CYBER Security Spring 2022

Case III

Cyber Security Assessment

1 Introduction

In order to challenge, exercise, and elaborate on the knowledge that you have obtained during the lectures and literature studies of this course, you are now asked to apply this knowledge in practise by creating a penetration testing procedure.

The scenario in this exercise is presented in the next chapter. The scenario is fictive, though it is based on events and experience from the industry. The (scientific) base that you are required to have by now is not only based on the lectures and course literature, but also on your own research material and information that you have found on the net (or elsewhere).

The purpose of this session is for you to learn to be able to create a penetration testing procedure from a given scenario - and also be able to identify security metrics for the threats you have identified. The expected learning outcomes are the following - you should be able from a given scenario:
- To identify strengths and weaknesses of an IT- and information infrastructure.
- To describe a possible and realistic penetration testing procedure.
- To identify security metrics for your proposed security controls that should aim to mitigate the threats you have identified.

The work with these cases are structured as follows.

- The case is published in iLearn 08.00 the Wednesday before the peer-review.
- The group spends 2 hours working on the case, any time before Friday 22nd April 13.00.
- The group members are not required to meet in person, use some on-line tool for communication.
- On Friday at 13.00 the group submits its work in iLearn to the fora called Case 3 Hand-in and it is important that the subject of the message is 'Case 3 Security Assessment Group X', where X is replaced by your own group number.
- At 13.00 on Friday the schedule for peer-review is published in iLearn.
- 13.05 the group starts going through the documentation of the group they will peer-review according to the schedule presented in iLearn.
- At 14.45 the group sends their comments and at least four questions to the other group by replying to the original message of their peer-review group, in the fora Case 3 Hand-in in iLearn.
- In this way their documentation, your comments and questions, and then their reply will be in the same message thread in iLearn.
- Now the group reads the answer sent in by the group that has done a peer-review of your group, and this message should be found as a reply to your own original message, with the hand-in of your documentation.
- At 14.45-15.45 the group discuss the feedback from their peer-review group and sends their answers and comments by replying to the correct message in iLearn.
- At 14.45 the group can read the answers of your comments and questions from the group you have peer-reviewed.
- A few days later the groups will get some feedback from the teacher on their documentation.

2 Scenario

Disclaimer: This scenario is meant for educational purposes only. Any resemblance to similar existing names is for realistic and dramatic effect to the case description in question. The scenario is the same as for case 2, since you may have use of the result of last week when working with this assignment.

Radio Sweden is a government owned national radio station that focuses on news and political matters. It is well renowned for its thorough, investigative journalism, its documentaries, and extensive news programmes. Since Radio Sweden broadcasts nationally and is a government owned radio channel, it also serves as a communication point in case of national emergency by broadcasting messages to the people. Radio Sweden does not have a CIO per se, but they have a head of IT who also is responsible for the cyber security of the organisation. She has enforced encryption and antimalware policies to the organisation but does not have time to manage the cyber security in the way it is needed to. Recently, Radio Sweden's top programme Skriet, published a sensitive story about corruption in an international construction company and have since then received anonymous threats via email and telephone - more severe and concrete than the threats have been before. In addition, there has been an incident with ransomware on one of the employee's computers. These events have made the CEO concerned with the cyber security threats and attack vectors of the organisation. Therefore, Radio Sweden needs help to make an overall assessment of the threats possible attack scenarios and defences strategies for these attack scenarios.

2.1 Infrastructure

The infrastructure of Radio Sweden is as follows. There is a simplified depiction of it in the appendix section as well:

- All employee computers run Windows 10 Professional (64 bits)

- All journalists' computers run Windows 10 with full disk encryption

- All computers run F-Secure Client Security anti malware software

- All employees, including freelance journalists, have access to work on distance using a VPN connection

In addition, Radio Sweden has several servers and other equipment that is connected to the internet, or some other kind of network. Due to the nature of the journalist profession, the firewall must be kept somewhat lenient in order for the journalists to conduct their research properly. Likewise, there is a need for the journalists to be able to receive tips via email - both encrypted and unencrypted. Also, the VPN must be available for freelance journalists, since Radio Sweden buys a lot of their material from freelance journalists and external production companies.

- Wireless networks: one gust WiFi, one restricted internal WiFi (Cisco Catalyst 9800 controller including Aironet 3800 access points)

- 14 Windows servers 2016 for internal systems (finance, internal communication, systems)

- 7 GNU/Linux Redhat servers for intranet, web servers, email, intrusion detection systems, log, FTP servers.

- 2 Solaris 11.1 servers for backups

- Cisco 8808 routers

- HP Office Connect 1850 Gigabit switches

- Cisco ASA 5500 firewall

2.2 A few Words about Physical Security

Radio Sweden is a so called "protection object" (Swe. Skyddsobjekt), which means that the building the organisation is situated in - and its surrounding area is protected by law (Skyddslag (2010:305)). This means that it has higher physical security than other buildings and must be protected from sabotage, terrorism, espionage, and robbery. Examples of other protection objects are Rosenbad (the Swedish parliament building), radio masts, the royal family's residences. The physical environment is considered to be "secure" and well protected in this case, so you do not have to take that into account when working with the scenario.

2.3 Task Description

Since you are working as an external security consultant at a well renowned cyber security company, you have been hired to make an assessment of the cyber security of Radio Sweden, and present it in form of a report to the head of IT at Radio Sweden. More in detail you are required to:

- Describe how a penetration test of Radio Sweden's infrastructure could be done - including a step-by-step description that is based on what you have learnt from the last couple of lectures and from the course literature.

- Provide and motivate examples of security controls and security metrics for these security controls, that mitigate the vulnerabilities identified in the penetration test. You could of course use the threat model and its security controls that you created last seminar if you find them relevant for this exercise.

2.4 Requirements

There is no template for this seminar assignment - you are free to present the result in any way you find most sufficient and appropriate. The following requirements must be fulfilled in order to pass the exercise:

- Group size should be 3-4 people

- Groups must be registered in iLearn

- All group members should be active in the group work

- Files should be submitted to iLearn before the deadline.

- The submission file must include group number, e.g. GroupX_case_3.pdf

If you have any questions regarding the case, you can post your question in Supervision in iLearn. Since the groups can work with the case any time between Wednesday and Friday the teachers may not read the Supervision fora immediately after you have sent the question, so there could be some time before you get the answer. Remember: Internet search engines could provide you with the most detailed and adequate answers for some of the questions that you may have.

2.5 Resources

Other than the course literature and the lecture slides, these might be useful resources for completing this exercise.

- MyAppSecurity - Manage Your Risk with Threat Modeling (slides 8-14): https://owasp.org/www-pdf-archive/Manage_Your_Risk_With_ThreatModeler.pdf

- MITRE - CAPEC list: https://capec.mitre.org/data/index.html

- Cisco Security Advisories: https://tools.cisco.com/security/center/publicationListing.x

- SANS Checklists for Systems Security: https://www.sans.org/score/checklists/

- Microsoft - Enterprise Security Best Practises: https://technet.microsoft.com/en-us/library/dd277328.aspx

3 Appendix

Below is a simplified depiction of Radio Sweden's IT infrastructure, although some of the products are newer version according to the earlier description, but the setup is correct.