cphbusiness

COPENHAGEN BUSINESS ACADEMY

Security, Spring 2019

Outline

- Intro to the course
  - Background of students and teachers
  - Overview of the semester and materials
- Prevention, Detection, Response
- OWASP
- Firewalls
- Exercises for today and for week 3 (13/2)
- Recab of some Linux things
  - grep, sort, uniq
  - users, user rights, and groups

Background

- Lars Mortensen
  - lam@cphbusiness.dk
- Anders Kalhauge
  - aka@cphbusiness.dk
  - 21 72 44 11

- You?

- Materials at link via Moodle – bookmark it!

  https://github.com/securitydatspring2019/main

The course

- OWASP as backbone
- InfoSecurity as inspiration
  - Please register one of these days – it's free
- See one, Do one, Teach one
- IT Seminar as challenge

https://www.it-seminar.info

The aspects of Security

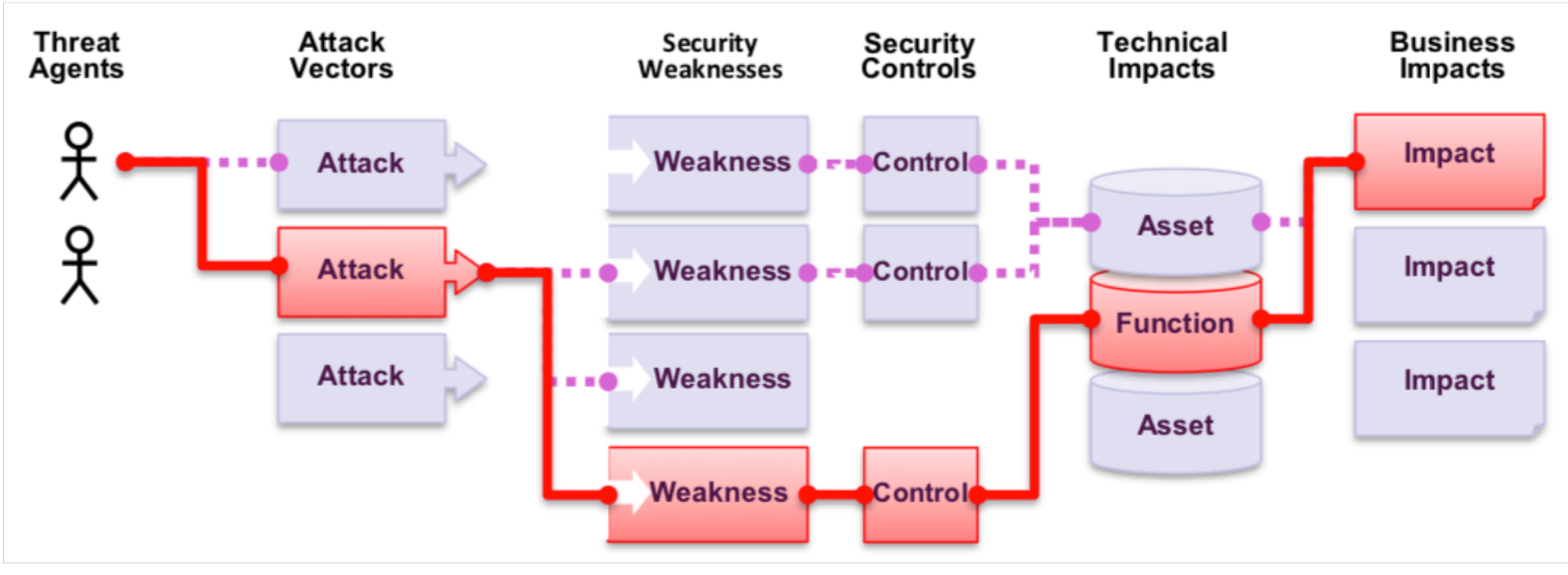
- Prevention
- Detection
- Response / Recovery

- The main part of the course will be about Prevention
- This week will have its focus on Detection

OWASP top 10, 2013 & 2017

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Threat -> impact



OWASP Risk Rating Methodology

information about:

- the threat agent involved,
- the attack that will be used,
- the vulnerability involved, and
- the impact of a successful exploit on the business.

```
Risk = Likelihood * Impact
```

Threat Agent Factors

- **Skill level**. How technically skilled is this group of threat agents?
  - Security penetration skills (9), network and programming skills (6), advanced computer user (5), some technical skills (3), no technical skills (1)
- **Motive**. How motivated is this group of threat agents to find and exploit this vulnerability?
  - Low or no reward (1), possible reward (4), high reward (9)
- **Opportunity**. What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability?
  - Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)
- **Size**. How large is this group of threat agents?
  - Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

Vulnerability Factors

Estimate the likelihood of the particular vulnerability involved being discovered and exploited.

- **Ease of discovery**. How easy is it for this group of threat agents to discover this vulnerability?
  - Practically impossible (1), difficult (3), easy (7), automated tools available (9)
- **Ease of exploit**. How easy is it for this group of threat agents to actually exploit this vulnerability?
  - Theoretical (1), difficult (3), easy (5), automated tools available (9)
- **Awareness**. How well known is this vulnerability to this group of threat agents?
  - Unknown (1), hidden (4), obvious (6), public knowledge (9)
- **Intrusion detection**. How likely is an exploit to be detected? Active detection in application
  - (1), logged and reviewed (3), logged without review (8), not logged (9)

Technical Impact Factors

- **Loss of confidentiality**. How much data could be disclosed and how sensitive is it?
  - Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)
- **Loss of integrity**. How much data could be corrupted and how damaged is it?
  - Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9).
- **Loss of availability**. How much service could be lost and how vital is it?
  - Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)
- **Loss of accountability**. Are the threat agents' actions traceable to an individual?
  - Fully traceable (1), possibly traceable (7), completely anonymous (9)

Business Impact Factors

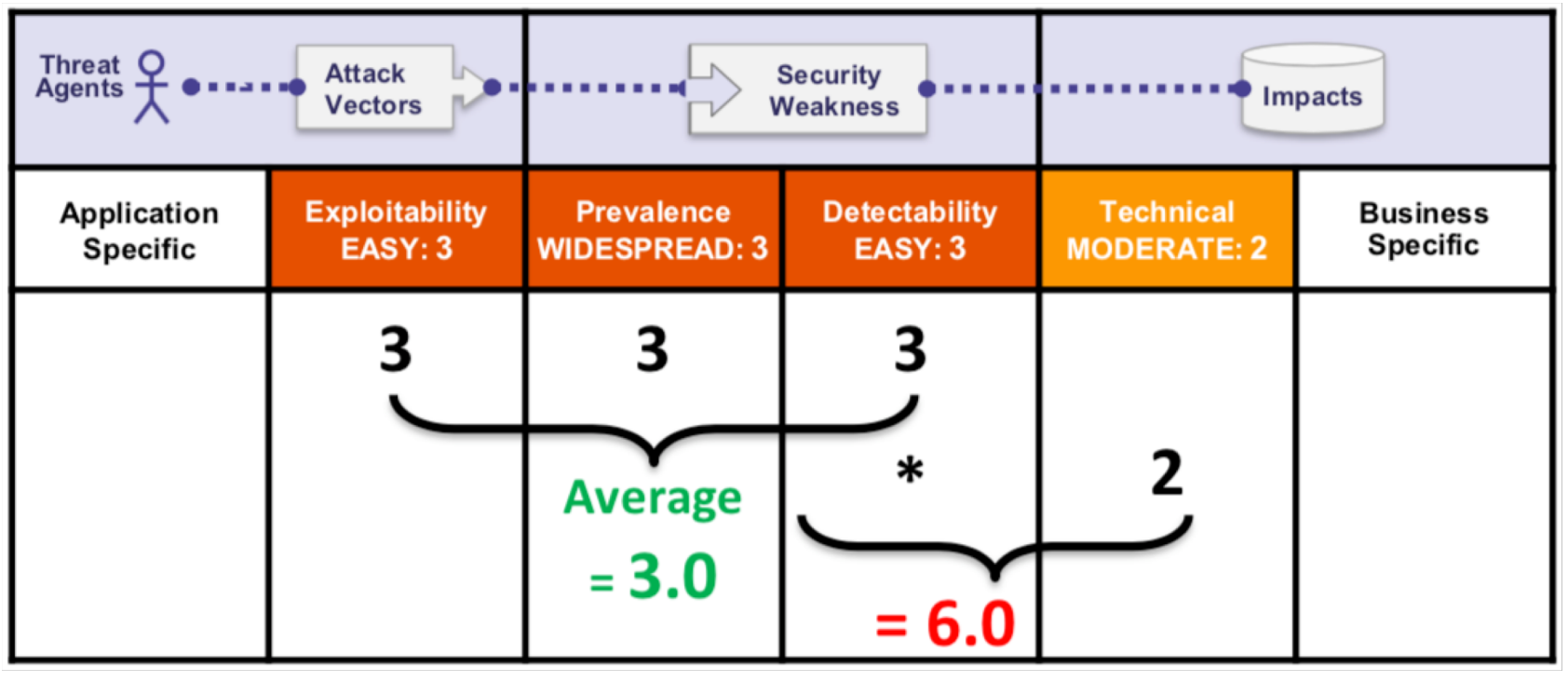
- **Financial damage**. How much financial damage will result from an exploit?
  - Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)
- **Reputation damage**. Would an exploit result in reputation damage that would harm the business?
  - Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)
- **Non-compliance**. How much exposure does non-compliance introduce?
  - Minor violation (2), clear violation (5), high profile violation (7)Privacy violation
- How much **personal**ly identifiable **information** could be disclosed?
  - One individual (3), hundreds of people (5), thousands of people (7), millions of people (9)

Determining Severity

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Ratings calculated



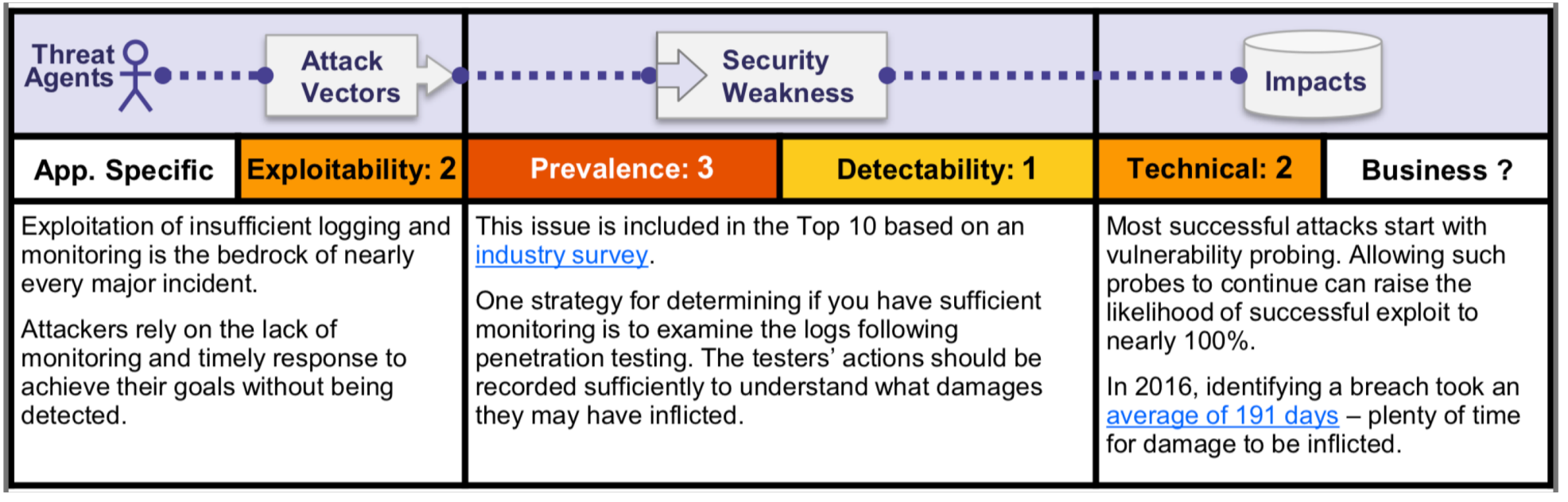
Ratings

RISK	Threat Agents	Attack Vectors: Exploitability	Security Weakness: Prevalence	Security Weakness: Detectability	Impacts: Technical	Impacts: Business	Score
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Detection

A10:2017-Insufficient Logging&Monitoring

(See page 16 of OWASP 2017)



Prevalence (*forekomst*): not from methodology, but from statistics OWASP has gathered from elsewhere

Two next exercises:

Solve these in pairs

Today:

- Firewalls – to see where we are attacked

Monday February 13th:

- Remote logging – logging to a remote server

Firewalls – what do we know?

- Where do we have them
- What are the components
- Do you need them
- Should you ever prevent outgoing traffic?