**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**

1. 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**

1. 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**

Evil Twin mitigation

* One of the preferred mitigation steps against an Evil Twin attack is to configure all mobile users to use a VPN. VPNs were designed to prevent monitoring and keep traffic secure. This provides a layer of security even in the event a mobile user does connect to an Evil Twin.
* Continuous monitoring of WLAN for both attacks and vulnerability
* Conduct regular assessments to evaluate the overall security of the WLAN

**Second Mitigation WLAN**

Denial of Service

* Enable DoS protection – This allows for thresholds to be set for specific types of traffic, upon reaching said thresholds, the WLAN device can take an action such as block listing the attacking address. (TP-Link,)
* Deploy a Wireless Intrusion Preventions System (WIPS) or a Wireless Intrusion Detection System (WIDS).

**First Mitigation for Mobile devices**

Malicious Applications (Malware)

* Prohibit Jailbreaking / Rooting of mobile devices
* Police third-party downloads
* Stored data encryption
* Mobile Application Management (MAM)
* Mobile Device Management (MDM)

**Second Mitigation for Mobile devices**

Browser Exploits

* Due Diligence / Training
* Only use HTTPS
* Anti-Virus
* App Permissions

**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**

**Denial of Service**

* Conduct regular assessments to evaluate the overall security of the WLAN
* Use semi-directional antennas, this will decrease the overall footprint and contain the signal to the building. For the patio, it

**Evil Twin**

* SSID Cloaking, this will prevent the SSID from being broadcast. Making the SSID of the WLAN more difficult to mimic.
* VPN over wireless, this ensures data encryption in the event of accidentally connecting to an Evil Twin.
* Disable the auto connect feature in the settings on mobile devices
* Always use a VPN, an example being Global Protect VPN from Palo Alto Networks, this ensures all traffic that is configured to traverse the VPN is encrypted.

**Preventative Measure for Mobile environment**

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

Malware – Mobile Application Management (MAM)

* Restrict access to devices that have circumvented security by “Jailbreaking” or “Rooting” a device.
* Implement Mobile Device Management with a software gateway for users to install “trusted” applications.

Brower Exploits

* Mobile Device Management (MDM)
* Restrict access to devices that have circumvented security by “Jailbreaking” or “Rooting” a device.
* Stored Data Encryption

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

PII – The Gramm-Leach-Bliley Act (GLBA), enacted in 1999 is to secure and protect personally identifiable information (Doherty, J. (2021))

Personal Data – General Data Protection Regulation (GDPR) and California Customer Privacy Act (CCPA) (Doherty, J. (2021))

**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.

1. Panda Security - Evil Twin - https://www.pandasecurity.com/en/mediacenter/security/what-is-an-evil-twin-attack/

2. Wireless and Mobile Device Security - 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>.

3. TP-LINK DoS Protection <https://www.tp-link.com/us/support/faq/2658/>

4. Doherty, J. (2021). Wireless and mobile device security. Jones & Bartlett Learning, LLC.