Cybersecurity BootCamp
week 4

ZERNA Lesly

October 2017

1 Introduction

Cybersecurity BootCamp by CyberWayFinder SPRL consists in a four week training in topics to be introduced into the cybersecurity field. This training is mainly focused on women inclusion into this field.

This document contains my personal notes and extra info about the topics involved during the 4 weeks.

2 Class 10 - Access Control

Domain 2 -> Access Control

- Principal operation security: IT political and governance
- Security Operation Center: create and grant access
- Implementation of access control:
  - Physical controls based on access control policies
  - Strong authentication driven by policies
- IT Governance -> inventory of assets (CMDB)
- CMDB includes servers, applications, etc. It is a key component to support activities in Cybersecurity.

Subject Access Object

- **Subject** -> active (person, program, process)
- **Object** -> passive

Consider this 2 principles

- **Need to know** -> SoD, involves "remove access from users".

- **Least-privilege** -> each person focuses and accesses only in his/her tasks, no more credentials granted. (Controls in the IAM)

IAM Identity and Access Management

- authentication
- authorization
- tracking/tracing

When deploying a solution -> **PDCA** -> Plan, Do, Check, Act

Problems with authorization (SIEM)

- Usage of generic accounts
- Service accounts

"Security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware."[wikipedia]

Note Do not run as "root", never!!!

Threats

Threats can cause... "loss of accountability", "covert channel", etc.

"Covert channel is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy."[wikipedia]
For mitigation, it is possible to use DLP software:
"Data loss prevention software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage)."[wikipedia]

Other attack with "ping request" (ICMP protocol). Prevention, in this case, good access control in the network and continuos review of access.

Can a developer be a threat?
Maybe! It depends of the IDE, the compilers, anti virus that he/she uses.

Control types

- Detective
- Corrective

- Recovery

DRP "A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster."[wikipedia]

IAAA -> review ACL
"An access control list (ACL) is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects."[wikipedia]

PKI
"A Public Key Infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email."[wikipedia]

LDAP
"The Lightweight Directory Access Protocol (LDPA) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network."[wikipedia]

RBAC
"Role-Based Access Control (RBAC) is an approach to restricting system access to authorized users. It is used by the majority of enterprises with more than 500 employees, and can implement mandatory access control (MAC) or discretionary access control (DAC). RBAC is sometimes referred to as role-based security."[wikipedia]

3 Class 11 - ISC2 NIGHT - Security Awareness

Link Event -> https://www.eventbrite.fr/e/billets-isc2-belux-chapter-security-awareness-behaviour-and-culture-37980044335#
Presentation about "Security awareness", with the presentation from a representative from Apalala, the Centre for Cybersecurity Belgium and the European Commission. Also two experts from Corporate Banking BNPP Fortis who talked about the security awareness of front-office, back-office and customers.

4 Class 12 - Business Continuity Disaster Recovery

Differentiate between:

- **BCP** -> Business Continuity Planning. This is preventive.
- **DRP** -> Disaster Recovery Planning. This is reactive, this should ensure the recovery of the sytem to work again in full mode.

Parameters to consider:

- Business Impact Analysis [8]
- Recovery Time Objective
- Recovery Point Objective
- Performance and response time?
- Capacity?
- Quality?

Define a DRP (Disaster Recovery Plan).
Design the network considering Firewall and independent internal networks.
The Cybersecurity trinity **People, processes and technology**
Consider IT Services **ITIL** and **Security Governance** [9]
Security technologies can be "physical" (smoke detectors, CCTV, fences, access control, ...) and "logical" (firewalls, VPNs,...)

Acronyms

- **SOC** -> Security Operation Center
- **ISMS** -> Information Security Management System
- **CMDB** -> Configuration Management Database
- **SoD** -> Separation of duties / Segregation of duties
- **IAM** -> Identity and Access Management
- **SIEM** -> Security Information Event Management
- **DBMS** -> Database Management System
- **SIM** -> Security Information Management
- **SEM** -> Security Event Management

- **DLP** -> Data Loss Prevention
- **ICMP** -> Internet Control Message Protocol Management
- **IDE** -> Integrated development environment
- **DRP** -> Disaster Recovery Plan
- **IAAA** -> Identification, Access Control, Authentication, and Accounting
- **ACL** -> Access Control List
- **PKI** -> Public Key Infrastructure
- **LDPA** -> Lightweight Directory Access Protocol
- **RADIUS** -> Remote Authentication Dial-In User Service
- **RBAC** -> Role-Based Access Control
- **MAC** -> Media Access Control Address
- **MAC** -> Mandatory Access Control
- **DAC** -> Discretionary Access Control
- **BCP** -> Business Continuity Planning
- **DRP** -> Disaster Recovery Planning
- **BIA** -> Business Impact Analysis [8]
- **RTO** -> Recovery Time Objective
- **RPO** -> Recovery Point Objective
- **ITIL** -> Information Technology Infrastructure Library
- **VPN** -> Virtual Private Network

References

Security information and event management, https://en.wikipedia.org/wiki/Security_information_and_event_ [cited October 2017].

Covert channel, https://en.wikipedia.org/wiki/Covert_channel [cited November 2017].

Data Loss Prevention Software, https://en.wikipedia.org/wiki/Data_loss_prevention_software [cited November 2017].

Disaster Recovery Plan, https://en.wikipedia.org/wiki/Disaster_recovery_plan [cited November 2017].

Access Control List, https://en.wikipedia.org/wiki/Access_control_list [cited November 2017].

Lightweight Directory Access Protocol, https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protoco [cited November 2017].

Role-based access control, https://en.wikipedia.org/wiki/Role-based_access_control [cited November 2017].

Business Impact Analysis (BIA), https://www.gartner.com/it-glossary/bia-business-impact-analysis [cited November 2017].

Cyber Security Governance, https://www.mitre.org/publications/technical-papers/cyber-security-governance [cited November 2017].