**Overview/review**

1. (This exact question will be on the final. Prepare your answer before the exam) Explain the risks involved with using SSL where the server’s public key is signed and where the server’s public key is not signed. Include examples where risk is too high and where the risk is probably not too high. In your description, be sure to include the following
   1. Describe the vulnerability involved in accessing a web site with an unsigned public key.
      1. Unsigned public key means that the client cannot verify that the received public key is actually the server’s public keys vs an attacker’s key. This means that an attacker can perform a man-in-the-middle attack and the client would not be able to detect it. On the other hand, the data is still encrypted and so eavesdropping is not possible.
   2. Describe the vulnerability involved in accessing a web site with a signed public key.
      1. If the public key is signed by the CA, then the vulnerability is associated with the public key being received by the client is not the server’s public key. This can happen in two scenarios
         1. The CA has incorrectly issued a signed public key that is not the server’s public key. The CA should only issue signed public keys where the public key is from the owner of the server. But the CA could make a mistake and incorrectly sign a public key that is not owned by the server
            1. The CA needs to make a “mistake”
         2. The public key of the CA is incorrect on the browser, that is the attackers fake CA public key is stored by the browser. Recall, the server sends (K, KCA\_private\_key(H(K)), then the browser decrypts , KCA\_private\_key(H(K)) with the CA public key. The we have the wrong CA public key, then (K, KWrongCA\_private\_key(H(K)) could pass our test with the wrong CA public key
            1. Need to change the browsers CA public key
      2. However, when the client receives an incorrect public key, the attack to decrypt and infiltrate the connection requires a man-in-the-middle attack is performed. Such an attack is non-trivial to accomplish.
   3. Describe a scenario where the risk of having an unsigned public key is acceptable
      1. Many scenarios where the data being exchanged is not important, you can think of some
   4. Describe a scenario where the risk of having an unsigned public key is not acceptable but the risk of having a signed public key is acceptable
      1. Amazon ordering, credit card stuff, etc. You can think of some
   5. Describe a scenario where risk of using a signed public key is not acceptable
      1. Missile launch web-UI, critical infrastructure, etc.
2. ~~Explain the role that policy plays in cyber security?~~
3. What is CIA?
4. Compare/contrast: Threat vs. Vulnerability

**Chapter 21**

1. What is auditing
   1. Collecting details data about whether policy is being enforced and other security data
   2. Audting is collecting and analysising of information logs in a clear and accurate manners
2. List 5 things that might be logged
   1. Web server logs, DB logs, machine log-in, file access, application log-in, application logs
3. Policy and Auditing
   1. How does policy relate to auditing?
      1. Auditing should produce evidence that policy is being enforced
   2. Gives one or more example of how policy impacts auditing?
      1. If policy states that a machines’ ACL should only contain “Stephan”, then the audit logs should be the ACL for that machine
   3. Does policy dictate all auditing?
      1. Partly, but auditing should/can collect other data as well
4. Why might logs need to be sanitized? What are the drawbacks of data sanitization?
   1. Confidential data can end up in logs and must be removed.
   2. Removing data from logs, the logs can be more difficult to interpret
5. (star) What are the pros and cons of logging/auditing products such as New Relic where the logs are stored in the cloud and managed by a vendor.
   1. Pros: no need to maintain servers with log data
   2. Cons: potentially confidential information is on some other company’s servers

**Chapter 22**

1. One characteristic of a system not under attack is “User actions conform to statistical pattern.” Give an example where a system getting attacked or a user attacking a system might behave differently than the normal user or system.
   1. A regular user gains root access
2. (star) A Trojan installs a backdoor that allows the attacker to connect to the system via port 9321. How can this type of behavior be detected?
   1. With host-based IDS without a firewall?
      1. Answer: Host-based IDS can detect an unknown process listening on port 9321 and detect incoming connections
   2. With host-based IDS with a firewall that blocks port 9321?
      1. Answer: Host-based IDS can detect an unknown process listening on port 9321
   3. With network-based IDS without a firewall?
      1. Answer: The network-based IDS can detect incoming connections to the host to port 9321
      2. Answer continued: Policy says that this machine is not a server and/or there are no known/allowed processes listening on port 9321 on this machine
   4. With network-based IDS with a firewall that blocks port 9321?
      1. Answer: Networking-based IDS **cannot** detect the trojan if connections to the trojan are blocked
      2. (aside: network port scanning can detect the open port)
3. IDS
   1. Define false positive and false negative.
   2. Explain how IDS false negative can result in a successful attack
   3. Explain how IDS false positives can result in successful attacks
      1. Too many false positive will result in users ignoring the IDS
4. What is a significant (perhaps the most significant) challenge facing the design of a statistical-based anomaly detection system?
   1. These methods are based on the idea that there is normal behavior which is different from attack behavior. However, it is difficult to precisely define what is normal behavior. If normal behavior is classified as abnormal, then we get a false alarm. And if an attack mimics normal behavior, then we get a false negative.
5. Define and compare host-based IDS to network-based IDS.
   1. See notes
6. If all network traffic is encrypted, then is there any use for network-based IDSs?
   1. Answer: flow-based IDS is possible
   2. Answer continued: However, deep packet inspection is difficult. In order for deep packet inspection to work, man-in-the-middle message eavesdropping must be possible, which requires that the SSL encryptions must be broken, which can be done by installing bogus CA public keys on the machines.