1.1. SSH Kullanımı

SSH (Secure Shell) bilgisayara güvenli bir şekilde uzaktan erişim için kullanılan bir araçtır. SSH'in birçok fonksiyonu vardır. Aşağıda SSH'e ait temel fonksiyonlar açıklanmıştır.

- **Uzaktan erişim (Remote Login)**

Kullanıcılara ait bilgiler(username and password) ve iletişim bilgileri kodlanır. Böylece uzaktan güvenli erişim mümkün hale gelir.

- **Bir bigisayardan diğer bilgisayara ait programın çalıştırılması**

Yerel bilgisayardan uzaktaki bir bilgisayara (SSH sunucu) ait program çalıştırılır ve sonuç yerel bilgisayarda görüntülenir.

- **Dosya Transferi**

Dosya güvenli bir şekilde transfer edilir. SSH "ftp" komutu yerine kullanılabilir.

- **TCP/IP port sevki (TCP/IP port forwarding)**

Örneğin POP3 üstündeki şifre networkte kodlanmadan iletilir. Eğer SSH tüneli kullanılırsa şifre kodlanabilir.

➢ **Public Key kriptosistem kullanılarak güvenli kontrol**

SSH'te, kodlama tekniği olarak " Public key kriptosistem " kullanılabilir. Kontrol; genel anahtar(public key) ve gizli anahtar(secret key) kullanılarak yapılır.

2.1.1.2. SSH Çeşidi

Genelde kullanılan SSH çeşitleri aşağıda belirtilmiştir.

SSH — SSH şirket ürünü

Open SSH — Açık Kaynak

➢ SSH

Ticari ve ticari olmayan iki çeşidi vardır.

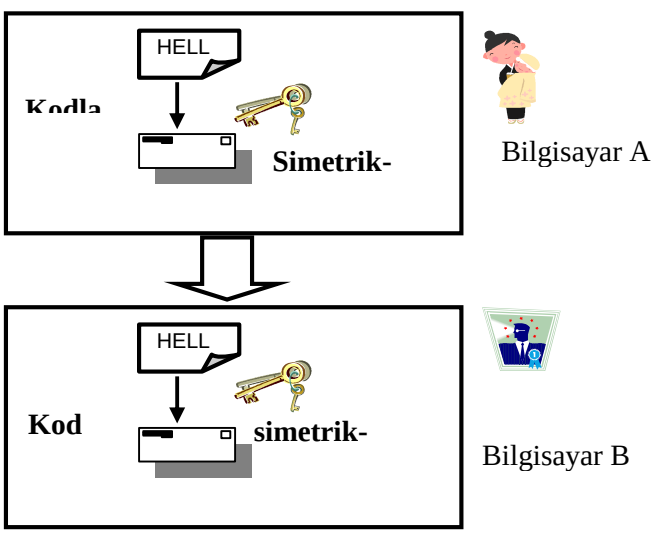
➢ OpenSSH

Açık kaynak SSH'tir. Linux'ta standart bir SSH mevcuttur. OpenSSH bu kitapta işlenmiştir.

2.2.1.3. SSH'teki Kodlama Teknolojisi

2.2.1.3.1. Genel Anahtar Sistemi

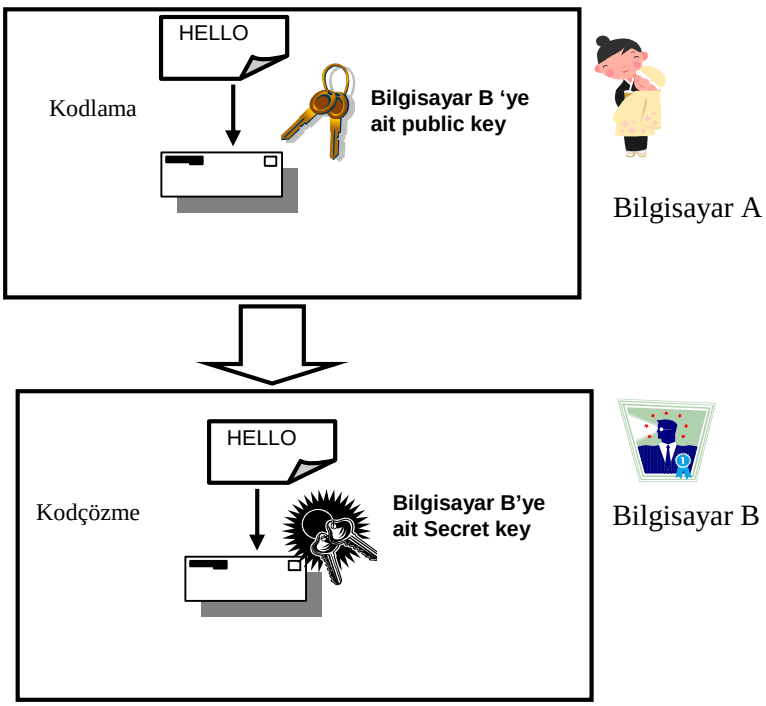
SSH'te kullanılan kriptografik teknolojiye Public key kriptosistemi denir. Daha önce kullanılan kodlama teknolojisine ise genel anahtarlama sistemi denmektedir. Bu sistemde bilgiyi kodlayan ve kodu çözen kişi aynı anahtara sahiptir. Bu teknolojide güvenlik yeterli değildir.



Şekil.3.1:Genel anahtar sistemi

2.2.1.3.2. Public Key Kripto Sistem

"genel anahtar(public key)" ve "gizli anahtar (secret key)" kullanılır. Bu bir çift anahtardır. Kodlama "public key " 'le yapılır ve "secret key" 'le kod çözülür.



Şekil.3.2:Public key kriptosistem

2.2.1.4. SSH'e Ait Haberleşme Mekanizması

SSH kullanıldığında uygulanan kontrol ve haberleşme prosedürü aşağıda belirtilmiştir.

- Host Kontrolü
- Kullanıcı Kontrolü
- Kodlanan Haberleşme

Host SSH severa bağlandığı zaman hosta ait bağlanma izninin olup olmadığına bakılır. Host kontrolünde "public key kriptosistem" kullanılır. Host kontrolü bittiğinde random sayı tarafından genel bir anahtar yapılır. Genel kodlama sistemi tarafından yapılan kodlamadan sonra haberleşme kurulur.

Kullanıcı kontrolünde "şifre kontrolü" veya "public key kriptosistem" kullanılır. "şifre kontrolü" kullanılsa dahi haberleşme kodlanır. Böylece bir kullanıcının hesabına ait bilgilerin kullanılma ihtimali düşüktür.

2.2.2. SSH ile Uzaktan Bilgisayara Erişim

2.2.2.1. Kullanıcı İsmi ve Şifre ile Erişim

ÖRNEK: Kullanıcı İsmi ve Şifre İle Erişim

Bu alıştırmada kullanıcı bilgilerini kullanarak SSH sunucusuna erişim methodunu öğreneceğiz. Metod “telnet” ‘in hemen hemen aynısıdır. Fakat bütün bilgiler kodlandığı için güvenlik yüksektir.

- **Erişim kontrolü**

"sshd" ,TCP Wrapper’a (libwrap) ait bir kütüphaneye sahiptir. Bu özellik sayesinde erişim kontrolü aşağıdaki dosyalarla yapılır.

/etc/hosts.allow

/etc/hosts.deny

Bu alıştırmada bütün bilgisayarlara(hostlar) "sshd" ile bağlantı izni verilir.
vi /etc/hosts.allow

```
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
sshd: ALL
```

- “sshd” yeniden başlatılır.
- "ssh" komutuyla Log in yapılır.

Komutun formatı aşağıda gösterilmiştir.
ssh -l <user name> <host name>
ssh -l yoichi ie

Mesaj

```
[root@ie root]# ssh -l yoichi ie
The authenticity of host 'ie (127.0.0.1)' can't be established.
RSA key fingerprint is 61:5d:f1:b5:80:42:d5:f0:0e:39:8c:7f:48:18:78:09.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ie' (RSA) to the list of known hosts.
yoichi@ie's password:
/usr/X11R6/bin/xauth:  creating new authority file /home/yoichi/.Xauthority
[yoichi@ie yoichi]$
```

The authenticity of host 'ie (127.0.0.1)' can't be established.
Bu hostun lokalhost kısmında kaydedilmediği belirtilmektedir.
RSA key fingerprint is 61:5d:f1:b5:80:42:d5:f0:0e:39:8c:7f:48:18:78:09.
Public anahtara ait parmak izini belirtir. Anahtarda meydana gelen herhangi bir tahrifat bu numarayla kontrol edilebilir.

Are you sure you want to continue connecting (yes/no)? yes
"yes" denildiği zaman hosta ait public anahtar aşağıda gösterilen dosyaya kaydedilir.
~/.ssh/known_hosts

Bundan sonraki uygulamalarda host kontrolü bu public anahtarla yapılır.
Warning: Permanently added 'ie' (RSA) to the list of known hosts.
yoichi@ie's password:
[yoichi@ie yoichi]$
Password sunucuya kaydedildiği zaman Log in işlemi bitmiştir.

- Log out

Exit

- Yeniden Log in

ssh -l yoichi ie

İkinci defa Log in yapılacağında sadece password yazılır.(Hosta ait public anahtarı daha önceden kaydedilmişti.)

Mesaj

[root@ie root]# ssh -l yoichi ie
yoichi@ie's password:
[yoichi@ie yoichi]$

2.2.2. Public Key Kriptosistem ile Login

ÖRNEK: Public Key Kriptosistem ile Log in

Public Key Kriptosistem uzaktan daha güvenli Log in(erişim) yapmak için gereklidir. Public Key Kriptosistemde kontrol bir çift anahtarla yapılır.

- Public anahtar
- Secret anahtar

NOT: Public Anahtar Kriptosistem İle Kontrolün Ana Hatları

Server public anahtarı "~/.ssh" dizininden alır. Sonra "random sayı" oluşturulur. Random sayı public anahtar tarafından kodlanır ve istemci bilgisayara gönderilir.

Kullanıcı istemci bilgisayar tarafından şifreyi girerek gizli (secret) anahtarı alır. Sunucu tarafından gönderilen Random sayının kodu secret anahtar tarafından kodu çözülür. Random sayı tekrar sunucuya gönderilir.

Herşeyden önce sunucu aşağıdaki değerleri okur. Server doğru kullanıcıyı bulmak için aşağıdaki iki değeri kontrol eder. Bu değerler sunucudaki değerlere karşılık geliyorsa erişime izin verilir.

Sunucunun oluşturduğu Random sayı

İstemci bilgisayarın kodunu çözdüğü Random sayı

- Public Anahtar ve Secret Anahtar Oluşturulması

İki anahtar "ssh-keygen" komutuyla oluşturulur.Komutun kullanımı aşağıda gösterilmiştir.

ssh-keygen -t <type>

İkinci adım olarak anahtar tipi tanımlanır.
rsa1SSH protocol For version 1 RSA1 authentication
rsaSSH protocol For version 2 RSA authentication
dsaSSH protocol For version 2 DSA authentication

Bu alıştırmada "rsa" kullanılarak anahtar çiftinin oluşturulmasını öğreneceğiz. İlk olarak username ile log in olunur.

ssh -l yoichi ie
Sonra "ssh-keygen" komutu kullanılarak anahtar çifti oluşturulur.

ssh-keygen -t rsa
Komut icra edilir ve mesaja göre "passphrase" uygulanır. Bunlardan sonra anahtar çifti oluşturulur.Oluşturulan secret anahtar kodlanır. Bundan dolayı secret anahtar çalınsa bile üçüncü bir kişi secret anahtarı kullanamaz.

Mesaj

[yoichi@ie yoichi]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/yoichi/.ssh/id_rsa): **(Enter tuşuna basın)**
Created directory '/home/yoichi/.ssh'.
Enter passphrase (empty for no passphrase): **(Şifrenizi yazın)**
Enter same passphrase again: **(Şifrenizi tekrar yazın)**
Your identification has been saved in /home/yoichi/.ssh/id_rsa.
Your public key has been saved in /home/yoichi/.ssh/id_rsa.pub.
The key fingerprint is:
ff:7c:66:37:17:09:ba:28:1f:db:6e:60:8e:ec:68:9e yoichi@ie.masuda.com

Anahtarın kaydedilmesi için dosyaya giriş
(/home/yoichi/.ssh/id_rsa):
Secret anahtarın kaydedildiği yer tanımlanır.. “Enter “ tuşuna basılır. Çünkü secret anahtar varsayılan olarak kaydedilen yerde saklanır.

Passphrase için Enter’ a basılır. (empty for no passphrase):
Aynı passphrase için yeniden Enter’ a basılır.
"passphrase" girilir.
Fingerprint anahtarı:
ff:7c:66:37:17:09:ba:28:1f:db:6e:60:8e:ec:68:9e yoichi@ie.masuda.com
"fingerprint" public anahtar için kullanılan değerdir.

- Anahtar Çiftinin Kontrolü

Anahtar çifti kontrolü yapılır.
ls -l .ssh

Mesaj

[yoichi@ie yoichi]$ ls -l .ssh/
total 8
-rw------- 1 yoichi yoichi 951 Nov 22 13:58 id_rsa
-rw-r--r-- 1 yoichi yoichi 230 Nov 22 13:58 id_rsa.pub

id_rsa	Gizli anahtar
id_rsa.pub	Açık anahtar

➢ Public anahtar kontrolü

Public anahtar bir text dosyasıdır ve içeriği kontrol edilebilir.
cat ~/.ssh/id_rsa.pub

Mesaj

```
[yoichi@ie yoichi]$ cat ~/.ssh/id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAtNfy24bP/RXLoX3bC7EE0Pd66a+J9Fglu7unruj
4Ze63B4BdbEXMJ3J9kanBXwbAVOUDh8N9nHNSPL/d9PBlJEA8SGrcfd6aELWQ0j5mb
6Y4bBBXPk0gf2y2MUaSqlg0A8o/NvflOaTOqivf8FQwyd9YnYnIP0JrxhrmNfrLJ/E=
yoichi@ie.masuda.com
```

➢ Public Anahtarın Kaydı

SSH servera public anahtarın kaydedilmesi gereklidir.
İlk olarak public anahtar hosta gönderilir.

scp ~/.ssh/id_rsa.pub yoichi@ie:

Mesaj

```
[yoichi@ie yoichi]$ scp ~/.ssh/id_rsa.pub yoichi@ie:
The authenticity of host 'ie (127.0.0.1)' can't be established.
RSA key fingerprint is 61:5d:f1:b5:80:42:d5:f0:0e:39:8c:7f:48:18:78:09.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ie' (RSA) to the list of known hosts.
yoichi@ie's password:
id_rsa.pub                    100%  230   238.9KB/s   00:00
```

Sonra SSH sunucuda public anahtar kaydedilir.
cat id_rsa.pub >> ~/.ssh/authorized_keys

➢ Dosya İzni Değiştirilir.

Dosyaya yazma ve okuma yetkisi sadece dosya sahibine verilir.

chmod 600 .ssh/authorized_keys
İzin kontrol edilir.

ls -l ~ /.ssh/

Mesaj

```
[yoichi@ie yoichi]$ ls -l ~/.ssh/
total 16
-rw-------  1 yoichi  yoichi  230 Nov 22 14:31 authorized_keys
-rw-------  1 yoichi  yoichi  951 Nov 22 13:58 id_rsa
-rw-r--r--  1 yoichi  yoichi  230 Nov 22 13:58 id_rsa.pub
-rw-r--r--  1 yoichi  yoichi  212 Nov 22 14:23 known_hosts
```

- Log out Yapılır

exit

- Log in Yapılır

Log in yapılmasının sebebi public anahtar kriptosistemi ile log in için yapılan hazırlık bitmiştir.

ssh -l yoichi ie

- Log out Yapılır

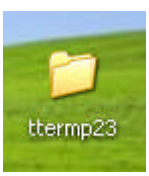
exit

2.2.3. SSH Kullanımı

2.2.3.1. Tera Term Pro + TTSSH

"Tera Term Pro" Windows'ta çalışan bir terminal emulator programıdır. "Tera Term Pro kullanarak SSH servera erişemeyiz. "TTSSH" (Tera Term SSH) SSH servera ulaşamak için geliştirilen bir modüldür. Bu programı internetten temin edebilirsiniz.

ÖRNEK 1.3. Tera Term Pro 'nun yüklenmesi ve temel ayarlarının yapılması



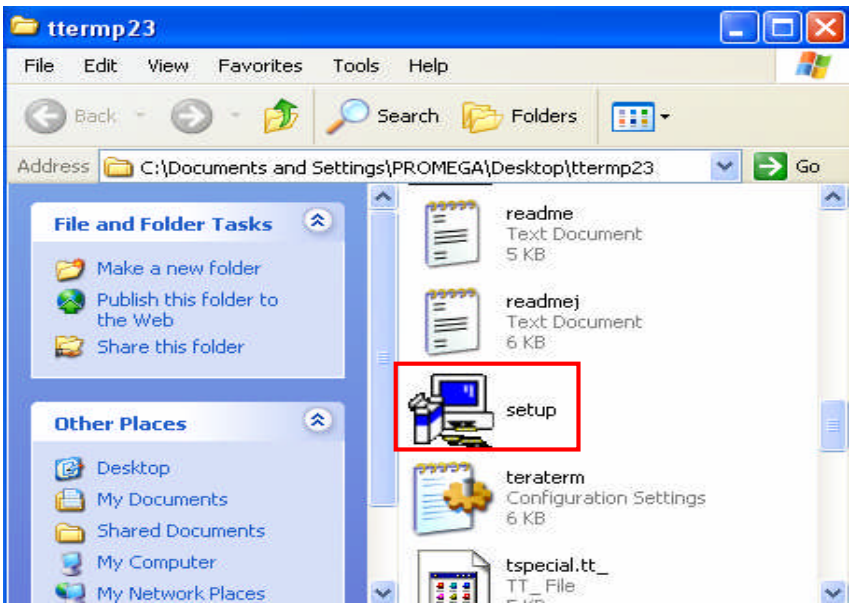
Şekil.3.3: ttermp23 dosyası

- Programın Yüklenmesi İçin Hazırlık Aşaması

"ttermp23" dosyası açılır.

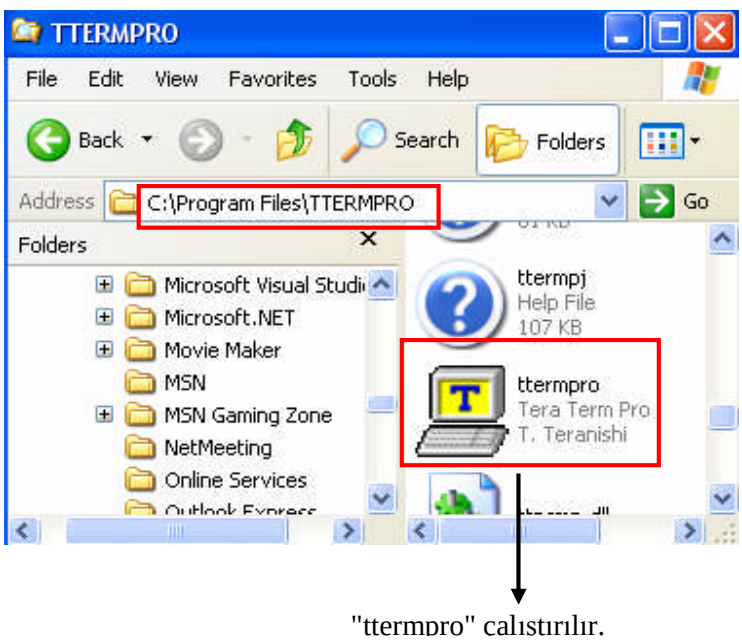
- Yükleme

"Setup.exe" 'ye yüklemenin başlatılması için çift tıklanır.



Sekil.3.4: ttermp23

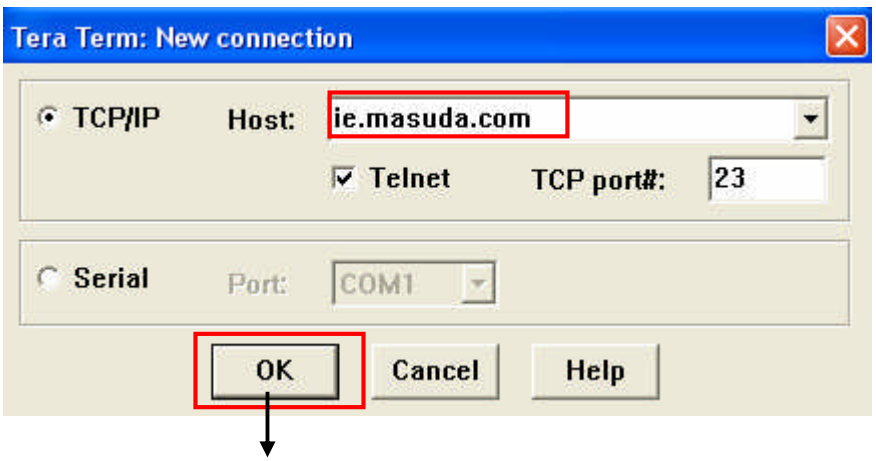
➢ **Programın çalıştırılması:** Çalıştırılacak program aşağıdaki dosyaya yüklenir. **C:\Program Files\TTERMPRO**



Şekil.3.5: ttermpro çalıştırılması

➢ **Bilgisayar ayarları yapılır**

Bilgisayar ayarı aşağıdaki şekilde gösterilmiştir.

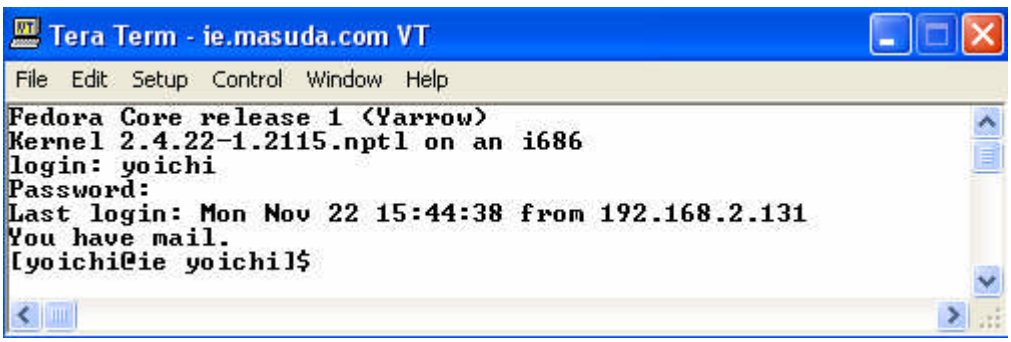


"OK" 'ye basın ve servera bağlanın.

Şekil.3.6: Server'la bağlantı kurulması

➢ **Log in(erişim)**

Kullanıcı ID'nizi uygulayarak erişimin yapılabildiğini kontrol ediniz.

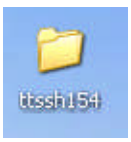


Şekil.3.7: Log in (erişim)

➢ **Log out (Çıkış)**

Logout

ÖRNEK: TTSSH'in yüklenmesi ve temel ayarları



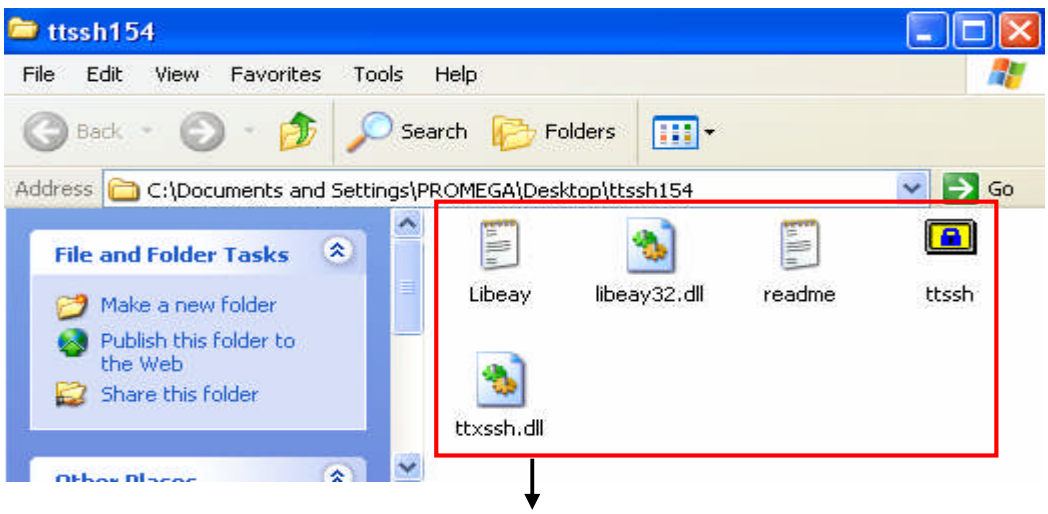
Şekil.3.8: ttssh154 dosyası

- Programın Yüklenmesi İçin Hazırlık Aşaması

"ttssh154" dosyası açılır.

- Yükleme ve Çalıştırma

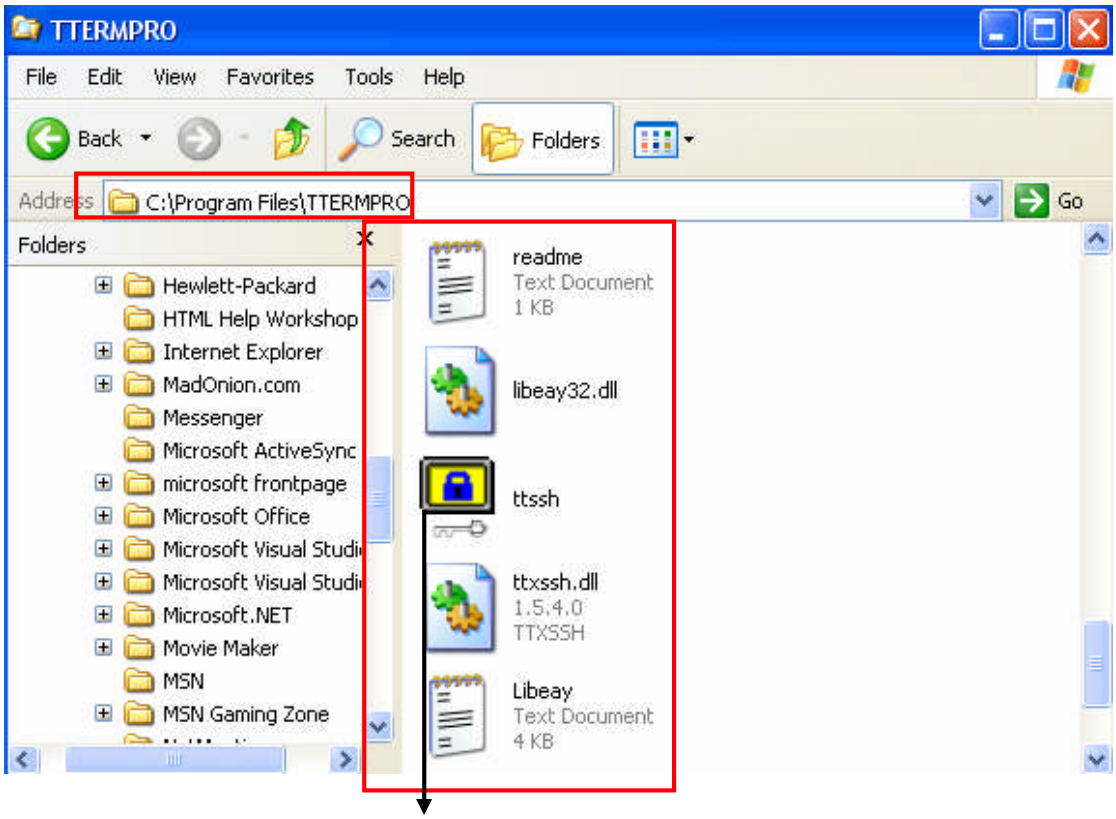
Aşağıdaki beş dosyanın olup olmadığını kontrol edin.



Bu dosyaları aşağıdaki dosyaya kopyalayın.

Şekil.3.9: ttssh154 dosyalarının kontrolü

C:\Program Files\TTERMPRO

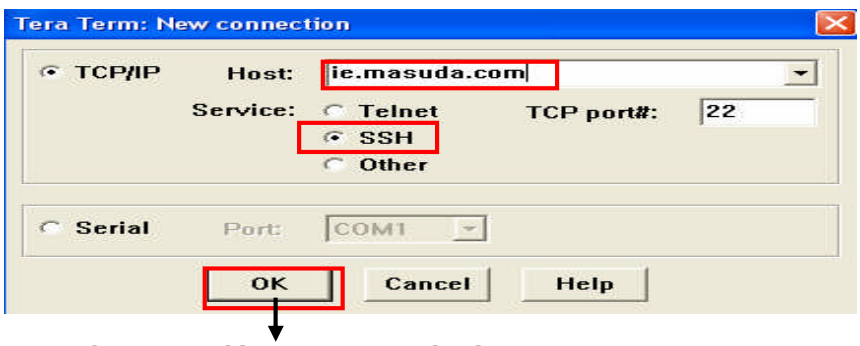


"ttssh.exe" 'yi çalıştırın.

Şekil.3.10: Dosyaların TTERMPRO klasörüne kopyalanması

3) Bilgisayar (host) Ayarları

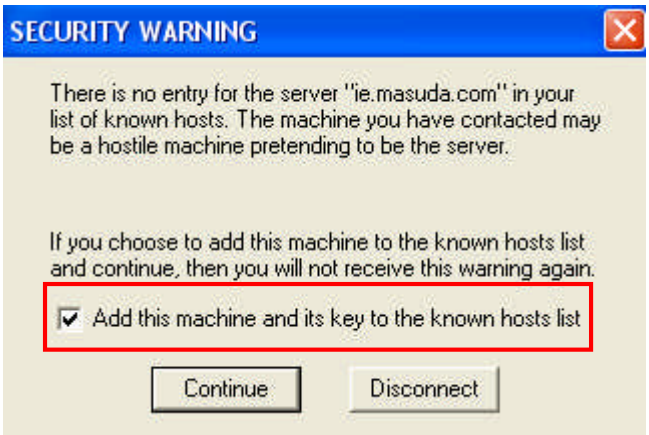
Bilgisayarınızı aşağıdaki şekilde ayarlayın. Ve "SSH" 'i seçin.



"OK", butonuna tıklayın ve servera bağlanın.

Şekil.3.11: Bilgisayar ayarları

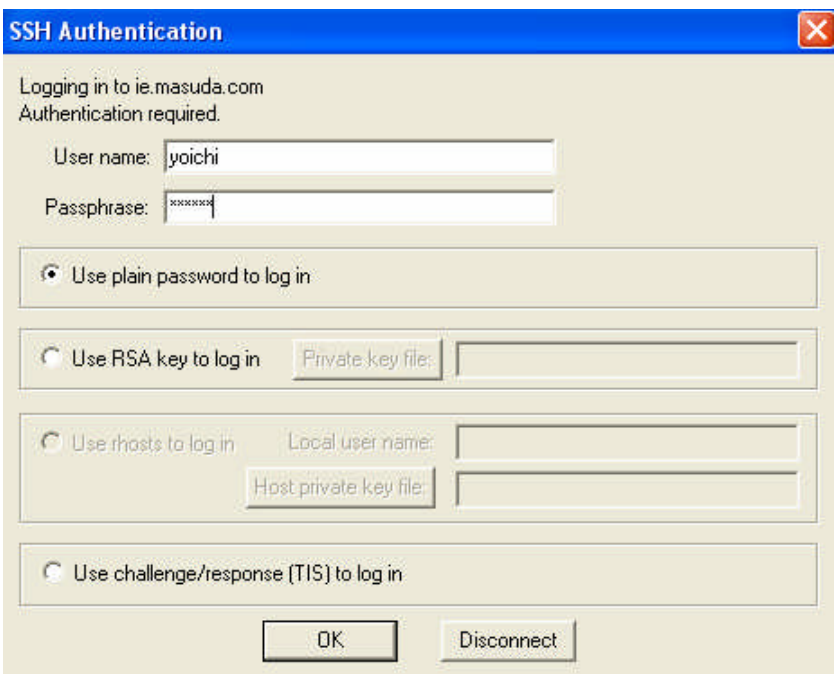
Aşağıdaki bölümü kontrol edin.



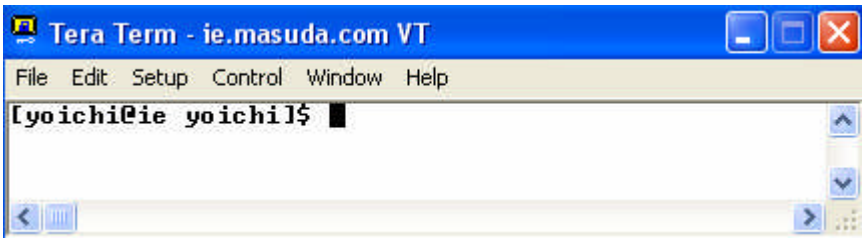
Şekil.3.12: Güvenlik uyarısı

- Log in (Erişim)

Kullanıcı ID'nizi kullanarak erişim olup olmadığını kontrol edin.



Şekil.3.13: Kullanıcı ID kullanarak erişim



Şekil.3.14: Bağlantının sağlanması

2.3. VNC Sunucu

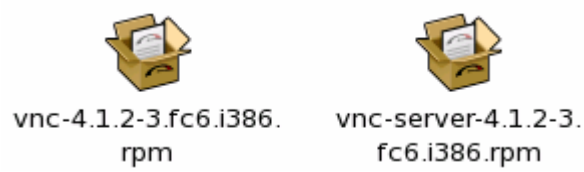
2.3.1.VNC Sunucu

Masaüstünüzü internet veya yerel ağ üzertinden kontrol etmeye yarayan programdır. Vncserver sayesinde masaüstüzü farklı bir bilgisayardan fare ile kontrol edebilir , klavyeniz ile giriş yapabilirsiniz.

Şimdi Vncserverin Linux üzerinde nasıl kurulacağını ve nasıl kullanılacağını öğrenelim.Vncserver yazılımı birçok Linux sürümü ile beraber ücretsiz olarak gelmektedir.

2.3.1.1 Kurulum

Biz kurulumumuzda Fedora Linux kullanacağız. İlk olarak Fedora CD'deki içerisindeki "/FEDORA/RPPMS/" klasörü içerisinden aşağıda gösterilen iki dosyamızı kuralım. İstenirse bu dosyalara çift tıklayarak ya da terminalden aşağıdaki komutu yazarak kurulum yapabilirsiniz. Biz bu bölümde "rpm" komutu ile term,nalden kurulum yapacağız.



Şekil.4.1: Vnc Server Paketleri

Öncelikle cd içerisnden bu dosyalar kök dizne kopyalanır. Ardından kök dizinde iken;

rpm –i vnc-4.1.2-3.fc6.i386.rpm
Ve
rpm –i vnc-server-4.1.2-3.fc6.i386.rpm
Komutları ile paketleri kurulur.Kurulum sonrasında sunucu başlatılır.

service vncserver start

Sunucu sorunsuz olarak başlatıldıktan sonra, vncserver'a bir şifre ile bağlanabilinmesi için aşağıdaki komut ile bu şifre belirlenir.

```
# vncpasswd
Password : ********
Verify : *******
```

Şifre asla unutulmamalıdır. Çünkü vnc sunucu bulunan bilgisayarımıza bu şifre ile bağlanacağız.Bu işlemlerin ardından vncserver yapılandırma dosyasının oluşturulması için aşağıdaki komutu uygulamamız gerekiyor.

```
root@a etc]# vncserver
New 'a.mzorlu.com:1 (root)' desktop is a:1
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/a:1.log
[root@a etc]#
```

Yukarıdaki çıktı ile karşılaşılırsa vncserver doğru olarak kurulmuş demektir.Şimdiki basamakta vncsunucu ya bağlandığında açılmasını istediğimiz arayüz için gerekli ayarlamaları yapacağız. Üst kısımdaki bütün basamakaları tamamladıysanız kök dizinde ulunan root klasörü içerisinde gizli bir ".vnc" klasörü oluşturulmuş olacaktır. Şimdi bu klasöre girelim:

```
#cd /root/.vnc
```

Bu klasör içinde bulunan xstartup dosyasını açarak içeriğini aşağıdaki hale getirelim.

```
#!/bin/sh

# Uncomment the following two lines for normal desktop:
unset SESSION_MANAGER
exec /etc/X11/xinit/xinitrc

[ -x /etc/vnc/xstartup ] && exec /etc/vnc/xstartup
[ -r $HOME/.Xresources ] && xrdb $HOME/.Xresources
xsetroot -solid grey
vncconfig -iconic &
xterm -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &
startx &
```

Bu işlemlerden sonra vncserverimizi yeniden başlatalım.

```
# service vncserver restart
```

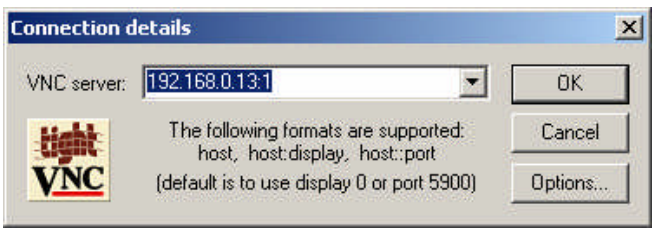
2.3.2 VNCSERVER Testi

Bir başka bilgisayardan vncserver' a baplantı yapmak için bir vncwiever programına ihityacımız olacak. Bunu da internetten ücretsiz olarak indirebilirsiniz. Biz bu uygulamamızda sunucumuz ile aynı ağda bulunan bir Windows makine üzerinden Fedora yüklü ve üzerinde vncserver kurulu olaman bilgisayara bağlanacağız. Vnc wiever programını aşağıdaki adresten indirebilirsiniz.

Tightvnc programı: http://www.skullbox.net/sd/vncclient.exe

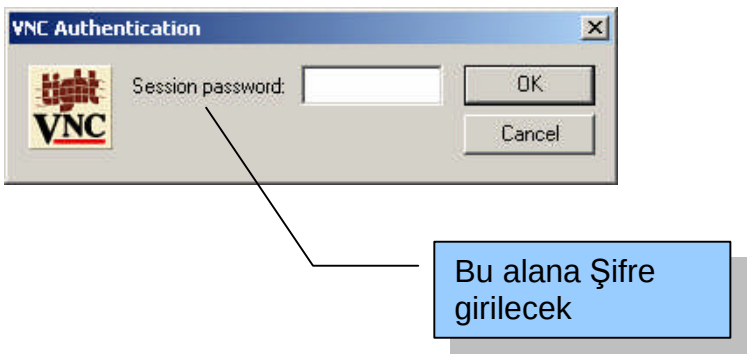
Bu programı bilgisayaranıza indirerek kurabilirsiniz. Program kurulumu bittikten sonra programı çalıştırarak bağlantı yapalım.

Örneğin bizim kurulumumunu yaptığımız sunucunun Ip numarası: 192.168.0.13 olsun Tightvnc programını çalıştırdığımızda karşımıza aşağıdaki pencere açılacaktır. Ip numarasının yanına yapılandırma dosya numarası olarak: 1 girilmelidir.



Şekil.4.2: Vnc Server IP numarası

Ardından bize vncserver için tanımladığımız şifre sorulacaktır.



Şekil.4.3: Vnc Server şifre

Şifre doğru girildi ise karşımıza aşağıdaki ekran gelecektir.

Şekil.4.4: Vnc Server erişimi

UYGULAMA FAALİYETİ

Aşağıdaki işlem basamaklarına göre uygulama faaliyetini yapınız.

Bilgisayarınızda otomasyon isimli bir kullanıcı oluşturun ve SSH kullanarak Public Key Kriptosistem ile anahtar çiftini oluşturduktan sonra log in olun.

İşlem Basamakları	Öneriler
➢ Kullanıcı oluşturmak için **Uygulamalar – Sunucu Ayarları – Kullanıcılar ve Gruplar – Kullanıcı Ekle** sıralamasını takip ederek otomasyon kullanıcısını oluşturmak ➢ Terminal Konsolunu açmak ➢ ssh –l otomasyon <host ismi> komutunu uygulamak ➢ ssh-keygen –t rsa komutunu uygulayın ➢ Karşımıza gelen mesajda Alıştırma 1-2'de olduğu gibi şifrenizi belirlemek ➢ ls –l .ssh/ ile anahtar çiftini kontrol etmek ➢ cat ~/.ssh/id_rsa.pub komutuyla public anahtar kontrolü yapmak ➢ scp ~/.ssh/id_rsa.pub otomasyon@<host ismi> komutuyla public anahtarı kaydetmek ➢ cat id_rsa.pub >> /..ssh/authorized_keys ile SSH Server'da public anahtarı kaydetmek ➢ chmod 600 .ssh/authorized_keys komutuyla dosya izni değiştirmek ➢ ls –l ~/.ssh/ komutuyla izni kontrol etmek. ➢ exit komutunu uygulamak ➢ ssh –l otomasyon <host ismi> ile tekrar log in olmak ➢ exit komutunu uygulamak	➢ Komutları uyguladıktan sonra hata mesajları alırsanız yazdığınız komutları tekrar kontrol edin. Yazım yanlışlıklarına dikkat edin. ➢ **Uygulamalar – Sunucu Ayarları – Servisler - sshd** sıralamasını takip ederek sshd servisinin çalışır durumda olduğunu kontrol edin.

ÖLÇME VE DEĞERLENDİRME

OBJEKTİF TEST (ÖLÇME SORULARI)

Aşağıda verilen soruları doğru ya da yanlış olarak cevaplayınız.

1. Telnet ile uzaktan erişim SSH sunucu kullanılarak yapılan uzaktan erişimden daha güvenlidir.

2. Telnet komutuyla başka bir bilgisayara bağlanmak için bağlanacağımız bilgisayarda tanımlı olan kullanıcı ismi ve şifremizi bilmemiz gerekir.

3. SSH sunucu ile bağlantıda 23 nu'lu port kullanılır.

4. Public key kriptosistem genel anahtarlama sistemine göre daha güvenlidir.

5. SSH Server'da tanımlı kulanıcılar için ayrı ayrı public key kripto sistem ile kodlama yapılarak her kullanıcıya ait bir SSH tüneli oluşturulur.

6. telnet kullanarak Web Server'ın index.html sayfası görüntülenebilir.

7. OpenSSH açık kaynak SSH çeşididir.

8. TTERMPRO programıyla SSH Server'a bağlanmak için Server'ın IP adresini kullanabiliriz.

9. ie.masuda.com Server'ın kurulduğu bilgisayarın DNS ismidir.

10. Telnet 22 no'lu portu kullanır.

11. İnternet veya yerel ağdan herhangi bir bilgisayarın masaüstüne ulaşmamızı sağlayan sunuculara VNC sunucu denir.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete geri dönerek tekrar inceleyiniz.

MODÜL DEĞERLENDİRME

UYGULAMALI TEST (YETERLİK ÖLÇME)

Modülde yaptığınız uygulamaları tekrar yapınız. Yaptığınız bu uygulamaları aşağıdaki tabloya göre değerlendiriniz.

AÇIKLAMA: Aşağıda listelenen kriterleri uyguladıysanız **Evet** sütununa, uygulamadıysanız **Hayır** sütununa **X** işareti yazınız.		
DEĞERLENDİRME ÖLÇÜTLERİ	**Evet**	**Hayır**
Netstat komutunu kullanarak bilgisayarın portlarını kontrol ettiniz mi?		
Telnet ile sunucuya bağlantı yaparak, index.html sayfasının kodlarını gördünüz mü?		
SSH sunucuda kodlama teknolojileri arasındaki farkı öğrendiniz mi?		
SSH sunucuda kullanıcı isminizle login oldunuz mu?		
Tera Term Pro programının çalışmasını öğrendiniz mi?		
VNC sunucu kurulumunu öğrendiniz mi?		

DEĞERLENDİRME

Hayır cevaplarınız var ise ilgili uygulama faaliyetini tekrar ediniz. Cevaplarınızın tümü evet ise bir sonraki modüle geçebilirsiniz.

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1'İN CEVAP ANAHTARI

SORU	CEVAP
1	D
2	D
3	D
4	D
5	Y
6	Y
7	Y
8	D
9	D
10	D

ÖĞRENME FAALİYETİ-2'NİN CEVAP ANAHTARI

SORU	CEVAP
1	Y
2	D
3	Y
4	D
5	D
6	D
7	D
8	D
9	D
10	Y
11	D

KAYNAKÇA

- BUYRUKBİLEN Yavuz,Yoichi MASUDA, **Ağ Sunucuları ve Güvenliği,** ETOGM–JICA, Konya, Ağustos 2005