IP : nnn.nnn.nnn.n
Hostname : example.domain.com
OS : CentOS release 6.6 (Final)

The following is a report on the security and performance of your server. It includes a few suggestions that will help in the better running of your server. Once you have gone through the entire report, you can discuss with us on the things you can implement from the suggestions in our report.

Please note that some of the suggestions will require us some time to implement them. If the listed issue is urgent (ask us), one of us will fix it when you get back to us, otherwise the tech who sent this report will fix it when the tech is on the shift.

Kernel

The kernel is the core software that controls all the hardware resources on your server. It is advisable to have the latest. kernel running on your server for security and compatibility reasons.

The current version installed on your server is 2.6.32-431.5.1.el6.x86_64 and it's the latest available.

SSH

SSH is used to securely access the command line on the server via the Internet. Currently it is using the default setup as described below.

SSH is open to the world. We can restrict access and only allow connections from approved IP(s) to make it more secure. SSH direct root login is currently allowed. We can disable it and make it so only certain users can get access, via sudo (sudo users are privileged users who can run as root via password authentication).

The SSH port is set to the default. Changing to a non default port would make it more secure.

Bash shell is enabled for normal users as follows. It is advisable to be disabled unless you absolutely require a shell. If you do need it, you should only accept logins from approved IP(s).

theewfin

FTP

The FTP service runs on your server to allow normal users to transfer or modify their website content, files and folders. The default setup on your server is less secure.

It is advisable to disable FTP from all locations and allow connections from approved IP(s) only, so that unauthorized changes to files from unknown parties can be prevented.

Secure mount temporary filesystems

The temp partitions/space on a server allows the running programs to use that space to create temporary files. These partitions should be securely mounted, to prevent unauthorized executions of some malicious programs.

The temp partitions are mounted on your server as below. They are secured.

/usr/tmpDSK on /tmp type ext3 (rw,noexec,nosuid,loop=/dev/loop0)
/tmp on /var/tmp type none (rw,noexec,nosuid,bind)

Disk space

Current disk space usage on your server is shown below.

```
root@webserver [~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       39G  8.2G   29G  23% /
tmpfs           935M     0  935M   0% /dev/shm
/usr/tmpDSK     2.0G   36M  1.8G   2% /tmp
root@webserver [~]#
```

PHP

There are certain PHP functions that allow normal users to access system level functions. These dangerous PHP functions listed below should be restricted on a production server.

exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_source

They are not restricted on your server at the moment.

Also, the below options may be set as shown below in the global php.ini to restrict access further.

```
display_errors = Off
log_errors = On
allow_url_fopen = Off
safe_mode = On
expose_php = Off
enable_dl = Off
```

These changes may cause problems to certain sites because their code may be using the above disabled functions (which is not best practice while coding).
If your site does encounter troubles, we can enable the functions, however please be aware of the risks.

Apache

Apache is the web service that runs on your server to serve the websites

hosted on your server to the Internet. It is advisable to disable certain apache parameters in its configuration file to make it more secure.

ServerTokens Prod
ServerSignature Off
Options -Indexes

We can further optimize the mpm parameters of apache namely StartServers, MinSpareServers, MaxSpareServers, ServerLimit, MaxClients, MaxRequestsPerChild, Timeout, KeepAlive, KeepAliveTimeout. However this will be trial and error method to achieve the best possible configuration as each server has different requirements.

MySQL

The MySQL service on your server handles the databases of the websites on your server.

The current MySQL server configuration on your server appears to be not optimized.

We can run a popular MySQL tuner script to analyze the server and tune the service considerably. This can help the MySQL service to run more efficiently. Again, this optimization is also a trial and error method.

Files and Folders

The website files on your server that are hosted publicly on the Internet have world writable permission. This will pose a significant security risk because they can be exploited by hackers.

To mitigate this, it is always advisable to run on suphp with suexec, which slightly affects the speed of php execution, but improves security.

Malware and Rootkits

Malwares are exploitative programs that can stop a server working properly. Rootkits are a different kind of exploitative program that also affect the functioning of the server and also take part in automated illegal activities. Scanning of your server with popular malware and rootkit scanners is best practice and can lead to early detection.

Below is a report for your server take from a popular malware scanner called Linux Malware Detect.

malware detect scan report for Example.domain.com
SCAN ID: nnnnnn.nnnn.nnnn
TIME: Month YY 10:03:19 +0300
PATH: /home//public_html/*
TOTAL FILES: 6266
TOTAL HITS: 0
TOTAL CLEANED: 0

The popular rootkit scanner, rkhunter doesn't showed any possible rootkits on this server.

IP reverse PTR or rDNS

A reverse PTR record for a server IP is a dns record setup for that IP to determine its authenticity. As a best practice every public IP you have on your server should have a rDNS to verify to the Internet that your IP has a genuine identity. The server has the following IP(s). Listed next to each one is its rDNS.

nnn.nnn.nnn.n - example.domain.com

Mail IP Reputation and blocklist listings

The reputation of server IP(s) play an important role in the mail delivery from the server. There are a series of public blacklists that every mail handling service checks to determine the reputation of the IP from which it received an email.

Our check reveals that your server IP appears to be not listed on any of the blacklists.

*Checking nnn.nnn.nnn.n against **88** known blacklists...*
*Listed **0** times with **0** timeouts*

Firewall

Your server doesn't have any firewall installed. A firewall is an important application that runs on a server to keep it safe from unauthorized access, attacks and exploits.

Load Averages , Resources and Memory

A server uses cpu, memory and other resources to keep it running. Monitoring the resource usage on a server is very important for its efficient working. We have installed a simple logging script on your server and it shows load average as normal.

Nagios

Nagios is our monitoring service that we use as part of our managed service monitoring policy. The standard services on your server shown below have been added to our nagios monitoring service, which will alert us to any issues so that we can take appropriate action.

Current Load - load avg is checked

Filesystem - filesystem writable
HTTP - http status 200
Memory - free system memory
MySQL - MySQL port connection
PING - packet loss to host

POP - port110 pop server connection
SMTP - port 25 smtp connection
SSH - ssh port up
Swap Usage - swap is free enough
TMP folder - tmp is writable
Total Processes - processes number under threshold
Zombies - checking for zombie processes