MUNI
FI

Asset Management

PA211 Advanced Topics of Cyber Security

September 20, 2022

Lukáš Sadlek, Jan Vykopal, and Pavel Čeleda

Exit tickets from last week – I

- **Q:** I will appreciate more information about **grading**.
- **A:** Minimum to **pass course > 50 pts** (i.e., 51+), based on **homeworks** (4x15pts) + final **exam** (40pts). Minimum to **pass exam >= 15 pts**.

  Grading is based on **ECTS grading scale** – **link**
  A – 95 and more
  B – 83
  C – 68
  D – 56
  E – 51 (at least 15 from exam)
  F – 50 and less

Exit tickets from last week – II

- **Q:** How many hours will homeworks take? Maybe also some more general information about homeworks.
- **A:** *HW is generally designed to take approx. **2 hours**, but exact spend time depends on **your skills** and **knowledge**. HW is a **follow-up** to your **seminar** activities.*

- **Q:** What is the purpose of ELK stack in activities we will do in the course and what we can do with it?
- **A:** *Visualization, analysis, import, **Elastic SIEM** (Security information and event management). ELK stack allows to **analyze** security **data**, supports their **import** and their formats (e.g., Windows Event Logs).*

Exit tickets from last week – III

- **Q:** Did you intentionally not add the user `vagrant` to the `docker` group on the `elk` machine? Is it a good security practice or you just omitted the post-installation docker steps for the sake of time?
- **A:** *Ability to run docker containers implies escalation of privileges, attack surface becomes larger* – see more on this topic.

```
sudo usermod -aG docker $USER
```

- **Q:** Is "shutting IT and starting again" really the only recommended solution to problems occurring? What should I look for in the logs?
- **A:** *This solution is suitable for our setup.*
  Look at open ports, find errors in logs, restart containers.

Goals of this lecture

- Become acquainted with
  - asset **management**
  - asset **inventory**
  - approaches for asset **discovery**
  - **standards** and **enumerations** for asset management

Essential terminology

CSIRT vs. SOC – I

- **CSIRT**
  - **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam
  - An **organizational unit** or a capability
  - Preventing, detecting, handling, and responding to **incidents**
  - Has a defined **constituency** and **mission**

MUNI
CSIRT-MU

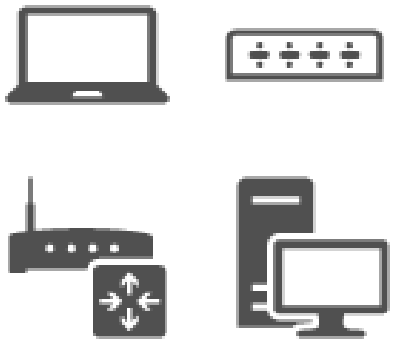
- **SOC**
  - **S**ecurity **O**perations **C**enter
  - A **centralized unit**
  - Ongoing monitoring and analyzes of an organization's **security posture**

CSIRT vs. SOC – II

- **Difference**
  - SOC usually **finds** potential security **incidents** in data, e.g., in logs
  - CSIRT **handles incidents** discovered by the SOC
- **Security operations**
  - Implementation of **IT services** in a **secure** way
  - Combine **security** and IT **operations** practices
- **Security operations management**
  - Collection of activities for **maintaining** organization's **security posture**
  - Activities process, e.g., **incidents, assets, vulnerabilities,** and **weaknesses**

IT asset

- An **item of value**
- Ensures achievement of organizational **mission** or **business objectives**
- **Examples**
  - **Tangible** (hardware, software, network device)
  - **Intangible** (information, data, reputation)



Asset management

- **IT asset management (ITAM)**
  - Provides an accurate account of technology **asset lifecycle costs** and risks
  - Maximizes the **business value** of technology strategy, funding, and contractual decisions
- **Cybersecurity asset management**
  - **Narrower** definition
  - Continuous process that discovers and **manages assets**
  - The purpose is **to protect them**, e.g., finding their potential risks
  - Focuses on **inventorying** assets, **mapping** their communication, and their **prioritization**
  - Focus of **this lecture**

Asset management in an organization – I

- Organization's **missions** supports strategic **objectives**
- **Service**
  - The **limited number of activities**
  - Carried out in the performance of a duty or in the production of a product
- **Asset**
  - **Material** that the service needs to operate

Asset management in an organization – II

- **Example of service**
  - **MUNI Unified Login** (`id.muni.cz`)
  - Provides a way to **sign into** several **web services** while ensuring security
- **Examples of assets**
  - **MUNI Unified Login** uses OIDC protocol
  - The scheme requires **authorization server**
  - Specific **application** issues client **tokens** and controls **access policies** to resources servers
  - Assets are **authorization server** and the **application**

IT assets

ISO 27005

- **Name:** Information technology – Security techniques – Information security risk management
- **Primary assets**
  - **Definition:** core processes/activities and information
  - **Examples:** offered services and their data
- **Secondary (supporting) assets**
  - **Definition:** assets that support primary assets
  - **Examples:** cables, routers, servers, human resources

CERT Resilience Management Model – I

- Created by **Software Engineering Institute** of Carnegie Mellon University
- Asset management is a **process areas** with four asset types
- **Information**
  - Collection of **data with value** for organization
  - **Examples:** emails, documents, and encryption keys

CERT Resilience Management Model – II

- **People**
  - People **execute** process and **monitor** it
  - **Examples:** employees and suppliers
- **Technologies**
  - Technological components **supporting** or automating **a service**
  - **Examples:** software, hardware, firmware, and cabling
- **Facilities**
  - **Places** where services are executed
  - Possibly owned by an **external partner**
  - **Examples:** office buildings, data centers, …

Asset inventory – I

- A list of organization's **assets** and their **details**
- **Content**
  - Technology, software, data, ...
  - IP address management (**IPAM**)
  - Location, function
  - Relationship to other assets (OS of a device, …)
- **Advantages**
  - Increases **productivity**, decreased costs
  - Easier **maintenance** of assets
  - **Tracking** and **recovering** assets

Asset inventory – II

- **Examples**
  - **Excel** sheet
  - **Netbox** asset inventory
  - **GLPI** asset inventory
  - **SolarWinds** SPCB (Server Performance and Configuration Bundle)

Asset discovery

Asset discovery – data sources – I

- **Passive network monitoring**
  - Observation of network traffic at the **observation point**
  - **IP flow:** a **set of packets** transmitted between source and destination **IP address** and **port** using specific **protocol** during some time window
  - **IP flow** and **packet** capture
- **Active network monitoring**
  - Information is obtained from actively sent **network probes**
  - Scanners send artificial requests to network services
  - **Network scanning**

Asset discovery – data sources – II

- **System and application logs**
  - System and applications store **messages** in log files
  - **Windows Event Logs** – record of **Windows system** and application notifications
  - **Syslog** – standard for message logging on **UNIX-like systems**

Asset discovery – use of agents

1) **Agent approach**
2) **Agentless approach**
   a) Passive network monitoring
   b) Active network monitoring

Agent approach

- **Agent**
  - A software **gathering information** from desktops, servers, mobile endpoints, and other devices
  - The information is transmitted to a **monitoring station**
  - Agents often track **logs** or obtain **system information**
  - Determines installed, removed, and updated **applications**
- **Examples**
  - Pakiti,
  - Solarwinds Asset Discovery
  - HP Asset Manager

Agentless approach

- **Passive** and **active** network monitoring
- Most popular methods: **OS fingerprinting** and **banner grabbing**
- **Examples**
  - Nmap
  - WhatWeb scanner
  - curl
  - SolarWinds Asset Discovery

OS fingerprinting

- **Passive fingerprinting**
  - Captures network **connection properties** to infer the device's operating system
- **Active fingerprinting**
  - Scanner sends packets to a host and **examines the response**
- **Example attributes and properties**
  - TCP SYN packet length
  - TCP window size
  - Time to Live (TTL)
  - User agents
  - Specific domains

Banner grabbing

- Captures **banner information** transmitted by a remote port when a connection is **initiated**
- **Banner**
  - **"welcome screen" -** a text displayed by a host server
  - contains details like **software type** (also OS type) and **version**
- **Disadvantage:** administrator can **alter** the transmitted banners
- **Example**: Apache server

```
Server: Apache/2.4.18 (Ubuntu)
```

Comparison – agent approach

- **Advantages**
  - Precise
- **Disadvantages**
  - Installation
  - Infrastructure
  - Computing **overhead**
  - **Privacy** and security issues

Comparison – agentless approach

- **Advantages**
  - **No installation** and maintenance (asset is not modified)
- **Disadvantages**
  - Susceptible to **network issues**
  - Relatively **superficial insight** into inventory and performance
  - Greater network **overhead**

Current challenges

- **Situational awareness**
  - Most professionals **cannot** automatically **discover** all assets in the organization
- **Management chaos**
  - No asset inventory
- **Network without perimeter**
  - **Cloud** devices
  - **3rd party** services

Common Platform Enumeration

Standards and enumerations

- Motivation:
  - Unified naming **conventions**
  - **Machine-readable** names of software and hardware products
  - **Simplified process** of vulnerability identification
  - Nmap scanner and the National Vulnerability Database (NVD) uses **Common Platform Enumeration (CPE)**

Common Platform Enumeration

- A **standardized method** of describing **product classes**
  - **Classes:** applications, operating systems, and hardware devices
  - **Current version**: 2.3
- **Well-formed CPE name (WFN)**
  - **Content:** attribute-value pairs
  - **Syntax:** *wfn:[…, target_hw="x64", update=ANY,…]*
- Binding to **CPE match string**
  - Each attribute has its **specified position**
  - CPE match string is **more popular** than WFN
  - Used in the **National Vulnerability Database (NVD)**

CPE match string

cpe:2.3:<part>:<vendor>:<product>:<version>:<update>:<edition>

:<language>:<sw_edition>:<target_sw>:<target_hw>:<other>

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:datacenter:*:x86:*

- **Part** contains three values:
  - **“a”** – applications
  - **“o”** – operating systems
  - **“h”** – hardware
- **Vendor –** a person or a company which manufactured the product

CPE match string

cpe:2.3:<part>:<vendor>:<product>:<version>:<update>:<edition>

:<language>:<sw_edition>:<target_sw>:<target_hw>:<other>

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:datacenter:*:x86:*

- **Product**
  - The official **product name**
- **Version**, **update**, and **sw_edition**
  - A version, an update, and an edition of the product

CPE match string

cpe:2.3:<part>:<vendor>:<product>:<version>:<update>:<edition>:

<language>:<sw_edition>:<target_sw>:<target_hw>:<other>

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:datacenter:*:x86:*

- **Edition**
  - **Deprecated** field
  - Contains value ANY unless it is necessary to specify it for the **backward compatibility** with CPE 2.2
- **Language**
  - Language of **user interface** conforming to RFC 5646, e.g., *en*

CPE match string

cpe:2.3:<part>:<vendor>:<product>:<version>:<update>:<edition>:

<language>:<sw_edition>:<target_sw>:<target_hw>:<other>

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:datacenter:*:x86:*

- **Target SW**
  - **Operating environment** of product, e.g., *windows_8.1*
- **Target HW**
  - **Architecture**, e.g., *x64*
- **Other**
  - Information that **does not fit** into previous fields

Comparison rules

- **Special values**
  - **ANY**
    - Denoted as **asterisk (*)**
    - Contains literally **any value**
  - **NA (not applicable)**
    - Denoted as **dash (-)**
    - **No legal or meaningful value** for the attribute or attribute is not used for description
    - Similar to **null** value
- **Comparison rules**
  - Exact values **will not** match to NA
  - Anything **will** match to ANY

Supplementary materials

- **B. A. Cheikes, D. Waltermire, and K. Scarfone**, "*Common Platform Enumeration: Naming Specification Version 2.3*," National Institute of Standards and Technology, NIST IR 7695, 2011. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7695.pdf
- **CARALLI, Richard A.; ALLEN, Julia H.; WHITE, David W.** *"CERT Resilience Management Model – CERT-RMM: A Maturity Model for Managing Operational Resilience."* Glenview, IL, USA: Addison-Wesley Educational Publishers Inc, 2016. ISBN 978-0-13-454506-6.
- **MUNIZ, Joseph; MCINTYRE, Gary; ALFARDAN, Nadhem.** "*Security Operations Center: Building, Operating, and Maintaining Your SOC."* Indianapolis (USA): Cisco Press, 2016. ISBN 978-0-13-405201-4.

MUNI

FI