1. How is authentication different from authorization? **1 / 1 point**

- ○ They're the same thing.
- ○ Authentication is verifying access to a resource; authorization is verifying an identity.
- ○ Authentication is identifying a resource; authorization is verifying access to an identity.
- ◉ Authentication is verifying an identity; authorization is verifying access to a resource.

Correct
Right on! Authentication is proving that an entity is who they claim to be, while authorization is determining whether or not that entity is permitted to access resources.

2. What are some characteristics of a strong password? Check all that apply, **1 / 1 point**

- ☑ Is at least eight characters long

Correct
You got it! A strong password should contain a mix of character types and cases, and should be relatively long -- at least eight characters, but preferably more.

- ☐ Contains dictionary words
- ☐ Is used across accounts and systems
- ☑ Includes numbers and special characters

Correct
You got it! A strong password should contain a mix of character types and cases, and should be relatively long -- at least eight characters, but preferably more.

3. In a multi-factor authentication scheme, a password can be thought of as: **1 / 1 point**

- ◉ something you know.
- ○ something you are.
- ○ something you use.
- ○ something you have.

Correct
Wohoo! Since a password is something you memorize, it's something you know when talking about multi-factor authentication schemes.

4. What are some drawbacks to using biometrics for authentication? Check all that apply. **1 / 1 point**

- ☐ Biometrics are easy to share.
- ☑ There are potential privacy concerns.

Correct
That's exactly right! If a biometric characteristic, like your fingerprints, is compromised, your option for changing your "password" is to use a different finger. This makes "password" changes limited. Other biometrics, like iris scans, can't be changed if compromised. If biometric authentication material isn't handled securely, then identifying information about the individual can leak or be stolen.

- ☑ Biometric authentication is difficult or impossible to change if compromised.

Correct
That's exactly right! If a biometric characteristic, like your fingerprints, is compromised, your option for changing your "password" is to use a different finger. This makes "password" changes limited. Other biometrics, like iris scans, can't be changed if compromised. If biometric authentication material isn't handled securely, then identifying information about the individual can leak or be stolen.

- ☐ Biometric authentication is much slower than alternatives.

5. In what way are U2F tokens more secure than OTP generators? 1 / 1 point

- (●) They're resistant to phishing attacks.
- ( ) They're password-protected.
- ( ) They can't be cloned.
- ( ) They're cheaper.

Correct
Great job! With one-time-password generators, the one-time password along with the username and password can be stolen through phishing. On the flip side, U2F authentication is impossible to phish, given the public key cryptography design of the authentication protocol.

6. What elements of a certificate are inspected when a certificate is verified? Check all that apply. 1 / 1 point

- [x] "Not valid before" date

Correct
Yep! To verify a certificate, the period of validity must be checked, along with the signature of the signing certificate authority, to ensure that it's a trusted one.

- [ ] Certificate key size
- [x] "Not valid after" date

Correct
Yep! To verify a certificate, the period of validity must be checked, along with the signature of the signing certificate authority, to ensure that it's a trusted one.

- [x] Trust of the signatory CA

Correct
Yep! To verify a certificate, the period of validity must be checked, along with the signature of the signing certificate authority, to ensure that it's a trusted one.

7. What is a CRL? 1 / 1 point

- ( ) Certified Recursive Listener
- ( ) Certificate Recording Language
- ( ) Caramel Raspberry Lemon
- (●) Certificate Revocation List

Correct
Good job! CRL stands for "Certificate Revocation List." It's a list published by a CA, which contains certificates issued by the CA that are explicitly revoked, or made invalid.

8. What are the names of similar entities that a Directory server organizes entities into? 1 / 1 point

- ( ) Groups
- ( ) Trees
- (●) Organizational Units
- ( ) Clusters

Correct
Awesome! Directory servers have organizational units, or OUs, that are used to group similar entities.

9. True or false: The Network Access Server handles the actual authentication in a RADIUS scheme. **1 / 1 point**

- ○ True
- ◉ False

Correct
Nice work! The Network Access Server only relays the authentication messages between the RADIUS server and the client; it doesn't make an authentication evaluation itself.

10. True or false: Clients authenticate directly against the RADIUS server. **1 / 1 point**

- ○ True
- ◉ False

Correct
Correct! Clients don't actually interact directly with the RADIUS server; the authentication is relayed via the Network Access Server.

11. What does a Kerberos authentication server issue to a client that successfully authenticates? **1 / 1 point**

- ○ A master password
- ○ An encryption key
- ◉ A ticket-granting ticket
- ○ A digital certificate

Correct
Exactly! Once authenticated, a Kerberos client receives a ticket-granting ticket from the authentication server. This TGT can then be presented to the ticket-granting service in order to be granted access to a resource.

12. What advantages does single sign-on offer? Check all that apply. **1 / 1 point**

- ☑ It reduces time spent authenticating.

Correct
You nailed it! SSO allows one set of credentials to be used to access various services across sites. This reduces the total number of credentials that might be otherwise needed. SSO authentication also issues an authentication token after a user authenticates using username and password. This token then automatically authenticates the user until the token expires. So, users don't need to reauthenticate multiple times throughout a work day.

- ☑ It reduces the total number of credentials,

Correct
You nailed it! SSO allows one set of credentials to be used to access various services across sites. This reduces the total number of credentials that might be otherwise needed. SSO authentication also issues an authentication token after a user authenticates using username and password. This token then automatically authenticates the user until the token expires. So, users don't need to reauthenticate multiple times throughout a work day.

- ☐ It provides encrypted authentication.
- ☐ It enforces multifactor authentication.

13. What does OpenID provide? **1 / 1 point**

- ○ Cryptographic hashing
- ○ Digital signatures
- ○ Certificate signing
- ◉ Authentication delegation

Correct
Yep! OpenID allows authentication to be delegated to a third-party authentication service.