Lab 5 – Explore Security Options

Brandon Trinkle

Arizona State University

IFT 380

Professor Shaun Usman

February 24, 2025

Lab 5 – Explore Security Options

1. What unsafe setting would you have to set to be able to finish creating the policy, and why?
   1. The unsafe setting is allowing BitLocker without pre-boot authentication. For example, enabling auto-lock without a pin or password. This makes the system vulnerable because an attacker with physical access could boot the machine without authentication.
2. There are two reasons why it would not matter -- what are they?
   1. The client must have the BitLocker Management feature enabled. We do not have that feature enabled.
   2. BitLocker requires Group Policy settings from Active Directory to apply encryption successfully.
3. A computer screen with a computer screen

   AI-generated content may be incorrect.
   1. 1. Attack Surface Reduction (ASR)
      1. Protects against fileless malware attacks, which are often used in phishing campaigns.
   2. 2. Controlled Folder Access
      1. Prevents unauthorized applications from modifying critical folders.
   3. 3. Exploit Protection
      1. Mitigates memory corruption vulnerabilities that are exploited in zero-day attacks.
   4. 4. Network Protection
      1. Blocks outbound connections to malicious domains and IP addresses.

A screenshot of a computer

AI-generated content may be incorrect.

1. Why does the Application Guard policy that was configured not work in the lab environment?
   1. We are running windows server. This can only work on windows 10 and 11 environments.