12- Implementing Host Security Solutions

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

12.1- Implement Endpoint Security

Labs

Lab 19: Implementing Endpoint Protection

HARDENING

- The process of putting an operating system or application in a secure configuration is called hardening.
- When hardening a system, it is important to keep in mind its intended use, because hardening a system can also restrict the system's access and capabilities.
- The need for hardening must be balanced against the access requirements and usability in a particular situation.

PATCH MANAGEMENT

- No operating system or software application is wholly free from vulnerabilities.
- As soon as a vulnerability is identified, vendors will try to correct it.
- At the same time, attackers will try to exploit it.
- Automated vulnerability scanners can be effective at discovering missing patches for the operating system, plus a wide range of third-party software apps and devices.
- Scanning is only useful if effective procedures are in-place to apply the missing patches, however.

PATCH MANAGEMENT (cont.)

- On residential and small networks, hosts will be configured to auto-update, meaning that they check for and install patches automatically.
- The major OS and applications software products are well-supported in terms of vendor-supplied fixes for security issues.
- There can also be performance and management issues when multiple applications run update clients on the same host.
- For example, as well as the OS updater, there is likely to be a security software update, browser updater, Java updater, OEM driver updater, and so on.
- These issues can be mitigated by deploying an enterprise patch management suite.
- Some suites, such as Microsoft's System Center Configuration Manager (SCCM).

ENDPOINT PROTECTION

- Antivirus (A-V)/Anti-Malware
  - ✓ The first generation of antivirus (A-V) software is characterized by signature-based detection and prevention of known viruses.
  - ✓ An "A-V" product will now perform generalized malware detection, meaning not just viruses and worms, but also Trojans, spyware, PUPs, cryptojackers, and so on.
  - ✓ While A-V software remains important, signature-based detection is widely recognized as being insufficient for the prevention of data breaches.

ENDPOINT PROTECTION

- Host-Based Intrusion Detection/Prevention (HIDS/HIPS)
  - ✓ Host-based intrusion detection systems (HIDS) provide threat detection via log and file system monitoring.
  - ✓ HIDS come in many different forms with different capabilities, some of them preventative (HIPS).
  - ✓ File system integrity monitoring uses signatures to detect whether a managed file image—such as an OS system file, driver, or application executable—has changed.
  - ✓ Products may also monitor ports and network interfaces, and process data and logs generated by specific applications, such as HTTP or FTP.

ENDPOINT PROTECTION

- Endpoint Protection Platform (EPP)
  - ✓ Endpoint protection usually depends on an agent running on the local host.
  - ✓ If multiple security products install multiple agents (say one for A-V, one for HIDS, another for host-based firewall, and so on), they can impact system performance and cause conflicts, creating numerous technical support incidents and security incident false positives.
  - ✓ An endpoint protection platform (EPP) is a single agent performing multiple security tasks, including malware/intrusion detection and prevention, but also other security features, such as a host firewall, web content filtering/secure search and browsing, and file/message encryption.

ENDPOINT PROTECTION

- Data Loss Prevention (DLP)
  - ✓ Many EPPs include a data loss prevention (DLP) agent.
  - ✓ This is configured with policies to identify privileged files and strings that should be kept private or confidential, such as credit card numbers.
  - ✓ The agent enforces the policy to prevent data from being copied or attached to a message without authorization.

Lab

Lab 19: Implementing Endpoint Protection