Jasmyn Wilhelm 12 September 2024

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?

Computers and other devices are connected to a network so they can share resources through software called a network operating system. Among its core responsibilities are setting and managing resources, restricting access to resources, establishing communication, diagnosing the network, and creating and maintaining user accounts. The two types of networks are client/server and peer-to-peer. Among the advantages are high stability, security, simplicity in updating, and remote access.

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

Networks of any size can benefit from DHCP since it provides centralized control over IP address distribution, lease terms, and setup parameters. DHCP offers flexibility and management features that APIPA lacks, hence it is meant to be a temporary solution for small networks or isolated devices. When a DHCP server is not accessible, APIPA is helpful in short-term network configurations, peer-to-peer networks, and compact home networks.

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

A variable in PowerShell is a value that can be modified at any time. A constant is a value that cannot be modified once it's set. Constants are used for data that must remain constant, and variables are used when the data may change. If you attempt to modify a constant, an error will occur.

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?

Windows PowerShell has two essential tools to maintain system security and integrity: the System File Checker (SFC) and the File Signature Verification (Sigverif). SFC uses digital signatures to confirm the authenticity of files, and Sigverif uses scans to recover corrupted files. It is simple for administrators to use PowerShell to combine these technologies, which offers increased security against manipulation and unauthorized changes.

Jasmyn Wilhelm 12 September 2024

Listen to "Episode #53: Shadow Brokers" of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/53/

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 Shadow Brokers are believed to have some connection to Russia, but this is speculation. The first time the Shadow Brokers appeared was in 2016, leaking hacking tools allegedly stolen from the NSA. The timing of these 'dumps', lined up with high tensions between the U.S. and Russia, led to suspicions of Russia. It was speculated that Edward Snowden, who was residing in Russia at the time, might have played a role, but there is no evidence to support this. While there are assumptions, the true origins and allegiances of the Shadow Brokers remain unknown.

6) The Shadow Brokers declared their allegiance to which President of the United States, and what implications did this decision have?

The Shadow Brokers seem to have an allegiance to Donald Trump to some degree. The Shadow Brokers made a public post calling Joe Biden a "dirty grandpa", but said "goodbye" once Trump won the election. The group uploaded this information along with the post stating "The Shadow Brokers voted for you. The Shadow Brokers supports you. The Shadow Brokers is losing faith in you, Mr. Trump. It's appearing you are abandoning your base, the movement, and the peoples who getting you elected."

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?

After stealing NSA hacking tools, the Shadow Brokers attempted to auction them off to the highest bidder in exchange for Bitcoin. To show the 'authenticity' of their claim, they released one ZIP file as proof that these were classified NSA tools and documents. Additionally, they publicly announced that they would release all the files to the public if paid 1 million Bitcoin. This incident raises concerns about the security of government networks and the safety of confidential data, as it demonstrates vulnerabilities that could be exploited by malicious actors. Jake was targeted because of a tweet he made revealing his background and leading to changing his routine and travel.

Jasmyn Wilhelm 12 September 2024

Resources

Shadow brokers – darknet diaries. (n.d.). https://darknetdiaries.com/episode/53/