NetAnalyzer Guide

Index:

Securing Ports

Open ports:

Ports in networking are used to allow devices to communicate with each other both from outside and within the local network. Each port number has a specific purpose for being open, ports should not be open unless there is a purpose they are serving, for example, if you have a web server running it would make sense for port 80 or 8080 to be open, otherwise, this could be a risk and a path for malicious actors to infiltrate your network.

Method for mitigating unknown open ports:

Linux:

Step 1: Run the command “sudo ufw deny (Insert port number here)”

Step 2: Run NetAnalyzer again to ensure the port is now closed.

Windows:

Step 1: From the Windows Control Panel, navigate to the “System and Security -> Windows Firewall” section and click the “Advanced Settings” menu item.

Step 2: In the “View and create firewall rules” section, select the “Inbound Rules” menu item.

Step 3: From the list of inbound rules, find the rule for the port you wish to close. Select the rule and click the “Delete” menu item to delete the rule and close the corresponding port.

macOS:

Step 1: Locate the process ID using this command: “sudo lsof -i (Insert port number here)”

Step 2: After that, run the command “sudo kill (Insert process ID here)”

Step 3: Run NetAnalyzer again to ensure the port is now closed.

Software Updates

Software Updates:

It is important to keep your software updated to ensure everything has the latest security patches to reduce the risk of any bugs or exploits that may have affected earlier versions of the software. It is also important to keep your operating system up to date for the same reasons. There are continuously new security patches being released that will harden the system making it more difficult for attackers to get in. The best way to make sure updates get installed promptly is to enable automatic updates for the different programs you use and the operating system.

Firewall

Firewall:

The main purpose of a firewall is to block malicious internet traffic from entering the internal network. For example, specific applications can be whitelisted by the firewall to have their traffic allowed, this would be the most secure way of using a firewall so that way any

unknown applications do not have access to the internet and can only act within the internal network.

Physical Security

HID Attacks

HID or Human Interface Device attacks exploit the way computers trust common HID peripherals such as keyboards or mice. Essentially, an attacker can use a USB device designed to be detected as a keyboard so the computer can trust it but then be able to run code remotely. These devices are most commonly in the form of USB flash drives or made to resemble smartphone charging cables.

Mitigating HID Attacks:

These types of attacks can be easily prevented, first by only plugging in trusted devices to your system, and also if the system is in a public place it is a good idea to periodically check the USB ports for any unknown devices. Our program checks for these types of devices by searching through a database of common USB ID numbers.

References

https://docs.bitnami.com/installer/faq/windows-faq/administration/use-firewall-windows/