Implementing Network Device Security

Modality: On Demand

Duration: 1 Hour

About this Course:

The security of your network devices is really important. Because it holds your valuable data which is at stake all the time from being hacked, altered or removed. Some devices also do not have built-in security systems. So, it is important that you must be familiar with the concept of network device security and knows how to implement various measures to secure your devices.

Course information:

Your network device can be at stake due to many reasons like outdated network devices if the SNMP is set to public or some issue with the default credentials. If your network devices are well-secured, then the performance of the devices will also be updated. In this way, secure networks can prove to be beneficial for the effectiveness and growth of any company. If you have multiple network devices then it is important to secure and manage all the shared networks and relevant shared data. Implementing network device security is very much critical to your information security.

Following are some of the ways you will learn in the course to save your network devices from the possible potential risks:

Firewalls:

In lay-man terms, firewalls are the blocking walls between your network devices and the other potential threats. It keeps away all the harmful threats from being imposed to your valuable data. It is important you know how to enable firewalls in your network devices. It is important to have the settings maintained with the security policy changes. Firewalls are the most convenient way to protect your networks from unwanted harmful threats.

Routers security:

The user should have routers security updated and maintained while using the internet. Any weak network is vulnerable to any kind of virus or threat. So, the routers should be well-secured. The password for the security system is really important as it is the first and foremost way to make your network safe. Any interruption with the SSID broadcast can provide an easy target to the hackers or related problems.

Web security gateways:

When working in corporate offices, all the network devices are connected and the data is freely available to share. But sometimes your device carries information you do not want to share with the third party. In this case, you should have web security gateways. It is one of the most applied security solutions in implementing network device security. It blocks all the unwanted and unsecured traffic

from entering a closed shared network. These security gateways are used to secure network devices from any malfunctioning caused by viruses or malware.

An intrusion detection system (IDS):

It is a security system to protect your device and monitor any unwanted activity on your device. It detects any kind of external attack on the network and works well in helping to determine the backward track of attack. It has two parts: NIDS & NIPS. Both these parts of the system detect any suspicious activity and give warning to the system.

URL filters:

URL filters help the user to maintain a well-secure network device and avoid any kind of entry of viruses or malware. As the name suggests, URL filters determine which URLs are safe to open and secured and which are not. Thus, minimizing the chance of transmission of virus attack into the system.

Course Outline:

- The network devices hold some great importance for someone who wants to get connected to the internet since they are his ticket for the connection. But the security of those network devices is very important since one might be at some potential risk of data theft and the data alteration which can be dear to someone. The network devices can be secured in many ways. After securing one can ensure some good performance and can hence improve the productivity of his company.