- Filename: eccouncil-ceh31250-v10-5-2-1-vulnerability_analysis_tools.md
- Show Name: CEHv10 (312-50)
- Topic Name: Information Gathering and Vulnerability Identification
- Episode Name: Vulnerability Analysis Tools
- Description: In this episode, Daniel and Zach demonstrate and discuss a few tools you may use to perform a vulnerability assessment. Here they will walk you through the different types of assessment tools and then take you through some of the options and output from tools like Nikto, MBSA, and OpenVAS. Finally, they cover vulnerability assessment attributes and references like the CVSS, CCVE, and NVD.

==========

Vulnerability Analysis Tools

- **When it comes to vulnerability assessments, are they all just the same with a different wrapper, or are there different types?**
    - Product-based solutions
        - Installed on the client's internal network
        - Sometimes doesn't detect external attacks
    - Service-based solutions
        - Can be hosted internally and/or externally
    - Tree-based assessments
        - Scans are tailored towards what's being scanned by information given from the administrator
            - Web service
            - OS type
            - Database
    - Inference-based assessments
        - Scans are tailored based on discovered protocols
            - Only scans for vulns relevant to that fingerprint
- **So are there different types of ASSESSMENT TOOLS as well?**
    - Host-based
        - Check OS for vulns
    - Depth
        - Finds zero-day bugs
        - Fuzzer
    - Application-Layer
        - Web apps, software apps, databases
    - Active
        - Actively probes for information
        - Consumes resources
    - Passive
    - Scope tools
        - Covers the range of the scoped engagement
            - Scans both OS and Apps
- **Now that we understand the different types of tools, can you show us some specific examples of tools we may see or use?**

    - GFI LanGuard
        - Show screenshots from website
    - Qualsys Freescan
    - Nikto
        - `nikto -h http://10.0.0.175 -root /bWAPP -id bee:bug -Tuning x -C all -output scan1`
    - WPScan
    - Nessus
        - Has mobile scanner too
    - OpenVAS
        - DEMO
    - MBSA
    - Net Scan
        - Mobile scanner
- **Can you walk us through the scan report results and explain some of what we're seeing there?**
    - Common Vulnerability and Exposures (CVE)
    - Common Vulnerability Scoring System (CVSS)
        - DIAGRAMS
    - National Vulnerability Database (NVD)