Vulnerability Scanning with OpenVAS

TASK-2

JULY 7, 2024

HAFIZ NAVEED UDDIN,
(KAIRIZ CYBER TECHNOLOGIES (SMC-PRIVATE LTD)

To begin with, I installed OpenVAS on Kali Linux using the command `sudo apt-get install OpenVAS`. Once installed, I initialized OpenVAS using `sudo OpenVAS-setup`. For enhanced security, I created an administrative user with the username and password both set to "ADMIN" for the OpenVAS web interface. Following setup, I accessed the OpenVAS web interface via the URL: https://127.0.0.1:9392/.

In the configuration phase, I defined a target with specific details including its IP address and name. The target's IP address was 192.168.133.1, and I specified Port Ranges (841) among other parameters such as User Tags (0) and Permissions (2).

The OpenVAS version used was 20200827, and the scan configuration involved checking 5836 ports in total, all of which were TCP ports. No UDP ports were specified for scanning. This configuration was tailored for the "Lab Network" environment.

Subsequently, I proceeded to create a new scanning task named "Lab Network Scan" specifically designed to assess vulnerabilities within the network. After initiating the scan, I obtained a comprehensive vulnerability report detailing potential security issues identified during the scan process. Additionally, the report included detailed insights spread across multiple pages, highlighting critical findings and recommendations for further security enhancements.