Desmond Hughes

Purdue University Global

IT278 Windows Administration

Eva White

August 7, 2022

Part 1: The problem is a hacker has breached the company’s network and is now can access the employee’s classified information, their usernames, passwords, phone numbers, emails, address, and etc. The hacker gain access from vulnerable leaks in the security, and finding the access tokens, which can give the hacker control of personal details. Now the company wants to become stricter and find a way to cover the vulnerable spots so that hackers and other malicious activity.

A way the company can ensure that their data and network is secure is to make sure that all of the devices connected to the network are adequately secured. The devices connected to eh network should always be update with its patches when they are available. Doing that will have the devices connected tot the network updated with new security threats and attacks. Also, when it comes to the devices make sure that all of the downloads are trusted and also secured.

One way the company can improve their security is by making their employee’s identity a central component, with it being one of their top concerns. The company would make users use authentication like encrypted technology to make sure that they are who they say they are, and so that third-party hackers will not be able to get into the company’s network as easy. Giving administrator the authority to control who can access the data. They can also limit the control of editing and accessing the company’s main way to access the employee directory, making it so that the administrator, and upper management only has access.

To me the best option is to use a network scanner. A way a company can is use a scanner to detect vulnerable spots in the security. For example, the company can use Acunetix, beSECURE, Frontline, and etc. Many companies benefit from using a scanner to test their vulnerability. Using this method will help get rid of the weaknesses in the network’s environment.

Part 2: Containers in Windows Server 2016 operating system are like Virtual Machines (VMs), they are environments that are isolated for applications. Containers shares the operating system so that it doesn’t interfere with the function of the system. Containers are also managed by PowerShell tools, which is used for building, testing, and solutions, and also managed by Dockers, which are an open-source containerization platform.

There are two types of Containers in Windows Server 2016. The two types are Windows Server Container, and Hyper-V Container. Windows Server Container uses process and namespace and shares a kernel with the operating system. Windows Server Container can also be known as process-isolated containers, and also affects the processes and how they run. Hyper-V Container doesn’t share a kernel with the Operating System, which means that they have their own storage network and memory, which also allows them to have the same security settings as VMs. Also, with Hyper-V Containers having their own kernel they can have different configurations that the operating system.

References

Upadhyhay, I. (2020). Top 20 Network Scanning Tools-Network and IP scanner. Retrieved 8 August 2022, from https://www.jigsawacademy.com/blogs/cyber-security/network-scanning-tools/

"Windows Containers in Windows Server 2016: Definition, Installation & Configuration." *Study.com*, 11 July 2019, study.com/academy/lesson/windows-containers-in-windows-server-2016-definition-installation-configuration.html