Factory Reset

*Palo Alto – Password Recovery*

Adv Cisco Cybersecurity – Lab 1

Jason Liu

Cybersecurity – Mr. Mason & Mr. Hansen

Period 5

*Lab 1: PA 220 - Factory Reset*

**Purpose**

The objective of the lab was to understand and configure a factory reset on Palo Alto’s PA 220 firewall to configure our own password for use.

**Background Information**

Firewalls are a security device that monitors and controls traffic that passes through it. Configurations are done to create policies that define the actions of when and what the firewall can do. Palo Alto is a company that creates a brand of firewalls. They have their own infrastructure and security tools that are considered industry-level. Certain unique features are real-time content scanning, inspection of SSL encrypted traffic, and classifying traffic based on identification categories, not just protocol data.

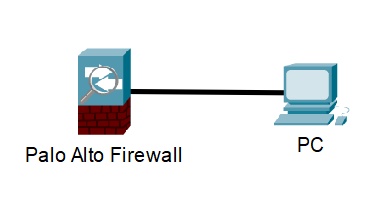
Palo Alto firewalls are configured with a password. Given that an unknown previous password was on the device, it’s important to be able to recover the device’s functions even without the password. This is done through a *factory reset*. A factory reset deletes all previous configuration and resets all security credentials to the default username and password. The default credential is “admin” for all fields. After a factory reset, the firewall prompts a new password.

**Lab Summary**

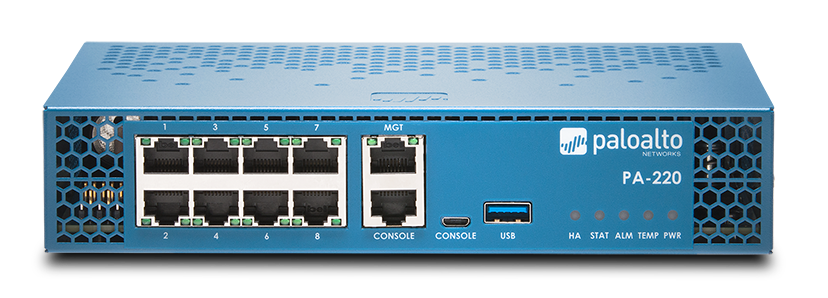
The process is straightforward. By rebooting the firewall through a power reboot, such as disconnecting power, there opens a short window of time to enter the *maintenance mode* upon its initial restart. Consoling into the firewall and using a software like PuTTY, a client can access the CLI of the firewall. On reboot, there is a five second window to press the *m* key and then entering *“maint”* into a prompted field to enter the maintenance mode. There are multiple options from here, but “*factory reset*” is one of them. Wait for the reset status to declare success, and the CLI will prompt a new password of your choice upon the next deployment. The old username, “admin,” will stay constant, but users have the option to change it later. Test the password by accessing the firewall again. The firewall will prompt the new credentials.

**Lab Commands**

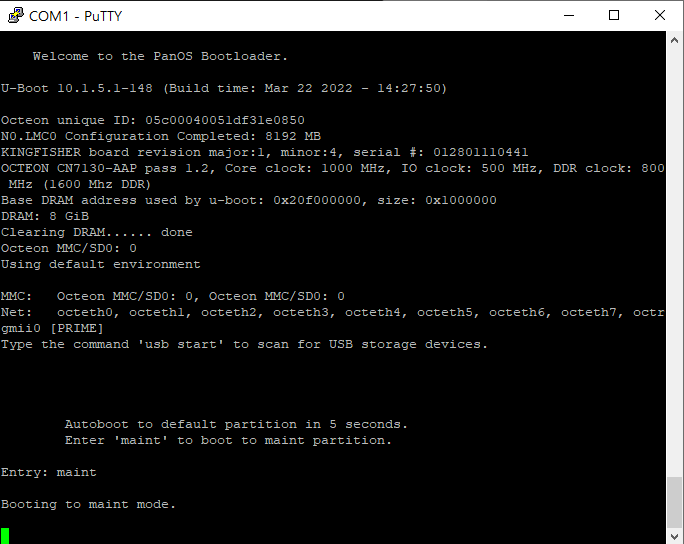
On the firewall, there were not traditional CLI commands, as it was a series of menus, and later a graphical interface. However, there are a few that deal with the console interface in future labs.

****

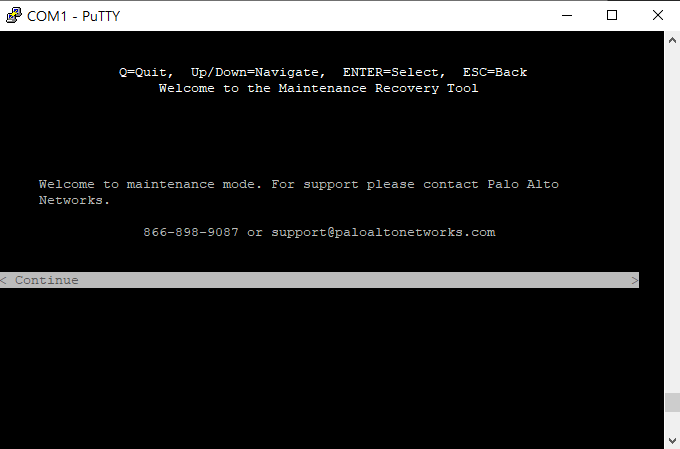
Consoling into the Firewall.



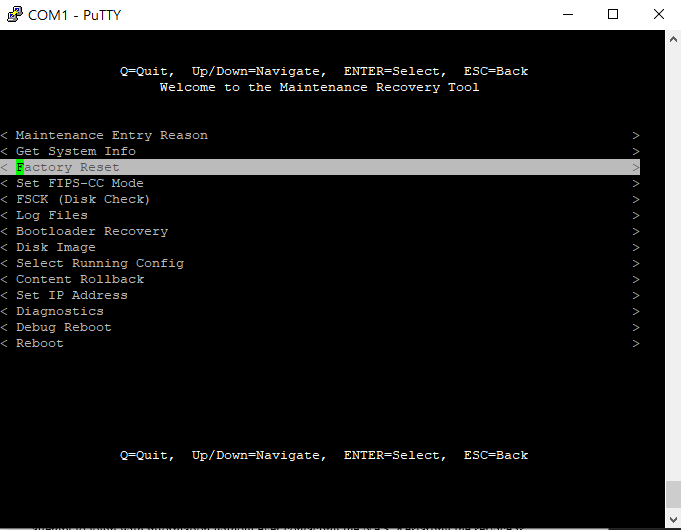
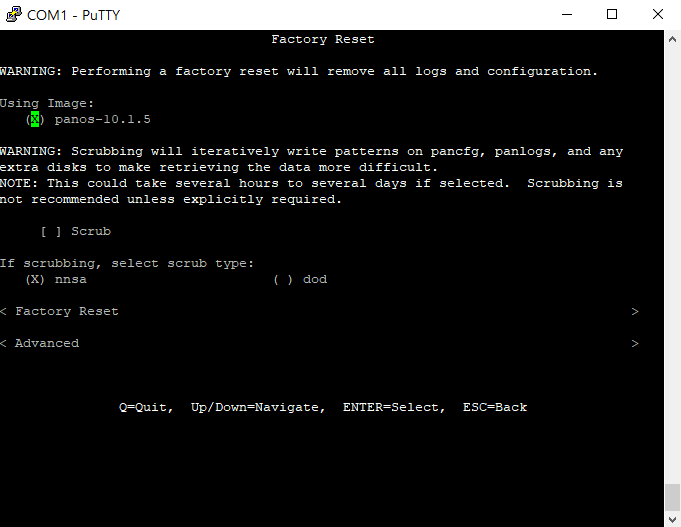
Console port above was used.

**Procedure**

Upon initial startup, enter “*maint*” within 5 seconds of prompt to boot in maintenance mode.

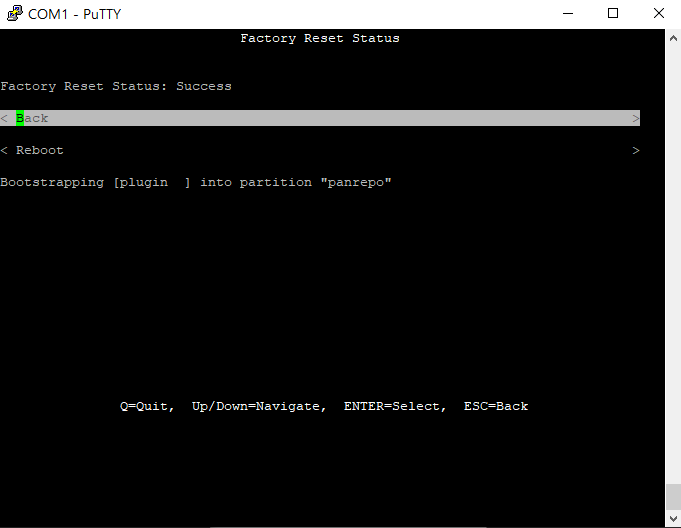
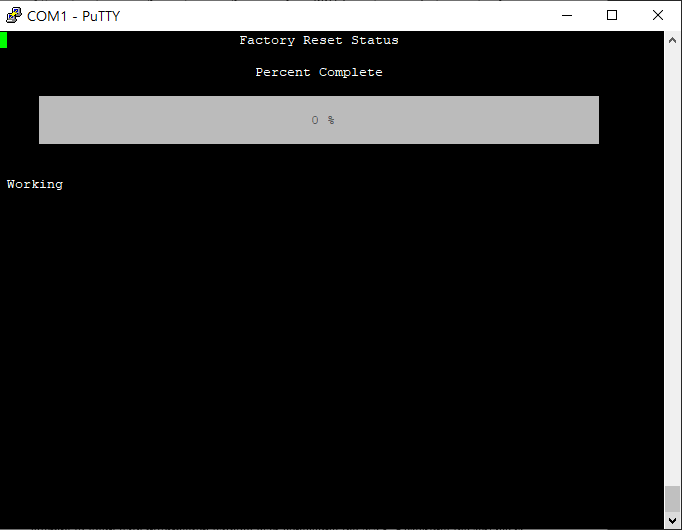
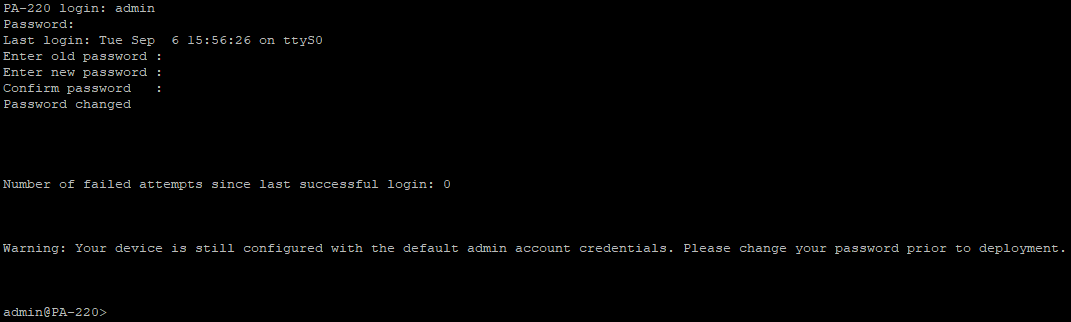
****

Successfully entered maintenance mode.

****

Select Factory Reset in the maintenance mode menu.

Factory reset confirmation. Continue by selecting “Factory Reset.”

****

Factory Reset Status Bar and Success Screen.

Setting new Login and Password after signing with old credentials “admin.”

**Problems**

Even if it was straightforward, there were still issues. Mainly, the input delay for entering the maintenance mode. There was a loading window where the PuTTY wouldn’t update fast enough with the actual firewall while the 5 second window was still counting. We tried multiple attempts, but we eventually solved the problem by preemptively typing “*maint*” so it registered into the router despite not fully loading the lines on the CLI. Otherwise, smaller issues consisted of mistyping our passwords on the password reset prompt, leading to us to have to completely restart.

**Conclusion**

As in introduction to the Cybersecurity curriculum, it is an easy transition to getting to know our firewalls. The simple process was not hard to follow, and the steps are self-explanatory. The practical use of factory resetting a firewall can also become applicable in real life, such as buying supplies from previous owners. This has happened before for other devices like routers and access points. In conclusion, this lab was informative and important to understand.