True or False

Decide if the following statements are TRUE (A) or FALSE (B) and give an explanation why.

1. Public key certificates have expiration dates.
2. The SOP for the DOM API including matching the hostname and path.
3. The SYN packet for a TCP connection always has a sequence number of 0.
4. Users can always detect if DNS poisoning has occured if they use DNS-over-HTTPS (DoH)
5. Users can always detect if DNS poisoning has occured if they use TLS
6. Referer validation is a defense against code injection attacks.
7. LetsEncrypt certificates use TOFU as their security model.
8. An off-path attacker has to guess TCP sequence numbers to perform a TCP injection attack.
9. Randomizing the source port helps defend against an off-path attacker performing Kaminsky DNS cache poisoning.
10. Preventing iframes from having any transparency (i.e., it must be either fully visible or fully hidden) prevents clickjacking attacks.
11. The same-origin policy only applies to web cookies.
12. ARP poisoning is not a concern if the DNS results are correct.
13. A web attacker main interaction with the victim is by presenting a webpage the user is visiting.
14. The HTTP cookie same origin policy ignores the schema.

Multiple Choice

15. The notion that security is often at odds with convenience best applies to the following protocol:
    (a) TCP
    (b) DHCP
    (c) TLS
    (d) AES
    (e) Kerberos
16. Which of the following certificate revocation checking mechanisms involves downloading all revoked unexpired certificates?
    (a) OCSP
    (b) CRL
    (c) PKI certificate chains
    (d) short-lived certificates
    (e) TOFU

17. In Kerberos, why does the ticket granting service need to know the service's (i. e., printer) key (i.e., k_v)?
    (a) to assess whether the user should be granted a ticket
    (b) to encrypt a message from the TGS to the service
    (c) to decrypt the service's ticket request
    (d) to authenticate the service
    (e) none of the above because the ticket granting service does not know the services's key
18. Teardrop is what kind of attack?
    (a) man-in-the-middle attack
    (b) mafia fraud attack
    (c) denial-of-service attack
    (d) clickjacking attack
    (e) none of the above
19. Teardrop attacks which protocol?
    (a) TCP
    (b) IP
    (c) DNS
    (d) ICMP
    (e) none of the above
20. A DNS "NS" record is what?
    (a) MAC address
    (b) server name
    (c) IP address
    (d) DNS server
    (e) domain name
21. An offpath attacker can become onpath with what kind of an attack?
    (a) XSS attack
    (b) DoS attack
    (c) DNS poisoning attack
    (d) cookie theft attack
    (e) TCP injection attack
22. Bootstrapping trust is hard. Which of the following is this least relevant for:
    (a) DNS poisoning
    (b) ARP spoofing
    (c) root CAs
    (d) DHCP protocol
    (e) HSTS

23. Which Internet layer is used to communicate XSRF tokens?
    (a) application
    (b) transport
    (c) network
    (d) link
    (e) physical

24. `Secure` cookies are:
    (a) cookies sent over over HTTP
    (b) cookies never sent over HTTPS
    (c) cookies only sent over HTTPS
    (d) cookies inaccessible by scripts
    (e) cookies only accessible by scripts

25. Bob runs a public query–reply service over UDP whose replies include the full query. An attacker can use Bob's service for:
    (a) ARP spoofing
    (b) DNS poisoning
    (c) DoS amplification
    (d) TCP injection
    (e) UDP injection

26. The TCP header checksum is computed over
    (a) entire tcp header including tcp options, and entire ip header
    (b) entire tcp header including tcp options, entire ip header, and tcp payload
    (c) entire tcp header including tcp options, and tcp payload
    (d) entire tcp header including tcp options, and part of the ip header
    (e) entire tcp header including tcp options, part of the ip header, and tcp payload

27. Suppose a website users anti-XSRF tokens and HttpOnly cookies, but is vulnerable to an XSS reflection attack. How could a web attacker make forged requests to the website?
    (a) XSS vulnerabilities are forged requests.
    (b) XSS vulnerabilities can inject scripts to read HttpOnly cookies
    (c) XSS vulnerabilities can inject scripts to read anti-XSRF tokens
    (d) XSS vulnerabilities can inject scripts to read both HttpOnly cookies and anti-XSRF tokens
    (e) none of the above because the website would not be vulnerable to forged requests in this case.

28. Which of the following is not an cookie attribute discussed in class?
    (a) httponly
    (b) domain
    (c) range
    (d) secure
    (e) path

29. What is an example of non-script-based XSS?

    (a) reflected XSS

    (b) forms encapsulating forms

    (c) clickjacked XSS

    (d) insecure web cookies

    (e) none of the above

30. (2 points) Suppose you sit down at a brand new computer after installing a fresh operating system, click on a public open Wi-Fi network and connect automatically, and go to `https://www.cbc.ca`. Suppose that the resulting connection to cbc.ca is *secure and authentic*: no adversary is able to eavesdrop on your message or insert fake messages. The fact that this was delivered secure and authentically likely involved all of the following except:

    (a) DNS

    (b) DHCP

    (c) HSTS

    (d) cryptographic primitives like AES and SHA-256

    (e) none of the above (all were needed)

31. (2 points) Adding specific, conspicuous values to the server randomness in a TLS handshake is a security mechanism against what attack?

    (a) TLS ciphersuite attack

    (b) TLS handshake attack

    (c) TLS stripping attack

    (d) TLS version downgrade attack

    (e) none of the above

Written Answers

32. Consider a simple web messaging system. You get a bunch of messages from other users, and the dashboard of the system shows all the messages ever sent to you. Its HTML looks like this:

```
<pre>
Eve: Alice! Where are you??
Amazon: Your account verification code is 347214
Eve: Hello????
Amazon: Thank you for your purchase of a <b>shrubbery</b> <img
src="https://www.amazon.ca/assets/thankyou.png>
</pre>
```

    This site allows users to send *arbitrary HTML code* that is just concatenated into the page *unsanitized*. For the sake of argument, however, suppose that they have a magical technique to prevent *any kind of JavaScript* code from running. Give an example message or sequence of messages that Eve could send Alice so that when Alice views her own dashboard, Eve is able to snoop on Alice's other messages.

33. Recall DNS-over-HTTPS (DoH), where a client uses TLS to connect to a highly shared DNS resolver. While this does not protect against DNS poisoning, it still makes DNS poisoning harder and gives security against certain kinds of attacks. Give two examples where DoH makes DNS poisoning harder, clearly state the type of attacker and why DoH makes it harder to poison.

34. Recall the network layers: physical layer, link layer, network layer, transport layer, and application layer. In class we looked at attacks that can happen at the link layer and above. Select two different layers and detail a specific attack we covered at that layer. Be sure to include: the name of the attack, the consequence of the attack, why an adversary may mount the attack, the adversarial abilities required to mount the attack, defences against the attack and their efficacy.

35. Recall the design principle of security by design. Give three different protocols discussed in class and explain how this principle relates to that protocol, i.e., by being present in the design thus preventing an attack, or being absent and resulting in an attack. Explain how the attack is prevented or exploited.

36. "Port knocking" is a security mechanism where a sequence of TCP connections are made to a server in some order, such that a connection is only granted if the sequence is correct. For example, suppose that the user tries to connect to ports 1000, 2000, and 3000, at which point port 22 is then listened to on the server and so ssh access is then briefly available.

    Given that port knocking is a security mechanism:

    1. What is the asset?
    2. What is the security policy?
    3. Who is an adversary?

    Which of the following adversaries would port knocking defeat and why, assuming that the adversary's goal is to learn the correct knock sequence to log in at a later time (e.g., if they later steal the user's password).

    1. on-path active network attacker
    2. on-path passive network attacker
    3. off-path non-blind network attacker
    4. off-path blind network attacker

37. For each of the following threats, explain in detail what mechanism is used in SSL/TLS to provide protection, and how it is used.

    1. A network attacker modifies the client's "Hello" message in transit and tricks the server into thinking that the client supports a weak encryption algorithms.
    2. A network attacker captures the client's outgoing messages and send them back to the client (without altering them) but making it look like they came from the server.
    3. The client goes to evil.com, run by a Web attacker, who opens a connection to bank.com and sits between the client and bank.com, monitoring all the traffic, and convinces the client that it is connected to bank.com.