



HWG Sababa

Progetto SCADAsploit

Sintesi del Progetto

Il progetto **SCADAsploit** nasce dall'esigenza di avere uno strumento molto flessibile e potente durante le operazioni di **Adversary Simulation e Penetration Testing in ambiente ICS** (Industrial Control System – sistemi di automazione per il controllo della produzione).

Il progetto SCADAsploit si pone come obiettivo il fornire una piattaforma per eseguire **attività di ricerca cyber sui dispositivi PLC** (Programmable Logic Controller – sistema di controllo e gestione degli impianti di automazione industriale) dei principali vendor, finalizzate a individuare e risolvere problemi di sicurezza cibernetica nel mondo delle infrastrutture critiche. La tecnologia implementata prevede lo sviluppo di moduli di auto-apprendimento basati su algoritmi di Machine Learning, che favoriscano ed accelerino l'individuazione di vulnerabilità e falle nella sicurezza dei sistemi industriali analizzati.

Risultati attesi

- Coprire l'attuale mancanza di strumenti mirati alla ricerca e penetration testing in ambito ICS;
- Realizzare una piattaforma modulare, flessibile, facilmente espandibile e aggiornabile;



- Agevolare le fasi di messa in sicurezza delle infrastrutture critiche e dei siti di produzione

SCADAexploit sarà la **base tecnologica** verso cui far convergere gli **strumenti di ricerca, analisi, risoluzione di vulnerabilità e debolezze cibernetiche di HWG Sababa**.

Sarà utilizzata anche per coprire altri settori oltre a quello ICS, come nel caso dell'Automotive (analisi delle centraline elettroniche ECU) e dell'IoT (Internet of Things) integrandosi perfettamente con il progetto SPAT (HWG Sababa Portable Automotive Testbed).





HWG Sababa

Progetto TESTBED

Sintesi del Progetto

Il progetto definisce le linee guida per la realizzazione del prodotto “**HWG Sababa Portable Automotive Testbed**” (SPAT).

SATP è un **laboratorio di test portatile ed espandibile per eseguire test di cyber security**. Si tratta di una sorta di laboratorio all’interno di una valigia molto robusta (es. Peli Cases), che al suo interno include la principale elettronica tipica di un veicolo come HeadUnit, ECU, TCU, Car Gateway, rete CAN, sensoristica.

Grazie a questo strumento gli specialisti di sicurezza saranno in grado di **simulare test di sicurezza** sui veicoli, su componenti dei veicoli e sull’infrastruttura a supporto, senza la necessità di avere a disposizioni il veicolo stesso.

Funzionalità

