COURSE: SECURITY+ SY0-401

MODULE 3: THREATS AND VULNERABILITIES

Part B
Overview

• Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities

• Explain the proper use of penetration testing versus vulnerability scanning
Security Threats and Vulnerabilities

Tools and Techniques to Discover Security Threats and Vulnerabilities

• Assessment types
  • Risk
  • Threat
  • Vulnerability

• Assessment technique
  • Baseline reporting
  • Code review
  • Determine attack surface
  • Review architecture
  • Review designs
Security Threats and Vulnerabilities

Tools and Techniques to Discover Security Threats and Vulnerabilities

- Risk calculations
  - Threat vs. likelihood

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>LIKELIHOOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
</tr>
<tr>
<td>3</td>
<td>Medium</td>
</tr>
<tr>
<td>4</td>
<td>Medium</td>
</tr>
<tr>
<td>5</td>
<td>High</td>
</tr>
</tbody>
</table>
Security Threats and Vulnerabilities

Tools and Techniques to Discover Security Threats and Vulnerabilities

- Interpret results of security assessment tools
- Tools
  - Protocol analyzer
  - Vulnerability scanner
  - Honeypots
  - Honeynets
  - Port scanner
  - Passive vs. active tools
  - Banner grabbing
Penetration Testing versus Vulnerability Scanning

Penetration testing
- Verify a threat exists
- Bypass security controls
- Actively test security controls
- Exploiting vulnerabilities
Penetration Testing versus Vulnerability Scanning

• Vulnerability scanning
  • Passively testing security controls
  • Identify vulnerability
  • Identify lack of security controls
  • Identify common misconfigurations
  • Intrusive vs. non-intrusive
  • Credentialed vs. non-credentialed
  • False positive
• Black box
• White box
• Gray box
Security Threats and Vulnerabilities

Demonstration

Penetration Testing

Vulnerability Scanning
THANK YOU