**Getting Started Task 2 Template**

Use the template outline below to capture the rubric requirements and key points and to serve as your task report. After you have captured the appropriate data, massage each section into the required number of paragraphs and ensure you have captured all the required points highlighted.

**A. WLAN Vulnerabilities**

**First vulnerability for WLAN**

Evil Twin - "An evil twin attack is a spoofing cyberattack that tricks a user into connecting to a fake Wi-Fi access point that mimics a legitimate network". (Panda Security, Many Evil Twin attacks involve a captive portal, designed to mimic the captive portal login page of the original WLAN. This allows malicious attackers to harvest credentials. When an Evil Twin attack is used on a corporate WLAN the attacker is able to harvest domain credentials, they are also able to monitor traffic that is being passed through the Evil Twin.

**Second vulnerability for WLN**

Denial of Service (DoS) – “WLAN and mobile networks are vulnerable to both network-based DoS attacks and those created specifically to attack the inherent weaknesses of radio-based systems”. (Doherty, 2021) A denial of service can quickly bring an organization to a stop and prevent them from conducting business.

**B Mobile Vulnerabilities**

**First vulnerability for Mobile devices**

Wireless Phishing – “Phishing involves sending fame emails or SMS messages to a target in an attempt to get the victim to click a link that will take them to a fraudulent website”. (Doherty, 2021) Mobile phishing has been increasingly beneficial for attackers as URL obfuscation and shortening are increasingly difficult to detect. Due to the smaller screen size on phones users are less likely to scrutinize the full URL prior to clicking on links. This is quickly exacerbated by an organization with a B.Y.O.D cellular policy due to inconsistent mail application usage, spam filtering, and general lack of reliance on enterprise email security products generally used on an organizations network.

**Second vulnerability for Mobile devices**

Browser Exploits – “Specifically targeting mobile users, these exploits take advantage of vulnerabilities on mobile web browsers”. (Doherty, 2021) Increasingly difficult to protect against in an organization that follows a B.Y.O.D cellular policy. Less ability to manage updates or mandate an update schedule. This leaves mobile users vulnerable to exploitation by simply just visiting an unsafe site.

**C. Mitigation**

**First Mitigation for WLAN**

And steps, tools, and documentation (citation)

Evil Twin

To mitigate against an Evil Twin attack businesses that provide Wi-Fi to their employees and customer are advised to implement a “Wireless Intrusion Prevention System” (WIPS). This will assist in detecting the presence of an evil twin access point and significantly reduce any managed devices from connecting to one. (Orsi, 2018). An example of a WIPS is WatchGuard, which has a variety of methods for configuration, including acting as a hybrid access point and monitoring sensor at the same time. documentation and configuration can be found on the Guardsite website. (Watchguard, 2022)

**Second Mitigation WLAN**

And steps, tools, and documentation

Denial of Service

To mitigate the risk of a denial of service attack the SANS institute recommends that organizations deploy a WLAN Intrusion Detection System (WIDS). This intrusion detection system can be leveraged for logging and alerting however does not have the capability of stopping the attack. To further mitigate against denial-of-service attacks it is highly recommended that organizations use three or more sensors appropriately placed to assist with triangulation methods, this will assist in detecting the source of transmission. (“2108.pdf On”)

**First Mitigation for Mobile devices**

And steps, tools, and documentation

Wireless Phishing

To mitigate the risk against phishing on mobile devices, an email security software such as Proofpoint, Cisco’s Iron Ports, or Symantec’s Email Security.Cloud is recommended. Tools such as these are designed to perform advanced scanning of emails prior to delivery through the email systems. The further configuration of DKIM, SPF, and DMARC all play a vital role in reducing the number of malicious emails delivered to end users. In addition to reducing the over-all quantity of malicious emails, these services tend to offer a real-time scanner of links that are included in the in the emails. These tools can be configured to utilize a content engine, block/allow lists, and RBL checking. Proofpoint uses an advanced AI and Machine learning detection engine named “Advanced BEC Defense”, this detection engine analyzes multiple message attributes such as; message headers, sender IP addressing, and message body, applying logic to determine if the email is a threat. (“Email Protection - Email Security Solutions | Proofpoint US”)

**Second Mitigation for Mobile devices**

And steps, tools, and documentation

Browser Exploits

To mitigate the impact of browser exploits it is recommended that all servers have been supplied with a digital certificate for SSL/TLS and enforce HTTPS instead of allowing HTTP. This ensures the connection is encrypted prior to any critical data being provided. It is also recommended that any device that is being used for corporate function is configured to block “pop-ups” as this is the primary vector of attack for browser exploitation. (Doherty, 2021) It is also recommended to remove any unused/unwanted application, to check application permissions, and practice due diligence.

**D. Preventative Measures**

**In this section, you need to list preventive measures that will increase the security posture of the WLAN and mobile environment. You need to list a preventative measure for EACH**

**Preventative Measure for WLAN**

Description of measure and narrative (NIST 800-153 has good info for this)

**Preventative Measure for Mobile environment**

Description of measure and narrative of preventative measure (NIST 1800-22 is a good source of information for this).

**Reference federal, state, or industry regulations that justify these measures.**

Here you must use a regulation to support your preventative measures. You can use any REGULATION from chapter 4 of the course material. **(NIST and ISOs are standards, not regulations, and will not suffice as such!!)**

PCI recommends WIPS ….

**E. Recommended BYOD Approach**

**First Recommendation**

Industry or academic research

**Second Recommendation**

Industry or academic research

NIST 1800-22 has some good guidance on the BYOD approach

**References**

In-text, citations must be in an acceptable format. I recommend APA, but you can use MLA or Chicago style as well.

Doherty, Jim. *Wireless and Mobile Device Security*, Jones & Bartlett Learning, LLC, 2021.*ProQuest Ebook Central*, https://ebookcentral.proquest.com/lib/westerngovernors-ebooks/detail.action?docID=6461875.

Orsi, Ryan. “Understanding Evil Twin AP Attacks and How to Prevent Them.” *Dark Reading*, 14 Nov. 2018, [www.darkreading.com/attacks-breaches/understanding-evil-twin-ap-attacks-and-how-to-prevent-them](http://www.darkreading.com/attacks-breaches/understanding-evil-twin-ap-attacks-and-how-to-prevent-them).

*WatchGuard Wireless Intrusion Prevention System (WIPS)*. www.guardsite.com/WIPS.asp. Accessed 25 Sept. 2022.

“2108.pdf On.” *Egnyte*, sansorg.egnyte.com/dl/zdm4VXjMja. Accessed 25 Sept. 2022.

“Email Protection - Email Security Solutions | Proofpoint US.” *Proofpoint*, 9 Sept. 2022, www.proofpoint.com/us/products/email-security-and-protection.