Question 1
Fill in the blank: A vulnerability _____ refers to the internal review process of an organization's security systems. 1 / 1 point
patch
scoring
==assessment==
scanner
Correct
A vulnerability assessment is an internal review process of an organization's security systems.
Question 2
What are the goals of a vulnerability assessment? Select two answers. 1 / 1 point
To detect network traffic
==To identify existing weaknesses==
Correct
The goals of a vulnerability assessment are to identify existing weaknesses and reduce overall threat exposure.
==To reduce overall threat exposure==
Correct
The goals of a vulnerability assessment are to identify existing weaknesses and reduce overall threat exposure.
To audit regulatory compliance
Question 3
Which of the following remediation examples might be implemented after a vulnerability scan? Select two answers. 1 / 1 point
Locating vulnerabilities in workstations
==Training employees to follow new security procedures==
Correct
Examples of remediations that might be performed after a vulnerability scan include training employees on new procedures and installing software updates and patches.
==Installing software updates and patches==
Correct
Examples of remediations that might be performed after a vulnerability scan include training employees on new procedures and installing software updates and patches.
Identifying misconfigurations in an application

Question 4
What are two types of vulnerability scans? Select two answers. 1 / 1 point
==Authenticated or unauthenticated==
Correct
Authenticated or unauthenticated and limited or comprehensive are two types of vulnerability scans. Internal and external is another common type of vulnerability scanning.
Patch or upgrade
Risk or threat
==Limited or comprehensive==
Correct
Authenticated or unauthenticated and limited or comprehensive are two types of vulnerability scans. Internal and external is another common type of vulnerability scanning.