**Name of Title:** Learning Nginx

**Video Name:** 05\_01 Security with nginx

**Estimated Length:**

**Author Name:** Michael Jenkins

**Chapter\_Section\_Video:**

**Video Objective:**

At the end of this video the learner will learn the ways you can make sites more secure with allow/deny directives, password protected locations, and SSL certificates.

**Introductory Statement:**

Type your introductory statement here.

**Speaking Points:**

1. Point\_1
2. Point\_2
3. Point\_3
4. Point\_4
5. Point\_5

**Script:**

SLIDE: 05\_01 Security with nginx

All too often, we hear news about websites getting hacked or otherwise compromised and the resulting damage that these intrusions can cause.

So as you’re learning about nginx, you might be wondering, “What can I do with nginx to help keep my sites secure”?

Here are a few things you should consider when it comes to nginx and security.

SLIDE: Security with Nginx

1. Keep your operating system and software patched and up to date
2. Restrict access where possible
3. Use passwords to protect sensitive information
4. Use SSL to protect transmissions and identify your site

The first thing you can do is make sure your operating systems and software are using the latest versions possible and have all security updates applied. This will help make sure you're protected against known vulnerabilities.

Next, you can restrict access to certain parts of your site. We’ll take a look at how you can configure nginx to allow access to certain pages based on IP address.

You can also use passwords. This can help keep sensitive information protected and slow down intruders.

And you can also apply SSL or Secure Sockets Layer. SSL is a protocol for establishing encrypted links between a web server and a browser. This helps keep communications private between the web server and the person requesting the content. Also, using SSL certificates that have been verified can help to identify sites as being who they say they are

Earlier in the course, we discussed installing the latest versions of Ubuntu and nginx. Now let’s take a look at these other ways we can keep things secure on the web.

**Conclusion:**

Type your conclusion statement here.

**Script and Media:**

Break the script up into parts and align it with any media (slides, web, CLI, etc.)

| **Part** | **Script** | **Media** |
| --- | --- | --- |
|  |  |  |

**Exercise Files:**

**Basement:**

<https://www.webarxsecurity.com/website-hacking-statistics-2018-february/>

Websites listed in our data were either defaced, hosting known malware or were redirecting traffic to malicious third-party sites.

Mostly through CMS software like Wordpress, Joomla, Drupal, Magento

A new report from security firm Sitelock has revealed that the typical small business website is attacked 44 times a day and software “bots” are visiting these sites globally an average of 152 million times a week.

The report, based on the company’s analysis of more than six million websites during the last quarter of 2017, found bots, malware, backdoors, and other malicious software on so many of these sites that the company estimated that more than 18.5 million websites are infected at any given moment.

<https://www.digitalocean.com/community/tutorials/how-to-secure-nginx-on-ubuntu-14-04>

## Step 2 — Configuring SSL

Step 3 — Restricting Access by IP

## **#21: Keep your software up to date**

You must keep your software and kernel up to date all time. Apply patch as per your version or distro. If you are using a Debian/Ubuntu Linux use [apt-get command](https://www.cyberciti.biz/tips/linux-debian-package-management-cheat-sheet.html)/[apt command](https://www.cyberciti.biz/faq/ubuntu-lts-debian-linux-apt-command-examples/) to apply patches:

$ sudo apt-get update

$ sudo apt-get upgrade