Module 1 & 2

And

Episode #53: Shadow Brokers

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 280 - Windows Systems Management and Security, Professor Malik A. Gladden

June 3, 2025

Assignment: Homework 3

Short Answer Questions: Short answers should typically be three to four sentences long. It is crucial to be concise while providing a thorough response. Alternatively, you have the option to upload a two-minute audio or video recording to answer the questions.

Module 1 & 2

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

A Network Operating System (NOS) manages network resources and enables communication between devices. It supports resource sharing—such as files, printers, hypervisors, virtual machines, and servers. It also provides security through authentication and encryption. NOS facilitates network management with tools for configuration and monitoring, ensuring scalability and interoperability. Examples include Windows Server and Linux-based systems.

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

DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses and network settings to devices to help simplify network management. APIPA (Automatic Private IP Addressing) assigns IP addresses (169.254.x.x) when DHCP fails, enabling local network communication without manual configuration. DHCP is ideal for large, managed networks, while APIPA ensures basic local network connectivity in small or failed DHCP scenarios.

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

In PowerShell, a variable stores data that can be changed during script execution, declared using $variable = value. A constant, created with *Set-Variable -Option* Constant, holds a fixed value that cannot be modified. Variables are flexible for dynamic scripting, while constants ensure critical values remain unchanged. This distinction enhances script reliability and flexibility.

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

System File Checker (SFC) scans and repairs corrupted Windows system files, ensuring proper versions and system integrity. File Signature Verification (Sigverif) checks the digital signatures of files to verify their authenticity. SFC is critical for fixing system errors, while Sigverif helps detect unauthorized file modifications and unsigned system and device driver files. Both tools in PowerShell enhance system security and stability by addressing different file integrity issues.

"Episode #53: Shadow Brokers" of the DarkNet Diaries podcast

https://darknetdiaries.com/transcript/53/

Based on the podcast, answer the following questions.

1. The Shadow Brokers are believed to be affiliated with which country, and what do we know about their origins and allegiances?

Authorities and those in the cybersecurity world believe the Shadow Brokers affiliate themselves with Russia, with speculation pointing to Russian intelligence or state-sponsored actors due to their sophisticated tactics and geopolitical motives. Their origins remain murky, emerging in 2016 with no clear identity, possibly as a front for a larger hacking group or government entity. They claimed no explicit allegiance to any nation but used broken English and cultural references to obscure their true affiliations (i.e., Twitter messages). Like leaking NSA tools to the public, their actions suggest an intent to disrupt U.S. cybersecurity dominance, aligning with Russian interests at the time.

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

The Shadow Brokers declared allegiance to President Donald Trump in early 2017, initially praising his leadership style in their communications. This move was likely strategic, aiming to sow confusion and chaos by aligning with a polarizing figure to amplify their impact. It raised questions about their motives, suggesting possible manipulation of U.S. political narratives or an attempt to curry favor with certain factions. The declaration complicated the perception of their leaks, blending cybercrime with political theater and intensified scrutiny of foreign influence in U.S. politics.

3. 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?

The Shadow Brokers stole advanced NSA hacking tools and initially attempted to auction them online to the highest bidder; however, they later leaked them publicly when the auction failed, exposing exploits such as EternalBlue. Their leaks enabled widespread cyberattacks, including WannaCry and NotPetya, resulting in significant global damage. This breach raises concerns about the security of government networks, as it revealed vulnerabilities in NSA's tool safeguarding. It also highlights risks to confidential data, as stolen tools could be weaponized by malicious actors, undermining trust in government cybersecurity. Lastly, concerns are further raised about NSA's offensive posture versus defensive posture because when they found vulnerabilities, they kept the information for themselves to use against enemies like other nation-states (i.e., espionage and surveillance of networks) instead of reporting those vulnerabilities to the software vendors for immediate fixing (i.e., Microsoft).