

Apache Web Sunucusu ve Güvenlik



Serbülent ÜNSAL
serbulentu[et]gmail.com

Neler Bekliyor Bizi ?

- Nerden Çıktı Bu Seminer ?
- Apache Nedir ?
- Apache'nin Konfigürasyonu
- Apache'nin Yapısı
- Apache ve Web Programlama
- LAMP
- Sanal Alanlar
- Bant Genişliği Kontrolü
- Dizin Erişimlerinin Kısıtlanması
- Log Analizi ve İstatistikler

Ve Güvenlik...

- Güvenli Apache Sunucu (SSL)
- Web Uygulamalarına Tehditler
- Apache Sunucunun Güvenliđi Nasıl Sağlandı
 - 20 Temel İpucu
 - Mod_Chroot ile Kolay Kafesleme
 - Mod_Security
 - Güvenli Uygulama Geliřtirme
- Kaynaklar
- Sorular

Nerden Çıktı Bu Seminer ?

- Ben Kimim ?
 - 4 Yıllık Sistem Yönetimi Deneyimi
 - 1 Defa Hacklenme Deneyimi :)
- Deneyimlerin Paylaşılması
- Apache Sizin İçin Neler Yapabilir ?
- Daha önceki tecrübeleriniz ve seminerden beklentileriniz

Apache Nedir ?

- ***Güçlü, sağlam, yetenekli ve esnek bir http (web) sunucusudur.***
- ***Apache Software Foundation (ASF) tarafından geliştirilir. ASF, Apache yazarları tarafından 1999'da yazılım için yasal bir şemsiye olması için oluşturulmuştur.***
- ***Açık kaynak kodlu bir yazılımdır, lisansı ücretsizdir. Yazılım firmaları, kurumlara verdikleri hizmetten (kurulum, teknik destek, vb) kazanç sağlarlar.***
- ***1995'ten beri geliştirilmektedir.***

APACHE'NİN DOĞUŞU

1995 Şubatında dünyanın en popüler web sunucusu, Illinois Üniversitesi National Center for Supercomputing Applications'da **Rob McCool** tarafından geliştirilen **NCSA** idi. Ancak 1994 ortalarında McCool NCSA'den ayrıldığından beri gelişimi durmuştu. Birçok webmasterlar kendileri NCSA üzerinde hataları düzeltiyor ve ek kısımlar geliştiriyorlardı ve ortak bir dağıtıma gereksinim vardı.

Webmasterlardan küçük bir grup, kendi aralarında özel olarak e-maileşerek yamalar (patch) halinde bir dağıtım yapılmasını koordine etmeye çalıştılar. HotWired tarafından sponsore edilen bir bant genişliğine bir sunucu yerleştirildi, herkesin kendi loginlerinin olduğu bir bilgi paylaşım alanı ve bir e-mail listesi oluşturuldu. Şubatın sonunda kurucu **Apache Grubu** kurulmuştu. 8 kişiden oluşuyordu, 3 kişi de dışarıdan katkıda bulunuyordu.

APACHE'NİN DOĞUŞU

NCSA 1.3 baz alınarak, tüm yayınlanmış olan yamalar ve önemli yenilikler bulunarak eklendi ve sağlanan sunucu üzerinde denendi.

Nisan 1995'te A Patchy Server (Apache)'nin ilk sürümü 0.6.2 piyasaya çıktı. Rastlantı eseri Mart'ta NCSA de yeniden geliştirilmeye başlanmıştı. İki projenin bilgi paylaşabilmesi için o ekip de e-mail listesine "onur üyesi" olarak katıldı.

İlk Apache sunucusu çok büyük ilgi görmesine karşın Apache Grubu temel kodun ciddi bir yeniden dizayn ve genel bir gözden geçirmeye ihtiyacı olduğunun farkındaydı. Mayıs-Haziran 1995'te gruptan **Rob Hartill** ve ekibi yeni özellikler geliştirmeye ve büyük bir hızla büyüyen Apache topluluğuna (community) destek verirken; **Robert Thau**, Shambnala kod adlı yeni bir sunucu mimarisini geliştirmeye başladı. Grup Temmuz'da birçok yenilik içeren yeni sunucu mimarisine geçti ve o sırada geliştirilen yeni özellikleri de ekleyerek **Apache 0.8.8'i çıkardı**.

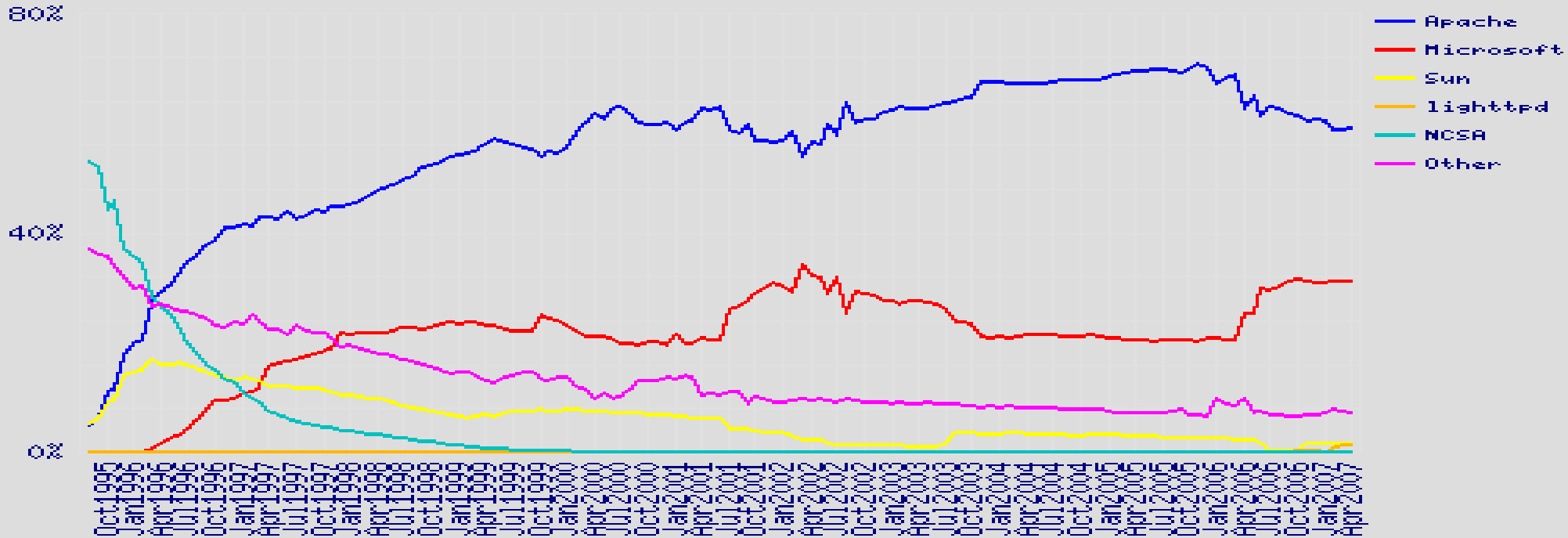
APACHE'NİN DOĞUŐU

Uzun ve detaylı beta testlerden, birçok platforma port edilmesinden, yeni bir doküman seti hazırlanmasından sonra 1 Aralık 1995'te Apache 1.0 çıktı.

Grup oluşturulduktan bir sene bile geçmeden Apache, NCSA'i geçerek internetin bir numaralı sunucusu haline geldi.

Bugün Netcraft verileri, Apache'nin diğer tüm web sunucularının toplamından çok daha yaygın olarak kullanıldığını göstermektedir.

APACHE'NİN YERİ



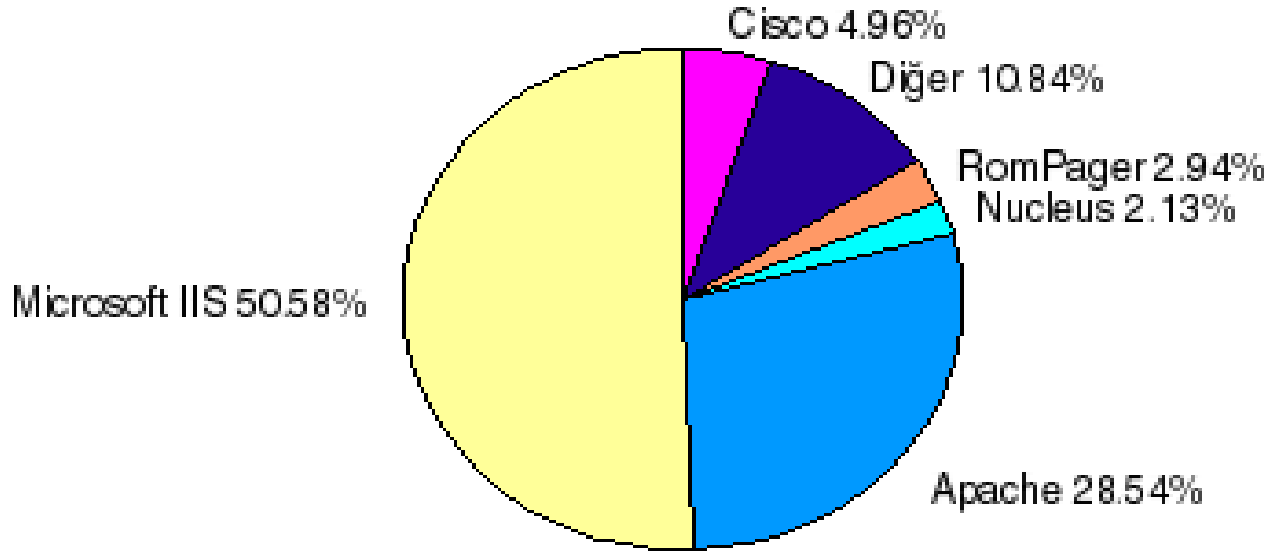
- İnternetteki web sitelerinin %60'ı Apache üzerinde çalışmaktadır. Apache, en yakın rakibi Microsoft'un web sunucularının 3 katı pazar payına sahiptir.

- Nisan 2006 itibariyle 66.899.485 web sitesi **Apache** kullanmaktadır

Bir Başkadır Benim Memleketim !

Türkiye Web Sunucu Tercihleri

Ocak 2006



<http://www.ilkertemir.com/websurvey/current>

Zenginlik Başka Şey Canım.....

Türkiye'de Kimler Apache Kullanıyor ?

- Turkcell, Vodafone, AVEA
- Sabah Gazetesi
- ULAKBİM
- Sabancı Üniversitesi
- Orta Doğu Teknik Üniversitesi
- Türkiye Odalar ve Borsalar Birliği
- İstanbul Menkul Kıymetler Borsası
- Superonline

Dünyada Kimler Apache Kullanıyor ?

- Oracle
- Mercedes-Benz
- Ericsson
- Siemens
- BBC
- Hewlett-Packard
- Financial Times
- Toyota

En Son Ne Zaman Uyudunuz ?

- Netcraft'ın 27/04/2007 itibarıyla en yüksek uptime'a sahip 50 sunucu sıralamasında :
- 34 Apache Sunucu Bulunmaktadır.
- Ayrıca ilk 3 sırayı yine Apache sunucular paylaşmaktadır.
- En yüksek ayakta kalma rekoruna sahip sunucu 1390 gün ile Apache dir.
- En yakın diğer ürün 785 günle oldukça geriden gelmektedir.

En Son Ne Zaman Uyudunuz ?

- Uptimes Project verilerine göre,
- 2500+ kayıtlı Linux sunucunun ortalama uptime süresi : 67 gün
- 1200+ kayıtlı Windows sunucunun ortalama uptime : 16 gün

APACHE'NİN AYARLANMASI

- Apache'nin kurulum sonrası ayarları **httpd.conf** dosyasından yapılmaktadır.
- Çoğunlukla `/etc/httpd/conf/httpd.conf` da bulunur.
- Bulamadıysanız;
`find . / -name 'httpd.conf'`

Apache için Grafik Arayüzleri

- Apache'yi ayarlamak için kullanılabilecek grafik arayüzleri :
- Comanche
 - <http://www.comanche.org>
- Mohawk
 - <http://eunuchs.org/linux/Mohawk>
 - Uzaktan kontrol, tek bir mohawk ile birçok Apache sunucusunda işlem yapabilme
 - Ayarların yanı sıra, sunucuların gerçek zamanlı gözetlenmesi ve istatistiklerinin grafik raporlanması
- Webmin
 - <http://webmin.bilkent.edu.tr>
 - Türkçe
 - Web tabanlı yönetim, herhangi bir işletim sisteminden bağlanılabilir

Nereden Başlasak ?

- Neden Ayar Dosyası ?
- <http://www.ulakbim.gov.tr/dokumanlar/sunucuayar/ApacheAyar.uhtml>
- Adım adım okuyun, kendi ayar dosyanıza göre güncelleyin.
- Anlamadığınız yerleri araştırıp kendi ayar dosyanıza yorum olarak ekleyin
- --- Acılı bir süreç vakit alıyor
- + Verdiğiniz emeğe değer sisteminize gerçekten hakim olursunuz.

httpd.conf

- ServerTokens Prod / Full
 - Biz Full yapalım ;-)
- ServerType standalone / inetd
 - standalone yapalım
- ServerRoot "/etc/httpd"
 - Dizin isminin sonunda / OLMAMALIDIR!
- Timeout 45
 - Sunucu istemciden yanıt almadan ne kadar beklesin ?
- KeepAlive On/Off
 - On yapalım. Açılan bağlantı Timeout a kadar sürer.

httpd.conf

- MaxKeepAliveRequests 100
 - En fazla kaç kalıcı bağlantı
- KeepAliveTimeout 15
 - Bu süre geçerse bağlantı artık kullanılmıyor demektir
- Çok çocuklu bir aile
 - MinSpareServers 3
 - MaxSpareServers 15
- StartServers 3 Başlangıçta kaç sunucu başlayacak ?
- MaxClients 150 (Aynı anda bağlanabilecek istemci sayısını kısıtlar)
- Listen 127.0.0.1:80

httpd.conf

- DocumentRoot "/var/www"
- UserDir public_html
 - <http://www.firma.com.tr/~unsal/>
- HostnameLookups Off
- ErrorDocument 404 /kayip_sayfa.html

httpd.conf

(Apache Dizinleri)

- `<Directory />`
Options None
DirectoryIndex index.html index.htm default.htm index.php
AllowOverride None
`</Directory>`
- `<Directory /var/www/html>`
Options FollowSymLinks
DirectoryIndex benim.html bizim.htm özel.php
AllowOverride None
Order allow,deny
Allow from 193.140.90.
Deny from all
`</Directory>`

APACHE'NİN MODÜLER YAPISI

- Apache'nin birçok fonksiyonu Apache "çekirdeğinin" üzerine modül olarak eklenmiştir, istenilen birçok özellik Apache'ye eklenebilir veya çıkarılabilir. Yöntem olarak Linux çekirdeğine benzetilebilir
- Bu sayede Apache'nin bütünlüğü bozulmadan bağımsız olarak birçok programcı Apache'ye çeşitli işlevleri olan yüzlerce ek modül geliştirmiştir.
- Apache'nin "kayıtlı" modüllerinin listesine <http://modules.apache.org> adresinden ulaşılabilir.
- Apache'ye modüller iki şekilde eklenebilir. Derlenme aşamasında statik olarak eklenebilir ya da derlenmiş Apache'ye DSO olarak eklenebilir (DSO = Dynamic Shared Object)

APACHE'NİN MODÜLER YAPISI

- Modül kullandığınızda , kullanmayacağınız özellikleri çalıştırmazsınız.
 - Boyut küçülür, performans artar.
 - Güvenlik artar (olmayan kapı kırılmaz :))
 - Özellik ekleme çıkartma işi çok kolaylaşır

APACHE'NİN MODÜLER YAPISI

- Statik

- Modüller derleme aşamasında Apache binary'sine dahil edilirler.
- Derleme sonrası yeni modül eklenmesi için tüm Apache'nin tekrar derlenmesi gerekir.

- DSO

- Derleme aşamasında modüller DSO olarak derlenir. Apache'nin çalıştırılma sırasında ayar dosyasında (httpd.conf) belirtilen modüller Apache'ye eklenir.
- DSO modüller Apache tekrar derlenmeden, Apache'ye eklenebilir ve çıkarılabilir.
- Apache çalıştırılırken %20, çalışma sırasında ise %5 daha yavaş çalışır.

APACHE'NİN MODÜLER YAPISI

- Apache modüllerinden çeşitli örnekler :
 - Mod_ssl
 - Mod_php
 - Mod_python
 - Mod_chroot
 - Mod_security

Apache ve Web Programlama

- Neden web programlama ?
- Modül Tekniği veya Bağımsız Sunucu
- SSI
- CGI
- PHP, JSP , ASP
- Ve ötesi (RoR , JSF , ASPX)

SSI (Server Side Includes)

- Sunucunuzda SSI kullanılabilmesi için;
- LoadModule mod_include.so
- LoadModule mod_expires.so
- AddType text/html .shtml
- AddHandler server-parsed .shtml
- Options Includes

SSI (Server Side Includes)

- Basit birkaç SSI komutu;
 - <!--komut-->
 - <!--#echo var="DATE_LOCAL"-->
 - Monday, 01-Oct-2001 13:32:05 GMT+2
 - <!--#exec cgi="dunyayi_ele_gecir.pl"-->
- Options IncludesNOEXEC

CGI (Common Gateway Interface)

- CGI bir programlama dili değildir. Piyasadaki, bir girdiyi işleyip, çıktı üretebilen her dil CGI programları geliştirmek için kullanılabilir. Örneğin Perl, C, Python, Tcl, AppleScript, Shell script'leri geliştirme için en çok tercih edilen dillerdir.
- CGI in tasarım hedefleri;
 - CGI programları sunucudan bağımsız olmalıydı
 - CGI programları hemen her dille yazılabilmeliydi
 - Hemen her istemcide çalışabilmeliydi

CGI'ı Etkinleştirmek

- LoadModule cgi_module modules/mod_cgi.so
- CGI programları için Öntanımlı olarak /var/www/cgi-bin dizini kullanılır.
- Bir dizini cgi-bin için hazırlamak;

```
ScriptAlias /mailman/ "/var/mailman/cgi-bin/"
```

```
<Directory "/var/mailman/cgi-bin/">  
    AllowOverride None  
    Options ..... ExecCGI ... ..  
</Directory>
```

PHP

- PHP, Apache'ye hem modül olarak eklenebilmekte; hem de CGI olarak dışarıdan kullanabilmektedir. Yüksek performans ve güvenlik için modül olarak kullanılması tavsiye edilir. Modül olarak kullanıldığında herhangi bir html dizininde kolaylıkla kullanılabilir.
- PHP modülü Apache kaynak koduyla beraber gelmemektedir, <http://tr.php.net> adresinden alınabilir.
- Sunucunuzda PHP4 kullanılabilmesi için httpd.conf dosyasında aşağıdaki satırların aktif hale getirilmesi gerekir.

```
#AddType application/x-httpd-php .php
```

```
#AddType application/x-httpd-php-source .phps
```

ASP

- ASP, Apache kaynak kodu ile beraber gelmemektedir. Çeşitli ASP programlarından biri kullanılabilir.
- Apache :: ASP <http://www.apache-asp.org>
- Instant ASP <http://www.halyconsoft.com>
- Chili!soft ASP <http://www.chilisoft.com/chiliasp/>
- Özellikle Unix (ve Linux) platformlarında daha performanslı, güçlü ve esnek olduğundan PHP tercih edilmektedir.
- Peki ya ASP.NET ?

Java Servlets ve JSP

- Java Servlet modülü Apache kaynak kodu ile beraber gelmemektedir.
<http://java.apache.org> adresinden alınabilir.
- Sunucuda aynı zamanda Java Development Kit (JDK) kurulu olmasına gerektirir.
- Ancak Apache-Tomcat daha doğru bir tercih

LAMP

- Linux + Apache + MySQL + PHP
- Hem internette hem intranette web-veritabanı entegrasyonunun sağlanması için kullanılabilir.
- B2C (firmadan müşteriye) ve B2B (firmadan firmaya) internet projelerinde yoğun bir biçimde kullanılmaktadır.
- PHP, Apache'ye gömülü bir modül olarak çalışabildiğinden çok verimli çalışır.
- MySQL, bir veritabanı sunucusunun birçok web programında kullanılmayan özelliklerini taşımadığından, küçük ve orta ölçekli sitelerde diğer veritabanı sunucularından çok daha verimlidir

LAMP

- PHP, hemen her veritabanını kullanabilmesine karşın, son dönemlerde PHP ve MySQL geliştiricileri ortak çalışarak PHP-MySQL ikilisinin beraber çalışma performansını arttırıcı değişikliklerde bulunmaktadır.
- Tamamen serbest yazılımlardan oluşması nedeniyle desteği çoktur, birçok hazır program ve model elde edilebilir. Son derece düşük maliyetlidir.

Sanal Sunucular

- Apache, aynı IP üzerinde yüzlerce farklı domain'i farklı web sayfalarına yönlendirerek tutabilmektedir.
- Ip sayıları sonsuz değil
- Düşünün bir internet firmasında 100 lerce web sitesi barındırmanız gerekiyor. Yaptığınız her değişikliği 100 lerce defa uygulamak pek pratik değil ;)

Sanal Sunucular

- Sanal sunucu oluşturmak için, httpd.conf dosyasında;

NameVirtualHost 10.0.0.16

<VirtualHost 10.0.0.16>

ServerName vimedks.ktu.edu.tr

DocumentRoot "/var/www/kullaniciilar"

DirectoryIndex index.html

ServerAdmin webmaster@vimedks.ktu.edu.tr

ErrorLog logs/kullaniciilar-error_log

CustomLog logs/kullaniciilar-access_log common

php_value engine off

</VirtualHost>

DOMAIN BAZINDA BANT GENİŞLİĞİ KONTROLÜ

- Apache'ye eklenen çeşitli modüllerle, Apache'nin virtualhost'lara özel bant genişliği sınırlamaları getirilebilir.
- Bazı bant genişliği kontrol modülleri :

```
# mod_throttle  
    http://www.snert.com/Software/Throttle/  
# mod_bandwidth  
    http://www.cohprog.com  
# bwshare  
    http://www.topology.org/src/bwshare/
```

- Her ne kadar Apache'nin böyle bir yeteneği de olsa, kısıtlanmak istenen domain ayrı bir sunucuya ayrılarak, firewall/proxy/router türü araçlarla bant genişliğinin kısıtlanması daha sağlıklıdır.

DİZİNLERİN ŞİFRELENMESİ

- Web sitenizde belirli bir dizine ve alt dizinlerine girişi isim/şifre ile kısıtlayabilirsiniz.
- httpd.conf dosyasından

```
<Directory /www/sifreli>  
    AuthName "restricted stuff"  
    AuthType Basic  
    AuthUserFile /etc/httpd/conf/sifreli.users  
    require valid-user  
</Directory>
```

- htpasswd programı ile sifreli.users dosyası oluşturulabilir.

DİZİNLERİN ŞİFRELENMESİ

- Şifrelenecek dizinde yaratılacak bir .htaccess dosyasına,

AuthName "restricted stuff"

AuthType Basic

AuthUserFile /etc/httpd/conf/sifreli.users

require valid-user

yazılır. Ve sunucu yeniden başlatılır

LOG ANALİZİ ve WEB İSTATİSTİKLERİ

- Webalizer
<http://www.webalizer.org>
- Wusage
<http://www.boutell.com/wusage>
- AwStats
<http://awstats.sourceforge.net/>
- Analog
<http://www.analog.cx/>

VE

GÜVENLİK

APACHE SECURE SERVER (SSL)

- Veri trafiğini neden şifrelemeliyiz ?
- Sunucuda bir SSL kütüphanesi kurulu olması gerekir. OpenSSL tavsiye edilir. <http://www.openssl.org> adresinden alınabilir.
- Apache-SSL ve Mod_SSL olmak üzere iki farklı çözüm bulunmaktadır. Apache-SSL, Apache kaynak kodunda değişiklik yaparak kendini yerleştirmekte; Mod_SSL ise Apache'nin yapısına olarak modül olarak Apache'ye eklenmektedir. Mod_SSL'in yazarı, aynı zamanda OpenSSL'i de geliştirmektedir.
- Apache-SSL yaması <http://www.apache-ssl.org>, Mod_SSL modülü <http://www.modssl.org> adreslerinden alınabilir.
- Programlarla gelen araçlar kullanarak kendi imzalayacağınız bir test dijital sertifikası üretebilir ve kullanabilirsiniz. Ancak web browser'lar tarafından tanınmış bir otorite tarafından imzalanmamış olacağından bağlanan kullanıcı uyarılacaktır.

APACHE SECURE SERVER (SSL)

- Gerçek bir dijital sertifika, tanınmış sertifika otoritelerinden (Verisign, Thawte, vb) yıllık 100\$'dan başlayan ücretlerle satın alınabilir ve sisteme katılabilir.
- OpenSSL ile anahtarı ve sertifikamızı oluşturalım;

```
# openssl genrsa -out hostname.key 1024
```

```
# openssl req -new -key hostname.key -out hostname.csr
```

- Sertifikamızı imzalayalım;

```
# openssl x509 -req -days 710 -in hostname.csr -signkey hostname.key -out  
hostname.crt
```

APACHE SECURE SERVER (SSL)

- httpd.conf da;

```
<VirtualHost sanal.sunucu.com:443>  
DocumentRoot /www/sanal.sunucu.com  
ServerName sanal.sunucu.com  
ServerAdmin webmaster@sanal.sunucu.com  
ErrorLog logs/error_log  
TransferLog logs/access_log  
SSLEngine on  
SSLCertificateFile conf/ssl.crt/server.crt  
SSLCertificateKeyFile conf/sserver.key  
</VirtualHost>
```

Web Uygulamalarına Tehditler

- Gizlilik (Confidentiality)
- Bütünlük(Integrity)
- Erişilebilirlik (Availability)
- Tehditler bu kavramlara yöneliktir

Open Web Application Security Project

- Hatalı veri giriş doğrulama
- Hatalı Erişim Kontrolü
- Hatalı Kimlik Doğrulama ve Oturum Yönetimi
- Çapraz Site Betik Açıkları
- Tampon Taşmaları
- Komut / Sorgu Ekleme Açıkları
- Güvenli Olmayan Saklama Problemleri
- Hizmet Engelleme Problemleri
- Sunucu Yapılandırmasından Kaynaklanan Açıklar

Apache Sunucunun Güvenliđi Nasıl Sađlandı

- Bir sabah uyandık ve baktık ki Hacklenmiřiz !!!
- İlk adım hasar tesbiti yapana kadar tüm ađ iletişimini kesin
- Saldırgan nerelere kadar erişmiř ve bunu nasıl yapmış ?

Apache Sunucunun Güvenliği Nasıl Sağlandı

- http://wiki.linux-sevenler.org/index.php/Apache_Konfigürasyonunuzu_Güvenli_Hale_Getirmenin_20_Yolu
- İlk olarak en son yamaları geçtiğimize emin olun.
- Apache sürüm numarasını ve diğer bilgileri gizleyin.
- Apache'yi kendi kullanıcı hesabı ve grubunda çalıştırın.
- Web klasörünün dışındaki dosyalara erişimi engelleyin.
- httpd.conf dosyasında ana klasör için

```
<Directory / >  
    Options None  
    AllowOverride None  
</Directory>
```
- Options -Indexes

Apache Sunucunun Güvenliği Nasıl Sağlandı

- Options -Includes -ExecCGI -FollowSymLinks
- .htaccess dosyaları için desteğin kaldırılması veya güvenli hale getirmek;
AccessFileName .htpoverride
- Gereksiz modülleri kapatın;
grep LoadModule httpd.conf
- Apache'nin konfigürasyon ve çalıştırılabilir dosyalarına sadece root'un okuma izni olsun;
*# chmod -R o-rwx /etc/httpd/
chown -R root.root /etc/httpd/*
- Timeout değerini DDos Saldırılarını engellemek için düşürün
Timeout 45
- Gönderilebilecek dosya boyutunu sınırlandırın
LimitRequestBody 1

Apache Sunucunun Güvenliđi Nasıl Sađlandı

- Apache aynı anda yapılan istekleri işleme ile ilgili olarak çeşitli konfigürasyon ayarları sunar. MaxClients isteklere hizmet için maksimum olarak kaç child process'in yaratılacağını belirler.
- Eğer sunucunuzun çok sayıda eşzamanlı isteđi karşılayacak kadar hafızası yoksa bu değeri yüksek tutmak isteyebilirsiniz.
- *ThreadsPerChild*
- *ServerLimit*
- *MaxSpareThreads*

Apache'yi Kafeste Kořturmak

- Chroot uygulaması bir sunucunun belli bir dizin içindeki kilitlemesidir.
- Böylece bizim tanımladığımız herhangi bir dizin örneğın /var/www sunucu için kök dizini (/) olur ve sunucu buradan yukarı çıkamaz.
- Bu durumda apache sunucusu ele geçirilse dahi verdiği zarar belirlediğimiz dizinden yukarı çıkamaz.

Apache'yi Kafeste Kořturmak

- Ben Apache yi kafes içinde alıřtırmak için 3 temel yöntem;
- Klasik chroot yaklařımları;
- Zor ve zahmetlidir (genellikle) ařağıdaki yapıyı chroot içinde oluřturmanız gerektirir;
- C kütüphanesi
- Pekok diđer kütüphane (libssl? libm? libmysqlclient?)
- özümleyici dosyalar (/etc/nsswitch.conf, /etc/resolv.conf)
- Kullanıcı dosyaları (/etc/passwd, /etc/group)
- log dosyaları için ayrı bir klasör
- Program tarafında kullanılacak modül dosyaları (for Apache: mod_php and other modules)

Apache'yi Kafeste Kořturmak

- Mod-security nin chroot fonksiyonu
- Basit ancak klavuzdaki sistem kaynak koddan kurulmuř bütn dosyaları 1 dizin içinde toplayan bir apache sunucusuna uygun. Dosyaları deęişik konumlara dağılmıř bir sunucuda uygulaması zor.

Apache'yi Kafeste Koşturmak

- Mod_Chroot yaklaşımı
- Basit hızlı ve kolay.
- Yalnızca chroot işlemine odaklanmış sade bir modül.
- Ek hiç bir dosyanın kopyalanmasına gerek kalmaz (1 - 2 istisnai durum olabilir :))

Mod_Chroot Yaklaşımı

- Mod-security ve Mod_chroot u kısaca kıyaslarsak;
- mod_chroot uzak istemcilerle iletişim kurmaz.
- mod_chroot yalnızca bir kere hafıza ayırır, başlangıçta.
- mod_chroot istekleri yakalamaz kendi işi ile uğraşır

Mod_Chroot Yaklaşımı

- Hazır Mod_Chroot Paketleri içeren dağıtımlar;
- FreeBSD
- DarwinPorts
- PLD Linux
- Gentoo Linux
- Debian stable
- NetBSD

Mod_Chroot Yaklaşımı

- httpd.conf da;

```
ChrootDir /var/www  
DocumentRoot /
```

- Eğer DocumentRoot u /var/www şeklinde bırakırsanız sunucu /var/www/var/www dizinide arayacaktır ana dizininizi
- mod_chroot Apache nin bütün işi bittikten sonra çağırılmalı bunun için modül listesinin en başına eklenmeli (Apache modülleri yazım sırasının tersine yükler) . Eğer modülü dinamik olarak derlediyseniz.

```
LoadModule chroot_module /usr/lib/httpd/modules/mod_chroot.so
```

- satırlarını modül listesinin en başına ekleyin. Tabi burada kullandığınız dağıtıma bağlı olarak mod_chroot.so dosyasının tam yolunu yazmalısınız

Mod_Chroot Yaklaşımı

- Apache yi Yeniden Başlatmak;
apachectl stop ve apachectl start
- Eğer veritabanı sunucunuz yalnız Unix soketlerini dinliyorsa onu 127.0.0.1 i de dinlemesi için ayarlamalısınız.
- <http://nightwalkers.blogspot.com/2006/07/hzl-ve-kirli-bir-modchroot-klavuzu.html> adresinde daha detaylı bir kurulum kılavuzu bulabilirsiniz.

Mod_Security

- ModSecurity, web uygulamaları için açık kaynak kodlu saldırı tespit ve önleme motorudur (engine).
- ModSecurity aynı zamanda web uygulama güvenlik duvarı olarak da adlandırılabilir.
- ModSecurity web sunucunun içine gömülmüş bir şekilde, güçlü bir şemsiye gibi davranarak uygulamaları saldırılardan korumaya çalışır.

Mod_Security

- Pek çok dağıtım için hazır paketi bulunuyor.
- httpd.conf da veya conf.d/mod_security.conf içerisinde

```
<IfModule mod_security.c>
```

```
# mod_security configuration directives
```

```
# ...
```

```
</IfModule>
```

Mod_Security

- Taramayı aktif hale getirir.

SecFilterEngine On

- Çıktılarda taramayı aktive eder

SecFilterScanOutput On

- Yalnız text içeriğe çıktı taraması uygulanır

SecFilterOutputMimeTypeTypes "(null) text/html text/plain"

Mod_Security

- delete insert select drop iceriklerini red et

SecFilter "delete[[:space:]]+from"

SecFilter "insert[[:space:]]+into"

SecFilter "select.+from"

SecFilter "drop[[:space:]]table"

SecFilter "update.+set"

- Sunucu IIS gibi davranır

SecServerSignature "Microsoft-IIS/5.0"

- Fatal Error çıktılarını önleyelim

SecFilterSelective OUTPUT "Fatal Error"

- Php yi yasaklayarak php kullanmak :)

SecFilter php

DirectoryIndex index.php

Güvenli Web Uygulamaları

- Güvenlik programı tasarlarken düşünölmeli.
- Mümkün olduđunca paranoyak düşünün bilmediđiniz hiçbir veri ve veya parametreye izin vermeyin.
- Güvensiz web uygulamaların sunucunuzda çalışmadıđından ve diđer hazır uygulamalarında düzenli güncellendiđinden emin olun.

Apache Kaynakları

Linux Kullanıcıları Derneği

<http://www.linux.org.tr/belgeler/>

Linux Listesi

<http://liste.linux.org.tr>

Apache Web Sitesi

<http://www.apache.org/httpd.html>

Devshed

http://www.devshed.com/Server_Side/Administration/

Apache Web sunucusu

Bora GÜNGÖREN , Oğuzhan KAYHAN. Seçkin Yayıncılık

??

SORULAR

?