- Filename: eccouncil-ceh31250-v10-5-1-1-vulnerability_analysis_concepts.md
- Show Name: CEHv10 (312-50)
- Topic Name: Information Gathering and Vulnerability Identification
- Episode Name: Vulnerability Analysis Concepts
- Description: In this episode, Daniel and Zach explore concepts that pertain to performing a Vulnerability Assessment. Here they will discuss the difference between a vulnerability scan and a penetration test as well as take you through the Vulnerability Management Life-Cycle which defines the steps taken during the Pre-assessment, Assessment, and Post-Assessment phases.

==========

Vulnerability Analysis Concepts

- **What is a vulnerability assessment and how does it differ from a Penetration test?**
    - Only looks to discover vulns
        - Categorize them
            - OS vuln
            - Configuration issues
            - Patch management
            - App vuln
        - Prioritize mitigation
    - Pentests attempt to exploit vulns
- **What types of vulnerability assessments should we be aware of?**
    - External
    - Internal
    - Web App/Application
    - Network/Wireless
- **How do we begin preparing for a Vulnerability Assessment?**
    - We have to understand the Vulnerability Management life cycle
        - DIAGRAM
            - Baselines/Pre-assessment
                - Learn the client's business
                    - What kind of business are they?
                    - How do they operate?
                    - What security controls are in place already?
                - Scope
                    - Define what apps, devices, services, data are in scope
                - Scheduling
                    - When can you perform assessment?
- **Now that we have the pre-assessment phase squared away, what can we expect in the actual assessment phase?**
    - Depends on what controls, processes, apps, services, etc that are in scope
        - Scan for known vulnerabilities in...
            - Apps/Web Apps
            - OS
        - Scan for misconfigurations
        - Physical site security

- Once you have those results...
    - Prioritize vulns
    - Contextualize to stakeholders how vulns could impact their business
        - In a way they will understand
            - Written and/or Verbal reports
                - Validation may be required

- **Now that we've performed our vulnerability assessment and we have all these vulnerabilities, how do we handle that information?**
    - Perform post-assessment activities
        - Engage in Risk Assessment
            - Determine threat, risk, and impact levels
        - Remediate
            - Prioritize
            - Develop mitigation strategy
            - Perform mitigations
            - After action report
            - Develop processes/procedures/training to prevent future risk
        - Verification
            - Check to see that mitigations are effective
        - Monitoring
            - IDS/IPS
            - Ensure processes/procedures/policies/controls are being adhered to