VPS Security Tips by tmzVPS

Steps to Improve your VPS Hosting Security

Any online server is subject to attempts to gain illegal access. Remote scanning for vulnerabilities by the bad guys is a round-the-clock nuisance. An intruder into your server can be problematic and depending on the degree, damaging to your business.

Taking proactive steps to secure your server takes a little bit of time initially, but returns dividends daily.

tmzVPS offers the following services for managed VPS and managed dedicated server customers.

If you have a question about your VPS security or would like to discuss how tmzVPS can help you secure your web hosting, please contact us here: https://www.tmzvps.com/contact/.

---

(1) Operating System Updates

An operating system is the base software (Linux or Windows) in which everything runs. Keeping your operating system updated is vital, and security updates should be installed as soon as they are available.

Cpanel/WHM has multiple options for automated nightly operating system upgrades.

After logging in to WHM navigate to: *Home >> Server Configuration >> Update Preferences*

More information on the cPanel update options can found here:
https://documentation.cpanel.net/display/ALD/Update+Preferences

If you are not using cPanel / WHM, then manual updates and scripting a CRON job to perform regular upgrades are necessary.

In CentOS/RedHat/Fedora run the following command as root:

#yum -y update

In Debian run the following command as root:

#apt-get update && apt-get upgrade -y

If there is a kernel update you would need to reboot your server after the update.

(2) Firewall - CSF / LFD

A firewall is the entryway doorman to a VPS. A firewall is a software that runs to control inbound and outbound packet traffic determining how such should be processed based on defined rules. All packets must travel through the firewall.

A proper firewall should prohibit all traffic except that which has been intentionally enabled.

Firewalls often perform other roles policing malformed packets, high volume situations, and prohibited access attempt blocking.

In Linux *iptables* is the package underneath common firewall solutions like CSF (ConfigServer Security & Firewall) and APF (APF Firewall). It is extremely powerful but is complicated and prone to administration errors. Using a simplified tool for iptables like CSF is therefore recommended.

---

(3) Passwords

Passwords are regular sources of security problems. Weak guessable passwords often result in security compromises. This includes the bad practice of reusing passwords across multiple sites or accounts.

Passwords should be unique per site and complex. To track your passwords you should use a secure password manager like KeePassX.

Your passwords should be a mix of uppercase, lowercase, characters, numbers and punctuation. Passwords with longer length are more secure.

To generate secure passwords you can use Norton's online password generator:
http://www.tmzvps.com/password-generator/

In Linux there is a free commandline tool called agp (Automated Password Generator):

```
apg -a 1 -n 5 -m 12 -x 12
```

(Generates five random passwords with a minimum and maximum length of 12 characters.)

(4) SSH Access Limits

Secured Socket Shell (SSH) is a text based terminal interface used on all Linux distributions to perform maintenance, configure software, etc.

To secure SSH access, you should consider limitting root access logins.

There is also a very useful and more secure means of using password-less SSH. This works by generating a key on your local computer then copying that key to your remote SSH server. When configured you can connect to your server using SSH without typing any password. Additionally, once enabled you can configure the SSH server to only allow password-less key based access, which will disallow any password based attempts and attacks.

Changing the SSH port from the default 22 to something else is recommended. This will prevent random scanners from quickly identifying your SSH server port .

Edit sshd_config to change SSH server port:

#vi /etc/ssh/sshd_config

Port 22 ← change to your new port

#service sshd restart ← to restart the SSH server

#ssh 80.20.10.40 -p 10000 ← connect to port 10000 on remote server – where you SSH server is now running

For more advanced protection, you can use iptables to limit SSH connections to five per minute and limit SSH access to only your own IP to further secure SSH access.

---

(5) Brute Force Protection

tmzVPS includes cPHulk Brute Force Protection with all managed VPS and dedicated servers. cPHulk monitors failed login attempts and takes proactive steps to block offending IP addresses. cPHulk protects from SSH attacks and email attack attempts.

For unmanaged VPS users, we recommend Fail2Ban. Fail2Ban monitors access attempts for SSH, Apache Web Server and FTP by default and takes proactive actions to block offenders.

---

(6) Antivirus

If an attack or compromise was successful against your server, the intruder usually leaves scripts in place to allow for future re-entry. Scanning your VPS routinely to detect such scripts is recommended.

There are several Linux packages to help keep your VPS clear of virus infections and rootkits.

ClamAV is an anti-virus scanner for Linux. It is available as a package in most distributions.

The two commonly used rootkit scanners are RKHunter and chkrootkit. RKHunter is scanner that looks for rootkits, backdoors, sniffers and other exploits.
