QUESTION 1

1. What exactly is a website fingerprint?

   a. A method of user identification based on web browsing habits.

   b. A method for identifying websites based on the patterns of network traffic they generate.

   c. A method for identifying websites based on their layout and information.

   d. A method for recognizing users based on their outward appearance.

5 points

QUESTION 2

1. Which of the following nefarious activities can be facilitated or enabled by website fingerprinting techniques? Please choose one.

   a. Illegal transactions.

   b. Cyberstalking.

   c. Denial of service attacks.

   d. Speculative adversarial attacks.

5 points

QUESTION 3

1. What are the four approaches to execute intrusion through web fingerprinting?

   a. Web Analysis, Feature Extraction, classification, Identification.

   b. Traffic Analysis, Payload creation, classification, patterns recognition.

   c. Traffic Analysis, Feature Extraction, Training Phase, Identification.

   d. None of the above.

5 points

QUESTION 4

1. Which features are extracted from the network traffic to create a fingerprint for website?

   a. Packet size.

   b. Payload content.

   c. TCP/IP headers.

   d. All of the above.

5 points

QUESTION 5

1. What is a website fingerprinting limitation?

   a. It can only distinguish between static websites.

   b. It isn't precise enough to pinpoint specific users.

   c. It is simple for modern web browsers to detect.

   d. It is useless for traffic that is encrypted.

5 points

QUESTION 6

1. Website fingerprinting attacks can be stopped using network-based defences like packet obfuscation and traffic mixing.

   True

   False

QUESTION 7

1. Which of the following techniques are used by VPN to obfuscate network traffic as a defense against website fingerprinting?

   a. Obfuscation the IP address.

   b. Encryption of network traffic.

   c. Network tunnelling.

   d. All of the above.

QUESTION 8

1. Which of the following best describes how website fingerprinting attacks are typically categorized?

   a. Active and passive fingerprinting.

   b. Web traffic and network analyse.

   c. Traffic intrusion and payload duping.

   d. Internal and external fingerprinting.

QUESTION 9

1. In the Web fingerprinting scenario, we had a folder named pcaps. What did it contain?

   a. Website traffic data packets.

   b. Website screenshots.

   c. Web browser config fils.

   d. None of the above.

QUESTION 10

1. Which of the following is a website fingerprinting countermeasure?

   a. Making use of a virtual private network (VPN).

   b. Web browser JavaScript blocking.

   c. Using anonymizing networks like Tor.

   d. All of the above.

QUESTION 11

1. Website fingerprinting can be used to discriminate against people based on their race, ethnicity, gender, religion, or other characteristics. This is known as _____?

a. Profiling.

b. Obfuscating.

c. Racism.

d. Unethical.

5 points

QUESTION 12

1. What are the techniques used for web fingerprinting attacks?

   a. Timing analysis.

   b. Content analysis.

   c. Flow size analysis.

   d. All of the above.

5 points

QUESTION 13

1. Which of the following option is an ethical ramifications of website fingerprinting?

   a. Privacy invasion.

   b. Data misuse.

   c. Reputation loss.

   d. A and B.

   e. B and C.

5 points

QUESTION 14

1. Website fingerprinting can unveil users' engagement in activities, such as tracking installed application data in smart devices?

   True

   False

5 points

QUESTION 15

1. In the Web fingerprinting scenario, we had a config file named config.json. What did it contain?

   a. System configuration.

   b. Browser configurations.

   c. Domain names for capturing.

   d. Web data for capturing.

5 points

QUESTION 16

1. What is RAPTOR, in context to website fingerprinting?

   a. Countermeasure technique.

   b. Privacy analysis technique.

c. Packet flow analyser.

d. Traffic analysis technique.

QUESTION 17

1. Which of the following is a website fingerprinting attack?

   a. CUMULUS.

   b. Ryuk.

   c. Jigsaw.

   d. None of the above.

QUESTION 18

1. What is/are the application(s) of website fingerprinting?

   a. Censorship circumvention.

   b. Web caching.

   c. Security testing.

   d. A and C.

QUESTION 19

1. Website fingerprinting can be used to get around internet censorship and access content that is blocked in nations where online freedom is constrained.

   True

   False

QUESTION 20

1. What is Tor (The Onion Router)?

   a. A physical router that routes packets.

   b. Free open sourced program to encrypts traffic.

   c. A proprietary browser that masks traffic.

   d. A filtering mechanism to access deepweb.