STRANDS AND STANDARDS

CYBERSECURITY ETHICAL HACKING

Course Description
This course will immerse you into the Hacker Mindset so that you will be able to ethically defend against future attacks. The security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment. This course puts you in the driver’s seat of a hands-on environment with a systematic process. Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be taught the five phases of ethical hacking and the ways to secure and approach your target to succeed! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

<table>
<thead>
<tr>
<th>Intended Grade Level</th>
<th>10-12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Units of Credit</td>
<td>0.5</td>
</tr>
<tr>
<td>Core Code</td>
<td>35.01.00.00.036</td>
</tr>
<tr>
<td>Prerequisite</td>
<td>Digital Literacy</td>
</tr>
<tr>
<td>Test Weight</td>
<td>0.0</td>
</tr>
<tr>
<td>License Type</td>
<td>CTE and/or Secondary Education 6-12</td>
</tr>
<tr>
<td>Required Endorsement(s)</td>
<td>Security</td>
</tr>
<tr>
<td>Endorsement 2</td>
<td>Linux, Network+,</td>
</tr>
<tr>
<td>Endorsement 3</td>
<td>Computer Programming</td>
</tr>
</tbody>
</table>
STRAND 1

Understanding Security Layers.

Standard 1
Understand core security principles.
  • Understand the concepts of confidentiality, integrity, availability.
  • Understand how threat and risk impact principles; principle of least privilege; social engineering; and attack surface.

Standard 2
Understand physical security.
  • Understand site security, computer security, removable devices and drives, access control, mobile device security, disable Log On Locally, and keyloggers.

Standard 3
Understand internet security.
  • Understand browser settings, zones, and secure Web sites

Standard 4
Understand wireless security.
  • Understand advantages and disadvantages of specific security types; keys, SSID, and MAC filters.

STRAND 2

Understanding Operating System Security.

Standard 1
Understand user authentication.
  • Understand multifactor, smart cards, RADIUS, and Public Key Infrastructure (PKI).
  • Understand the certificate chain, biometrics, Kerberos, and time skew using Run As to preform administrative tasks and password reset procedures.

Standard 2
Understand permissions.
  • Understand the following: file; share; registry; Active Directory; NTFS vs. FAT; enabling or disabling inheritance; behavior when moving or copying files within the same disk or onto another disk; multiple groups with different permissions; basic permissions and advanced permissions; take ownership; and delegation.
Standard 3
Understand password policies.
- Understand the following: password complexity; account lockout; password length; password history; time between password changes; enforce by using group policies; and common attach methods.

Standard 4
Understand audit policies
- Understand the following: types of auditing; what can be audited; enabling auditing; what to audit for specific purposes; where to save audit information; and how to secure audit information.

Standard 5
Understand encryption
- Understand the following: EFS; how EFS-encrypted folders impact moving and copying files; BitLocker (ToGo); Trusted Platform Module (TPM); software-based encryption; MAIL encryption and signing and other uses; VPN; public key and private key; encryption algorithms; certificate properties; certificate services; PKI/certificate services infrastructure; and token devices.

Standard 6
Understand malware.
Understand the following: buffer overflow; worms; Trojans; and spyware.

STRAND 3
Understanding Network Security.

Standard 1
Understand dedicated firewalls.
- Understand the types of hardware firewalls and their characteristics.
- Understand when to use a hardware firewall instead of a software firewall and stateful vs. stateless inspection.

Standard 2
Understand Network Access Protection (NAP).
- Understand the purpose of NAP and the requirements for NAP.
Standard 3
Understand network isolation.
  • Understand the following: VLANs; routing, honeypot, DMZ, NAT, NAT, VPN, IPsec, and Server and Domain Isolation.

Standard 4
Understand protocol security.
  • Understand the following: protocol spoofing; IPsec; tunneling; DNSsec; network sniffing; and common attack methods.

STRAND 4
Understand Security Software.

Standard 1
Understand client protection.
  • Understand the following: anti-virus; User Account Control (UAC); keeping client operating system and software updated; encrypting offline folders; software restriction policies.

Standard 2
Understand e-mail protection.
  • Understand the following: anti-spam; anti-virus; spoofing; phishing and pharming; client vs. server protection; SPF records; and PTR records.

Standard 3
Understand server protection.
  • Understand the following: separation of services; hardening; keeping server updated; secure dynamic DNS updates; disabling unsecure authentication protocols; Read-Only Domain Controllers; separate management VLAN; Microsoft Baseline Security Analyzer (MBSA).

STRAND 5
Understand Security Careers and Ethics.

Standard 1
Understand client protection.
  • Understand the following: anti-virus; User Account Control (UAC); keeping client operating system and software updated; encrypting offline folders; software restriction policies.
Standard 2
Understand e-mail protection.
  • Understand the following: anti-spam; anti-virus; spoofing; phishing and pharming; client vs. server protection; SPF records; and PTR records.

Skill Certificate Test Points by Strand

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Test #</th>
<th>Number of Test Points by Standard</th>
<th>Total Points</th>
<th>Total Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Ethical Hacking</td>
<td>8##</td>
<td>10  9  6  3  12  0</td>
<td>56</td>
<td>40</td>
</tr>
<tr>
<td>Industry Exam</td>
<td>9##</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>