

CYSE 280 - Windows Systems Management and Security

Professor Malik A. Gladden

Homework 3

Short Answer Questions (short answers should generally be at least three to four sentences in length. However, it is important to be as concise as possible when responding.) or you may choose to **Upload a Two-Minute Audio or Video recording** to answer the following questions.

Module 1 & 2

1. What are the main characteristics of a network operating system?

A Network Operating System is like a coordinator for computer networks. It helps computers in the network share files securely and manages who gets access. It uses tools to keep things safe, like a virtual lock and key and makes sure communication between devices is smooth. It also organizes tasks like printing and spreading out work among different computers. Essentially, it's a system that makes sure everything works well and stays safe in a group of connected computers.

2. Compare DHCP with APIPA. What are the benefits of having both protocols available within a network?

Dynamic Host Configuration Protocol (DHCP) and Automatic Private IP Addressing (APIPA) are like helpers for devices in a network. DHCP makes things easy by automatically giving devices their own addresses and setup details. APIPA steps in if a device can't get an address from DHCP, giving it a backup address for local communication. Having both is helpful because it makes setting up the network simple, ensures things keep working even if one part has an issue, and manages addresses well in both big and small networks. It's like having a plan B to keep everything running smoothly.

3. What are the main differences between a PowerShell variable and a constant?

In PowerShell, variables and constants are like containers for holding information, but they work a bit differently. A variable is like a flexible box that can hold different types of info, and you can change what's inside during a script. You create a variable by using the \$ symbol followed by a name, allowing for updates as needed. On the other hand, a constant is also a container, but once you put something in it, it stays the same throughout the script. Constants are handy when you want to make sure a value doesn't change accidentally. So, variables are like changeable boxes, and constants are like boxes that stay the same once you put something in.

4. Compare the System File Checker tool to the File Signature Verification tool (Sigverif). What are the benefits of having both of these tools available within PowerShell?

The System File Checker (SFC) tool and the File Signature Verification tool (Sigverif) are like security guards for your computer, but they do slightly different jobs. SFC looks at important system files and makes sure they're not messed up. If it finds any issues, it fixes them to keep your computer running smoothly. Sigverif, on the other hand, checks the digital signatures of files, especially those related to drivers and important system parts. It ensures these files are genuine and haven't been tampered with. Having both tools is like having extra layers of security. They work together to make sure your computer files are in good shape and haven't been messed with by anything harmful. And if you use PowerShell, you can automate these checks to happen regularly, making your computer even more secure and reliable.

Listen to “Episode #53: Shadow Brokers” of the DarkNet Diaries podcast which can be found at <https://darknetdiaries.com/episode/53/Links to an external site.>

Based on the podcast, answer the following questions.

5. The Shadow Brokers are believed to be affiliated with which country, and what do we know about their origins and allegiances? The identity and exact affiliation of The Shadow Brokers remain unclear, but there have been speculations and attributions suggesting links to Russia. However, these attributions are not definitively proven. The origins and allegiances of The Shadow Brokers remain shrouded in mystery, and there is no conclusive evidence to pinpoint their country of origin or the exact nature of their connections.
6. The Shadow Brokers declared their allegiance to which President of the United States, and what implications did this decision have? They didn't explicitly pledge loyalty to any U.S. president. In a post, they mentioned Donald Trump when he was President-elect, but their motives are unclear. Some think they aim to disrupt U.S. intelligence, and others think they just wanted money, but their connection to politics doesn't necessarily indicate formal support.
7. Once the Shadow Brokers group stole NSA hacking tools, what did they attempt to do with stolen tools, and should we have questions about the security of government networks and the safety of confidential data?

They tried to sell the tools, which made people wonder why they did it. Maybe for money or to expose spy agencies. The auction didn't go far, but it got people talking about how safe government networks are and if our confidential info is at risk. This event showed that even advanced cyber tools can end up in the wrong hands. It reminds us that we need to keep improving how we defend against online threats and protect sensitive data from misuse.

Due January 25, 2024