Wireless Security Midterm

Scenario Question (25pts)

You have been hired by Wayne Enterprises to set up a Wireless Network within their new facility in Gotham. This new facility will be a state of the art R&D (Research and Development) site. What considerations would you need to make to set up this network? Mr. Wayne is generous enough to give you a $30k budget on setting up this type of network. Please specify what tools, devices, and other items you will need to spend your money on. You will also need to provide some of the specs, the reasons why you chose those items, and the actual cost. In addition, explain how you would configure these devices and what type of secure authentication you would use. Mr. Wayne wants you to be very detailed in the "report", so do not insult Mr. Wayne's intelligence by only defining terms; he wants to know how to apply these devices and concepts. (15 pts) **If there are no sources listed, you will not receive credit for this portion.**

First, I would conduct a site survey. This would help me determine proper access point placement. I will need to know how many access points I need, where they need to be placed, and how they need to be configured. After the site survey is done, I will need to choose the equipment. This is going to need to be equipment especially designed for offices and businesses where a lot of devices will need to be connected. I would go with commercial grade equipment from Cisco. I am going to choose the Cisco Catalyst 9120 Series Access Points. They offer intelligence, resiliency, integrated security, and the benefits of the new, high-efficiency Wi-Fi 6 or 802.11ax standard. They cost about $1,130.00. Depending on the site survey, if I need more than 3 access points, I am also going to need a low maintenance on site cloud controller. This will help the access points communicate with one another. For this I would choose the Cisco Catalyst 9800. From what I found, this will be about $2,000. This can be deployed anywhere, it is built for all size corporations, and it has Cisco ETA and SD-access. For security I will need to choose switches, firewalls, and gateways. I would choose ones that are low-maintenance so that scaling isn't a problem. The Baracuda Cloudgen Firewall is top rated for business. Barracuda CloudGen Firewall is the ideal security and connectivity solution for multi-site enterprises with complex and dispersed network infrastructures. It's firewall technologies include; application profiling, intrusion prevention, web filtering, advanced threat and malware protection, antispam, and full-fledged network access control. Also, I would use a splash page to increase security. It acts as another layer of authentication. I would also want to use multiple SSIDs to manage the network and improve performance. Once, the site map is completed, I would work with Baracuda do figure out what we would need for the firewall. I am estimating this will be about $5,000 to $7,000. I would also use POE for access points. This is usually pretty affordable. This is also more cost effective than buying individual switches. PoE Switches

have a built-in Power over Ethernet injector to supply up to 100W Power over Ethernet (PoE) to standards-based and compliant devices such as wireless access points. The cost of these start at about $275.00 each.

Sources- https://www.madebywifi.com/blog/8-tips-setting-business-grade-wi-fi-network/

https://www.barracuda.com/products/cloudgenfirewall?utm_source=google&utm_medium=search_cpc&utm_campaign=2069419118&utm_adgroup=75518818479&utm_term=business%20firewalls&utm_position=1t2&utm_matchtype=e&utm_device=c&utm_content=367967673780&gclid=EAIaIQobChMIx86A3Zns5AIVx_7jBx2XpQuOEAAYAiAAEgJGfPD_BwE

https://www.secureitstore.com/C9120.asp

https://www.automationdirect.com/adc/overview/catalog/communications/industrial_ethernet_switches/unmanaged/poe?gclid=EAIaIQobChMI77i8upvs5AIVIv_jBx1I_AYHEAAYAiAAEgJp-_D_BwE#bodycontentppc

While gathering requirements, you will need to ask Mr. Wayne some questions. What kind of questions would you ask him when setting up this network? (5pts)

I would need to ask him how big the area is, what type of connectivity people will need who will be working in the area, and roughly how many devices a person would be connecting to the network. I would also need to know what type of furniture and structures will be present in the office.

What security measures would you place within the wireless network? Why? How would you test the security measures? (5pts)

I would use firewalls and SSIDs for sure. Firewalls help protect the network and add another layer of protection. Also, SSIDs helps maintain security because everyone is not using the same SSID. To test your Firewall you can do a probe and scan. Also, in the wireless network it is important to check the security settings menu. This is where you can check the SSID and determine the network uses. It is also important to make sure the encryption settings are selected and working.

Hint: To succeed with above scenario, you will need to apply the following when planning a network:

- Site Survey
- RF Considerations
- Organizational Needs
- Requirements (Business, User, ad Functional)
- Constraints
- Objectives

Wireshark Questions (8pts)

For this section, you will be analyzing the test-01.pcap file in Wireshark. If you are unable to access the file, please let the instructor know

1. What is the SSID for the base station? (1pt)]
   B4 00 b0 01 c0 33 5e 65 19 63 02 c0 ca 8d 70 2f

2. What is the vulnerability in this packet trace? What is the cause of this vulnerability? (2pts)
   The data is not protected

3. What is the MAC address for the device that is able to authenticate the SSID successfully? (1pt)
   02:c0:ca:8d:70:2f

4. What is the Wireshark filter to display the beacon frame? How many frames you see after running the filter? (2pts)
   wlan[0] != 0x80 and I see 1 frame

5. What channel is being used for the wireless router connection? (1pt)
   Channel 1

6. Go to frame 78. What is the full device name for the wireless router? (1pt)

   BelkIn_d7:95:1e

Short Answer (17pts)

1. What is DWALL? When would you use DWALL? When would you use SSLstrip? What are some countermeasures in preventing successful attacks with these tools? (4pts) I would use an SSLstrip to do an attack without the person realizing it and to get around the SSL certificates on HTTPS enabled websites. To prevent this type of attack enabling HTTPS on all webpages is a good thing and implementing a policy where a webpage won't open unless it uses HTTPS.

2. Name and explain a social engineering attack that is used within a ***wireless network*** (1pt)

Phishing is a social engineering attack that is used within a wireless network by obtaining personal information by using link shorteners or embedded links to redirect users to suspicious websites. Then, the attacker can get malware downloaded by the victim and this gives them access to the information that they want.

3. Explain EAP-TLS (2pt)

It is an authentication protocol used in network and internet connections. It is the original standard wireless LAN EAP authentication protocol.

4. List and explain three uses for a WiFi Pineapple (3pts)

Audit a wireless network, hack a wireless network, act as a hotspot imposter where it looks like you are connected to the internet that you have been connected to before, but you are not.

5. What is the difference between active scanning and passive scanning? (1pt)

Active scanning is when a client radio transmits a probe request and listens for a probe response from an AP. Passive scanning is when the client radio listens on each channel for beacons sent periodically by an AP.

6. How does 802.11a differ from 802.11n? (2pt)

802.11a uses 5Ghz Frequency Band, has 54 Mbit/sec data transfer rate, nly 90 foot range. It is also not as prone to interference as others. 802.11n supports maximum data rate 100 Mbit/sec and uses Multiple Input Multiple Output. It can also use both 2.4 and 5Ghz bands.

7. What are the two types of probe requests? (1pt)

The two types of probe requests are requests and responses

8. Give an example of 2-factor authentication (1pt)

When you type in your credit card information you must type in your zip code too

9. What is WiFi 6? List an example of a wireless router that is WiFi 6 capable. (1pt)

WiFi 6 is new and it includes higher data rates, increased capacity, better in environments with a lot of connected devices, and an improvement in power efficiency. It is basically the newest generation of WiFi connectivity. The new Google Wifi system is WiFi 6 capable.

10. Why should an enterprise use an wireless IPS, such as Extreme AirDefense, in their wireless network? (1pt)

Wireless IPS prevents unauthorized network access to local area networks and can be used with Wireless LAN infrastructure. It stands for intrusion prevention system, and that is what it does. It compares MAC addresses of all wireless access points on the network and can spot if there is a discrepancy and then it will make an alert.