**Virtual Systems and Networking Concepts**

**Group Policy Changes**

**Change Windows User Account Control (UAC) prompt**

Graphical user interface, text, application, email

Description automatically generated

**Change local password policy setting**

Graphical user interface, text, application, email

Description automatically generated

**Change desktop background user rights assignment**

Graphical user interface, text, application, email

Description automatically generated

**Configure local audit policy setting**

Graphical user interface, text, application, email

Description automatically generated

**Configure default logon banner**

Graphical user interface, text, application, email

Description automatically generated

**Change default Windows firewall profile**

Graphical user interface, text, application

Description automatically generated

**Network Configuration Settings**

**PC1\_Kiosk**

Text

Description automatically generated

**PC2\_Kiosk**

Text

Description automatically generated

**PC3\_Kiosk**

A screenshot of a computer

Description automatically generated

**PC1\_Admin**

Text

Description automatically generated

**Network\_Router**

Text

Description automatically generated

**Server\_Domain**

Text

Description automatically generated

**The Reality of Using Virtualization in Sandboxing**

The use of virtualization technology for sandboxing can be very beneficial. It is known as cloud-based sandboxing. Sandboxing on its own, isolates a portion of the host's resources (Person, 2012). Adding a virtualization host will replicate the target host's whole system, not just the isolated portions. Scalability is one advantage of this technology. Virtualization removes the requirement for many devices. Therefore, more and more large companies are turning to cloud-based sandboxing. As a result, prices are reduced because less hardware is required. Sandboxing in this manner can also be more secure. Remote monitoring of virtualization sandboxing is possible (Person, 2012). This reduces the risk of an employee becoming vulnerable to threats when they leave the network because the network safeguards do not follow them.

Although cloud-based sandboxing is incredibly effective, it does have some disadvantages. One of reasons is that this technology is still very new and hasn't been widely implemented. They are exploited, as are all new security systems (Cobbler, 1019). Another issue is the testing of software updates. When utilizing the virtual machine, everything may operate smoothly, but when running directly on the host computer, the opposite may occur.

Virtualization is typically employed in the form of a remote desktop in addition to sandboxing. This enables authorized workers to access computers from locations where they are not physically present. This is useful for managing other devices and allowing IT staff to work on each employee's PC without having to physically visit them. This is extremely useful when you have folks working outside of the office who require assistance. When employing this technique, rigorous password rules are required. The host is vulnerable to brute-force attacks because it can be accessed remotely. Weak login credentials put the network at danger of being hacked.

References

Person. (2012, October 2). The Pros And Cons Of Application Sandboxing.

Retrieved from <https://www.darkreading.com/risk/the-pros-and-cons-of-application-sandboxing>

Cobbler, K. (2019, February 25). What is Sandboxing? How Does Cloud Sandbox Software Work?

Retrieved from https://www.avast.com/business/resources/what-is-sandboxing#pc