

Solutions

Exercises 1st Semester

Exercise 1.1 (Attacker Stereotypes)

Name	Characteristics / Motivation	Danger
Script Kiddie	Bragging rights & wreaking havoc	💀
Hacktivists	(Pseudo-)political & social goals	💀 💀
Competitors	Defamation & industrial espionage	💀 💀
Organized Crime	Monetization, e.g. extortion & fraud (Providing Cyber-Crime-as-a-Service)	💀 💀 (💀)
Evil Employees	Revenge & corruption Dangerous insider knowledge	💀 💀 💀
Nation States	Power! Unlimited resources & budget	💀x100

Exercise 2.1 (Threats to Security Goals)

Threat	C	I	A
Network Sniffing	✓		
DDoS Attack			✓
Rogue WiFi Access Point	✓	✓	
Electromagnetic Pulse (EMP)			✓
Whistleblower	✓		
Social Engineering	✓	✓	✓

Exercise 2.2 (CIA³ Measures)

Security Goal	Technical Measures	Organizational Measures
Confidentiality	e.g. AES/RSA, HTTPS, Tor , 2FA	e.g. Anonymous Payment Systems, Access Restrictions, Data Classification
Integrity	e.g. SHA2, HSTS, MACs, PGP/GPG, Blockchain	e.g. Version Control, Access Logs
Availability	e.g. Load Balancer, Circuit Breaker Pattern , Heartbeat Monitoring, RAID	e.g. 24/7 Support, On-Call-Duty, SLAs

Security Goal	Technical Measures	Organizational Measures
Accountability	!?	e.g. Security Policies, Risk Assessments, RACI Matrix, Segregation of Duties
Assurance	e.g. Vulnerability Scanner	e.g. KPIs, Customer/Supplier Audits, Penetration Test, Red Team

