Module 3 & 4,

And

Episode # 69: Human Hacker

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

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

June 20, 2025

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 3 & 4

1. Discuss the differences between physical switches and virtual switches.

Physical switches are hardware devices that operate at Layer 2 or 3 by connecting physical machines and network devices through Ethernet cables. Physical switches require physical space and additional/external power sources. However, Virtual switches are software-based, utilizing host resources, making them less resource-intensive and cost-effective. Virtual machines operate within virtualization platforms (i.e., hypervisor) to connect and manage traffic between virtual machines and the physical network. While physical switches offer reliable Layer 2 or 3 connectivity, virtual switches provide greater flexibility and advanced features in virtual environments, such as the use of VLANs and Trunking to divide up the broadcast domain, tagging, and traffic filtering.

2. Compare a production checkpoint to a standard checkpoint. What are the benefits of one over the other, and what are the situations where each would be used?

Checkpoints are considered “snapshots” of a system or network. A standard checkpoint uses Hyper-V to capture the VM's full state, including memory, device status, and running applications. A production checkpoint creates a clean backup using internal services to ensure data consistency and integrity. They are less resource intensive, using either Volume Shadow Copy for Windows guest OSs or the File System Freeze (fsfreeze) service for Linux guest OSs. Production checkpoints are more suitable for live, critical systems needing restoration, while standard checkpoints are useful for quick rollbacks in development and test environments. Production checkpoints usually take longer to ensure data integrity, while standard checkpoints are faster but risk data loss.

3. Why should an administrator spread Flexible Single Master Operations (FSMO) roles within a forest and domains amongst different domain controllers?

Distributing FSMO roles among different domain controllers increases fault tolerance and prevents performance bottlenecks. If one controller fails, the impact is limited to fewer roles rather than the entire domain's operations; the other controllers can handle critical operations, such as schema updates or domain naming. It also helps balance the workload across the domain and forest functions, improving overall efficiency and resilience while minimizing downtime across the network.

4. What are the advantages and disadvantages of using a read-only domain controller (RODC)?

An RODC increases security by storing a read-only copy of Active Directory, reducing the risk of compromise in untrusted locations. It requires fewer resources, prevents unauthorized changes, and limits credential exposure, reducing replication traffic and supporting local authentication. However, it can't make changes or handle writable operation requests, and some services relying on write access may not function properly.

Listen to "Episode #69: Human Hacker of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/69Links to an external site.
Based on the podcast, answer the following questions.

1. Describe what happened during the first Bank break in Jamaica and what did they hack?

Two American hackers breached a major Jamaican bank by exploiting weak employee credentials to gain access to the internal network. They gained access to critical systems, including ATM and bank payment controls, which enabled them to issue fraudulent cash transactions. It was highly coordinated and involved both physical and digital intrusion methods, utilizing sensitive financial data and disrupting operations.

2. Explain three of the five key strategies that the client could have implemented to prevent the first Bank in Jamaica from being hacked.

First, the bank could have implemented proper network segmentation to isolate critical systems and limit the hackers' ability to move laterally within the network system. Second, stronger employee training on social engineering tactics, such as phishing, would have reduced insider risks and vulnerabilities. Third, deploying endpoint detection and response tools could have helped detect and stop unusual activity early. Lastly, implementing multi-factor authentication (MFA) could have blocked unauthorized access using stolen credentials.

3. Give an overview of what transpired when the human hackers pretending to be a pest control worker.

The hackers disguised themselves as pest control workers to gain physical access to a company. They first scoped out the location and attempted to leave USBs with malicious software near the inside entrances of the building, and the security team later caught them. However, after the hackers were caught and revealed themselves to the security team, they questioned the security team's evening schedule and protocol. They later returned that same evening to hack their client's business network.

Once inside, they connected to the internal network using USBs to extract sensitive data remotely. Also, they used other devices to hack into the security cameras. They stole physical access control items (i.e., identification badges) to gain entry into other buildings associated with the client's company. Thus, the physical breach underscores the vulnerability of companies to well-executed social engineering tactics, which exploit trust in vendor roles, highlighting the need for stricter access controls.