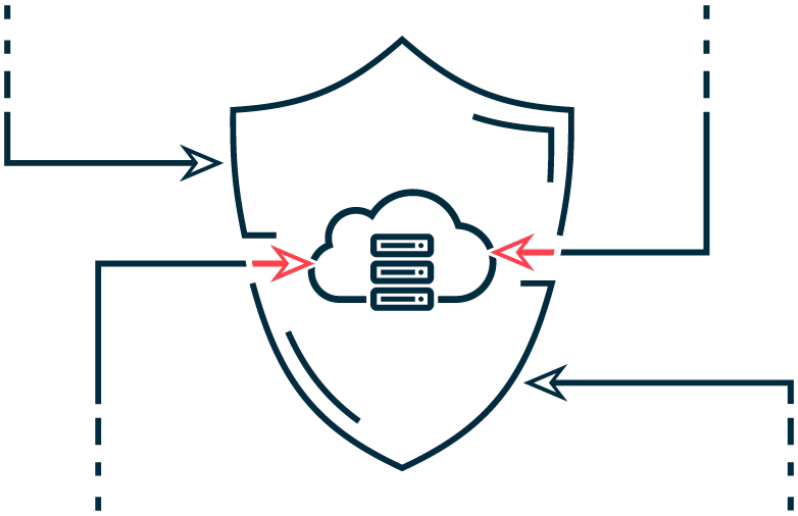
Project Plan

ICS Semester 4 - Group G
Secure Solution project plan

Nick Blom Jorn Kosterman Ryan Smith
Aleksandar Penev Mihai Glodici

May 8, 2023



Version History

Version	Changelog	Date	Rationale
v1.0	Initial release	May 9, 2023	Issued

Contents

1 Introduction **4**
1.1 Problem Definition 4
1.2 Goals 4
1.3 Scope 4

2 Research **5**
2.1 Research Questions 5

3 Deliverables **5**

4 Planning **5**

1 Introduction

1.1 Problem Definition

During off-time work hours, an employee tried fulfilling his duties on an internal server, from home. Using RDP (Remote Desktop Protocol), he connected to the remote server. However, his home desktop machine was infected with a key-logger. Some days later, the full network was compromised and all systems were encrypted. From the infected client device, the RDP credentials were stolen. The attackers demanded a ransom, which the company paid to get important information and data back. The attackers knew exactly how much money was a reasonable amount to lock their systems. However,the company knew very well that the infiltrators might left behind some remnants on their systems, so that they could strike again at any given time. Because of this, the company also paid a big amount of money for new equipment. They replaced everything that was ever part of the company's belongings and what was connected to their network.

This situation is based on a real event from a mid-sized enterprise in installation technology from Gelderland. This breach has never been disclosed and the company paid a ransom. We are not allowed to state its name or other details. What we are allowed to say, is that was a client of the company we are performing a pentest for, Win It. Win It acts as another stakeholder in this project, providing us with some details of the breach.

1.2 Goals

The goal of this project is to implement a secure network solution to tackle the problems described in the problem definition. The affected company does not want this to happen again, so we will create a secure, simulated network design that tackles the issues the affected company was facing.

1.3 Scope

This project is mainly about network security, or setting up a secure (simulated) network based on the problem definition. There will be various network security principles that can be applied in this project. Certainly, the following principles regarding network security will (at least) be applied during the Secure Solution project:

- Network separation and segmentation
- Intrusion detection (NIDS)
- Secure connections (RDP, to be further secured)
- Network security monitoring (NSM)

2 Research

During the project, it might be necessary to perform research on certain topics. We do so by using the DOT framework for applied research. The following research questions and its chosen methods will be of relevance during this project.

2.1 Research Questions

- How can RDP be securely used?
  - How does RDP work?
  - What options are already in place to secure RDP?
- How can network intrusions through remote access protocols be detected?
  - What does remote access protocol traffic look like in general?
  - What are the differences between popular remote access protocols, such as RDP and SSH?

3 Deliverables

For this project, we will deliver the following:

- This project plan.
- Findings on the defined research questions with the DOT framework.
- A secure network design based on the problem description and scope.
- An implementation of the secure network design on netlab.
- A final document explaining and justifying the design, and test results from the "Red versus Blue" event.

What we will not deliver, is a physical implementation of the network design.

4 Planning

Starting from week 11, the following phasing for the project is suggested:

Week	**Main duties**	**Workload**
Week 11-12	Project plan and set up	5-10 hours
Week 13	Perform defined research	3 20 hours
Week 14	Design & implement	3 10-15 hours
Week ??	Blue vs Red participation	4 hours
Week 15	Process results 10	6 hours
Week 16	Finalize all deliverables	10-20 hours