**Strategies for Network Security Management Use of Honeypot/Honeynet**

Student name

Institutional affiliation

Course number and name

Instructor’s name

**Strategies for Network Security Management Use of Honeypot/Honeynet**

A honeypot is a system that is always set up as a decoy within a network system to lure cyber attackers, detect and deflecting attacks into the information system (Seungjin et al., 2020). It represents itself within the network as a potential weak point vulnerable to attacks. It behaves like a server within the system primarily to gather information and update the defenders through notifications of any system-attack attempts (Seungjin et al., 2020). Honey applies hardened operating systems with additional security layers to reduce the chances of attack and exposure to threats and attackers. The primary purpose of honeypots is to capture information from unauthorized intruders by appearing as legitimate systems (Seungjin et al., 2020). They provide traps necessary for beefing systems security and network defenses against cyber-attacks.

Honeypot operation combines data, computers, and applications with the ability to simulate a real system attribute perceived by attackers as real targets (Seungjin et al., 2020). The system is always placed at the demilitarized zone on the network to ensure it is isolated from the main production network; however, the system remains part of the system isolated and closely monitored (Seungjin et al., 2020). To detect breaches through the internet, a honeypot may be put outside facing the internet outside the external firewall to detect attempted attacks within the internal network.

Honeypot allows analysis through viewing and logging into the system to view and study threat levels. The logs help identify types of threats a network infrastructure is exposed to while protecting the real assets from threats by distracting attackers (Seungjin et al., 2020). The system is also hosted in a virtual machine so that in case it is compromised; it can be quickly recreated. An example of honeypot works by responding to the server message block protocol requests used by WannaCry ransomware attacks. The system will appear as the serve or an enterprise database loaded with information being sort for by the attackers.

One of the limitations of using honeypot is that it is expensive to maintain; hence it is used primarily by research companies or large enterprises dealing in cybersecurity (Haseeb et al., 2020). Within such an organization, the honeypot system helps identify and defend information systems from advanced persistent threats. Cybercriminals can also use honeypots to gather intelligence and hijack the system and use them against the organization.

**Reference**

Seungjin, L., Abdullah, A., & Jhanjhi, N. Z. (2020). A review on honeypot-based botnet detection models for smart factory. *International Journal of Advanced Computer Science and Applications*, *11*(6), 418-435.

Haseeb, J., Mansoori, M., & Welch, I. (2020, December). A Measurement Study of IoT-Based Attacks Using IoT Kill Chain. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 557-567). IEEE.