Seminar Session 4: Evaluation exercise

Informations about assessments → Assessment deadline is on 21.12.2021 (Peer Review & Design Document)

Christmas Break: 21.12.2021-10.01.2022

Collaborative Discussion is going good and comes to an end.

Outline:

- Announcements (so above)
- Cyber Kill Chain
- Exercise: Software Evaluation
- Q&A

Cyber Kill Chain:

by Lockheed Martin

Widely adopted

Adv PT e.g. solarwinds

➔ main goal is to catch an attack in the kill chain as early as possible.

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploration
5. Installation
6. Command & Control
7. Actions on Objectives

Detect	Deny	Disrupt	Degrade	Deceive
Web analystics	Firewall ACL			
NIDS	NIPS			
Vigilant User	Proxy filter	Inline AV	Email Queuing	
HIDS	Vendor Patch	EMET,DEP		
HIDS		AV		
NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect
Audit log			Quality of Service throttle	Honeypot

Diamond model → the goal is to increase checkpoints and make sure that secure systems accomplish. → Further research for diamond model

Diamond model of intrusion → categorize security incidents

Exercise: Rating of the 8 penetration testing tools

Group 3:

Best tool: OWASP ZAP(~14%)

worst tool: Jawfish(~7%)

- ➔ Quite equal rating of nearly all tools (~13%)
- ➔ Active analysation of the tools/ virtual machine implementation

Group 1 (own group):

- ➔ Nearly same results like group 3 in general

Best tool: Kali Linux

worst tool: Jawfish