Instructions

There are **75 total points**. When asked to provide your answer within a figure or table, be careful to not exceed box boundaries. Bubbles must be filled out completely: ● is correct, ✓ ⊙ ⊗ are incorrect All answers must be given within the provided circles, answer boxes, figures or tables.

1. [1 point]: Write your full name in the box to acknowledge the instructions.

Ethics

2. [4 points]: Which ethics principle described in the Belmont Report best describes informed consent? (Select the best answer.)

◯ Respect for Autonomy

◯ Justice

◯ Beneficience

◯ Respect for Public Policy

◯ None of the above

Case Study: hiQ Labs, a data analytics company, used web scraping to gather publicly accessible data from LinkedIn profiles to analyze employee turnover trends. LinkedIn objected, claiming this scraping violated its terms of service and potentially compromised user privacy. They argued that users consented to LinkedIn's terms, which restrict data usage, and that scraping compromised user expectations of privacy. LinkedIn also applied technical barriers to prevent hiQ from accessing its data, which hiQ circumvented.
hiQ argued that the data it accessed was publicly available, and LinkedIn had no grounds to restrict access under the Computer Fraud and Abuse Act (CFAA), which typically protects against unauthorized access to private data. hiQ contended that restricting access to this data hampered competition and limited the public's ability to analyze openly accessible information on the internet.

3. [4 points]: Use the principle of *beneficience* to present an argument **in favor** of the experiment.

(Answer inside the box)

4. [4 points]: Use the principle of *beneficience* to present an argument **against** the experiment.

(Answer inside the box)

5. [4 points]: Edward Snowden, a former NSA contractor, released classified information in 2013 revealing that the NSA was conducting extensive, indiscriminate surveillance on American citizens and foreign nationals. This surveillance included monitoring phone calls, internet activity, and communications data without individuals' knowledge or consent, raising significant concerns about privacy and government overreach.

Snowden believed that individuals had a right to know how their personal information was being used. Which ethical principle does this belief best align with?

◯ Respect for Autonomy

◯ Justice

◯ Beneficience

◯ Respect for Public Policy

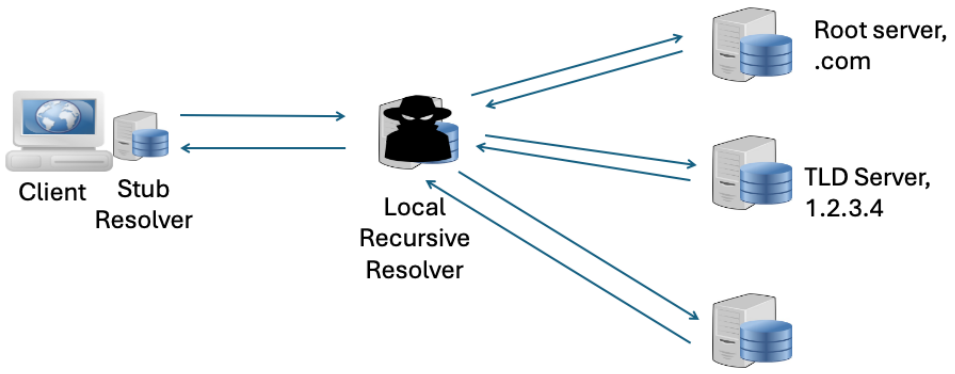
◯ None of the above

6. [2 points]: Institutional Review Board (IRB) approval of a research study implies that the study is ethical.

◯ Yes ◯ No

Denial of Service Attacks

7. [2 points]: Identify and circle the part of the Internet infrastructure responsible for sending reflected DNS traffic to the target.



Initials: ____

8. [4 points]: Which of the following is an example of amplification? (Select all that apply.)

◯ A small DNS query results in a DNS response that is redirected to a target IP address.

◯ A large number of packets is sent to a single IP address.

◯ A "ping" to a broadcast address generates reply messages sent to a target IP address.

◯ A large number of packets is sent to a single port.

9. [2 points]: Which of the following are characteristics of denial of service attacks? (Select all that apply.)

◯ They are often launched from multiple sources.

◯ The traffic they generate can be difficult to distinguish from legitimate traffic.

◯ They often involve "amplification" techniques.

◯ They always involve exhaustion of network bandwidth.

Public Key Infrastructure

10. [4 points]: In the assignment, you visited a website that used a self-signed certificate. Which of the following statements is true?

◯ Many browsers will issue warnings when visiting a website with self-signed certificate.

◯ A self-signed certificate is as secure as a certificate signed by a certificate authority.

◯ Traffic can be encrypted with a self-signed certificate if the server uses a secure protocol like HTTPS.

◯ The server can be impersonated by an attacker if it uses a self-signed certificate.

11. [4 points]: Which of the following statements correctly describes the role of a Certificate Authority (CA) in Public Key Infrastructure (PKI)? (Select all that apply.)

◯ A CA issues digital certificates that verify the ownership of public keys used in secure communications.

◯ A CA encrypts all communication between clients and servers in a PKI.

◯ A CA is responsible for verifying the identity of entities before issuing certificates.

◯ A CA stores the private keys of all clients in a PKI.

◯ If a CA's private key is compromised, attackers could potentially impersonate any entity certified by that CA.

12. [4 points]: Describe where Root Certificate Authorities (Root CAs) are typically stored in a client's environment.

(Answer inside the box)

13. [2 points]: Which aspects of the infrastructure must users trust when using Public Key Infrastructure (PKI)?

◯ The integrity of Root CAs.

◯ The security of Root CAs' private keys.

◯ The reliance on Certificate Authorities to properly verify entities before issuing certificates.

◯ The security of the network over which the root CAs are transmitted.

14. [3 points]: Suppose an attacker is able to install a "rogue" root CA on your machine. Which of the following statements is true about the incident? (Select all that apply.)

◯ The attacker may be able to decrypt all past and future messages sent to the server.

◯ Using the private key, an attacker can impersonate clients to the server.

◯ Using the private key, an attacker can impersonate the server to clients.

◯ The server can prevent against eavesdropping attacks by revoking its certificate.

◯ All of the above

Web Security

15. [4 points]: Given the following URL to a JavaScript file that dynamically displays messages on the web page: `https://example.com/displayMessage?message=` This script accepts a URL parameter 'message' to display a custom message on the page. Modify the URL to attempt injecting JavaScript that turns all of the text on the page red. Precise/correct syntax is not required, and pseudocode is fine. Show the general approach.

(Answer inside the box)

16. [3 points]: Which of the following best describes the concept of "origin" in the context of the Same-Origin Policy? (Select one.)

◯ The combination of protocol, hostname, and port of a URL.

◯ The domain name of the website only.

◯ The IP address of the server serving the webpage.

◯ Only the protocol (e.g., HTTP or HTTPS) of the webpage.

17. [4 points]: Which of the following actions can help prevent Cross-Site Scripting (XSS) attacks? (Select all that apply.)

◯ Sanitizing user input to remove or encode potentially harmful characters.

◯ Validating and restricting the types of inputs allowed (e.g., only allowing alphanumeric characters where possible).

◯ Allowing users to input and execute JavaScript code in their profiles.

◯ Escaping output in HTML templates to prevent injected scripts from running.

◯ Disabling cookies on the client's browser.

DNS Security and Privacy

18. [2 points]: Provide an argument for why DNS-over-HTTPS, as implemented in today's web browsers, might **improve** privacy and security for Internet users.

(Answer inside the box)

19. [2 points]: Provide an argument for why DNS-over-HTTPS, as implemented in today's web browsers, might **degrade** privacy and security for Internet users.

(Answer inside the box)

20. [2 points]: When encrypted DNS is enabled in your browser, the operator of the local WiFi network can no longer see the domain names that you are visiting.

◯ Yes ◯ No

Privacy and Tracking

21. [4 points]: Which of the following are commonly used techniques for web browser fingerprinting? (Select all that apply.)

◯ Collecting information about the user's browser and operating system settings, such as screen resolution and language.

◯ Using JavaScript to analyze hardware information, like the number of CPU cores and available memory.

◯ Identifying users solely based on IP address.

◯ Tracking installed browser plugins and fonts to create a unique user profile.

◯ Requiring users to log in to verify their identity on each visit.

22. [4 points]: If a user deletes cookies from a web browser after every visit to a webpage, does it prevent the website from tracking users across visits?

◯ Yes ◯ No

23. [4 points]: Why or why not?

(Answer inside the box)

Feedback

24. [1 point]: Interest (1=Boring!; 10=Amazing!): ☐ Difficulty (1=Too easy; 10=Too hard): ☐

25. [1 point]: 1. One thing you like. 2. One suggestion for improvement:

(Answer inside the box)

Initials: ____