Course Competency | Learning Outcomes
---|---
**Competency 1:** The student will be able to demonstrate an understanding of web server hacking by:

1. Describing the components of a web server.
2. Listing popular web servers.
3. Describing web server authentication and access control features.
5. Identifying the vulnerabilities specific to IIS servers.
6. Defining patch management and patch management tools.
7. Demonstrating tools used to attack web servers.

**Competency 2:** The student will be able to demonstrate an understanding of web applications hacking by:

1. Describing the architecture of web applications, web services, and service-oriented architecture.
2. Describing web application technologies, including the HTTP protocol methods and codes, AJAX, XML, JSON, and various encoding schemes.
3. Describing web authentication techniques and protocols, including cookie-based authentication, token-based authentication, Oauth, OpenID, and SAML.
4. Describing web authorization techniques and protocols, including OAuth2 and SAML.
5. Explaining common web server threats, such as injections, broken authentication, data exposure, XML External Entity (XXE), cross-site scripting (XSS), Cross-Site Request Forgery (CSRF), and Cookie/session Poisoning.
7. Analyzing web applications to map the attack surface.
8. Using vulnerability assessment tools to identify web servers’ vulnerabilities.
9. Using fuzzy testing to identify coding errors and security loopholes in web applications.
10. Performing documentation review and source code review to identify vulnerabilities in the code that cannot be identified by the traditional scanning tools, including application logic flaws.
11. Describing recent attack threats.

**Competency 3:** The student will be able to demonstrate an understanding of SQL injections by:

1. Defining and explaining SQL injections.
2. Comparing various SQL injection types, including UNION SQL injections, Error-based SQL injections, blind and double-blind SQL injections.
3. Explaining how SQL injections can be used to bypass authentication.
4. Using SQL injection tools to find and exploit SQL injection vulnerabilities.
5. Using fuzzy testing to detect SQL injection vulnerabilities.
6. Using static and dynamic source code analysis to detect SQL injection vulnerabilities.
7. Using intrusion detection systems (IDS) evasion techniques to perform SQL injections that bypass IDS.

**Competency 4:** The student will be able to demonstrate an understanding of session hijacking by:

- Critical thinking
- Information Literacy
- Computer / Technology Usage
1. Describing session management and session hijacking.
2. Explaining how session hijacking can be used to bypass authentication.
3. Characterizing the application-level session hijacking attacks, including CSRF, session replay, man-in-the-browser, session fixation, proxy servers, and SSL/TLS-related attacks.
4. Explaining network-level session hijacking attacks such as TCP/IP hijacking, Blind hijacking, man-in-the-middle, and RST hijacking.
5. Performing sequence number prediction.
6. Listing the steps in conducting a session hijacking attack.
7. Using session hijacking tools.
8. Describing approaches to prevent session hijacking.

**Competency 5:** The student will be able to demonstrate an understanding of IDS, firewalls, and honeypots evasion by:

1. Describing the types of IDS and intrusion prevention systems (IPS).
2. Explaining the types of IDS evasion techniques.
3. Using tools to evade IDS.
4. Specify methods to detect IDS attacks.
5. Explaining strategies to defend against IDS evasion.
6. Comparing the types of firewalls.
7. Explaining methods to identify and bypass a firewall.
8. Describing honeypots and honeynets.
9. Explaining methods to detect and defeat honeypots.

**Competency 6:** The student will be able to demonstrate an understanding of wireless networks hacking by:

- Critical thinking
- Information Literacy
- Computer / Technology Usage

Updated Spring 2021
1. Defining and differentiating types of wireless technologies.
2. Listing the advantages and disadvantages of a wireless network.
4. Identifying wireless access points.
5. Listing wireless threats, including disassociation attacks, EAP-failure, beacon flood, rogue access point, evil twin, key reinstallation attack (KRACK), jamming, etc.
7. Describing Wired Equivalent Privacy (WEP) vulnerabilities.
8. Describing Wi-Fi Protected Access (WPA), and its vulnerabilities.
9. Describing Wi-Fi Protected Access 2 (WPA2), and its vulnerabilities.
10. Using tools to scan, sniff and attack wireless networks.
11. Listing countermeasures to wireless attacks.

**Course Competency 7:** The student will be able to demonstrate an understanding of mobile platforms hacking by:

1. Describing the types of handheld devices and their operating systems.
2. Describing mobile attack vectors and vulnerabilities, including jail-broken and rooted devices, .app sandboxing vulnerabilities, mobile spam, SMS phishing attacks, etc.
3. Describing methods used to hack handheld devices.
4. Describing mobile device management policies and solutions.
5. Using tools to defend handheld devices attacks.

**Course Competency 8:** The student will be able to demonstrate an understanding of Internet of Things (IoT) hacking by:

1. Defining and describing the IoT.
2. Explaining the IoT architecture and IoT communication models.
3. Listing IoT technologies and protocols.
4. Explaining the vulnerabilities associated with the IoT.
5. Describing the IoT attack surface.
6. Explaining various IoT threats, including rolling code attack, blueborne attacks, firmware exploits, and Sybil attack.
7. Using tools and devices to hack IoT devices.
8. Listing strategies and tools to defend against IoT attacks.

**Course Competency 9:** The student will be able to demonstrate an understanding of cloud computing hacking by:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Describing the characteristics of cloud computing, including on-demand self-service, rapid elasticity, resource pooling, and virtualization.</td>
</tr>
<tr>
<td>2.</td>
<td>Comparing various virtualization platforms.</td>
</tr>
<tr>
<td>3.</td>
<td>Comparing the types of cloud computing (IaaS, PaaS and SaaS).</td>
</tr>
<tr>
<td>4.</td>
<td>Explaining the separation of responsibilities in the cloud.</td>
</tr>
<tr>
<td>5.</td>
<td>Describing the cloud deployment models (public, private, community, hybrid).</td>
</tr>
<tr>
<td>7.</td>
<td>Understanding shared storage options.</td>
</tr>
<tr>
<td>8.</td>
<td>Listing and explaining cloud computing threats, including VM-level attacks, lock-in, loss of governance, loss of encryption keys.</td>
</tr>
<tr>
<td>9.</td>
<td>Describing cloud computing attacks.</td>
</tr>
<tr>
<td>10.</td>
<td>Describing cloud computing security considerations and the cloud security control layers.</td>
</tr>
<tr>
<td>11.</td>
<td>Using cloud security tools to test cloud-based systems.</td>
</tr>
</tbody>
</table>

**Course Competency 10:** The student will be able to demonstrate an understanding of cryptographic attacks by:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Distinguishing secret-key cryptography from public-key cryptography.</td>
</tr>
</tbody>
</table>

- Critical thinking
- Information Literacy
- Computer / Technology Usage

Updated Spring 2021
2. Explaining cryptographic hashing functions.
3. Describing the RSA algorithm.
4. Defining Secure Socket Layer (SSL) and identifying its uses.
5. Describing the Secure Shell (SSH) protocol.
6. Distinguishing types of cryptographic attacks.