Cybersecurity Guided Notes

Lesson 2.8.2 - Elliptic Curves and Perfect Forward Secrecy

1. What kind of encryption is Elliptic Curve Cryptography (ECC)?

2. What makes ECC more resistant to attacks?

3. What is the purpose of SSL and TLS?

4. What happens during the establishment of an SSL/TLS session?

5. What can happen if a malicious user is able to access a server's private key?

6. What is perfect forwarding secrecy?

7. What is the purpose of perfect forward secrecy?

8. How often do encryption tools using perfect forward secrecy change their keys?

9. What are the disadvantages of using perfect forward secrecy (PFS)?