DUMPSBOSS.

Logical Operations CyberSec First Responder

Logical Operations CFR-210

Version Demo

Total Demo Questions: 10

Total Premium Questions: 100

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

An outside organization has reported to the Chief Information Officer (CIO) of a company that it has received attack from a Linux system in the company's DMZ. Which of the following commands should an incident responder use to review a list of currently running programs on the potentially compromised system?

A. task manager

B. tlist

C. who

D. top

ANSWER: D

QUESTION NO: 2

A suspicious laptop is found in a datacenter. The laptop is on and processing data, although there is no application open on the screen. Which of the following BEST describes a Windows tool and technique that an investigator should use to analyze the laptop's RAM for working applications?

A. Net start and Network analysis

B. Regedit and Registry analysis

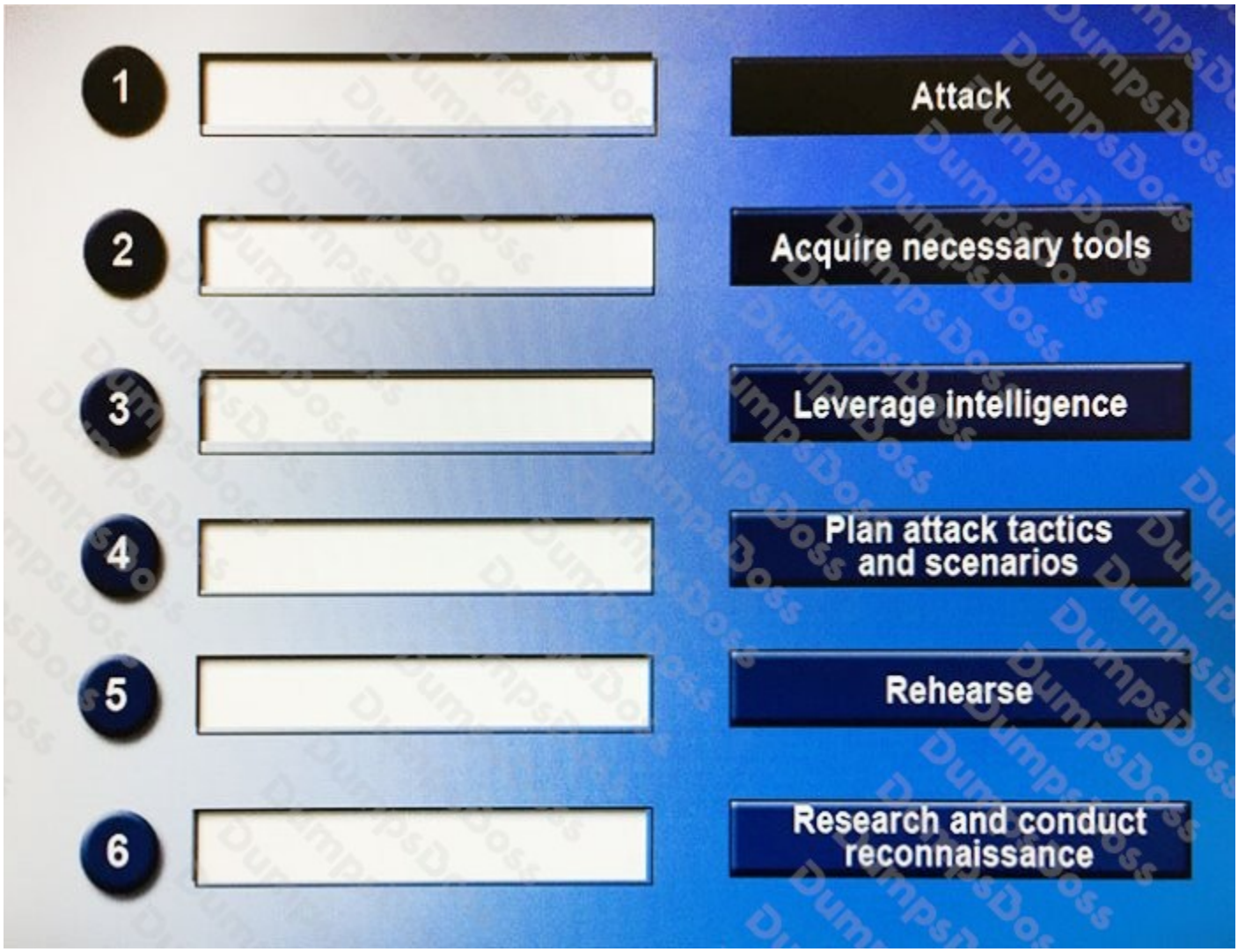
C. Task manager and Application analysis

D. Volatility and Memory analysis

ANSWER: B

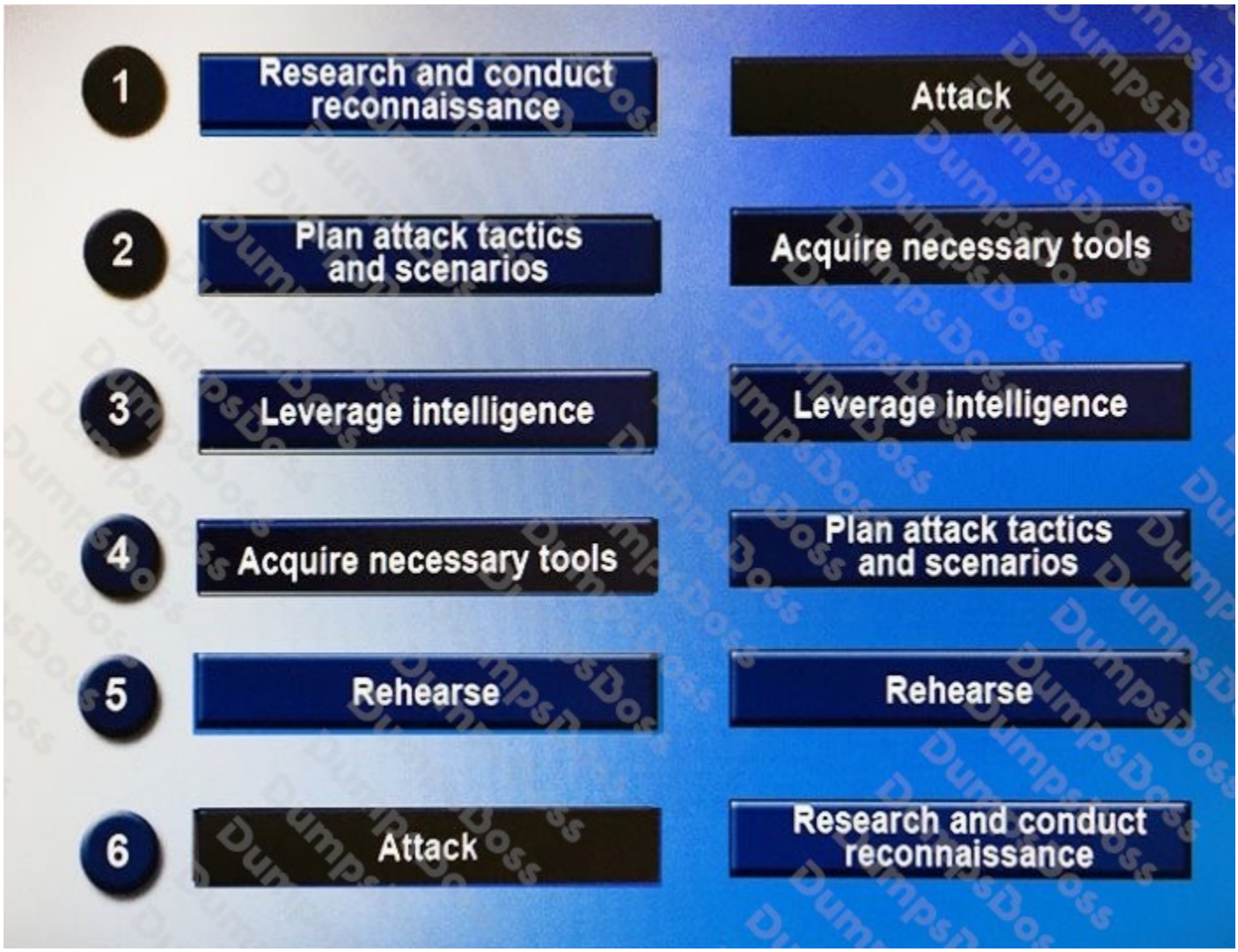
QUESTION NO: 3 - (DRAG DROP)

Drag and drop the following steps to perform a successful social engineering attack in the correct order, from first (1) to last (6).


1
2
3
4
5
6
Attack
Acquire necessary tools
Leverage intelligence
Plan attack tactics and scenarios
Rehearse
Research and conduct reconnaissance

ANSWER:

Explanation:



QUESTION NO: 4

A user reports a pop-up error when starting a Windows machine. The error states that the machine has been infected with a virus and instructs the user to download a new antivirus client. In which of the following locations should the incidentresponder check to find what is generating the error message? (Choose two.)

A. Auto-start registry keys

B. Device Manager

C. Event Viewer

D. Programs and Features

E. Browser history

ANSWER: A C

QUESTION NO: 5

During a network-based attack, which of the following data sources will provide the BEST data to quickly determine the attacker's point of origin? (Choose two.)

A. DNS logs

B. System logs

C. WIPS logs

D. Firewall logs

E. IDS/IPS logs

ANSWER: A D

QUESTION NO: 6

An incident responder notices many entries in an apache access log file that contain semicolons. Which of the following attacks is MOST likely being attempted?

A. SQL injection

B. Remote file inclusion

C. Account brute force

D. Cross-site scripting

ANSWER: A

QUESTION NO: 7

An administrator wants to block Java exploits that were not detected by the organization's antivirus product. Which of the following mitigation methods should an incident responder perform? (Choose two.)

A. Utilize DNS filtering

B. Send binary to AV vendor for analysis

C. Create a custom IPS signature

D. Implement an ACL

E. Block the port on the firewall

ANSWER: C E

QUESTION NO: 8

An alert has been triggered identifying a new application running on a Windows server. Which of the following tools can be used to identify the application? (Choose two.)

A. traceroute

B. nbstat

C. Hex editor

D. Task manager

E. Process explorer

ANSWER: D E

QUESTION NO: 9

Which of the following describes the MOST important reason for capturing post-attack metadata?

A. To assist in updating the Business Continuity Plan

B. To assist in writing a security magazine article

C. To assist in fortification of defenses to prevent future attacks

D. To assist in improving security awareness training

ANSWER: C

QUESTION NO: 10

Which of the following is the BEST way to capture all network traffic between hosts on a segmented network?

A. HIPS

B. Firewall

C. Router

D. Protocol analyzer

ANSWER: A