QUESTION 1
What is a difference between a threat and a risk?

A. A risk is a flaw or hole in security, and a threat is what is being used against that flaw.
B. A threat is a sum of risks, and a risk itself represents a specific danger toward the asset.
C. A risk is an intersection between threat and vulnerabilities, and a threat is what a security engineer is trying to protect against.
D. A threat can be people, property, or information, and risk is a probability by which these threats may bring harm to the business.

Correct Answer: C

QUESTION 2
Which attack method is being used when an attacker tries to compromise a network with an authentication system that uses only 4-digit numeric passwords and no username?

A. replay
B. SQL injection
C. dictionary
D. cross-site scripting

Correct Answer: C

QUESTION 3
Which option describes indicators of attack?
A. virus detection by the AV software
B. spam emails on an employee workstation
C. malware reinfection within a few minutes of removal
D. blocked phishing attempt on a company

Correct Answer: C

QUESTION 4
Why should an engineer use a full packet capture to investigate a security breach?

A. It reconstructs the event allowing the engineer to identify the root cause by seeing what took place during the breach.
B. It provides the full TCP streams for the engineer to follow the metadata to identify the incoming threat
C. It captures the TCP flags set within each packet for the engineer to focus on suspicious packets to identify malicious activity.
D. It collects metadata for the engineer to analyze, including IP traffic packet data that is sorted, parsed, and indexed.

Correct Answer: A

QUESTION 5
A SOC analyst detected connections to known C&C and port scanning activity to main HR database servers from one of the HR endpoints, via Cisco StealthWatch. What are the two next steps of the SOC team according to the NIST.SP800-61 incident handling process? (Choose two.)

A. Provide security awareness training to HR managers and employees.
B. Block connection to this C&C server on the perimeter next-generation firewall.
C. Isolate affected endpoints and take disk images for analysis.
D. Update antivirus signature databases on affected endpoints to block connections to C&C.
E. Detect the attack vector and analyze C&C connections.

Correct Answer: BC

QUESTION 6
What matches the regular expression c(rgr)+e?

A. crgrrgre
B. c(rgr)e
C. ce
D. crgr+e

Correct Answer: A

QUESTION 7
Which action matches the weaponization step of the Cyber Kill Chain model?

A. Construct the appropriate malware and deliver it to the victim.
B. Test and construct the appropriate malware to launch the attack.
C. Scan a host to find open ports and vulnerabilities.
D. Research data on a specific vulnerability.

Correct Answer: B

QUESTION 8
Which technique is a low-bandwidth attack?

A. phishing
B. social engineering
C. session hijacking
D. evasion

Correct Answer: D

QUESTION 10
According to CVSS, what is a description of the attack vector score?

A. It depends on how many physical and logical manipulations are possible on a vulnerable component.
B. The metric score will be larger when a remote attack is more likely.
C. The metric score will be larger when it is easier to physically touch or manipulate the vulnerable component.
D. It depends on how far away the attacker is located and the vulnerable component.

Correct Answer: B