****

**PA-220 Firewall**

**Factory Reset**

Ryan Chen

9/9/2024

**Purpose:**

The primary purpose of this lab is to bypass the password on an existing PA-220 firewall, given physical access. This allows us to familiarize with basic Palo Alto firewall access and control, such as interrupting the bootloader to access additional lower-level utilities.

**Background Information:**

Firewalls are networking devices primarily used to filter traffic coming in and out of a network. By nature, they are security devices, intended to protect users from malicious traffic. In this lab, we explore resetting the PA-220 firewall, a popular device manufactured by Palo Alto. Palo Alto is a company that specializes in cybersecurity and production of primarily network-based security equipment.

Due to the nature of this class, firewalls are shared amongst different years. Since passwords are set on previous year firewalls, they must be factory reset to be used once again. In the real world, this is the equivalent of providing used firewalls to a vendor. If they are not already reset, the passwords must be provided, or the operating system must be reset before being used.

To do so, we must interrupt the bootloader on the firewall to access more utilities, including the factory reset option. Palo Alto firewall maintenance options are obtained by searching up the options online, which Palo Alto provides documentation for.

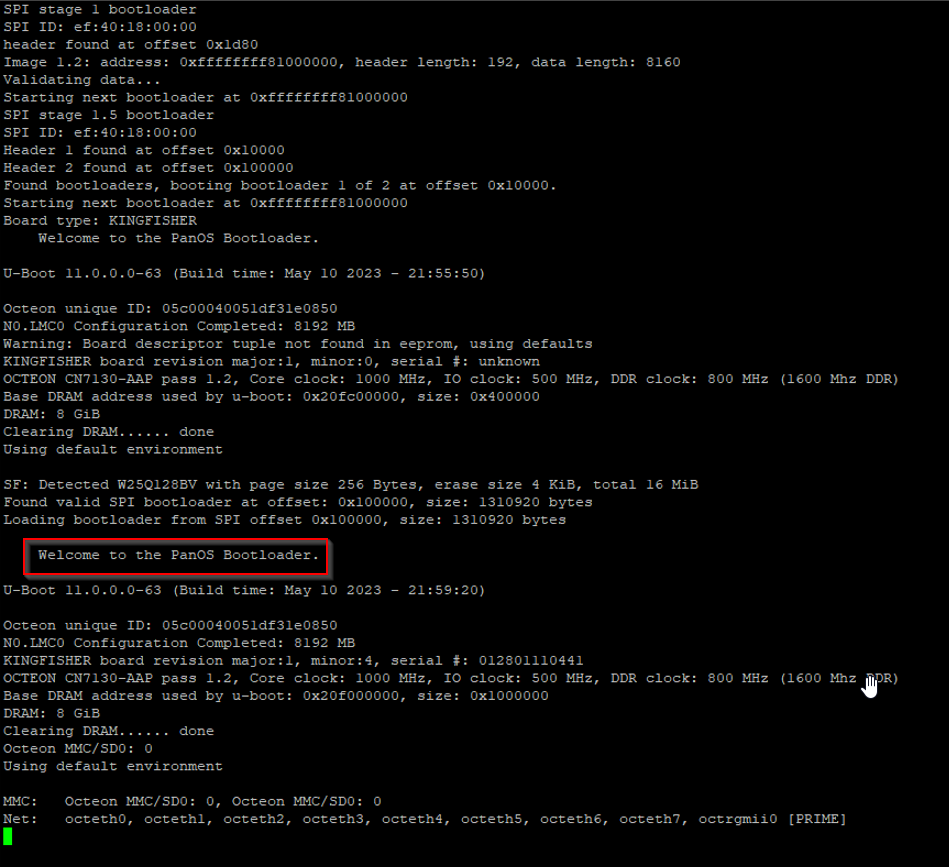
The bootloader of any networking device such as a router or firewall is meant to initialize low level information necessary for the operating system to be loaded. This includes things like mapping the memory out, then loading the operating system in memory. Interrupting a bootloader indicates pausing the process of loading the operating system in, so we can access lower-level utilities.

Palo Alto provides written low-level utilities for such cases. In the event where a user might have forgotten their password or needs to recover the disk/alter the disk image, the Maintenance Recovery Tool allows them to perform these without booting into the actual operating system. This eliminates the need to enter the password, or boot into the OS (in the event where the OS may be corrupted). Other tools are provided as well, such as diagnostics and low-level utilities for OS recovery or scanning.

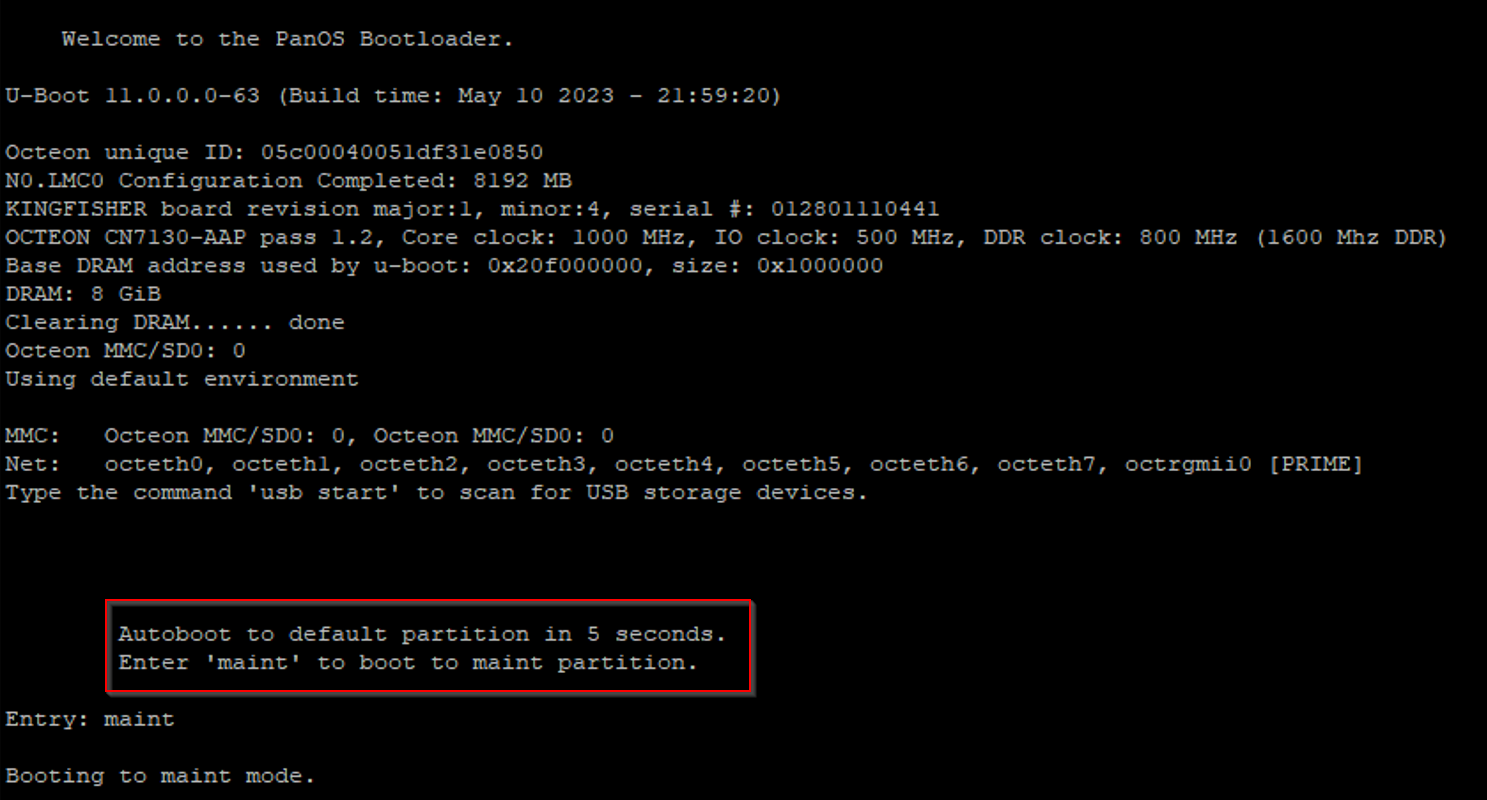
Palo Alto makes interrupting the bootloader simple by providing an interface for users to do so through a CLI. Users are required to type a sequence of text to stop the bootloader process and drop the firewall into a diagnostic state. This process will be demonstrated in this lab.

**Lab Summary:**

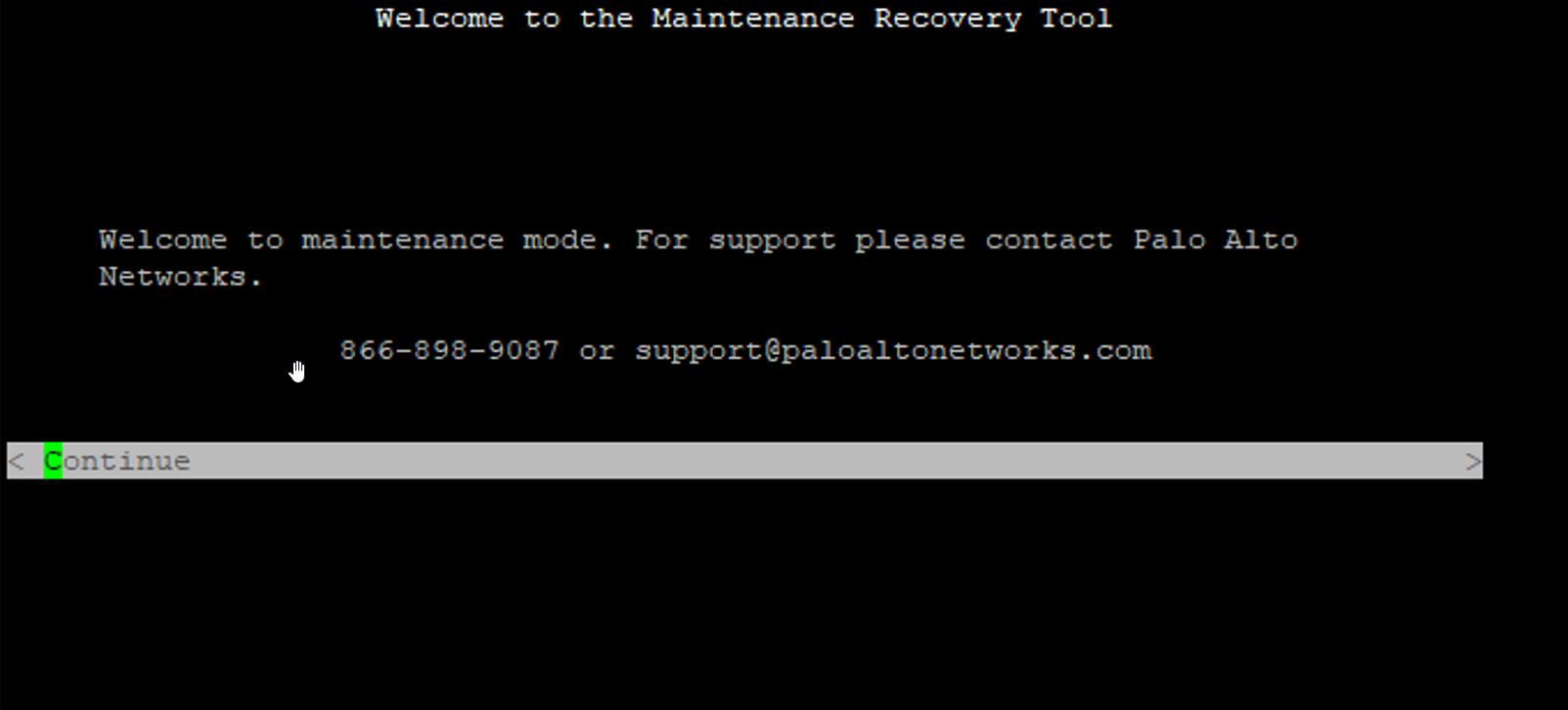
The first step to entering maintenance tools on the PA-220 is to interrupt the bootloader to boot into the utility. To do so, connect through console to the firewall port and power on the device. When the device is powered, text should appear documenting the process of startup.

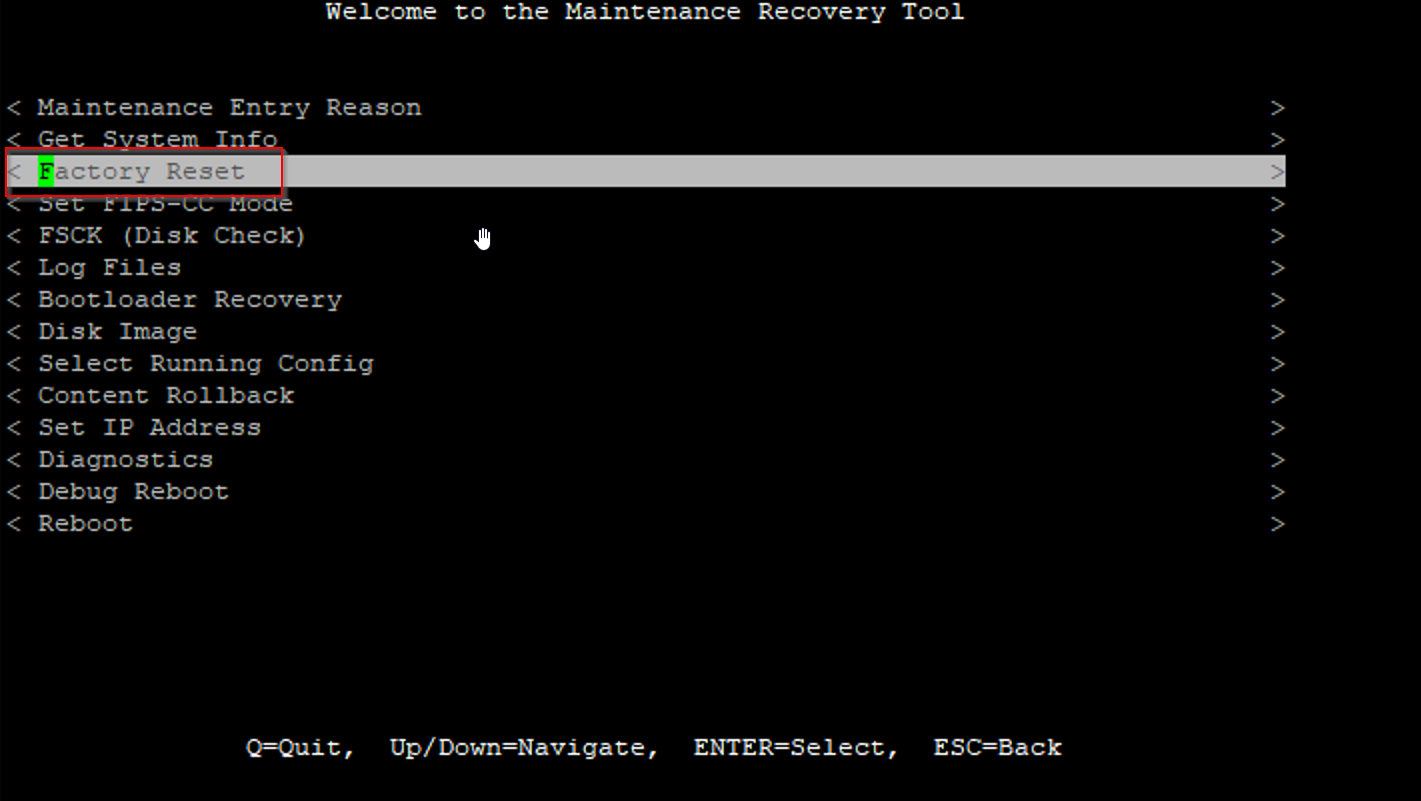


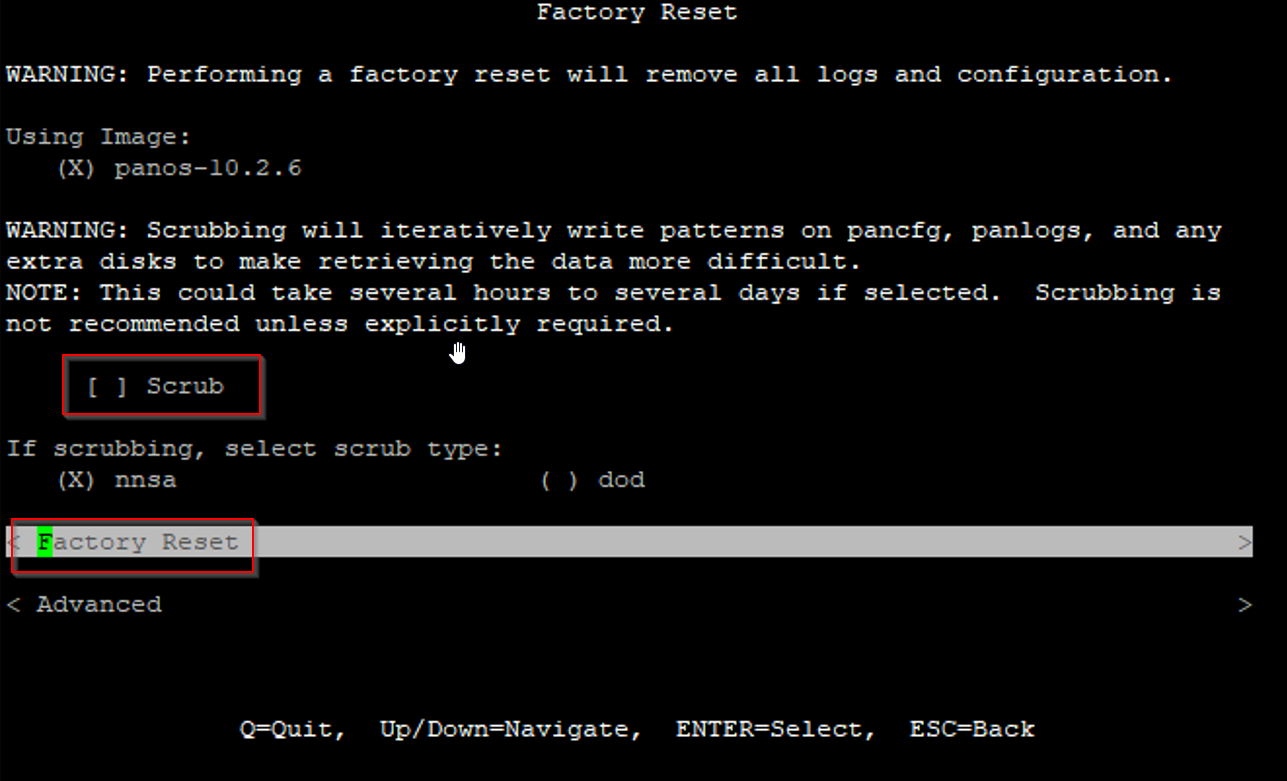
The bootloader will prompt for user input. Typing “maint” will interrupt the bootloader and drop the firewall into the recovery tools.



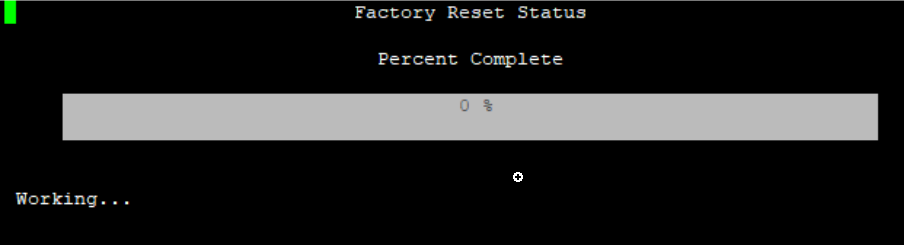
Note that this process takes approximately 5-10 minutes depending on the speed of the firewall.

When booted into the recovery tool, several options will appear.

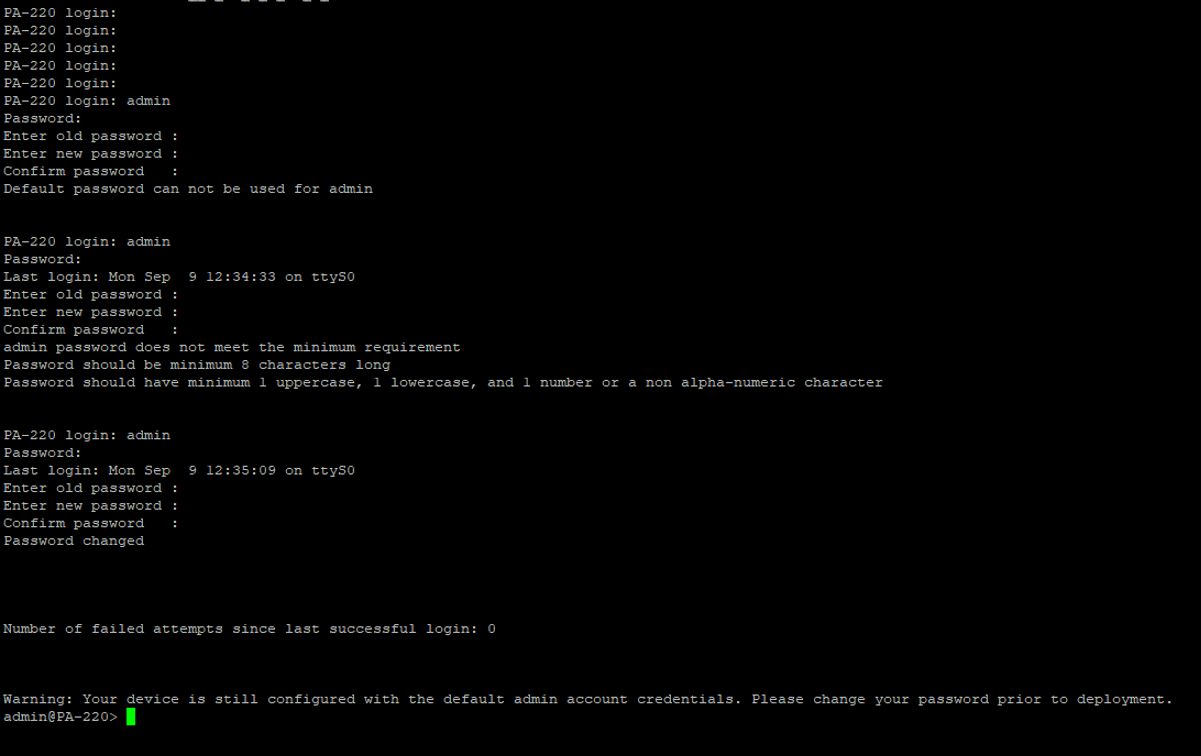
To factory reset, select the corresponding tool, and make sure “Scrub” is deselected. The scrub tool is used to securely wipe the firewall by rewriting existing data. This process, although secure, takes a long time and is unnecessary in this case.



When ready to reset, press enter and wait for the firewall to reset. There should be a progress bar to indicate the duration. After the firewall is done resetting, it should boot directly into login.



The login for a new firewall uses default credentials of “admin/admin”. After this, the firewall will prompt for a new password to be set, and the factory reset is completed.



**Lab Commands:**

The only new learned command in this lab is:

“maint” – (enter at bootloader menu)

*Stands for “maintenance”, used at the bootloader menu to enter Palo Alto maintenance tools.*

**Problems:**

1. **Firewall Loading Time**

The PA-220 firewall takes quite a long time to boot to anything, including OS/utilities. Our group was initially unaware of this, and thus we thought that we had a configuration issue with our console setup. After interrupting the bootloader, we saw no immediate change in startup. Instead, logging messages showed up indicating that the operating system was starting. We thought that this indicated a failure to interrupt the bootloader. However, we later realized that the firewall boot sequence takes a long time. After waiting a few minutes, the Maintenance Recovery Tool appeared, and we were able to proceed.

**Conclusion:**

This was an introductory lab required to proceed further with firewall configuration. Within this lab, skills necessary to reset the firewall were learned, such as interrupting the bootloader. This lab is also an introduction to CLI maintenance on Palo Alto firewalls, done through a console connection.

PA-220 Reset Signoff Sheet

Ryan Chen, P3-4 Cisco CCNP, Mr. Mason

NO SIGNOFF SHEET NEEDED

