ISEC 325 Homework 06

Answer the following questions based on your reading of the text books, the module key points, and the instructor's presentation this week.

1. [2 points] How is local authentication different from centralized authentication? How are they similar?

   Local authentication is when a server maintains a local file of usernames and passwords where it compares the username and password provided by the client. Local authentication is the most common and has a weakness due to passwords and how they can be forgotten, revealed or stolen. Centralized authentication is when a centralized server handles all the authentication. Active Directory is an example of centralized authentication. Centralized authentication allows access to multiple network and server resources. Two levels of trust must be maintained with centralized authentication the client has to trust the authentication server in that it has the right information and the application server must trust that the authorization server can correct identify and authorize the client.

2. [3 points] Pick two of the three AAA services (Kerberos, TACACS+, RADIUS) and research their features. Construct a comparison table based on the major characteristics of AAA for them.

   Kerberos

   - Authorization and encryption are standard on clients and servers.
   - Both the client and the server must be able to trust the Kerberos server.
   - Passes credentials in plain text so encryption is needed.
   - Makes use of security tickets and tokens which have a time limit.
   - Must be strongly secured due to the amount of trust placed in it.
   - Passwords are not stored.
   - Can be used across Unix and Windows operating systems.
   - Named from the three headed hound that guards the gates of Hades in Greek mythology.

   TACTACS+

   - Good to use when network traffic is slowed by heavy loads on firewalls. The TACTACS+ server takes the authentication from the firewall's responsibilities.
   - Utilized TCP so packets may be filtered by firewalls.
   - Encrypts both the header and data of the packets.
   - Passwords are stored in a database and may be encrypted.
   - Uses independent authorization, authentication and auditing.
   - No fancy name just an acronym that stands for Terminal Access Controller Access Control System Plus, which no one wants to say. Commonly referred to as Tac-plus.

3. [4 points] What is meant by “two factor authentication?” Describe three real-world (i.e. not related specifically to IT although IT may be involved) examples of two-factor authentication.

Two factor authentication is when you must use two means of authenticating such as a password and code that is sent directly to your phone. It would be something you know (password) and something you have (phone) and the two factors of authenticating. It is a secure form of authenticating. One real world form of two factor authentication is the ATM card it is something you have (card) and something you know (Pin number). The second would be the timeclock at my job which uses biometrics for something I am (fingerprint) and something I know (clock number). The third would be a VPN requiring a user to authenticate with something they know (password) and something they have (code sent to the phone they possess.).

On a personal note although the book tells us that two factor is a secure method it can still be compromised. At the Central Ohio Security Summit Dave Kennedy was one of the speakers. He told of how he was able to obtain a user token to gain access to a companies system however when he tried to log on a popup notified him that he needed to authenticate. He thought all his work was over. The employee who’s token was being used was at lunch and received a request to authenticate on his phone and did. It doesn’t matter how much security you have the user will always be the weakest point.

4. [2 points] In the context of VPNs, how can the term “tunnel” be misleading?

From the term tunnel it would seem like you are using the equivalent of a private leased line where a connection is made from a single line from endpoint to endpoint, it is not the same. The term tunnel refers to a virtual tunnel or pathway over a packet network. The virtual pathway makes use of internet based hosts and servers to transmit data the same as a TCP connection.

5. [3 points] What are the advantages and disadvantages of hub-and-spoke VPN configurations?

The advantages of a hub-and-spoke VPN configuration are that it is easy to increase the size of the VPN as new machines or offices only need to connect with the central VPN server. The centralized VPN server contains records of all Security Associations so that devices do not have to be updated only the centralized VPN server. The problem with the hub-and-spoke configuration is that it slows down traffic as the centralized VPN server can become a bottleneck for your network traffic. The bottleneck can significantly slow down traffic if it is intercontinental.

6. [3 points] What are the advantages and disadvantages of mesh VPN configurations?

In the Mesh configuration each user or device using the VPN has an approved relationship with all other users and devices. The Mesh configuration is more efficient as there is not bottleneck. The problem with the Mesh architecture is that to scale it up each user and device must be updated with new users and devices security association. Each user or device

needs added to the VPN state table as well. The Mesh configuration also requires each user and device to have sufficient memory to run the VPN software. The Mesh configuration is harder to scale.

7. [8 points] A common "work from home" scenario lets remote users install VPN software on their personal computers and connect to corporate resources. As a security professional, what kinds of additional concerns would you have when allowing employees to connect via VPN? How would you address those concerns? Frame your answer in terms of the McCumber cube.

   My concerns maintaining a VPN would be who would be using the VPN? You would not want your network exposed to unauthorized persons. Is the proper anti-virus software being used on the remote user's computer because viruses can make it through the perimeter if they are encrypted. I would also be concerned about the amount of time remote users were on the VPN due to the cost of company high speed internet used to maintain the VPN.

   The problem of whom is using the VPN fall into the intersection of confidentiality and processing on the McCumber cube. You would need to use 2 factor authentication at very least. The problem of having up to date anti-virus software falls into the intersection of integrity and transmission. You would need to use NAC or proprietary device monitoring software to ensure the remote user is current on anti- virus software. The amount of time that someone is on the VPN falls under the intersection of availability and processing and transmission. You would need to write rules with lease times on the VPN to prevent remote users from wasting bandwidth when they may not even be at their workstation.

8. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you're still confused about. In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

   I feel like I have a pretty good grasp on the first part of this week's topic. Authentication is a big part of any cyber security class, book, or seminar. I understand the importance of it and the challenges that come with it. It is always nice to get another look at it from another point of view, however. I see how it fits in with the second part of the chapter on VPNs.

   I found the information on VPNs to be very helpful. I knew what they were, but I didn't know exactly how they worked in an organizational environment. I didn't know about the VPN architectures and how they worked. I also was not aware of the dangers a VPN can present or

about the best practices involved with operating and maintaining them. It was also nice how you explained in the MEET session that if a VPN circumnavigates your firewalls it can be dangerous for your network.

References

Whitman, M. E. (2012). *Guide to Network Security, 1e.* Cengage Learning.