- Filename: eccouncil-ceh31250-v12-5-5-1-vulnerability-assessment-models-and-tools.md
- Show Name: CEHv12 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - Vulnerability Analysis
- Episode Name: Vulnerability Assessment Models and Tools
  ==

Vulnerability Assessment Models and Tools

Objectives:

- Define and describe the philosophical and tactical difference between VA solution models
- Describe the attributes of an effective VA solution
- List and define the common types of Vulnerability Assessment tools
- Identify the criteria for choosing a Vulnerability Assessment tool
- Recognize industry standard VA tools

- What types of Vulnerability Assessment Models do we need to be aware of?
  - Product-Based Methods
    - Install the VA software locally/internally
      - Won't be able to give you an 'outside-in' assessment
  - Service-Based Methods
    - 3rd-party runs scans
      - Both inside and outside assessments
        - Opens visibility into air-gapped systems
- What types of Vulnerability Assessments **strategies** do we need to be aware of?
  - Tree-based
    - Multiple scans are run
      - Scans are customized to the host/service/database
  - Inference-based
    - Scanner starts broad and utilizes discovered info to infer the next step
      - Find host
        - Discover protocols
          - Enumerate open ports
            - Enumerate service
              - Employ known vulns against service
- What Vulnerability Assessment tools types do we need to be aware of?
  - Host-based
  - Depth assessment
    - Discovers new vulnerabilities
      - Fuzzers
  - Application-layer
    - Web app assessment
    - Database assessment
  - Mobile Assessment Tools
  - Location and Data Examination Tools
    - Network-based

    - oddly enough is only able to scan the host it's installed on
- Agent-based
    - Scans the local host or can scan other hosts on the network
- Proxy scanner
    - Can scan the network from any machine on the network
- Cluster scanner
    - Same as proxy, but can scan multiple machines at one time