Quiz - First look at Penetration Testing and Digital Forensics

1. A skilled penetration tester wants to show her employer how smart she is in hopes of getting a promotion. Without obtaining permission, she hacks into the company's new online store to see if there are any weaknesses that can be hardened before the system goes live. She does not do any damage and writes a useful report which she sends over her boss's head to the CISO. What color hat was she wearing?   **1 / 1 point**

   ○ A White Hat

   ◉ A Gray Hat

   ○ A Black Hat

   ○ A Pink Hat

   ○ A Rainbow Hat

   > ✓ **Correct**
   > Correct! Her motivations were good, for the most part, but it is dangerous, a violation of the law and likely her company's computer security policies to access a system without permission. She may get promoted or she may get fired.

2. Which three (3) are resources that are available to help guide penetration testing efforts by cybersecurity specialists?   **1 / 1 po**

   ☐ General Data Protection Regulation (GDPR)

   ☑ NIST SP 800-42 Guidelines on Network Security Testing.

   > ✓ **Correct**
   > Partially correct! NIST is a great resource for pentesting and other cybersecurity issues.

   ☑ Open Source Security Testing Methodology Manual (OSSTMM).

   > ✓ **Correct**
   > Partially correct! As its name implies, this is a great resource.

   ☑ Information Systems Security Assessment Framework (ISSAF)

   > ✓ **Correct**
   > Partially correct! ISSAF is a great resource.

3. According to the Vulnerability Assessment Methodology, Potential Impacts are determined by which 2 factors?

   1 / 1 point

   ○ Identify Indicators and Exposure

   ◉ Exposure and Sensitivity

   ○ Sensitivity and Adaptive Capacity

   ○ Potential Impacts and Adaptive Capacity

> ✓ **Correct**
>
> Correct! Weigh potential exposure and the sensitivity of an event to determine its potential impact.

4. In digital forensics, the term Chain of Custody refers to what?

   1 / 1

   ○ This chain of custody is simply a written record of who possessed the evidence as it moves from collection to analysis to presentation in a court of law.

   ○ This is a physical chain that is place around a crime scene to protect the evidence from being disturbed.

   ◉ The record that documents the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.

   ○ This is a digital "chain" that isolated digital evidence from being disturbed until it can be analyzed by the police or other authorities.

> ✓ **Correct**
>
> Correct! This is a chain where each link represents the state of the evidence at any point in time.