Backing Up and Restoring System Files Lab

Ryan Coon

CYB-515

Dr. Edward Marchewka

October 9, 2024

Part 1:

Part 2:

Describe how you perform backups and restore data to the system from a backup.

For backups, I rely on a combination of techniques. I use **incremental backups** to capture only changes since the last full backup, saving time and storage space. I also employ **differential backups**, which capture all changes since the last full backup, offering a faster restore process.

For data restoration, I use the backup software's restore functionality. I can choose to restore the entire system, specific files or folders, or even individual files. The process involves selecting the backup image and specifying the target location for the restored data.

Provide a summary of what you were accomplishing when you completed the backup and tested whether it was functioning correctly.

I just finished creating a comprehensive backup of your system's critical data. This backup includes all essential files, configurations, and system settings, ensuring a complete snapshot of your current state. To verify the backup's integrity, I performed a test restore of a few crucial files. This confirmed that the backup process was successful and the data can be reliably restored if needed.

Explain why performing backups and having the ability to restore files is an essential skill for cybersecurity professionals.

Backups and restoration are crucial for cybersecurity professionals because they provide a safety net against data loss caused by malicious attacks or system failures. By having a reliable backup, professionals can quickly recover critical data and systems after a breach, minimizing downtime and potential financial losses. This ability to restore data helps ensure business continuity and protects sensitive information from falling into the wrong hands.