

## Preview Test: Hack Lab Scenario 1 Quiz (Due Feb 2)

### Test Information

Description Please complete the readings and videos in Scenario 1 and then attempt this Quiz, which tests basic concepts and information from those materials. You may attempt the Quiz up to **3 times**.

Instructions

Multiple Attempts This test allows 3 attempts. This is attempt number 1.

Force Completion This test can be saved and resumed later.

Your answers are saved automatically.

❖ Question Completion Status:

### QUESTION 1

1. What is the powerful tool commonly used in penetration testing and hacking activities?

Meterpreter

SMB

Linux

WannaCry

**10 points**

### QUESTION 2

1. What organization created the Eternalblue exploit?
  - a. The Hacking Group Anonymous
  - b. The U.S. National Security Agency (NSA)
  - c. The Federal Bureau of Investigation (FBI)
  - d. Microsoft Corporation

**10 points**

### QUESTION 3

1. Which of the following is an example of a file signature for a docx file?
  - a. 4D 5A
  - b. MZ
  - c. DOCX
  - d. 50 4B 03 04

**10 points**

### QUESTION 4

1. Which of the following is not part of the typical ransomware life cycle?

Exploit, expand, understand

Activation and encryption

Ransom demand  
Extradition and expulsion

**10 points**

#### **QUESTION 5**

1. Where are file signatures located in a file? Note that all files and data are stored and managed inside computers in binary format. End of the file in the below, for example, means last few binary bits of the file.
  - a. End of the file
  - b. Middle of the file
  - c. File header
  - d. Random locations

**10 points**

#### **QUESTION 6**

1. What happens when you change the extension of an office file to zip and double-click on the file?
  - a. The file is corrupted
  - b. The file opens as a zip file but shows an error
  - c. Prompts for a password
  - d. Nothing

**10 points**

#### **QUESTION 7**

1. What is another name for file signatures?
  - a. Metadata
  - b. Hexadecimal code
  - c. Magic numbers
  - d. File headers

**10 points**

#### **QUESTION 8**

1. Which of the following is not a preventative strategy for ransomware attacks
  - a. Regular data backups
  - b. Strong, unique passwords
  - c. Anti-phishing training
  - d. Cryptocurrency mining

**10 points**

#### **QUESTION 9**

1. What exploit was used in the wannacry ransomware?

- a. EternalBlue
- b. Phishing
- c. Meltdown spectre
- d. DDoS

**10 points**

#### QUESTION 10

1. What type of information can be found in Exif data (meta data)?
  - a. The file size
  - b. GPS coordinates
  - c. The file name
  - d. Both a and b

**10 points**

*Click Save and Submit to save and submit. Click Save All Answers to save all answers.*

Listen