Linux Sistem Güvenliği (Hardening)

Fatih Özavcı
IT Security Consultant

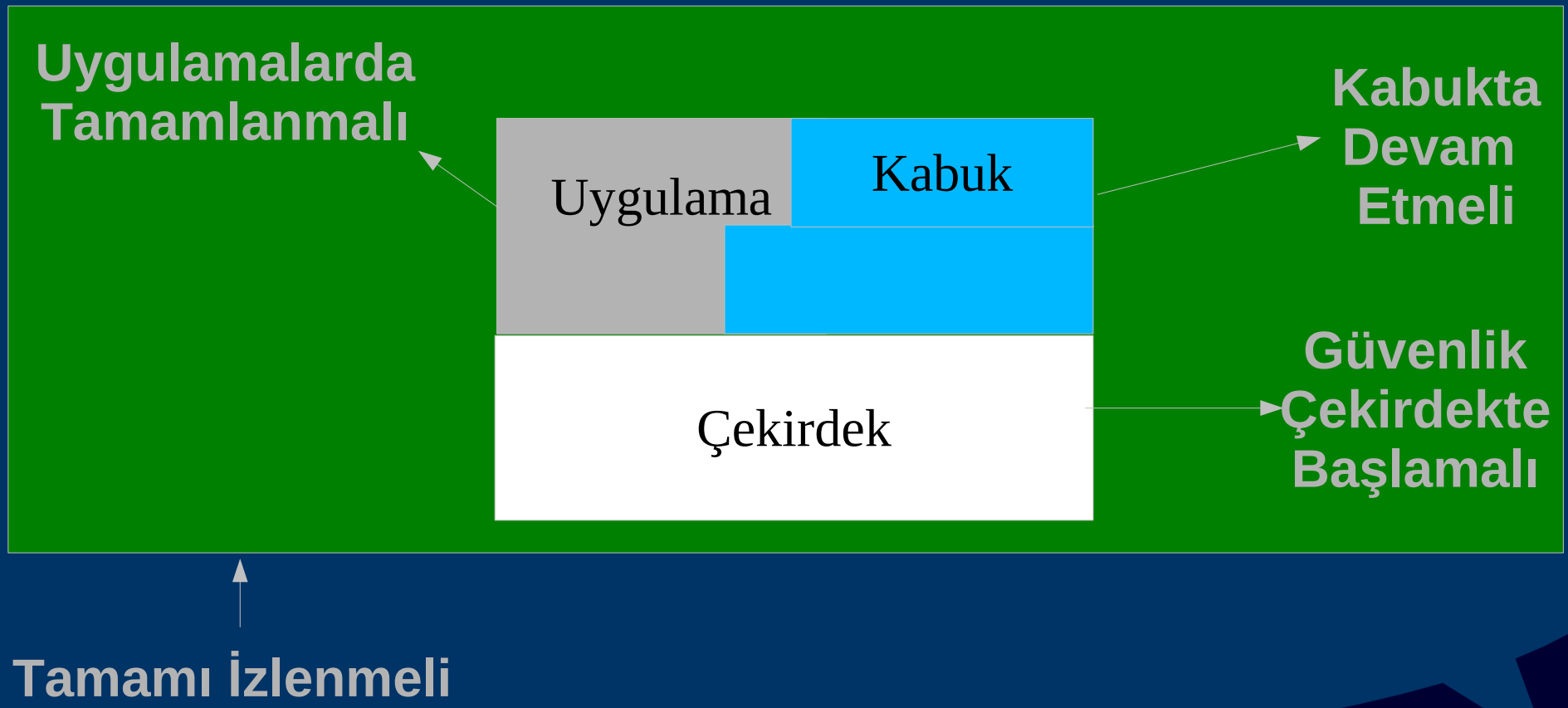
f.ozavci@btg.com.tr
http://www.btg.com.tr

holden@siyahsapka.com
http://www.siyahsapka.com

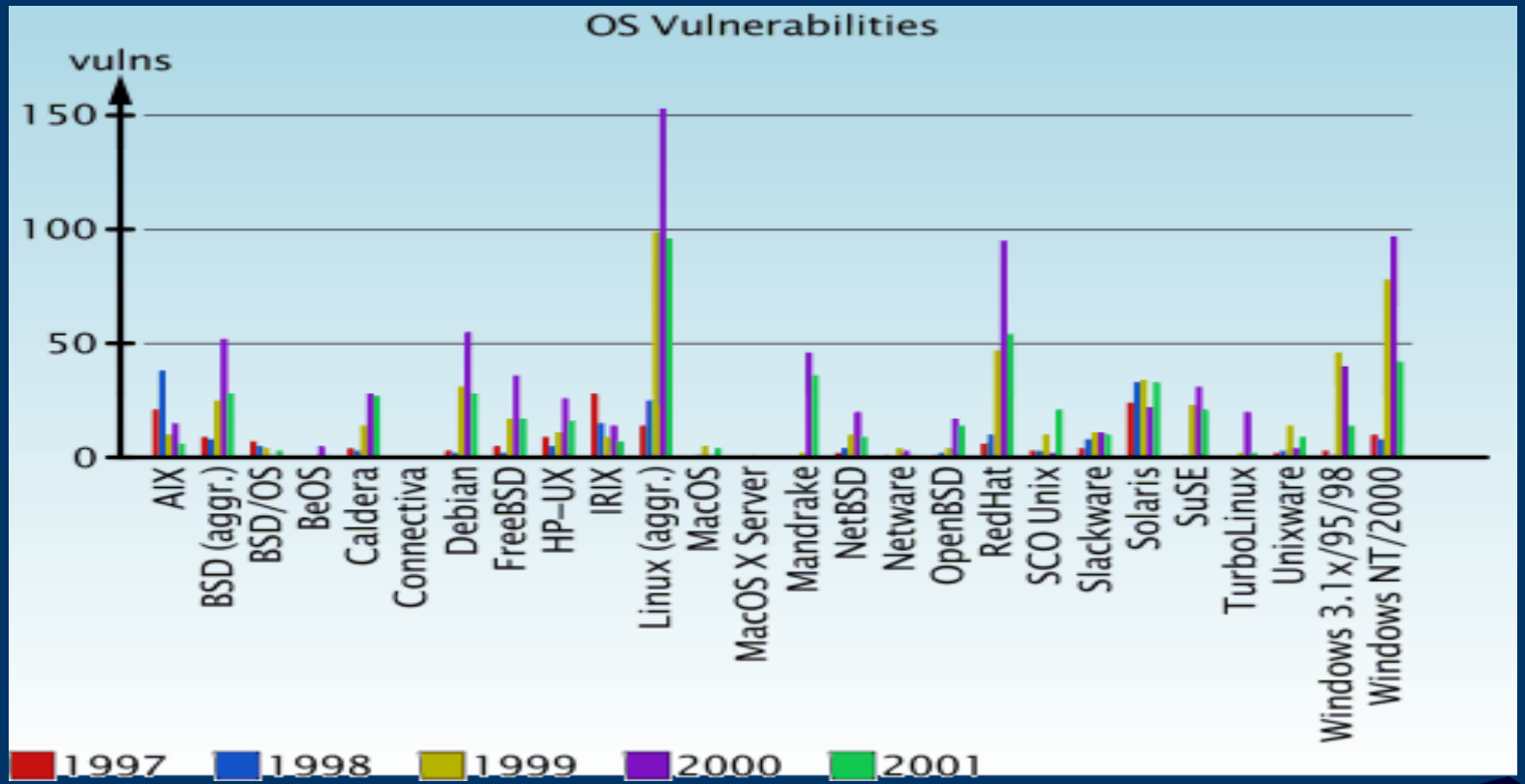
GNU/Linux

- Linux Çekirdeği Linus Torvalds Tarafından Geliştirilmiş ve İlk Sürüm 25 Ağustos 1991'de Duyurulmuştur
- Free Software Foundation'ın Hamiliğini Yaptığı GNU Projesi ile Birleştirilerek GNU/Linux İşletim Sistemi Oluşturulmuştur
- GPL Lisansı ile Dağıtılmaktadır
- Açık Kaynak Kodludur ve Gelişimi Gönüllü Kişilerce Yürütülmektedir
- Çok Kullanıcılı ve Çok Görevlidir
- Ölçeklenebilir, Farklı Mimariler ve Donanımlarda Çalışabilmektedir
- Açık Kaynaklı Olduğu İçin Güvenilirdir
- Linux Çekirdeği, Gnu Araçları ve Çeşitli Uygulamaları İçeren Birçok Linux Dağıtımı Bulunmaktadır

Linux'un Yapısı



İşletim Sistemi Zayıflıkları



Security Focus (http://online.securityfocus.com)

Hardening

- Bir Sunucu Üzerinde Daha Önceden Belirlenen Güvenlik Politikalarının Uygulanmasıdır
-
- Bazı Bileşenleri
  - Fiziksel Güvenlik
  - Kullanıcı / Grup Yönetimi
  - Dosya Sistemi Güvenliği
  - Süreç Yönetimi
  - Servis Güvenliği
  - Yazılım Güvenliği
  - Çekirdek Güvenliği
  - Süreç, Kullanıcı, Sistem ve Çekirdek İzleme
  - Uzak Yönetimi Güvenliği

Dağıtım Seçimi

- Standart Dağıtımlar
-
- Redhat
- Suse
- Mandrake
- Debian
- Slackware
- Gento
- Turbo Linux

- Güvenlik Temelli Dağıtımlar
-
- EnGarde
- Immunix
- Trustix
- Kaladix
- Astaro

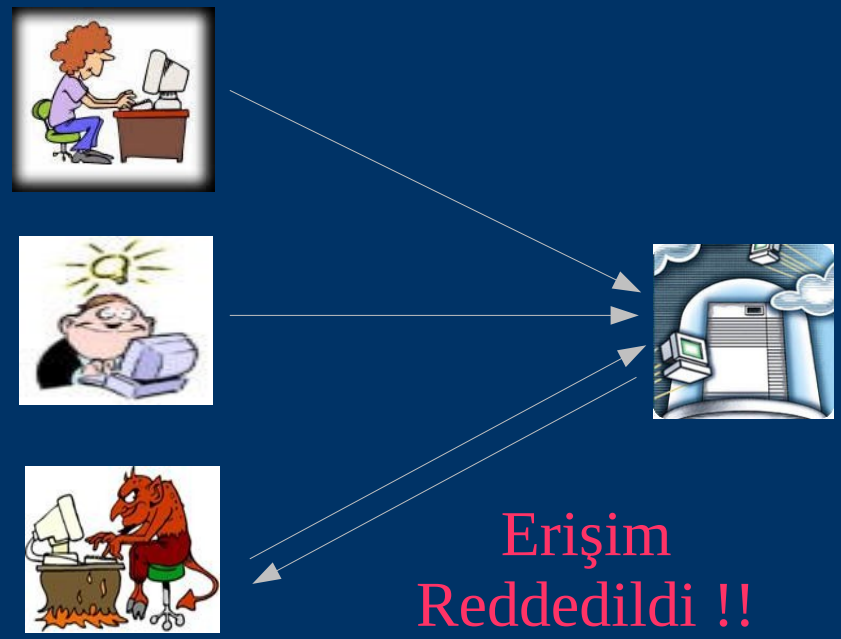
- Standart Dağıtımlar Daha Kullanışlı, Ancak Mutlaka Güvenliği Arttırılmalı

Fiziksel Güvenlik

- Sunucu Kasası Kilitlenebilir Olmalıdır
- Güç Kaynağı Kullanılmalıdır
- BIOS'tan Sabit Disk Dışındaki Açılış Seçenekleri Kaldırılmalıdır (Disket,CD,USB vb.)
- BIOS'a Şifre Koyulmalı ve BIOS'a Girişler Engellenmelidir
- İşletim Sisteminin Açılış Yöneticisine Şifre Koyulmalıdır (Lilo, Grub vb.)

Kullanıcı / Grup Yönetimi

- Sistemde Sadece Gerekli Olan Kullanıcılar ve Gruplar Bulunmalıdır
- Yetkiler Gruplara Verilmeli, Kullanıcılar Gruplara Dahil Edilmelidir
- Kullanıcılar Merkezi Bir Veritabanında Tutulmalı ve Tek Merkezden Doğrulanmalılar
- Kullanıcı Şifreleri ve Girişleri Zorlayıcı Politikalara Bağlı Olmalıdır



Şifre Kalitesi ve Politika Zorlaması

- Kullanıcı Şifreleri ve Girişleri Mutlak Bir Politikaya Bağlanmalıdır
-
- Örnek :
  - Kullanıcı Şifreleri En Az 5 En Çok 8 Karakter Olmalıdır
  - Kullanıcılar Şifrelerini 30 Günde Bir Değiştirmelidir
  - Tekrar Şifre Değiştirmek İçin En Az 5 Gün Beklenmelidir
  - Kullanıcı Şifre Değiştirmesi İçin 3 Gün Önce Uyarılmalıdır
  - 30 Gün Boyunca Şifresi Değişmeyen Hesap Geçici Olarak Kapatılmalıdır
  - Kullanıcıların 3 Hatalı Şifre Girişinden Sonra Hesap Geçici Olarak Kapatılmalıdır

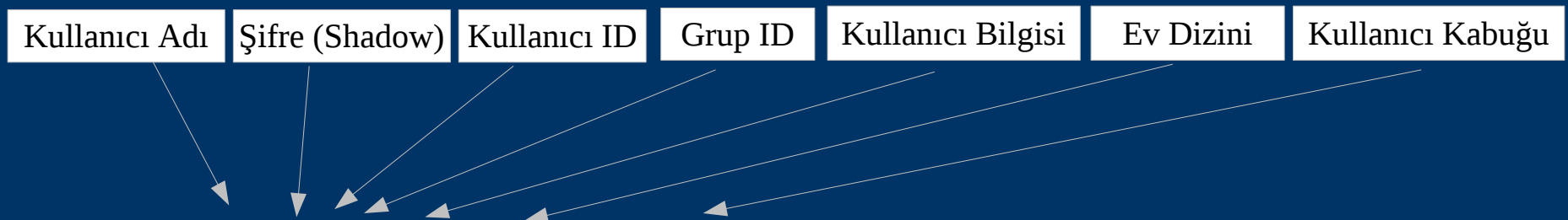
Pluggable Authentication Modules

- Harici Doğrulama Mekanizmalarının Kullanılmasını Sağlamaktadır
- Farklı Veritabanları Aracılığıyla Merkezi Kullanıcı Yönetimine Yardımcı Olmaktadır
- Kullanıcıların Girişlerinin Sınırlandırılmasını Sağlamaktadır
- Kullanıcıların Belirli Bir Dizine Hapsedilebilmesini Sağlamaktadır
- Şifrelerin Kolay Tahmin Edilebilir Olup Olmadığını Kontrol Edebilmektedir
- Kullanıcıların Çevre Değişkenlerinin Atanmasını Sağlayabilmektedir
- Grup Yönetimini Sağlamakta ve Kullanıcıların Ait Oldukları Gruplar Aracılığıyla Yetkilerinin Düzenlenmesini Sağlamaktadır
- Kullanıcılara Giriş Mesajları Verilmesini Sağlamaktadır

PAM Bileşenleri

- PAM_Access
- PAM_CHROOT
- PAM_Cracklib
- PAM_Deny
- PAM_Env
- PAM_FILTER
- PAM_Ftp
- PAM_Group
- PAM_Issue
- PAM_Krb4
- PAM_Lastlog
- PAM_Limits
- PAM_Listfile
- PAM_wam
- PAM_Mail
- PAM_Motd
- PAM_Nologin
- PAM_Permit
- PAM_pwdb
- PAM_radius
- PAM_rhosts_auth
- PAM_rootok
- PAM_securetty
- PAM_tally
- PAM_Time
- PAM_Unix
- PAM_userdb
- PAM_Wheel

/etc/passwd



- root:x:0:0:root:/root:/bin/bash
- bin:x:1:1:bin:/bin:/bin/bash
- daemon:x:2:2:Daemon:/sbin:/bin/bash
- lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
- mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
- games:x:12:100:Games account:/var/games:/bin/bash
- man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
- news:x:9:13:News system:/etc/news:/bin/bash
- nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
- uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash

/etc/shadow

- root:1Hodfgvr8o:12056:0:10000: : : :
- bin:*:8902:0:10000::::
- daemon:*:8902:0:10000::::
- lp:*:8902:0:10000::::
- mail:*:8902:0:10000::::
- games:*:8902:0:10000::::
- man:*:8902:0:10000::::
- news:*:8902:0:10000::::
- nobody:*:8902:0:10000::::
- uucp:*:8902:0:10000::::
- postfix:!:12039:0:99999:7:::

Diğer Önemli Yapılandırma Dosyaları

- /etc/group - Grup Özelliklerinin Tutulduğu Dosya
- /etc/gshadow - Grup Şifrelerinin Tutulduğu Dosya
- /etc/login.defs - Kullanıcıların Sisteme Giriş Seçeneklerinin Tutulduğu Dosya
- /etc/shells - Sistemdeki Geçerli Kabukların Tutulduğu Dosya
- /etc/securetty - “root” Kullanıcısının Girebileceği Terminallerin Tutulduğu Dosya
- /etc/security/ - PAM Yapılandırma Dosyalarının Bulunduğu Dizin
- /etc/issue - Sisteme Girişteki Karşılama Mesajı
- /etc/ftpusers - Sisteme FTP ile Giremeyecek Kullanıcıların Tutulduğu Dosya

Kullanıcı Yönetim Komutları

- useradd - Kullanıcı Ekler
- userdel - Kullanıcı Siler
- groupadd - Grup Ekler
- groupdel - Grup Siler
- w - Giriş Yapmış Kullanıcıları ve Bilgilerini Listeler
- who - Giriş Yapmış Kullanıcıları ve Bilgilerini Listeler
- whoami - Çalıştıran Kullanıcının Adını Verir
- passwd - Kullanıcıya Şifre Atanmasını veya Değiştirilmesini Sağlar
- ulimit - Kullanıcılara Limit Atanmasını Sağlar

su / sudo Kullanımı

- su : Kullanıcıların, kullanıcı değiştirmesini sağlar. Kullanıcı belirtilmezse varsayılan kullanıcı “root”tur.
- sudo : Kullanıcıların belirli yetkilerle farklı kullanıcıların haklarına sahip olmasını sağlar. /etc/sudoers yapılandırma dosyası aracılığıyla kullanıcıların, yetkileri olmayan işlemleri sadece belirtilen haklarla yapmasını sağlamaktadır.
  -
  - Örnek:
  -
  - #Tüm Kullanıcıların Cdrom'u Bağlayabilmesini ve Çözebilmesini Sağlar
  - %users ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
  -
  - #Wheel Grubunun Şifre Kullanmadan “root” Olabilmesini Sağlar
  - %wheel ALL=(ALL) NOPASSWD: ALL

Dosya Sistemi Güvenliği

- Önemli Dizinler Farklı Disk Bölümlerinde Bulunmalıdır, Böylece Kota Koyulabilir, Sadece Okunabilir Olarak Bağlanabilir, SUID ve GID Kullanılmaması Seçenekleri Kullanılabilir
- Önemli Yapılandırma Dosyaları ve Çalıştırılabilir Programların Yetkileri Gözden Geçirilmeli, Gerekenden Fazla Yetki Verilmemelidir
- Sistemde SUID veya SGID Bitine Sahip Hiç Bir Program Bulunmamalıdır
- Tüm Dosya / Dizinlerin Tarih, Tür ve Büyüklüğü Düzenli Olarak Kontrol Edilmelidir
- Sistemdeki Açık Dosyalar Sürekli Takip Edilmeli ve Kayıt Edilmelidir
- Sahipsiz Dosyalar Bulunmalı ve Sahiplendirilmelidir
- Herkesin Yazabileceği Dosyalar Bulunmalı ve Bu Özellikleri Alınmalıdır

Dosya ve Dizin Yetkileri

- Bir dosyaya okuma, yazma ve çalıştırma hakları verilebilir
- Bir dizine okuma, yazma ve içine göz atabilme hakları verilebilir
- Yetkiler, dosyanın sahibi, dosyanın sahibinin ait olduğu grup ve diğer kullanıcılar bazında verilebilir
- İstenmesi durumunda özel haklar olan SUID, SGID ve Sticky haklarının verilmesi mümkündür

Dosya/Dizin Yetki Değişim Komutları

- chmod Dosya/Dizin yetkilerinin değiştirilmesini sağlamaktadır
  - chmod u+x dosya_adi
  - chmod 755 dosya_adi
  - chmod 4777 dosya_adi
- chown Dosya/Dizin sahiplerinin değiştirilmesini sağlamaktadır
  - chown fatih dosya_adi
  - chown fatih:users dosya_adi
- chgrp Dosya/Dizin gruplarının değiştirilmesini sağlamaktadır
  - chgrp users dosya_adi
- umask Yaratılan dosya ve dizinlerin varsayılan haklarının belirlenmesini sağlamaktadır
  - umask 222
- chattr Dosya özelliklerinin değiştirilmesini sağlamaktadır
  - chattr +a dosya_adi
- lsattr Dosya özelliklerinin listelenmesini sağlamaktadır
  - lsattr dosya_adi

SUID ve SGID Programlar

- “root” Haklarına Sahip Olmayan Kullanıcıların Belirli İşlemleri Yapabilmesi Amacıyla Kullanıcı Yerine Programa Yetki Verilmesi Gerekli Olabilir
- “root” Kullanıcısı Hakları için SUID, “root” Grubu Hakları için SGID Yetkileri Verilmektedir
- SUID ve SGID Yetkilerine Sahip Programların İstismar Edilmesiyle Kötü Niyetli Kullanıcılar Yüksek Haklar Ele Geçirebilir. Bu Sebeple Sistemde Bu Yetkilere Sahip Programların Yetkileri Alınmalıdır
- SUID ve SGID Programları Bulmak İçin
  - find / -perm +2000 -ls
  - find / -perm +4000 -ls
- Dosya/Dizinin SUID ve SGID Yetkilerini Almak İçin
  - chmod -s dosya_adi

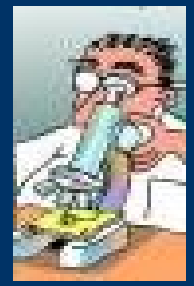
/etc/fstab Yapısı

/dev/hda1	/	ext3	nosuid,rw	1 1
/dev/hda3	/home	ext2	grpquota	1 2
/dev/hda6	/usr	ext3	nosuid,noexec,ro	1 2
/dev/hda2	swap	swap	pri=42	0 0
devpts	/dev/pts	devpts	mode=0620,gid=5	0 0
proc	/proc	proc	defaults	0 0
usbdevfs	/proc/bus/usb	usbdevfs	noauto	0 0

- nosuid : SUID bitli programların çalışması engellenir
- noexec : Herhangi bir programın çalışması engellenir
- grpquota, usrquota, noquota, quota : Kota uygulanması sağlanır
- ro : Sadece okunabilir olarak bağlanması sağlanır
- * : Tüm parametreler “mount” komutu ile de kullanılabilir

Bütünlük Doğrulama Sistemleri

- Dosya ve Dizinlerin Özelliklerini Bir Dosyada, Kriptolu Olarak Kayıt Ederler
- Çeşitli Zaman Aralıklarıyla Değişikliklerin Farkedilmesi ve Önlem Alınmasını Sağlarlar
- MD5, SHA-1 ve RMD60 Algoritmalarını Kullanabilirler
-
- Sıkça Kullanılan Bütünlük Doğrulama Sistemleri
  - Tripwire : http://www.tripwire.org
  - AIDE : http://www.cs.tut.fi/~rammer/aide/



Yazılım Yönetimi

- Sistemde Sadece Gerekli Yazılımlar Kurulu Olmalıdır
- Tüm Yazılımlara Gerekli Olan Yetkiler Verilmelidir
- Yazılımların Güvenlik Güncellemeleri Mutlaka Yapılmalıdır
- Yazılım Yükleme/Güncellemelerinde MD5 Bütünlük Toplamları ve PGP İmzaları Mutlaka Kontrol Edilmelidir

Zamanlanmış Görevler

- Cron ve AT'ye Görev Yükleyebilecek Kullanıcılar Belirlenmelidir
- /etc/crontab ve cron.* Dizinlerinin Yetkileri Gözden Geçirilmelidir
- “at” Grubunda Bulunan Kullanıcılar Gözden Geçirilmelidir
- Gerekmiyorsa AT Sistemden Kaldırılmalı ve Cron Kullanılmalıdır

Ağ Servisleri Güvenliği

- Sadece Gerekli Olan Servisler Kullanılmalıdır
- Uygulamaların Yapılandırma Dosyaları Dikkatlice Okunmalı ve Varsayılan Yapılandırma Değiştirilmelidir
- Uygulama Seçiminde Güvenlik Kriteri Gözönüne Alınmalıdır
- Tüm Duyurulan Yamalar ve Güncellemeler Vakit Geçirmeden Uygulanmalıdır
- Inetd Kullanımı Gerekiyorsa Yerine Daha Güvenli Olan Xinetd Kullanılmalıdır
- Mümkünse Tüm Servisler SSL Aracılığıyla Sunulmalıdır
- Kullanılması Zorunlu Ancak Güvenilmeyen Uygulamalar Chroot() Yapılmalıdır

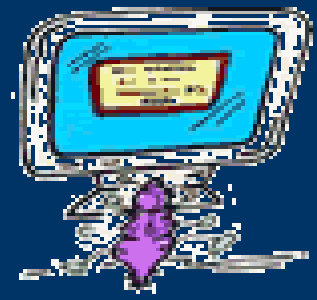
Tehlikeli Ağ Servisleri

- Telnet
- r* Hizmetleri
- Echo
- RPC Uygulamaları
- Time
- Talk/Ntalk
- NFS
- NIS
- Finger
- Systat
- Netstat
- X Sunucusu

- SSH
- Samba
- LDAP

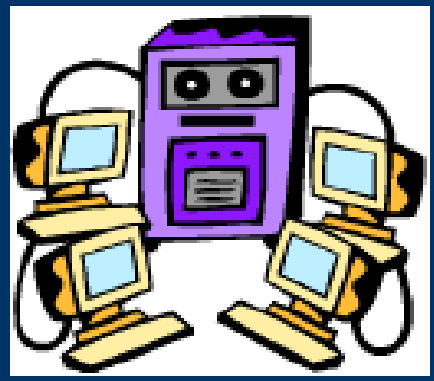
Sistem Kayıtları

- Tüm Kullanıcı Girişleri /etc/login.defs ve PAM Aracılığıyla Kayıt Edilmelidir
- “lsof” Aracılığıyla Sürekli Sistemdeki Açık Olan Dosyalar İzlenmelidir
- Tüm Sunucu Uygulamalarının Syslog Aracılığıyla Kayıt Tutması Sağlanmalıdır
- Sunucu Kayıtları “tail -f dosya_adı” Komutu ile Sürekli Olarak İzlenmelidir
- Syslog Sunucusunun Yeterli Olmadığı Durumlarda SQL Veritabanı Desteği Verilmeli yada Evlog Kullanılmalıdır
- Tüm Log Dosyaları Sadece Ekleme Özelliklerine Sahip Olmalıdır



Syslog Yapılandırması

- /etc/syslog.conf (Örnek)
  - Gerçek Zamanlı Konsoldan Log İzleme İçin
    - *.* /dev/tty10
  - Tüm E-Posta Uyarıları İçin
    - mail.* -/var/log/mail
- Syslog-ng Kullanarak Tüm Sistem Kayıtları Ayrı Bir Sunucuya Atılabilir
- Syslog+pgsql Yaması ile Tüm Kayıtlar PostgreSQL Sunucusuna Atılabilir
- Syslog+mysql Yaması ile Tüm Kayıtlar MySQL Sunucusuna Atılabilir



Çekirdek Güvenliği

- Her Sunucu İçin Özel Olarak Çekirdek Derlenmelidir, Sadece Gerekli Özellikler Dahil Edilmelidir
- Gerekiyorsa Kaynak Kodda “root” Yetkileri Kısıtlanmalıdır
- Çekirdek Güvenliği İçin Mutlaka Uygun Yamalar Uygulanmalıdır
  - Secure Linux Yaması - http://www.openwall.com/linux
  - LIDS (Linux Intrusion Detection System) - http://www.lids.org
  - RSBAC (Rule Set Based Access Control) - http://www.rsbac.de/rsbac
  - LOMAC (Low Water-Mark MAC) - ftp://ftp.tislabs.com/pub/lomac
  - Auditd - ftp://ftp.hert.org/pub/linux/auditd
  - Fork Bomb Defuser - http://rexgrep.tripod.com/rexfbdmain.htm
  - Netfilter - http://www.netfilter.org
  - GRSecurity - http://www.grsecurity.org
  - FreeSwan - http://www.freeswan.org

Ağ İçin Çekirdek Düzenlemesi - 1

- Tüm Ping Paketlerinin Gözardı Edilmesi
  - echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
- Yayın Adresi Ping Paketlerinin Gözardı Edilmesi
  - echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
- Bozuk ICMP Hata Cevaplarını Gözardı Etmek
  - echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
- Hedefi İmkansız Olan Paketler için Kayıt Tutulması
  - echo 1 > /proc/sys/net/ipv4/conf/all/log_martians
- IP Yönlendirmenin Pasifleştirilmesi
  - echo 0 > /proc/sys/net/ipv4/ip_forward
- TCPSynCookies'in Aktif Hale Gelmesi
  - echo 1 > /proc/sys/net/ipv4/tcp_syncookies
- Bölünmüş Paketlerin Gözardı Edilmesi İçin
  - echo 1 > /proc/sys/net/ipv4/ip_always_defrag

Ağ İçin Çekirdek Düzenlemesi - 2

- IP Spoofing Koruması
  - for dosya in /proc/sys/net/ipv4/conf/*/rp_filter ; do
  - echo 1 > $dosya ; done
- ICMP Redirect Paketlerinin Gözardı Edilmesi
  - for dosya in /proc/sys/net/ipv4/conf/*/accept_redirects ; do
  - echo 0 > $dosya ; done
- ICMP Redirect Paketlerinin Gönderiminin Engellenmesi
  - for dosya in /proc/sys/net/ipv4/conf/*/send_redirects ; do
  - echo 0 > $dosya ; done
- Kaynak Yönlendirmesi Yapılmış Paketlerin Gözardı Edilmesi
  - for dosya in /proc/sys/net/ipv4/conf/*/accept_source_route ; do
  - echo 0 > $dosya ; done
- Son Üç Seçenekte Gözardı Edilen Tüm Paketlerin Loglanması
  - for dosya in /proc/sys/net/ipv4/conf/*/log_martians ; do
  - echo 0 > $dosya ; done

Güvenli Sunucu Yönetimi

- Sunucunun X Arabirimine İhtiyaç Duyuluyorsa SSH Üzerinden Aktarılabilir (/etc/ssh/sshd_config'den Aktifleştirilmelidir)
  - ssh -X sunucu_adi
- Kullanılacak Servislerin SSH Üzerinden Aktarılması
  - ssh -L yerel_port:sunucu_ip:uzak_port sunucu_ip
- SSH Yapılandırılmasında v2 Protokolü Kullanılmalı
  - “Protocol 2” ---> /etc/ssh/sshd_config
- Güvenli Dosya Aktarımı
  - scp dosya_adi kullanici_adi@sunucu_adi:/dizin_adi/
- Güvenli Dosya Senkronizasyonu
  - rsync -e ssh

Hardening Yazılımları

- Harden (Debian)
  -
- Harden_Suse (Suse)
-
- Bastille-Linux (Redhat - Mandrake)
-
- SASTK (Slackware)

Diğer Güvenlik Yazılımları

- Güvenlik Duvarı
  - Iptables http://www.netfilter.org
- Saldırı Tespit Sistemi
  - Snort http://www.snort.org
  - LIDS http://www.lids.org
  - GRSecurity http://www.grsecurity.org
- Sanal Özel Ağ Sunucusu
  - FreeSWan http://www.freeswan.org
  - PoPToP http://www.poptop.org
- SSL Kütüphaneleri ve Araçları
  - OpenSSL http://www.openssl.org
- PGP Kriptolama
  - GnuPG http://www.gnupg.org
- Güvenlik Denetimi
  - Nessus http://www.nessus.org
  - Nmap http://www.insecure.org/nmap

Yararlı Kaynaklar

- Security Focus http://online.securityfocus.com
- Sans Reading Room http://rr.sans.org
- CERT http://www.cert.org
- LinuxDoc http://www.linuxdoc.org
- Linux Security http://www.linuxsecurity.com
- Redhat http://www.redhat.com
- Suse http://www.suse.com
- Linux.Org.TR http://www.linux.org.tr
- Belgeler.Org http://www.belgeler.org
- Siyah Şapka http://www.siyahsapka.com

Sorular ?

Teşekkürler.....