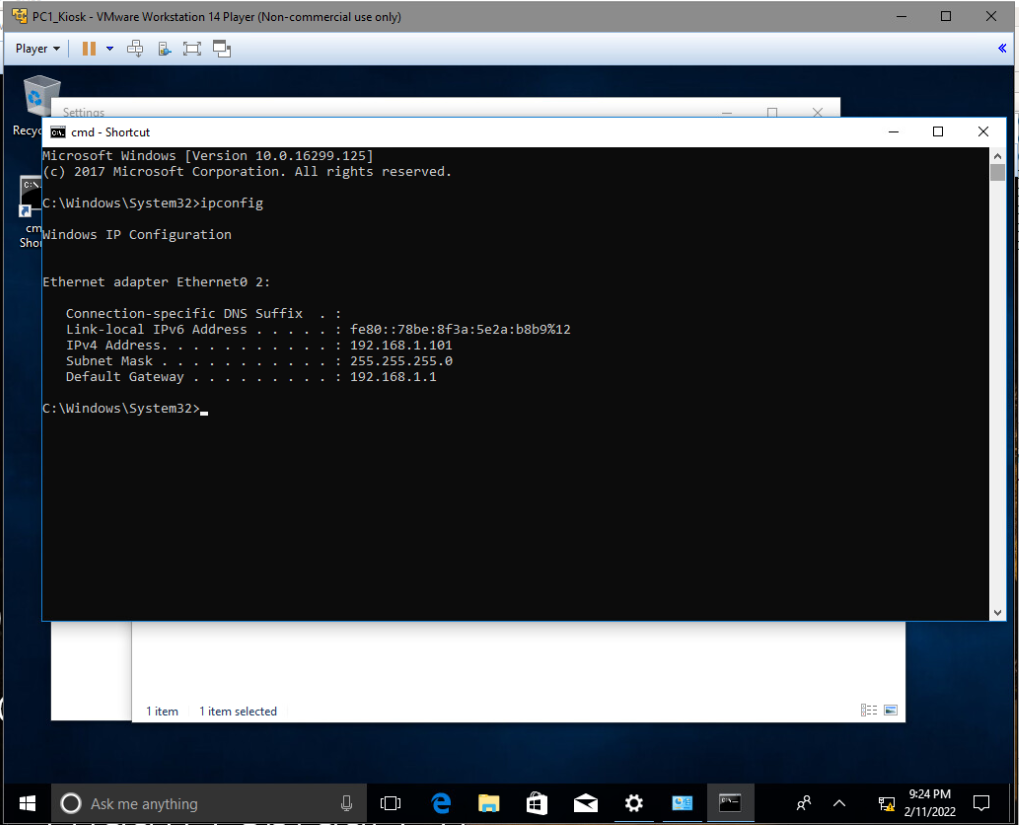
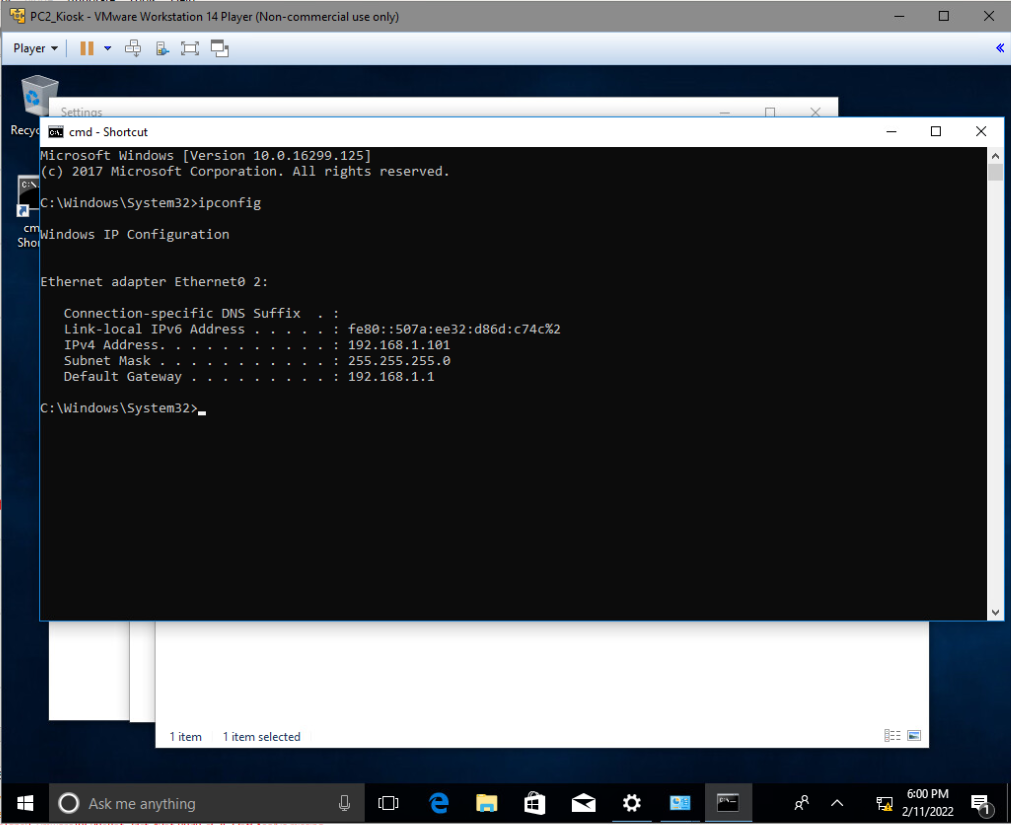
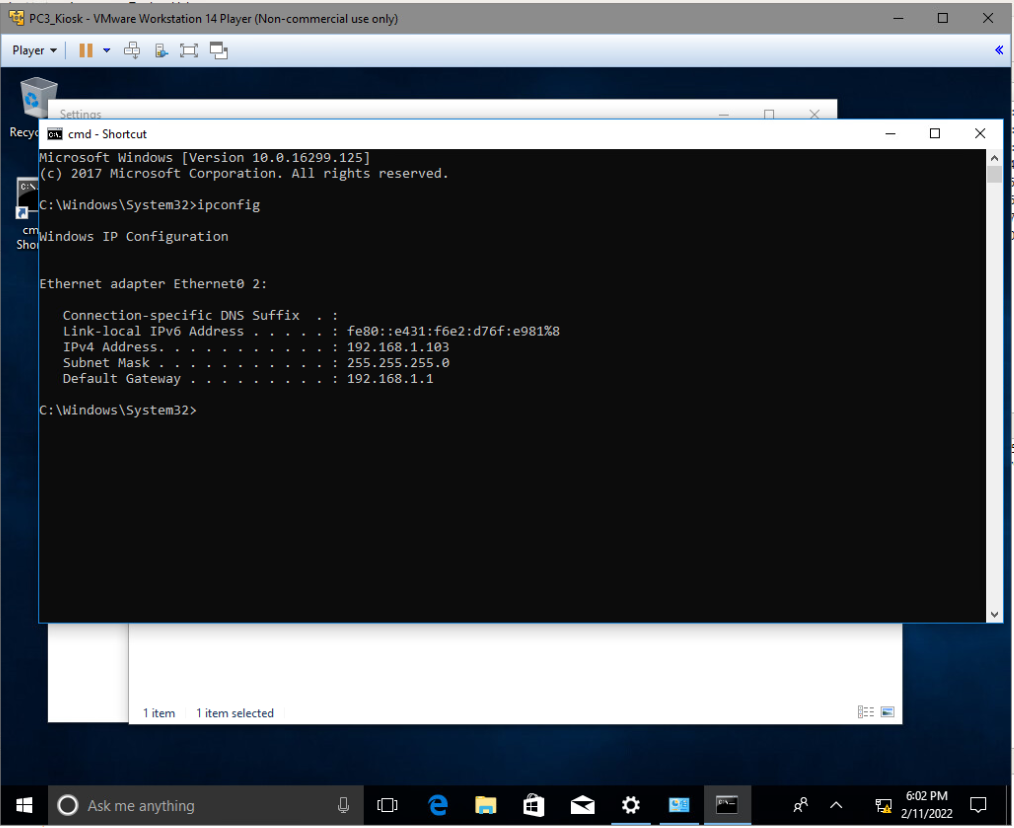
CYB 220 Project One

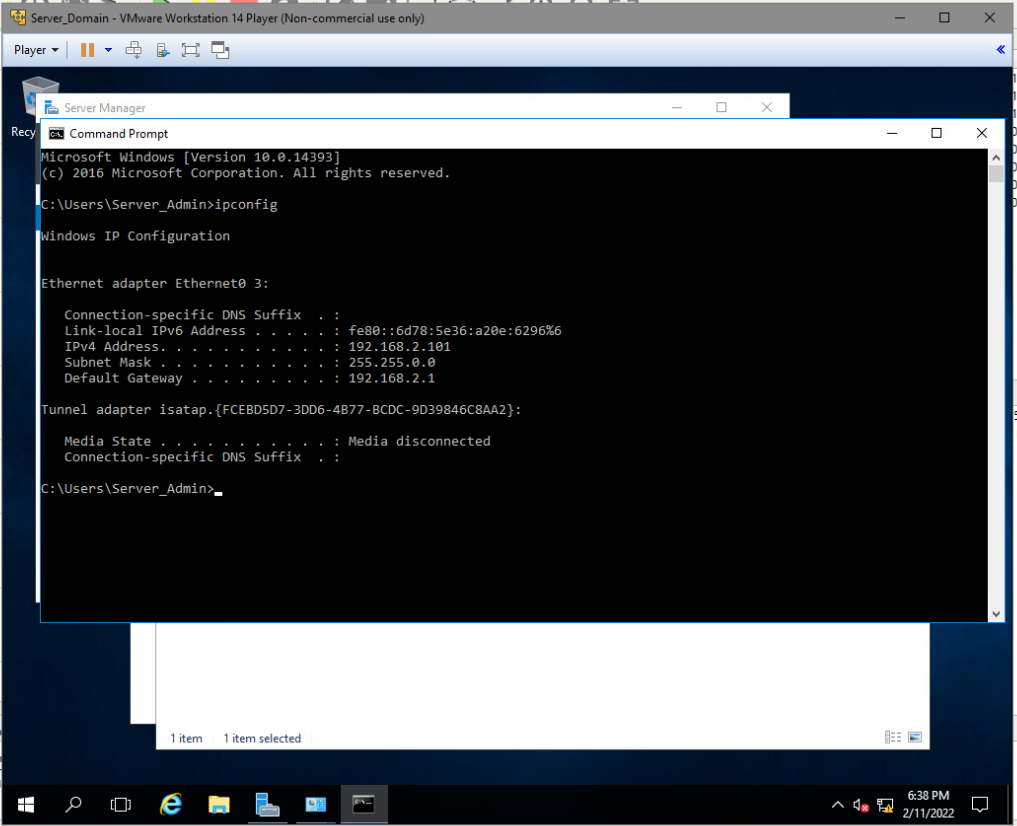
Douglas Few

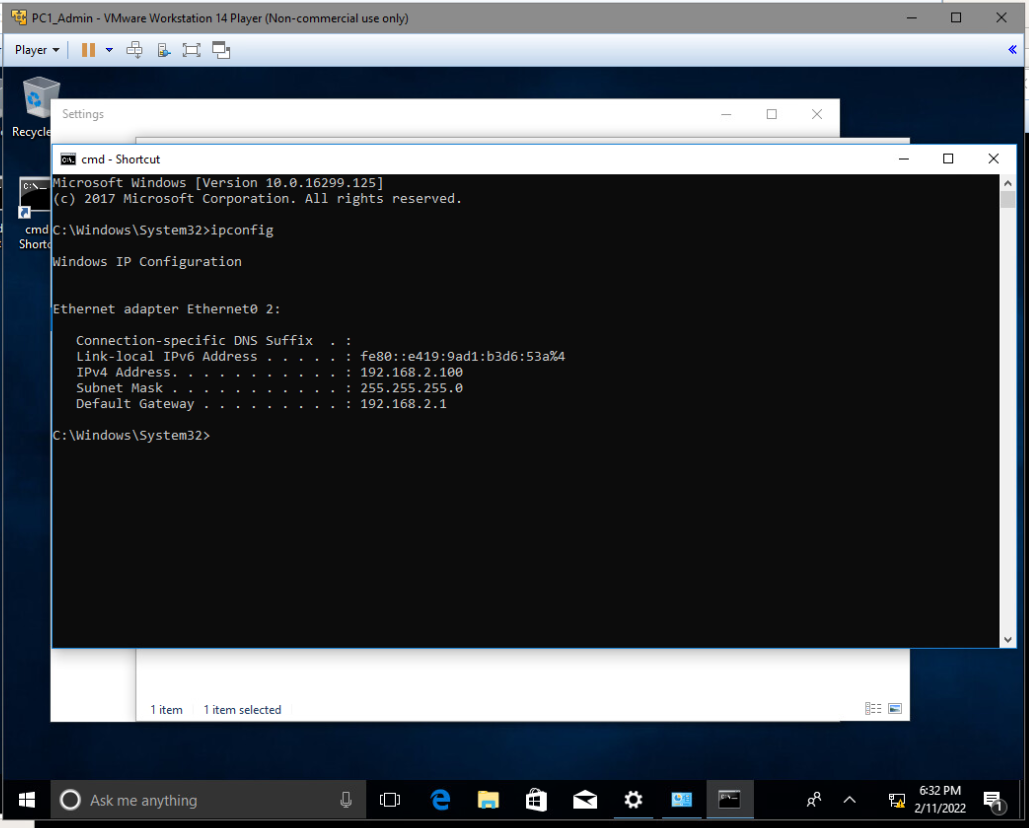
2/11/2022

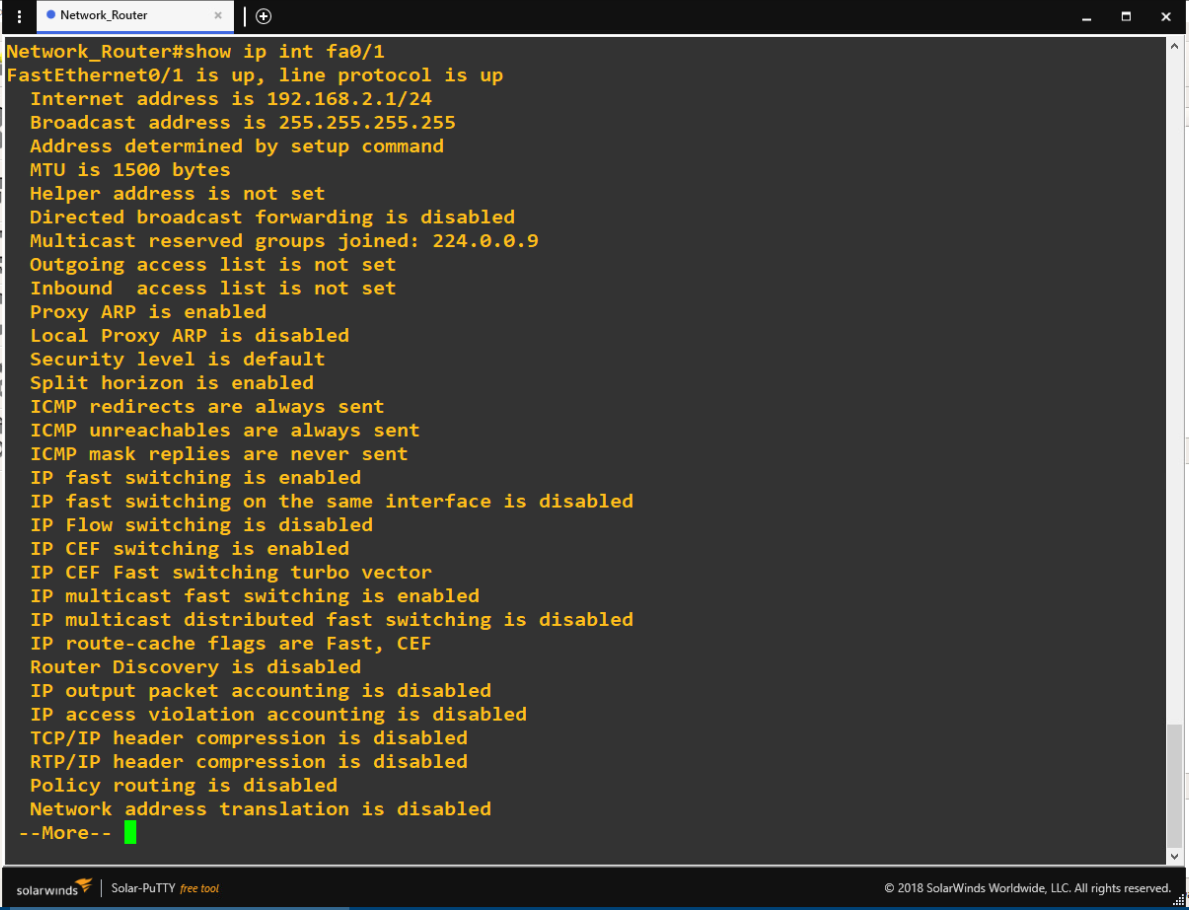
PC 1 KIOSK CONFIGURATION

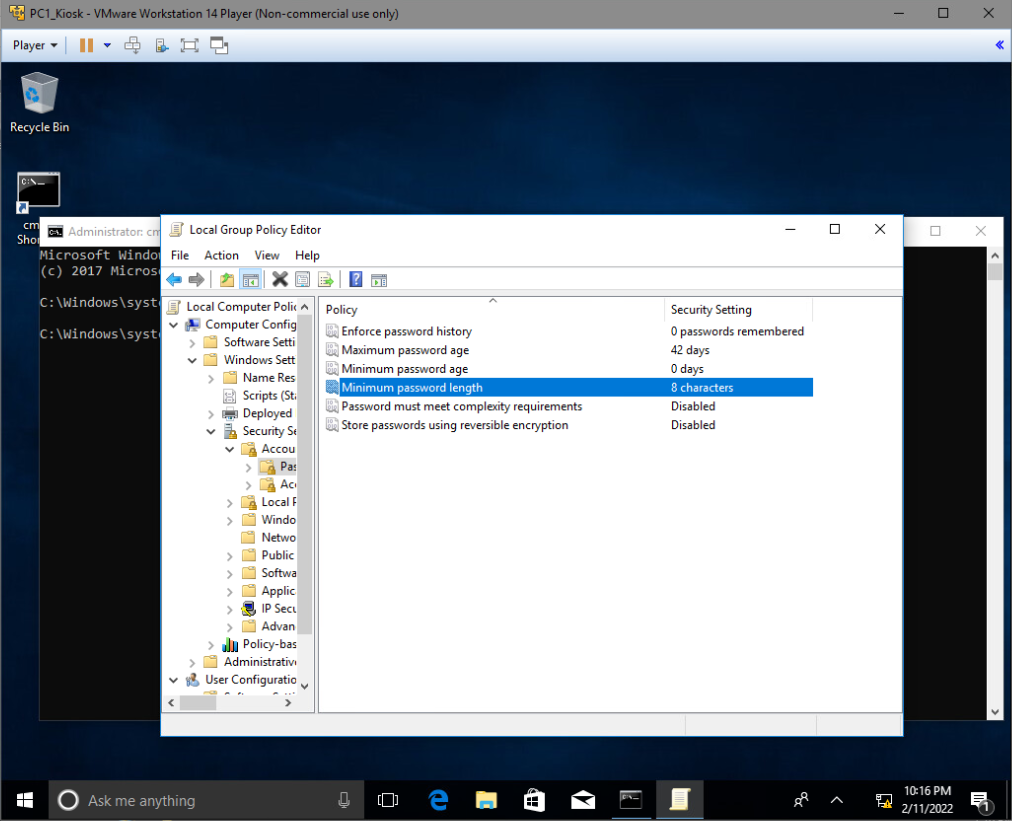
PC 2 KIOSK CONFIGURATION

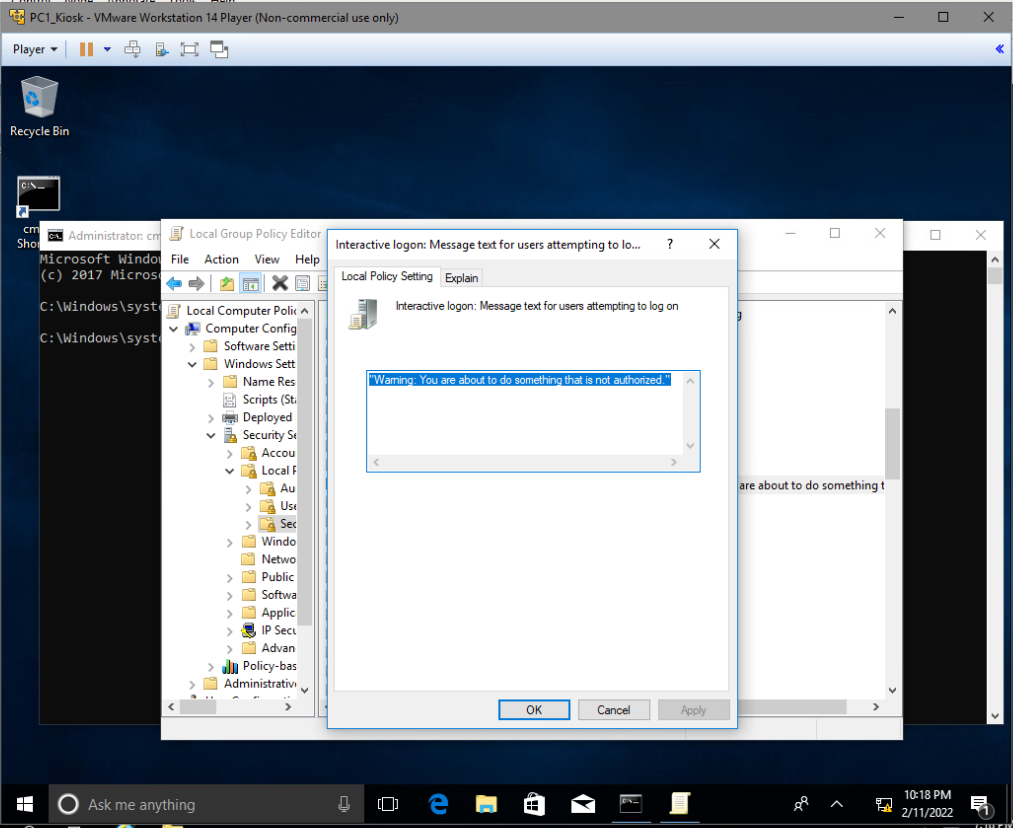
PC 3 KIOSK CONFIGURATION

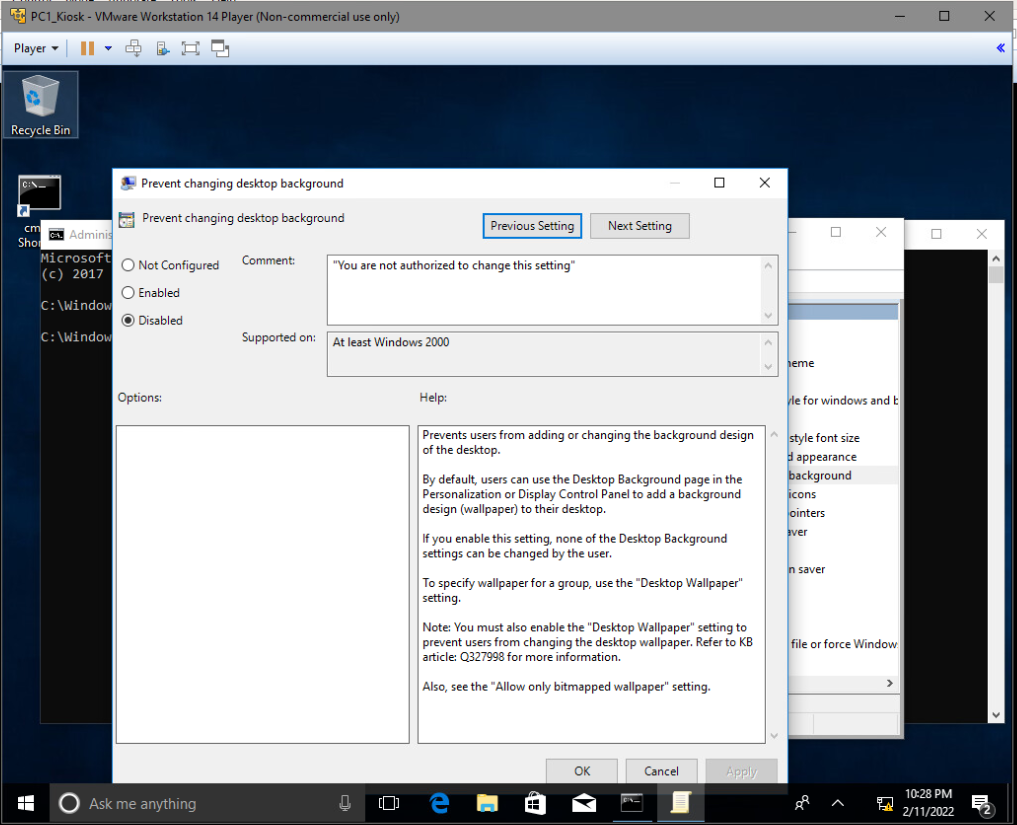
SERVER CONFIGURATION

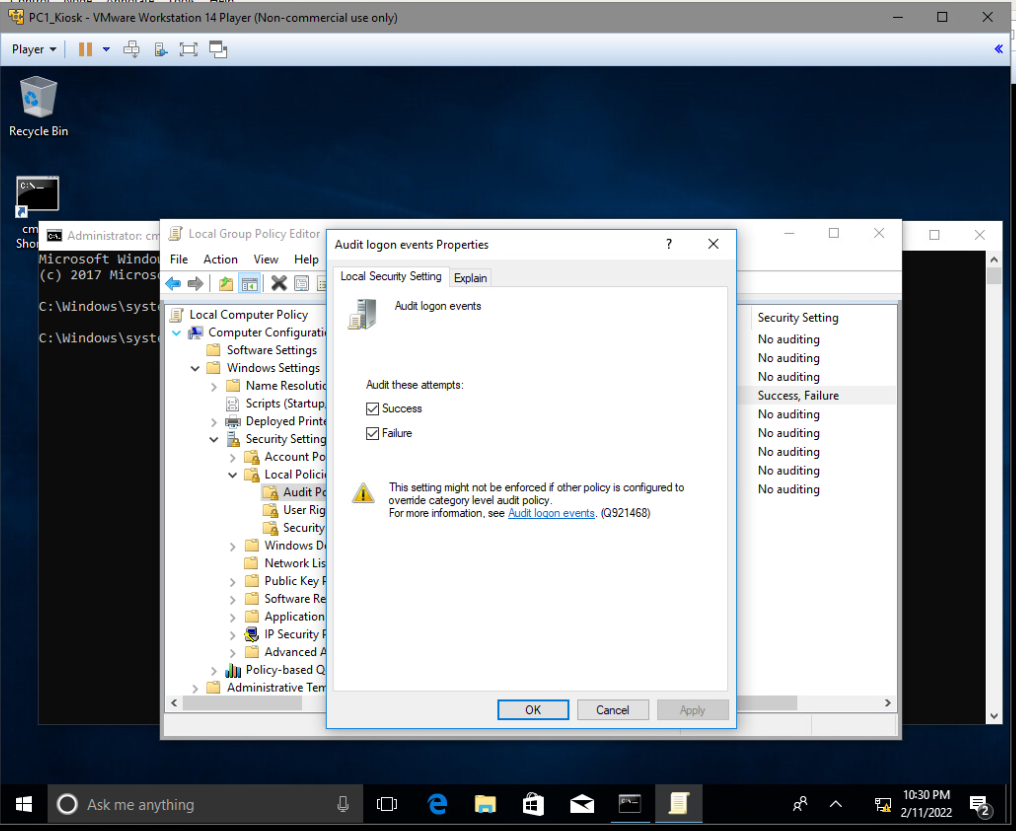
PC 1 ADMIN CONFIGURATION

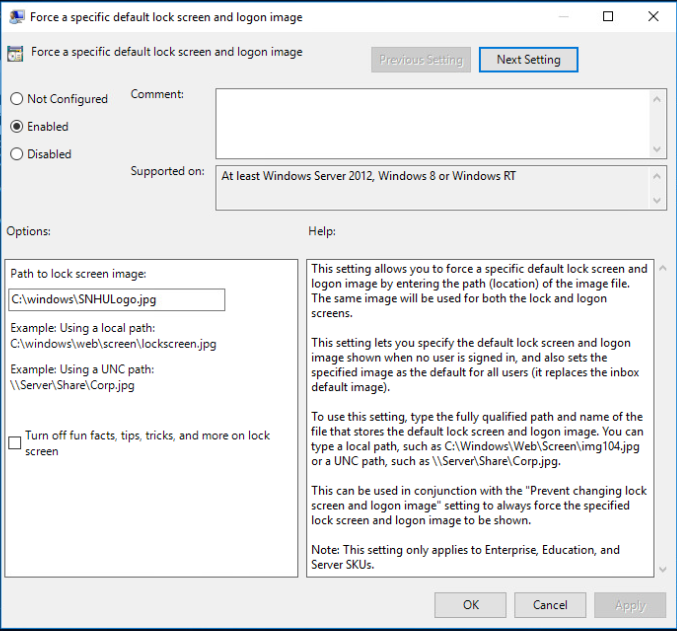
ROUTER CONFIGURATION

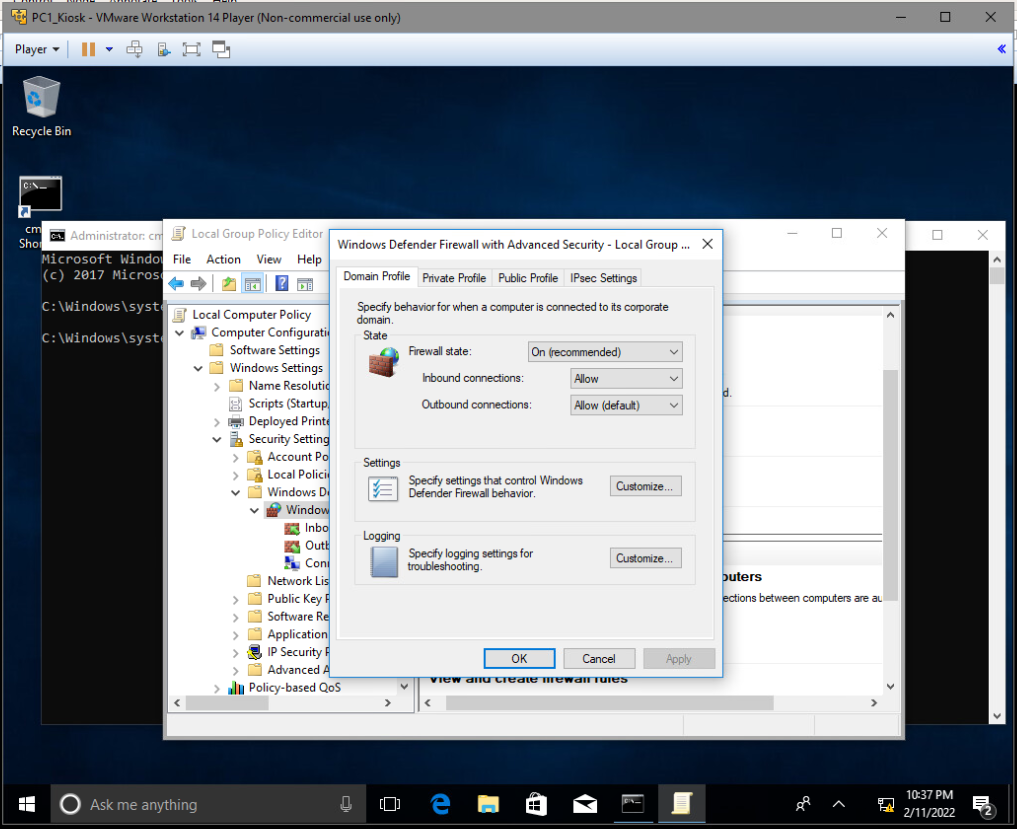
MINIMUM PASSWORD REQUIREMENT

LOGON ATTEMPT MESSAGE

DESKTOP BACKGROUND

AUDIT LOGON EVENTS

SET LOGON SCREEN

FIREWALL

Benefits

One major benefit of using virtualization technology in sandboxing is the fact that sandboxes allow for configuration of devices with no risk to physical hardware. Users can configure an entire network within the sandbox to test and verify that everything works before putting the work into the real network. This level of verification may seem to waste time when dealing with only a small number of nodes on a network, but can save a great deal of time and resources when implemented for a network of hundreds of computers.

Another benefit is the ability to run programs inside of an environment with little to no repercussions. For example, if a user were to come across a suspicious or questionable file, they might open that file in a virtualized sandbox in order to view its reaction before opening it on actual hardware (TechAdvisory, 2017). This allows for the possibility to not only detect potential malware, but also study and observe it.

Drawbacks

A drawback one might find with a virtualized sandbox is that not all malware is susceptible to it. Many advanced malware has been engineered to recognize when it has been released into a sandbox, and will not deploy if it recognizes it successfully (Lastline, 2018). Therefore, the sandbox will likely mistake the malware for a safe piece of software which will later be deployed onto a real, physical machine. An alternative would be to operate with an emulation instead of a virtualization-based sandbox. Emulators are much more difficult and expensive to develop compared to virtualization, but they are built to replicate a real operating system almost exactly. It is for this reason that emulators are more effective when it comes to detecting malicious software than a standard virtualized environment.

Situation

A popular method of virtualization that is used by many of the largest tech companies is cloud storage (Baca, 2021). Using cloud storage, companies utilize software to store data in a virtualized storage space instead of using physical storage disks. With the data being stored on the virtualized cloud, it allows for users to pull the data onto a physical device from anywhere where they are able to be connected.

References

Baca, S. (2021, November 19). *Virtualization for newbies: Five types of virtualization*. Worldwide IT Training. Retrieved February 12, 2022, from https://www.globalknowledge.com/us-en/resources/resource-library/articles/virtualization-for-newbies-five-types-of-virtualization/

Lastline. (2018, January 12). *Virtualization-based sandboxes are vulnerable to advanced malware*. Lastline. Retrieved February 11, 2022, from https://www.lastline.com/blog/virtualization-based-sandboxes/

TechAdvisory. (2017, April 28). *What is virtual "sandboxing"?* TechAdvisory.org. Retrieved February 11, 2022, from https://www.techadvisory.org/2017/04/what-is-virtual-sandboxing/