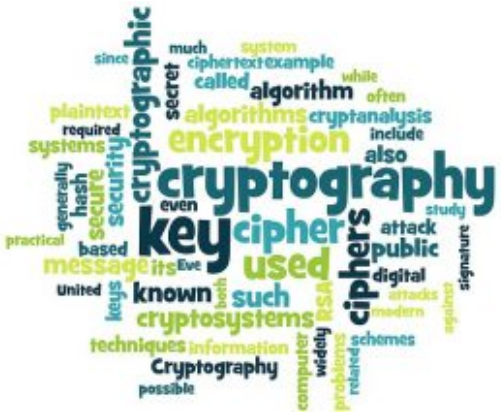
Keeping your dedicated server safe in 2020

Server security is of the utmost importance this year as cyber-criminal technologies are becoming increasingly advanced. What I've suggested below are simply tip-of-the-iceberg suggestions on how to keep your dedicated server safe in 2020 and beyond.

First, does your prospective dedicated service provider perform an extensive security check on the servers that they lease, prior to and during provisioning? Do they publish their security audit procedures?



Preventing exploits

Some things that you can do on your own

- Ensure that the traffic between your computer and server is encrypted. One way to accomplish this would be to use TLS protected interfaces. This provides a layer of security that makes it more difficult for cybercriminals to steal login info. Stolen logins give them the ability to execute attacks on your server. If you're using cPanel, services like webmail, SMTP, WHM and IMAP can be provisioned with TLS protection.
- When you're managing your server, ensure that every application you use is free of viruses and malware. In other words, ensure that you're only utilizing computers and networks that you trust when managing your server.
- Keep all active scripts up-to-date by installing and updating patches and other releases as soon as they're available.
- You could assign a different port for SSH, which would prevent *automated* brute force attacks.

Questions to ask

Important Queries

- **What are your PHP settings?** There are any number of PHP settings that could be disabled if not absolutely necessary. The end goal here is to prevent arbitrary

code execution and SQL injections, as well as any number of PHP based malware.

- **Are you using Mod Security Rulesets and are they up-to-date?** Unfortunately, Mod Security rulesets are not something you can set and forget because rulesets are continuously updated.
- **Are your server's system binaries up-to-date?** Again, check the versions of stuff like BIND and Apache for known exploits.
- **Unneeded services?** Just like WordPress, you should disable any services you don't need – to lessen the possibility of exploits.
- **Do you know what your kernel version is?** Kernels versions need to be kept up-to-date to prevent any vulnerabilities or exploits.
- **Security check configurations** When setting up your server, ensure that processes like Exim, cPanel, SSH, FTP, PHP and MySQL are optimized for security.
- **Have you checked and optimized your CSF/LFD settings?** The CSF/LFD firewall features automated processes to detect brute force attacks, SYN flood protections and other processes.

Scan for malware

Scan for known exploits and rootkits

Although there are a good number of anti-malware programs, free and paid, Emsisoft is very popular and stable. Their server version is based on Emsisoft Anti-Malware, but optimized for server systems. It includes email notifications on infections, and can used for file servers, mail servers and so on.

Rkhunter is also recommended. From TECmint's site, "Rkhunter (Rootkit Hunter) is an open source Unix/Linux based scanner tool for Linux systems released under GPL that scans backdoors, rootkits and local exploits on your systems. It scans hidden files, wrong permissions set on binaries, suspicious strings in kernel etc."

and offer a four (4) hour hardware replacement. Throw in IPMI for remote management, support for public and private networks, free operating system (OS) re-installs, and SATA, SAS & SSD (including NVMe) storage. Call +1 877 477 9454 or email us at Sales@ProlimeHost.com. We’re here to help.