Work Log: Code Explanation

File: logsql.py

Denne filen inneholder funksjoner for å logge SQL-forespørsler i systemet. Den hjelper med å samle og organisere databasehendelser for analyse.

File: settings.py

Denne filen inneholder konfigurasjonsinnstillinger for Dionaea-honeypot. Her kan brukeren tilpasse oppsettet for å overvåke nettverkstrafikk.

File: csv2sqlite.py

Denne skriptet konverterer CSV-filer til SQLite-databaser, som er nyttig for å analysere store datamengder raskt.

File: gnuplotsql.py

Dette skriptet bruker Gnuplot for å lage grafer fra SQL-databaser. Data kan visualiseres for enkel analyse av nettverkshendelser.

File: logsql2postgres.py

Dette skriptet migrerer SQL-loggfiler til en PostgreSQL-database, noe som gir bedre skalerbarhet og ytelse.

File: readlogsqltree.py

Dette verktøyet leser SQL-loggfiler og presenterer dem i en trestruktur for bedre oversikt over hierarkiske data.

File: retry.py

Skriptet inneholder en funksjon for å håndtere mislykkede operasjoner og prøve dem på nytt, noe som gjør systemet mer robust.

File: updateccs.py

Denne filen oppdaterer Command and Control (C&C)-innstillinger, sannsynligvis for honeypot-analyse.

File: pg_backend.py

Dette er en backend-fil for PostgreSQL. Den håndterer interaksjoner mellom honeypot-logger og PostgreSQL-databasen.

File: conpot.singlelogline.py

Logger individuelle hendelser fra Conpot-honeypoten, en SCADA/ICS-simulator.

File: dionaea-singlelogline.py

Logger enkeltstående hendelser fra Dionaea-honeypoten, som fanger malware og analyserer angrep.

File: glastopf-singlelogline.py

Logger hendelser fra Glastopf-honeypoten, som er fokusert på webangrep og HTTP-feller.

File: query_ELK.py

Dette skriptet utfører søk i ELK-stacken (Elasticsearch, Logstash, Kibana) for å hente logganalyser og visualisering.

File: inspect-to-csv.py

Konverterer inspeksjonslogger til CSV-filer, noe som gjør det lettere å analysere og dele data.