Problem title: Automated Vulnerability Assessment and Penetration Testing tool for CCTV cameras & DVRs

Description:

Background
The widespread use of CCTV cameras, especially in critical sectors and strategic locations, creates a large attack surface for threat actors. Existing Vulnerability Assessment and Penetration Testing framework/tools are not specific for analyzing a global network of CCTV cameras and DVR systems. The lack of automated tools for Vulnerability Assessment and Penetration Testing in this domain poses a significant security risk. Therefore, there is a requirement of Automated Vulnerability Assessment and Penetration Testing tool specific for CCTV cameras.

Description
Develop a comprehensive framework for automated Vulnerability Assessment and Penetration Testing of CCTV cameras and DVRs. This framework should integrate various techniques, including:

- (a) Vulnerability Scanning: Employing tools like Nmap and Shodan to identify publicly exposed cameras and their vulnerabilities.
- (b) Penetration Testing: Simulating attacks to assess the effectiveness of security measures and identify potential attack vectors.
- (c) Machine Learning: Utilizing machine learning algorithms to analyze large datasets of camera configurations and network traffic for anomaly detection and vulnerability prediction.
- (d) Scalable: The framework should be scalable and adaptable to different camera and DVR models and network configurations.

Expected Solution
Following major outputs are expected from the proposed framework/tool:

- (a) A scalable tool/software for Automated Vulnerability Assessment and Penetration Testing of CCTV cameras and DVRs.
- (b) Dashboard to show details of all discovered CCTV camera & DVRs worldwide, their locations (based on IPs or any other info from CCTV/DVRs) and other technical parameters and statistics.
- (c) Should able to gather data on CCTV camera like make & models, firmware versions, network configurations, and mapping with publicly disclosed vulnerabilities (e.g., using CVE database).
- (d) Capability to scan the specific CCTV cameras based on IP range, make & model etc. globally.
- (e) A Machine Learning (ML) model for identification and classification of common vulnerabilities in different types of CCTV cameras and DVR systems. ML Model should be able to link vulnerabilities with its CVEs and possible steps wise exploitation methodology.
- (f) Machine Learning (ML) model will also linked with a set of recommendations for mitigating the identified security vulnerabilities/ risks.
- (g) Tool/software should be user friendly by security professionals to proactively assess and improve the security of CCTV camera and DVR systems.