Latest Version: 6

Question: 1

An attacker performs reconnaissance on a Chief Executive Officer (CEO) using publicity available resources to gain access to the CEO's office. The attacker was in the CEO's office for less than five minutes, and the attack left no traces in any logs, nor was there any readily identifiable cause for the exploit. The attacker in then able to use numerous credentials belonging to the CEO to conduct a variety of further attacks. Which of the following types of exploit is described?

A. Pivoting
B. Malicious linking
C. Whaling
D. Keylogging

Answer: C

Question: 2

Which of the following is an automated password cracking technique that uses a combination of upper and lower case letters, 0-9 numbers, and special characters?

A. Dictionary attack
B. Password guessing
C. Brute force attack
D. Rainbow tables

Answer: C

Question: 3

A zero-day vulnerability is discovered on a company's network. The security analyst conducts a log review, schedules an immediate vulnerability scan, and quarantines the infected system, but cannot determine the root cause of the vulnerability. Which of the following is a source of information that can be used to identify the cause of the vulnerability?

A. www.virustotal.com
B. Security RSS feeds
C. Security software websites
D. Government websites

Answer: C

Question: 4

The Chief Information Officer (CIO) of a company asks the incident responder to update the risk management plan. Which of the following methods can BEST help the incident responder identify the risks that require in-depth analysis?

A. Qualitative analysis
B. Targeted risk analysis
C. Non-targeted risk analysis
D. Quantitative analysis

Answer: D

Question: 5

A security analyst for a financial services firm is monitoring blogs and reads about a zero-day vulnerability being exploited by a little-known group of hackers. The analyst wishes to independently validate and corroborate the blog's posting. Whichof the following sources of information will provide the MOST credible supporting threat intelligence in this situation?

A. Similar cybersecurity blogs
B. Threat intelligence sharing groups
C. Computer emergency response team press release
D. Internet searches on zero-day exploits

Answer: C

Question: 6

Which of the following could an attacker use to perpetrate a social engineering attack? (Choose two.)

A. Keylogger
B. Yagi
C. Company uniform
D. Blackdoor
E. Phone call

Answer: A,E

Question: 7

During review of a company's web server logs, the following items are discovered:
2015-03-01 03:32:11 www.example.com/index.asp?id=-999 or 1=convert(int,@@version)—
2015-03-01 03:35:33 www.example.com/index.asp?id=-999 or 1=convert(int,db_name())—
2015-03-01 03:38:25 www.example.com/index.asp?id=-999 or 1=convert(int,user_name())—
Which of the following is depicted in the log example above?

A. An administrator using the web interface for application maintenance
B. Normal web application traffic
C. A web application scan
D. An attempt at enumeration via SQL injection

Answer: D

Question: 8

An attacker has exfiltrated the SAM file from a Windows workstation. Which of the following attacks is MOST likely being perpetrated?

A. user enumeration
B. Brute forcing
C. Password sniffing
D. Hijacking/rooting

Answer: C

Question: 9

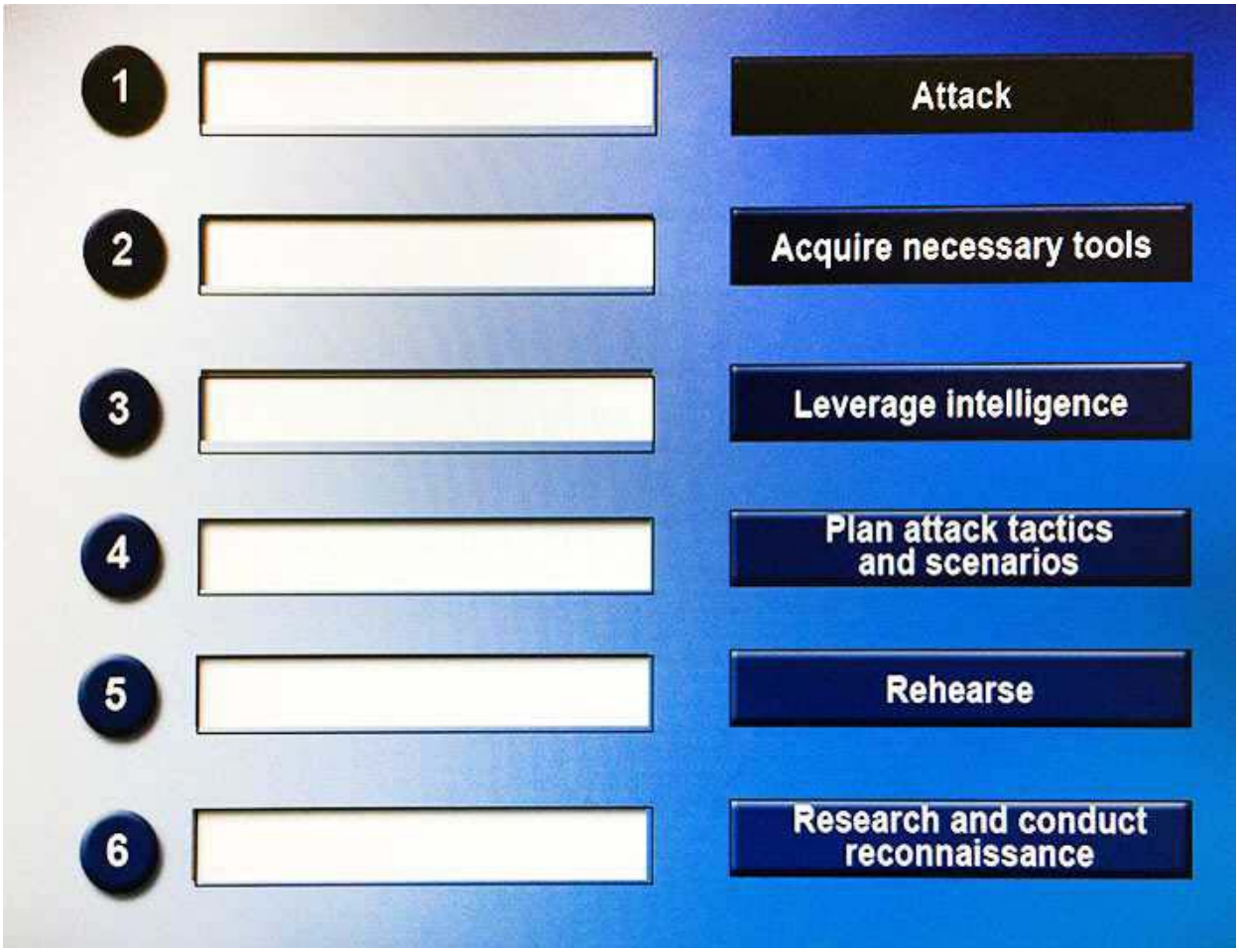
Which of the following describes the MOST important reason for capturing post-attack metadata?

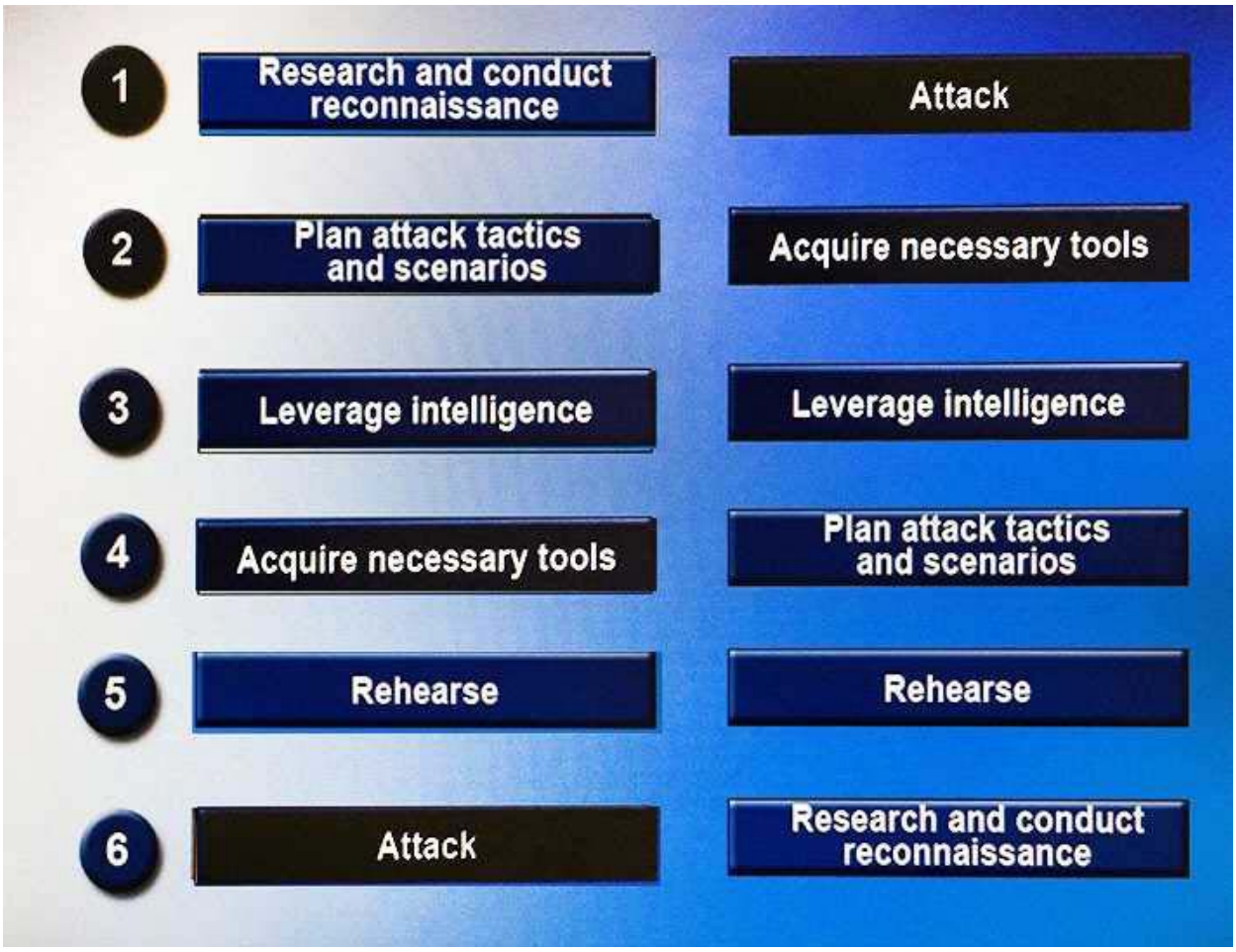
A. To assist in updating the Business Continuity Plan
B. To assist in writing a security magazine article
C. To assist in fortification of defenses to prevent future attacks
D. To assist in improving security awareness training

Answer: C

Question: 10

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