CAZ-IDS

Research, Goals, Milestones und Schedule

Ziele

- Ping Demo
 - Einfache Erkennung auf Basis von Pakettyp
- Datenanalyse
 - Dimensionsreduktion der Realdaten
- Anomalie-Erkennung im Datenfluss eines Netzwerks
 - Angriffserkennung mit Hilfe von Klassifikation des gesamten Netzwerkverkehrs

Schedule

Datum	Details
25.03	Anomalie-Melde-Interface definieren
01.04	Lesen vom Mirror-Port, (Golf 7) Realdaten analysieren
08.04	Reserviert - Training
15.04	Erkennen und Loggen von anomalen Paketen, Struktur der Analyseengine
29.04	Integration Test Demo, Anomalie melden über API, Verifikation der Analyseengine (Testangriffe)
06.05	Milestone 2 – Ping Demo, Ergebnispräsentation
13.05	Verknüpfung von Ping-Demo-Anwend. mit der Analyseengine zum IDS
20.05	Integration Test SDN u. IDS, Optimierung des IDS
27.05	
03.06	Milestone 3 – Ergebnispräsentation d. Release Candidate
11.06	User-IF und Simulationsanwendung, Analyseengine für Demo anpassen, Clientprogramm mit Angriffsmöglichkeiten
17.06	
24.06	Milestone 4 – Finale Präsentation

Links

- https://gitlab.informatik.haw-hamburg.de/acg157/po_caz_ids/