Fundamentals of UNIX & Linux for System Administrators

FUL-02: Web Server Applications

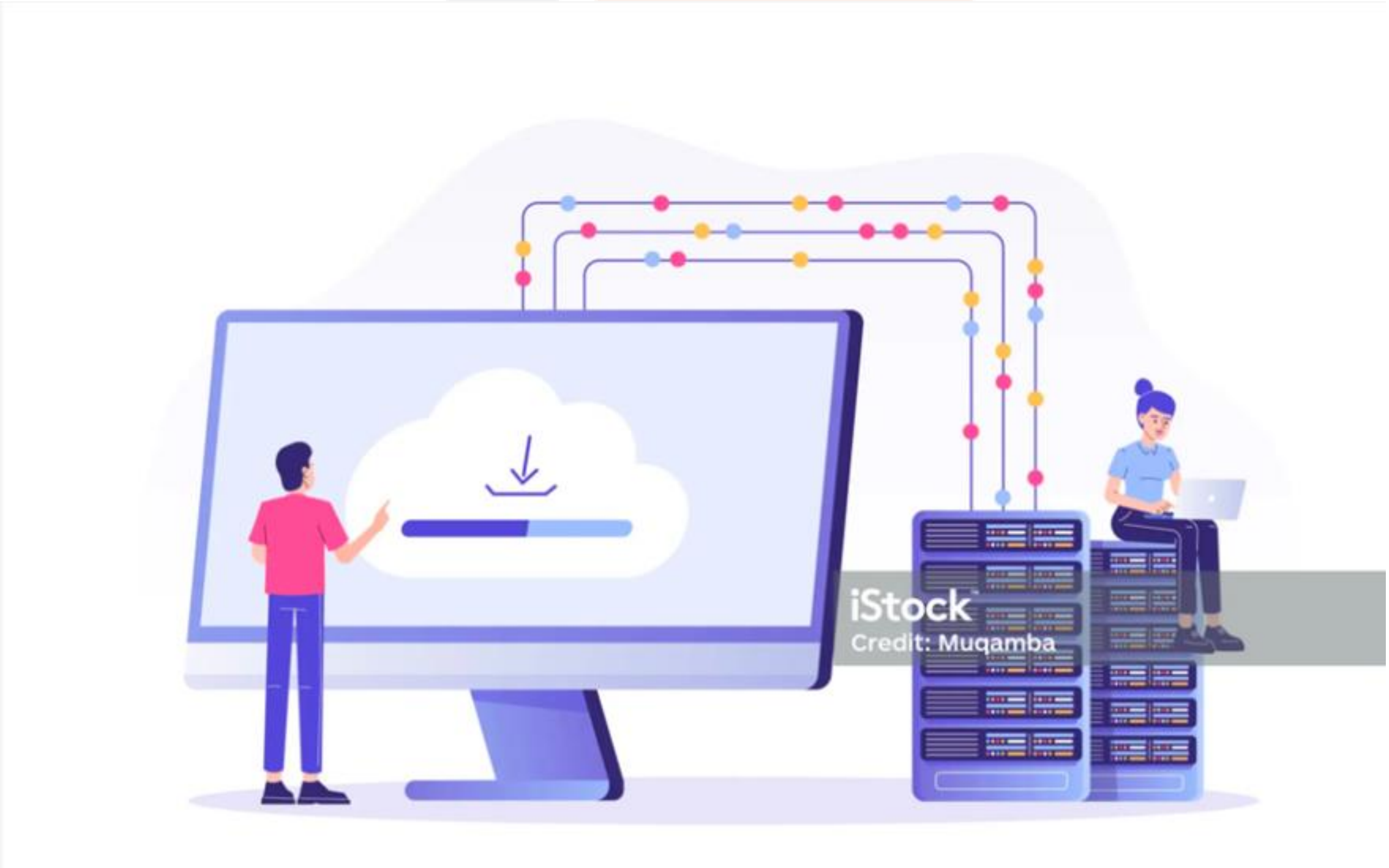
Joy Otuya Oyim

System Administrator, KENET

Agenda

- Popular Web Servers
- Common Website Attacks
- Website and Web Server Hardening
- Web Server Security Consideration

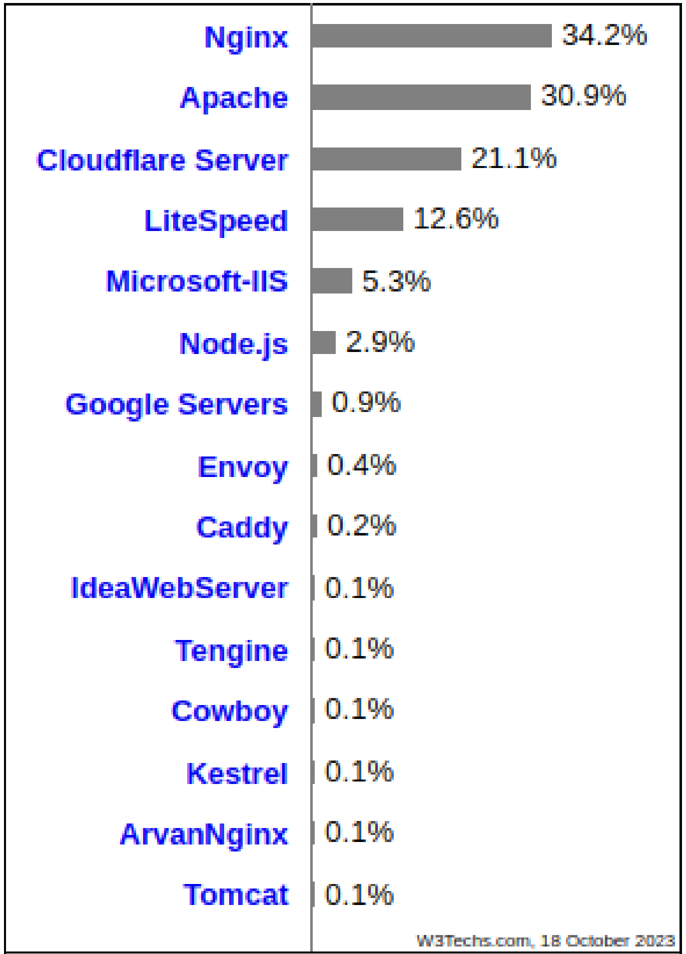
Webservers ?



Webservers ?

- A web server is **a software used for serving files to users on the Internet**. The web server software is responsible for ensuring the communication between the server and the client is secure and flawless. The software works as **a link between two machines** (a physical server and a user's device). When a user makes a request, the web server grabs the files from the physical server and delivers them to the user. So, web servers must serve different pages to different users at the same time.

Popular Webservers



W3Techs.com, 18 October 2023

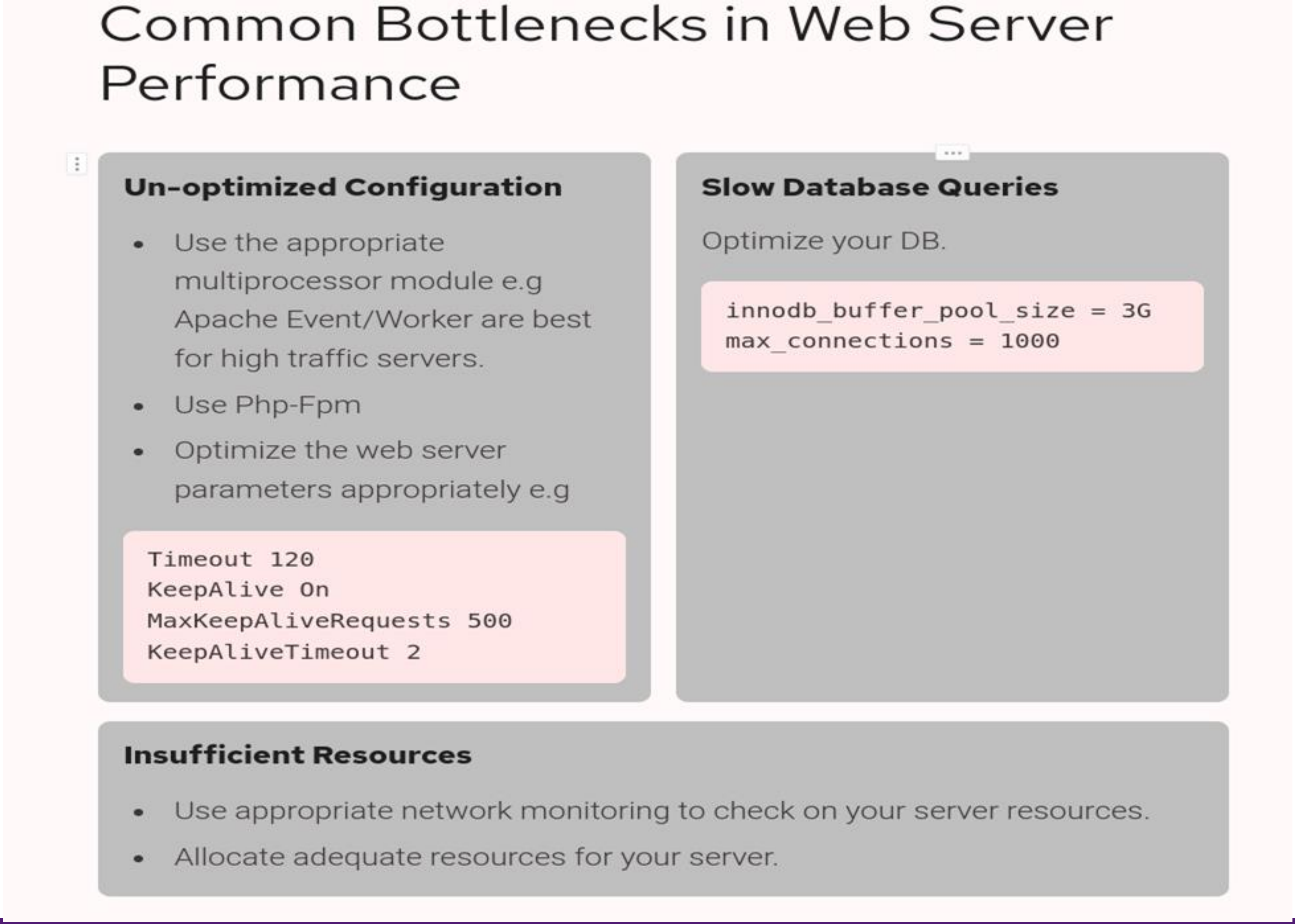
Percentages of websites using various web servers
Note: a website may use more than one web server

Common Web Application Attacks

- **SQL Injection Attacks**: occurs when an attacker inserts or "injects" malicious SQL (Structured Query Language) code into a web application's input fields or data input, which is then processed by the application's database.
- **Web shells**: A web shell is an executable code running on a server that gives an attacker remote access to functions of the server.
- **Malicious Advertisements (Malvertising)**: use of online, malicious advertisements to spread malware and compromise systems.
- **Denial-of-Service (DoS)**: Causing the web server to be unavailable through various methods. A common attack is the **DDoS attack**
- **Cross Site Scripting:** Attackers to inject malicious scripts (usually written in JavaScript) into web pages viewed by other users.

Website and Web Server Hardening

- **Remove all unnecessary web server modules.** A lot of web servers by default come with several modules that introduce security risks
- **Modify the default configuration settings.** For example, a lot of web servers support old SSL/TLS protocols in their default settings. This means that your server is vulnerable to attacks such as POODLE.
- **Turn on additional protection for web applications.** For example, introduce a Content Security Policy (CSP)
- **Install web application firewall (WAF)**: Most web servers support the open-source ModSecurity firewall.
- **Patch web application software**: Allows users to view and reuse previous commands, enhancing efficiency.
- **Regularly scan all your web applications** using a web vulnerability scanner.
- **Proper user management -** least privilege principal



Common Bottlenecks in Web Server Performance

Un-optimized Configuration

- Use the appropriate multiprocessor module e.g Apache Event/Worker are best for high traffic servers.
- Use Php-Fpm
- Optimize the web server parameters appropriately e.g

```
Timeout 120
KeepAlive On
MaxKeepAliveRequests 500
KeepAliveTimeout 2
```

Slow Database Queries

Optimize your DB.

```
innodb_buffer_pool_size = 3G
max_connections = 1000
```

Insufficient Resources

- Use appropriate network monitoring to check on your server resources.
- Allocate adequate resources for your server.

Securing the Apache web server

- **Hide Apache version and OS identity from errors**: When you install Apache, it displays the version of your Apache web server with the operating system name in the errors.
- **Disable Directory Listing:** By default, Apache lists all the content of Document root directory in the absence of index file
- **Keep updating Apache regularly**
- **Disable unnecessary modules:** It's always good to reduce the attack surface by disabling all those modules that are not currently in use.
- **Run Apache as separate User and Group:** For security reasons, it is recommended to run Apache in its own non-privileged account.
- **Use "Allow" and "Deny" options in the Apache config file to restrict access to directories.**
- **Enable Apache logging:** it is wise to enable Apache logging, because it provides more information, such as the commands entered by users that have interacted with your Web server.
- **Proper user management -** least privilege principle

Securing the Apache web server

- **Securing Apache with SSL Certificates**
- **Use ModSecurity Module (modsec) to secure Apache:** Modsec works as a firewall for our web applications and allows us to monitor traffic on a real time basis. It also helps us to protect our websites or web server from brute force attacks.

ModSecurity Rules

There are free updated rules from

1.**OWASP: the OWASP ModSecurity Core Rule Set (CRS)** is a set of generic attack detection rules for use with ModSecurity or compatible web application firewalls.
url: https://owasp.org/www-project-modsecurity-core-rule-set/
2.COMODO: Comodo ModSecurity is the best Web Application Firewall for web apps and websites running on Apache/Linux web-servers.
url: https://modsecurity.comodo.com/
NB:You can also write your own custom modsec rules

Q & A

kenet
Kenya Education Network

THANK YOU

www.kenet.or.ke
Jomo Kenyatta Memorial
Library, University of Nairobi
P. O Box 30244-00100, Nairobi.
0732 150 500 / 0703 044 500
support@kenet.or.ke / jotuya@kenet.or.ke