Материалы семинара по работе с VPS и физическими серверами

HOSTPRO

Организаторы:

Компания **HostPro** – лучший хостинг в Украине. Предоставляет весь спектр хостинговых услуг, начиная от доменов и заканчивая арендой физических серверов. На украинском рынке хостинга работает в течении восьми лет и занимает лидирующие позиции среди хостинговых компаний. Компания **HostPro** всегда следит за развитием IT-технологий и обеспечивает возможность работы с лучшими из них для своих клиентов.

Компания **«Бегун»** – основоположник и лидер российского рынка контекстной интернет-рекламы с 2002 года, сервис с оплатой за результат и аукционным ценообразованием. Входит в тройку крупнейших компаний, предлагающих услуги по размещению контекстной интернет-рекламы на рынке Украины.
Партнерская сеть «Бегуна» объединяет более 220 тыс. сайтов, среди которых Rambler.ru, Odnoklassniki.ru, Online.ua, UkrIndustrial.com, Ati.com.ua, livejournal.com и др.

Докладчик:

- Дмитрий Костюк, технический директор компании HostPro

Содержание

Установка и настройка cPanel/WHM

Для установки ПО cPanel/WHM необходимо ознакомиться с поддерживаемыми ОС (операционными системами) http://www.cpanel.net/products/cpwhm/cpanel11/sys_requirements.htm

Самой распространённой и рекомендуемой системой является CentOS

Минимальные системные требования:

- 266 MHz Processor или выше;
- 256MB of RAM (1+ GB рекомендовано для хостинга с большим числом сайтов);
- 10GB-2TB дисковая квота.

Для установки cPanel требуется выделенный статический IP адрес.

Скачать пакет автоматического установщика cPanel можно тут: http://layer1.cpanel.net

sh # wget –O http://layer1.cpanel.net/latest | sh
(в системе уже должен быть установлен пакет development tools).

Весь процесс установки в зависимости от скорости интернет соединения занимает от 40 минут до 1.5 часа.

Первичная настройка системы

- После удачной установки набираем в браузере http://IP:2086.
- Соглашаемся с лицензионным соглашением и переходим на вторую страницу.

Setup Wizard – Basic cPanel/WHM Setup.

Обязательные поля для заполнения:

Server Contact E-mail	Server Hostname
Default cPanel Theme	Primary Name Server
Default Home Directory	Secondary Name Server
Home Directory Prefix	CGI Script Alias
Main Shared Virtual IP	Apache Access Log

- Третий шаг - включение квот в системе (шаг можно пропустить и запустить его, когда будет удобно, через консоль **/scripts/initquotas** или через соответствующий пункт в панели WHM).

- Настройка ДНС, и имени сервера.

- Следующим этапом будет установка пароля для MySQL , этот шаг нельзя пропустить, иначе поле пароля будет пустым. (После создания пароля, он запишется в файл **/root/.my.cnf**).

- Важным этапом в настройке является указание e-mail адреса администратора сервера. На этот адрес будут поступать все сообщения (уведомления, сообщения об ошибках) с сервера. Уровень оповещения можно установить в панели управления WHM: **Main > Server Contacts > Contact Manager**

- Также не следует забывать о настройке уведомлений для сервисов: **WHM > Server Status > Service Status** , это поможет контролировать работу Вашего сервера.

Configuration Tweaks – Update Configuration

WHM -> Server Configuration -> Update Config

Можно установить автоматическое обновление панели управления по разным версиям (stable, release, current, edge) , можно установить обновление сервера вручную, или запретить обновление.

Все настройки сохранятся в файле **/etc/cpupdate.conf.**

Широкие возможности настройки нам представляет раздел меню **Tweak Settings** большинство настроек которого хранятся в **/var/cpanel/cpanel.config**:

- возможность выбора версии MySQL;
- включение и выключение webmail и статистики;
- возможность устанавливать лимиты на работу панели управления.

Настройка сервисов

Exim Configuration:

- листы доступа;
- фильтры;
- спам защита;
- установка чёрных списков;
- работа в продвинутом режиме.

FTP Configuration:

- установка анонимного доступа;
- количество одновременных подключений;
- количество одновременных подключений с одного адреса;
- максимальная нагрузка для работы анонимного доступа.

Apache Configuration:

- Global Configuration — настройка важных параметров в httpd.conf;
- PHP and SuExec Configuration — настройка PHP, выбор версии PHP, установка suEXEC;
- DirectoryIndex Priority — настройка приоритетов для документов по умолчанию;
- IncludeEditor — позволяет добавлять дополнительные настройки, или директивы в конфигурационный файл httpd.conf (до начала виртуальных хостов, и после);
- Reserver IP's Editor — позволяет настроить адрес на котором будет работать Apache;
- Memory Usage Restriction — подсчёт и установка ограничений по памяти и процессору на Apache сервера;
- Log Rotation — автоматический обработчик и архиватор лог файлов (архивы будут находится в **/usr/local/apache/logs/archive/**, архив будет создан, как только лог файл достигнет 300 МБ).

FTP Server Selection

Выбор версии сервера FTP который будет работать на сервере.

Если нужно больше настроек – нужно использовать ProFTPD, но он использует больше ресурсов, а также не может быть полностью безопасным, в отличии от PureFTPD, который использует меньше ресурсов, идеально подходит для хостинга.

Mailserver Configuration

Можно произвести IMAP и POP3 настройку сервера. Включение поддерживаемых протоколов, и количество соединений, и т.д.

Mailserver Selection

Выбор почтового сервера. который будет работать в системе. Можно выбрать между Courier и Dovecot. Первый является очень надёжным и ставится по умолчанию на сервер, недостатком является использование большого количества памяти.

Второй mail сервер более гибкий в конфигурировании, использует меньше ресурсов сервера, имеет лучшую производительность при работе с IMAP.

Nameserver Selection

Выбор сервера ДНС. BIND или NSD, второй очень быстрый и не использует много ресурсов, однако ограничен на работу с 512 адресами. Идеально подходит для реселлерских серверов.

Service Manager

Выбор сервисов, которые активны на сервере, а также наблюдение за ними.

Apache

Возможности Easyapache3

Конфигурирование

Безопасность

Решение проблем

Easyapache3

Доступно 3 главные версии Apache 1.3.x , 2.0.x, 2.2.x

Создание профайла

Поддержка 3rd party продуктов

Полная поддержка x64 систем

Конфигурирование

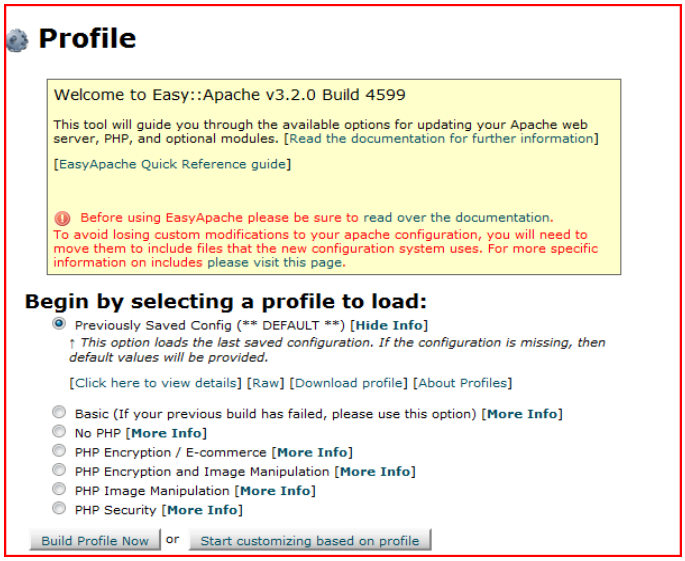
Есть два способа установить apache + php на сервер: **/scripts/easyapache**

WHM >>Software >> Apache Update

Есть возможность использовать предустановленные профайлы, которые можно разделить на две категории: профайл cPanel и пользовательский профайл.

Что входит в cPanel профайл:

- Basic
- No PHP
- PHP Encryption/E-Commerce
- PHP Encryption and Image Manipulation
- PHP Image Manipulation
- PHP Security



В этапы настройки входит:

1. выбор версии Apache;
2. выбор версии PHP (возможно установить одновременно две версии);
3. определение модулей и дополнений при конфигурации.

Для запуска сборки из командной строки можно

также использовать профайлы.

Они расположены тут: **/var/cpanel/easy/apache/profile/custom.**

cpanel_default.yaml

cpanel_no_php.yaml

cpanel_php_enc.yaml

cpanel_php_enc_img.yaml

cpanel_php_img.yaml

cpanel_php_sec.yaml

Everything.yaml

Пример запуска: **/scripts/easyapache --profile=Everything –build**

Apache/PHP ресурсы

Apache 1.3 documentation: http://httpd.apache.org/docs/1.3/

Apache 2.0 documentation: http://httpd.apache.org/docs/2.0/

Apache 2.2 documentation: http://httpd.apache.org/docs/2.2/

PHP Manual http://www.php.net/manual/en/

Полезно знать:

Конфигурционный файл apache /usr/local/apache/conf/httpd.conf

Конфигурационный файл PHP 5 /usr/local/lib/php.ini

Конфигурационный файл PHP 4 /usr/local/php4/lib/php.ini

Темплейты для Apache /usr/local/cpanel/src/templates

Установка модуля для Apache mod_evasive

Apache модуль поможет избежать ddos атаки.

Конфигурация по умолчанию блокирует адрес атакующего на 10 минут.

При этом не нужно активировать модуль frontpage,

Установка модуля: **cd /usr/local/src**

wget http://www.zdziarski.com/projects/mod_evasive/mod_evasive_1.10.1.tar.gz

tar -zxf mod_evasive_1.10.1.tar.gz
cd mod_evasive
/usr/local/apache/bin/apxs -cia mod_evasive.c

Добавление модуля в конфигурацию apache (httpd.conf)

<IfModule mod_evasive.c>
DOSHashTableSize 3097
DOSPageCount 5
DOSSiteCount 100
DOSPageInterval 2
DOSSiteInterval 2
DOSBlockingPeriod 600
</IfModule>

MySQL

Character Sets & Collations (кодировки)

В версиях Mysql, начиная с 4.1.x, можно указывать кодировки для базы данных и таблиц в них. Если же кодировка Вами не определена, будет использоваться кодировка по умолчанию latin1.

Для определения кодировки сервера баз данных следует отредактировать конфигурационный файл **/etc/my.cnf**

[mysqld]

--default-character-set=charset

--default-collation=collation

Несмотря на указанную кодировку, Вы можете создать базу данных с нужной Вам кодировкой.

- Создать базу данных с консоли

  mysql> CREATE DATABASE db_name CHARACTER SET charset COLLATE collation;

- Изменить кодировку уже существующей базы

  mysql> ALTER DATABASE db_name CHARACTER SET charset COLLATE collation;

- Создать таблицу в определённой кодировке

  mysql> CREATE TABLE tbl_name CHARACTER SET charset COLLATE collation;

- Изменить кодировку для существующей таблицы

  mysql> ALTER TABLE tbl_name CHARACTER SET charset COLLATE collation;

Для изменения использования ресурсов mysql сервисом, можно использовать предустановленные темплейты. **/usr/share/mysql/**

Оптимизация MySQL

query_cache_size= M ## 32MB for every 1GB of RAM

key_buffer= M ## 128MB for every 1GB of RAM

sort_buffer_size= M ## 1MB for every 1GB of RAM

read_buffer_size= M ## 1MB for every 1GB of RAM

read_rnd_buffer_size= M ## 1MB for every 1GB of RAM

thread_concurrency=2 ## Number of CPUs x 2

Exim

Exim — это почтовый сервис, который устанавливается по умолчанию в cPanel Mail Transfer Agent (MTA).

SMTP (Simple Transfer Protocol) используется для отправки сообщений с одного хоста на дургой. По умолчанию он использует 25 порт, в панели управления есть возможность включить дополнительный порт в том случае, если провайдер блокирует 25 порт.
(Main > Service Configuration > Service Manager > Exim to another port)

SMTP также может использовать зашифрованное соединение SSL, для этого зарезервирован специальный порт 465.
Конфигурационный файл exim находится тут: **/etc/exim.conf**.
Не рекомендуется его изменять чрез консоль сервера, потому как после обновления панели управления все изменения будут удалены. Для этого следует использовать Advanced Exim Configuration Editor в панели управления WHM.

Почтовая очередь сервера
Все сообщения на сервере под управлением EXIM имеют свой уникальный Message-ID.
Message-ID состоит из 16 символов, которые можно разделить на три секции
First Section: Unix time
Second Section: PID of the process
Third Section: Distinguish process from same PID and Unix Time

Почтовая очередь сервера физически расположена в **/var/spool/exim/input**
Очередь писем разбита на 62 подкаталога [a-z], [A-Z],[0-9]
Также очередь писем можно просмотреть через панель управления

WHM → Email → Mail Queue Manager

Команды для работы с exim на сервере через консоль:
exim -bp — посмотреть очередь через консоль
exim -bpc — количество сообщений на сервере
exim -Mvl 'MessageID' — посмотреть содержимое письма
exim -qff -v — очистить очередь сервера

Для поиска ошибок и анализа работы почтового сервиса на сервере существует 3 лог файла:
Exim Main Log: /var/log/exim_mainlog
Exim Reject Log: /var/log/exim_rejectlog
Exim Panic Log: /var/log/exim_paniclog

11 версия cPanel использует формат почтовых ящиков Maildir (cur, new, tmp), каждое письмо в ящике хранится как отдельный файл

Защита от спама (SpamAssassin)

SpamAssassing - автоматизированный фильтр почты, который использует широкий диапазон эвристических алгоритмов на заголовках почты и основном тексте сообщения, чтобы идентифицировать "СПАМ".

Для включения SpamAssassin глобально используем
WHM -> Server Configuration -> Tweak Settings

Для того, чтоб переустановить SpamAssassin в системе, следует выполнить команду в консоли сервера **/scripts/realperlinstaller --force Mail::SpamAssassin**

SpamBox - утилита, которая может использоваться вместе со SpamAssassin, которая позволит Вам направлять всю свою электронную почту СПАМА в определенную папку 'спам' ещё до того, как это письмо попадёт к Вам в почтовый ящик.

Доступ к этому ящику можно получить из подменю SpamAssassin в панели управления cPanel.

Использование чёрных списков на Вашем сервере позволит Вам снизить поток входящего спама, потому как в этих списках находятся IP адреса, которые определены как спам ресурсы.

Все письма, поступающие с таких адресов, будут немедленно удалены.
Примером таких списков являются RBL's: SPAMHAUS, SPAMCOP

Можно также создать свои собственные листы на сервере, которые будут работать параллельно с глобальными.

Для этого Вам следует создать следующие файлы:

/etc/rblblacklist - чёрный список, в котором хранятся имена хостов с которых не следует получать сообщения

/etc/rblbypass - адреса локальных доменов, которые не должны фильтроваться чёрным списком.

/etc/rblwhitelist — адреса, которые не следует блокировать на сервере.

Для создания указанных файлов, необходимо выполнить в консоли:

touch /etc/rblblacklist; touch /etc/rblbypass; touch /etc/rblwhitelist

Синтаксис этих файлов простой: указываем домен с новой строки.

anydomain.com

yourdomain.com

randomdomain.com

Ещё есть дополнительные фильтры почты, которые следят за вложениями **/etc/antivirus.exim**

Фильтры на уровне домена находятся по адресу **/etc/vfilter,** они же могут быть изменены через cPanel (**Cpanel-> Mail -> E-mail Filtering**)

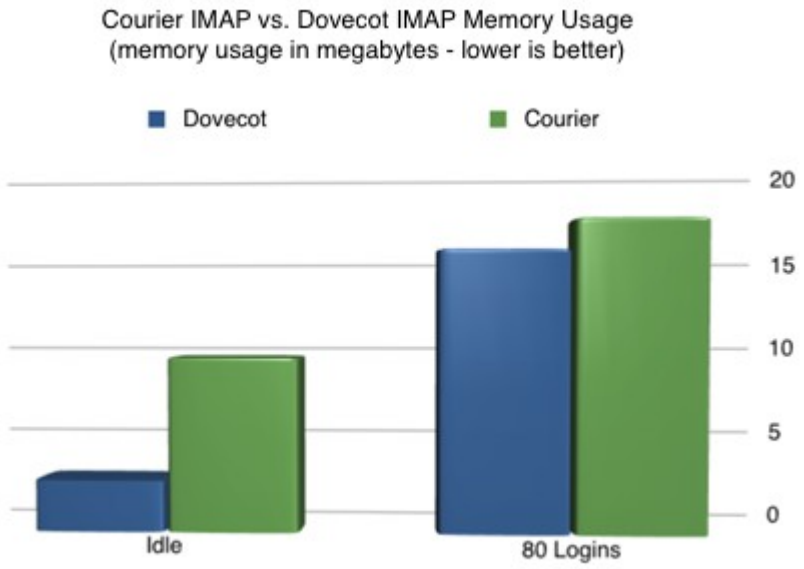
Настройка безопасности для почты

Установить флажок в **WHM - > tweak setings**

• Verify that the user “nobody” is unable to send out emails.
• Enable suExec (perl/cgi scripts)
• Enable phpSuExec (php scripts)
• Adding X-source headers

Dovecot

Появился в новой версии cPanel, который пришёл на замену courier, гораздо быстрее и надёжней, также использует меньше памяти сервера.



DNS

DNS (Domain Name System) — система, преобразующая символьные имена доменов в их IP-адреса (и наоборот), в сети Интернет.

Термины используемые в ДНС:
Record - запись внутри зоны.
Zone - серия записей используемых для домена
Named — сервер Интернет-имён
rndc — утилита для неймсерверов

Типы используемых записей

A запись - определяет IP-адрес для указанного имени.
Она указывает на физическое расположение сайта.

NS-запись - указание серверов DNS, обслуживающих данный домен.
Адреса DNS-серверов указываются в символьном виде

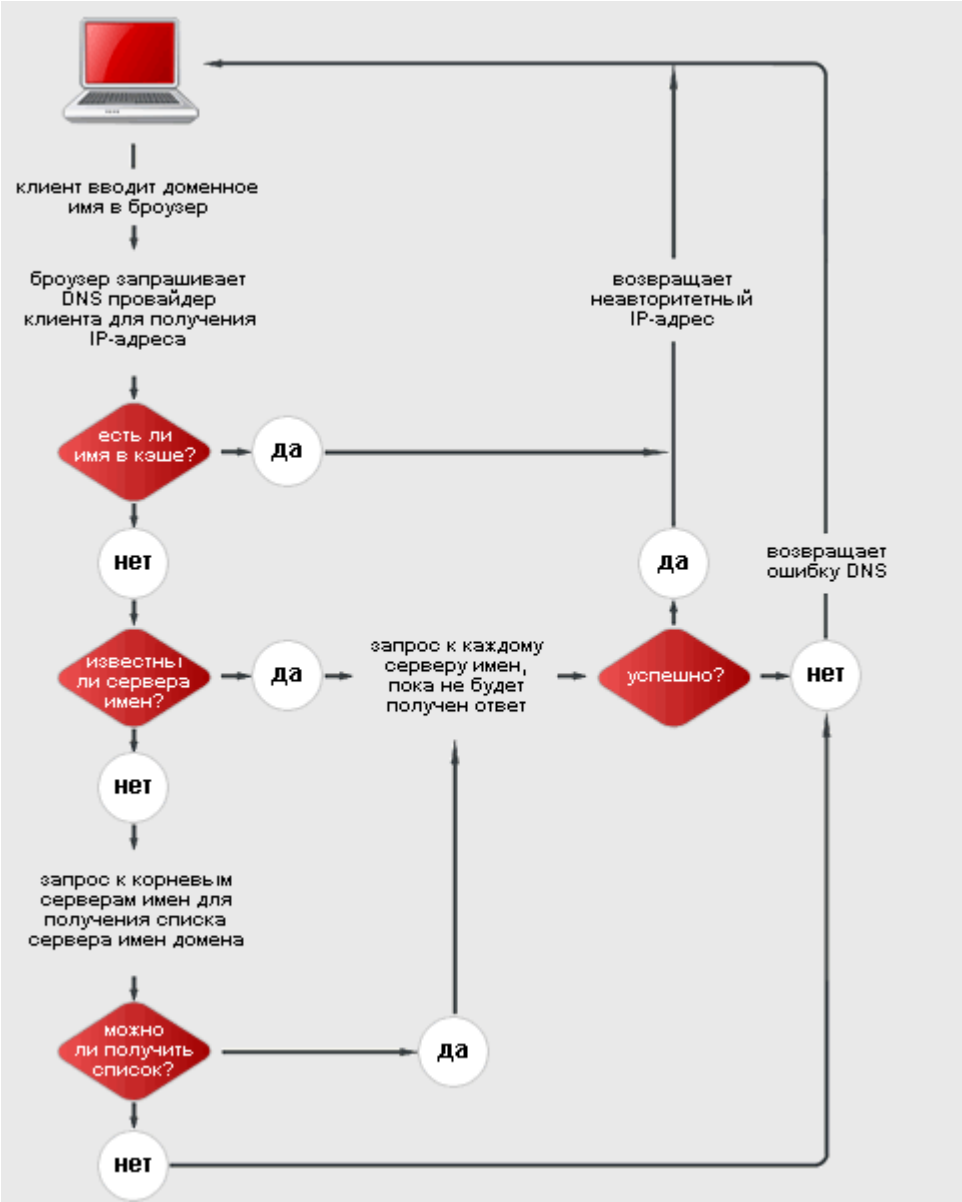
SOA-запись - обязательная запись для домена, в которой указывается различная служебная информация — e-mail администратора DNS, имя первичного (авторитативного) DNS-сервера этой зоны, период обновления информации.

MX-запись - указывает на сервер для приёма электронной почты, приходящую на адреса в указанном домене (вида <имя_ящика>@<домен>)

CNAME-запись - позволяет присваивать хосту псевдоним (алиас).
Запись представляет собой ссылку на другое доменное имя (указывающее на A-запись).

PTR — обратная ДНС запись

Принцип работы DNS



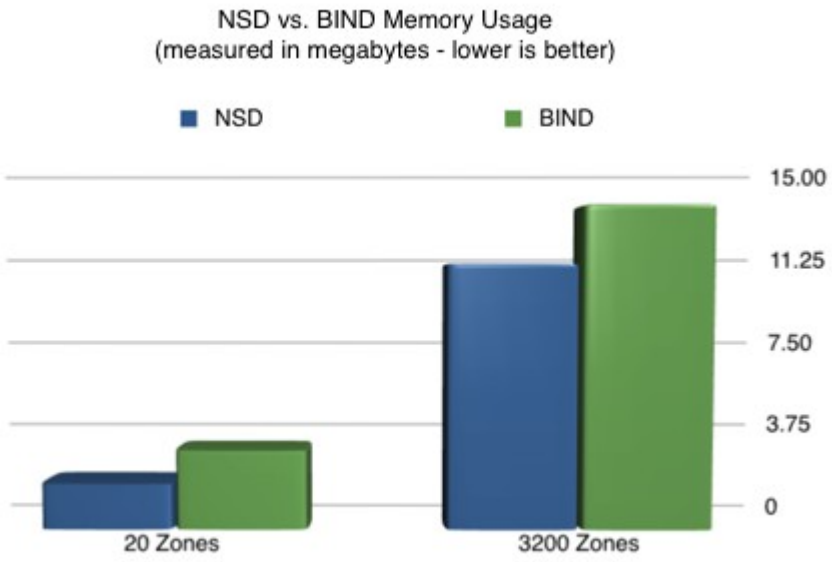
cPanel & DNS

В панели управления cPanel можно выбрать между двумя службами ДНС, это NAMED и NSD.

Эти две службы выполняют одну работу – обеспечивают работоспособность ДНС на Вашем сервере. Второй демон – NSD – является нововведением в панели управления. Его преимуществом является минимальное потребление памяти сервера, он быстрее отрабатывает запросы, которые к нему поступают, но главным недостатком его является небольшое количество обслуживаемых ДНС зон, а именно 512 (при превышении этого значения производительность его снижается).
Также его нельзя использовать для организации кластера ДНС.

BIND - это открытая и наиболее распространённая реализация DNS-сервера, обеспечивающая выполнение преобразования DNS-имени в IP-адрес и наоборот.

Сравнение двух DNS сервисов



Поиск ошибок в DNS

Логи про работу ДНС можно найти тут **/var/log/messages**
Также можно изменить файл, в который будут записываться логи,
сделать это можно в **/etc/named.conf**

Пример того, как быстро посмотреть логии, касающиеся работы ДНС:

tail -f /var/log/messages | grep named

Для поиска проблем в ДНС, для конкретного домена, можно воспользоваться следующими утилитами:
dig - проверка правильности работы сервера доменных имен
nslookup - утилита, предоставляющая пользователю интерфейс командной строки для обращения к системе DNS.
Host — используется для получения A или PTR записи для домена или IP
ping – возвращает IP- адрес зоны, которую мы опрашиваем
whois — показывает информацию о домене

Настройка безопасности

Passwords

Простой пароль - основная причина взлома сайта.

Следует использовать пароли длинной больше, чем 8 символов.

Использовать буквы и цифры в паролях.

Shell Access

Не выдавать SSH - доступ всем пользователям, только тем, кому он действительно необходим.

Всегда использовать JailShell.

Для обеспечения большей безопасности следует изменить порт для SSH протокола на Вашем сервере. Использовать протокол версии 2.

/etc/ssh/sshd_config

– Port 22 -> Port 1887

– Protocol 2,1 -> Protocol 2

WHM

- Shell Fork Bomb Protection

Не позволит пользователям запускать сервисы.

Securing /tmp

Большинство эксплоитов запускают именно из каталога /tmp

На физических серверах следует подключить раздел /tmp с опциями noexec, nosuid

Скрипт **/scripts/securetmp** подключит Ваш /tmp как временный файл для ещё большей безопасности.

WHM Compilers Tweak

Отключить возможность использовать компилятор с и с++ для всех пользователей.

И разрешить только тем, кому он действительно необходим.

WHM Brute Force Protection при подборе паролей закрывает на время доступ с этого адреса.

Permissions

Найти и определить права на запись к файлам и папкам доступны всем.

find / \(-perm -a+w \) ! -type l >> world_writable.txt

Найти файлы и папки, которые не имеют пользователя

find / -nouser -o -nogroup >> no_owner.txt

Ограничить права на следующие файлы:

chmod 750 /usr/bin/rcp
chmod 750 /usr/bin/wget
chmod 750 /usr/bin/lynx
chmod 750 /usr/bin/links
chmod 750 /usr/bin/scp

Использование sysctl поможет избежать лёгких ddos атак

/etc/sysctl.conf

```
# Disables packet forwarding
net.ipv4.ip_forward=0
# Disables IP source routing
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.lo.accept_source_route = 0
net.ipv4.conf.eth0.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
# Enable IP spoofing protection, turn on source route verification
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.lo.rp_filter = 1
net.ipv4.conf.eth0.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
# Disable ICMP Redirect Acceptance
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.eth0.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
# Enable Log Spoofed Packets, Source Routed Packets, Redirect Packets
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.lo.log_martians = 1
net.ipv4.conf.eth0.log_martians = 1
# Disables the magic-sysrq key
kernel.sysrq = 0
# Decrease the time default value for tcp_fin_timeout connection
net.ipv4.tcp_fin_timeout = 15
# Decrease the time default value for tcp_keepalive_time connection
net.ipv4.tcp_keepalive_time = 1800
# Turn off the tcp_window_scaling
net.ipv4.tcp_window_scaling = 0
# Enable TCP SYN Cookie Protection
net.ipv4.tcp_syncookies = 1
# Enable ignoring broadcasts request
net.ipv4.icmp_echo_ignore_broadcasts = 1
# Increase the tcp-time-wait buckets pool size
net.ipv4.tcp_max_tw_buckets = 1440000
```

Заменить значение eth0 на значение Вашей сетевой карты.

Чтобы применить изменения, выполняем следующие команды

/sbin/sysctl -p

/sbin/sysctl -w net.ipv4.route.flush=1

Безопасность PHP

PHPSuExec

- PHP работает как простое CGI приложение
- Нельзя запустить php как модуль для apache (mod_php)
- php_value/php_admin flags недоступны
- suPHP

Что следует добавить в php.ini для защиты сервера от взлома скриптов:

escapeshellarg — Escape a string to be used as a shell argument
escapeshellcmd — Escape shell metacharacters
exec — Execute an external program
passthru — Execute an external program and display raw output
proc_close — Close a process opened by proc_open and return the exit code of that process
proc_get_status — Get information about a process opened by proc_open
proc_nice — Change the priority of the current process
proc_open — Execute a command and open file pointers for input/output
proc_terminate — Kills a process opened by proc_open
shell_exec — Execute command via shell and return the complete output as a string
system — Execute an external program and display the output

Использование фаервола mod_security для веб-сервера:
http://www.modsecurity.org/download/index.html

Все ошибки в работе веб-сервера записываются в **/usr/local/apache/logs/error_log**

Логи доступа к серверу записываются в **/usr/local/apache/logs/access_log**

Пользовательские логи хранятся в **/usr/local/apache/domlogs/** (логи, трафик, фтп)