1. The two most common ways to authenticate a remote VPN peer are
   1. **PSK**
   2. FSK
   3. **RSA**
   4. AES
2. Which of the following would be considered part of Router Hardening? (Select all that apply)
   1. **Disable unused ports**
   2. **Disable unnecessary services**
   3. **Keep secure backup of OS**
   4. Disable UPS
3. Select the items below that would be considered a task for securing admin access (select all that apply)
   1. **Ensure access is only granted to authenticated users**
   2. Disable CDP
   3. **Account for and log all access**
   4. Permit HTTP services outbound
4. If properly configured, which command will show an administrator the source IP address of failed login attempts?
   1. Show AAa failures
   2. Show admin login
   3. Show denies username admin
   4. **Show login failures**
5. The default privelege level for a user a user at the “router>” prompt is\_\_\_\_
   1. 15
   2. 5
   3. 10
   4. **1**
   5. 0
6. An SNMP Manager has 2 primary types of requests (Select them below)
   1. Put
   2. Show
   3. **Set**
   4. **Get**
7. The router uses the \_\_\_ key pair for authentication and encryption of transmitted SSH data
   1. SSH
   2. **RSA**
   3. Diffie-Hellman
   4. AES
8. Which protocol that can be used between AAA clients and servers is considered to be more secure?
   1. RADIUS
   2. **TACACS+**
   3. Telnet
   4. SNMP
9. A remote site is connected to the central HQ location. The remote site host has no knowledge that there is a VPN. This is considered a \_\_\_\_ VPN
   1. Site-to-site
   2. Virutal-office
   3. **Remote-access**
   4. SOHO
10. ESP \_\_\_\_\_ mode secures the entire original IP packet
    1. E2E
    2. **Tunnel**
    3. Transport
    4. GRE