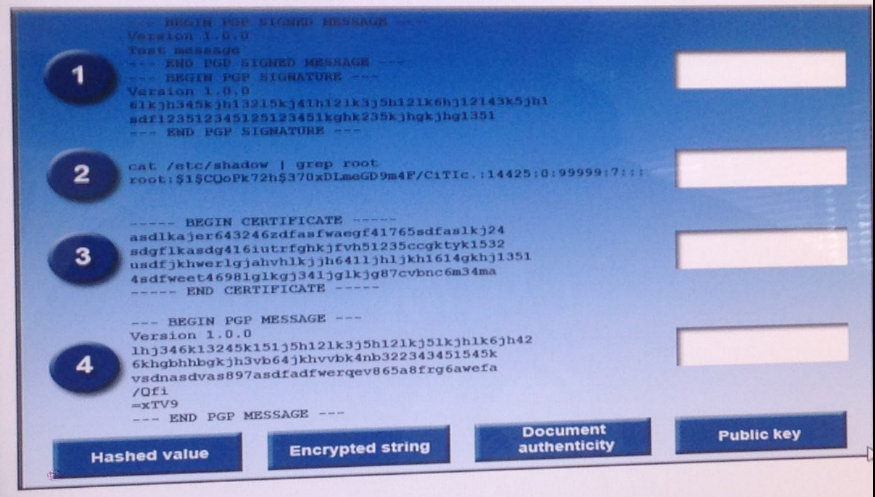
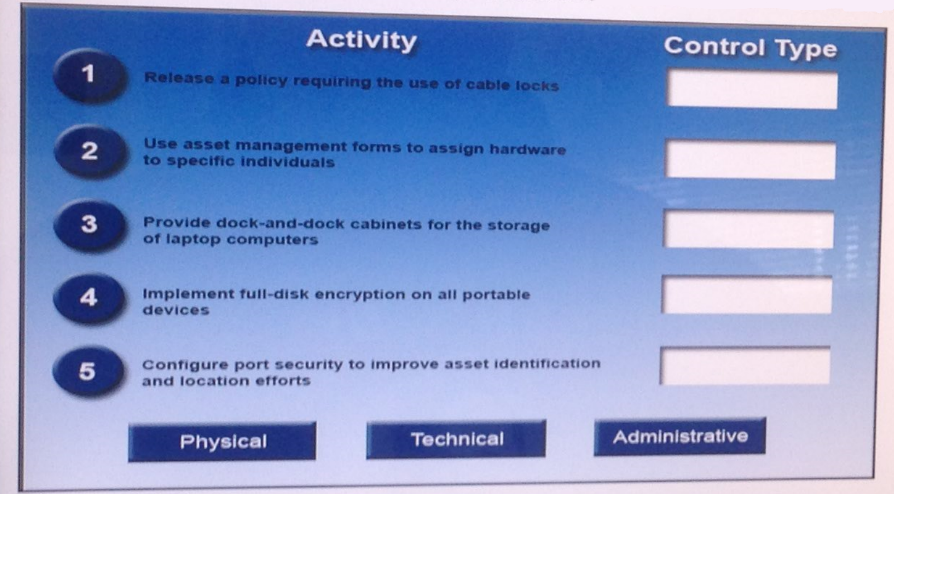
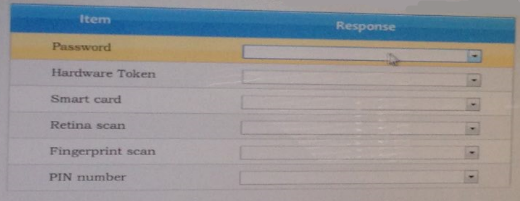
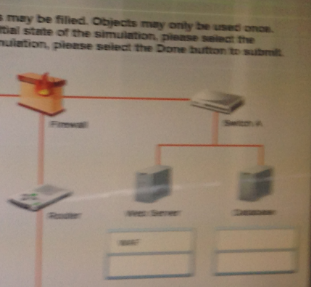
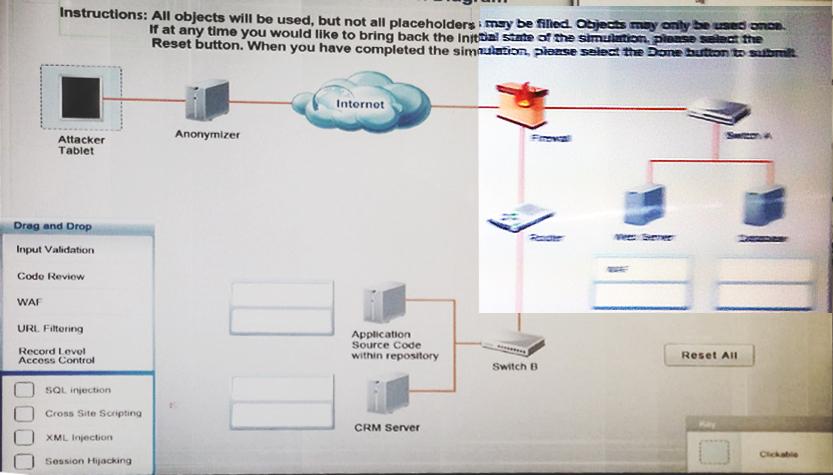
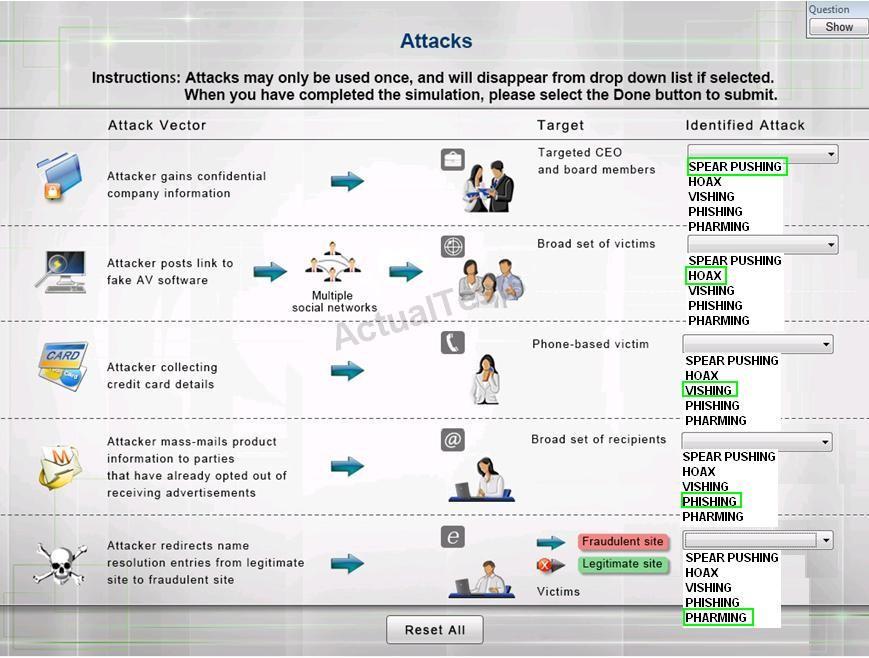
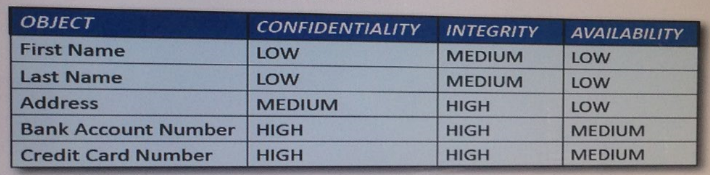
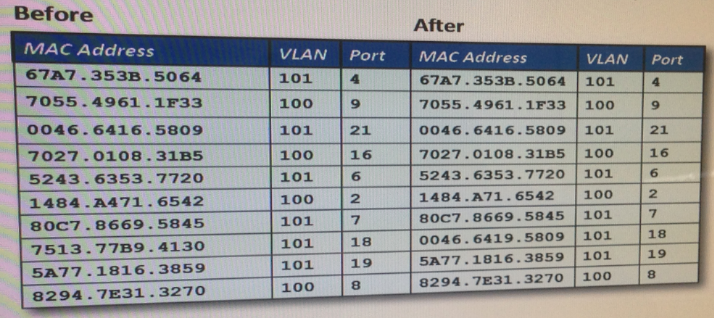
1. 
2. A security administrator has been asked to provide a corrective action plan in response to a recent audit. The audit identified deficiencies in the processes supporting the asset management process within the organization. The administrator has been asked to identify physical, technical, and administrative controls that will improve security and accountability within the corporate asset management lifecycle. Drag and drop the relevant activities identified below to the appropriate control type discussed in the corrective action plan. Options may be used more than once.  
3. 
4. 
5. 
6. A company has classified the following database records.

Which of the following is a management control the company can implement to increase the security of the above information respect to confidentiality?

* 1. Implement a client-based software filter to prevent some employees from viewing confidential information.
  2. Use a privacy screen on all computers handling and displaying sensitive information.
  3. Encrypt the records that have a classification of HIGH in the confidentiality column.
  4. Disseminate the data classification table to all employees and provide training on data disclosure.

1. Which of the following is MOST effective at cracking hashed passwords?
2. Rainbow Tables
3. Dictionary Attack
4. Birthday Attack
5. Brute Force Attack
6. An old 802.11b wireless bridge must be configured to provide confidentiality of data in transit to include MAC addresses of communicating endpoints. Which of the following can be implemented to meet this requirement?
7. MSCHAPv2
8. WPA2
9. WEP
10. IPsec
11. An Administrator wants to configure the security setting in the AD domain to force users to use a unique new password at least ten times before an old password can be reused. Which of the following security controls is the administrator enforcing?
12. Password age
13. Password expiration
14. Password history
15. Password complexity
16. During a recent audit, it was discovered that several database services were running with local user accounts named “admin” and “dbadmin.” Which of the following controls will prevent network administrators from using these types of usernames for services in the future? (Select TWO).
    1. Use shared account policies
    2. Prohibit generic or default accounts
    3. Perform continuous access monitoring
    4. Perform user account access reviews
    5. Require dedicated service accounts
17. Which of the following mobile device controls can be used to ensure company data is containerized in BYOD environment?
    1. Sensitive data encryption
    2. Removable storage security
    3. Mobile application control
    4. Storage segmentation
18. Ann, a security analyst, is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call-back domain. Which of the following tools would aid her decipher the network traffic?
    1. Vulnerability Scanner
    2. Nmap
    3. Netstat
    4. Packet Analyzer
19. A company uses digital signatures to sign contracts. The company requires external entities to create an account with a third-party digital signature provider and sign an agreement stating they will protect the account from unauthorized access. Which of the following security goals is the company trying to address in the given scenario?
    1. Availability
    2. Non-repudiation
    3. Authentication
    4. Confidentiality
    5. Due diligence
20. A web server at an organization has been targeted of distributed denial of service attacks. Which of the following, if correctly configured, would BEST mitigate these and future attacks?
    1. SYN cookies
    2. Implicit deny
    3. Blacklisting
    4. URL filter
21. A security administrator suspects that an employee has altered some fields with a noSQL database. Which of the following should the security administrator do to confirm the suspicion and identify the employee?
    1. Review the video of the employee’s workstation
    2. Review the database access log files.
    3. Capture a system image of the entire server
    4. Generate file hashes of the database to compare to the last version.
22. An organization that uses a cloud infrastructure to present a payment portal is using:
    1. Software as a service
    2. Platform as a service
    3. Monitoring as a service
    4. Infrastructure as a service
23. A server administrator is investigating a breach and determines that an attacker modified the application log to obfuscate the attack vector. During the lessons learned activity, the facilitator asks for a mitigation response to protect the integrity of the logs should a similar attack occur. Which of the following mitigations would be MOST appropriate to fulfill the requirement?
    1. Host-based IDS
    2. Automated log analysis
    3. Enterprise SIEM → (**Security Information event management**)
    4. Real-time event correlation
24. Ann, a security administrator, needs to implement a transport encryption solution that will enable her to detect attempts to sniff packets off the wire.
    1. Elliptic curve algorithms
    2. Ephemeral keys
    3. Quantum cryptography
    4. Steganography
25. A forensics expert needs to be able to prove that digital evidence was not tampered with after being taken into custody. Which of the following is useful in this scenario?
    1. Encryption
    2. Non-repudiation
    3. Hashing
    4. Perfect forward secrecy
    5. Steganography
26. Based on a review of the existing access policies, the network administrator determines that changes are needed to meet the current regulatory requirements for the organization’s access control process. To initiate changes in the process, the network administrator should FIRST:
    1. Update the affected policies and inform the user community of the changes
    2. Distribute a memo stating that all new accounts must follow current regulatory requirements
    3. Inform senior management that changes are needed to existing policies
    4. Notify the user community that non-compliant accounts will be required to use the new process
27. A security administrator wishes to perform authentication, authorization, and accounting, but does not wish to use a proprietary protocol. Which of the following services would fulfill these requirements?
    1. SAML
    2. RADIUS
    3. TACACS+
    4. Kerberos
28. A security administrator has been tasked with hardening operating system security on tablets that will be deployed for use by floor salespeople at retail outlet. Which of the following could the administrator implement to reduce the likelihood that unauthorized users will be able to access information on the tablets?
    1. GPS device tracking
    2. Remote wiping
    3. Cable locks
    4. Password protection
29. A company has begun construction on a new building. The construction crews have noticed that valuable materials have been stolen from the site. Which of the following preventative controls should be used by the Chief Security Officer (CSO) to prevent future theft?
    1. Motion sensors
    2. CCTV
    3. Fencing
    4. Lighting
30. A system administrator wants to ensure that only authorized devices can connect to the wired and wireless corporate systems. Unauthorized devices should be automatically placed on a guest network. Which of the following MUST be implemented to support these requirement? (Select TWO).
    1. Port security
    2. 802.1x
    3. Proxy
    4. VLAN
    5. NAT
31. A security administrator is performing a vulnerability scan and discovers that port 21 and 22 are open to support FTPS. Which of the following is this an example of?
    1. False positive
    2. Input validation
    3. Banner grabber
    4. Common misconfiguration
32. A risk assessment team is concerned about hosting data with a cloud service provider (CSP). Which of the following finding would justify this concern?
    1. The CSP utilizes encryption for the data at rest and data in motion
    2. The CSP takes into account multinational privacy concerns
    3. The financial reviews indicates the company is a startup
    4. SLAs state service tickets will be resolved in less than 15 minutes.
33. The help desk team at a company needs the ability to create/modify/delete users as well as reset passwords. Which of the following would be the BEST method to assign the appropriate privileges?
    1. Individually assign the appropriate privileges to each user
    2. Make each user a domain administrator
    3. Make each user an administrator on the domain controllers
    4. Place the users in a security group and assign the correct privileges

1. A forensics engineer is performing an analysis on a computer with a static IP address that is connection to various malicious websites. The engineer wants to retain information that would otherwise be list if the computer reboots. Which of the following outputs should the engineer capture FIRST?
   1. Hostname
   2. Netstat
   3. Ipconfig
   4. DIR
2. The first responder to an incident has been asked to provide an after action report. Which of the following incident response procedures does this support?
   1. Incident identification
   2. Mitigation
   3. Lessons learned
   4. Escalation/notification
3. A company uses PKI certificates stored on a smart-chip-enabled badge. The badge is used for a small number of devices that connect to a wireless network. A user’s badge was reported stolen. Which of the following could the security administrator implement to prevent the stolen badge from being used to compromise the wireless network?
   1. Asset tracking
   2. Honeynet
   3. Strong PSK
   4. MAC filtering
4. **When** implementing a new system, a systems administrator works with the information system owner to identify and document the responsibilities of various positions within the organization. Once responsibilities are identified, groups are created within the system to accommodate the various responsibilities of each position type, with users being placed in these groups. Which of the following principles of authorization is being developed?
   1. Rule-based access control
   2. Least privilege
   3. Separation of duties
   4. Access control lists
   5. Role-based access control
5. An administrator sees the following entry in a system log:  
   02:23:41AM Mar 09 2015 www: MD5 checksum on file /etc/sudoers has changed. Please update db if this change is expected.  
   Which of the following describes the type of application that generated this log entry?
   1. Change management
   2. Security patch management
   3. SELinux audit utility
   4. File integrity management
6. A malicious individual is attempting to insert special characters (e.g., apostrophe) into a data entry field. Which of the following attacks would this be?
   1. Session hijacking
   2. Integer overflow
   3. SQL injection
   4. Cross-site scripting
7. A network administrator discovers that telnet was enabled on the company’s Human Resources (HR) payroll server and that someone outside of the HR subnet has been attempting to log into the server. The network administrator has disabled telnet on the payroll server. Which of the following is a method of tracking attempts to log onto telnet without exposing important company data?
   1. Banner grabbing
   2. Active port monitors
   3. Honeypot
   4. Passive IPS
8. A network administrator is in the process of developing a new network security infrastructure. One of the requirements for the new system is the ability to perform advanced authentication, authorization, and accounting services. Which of the following technologies BEST meets the stated requirement?
   1. Kerberos
   2. SAML
   3. TACACS+
   4. LDAPS
9. A PKI architect is implementing a corporate enterprise solution. The solution will incorporate key escrow and recovery agents, as well as a \*\*\*\* architecture. Which of the following is required in order to implement the architecture correctly?
   1. Certificate revocation list
   2. Strong ciphers
   3. Intermediate authorities
   4. IPsec between CAs
10. -
11. -
12. A security auditor has full knowledge of company configuration and equipment. The auditor performed a test on the network, resulting in an exploitation of a zero-day vulnerability. Which of the following did the security auditor perform?
    1. Grey box test
    2. Vulnerability scan
    3. Black box test
    4. Penetration test
13. A risk manager is drafting an internal national travel guideline for securing electronic devices. Which of the following are the MOST appropriate components that should be included in the guidelines with regards to physically securing devices while traveling? (Select TWO).
    1. Hashing
    2. Cable Locks
    3. Safe
    4. Full-disk encryption
    5. TPM
    6. Memory encryption
14. A security administrator runs a port scan against a server and determines that the following ports are open:  
    TCP 22  
    TCP 25  
    TCP 80  
    TCP 631  
    TCP 995  
    Which of the following MOST likely describes the server?
    1. It is an email server that requires secure email transmittal
    2. It is a web server that requires secure communication
    3. It is a print server that requires secure authentication
    4. It is an email server that requires secure email retrieval.
15. A company has implemented a public-facing authentication system that uses PKI and extended attributes to allow third-party, web-based application\*\*\* integration. Which of the following is this an example of? (Select THREE).
    1. Federation (wiki gives explanation)
    2. Two-factor authentication
    3. Transitive trust
    4. Trusted OS
    5. Single sign-on
    6. TOTP
    7. MAC
16. A company has completed the continuity of operations plan and needs to validate that everyone knows what actions to perform. Which of the following can be performed instead of completing a full fail over to validate this requirement?
    1. Tabletop exercise
    2. Sandboxing
    3. Business impact analysis
    4. Risk assessment
17. A datacenter has suffered repeated burglaries that led to equipment theft and arson. In the past, the thieves have demonstrated a determination to bypass any installed safeguards. After mantraps had been installed to prevent tailgating, the thieves crashed through the wall of the datacenter with a vehicle after normal business hours. Which of the following option could further improve the physical safety and security of the datacenter? (Select TWO).
    1. Cipher locks
    2. CCTV
    3. Escape routes
    4. K-rated fencing
    5. FM200 fire suppression
18. Which of the following MUST be implemented to ensure accountability?
    1. Employ access control lists
    2. Configure password complexity
    3. Disable shared accounts
    4. Change default passwords
19. A finance manager is responsible for approving wire transfers and processing the transfer using the software provided by the company \*\*\* number of discrepancies have been found related to the wires in a recent financial audit and the wires appeared to be fraudulent. Which of the controls should be implemented to reduce the likelihood of fraud related to the use of wire transfer?
    1. Separation of duties
    2. Least privilege
    3. Qualitative auditing
    4. Acceptable use policy
20. A recent audit has revealed that a large percentage of laptop computers on the internal network are missing critical system updates. Which of the following will MOST effectively reduce the likelihood that these machines will become compromised by unknown malware?
    1. Access control lists
    2. Antivirus software
    3. Patch management
    4. Behavior-based IPS
21. A security analyst would like to prevent malicious users from detecting systems on the network. Which of the following protocols would the security analyst block so that a ping sweep would not reply to this type of scanning?
    1. ICMP
    2. DNS
    3. NetBIOS
    4. WINS
22. \*\*\*\*\*\* domains. The administrator connects to the switch and adds a MAC filter to Port 18 to block the system from the network.  
      
    A few minutes later, the same malicious traffic starts again from a different IP. Which of the following is the MOST likely reason that the system is able to bypass the administrator’s MAC filter?
    1. The system is now ARP spoofing a device on the switch
    2. The system is now VLAN hopping to bypass the switch port MAC filter
    3. The system is now spoofing a MAC address
    4. The system is now connecting to the switch
23. Which of the following network design components would assist in separating network traffic based on the logical location of users?
    1. IPsec
    2. NAC
    3. VLAN
    4. DMZ
24. A recent policy change at an organization requires that all remote access connections to and from file servers at remote locations must be encrypted. Which of the following protocols would accomplish this new directive? (Select TWO).
    1. TFTP
    2. SSH
    3. FTP
    4. RDP
    5. HTTP
25. Which of the following would be MOST appropriate for securing large amounts of data-in-motion?
    1. SHA
    2. RSA
    3. Diffie-Hellman
    4. AES
26. A company is experiencing problems with performance and downtime because application updates and patching are being conducted on production systems during business hours. Users and other information technology staff are not being notified of the updates. Which of the following need to be instituted to BEST resolve the problems?
    1. Incident management
    2. Change management
    3. User rights review
    4. Acceptable use policy
27. Which of the following methods should be used to minimize the impact of network congestion on a building automation system?
    1. Intrusion detection system
    2. Network access control
    3. Host-based firewall
    4. Network segmentation
28. Which of the following remote authentication methods uses a reliable transport layer protocol for communication?
    1. RADIUS
    2. LDAP
    3. TACACS+
    4. SAML
29. Joe a helpdesk specialist. During a routine audit, a company discovered that his credentials were used while he was on vacation. The investigation further confirmed that Joe still has his badge and it was last used to exit the facility. Which of the following access control methods is MOST appropriate for preventing such occurrences in the future?
    1. Access control where the credentials cannot be used except when the associated badge is in the facility
    2. Access control where system administrators may limit which users can access their systems
    3. Access control where employee access permissions are based on job title
    4. Access control system where badges are only issued to cleared personnel
30. An employee connects a wireless access point to the only jack in the conference room to provide internet access during a meeting. The access point is configured to secure its users with WPA2-TKIP. A malicious user is able to intercept clear text HTTP communication between the meeting attendees and the internet. Which of the following is the reason the malicious user is able to intercept and see the clear text communication?
    1. The malicious user is running a wireless sniffer
    2. The wireless access point is broadcasting the SSID
    3. The malicious user is able to capture the wired communication
    4. The meeting attendees are using unencrypted hard drives
31. A company has noticed a recent increases in machines that have been exploited using vulnerabilities via third-party software. Which of the following would BEST help the company reduce the likelihood of vulnerabilities within the software creating future problems?
    1. Patch management
    2. Host-based firewall
    3. Antivirus software
    4. White-listing applications
32. Several computers in an organization are running below the normal performance baseline. A security administrator inspects the computers and finds the following pieces of information:  
     -Several users have uninstalled the antivirus software  
     -Some users have installed unauthorized software  
     -Several users have installed pirated software  
     -Some computers have had automatic updating disabled after being deployed  
     -Users have experienced slow responsiveness when using the internet browser  
     -Users have complete control over critical systems properties  
    Which for the following solutions would have prevented these issues from occurring? (Select TWO)
    1. Using snapshots to revert unwanted user changes
    2. Using an IPS instead of an antivirus
    3. Placing users in appropriate security groups
    4. Disabling unnecessary services
    5. Utilizing an application whitelist
    6. Utilizing an application blacklist
33. An employee connects to a public wireless hotspot during a business trip. The employee attempts to go to a secure website but instead connects to an attacker who is performing a man-in-the-middle attack. Which of the following should the employee do to mitigate the vulnerability described in the scenario?
    1. Connect to a VPN when using public wireless networks
    2. Only connect to WPA2 networks regardless of whether the network is public or private
    3. Ensure a host-based firewall is installed and running when using public wireless networks
    4. Check the address in the web browser before entering credentials
34. An organization’s security policy requires secure file transfer to and from internal hosts. An employee is attempting to upload a file using an unsecure method to a Linux-based dedicated file server and fails. Which of the following should the employee use to transfer the file?
    1. FTP
    2. HTTPS
    3. SSL
    4. SCP
    5. TLS
35. A company is \*\*\*\*\*\*\*\*\*\*\*\*\* to blurry \*\*\*\*\*\*\*\*
36. A technician received a ticket from a project manager while working on an enterprise SIEM architecture deployment. The project manager has requested a specific executable be authorized for use on the network. Which of the following configuration items would be MOST appropriate for the technician to modify in support of the requirement?
    1. Application whitelist
    2. Antivirus configuration
    3. Command line interface
    4. Host software baseline
    5. DNS blacklist
37. The network administrator wants to assign VLANs based on which user is logging into the network. Which of the following should the adr\*\*\* to accomplish this? (Select TWO).
    1. MAC filtering
    2. RADIUS
    3. 802.3af
    4. 802.11ac
    5. 802.1x
    6. 802.3q
38. Which of the following network configurations provides security analysts with the MOST information regarding threats, while minimizing the risk to internal corporate assets?
    1. Configuring the wireless access point to be unencrypted
    2. Increasing the logging level of internal corporate devices
    3. Allowing inbound traffic to a honeypot on the corporate LAN
    4. Placing a NIDS between the corporate firewall and ISP
39. A security administrator is reviewing the event logs for a company server. There are numerous entries for attempts to log into the telnet service with an account named “root.” After further review of the access to the server, the security administrator determines there is a business need for another server in the company to connect via telnet to the server under review. Which of the following tasks should the security administrator perform to improve the security posture of the server? (Select TWO).
    1. Change the timeout values on the telnet service
    2. Allow the telnet access to the server through the firewall
    3. Configure the telnet service to only accept traffic from the other server
    4. Configure the telnet service to log at the debug level
    5. Disable root access within the telnet service
    6. Set the telnet service to enforce password changes every 90 days.
40. An employee is conducting a presentation at an out-of-town conference center using a laptop. The wireless access point at the employee’s office has an SSID of *OFFICE*. The laptop was set to remember wireless access points. Upon arriving at the conference, the employee powered on the laptop and noticed that it was connected to the *OFFICE* access point. Which of the following MOST likely occurred?
    1. The laptop connected to a legitimate WAP
    2. The laptop connected as a result of an IV attack
    3. The laptop connected to an evil twin WAP
    4. The laptop connected as a result of near field communication
41. A system administrator is configuring a site-to-site IPsec VPN tunnel. Which of the following should be configured on the VPN concentrator for payload encryption?
    1. ECDHE
    2. SHA256
    3. HTTPS
    4. 3DES ???Maybe
42. A company is hosting both sensitive and public information at a cloud provider. Prior to the company going out of business, the administrator wants to decommission all virtual server hosted on the cloud. When wiping the virtual hard drive, which of the following should be removed?
    1. Hardware specifications
    2. Encrypted files
    3. Data remnants
    4. Encrypted keys
43. A company has a proprietary device that requires access to the network be disabled. Only authorized users should have access to the device. To further protect the device from unauthorized access, which of the following would also need to be implemented?
    1. Install NIPS within the company to protect all assets
    2. Block port 80 and 443 on the firewall
    3. Install a cable lock to prevent theft of the device ????
    4. Install software to encrypt access to the hard drive
44. A penetration tester is attempting to determine the operating system of a remote host. Which of the following methods will provide this information?
    1. Protocol analyzer
    2. Honeypot
    3. Fuzzer
    4. Banner grabbing
45. After a private key had been compromised, an administrator realized that downloading a CRL once per day was not effective. The administrator wants to immediately revoke certificates. Which of the following should the administrator investigate?
    1. CSR
    2. PKI
    3. IdP
    4. OCSP