312-38$^{Q\&As}$

Certified Network Defender (CND)

Pass EC-COUNCIL 312-38 Exam with 100% Guarantee

QUESTION 1

Which of the following honeypots provides an attacker access to the real operating system without any restriction and collects a vast amount of information about the attacker?

A. High-interaction honeypot

B. Medium-interaction honeypot

C. Honeyd

D. Low-interaction honeypot

Correct Answer: A

A high-interaction honeypot offers a vast amount of information about attackers. It provides an attacker access to the real operating system without any restriction. A high-interaction honeypot is a powerful weapon that provides opportunities to discover new tools, to identify new vulnerabilities in the operating system, and to learn how blackhats communicate with one another. Answer option D is incorrect. A low-interaction honeypot captures limited amounts of information that are mainly transactional data and some limited interactive information. Because of simple design and basic functionality, low-interaction honeypots are easy to install, deploy, maintain, and configure. A low-interaction honeypot detects unauthorized scans or unauthorized connection attempts. A low-interaction honeypot is like a one-way connection, as the honeypot provides services that are limited to listening ports. Its role is very passive and does not alter any traffic. It generates logs or alerts when incoming packets match their patterns. Answer option B is incorrect. A medium-interaction honeypot offers richer interaction capabilities than a low-interaction honeypot, but does not provide any real underlying operating system target. Installing and configuring a medium- interaction honeypot takes more time than a low-interaction honeypot. It is also more complicated to deploy and maintain as compared to a low-interaction honeypot. A medium-interaction honeypot captures a greater amount of information but comes with greater risk. Answer option C is incorrect. Honeyd is an example of a low-interaction honeypot.

QUESTION 2

Sophie has been working as a Windows network administrator at an MNC over the past 7 years. She wants to check whether SMB1 is enabled or disabled. Which of the following command allows Sophie to do so?

A. Get-WindowsOptionalFeatures -Online -FeatureNames SMB1Protocol

B. Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

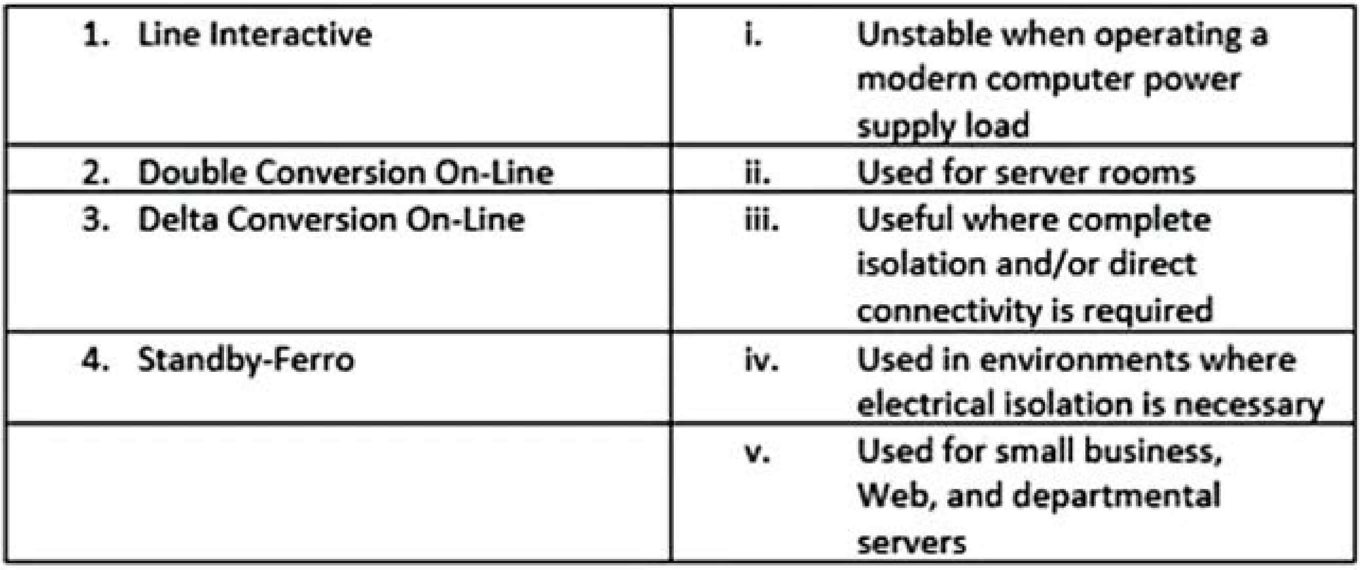
C. Get-WindowsOptionalFeature -Online -FeatureNames SMB1Protocol

D. Get-WindowsOptionalFeatures -Online -FeatureName SMB1Protocol

Correct Answer: B

QUESTION 3

Your company is planning to use an uninterruptible power supply (UPS) to avoid damage from power fluctuations. As a network administrator, you need to suggest an appropriate UPS solution suitable for specific resources or conditions. Match the type of UPS with the use and advantage:



1. Line Interactive	i.	Unstable when operating a modern computer power supply load
2. Double Conversion On-Line	ii.	Used for server rooms
3. Delta Conversion On-Line	iii.	Useful where complete isolation and/or direct connectivity is required
4. Standby-Ferro	iv.	Used in environments where electrical isolation is necessary
	v.	Used for small business, Web, and departmental servers

A. 1-i,2-iv,3-ii,4-v

B. 1-v,2-iii,3-i,4-ii

C. 1-ii,2-iv,3-iii,4-i

D. 1-iii,2-iv,3-v,4-iv

Correct Answer: C

QUESTION 4

Which of the following is a kind of security, which deals with the protection of false signals transmitted by the electrical system?

A. None

B. emanation Safety

C. hardware security

D. physical security

E. communications Security

Correct Answer: B

QUESTION 5

Which of the following types of information can be obtained through network sniffing? (Choose all that apply.)

A. DNS traffic

B. Telnet passwords

C. Programming errors

D. Syslog traffic

Correct Answer: ACD