* Vulnerability Management:
  + Programs that play a crucial role in identifying, prioritizing, and remediating vulnerabilities in our environments.
  + They use vulnerability scanning to detect new vulnerabilities as they arise and then implement a remediation workflow that addresses the highest-priority vulnerabilities.
  + All organizations should incorporate this.
* Identifying Scan Targets:
  + Once an organization device that it wishes to conduct vulnerability scanning and determines which, if any, regulatory requirements apply to their scans, they move on to the more detailed phases of the planning process.
  + They need to identify the systems that will be covered by the vulnerability scans.
    - Some organizations choose to cover all systems, while others scan different systems in different ways.
  + When choosing a scan target, they must ask:
    - What is the data classification of the information stored, processed, or transmitted by the system?
    - Is the system exposed to the Internet or other public or semipublic networks?
    - What services are offered by the system?
    - Is the system a production, test, or development system?
  + Automated techniques exist to identify the systems that may be covered by a scan.
    - Tools can search the network for connected systems, which may have been known or unknown, to build an **asset inventory**.
    - Tools like Qualys can help build asset maps to visually see how systems are connected.
      * Based on the info gathered from these tools, administrators may give more information on specific systems, and it can be determined which systems are critical.
        + **Asset criticality** information helps guide questions on the types of scans that are performed, and how often and how much priority should be put on them.
* Determining Scan Frequency:
  + Tools like Nessus were the first vulnerability scanners on the market and has a feature to schedule how often scans should take place – if its weekly, daily, monthly, the date and time it starts, and so on.
    - These tools can alert administrators when a new vulnerability is detected, and even produce automated email reports of scan results.
  + Many factors influence how often an organization decides to conduct vulnerability scans against its systems:
    - The organization’s **risk appetite** is its willingness to tolerate risk within the environment. If an organization is extremely risk averse, it may choose to conduct scans more frequently to minimize the amount of time between when a vulnerability comes into existence and when it is detected by a scan.
    - **Regulatory requirement** such as those imposed by the **Payment Card Industry Data Security standard (PCI DSS)** or the **Federal Information Security Management Act (FISMA)** may dictate a minimum frequency for vulnerability scans. These requirements may also come from corporate policies.
    - **Technical Constraints** may limit the frequency of scanning.
      * For example, the scanning system may only be capable of performing a certain number of scans per day.
    - **Business Constraints** may limit the organization from conducting resource-intensive vulnerability scans during periods of high business activity to avoid disruptions of critical processes.
    - **Licensing Limitations** may curtail the bandwidth consumed by the scanner or the number of scans that may be conducted simultaneously.
* Configuring Vulnerability Scans:
  + Vulnerability management solutions provide administrators with the ability to configure many different parameter related scans.
    - This includes the types of checks performed by the scanner, provide credentials to access target servers, install scanning agents on target servers, and conduct scans from a variety of network perspectives.
    - Configuration Reviews are important to conduct regularly to ensure scan settings match current requirements.