RICO, JUSTROILON C.
BSIT - IT42S2 - PRELIM
CBS 404A-IT42S2 - Cyber Threat Analysis and Modeling

Objective: Research sample scenario that uses wireshark for hacking/reconnaissance.

Steps.:

1. Conduct research on hacking incidents or ethical hacking practices involving the use of Wireshark.

In a legal scenario, a network administrator utilizes Wireshark to troubleshoot connectivity issues within their organization's network. Users have reported intermittent internet loss and sluggish network speeds. Launching Wireshark on a mirrored port of the network switch, the administrator captures packets flowing through the network. Analysis reveals a surge in broadcast traffic from a specific subnet. Further investigation uncovers a misconfigured device generating excessive ARP requests, flooding the network and causing congestion. By identifying and isolating the misconfigured device, the administrator resolves connectivity issues and optimizes network performance, ensuring smooth operations. This exemplifies Wireshark's legitimate use as a network troubleshooting tool for diagnosing and resolving network problems within an organization.

2. Seek pertinent information related to the incidents or hacking practices.

To gather pertinent information related to incidents or hacking practices using Wireshark, analysts focus on detecting anomalies within captured network traffic. This involves scrutinizing traffic patterns for unusual spikes in data volume, unexpected protocol usage, or suspicious source-destination pairs. Additionally, analysts examine packet payloads to identify signs of malicious activity, such as malware signatures or unauthorized file transfers. They also monitor for reconnaissance activities like port scans or enumeration attempts, which may indicate potential threats. By correlating findings with known hacking techniques and incident response procedures, analysts can effectively detect unauthorized access attempts, identify indicators of compromise, and mitigate security risks within the network infrastructure.

3. Examine and offer a concise overview of the conducted incident or hacking practice, along with insights on preventive measures to avoid recurrence.

The incident involved a sophisticated phishing attack aimed at employees via deceptive emails containing harmful attachments. Upon opening these attachments, they executed code, establishing a hidden connection to a command-and-control server, enabling attackers to breach the organization's network undetected. To prevent a recurrence, it's vital to implement comprehensive security measures, including robust email filtering to intercept phishing attempts, regular security training to educate employees on phishing dangers, and endpoint protection solutions to identify and prevent malicious activities. Moreover, enforcing network segmentation and access controls can restrict lateral movement by attackers. Continuous monitoring and sharing threat intelligence can further bolster detection capabilities, facilitating a prompt response to emerging threats and reducing the impact of future incidents.