

Doküman Kodu: BGT-3004

SOLARİS İŞLETİM SİSTEMİ GÜVENLİĞİ KILAVUZU

SÜRÜM 1.00

3 MART 2008

Hazırlayan: Gökhan ALKAN

*P.K. 74, Gebze, 41470 Kocaeli, TÜRKİYE
Tel: (0262) 648 1000
Faks: (0262) 648 1100
<http://www.bilgiguvenligi.gov.tr>
teknikdok@bilgiguvenligi.gov.tr*

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile, bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman "Ulusal Bilgi Sistemleri Güvenlik Projesi" kapsamında hazırlanmış olup ihtiyaç sahiplerini bilgi sistemleri güvenliği konusunda bilinçlendirmeyi hedeflemektedir. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda bahsi geçen belirli ticari marka isimleri kendi özgün sahiplerine aittir. Burada anlatılanlar tamamen tavsiye niteliğinde olup değişik ürünler/yapılandırmalar için farklılık gösterebilir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geen Ađ Güvenliđi personeline ve dokümanı gözden geirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Tahsin TÜRKÖZ'e teşekkürü bor biliriz.

İÇİNDEKİLER

1. GİRİŞ	7
1.1 Amaç ve Kapsam.....	7
1.2 Hedeflenen Kitle.....	7
1.3 Kısaltmalar.....	7
1.4 Dokümanda Kullanılan Semboller	8
2. İŞLETİM SİSTEMİ GÜVENLİĞİ GİRİŞ.....	9
3. İŞLETİM SİSTEMİ YAMA SETİNİN UYGULANMASI.....	10
4. GEREKSİZ SERVİSLERİN BELİRLENMESİ	11
4.1 Yazıcı Servisinin Devre Dışı Bırakılması.....	11
4.2 VolumeArayüz Yönetiminin Devre Dışı Bırakılması	11
4.3 Rlogin ve Shell Hizmetlerinin Devre Dışı Bırakılması	11
4.4 NFS Servisinin Devre Dışı Bırakılması.....	12
4.5 Sistem Açılış Servislerinin Devre Dışı Bırakılması	12
4.6 DNS Servisinin Devre Dışı Bırakılması	12
4.7 FİNGER Servisinin Devre Dışı Bırakılması.....	12
4.8 XFS Servisinin Devre Dışı Bırakılması.....	13
4.9 Automount Servisinin Devre Dışı Bırakılması.....	13
4.10 TELNET Servisinin Devre Dışı Bırakılması	13
4.11 Rlogin Servisinin Devre Dışı Bırakılması	13
4.12 DHCP Servisinin Devre Dışı Bırakılması	14
4.13 FTP Servisinin Devre Dışı Bırakılması	14
5. ÇEKİRDEK AYARLARININ YAPILANDIRILMASI	15
5.1 Bellek Dökümü Alımının Kısıtlanması	15
5.2 Yığın Korumasının Etkin Hale Getirilmesi	15
5.3 NFS İstemci İsteklerinin Kısıtlanması.....	16
5.4 Daha İyi TCP Sıra Numarası Kullanılması	16
6. SİSTEM KAYITLARININ YAPILANDIRILMASI	17

6.1 INETD Servisi İçin Kayıt Tutma Özelliğinin Aktif Hale Getirilmesi.....	17
6.2 FTP Servisi İçin Kayıt Tutma Özelliğinin Aktif Hale Getirilmesi.....	17
6.3 FTP ve INETD Servisleri İçin Kayıtların Ayrı Bir Dosyada Tutulması	18
6.4 Sisteme Gerçekleştirilen Başarısız Kimlik Doğrulama Girişim Denemelerin Kayıtlarının Tutulması	18
6.5 Cron Kayıtlarının Tutulması.....	19
6.6 Sistem Kayıt Dosyalarının İzinlerinin Doğrulanması.....	19
7. ERİŞİM HAKLARININ DÜZENLENMESİ	21
7.1 Sistem Üzerinde Bulunan Servisler İçin UMASK Değeri İçin Ön Tanımlı Değerinin Belirlenmesi.....	21
7.2 Nosuid Değerinin /etc/rmmount Dosyasına Eklenmesi.....	21
7.3 Passwd , Shadow ve Group Dosyalarının İzinlerinin Doğrulanması	21
7.4 Herkes Tarafından Yazılabilir Dizinlerin Bulunması	22
7.5 Herkes Tarafından Yazılabilir Dosyaların Bulunması	22
7.6 Sahibi Olmayan Dosya ve Dizinlerin Belirlenmesi.....	23
7.7 Yetkilendirilmiş Dosyaların Tespit Edilmesi	23
8. YETKİLENDİRME VE KİMLİK DOĞRULAMA İŞLEMLERİ	24
8.1 Seri Portlar İçin “Prompt:” Ekranının Devre Dışı Bırakılması	24
8.2 SSH Servisinin Yapılandırılması	24
8.3 FTP Servisini Kullanabilecek Kullanıcıların Belirlenmesi	25
8.4 Sendmail Sunucu Yazılımının Yapılandırılması	25
8.5 Syslog Servisinin Yapılandırılması	26
8.6 At ve Cron İşleri İçin Yetkili Kullanıcıların Belirlenmesi	26
8.7 Boş Crontab Dosyalarının Belirlenmesi ve Erişim Yetkilerinin Ayarlanması.....	27
9. KULLANICI HESAPLARININ DENETİMİ.....	28
9.1 Sistem Hesaplarının Engellenmesi	28
9.2 Sistem Üzerinde Şifresi Boş Olan Kullanıcıların Tespit Edilmesi.....	29
9.3 Güvenli Şifre Politikasının Atanması	29
9.4 Sistem Üzerinde Bulunan Root Yetkili Kullanıcıların Tespit Edilmesi.....	31

9.5 Root Kullanıcısının Dahil Olduğu Grubun Root Grubu Olarak Ayarlanması	31
9.6 Kullanıcı Ev Dizini Yetkilerinin Belirlenmesi	31
9.7 Kullanıcı Dizinlerinde Bulunan.netrc Dosyalarının Kaldırılması	32
9.8 Kullanıcılar İçin Ön Tanımlı Umask Değerinin Belirlenmesi.....	32
9.9 FTP Kullanıcıları İçin Kullanılacak Öntanımlı Umask Değerinin Belirlenmesi.....	33
10. UYARI MESAJLARININ YAPILANDIRILMASI.....	33
10.1 Standart Giriş Servisleri İçin Uyarı Mesajlarının Yapılandırması	33
10.2 Grafikselle Ara Yüz İçin Uyarı Mesajının Belirlenmesi	34
10.3 FTP Sunucu Servisi İçin Uyarı Mesajının Belirlenmesi.....	35
10.4 Sistem Açılış Uyarı Mesajlarının Belirlenmesi	35

1. GİRİŞ

Bu dokümanda Solaris 10 sürümü baz alınarak, işletim sistemi güvenliği konusu anlatılacaktır.

1.1 Amaç ve Kapsam

Bu dokümanda amaç, Solaris işletim sisteminin uygulamalardan bağımsız nasıl güvenli bir hale getirileceği esasları belirlemektir. Esaslar belirlenirken, belirli bir kritiklik derecesindeki uygulamalar hedef alınmamıştır. Fakat bazı esasların daha kritik sistemlerde nasıl uygulanması gerektiği üzerinde durulmuştur.

1.2 Hedeflenen Kitle

Bu doküman Solaris işletim sistemi yöneticiliği konusunda aktif görev alan ya da görev almak isteyen kişiler tarafından kullanılabilir.

1.3 Kısaltmalar

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

IP : Internet Protocol

DHCP : Dinamik Host Configuration Protocol

NFS : Network File System

SSH : Secure Shell

DNS : Domain Name Service

SCP : Secure Copy

SFTP : Secure File Transfer Protocol

UID : User ID

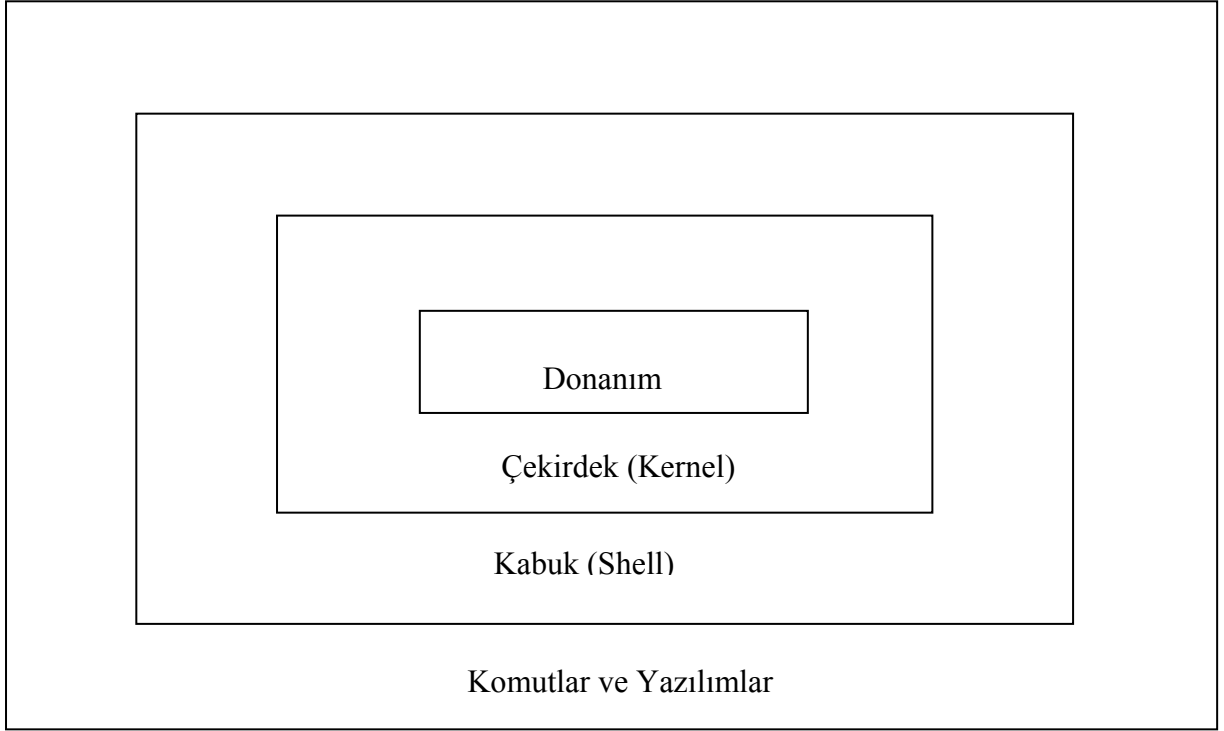
GID : Group ID

1.4 Dokümanda Kullanılan Semboller

Sembol	Açıklaması
(yabancı terim)	İngilizce terimleri belirtmek içindir.
komut	Kod parçalarını ve betikleri belirtmek içindir.
“dosya yolu”	Dosya veya dizin yollarını göstermek içindir.

2. İŞLETİM SİSTEMİ GÜVENLİĞİ GİRİŞ

İşletim sistemi, bütün donanım unsurlarını ayrıntılı bir biçimde tanıyan, dolayısıyla kullanıcıyı donanım ayrıntılarından uzak tutan ve uygulamaların üzerinde koştuğu yazılımlar olarak nitelendirilebilir. Donanım ayrıntılarına hâkim olarak kullanıcıyı donanım detaylarından uzak tutarak donanım ve kullanıcı arasında ara yüz oluşturmaktadır. Şekil 1’de Unix/Linux işletim sistemleri ailesi için işletim sistemi, donanım , kabuk ve uygulamalar arasındaki ilişki gösterilmektedir.



Şekil 1 İşletim sisteminde çekirdeğin yeri

Unutulmamalıdır ki zincir en zayıf halkasından kırılır. Bundan dolayı uygulamaların güvenli bir şekilde sistem üzerinde çalışabilmesi için öncelikle işletim sisteminin güvenliği sağlanmalıdır.

3. İŞLETİM SİSTEMİ YAMA SETİNİN UYGULANMASI

Güncellemeler işletim sistemi güvenliğinde büyük rol oynamaktadır. Sistem üzerinde kurulu her yazılım aslında sistem güvenliği açısından bir tehdit oluşturmaktadır. Özellikle bazı uygulamaların sık bir biçimde güncel sürümlerinin çıktığı düşünüldüğünde güncellemelerin önemi daha da artmaktadır. Gerek uygulamalarda meydana gelebilecek güvenlik açıklarının önüne geçmek, gerekse güncel sürümler ile birlikte yazılımlara eklenen yeni özelliklerin etkin olabilmesi için güncellemeler düzenli olarak takip edilmeli ve sistem güvenlik politikasına göre gerekli analizin gerçekleştirilmesinin ardından bu güncellemeler sisteme uygulanmalıdır. **Solaris** işletim sistemi için gerekli güncellemeler ücretli olarak temin edilebilmektedir. Belirli aralıklarla sürümü yayınlanan “Recommended” isimli yama seti temin edilip sistem kurulumu gerçekleştirilmelidir.

Yama setinin (10_Recommended.zip) “/tmp” dizini ya da uygun bir dizine indirip aşağıdaki adımlar uygulanmalı ve daha sonra sistem yeniden başlatılmalıdır.

```
#unzip-q10_Recommended.zip  
#cd10_Recommended  
# ./install_cluster
```

4. GEREKSİZ SERVİSLERİN BELİRLENMESİ

Sistem üzerinde çalışan kullanılmayan servisler sistem güvenliği için bir tehdit unsuru oluştururlar. Sistem üzerinde çalışan servislerden kaynaklanacak güvenlik açıklıkları sistemin güvenliğini de tehdit etmektedir. Bundan dolayı sistem üzerinde kullanılmayan servislerin çalışmaması hatta bu servisler için gerekli paketlerin sistemden kaldırılması gerekmektedir. Sistem kurulum seçeneklerine göre çeşitli servisler sisteme kurulmaktadır. Sistem ihtiyaç ve güvenlik politikaları doğrultusunda bu servisler analiz edilip istenmeyen servislerin çalışması engellenmelidir. Sistem üzerinde çalışan servisler “svcs -a” komutu yardımı ile görüntülenebilir.

4.1 Yazıcı Servisinin Devre Dışı Bırakılması

Eğer sistem yazıcı servisi olarak hizmet vermeyecek ise bu servisler devre dışı bırakılmalıdır. Yazıcı servisini devre dışı bırakmak için aşağıdaki adımlar uygulanmalıdır.

```
# svcadm disable svc:/application/print/server:default
# svcadm disable svc:/application/print/cleanup:default
# svcadm disable svc:/application/print/rfc1179:default
```

4.2 Volume Arayüz Yönetiminin Devre Dışı Bırakılması

Solaris volume yönetimi yazılımsal olarak RAID kullanımını sağlayan sistemdir. Bu sistem işletim sistemi ile sağlanan bir ara yüz ile ya da komut satırından gerçekleştirilebilir. Bu hizmetin kullanılabilmesi için birkaç servisin çalışması gerekmektedir. Eğer bu hizmet kullanılmayacak ise devre dışı bırakılmalıdır. Bu servisleri devre dışı bırakmak için aşağıdaki adımlar uygulanmalıdır.

```
# svcadm disable svc:/network/rpc/mdcomm:default
# svcadm disable svc:/network/rpc/meta:default
# svcadm disable svc:/network/rpc/metamed:default
# svcadm disable svc:/network/rpc/metamh:default
```

4.3 Rlogin ve Shell Hizmetlerinin Devre Dışı Bırakılması

Bu servisler sistem üzerinde kullanılmayacak ise devre dışı bırakılmalıdırlar. Bu servisleri devre dışı bırakmak için aşağıdaki adımlar uygulanmalıdır.

```
# svcadm disable svc:/network/shell:default  
# svcadm disable svc:/network/login:rlogin
```

4.4 NFS Servisinin Devre Dışı Bırakılması

Sistem eğer NFS sunucu olarak hizmet vermeyecekse NFS sunucusu için gerekli servisler devre dışı bırakılmalıdır. Bu servisleri devre dışı bırakmak için aşağıdaki adımlar uygulanmalıdır.

```
# svcadm disable svc:/network/nfs/server:default  
# svcadm disable svc:/network/nfs/nlockmgr:default  
# svcadm disable svc:/network/nfs/status:default  
# svcadm disable svc:/network/nfs/mapid:default  
# svcadm disable svc:/network/nfs/cbd:default
```

4.5 Sistem Açılış Servislerinin Devre Dışı Bırakılması

Sistem diğer makineler için ön yükleme sunucusu olarak hizmet vermeyecek ise bu servisler devre dışı bırakılmalıdır. Bu servisleri devre dışı bırakmak için aşağıdaki adımlar uygulanmalıdır.

```
# svcadm disable svc:/network/rpc/bootparams:default  
# svcadm disable svc:/network/rarp:default
```

4.6 DNS Servisinin Devre Dışı Bırakılması

Sistem DNS servisi olarak hizmet vermeyecek ise DNS servisi devre dışı bırakılmalıdır. DNS servisini devre dışı bırakmak için aşağıdaki adım uygulanır.

```
# svcadm disable svc:/network/dns/server:default
```

4.7 FİNGER Servisinin Devre Dışı Bırakılması

FİNGER servisi FİNGER istemcilerinin sorgularına sistem ya da kullanıcı hakkında çeşitli bilgileri sunarlar. Eğer sistemde FİNGER servisinin çalışması istenmiyorsa aşağıdaki adım uygulanmalıdır.

```
# svcadm disable svc:/network/finger:default
```

4.8 XFS Servisinin Devre Dışı Bırakılması

XFS servisi sistemin X font sunucu olarak çalışmasını sağlar. XFS istemcileri sunucuya X font istekleri için bağlanırlar, sunucuda diskten font dosyalarını okur ve istemcilere sunar. Eğer sistem X Font sunuculuğu görevini yerine getirmeyecek ise XFS servisi devre dışı bırakılmalıdır. XFS servisini devre dışı bırakmak için aşağıdaki adımlar uygulanmalıdır.

```
# svcadm disable svc:/application/x11/xfs:default
```

4.9 Automount Servisinin Devre Dışı Bırakılması

Automount servisi ihtiyaç duyulduğunda uzak dosya sunucularından otomatik olarak NFS dosya sistemlerini bağlamak için kullanılır. Bu daha çok masaüstü sistemler için yararlı olabilecek bir yöntemdir. Sunucu sistemler için kullanılması tavsiye edilmez. Automount servisini devre dışı bırakmak için aşağıdaki adım gerçekleştirilmelidir.

```
# svcadm disable svc:/system/filesystem/autofs:default
```

4.10 TELNET Servisinin Devre Dışı Bırakılması

TELNET servisi kendisi ile aynı adı taşıyan protokolünü kullanan SSH servisinde olduğu gibi uzak bağlantı sağlayan bir servistir. Telnet kullanıcının oturum açmasından telnet oturumunun kapatılmasına kadar geçen sürede veriler şifrelenmemiş olarak açık bir şekilde uç sistemler arasında aktarılır. SSH kullanıldığında ise veriler şifrelenmiş olarak uç birimler arasında iletilir. Eğer sunucu sistemin yönetimi uzak bağlantı ile sağlanmak isteniyorsa telnet servisi yerine daha güvenilir bir servis olan SSH servisi tercih edilmelidir. Telnet servisini devre dışı bırakmak için aşağıdaki adım uygulanmalıdır.

```
# svcadm disable svc:/network/telnet:default
```

4.11 Rlogin Servisinin Devre Dışı Bırakılması

Rlogin uzak sistemlerde bulunan kullanıcıların ağ üzerinden SSH ya da telnet servislerinde olduğu gibi sisteme bağlanmasını sağlayan servistir. Telnete benzer şekilde çalışır ve TELNET’de olduğu gibi veriler şifrelenmemiş olarak uç birimler arasında iletilir. Bu servis yerine SSH kullanılması önerilmektedir. Rlogin servisini devre dışı bırakmak için aşağıdaki adım uygulanmalıdır.

```
# svcadm disable svc:/network/login:rlogin
```

4.12 DHCP Servisinin Devre Dışı Bırakılması

DHCP servisi IP adresi, ağ geçidi, altağ maskesi gibi TCP/IP bilgilerini otomatik olarak ağdaki istemcilere atama görevini üstlenen servis olarak çalışmaktadır. Eğer sistem DHCP servisi olarak görev yapmayacak ise servis devre dışı bırakılmalıdır. Bunun için aşağıdaki adım uygulanmalıdır.

```
# svadm disable svc:/network/dhcp-server:default
```

4.13 FTP Servisinin Devre Dışı Bırakılması

FTP aynı adı taşıyan FTP protokolü ile ağ üzerinden dosya transferi yapmayı sağlayan servis olarak çalışmaktadır. Telnet servisinde olduğu gibi kullanıcının oturum açmasından oturumunun kapatılmasına kadar geçen sürede veriler şifrelenmemiş olarak açık bir şekilde uç sistemler arasında aktarılır. Bunun yerine SSH ile gelen SCP ya da SFTP kullanılarak ağ üzerinden akan veriler şifreli bir biçimde uç birimler arasında iletilir. Bundan dolayı dosya transferi için SFTP ya da SCP kullanımı önerilir. FTP servisini devre dışı bırakmak için aşağıdaki adım uygulanmalıdır.

```
#svcadm disable svc:/network/ftp:default
```

5. ÇEKİRDEK AYARLARININ YAPILANDIRILMASI

5.1 Bellek Dökümü Alımının Kısıtlanması

Sistem üzerinde çalışan yazılımların normal olmayan bir şekilde sonlanması ile belleğin dökümü diske kaydedilir. Özellikle set-UID ve set-GID programlarının hassas (kritik) bilgiler içermesinden dolayı, bellek dökümünün alımı devre dışı bırakılmalıdır. Bu işlem sistem üzerinde çalışan bir servisin istenmeyen bir şekilde sonlanması ile meydana gelecek bellek dökümü işlemlerinin kayıtlarını sistemde tutacaktır. Aşağıdaki adımlar gerçekleştirilerek bellek dökümü alım işlemi devre dışı bırakılabilir.

```
# mkdir -p /var/core
# chown root:root /var/core
# chmod 700 /var/core
# coreadm -g /var/core/core_%n_%f_%u_%g_%t_%p \
-e log -e global -e global-setid \
-d process -d proc-setid
#
```

5.2 Yığın Korumasının Etkin Hale Getirilmesi

Sistem üzerinde çalışan herhangi bir servis de meydana gelebilecek bellek taşması açıklığı sonucu yerel ya da uzak saldırılar ile sistem üzerinde “root” kullanıcı yetkilerine sahip olunabilir.

Yığın koruması sadece SPARC ve AMD64 tabanlı işlemcili sistemlerde uygulanabilir. Yığın korumasını aktif hale getirmek için “/etc/system” dosyasında aşağıda belirlenen değişiklikler yapılmalıdır.

```
# vi /etc/system
set noexec_user_stack = 1
set noexec_user_stack_log = 1
#
```

5.3 NFS İstemci İsteklerinin Kısıtlanması

Güvenilen port numaraları (<1024) haricinde NFS istemci isteklerinin kabul edilmemesi sağlanır. Bu şekilde yetkisiz kullanıcılar tarafından çalıştırılacak otomatikleştirilmiş NFS saldırılarını engeller. Ancak normal NFS işlemlerini engellemez. Bunun için

```
# vi /etc/system
```

Solaris 2.5 öncesi sürümler için

```
set nfs:nfs_portmon = 1
```

Solaris 2.5 sonrası sürümler için

```
set nfssrv:nfs_portmon = 1
```

5.4 Daha İyi TCP Sıra Numarası Kullanılması

Daha iyi bir TCP başlangıç sıra numarası seçimi algoritması kullanarak oturum çalma ya da TCP sıra numarası tahmini üzerine yapılan ağ tabanlı saldırılar için önlem alınabilir. Bunun için;

```
# cd /etc/default
# awk '/TCP_STRONG_ISS=/ { $1 = "TCP_STRONG_ISS=2" }; \
{ print }' inetinit > inetinit.new
# mv inetinit.new inetinit
#pkgchk -f -n -p /etc/default/inetinit
```

6. SİSTEM KAYITLARININ YAPILANDIRILMASI

6.1 INETD Servisi İçin Kayıt Tutma Özelliğinin Aktif Hale Getirilmesi

TCP kullanılarak yapılan ağ bağlantılarının kayıtlarının tutulması için INETD servisi syslog kullanır. INETD servisinin yapılandırma dosyasında belirtildiği şekilde, birçok ağ servisi için gelen TCP ve UDP paketlerini INETD bu servislerin yerine dinler ve servisleri çalıştırarak servis ile iletişimi sağlar. Eğer sistemde INETD servisi kullanılıyorsa bütün servisler ya da sadece istenilen servisler için kayıt tutması sağlanabilir. Ön tanımlı INETD davranışını görüntülemek için;

```
# inetadm -p | grep "tcp_trace"  
  
tcp_trace=FALSE  
  
#
```

Bu çıktıya göre INETD servisi için bu özellik etkin değildir. Etkin hale getirmek için;

```
# inetadm -M tcp_trace=TRUE
```

Sadece istenen bir servis için bu özelliğin etkin hale getirilmesi isteniyorsa “inetadm -l” servis_adi şeklinde kullanılabilir. Örneğin telnet servisi için;

```
# inetadm -m telnet tcp_trace=TRUE
```

Yapılan değişikliği doğrulamak için;

```
# inetadm -l telnet | grep "tcp_trace"  
  
tcp_trace=TRUE  
  
#
```

6.2 FTP Servisi İçin Kayıt Tutma Özelliğinin Aktif Hale Getirilmesi

```
# inetadm -m svc:/network/ftp exec="/usr/sbin/in.ftpd -a -l -d"
```

Eğer sistemde FTP servisi kullanılıyorsa -d parametresi ile hata ayıklama kayıtlarının tutulması, -l parametresi ile ftp aktivitelerinin kayıtları tutulabilir. Fakat hata ayıklama kayıtlarının tutulması için -d parametresi kullanıldığında kullanıcı adı ve şifre ikilisi açık bir şekilde sistem logların da görülebilecektir.

6.3 FTP ve INETD Servisleri İçin Kayıtların Ayrı Bir Dosyada Tutulması

Eğer sistem üzerinde FTP ve INETD servisleri aktif ise ve bu servisleri için 4.1 ve 4.2 maddelerde anlatılan kayıt tutma özellikleri aktif hale getirilmiş ise bu servisler için kullanılan kayıt tutma işlemleri “syslog” servisi tarafından gerçekleştirilir. Bu servisler için tutulan kayıtların ayrı bir dosyada tutulması daha sonra bu kayıtların analiz etme işini kolaylaştıracaktır. Kayıtların ayrı bir dosyada örneğin “connlog“ dosyasında tutulması için aşağıdaki adımlar sırası ile uygulanmalıdır..

```
# if [ ! "` cat /etc/syslog.conf | grep -v "#" | grep -v "^$" | grep
/var/log/connlog`" ]
    then
        echo -e "daemon.debug\t\t\t/var/log/connlog">>/etc/syslog.conf
        touch /var/log/connlog
        chown root:root /var/log/connlog
        chmod 600 /var/log/connlog
        logadm -w connlog -C 13 -a 'pkill -HUP syslogd' /var/log/connlog
    fi
#
```

6.4 Sisteme Gerçekleştirilen Başarısız Kimlik Doğrulama Girişim Denemelerin

Kayıtlarının Tutulması

Sisteme giriş için gerçekleştirilen başarısız denemelerin kayıtları “/var/adm/loginlog” dosyasında tutulur. Ön tanımlı olarak bu dosya yoktur. Ayrıca “/etc/default/login” dosyasında SYSLOG_FAILED_LOGINS değeri ile kaç tane başarısız girişimden sonra kayıtların tutulacağı da belirlenebilir. Bu değerın ”0” olması sayı limiti olmadan bütün başarısız sisteme giriş denemelerinin kayıtlarının tutulması anlamına gelmektedir. Bunun için aşağıdaki adımlar sırası ile uygulanmalıdır.

```
# touch /var/adm/loginlog
# chown root:sys /var/adm/loginlog
# chmod 600 /var/adm/loginlog
# cd /etc/default
# awk '/SYSLOG_FAILED_LOGINS=/{ $1 = "SYSLOG_FAILED_LOGINS=0" }; \
```

```
{ print }' login >login.new  
  
# mv login.new login  
  
# pkgchk -f -n -p /etc/default/login  
  
#logadm -w loginlog -C 13 /var/adm/loginlog
```

6.5 Cron Kayıtlarının Tutulması

Sistemde çalıştırılan her cron işinin kaydı tutularak sistem üzerindeki denetim etkisi artırılabilir. İşlem kayıtları “/var/cron/log” dosyasından takip edilebilir. Bunun için aşağıdaki adımlar sırası ile uygulanmalıdır.

```
# cd /etc/default  
  
# awk '/CRONLOG=/ { $1 = "CRONLOG=YES" }; { print }' cron > cron.new  
  
# mv cron.new cron  
  
# pkgchk -f -n -p /etc/default/cron
```

6.6 Sistem Kayıt Dosyalarının İzinlerinin Doğrulanması

Sistem kayıtlarının izlenmesi sistem denetimi ve sistem güvenliği açısından önemi yüksektir. Sistem kayıtlarının yetkisiz kişiler tarafından değiştirilmesi ya da sadece sistem üzerinde yetkili kişi tarafından erişilebilecek kayıtların yetkisiz kişiler tarafından görüntülenmesi bir güvenlik açığına yol açabilir. Bu dosyaların yetkileri gerektiği gibi düzenlenmelidir. Bunun için aşağıdaki adımlar sırası ile uygulanmalıdır.

```
# pkgchk -f -n -p /var/log/syslog  
  
# pkgchk -f -n -p /var/log/authlog  
  
# pkgchk -f -n -p /var/adm/utmpx  
  
# pkgchk -f -n -p /var/adm/wtmpx  
  
#chown root:sys /var/adm/loginlog  
  
# chown root:root /var/cron/log /var/adm/messages /var/log/connlog  
  
# chmod go-wx /var/adm/messages  
  
# chmod go-rwx /var/adm/loginlog /var/cron/log /var/log/connlog  
  
# chown sys:sys /var/adm/sa/*  
  
# chmod go-wx /var/adm/sa/*  
  
# dir=`awk -F: '($1 == "dir") { print $2 }' /etc/security/audit_control`
```

```
# chown root:root $dir/*  
  
# chmod go-rwx $dir/*
```

7. ERİŞİM HAKLARININ DÜZENLENMESİ

7.1 Sistem Üzerinde Bulunan Servisler İçin UMASK Değeri İçin Ön Tanımlı Değerinin Belirlenmesi

Sistem üzerinde kullanılan ön tanımlı umask değeri en azından 022 olmalıdır. Bu şekilde sistem süreçleri tarafından ön tanımlı olarak üretilecek dosyaların herkes tarafından yazılabilir olması engellenebilir. Aktif hale getirmek için aşağıdaki adımlar sırası ile uygulanmalıdır.

```
# cd /etc/default
# awk '/^CMASK=/ { $1 = "CMASK=022" }
{ print }' init >init.new
# mv init.new init
# pkgchk -f -n -p /etc/default/init
```

7.2 Nosuid Değerinin /etc/rmmount Dosyasına Eklenmesi

Bu değer “/etc/rmmount” dosyasında aktif edilerek CD-ROM ve Floopy sürücülerini üzerinden sisteme aktarılacak set-UID bitli yazılımlar engellenir. Bu değeri “/etc/rmmount” dosyasına eklemek için aşağıdaki adımlar sırası ile gerçekleştirilmelidir.

```
# if [ ! "`grep -- '-o nosuid' /etc/rmmount.conf`" ]; then
fs=`awk '($1 == "ident") && ($2 != "pcfs") \
{ print $2 }' /etc/rmmount.conf`
echo mount \* $fs -o nosuid >>/etc/rmmount.conf
f
#
```

7.3 Passwd , Shadow ve Group Dosyalarının İzinlerinin Doğrulanması

passwd, shadow ve group dosyalarının erişim izin ve sahiplerinin ön tanımlı değerlerinin doğrulanması gereklidir. “/etc/passwd” dosyası sistem üzerinde bulunan kullanıcıları içeren, “/etc/group” dosyası sistem üzerinde tanımlanmış grupları içeren ve “/etc/shadow” dosyası sistem üzerinde tanımlanmış kullanıcıların şifreleri içeren dosyadır. Bu dosyaların güvenliği sistem güvenliği açısından önemli rol oynamaktadır. Bu dosyaların yetki kalıplarının doğrulanması için aşağıdaki adımlar gerçekleştirilmelidir.

```
# pkgchk -f -n -p /etc/passwd
# pkgchk -f -n -p /etc/shadow
# pkgchk -f -n -p /etc/group
```

7.4 Herkes Tarafından Yazılabilir Dizinlerin Bulunması

Herkes tarafından yazılabilir dizinler içerisinde bulunan dosya ve dizinler değiştirilebilir sistemden kaldırılabilir. Bunu önlemek için dizin erişim yetkilerinde **sticky** bit etkinleştirilerek dizin okuma yazma yetkileri ne olursa olsun dosya üzerindeki asıl yetkilerin kendi erişim yetkisinin kullanılması sağlanır. Eğer sistem üzerinde kullanılan uygulamaya özel erişim izinleri haricinde bu dizinler için **sticky** bit etkinleştirilebilir. Öncelikle sistemde bulunan herkes tarafından yazılabilir dizinlerin tespit edilmesi gerekmektedir. Bunun için aşağıdaki adım uygulanmalıdır.

```
# find / \( -fstype nfs -o -fstype cacheefs \) -prune -o -type d \
  \( -perm -0002 -a ! -perm -1000 \) -print
#
```

Bu dizinler için sistem üzerindeki uygulamalar dikkate alınarak **sticky** bit etkinleştirilebilir ya da yetkiler sıkılaştırılabilir.

7.5 Herkes Tarafından Yazılabilir Dosyaların Bulunması

Sistem üzerinde bulunan herkes tarafından yazılabilir dosyalar sistem güvenliği için bir gedik oluşturmaktadır. Bu dosyaların içerikleri değiştirilebilir, dosyalar sistemden kaldırılabilir. Sistem üzerinde bulunan herkes tarafından yazılabilir dosyaların tespit edilip sistem politikalarına göre gerekli yetki kalıpları bu dosyalar üzerinde gerçekleştirilmelidir. Sistem üzerinde bulunan herkes tarafından yazılabilir dosyaları tespit etmek için aşağıdaki adımlar gerçekleştirilir.

```
# find / \( -fstype nfs -o -fstype cacheefs \) -prune -o \
  -type f -perm -0002 -print
#
```

7.6 Sahibi Olmayan Dosya ve Dizinlerin Belirlenmesi

Sistem üzerinde bulunan sahibi bulunmayan dosya ve dizinler sistem güvenliği için bir gedik oluşturabilir. Bu dosyalar tespit edilip sistem politikalarına göre gerekli yetki sıkılaştırması gerçekleştirilmelidir. Bu dosyaları tespit etmek için aşağıda belirtilen komut uygulanmalıdır.

```
# find / \( -fstype nfs -o -fstype cacheefs \) -prune -o \( -nouser -o -  
nogroup \) -print  
  
#
```

7.7 Yetkilendirilmiş Dosyaların Tespit Edilmesi

Sistem üzerinde bulunan yetkilendirilmiş dosyalar saldırgan ya da kötü niyetli kişiler tarafından kullanılabilir. Bu dosyalar tespit edilip sistem politikasına göre yetki sıkılaştırması gerçekleştirilmelidir. Bu dosyaları tespit etmek için aşağıdaki işlem yapılır.

```
# find / \( -fstype nfs -o -fstype cacheefs \) -prune -o -xattr -print
```

8. YETKİLENDİRME VE KİMLİK DOĞRULAMA İŞLEMLERİ

8.1 Seri Portlar İçin “Prompt:” Ekranının Devre Dışı Bırakılması

Sistem üzerinde bulunan seri aygıtlar için “login:” devre dışı bırakarak yetkisiz kullanıcıların sisteme modem, terminal ve uzak erişim aygıtlarını takması daha da zor hale getirilir. **Prompt** ekranının devre dışı bırakılması için aşağıdaki adımlar uygulanmalıdır.

```
# pmadm -d -p zsmon -s ttya
# pmadm -d -p zsmon -s ttyb
```

8.2 SSH Servisinin Yapılandırması

SSH (Güvenli Kabuk) ağ üzerinden başka bilgisayarlara erişim sağlamak, uzak bir bilgisayarda komutlar çalıştırmak ve bir bilgisayardan diğerine dosya transferi amaçlı geliştirilmiş bir protokoldür. Açık metin olarak iletişim sağlayan protokollerin yerine alternatif olarak geliştirilmiştir. “/etc/ssh_config” dosyası içerisinde SSH istemcisi için geçerli olan yapılandırma değerleri “/etc/ssh/sshd_config” dosyası içerisinde de SSH sunucu için geçerli değerler yer almaktadır. Bunun için aşağıdaki adımlar sırası ile uygulanmalıdır.

```
# cd /etc/ssh
# cat <<EOCliConfig >>ssh_config
    Host *
    Protocol 2
        EOCliConfig
# awk '/^Protocol/ { $2 = "2" }; \
/^X11Forwarding/ { $2 = "yes" }; \
/^MaxAuthTries/ { $2 = "5" }; \
/^MaxAuthTriesLog/ { $2 = "0" }; \
/^IgnoreRhosts/ { $2 = "yes" }; \
/^RhostsAuthentication/ { $2 = "no" }; \
/^RhostsRSAAuthentication/ { $2 = "no" }; \
/^PermitRootLogin/ { $2 = "no" }; \
/^PermitEmptyPasswords/ { $2 = "no" }; \
```

```
/^#Banner/ { $1 = "Banner" } \  
  
{ print }' sshd_config > sshd_config.new  
  
# mv sshd_config.new sshd_config  
  
# pkgchk -f -n -p /etc/ssh/sshd_config
```

8.3 FTP Servisini Kullanabilecek Kullanıcıların Belirlenmesi

“/etc/ftpd/ftpusers” dosyası sisteme ftp bağlantısı kurmasına izin verilmeyen kullanıcıların listesini içerir. Özellikle **root** kullanıcısının sisteme ftp bağlantısı yapmaması gerekmektedir. Belirtilen kullanıcılar haricinde sistem üzerinde çalışan uygulamalara göre diğer kullanıcılar da “/etc/ftpd/ftpusers” dosyasına eklenebilir.

```
# cd /etc/ftpd  
  
# for user in root daemon bin sys adm lp uucp nuucp smmsp listen gdm \  
webservd nobody noaccess nobody4  
  
do  
  
    echo $user >>ftpusers  
  
done  
  
# sort -u ftpusers >ftpusers.new  
  
# mv ftpusers.new ftpusers  
  
# pkgchk -f -n -p /etc/ftpd/ftpusers
```

8.4 Sendmail Sunucu Yazılımının Yapılandırılması

Solaris işletim sistemi ile birlikte ön tanımlı olarak Sendmail eposta sunucu yazılımı tcp 25. portu dinleyecek şekilde gelmektedir. Eğer sistem eposta sunucu yazılımı olarak kullanılmayacak ise ve ağ üzerindeki herhangi bir makineden eposta almasını gerektirecek bir neden yoksa **sendmail** sunucu yazılımı sadece 127.0.0.1 ip adresinde çalışacak şekilde yapılandırılmalıdır. Bu şekilde **sendmail** yazılımı için uzak bağlantılar kabul edilmeyecektir. **Sendmail** servisini sadece 127.0.0.1 ip adresini dinleyecek şekilde yapılandırmak için aşağıdaki adımlar gerçekleştirilmelidir.

```
# cd /etc/mail  
  
# awk '/DaemonPortOptions=/ && /inet6/ { print "#" $0; next };  
  
/DaemonPortOptions=/ && !/inet6/ \  

```

```
{ print $0 " , Addr=127.0.0.1"; next };  
{ print }' sendmail.cf >sendmail.cf.new  
# mv sendmail.cf.new sendmail.cf  
# pkgchk -f -n -p /etc/mail/sendmail.cf
```

8.5 Syslog Servisinin Yapılandırılması

Eğer sistem kayıt sunucu olarak kullanılmayacak ise ya da ağ üzerinden **syslog** mesajlarını alması için bir sebep yoksa **syslogd** servisi yerel olarak çalışacak şekilde yapılandırılmalıdır. Ön tanımlı olarak **syslogd** servisi ağ üzerinden **syslog** mesajlarını kabul edecek şekilde çalışmaktadır. Kullanılan protokol gereği bu işlemler esnasında hiç bir kimliklendirme işlemi olmadan gerçekleşmektedir. Bu durum kullanılarak servis dışı bırakma gibi saldırılar gerçekleştirilebilir. Bunun için aşağıdaki adımlar uygulanmalıdır:

```
# cd /etc/default  
# awk '/LOG_FROM_REMOTE=/ { $1 = "LOG_FROM_REMOTE=NO" }  
{ print }' syslogd >syslogd.new  
# mv syslogd.new syslogd  
# pkgchk -f -n -p /etc/default/syslogd
```

8.6 At ve Cron İşleri İçin Yetkili Kullanıcıların Belirlenmesi

At ve **Cron** sistem üzerinde zamanlanmış işlerin gerçekleşmesi sağlanmaktadır. Aynı şekilde “at.allow” ve “cron.allow” dosyaları da zamanlanmış görevleri gerçekleştirebilen kullanıcıları içermektedir. “cron.deny” ve “at.deny” dosyaları zamanlanmış görevleri gerçekleştiremeyen kullanıcıları içermektedir. Bu dosyada yer almayan kullanıcılar zamanlanmış işleri gerçekleştirebilmektedir. Sadece izin verilmeyen kullanıcıları belirtmektense sadece izin verilen kullanıcılar belirtilerek yetkilendirme işlemi aşağıdaki adımlar sırası ile uygulanarak sağlıklı bir biçimde gerçekleştirilebilir.

```
# cd /etc/cron.d  
# rm -f cron.deny at.deny  
# echo root >cron.allow  
# cp /dev/null at.allow  
# chown root:root cron.allow at.allow
```

```
# chmod 400 cron.allow at.allow
```

8.7 Boş Crontab Dosyalarının Belirlenmesi ve Erişim Yetkilerinin Ayarlanması

Sistem üzerinde bulunan **crontab** dosyaları sadece **root** kullanıcı yetkileri ile çalıştırılan cron servisi tarafından ve **crontab** komutu tarafından erişilebilir. Boş **crontab** dosyaları bulunmalı ve sistemden kaldırılmalı. Bunun yanında ayrıca **crontab** dosyalarının erişim yetkileri de sıkılaştırılmalıdır. Bunun için aşağıdaki adımlar sırası ile uygulanmalıdır.

```
# for file in /var/spool/cron/crontabs/*
do
    lines=`grep -v '^#' $file | wc -l | sed 's/ //g'`
    if [ "$lines" = "0" ]
    then
        crontab -r $file
    fi
done
# chown root:sys /var/spool/cron/crontabs/*
# chmod 400 *
```

9. KULLANICI HESAPLARININ DENETİMİ

9.1 Sistem Hesaplarının Engellenmesi

Sistemdeki düzenli kullanıcılar tarafından kullanılmayan kullanıcı hesapları ile sisteme erişim gerçekleştirilmesi engellenmelidir. Bu işlem “/etc/shadow” dosyasında istenilen kullanıcı için *LK* karakter dizgisi eklenerek sağlanabilir ya da **passwd -l** kullanıcı_adı ile gerçekleştirilebilir. Yalnız sadece sisteme erişim gerçekleştirilmesi istenmeyen kullanıcılar için **passwd** komutunun -l parametresi ile çalıştırılmasının yanında bu kullanıcıların kabukları da değiştirilmelidir. “/dev/null” geçerli bir kabuk değeri olmadığı için kullanılabilir. Ayrıca **passwd** komutuna -l parametresi verilerek bir kullanıcı için kullanıldığı da bu kullanıcı için bütün **cron** işleri geçersiz kılınmış olur. Bunun için aşağıdaki adımlar uygulanmalıdır.

```
# passwd -l daemon
# for user in bin nuucp smmsp listen gdm webservd nobody noaccess nobody4
do
    passwd -l $user
    /usr/sbin/passmgmt -m -s /dev/null $user
done
# passwd -N sys
# for user in adm lp uucp
do
    passwd -N $user
    /usr/sbin/passmgmt -m -s /dev/null $user
done
#
```

9.2 Sistem Üzerinde Şifresi Boş Olan Kullanıcıların Tespit Edilmesi

Saldırgan ya da kötü niyetli kişiler sistem üzerinde boş şifresi bulunan kullanıcıların kullanıcı adını kullanarak hiçbir şifre bilgisi olmadan sisteme kolaylıkla erişim sağlayabilir. Sistem üzerinde bulunan bütün kullanıcıların şifresi olmalı ve bu şifre seçimi sistem güvenlik politikasına uygun bir seçilmelidir. Sistem üzerinde bulunan şifresi olmayan kullanıcıları tespit etmek için aşağıdaki adım uygulanır. Sistem üzerinde boş şifresi olan kullanıcıları doğrulamak için **logins** -p komutunun çıktısı boş olmalıdır.

```
# logins -p
```

9.3 Güvenli Şifre Politikasının Atanması

Kullanıcının sisteme başarılı bir şekilde giriş gerçekleştirebilmesi için kullanıcı adı ve şifre bilgilerini doğru olarak kullanıcıya sunulan ekrandan girmesi gerekmektedir. Bundan dolayı da kullanıcı şifre seçimi sistem güvenliği açısından önemli bir yer tutmaktadır. Sistem üzerinde bulunan kullanıcılar için güvenli şifre politikası belirlenip uygulanmalıdır. Aşağıda belirtilen değerler önerilen değerler olmakla beraber sistem güvenlik politikasına göre değişiklik gösterebilir. Burada belirlenen politikaya göre kullanıcılar 91 gün içerisinde şifrelerini değiştirmeli ve 28 gün önceden şifrelerini değiştirme tarihi kullanıcıya bildiriliyor ve ayrıca 7 gün içerisinde şifre değiştirmeye izin verilmiyor.

```
# logins -ox |awk -F: '($1 == "root" || $8 == "LK") { next }
{ $cmd = "passwd" }
($11 <= 0 || $11 > 91) { $cmd = $cmd " -x 91" }
($10 < 7) { $cmd = $cmd " -n 7" }
($12 < 28) { $cmd = $cmd " -w 28" }
($cmd != "passwd") { print $cmd " " $1 }' > /etc/upd_accounts
# /sbin/sh /etc//etc/upd_accounts
# rm -f /etc//etc/upd_accounts
# cd /etc/default
# grep -v WEEKS passwd >passwd.new
# cat <<EODefaults >>passwd.new
MAXWEEKS=13
MINWEEKS=1
```

```
WARNWEEKS=4

EODefaults

# mv passwd.new passwd

# pkgchk -f -n -p /etc/default/passwd
```

Sistem üzerinde bulunan kullanıcılar için belirlenen şifre değiştirme politikasının yanında kullanıcıların şifre değiştirme zamanlarında seçecekleri şifrelerin politika gereği güçlü şifreleri olması sağlanmalıdır.

```
# cd /etc/default

# awk '/PASLENGTH=/ { $1 = "PASLENGTH=6" };

/NAMECHECK=/ { $1 = "NAMECHECK=YES" };

/HISTORY=/ { $1 = "HISTORY=4" };

/MINDIFF=/ { $1 = "MINDIFF=3" };

/MINALPHA=/ { $1 = "MINALPHA=2" };

/MINUPPER=/ { $1 = "MINUPPER=1" };

/MINLOWER=/ { $1 = "MINLOWER=1" };

/MINNONALPHA=/ { $1 = "MINNONALPHA=1" };

/MAXREPEATS=/ { $1 = "MAXREPEATS=2" };

/WHITESPACE=/ { $1 = "WHITESPACE=YES" };

/CTIONDBDIR=/ { $1 = "CTIONDBDIR=/var/passwd" };

/CTIONLIST=/ \

{ $1 = "CTIONLIST=/usr/share/lib/dict/words" };

{ print }' passwd >passwd.new

# mv passwd.new passwd

# pkgchk -f -n -p /etc/default/passwd
```

En az kaç şifrenin arka arkaya kullanılamayacağı ya da sözlük kullanımı gibi şifre kullanım politikaları sistem güvenlik politikasına göre belirlenebilir.

9.4 Sistem Üzerinde Bulunan Root Yetkili Kullanıcıların Tespit Edilmesi

Sistem üzerinde bulunan ve UID'si 0 olan kullanıcılar **root** kullanıcı yetkilerine sahip olmaktadır. Ön tanımlı olarak sadece **root** kullanıcısı bu yetkilere sahiptir ve sistem politikası gerektirmiyorsa başka bir kullanıcıya **root** kullanıcı hakları verilmemelidir. Sistem üzerinde **root** kullanıcı haklarına sahip kullanıcıları tespit etmek için kullanıcıları tespit etmek için aşağıdaki adım gerçekleştirilmelidir.

```
# logins -o | awk -F: '($2 == 0) { print $1 }'
```

9.5 Root Kullanıcısının Dahil Olduğu Grubun Root Grubu Olarak Ayarlanması

root kullanıcısı için ön tanımlı grup olarak GID'si "0" olan **root** grubu olmalıdır. Bunun için Solaris 9 ve öncesi sürümlerinde **root** grubu yoktu ve sistem üzerinde bulunan diğer kullanıcılar tarafından paylaşılacak olan "other" grubu kullanılıyordu. **root** kullanıcısını **root** grubuna eklemek için aşağıdaki adım gerçekleştirilmelidir.

```
# passmgmt -m -g 0 root
```

9.6 Kullanıcı Ev Dizini Yetkilerinin Belirlenmesi

Sistem üzerinde bulunan kullanıcı ev dizinlerinin erişim yetkilerinin herkes tarafından yazılabilir olması bu dizinler içerisinde yer alan dosyaların okunmasına ya da değiştirilmesine neden olabilir. Bunu önlemek için grup yetkilerinden yazma diğer kullanıcılar için kullanılan yetkiler için bütün yetkiler alınmalıdır. Bu yetki kalıbı sistem politikasına göre değişiklik gösterebilir. Bunun için aşağıdaki adımlar gerçekleştirilmelidir.

```
# for dir in `logins -ox | awk -F: '($8 == "PS" && $1 != "root") { print $6 }`  
do  
    chmod g-w $dir  
    chmod o-rwx $dir  
done  
#
```

9.7 Kullanıcı Dizinlerinde Bulunan.netrc Dosyalarının Kaldırılması

“.netrc” ağ üzerinden uzak sistemlere FTP ile otomatik olarak dosya transferi yapmak için veriler içeren dosyadır. “.netrc” dosyası içerisinde kullanıcı adı ve şifre bilgileri açık halde bulunmaktadır. Kullanıcı ev dizinin de bulunan. “.netrc” dosyalarını sistemden kaldırmak için aşağıdaki adımlar gerçekleştirilmelidir.

```
# for dir in `logins -ox |awk -F: '($8 == "PS") { print $6 }`  
  
do  
  
    rm -f $dir/.netrc  
  
done  
  
#
```

9.8 Kullanıcılar İçin Ön Tanımlı Umask Değerinin Belirlenmesi

umask değeri ile sistem üzerinde oluşturulan dosya ve dizinler için ön tanımlı yetki kalıbı belirlenir. **umask** değerinin 077 olarak belirlenmesi ile dosya ve dizinlerin sahibi dışında kalan kullanıcılar için okuma ve yazma hakkı olmadan yetki kalıbı belirlenebilir. **umask** değeri 022 yapılarak diğer kullanıcılar için oluşturulan dosya ve dizinlere yazma hakkı verilmemiş olur. **umask** değeri belirlenecek politikaya göre değişiklik gösterebilir. Daha katı bir **umask** değeri de kullanılabilir. **umask** değerinin 022 olarak belirlenmesi için aşağıdaki adımlar gerçekleştirilmelidir.

```
# cd /etc/default  
  
# awk '/UMASK=/ { $1 = "UMASK=022" } { print }' login >login.new  
  
# mv login.new login  
  
# cd /etc  
  
# for file in profile .login  
  
do  
  
    if [ "`grep umask $file`" ]  
  
    then  
  
        awk '$1 == "umask" { $2 = "022" } { print }' $file > $file.new  
  
        mv $file.new $file  
  
    else
```

```
        echo umask 077 >>$file

    fi

done

# pkgchk -f -n -p /etc/default/login
# pkgchk -f -n -p /etc/profile
# pkgchk -f -n -p /etc/.login
```

9.9 FTP Kullanıcıları İçin Kullanılacak Öntanımlı Umask Değerinin Belirlenmesi

Ftp kullanıcıları için kullanılabilir ön tanımlı **umask** değeri “/etc/ftpd/ftpaccess” dosyasından belirlenir. Belirtildiği üzere **umask** değeri belirlenen güvenlik politikasına göre değişiklik gösterebilir.

```
# cd /etc/ftpd
# if [ "`grep '^defumask' ftpaccess`" ]
    then
        awk '/^defumask/ { $2 = "022" } { print }' ftpaccess
>ftpaccess.new
        mv ftpaccess.new ftpaccess
    else
        echo defumask 022 >>ftpaccess
    fi
# pkgchk -f -n -p /etc/ftpd/ftpaccess
```

10. UYARI MESAJLARININ YAPILANDIRILMASI

10.1 Standart Giriş Servisleri İçin Uyarı Mesajlarının Yapılandırılması

Sistem konsolunda ya da telnet ile sisteme giriş yapmadan önce “/etc/issue” dosyasının içeriği ekrana bastırılır. Sisteme gerçekleştirilen başarılı girişlerin ardından ise “/etc/motd” dosyasının içeriği ekrana bastırılır. Bu bilgilerin ekrana bastırılması yerine belirlenen politikaya göre istenen mesajlar ekrana bastırılarak sistem hakkında daha az bilgi verilmiş olur. Bunun için aşağıdaki adımlar gerçekleştirilir.

```
# echo "Sadece yetkili kullanım için ..." > /etc/motd
# echo " Sadece yetkili kullanım için ..." >/etc/issue
```

```
# pkgchk -f -n -p /etc/motd
# chown root:root /etc/issue
# chmod 644 /etc/issue
```

10.2 Grafiksel Ara Yüz İçin Uyarı Mesajının Belirlenmesi

Kullanıcının sisteme başarılı bir biçimde giriş gerçekleştirebilmesi için kullanıcının standart ara yüz ile karşısına gelen kullanıcı adı ve şifre bilgisini doğru bir biçimde belirtmesi gerekmektedir. Kullanıcı adı bilgisi ile kullanılan birinci kullanıcı dialog ara yüz uyarı mesajı “Dtlogin*greeting.labelString” ile belirlenir. Kullanıcı şifre ekran bilgisi ile kullanılan kullanıcı dialog arayüz ekranı ise “perslabelString” ile belirlenir. Belirlenen sistem politikasına göre istenen uyarı mesajları belirtilmelidir.

```
# for file in /usr/dt/config/*/Xresources
do
    dir=`dirname $file | sed s/usr/etc/`
    mkdir -p $dir
    if [ ! -f $dir/Xresources ]
    then
        cp $file $dir/Xresources
    fi
    echo          'Dtlogin*greeting.labelString:  Authorized  uses  only!'
>>$dir/Xresources
    echo 'Dtlogin*greeting.persLabelString: All activity may be monitored.'
>>$dir/Xresources
done
# chown root:sys /etc/dt/config/*/Xresources
# chmod 644 /etc/dt/config/*/Xresources
cd /etc/X11/gdm
awk '/^#?Greeter=/ \
{ print "Greeter=/usr/bin/gdmlogin"; next }
/^#?Welcome=/ \
{ print "Welcome=Authorized uses only!\n" \
```

```
"All activity may be monitored " \  
"and reported."  
next }  
{ print }' gdm.conf >gdm.conf.new  
mv gdm.conf.new gdm.conf  
pkgchk -f -n -p /etc/X11/gdm/gdm.conf
```

10.3 FTP Sunucu Servisi İçin Uyarı Mesajının Belirlenmesi

Solaris işletim sistemi ile ön tanımlı olarak kullanılan FTP sunucu servisi için uyarı mesajı “/etc/ftpd/banner.msg” dosyasında belirtilir. Eğer sistemde FTP sunucu servisi hizmet verecek ise belirlenen sistem politikasına göre gerekli uyarı mesajı FTP servisi için belirlenmelidir.

```
# echo Authorized uses only. All activity may \  
be monitored and reported. >/etc/ftpd/banner.msg  
# chown root:root /etc/ftpd/banner.msg  
# chmod 444 /etc/ftpd/banner.msg
```

10.4 Sistem Açılış Uyarı Mesajlarının Belirlenmesi

Bu ayar sadece SPARC tabanlı sistemlerde uygulanabilmektedir. Sistem açılışındaki uyarı mesajını belirlenen politikaya göre istenen biçimde belirlemek için aşağıdaki adımlar gerçekleştirilmelidir.

```
# eeprom oem-banner="Authorized uses only. All activity \  
may be monitored and reported."  
# eeprom oem-banner\?=true
```

KAYNAKÇA

- [1] <http://www.cisecurity.org/>
- [2] <http://docs.sun.com/app/docs>
- [3] <http://www.sun.com/blueprints/0100/security.pdf>
- [4] Unix, Solaris And Linux: A Practical Security Cookbook
ISBN-10: 1420807056
ISBN-13: 978-1420807059
- [5] Sun Certified Security Administrator for Solaris 9 & 10 Study Guide
ISBN-10: 0072254238
ISBN-13: 978-0072254235
- [6] J. Michael Stewart, Ed Tittel, Mike Chapple, *Certified Information System Security Professional*, 3. Edition, 2005, ISBN ISBN-10: 0072254238, Sybex Inc.