Memo For Count Viktor Thunderclaw

Date: 5/6/2024

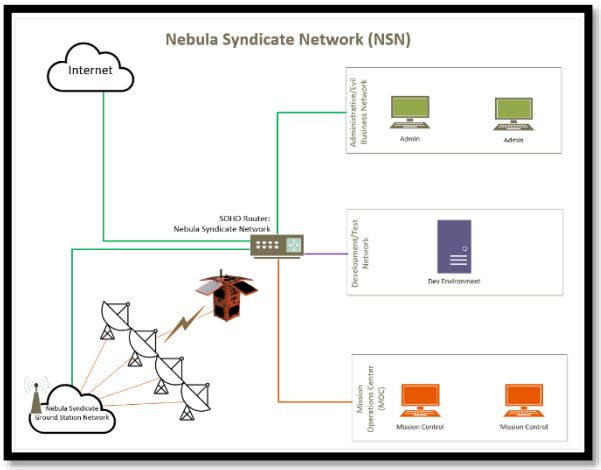
Subject: Nebula Syndicate Network, how to make it more secure and do other things gooder too… meeting minutes

Network administrators have expressed concerns about the security posture of the Nebula Syndicate Network (NSN). This meeting was an airing of grievances by the overwork and underappreciated team of network admins and IT security team members.

1. Internet Connectivity:
    a. While the NSN's connection to the internet is protected by a SOHO router with a firewall capability, no one is maintaining it or monitoring the logs or alerts. The exact posture of the firewall rules are unknown. A fear exists that some rules may leave large parts of the internal NSN accessible from the public Internet.
2. Lack of Internal Network Segmentation and Security:
    a. The Development Network, used to develop the software for the Space Laser, is directly accessible to the Internet through the SOHO router – with no additional network security or segmentation. Furthermore, several sensitive DevSecOps platforms are accessible from the Internet and use default security settings and have anonymous access for viewing and downloading files, specifically the Nexus Repo: **IP 44.205.120.122**, if someone were to NMAP that IP address they would learn some interesting things.
    b. That same SOHO router, in a flat topology, connects the Administrative/Evil Business Network, Development/Test Network, and the Mission Operations Center that manages the Nebula Syndicate Ground Station Network. The administrative level and mission control components connected to the Internet need robust firewalling and intrusion detection systems to mitigate these risks.
3. Data Encryption:
    a. There are several parts of the network that do not use secure protocols. TELNET is heavily used throughout the network specifically in the Nebula Syndicate Ground Station Network. Administrators have even seen FTP used.
4. Mission Operations Center (MOC):
    a. Mission Control Security: The mission control systems are critical and should be protected with strict access controls, rigorous authentication processes, and physical security measures to prevent any unauthorized access. Currently, accounts are shared between users and weak passwords are used.
5. MOC and Ground Station Physical Security:
    a. All the funds allocated for physical security at the MOC and the four ground station locations were diverted to the development of the Space Laser. Beyond

the basic locks installed on manufacturer-provided doors and standard etched keys, no additional measures have been implemented to safeguard against tampering, sabotage, and unauthorized physical access.

6. Network Monitoring:
    a. The MOC and the rest of the NSN lacks continuous monitoring of the network for unusual activities or anomalies. The IT Security team is unable to detect and respond to potential security threats promptly.
7. Space Laser Communication Links:
    a. The radio frequency (RF) links between the ground station antenna and the Space Laser Satellite currently operate without encryption. This means that the bulk transmissions from the ground station to the satellite are unencrypted. While the traffic within the RF signal could use encryption, this is also lacking. It is essential to implement encryption measures to safeguard these communications against potential eavesdropping.
    b. There is no authentication mechanism in place for messages sent to the Space Laser Satellite. This oversight leaves the system vulnerable to replay attacks, where a sophisticated attacker could capture and retransmit communications to compromise satellite operations.
    c. The absence of command sequence tracking in the system's operations is a significant concern. Implementing command sequence tracking would alert satellite operators to any anomalies in the sequence numbers, such as out-of-order commands, which could indicate malicious interference with the satellite.
    d. The CCSDS Space Packet Protocol, which is currently used for the link, supports an extension known as the Space Data Link Security Protocol. This extension could be effectively utilized to enhance the security of the traffic between the ground station and the satellite, thereby mitigating the identified vulnerabilities. This protocol can both encrypt and authenticate the space packets.



ct3_flag_6265747465727365637572657965F75726769747265706F73