- Filename: eccouncil-ceh31250-v11-5-1-1-vulnerability-assessment-concepts-and-resources.md
- Show Name: CEHv11 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - Vulnerability Analysis
- Episode Name: Vulnerability Assessment Concepts and Resources
  ==========

Vulnerability Assessment Concepts and Resources

Objectives:

- Define vulnerability research and explain its usefulness in the VA process
- List common resources used when conducting vulnerability research
- Define and explain the concepts and practices of Vulnerability Assessments
- Explain the concept and application of vulnerability databases and scoring systems

---

- What is a Vulnerability Assessment?
    - Looking at a system to discover security weaknesses
        - Helps get ahead of potential breaches
            - Test new security controls and their effectiveness
- How do Vulnerability Assessors / Ethical Hackers stay current with contemporary vulnerabilities and exploits?
    - Vulnerability Research
        - Threat Feeds
        - Discovered Security Flaws
        - Professional Development
- How is a VA done?
    - Active and Passive scanning
        - Software
            - Nessus
            - OpenVAS
- Tell us about Vulnerability Metrics and Databases?
    - Common Vulnerability Scoring System (CVSS)
        - Multiple versions
            - 2.0, 3.0, 3.1
                - https://www.first.org/cvss/v3.0/specification-document
                - 3.0 Specs
                    - None 0.0
                    - Low 0.1 - 3.9
                    - Med 4.0 - 6.9
                    - High 7.0 - 8.9
                    - Crit 9.0 - 10.0
    - Common Vulnerabilities and Exposures (CVEs)
        - https://cve.mitre.org/
        - Details about discovered vulnerabilities

- National Vulnerability Database (NVD)
  - https://nvd.nist.gov/
  - US Gov run/maintained
- Common Weakness Enumeration (CWE)
  - https://cwe.mitre.org/