Project Plan

| **Version** | **Date** | **Author(s)** | **Amendments** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | 06-03-2024 | Nikolov, Bogdan B.N  Linden, Ben B.C.H. van der  Kessels, Roan R.A.F.  Fleetwood-Bird, Andrew A.T.  Dooren, Reuel R. van  Ali, Khaled K. |  | Initial Draft |
| 2 | 15-03-2024 | Nikolov, Bogdan B.N  Linden, Ben B.C.H. van der  Kessels, Roan R.A.F.  Fleetwood-Bird, Andrew A.T.  Dooren, Reuel R. van  Ali, Khaled K. | Added research questions  Updated sprints | amendment |
| 3 | 19-04-2024 | Nikolov, Bogdan B.N  Linden, Ben B.C.H. van der  Kessels, Roan R.A.F.  Fleetwood-Bird, Andrew A.T.  Dooren, Reuel R. van  Ali, Khaled K | Updated research question based on feedback | amendment |
| 4 | - |  | - | - |

[**Project Assignment 3**](#_ik933voesn3i)

[**1.1 Goal of the project 3**](#_pnwh1pg2l5ci)

[**1.2 Context/Investigation 3**](#_lieaxq053pk)

[**2. Approach and Planning 4**](#_k3ixvthnzvyr)

[2.1 Approach 4](#_hhra9j780u7x)

[2.2 Research questions and sub questions 4](#_pe30zweoyp23)

[2.3 Project Scope 6](#_mbg6ocifwkbe)

[2.3a Project Objectives 6](#_7ye4vvjxmprz)

[2.4 Project Team 7](#_pxocdqashphr)

[2.5 Sprint deliverables 8](#_7t9vxlwu0f3x)

[2.6 Stakeholder Communication/Wishes 9](#_waow0qwsxqu4)

[2.7 Work Delivery 9](#_p7exljr325b7)

[2.8 Risk assessment 10](#_qpso1lx6umtc)

[2.9 Project Constraints 11](#_wku1bz4sy0o)

[2.9.1 Time Constraints 11](#_chy61sca4cz3)

[2.9.2 Client Constraints 12](#_eyke74m6wxvy)

[2.9.3 Scope Creeps 12](#_bklad9w3serc)

# **Project Assignment**

# **1.1 Goal of the project**

The primary objective of this project would be to simulate an environment that we can monitor to learn what is exactly happening inside, learn who's exactly attacking and checking the behavior behind the attacks. The idea in the end is that we have a better understanding of cybersecurity threats in the real world out there through monitoring

Honeypots can be a good way to expose vulnerabilities in systems, A honeypot doesn’t get any legitimate traffic, so any activity logged is likely to be a probe or intrusion attempt. That makes it much easier to spot patterns, Honeypots can give you reliable information about how threats are evolving. They deliver information about attack vectors, exploits, and malware. Hackers constantly refine their intrusion techniques; a honeypot helps to spot new threats and intrusions.

# **1.2 Context/Investigation**

Groups were asked to investigate a current security problem in the field of IT Security and design and develop a solution to this. We picked Design and implementation of a honeypot network, which asked the following from us: How can we design and implement a honeypot network to gain insight to the behavior of hackers without having impact on the production network?

# **2. Approach and Planning**

## **2.1 Approach**

We will be using the Agile method to try to deliver something every two weeks. We will be using sprints to divide our work into parts. Stand-up meetings will be held at the beginning and at the end of each week, with also potential demos being shown-off. Meetings with the client will be done every sprint to keep them up to date with the progress of the project.

## **2.2 Research questions and sub questions**

**Main research question:**

Can we effectively distinguish between human and automated (bot) attackers

**Sub questions**

1) What are the needed components and requirements for creating a honeypot?

2) What are the different types of honeypots, and how do they differ in deployment and management?

3) What are the best practices for managing and maintaining a honeypot

4) How do we monitor and analyse honeypot data to identify and respond to security threats?

5) What are the resource requirements, hardware, software, needed to create, deploy, and manage a honeypot effectively?

6) What are the common challenges and pitfalls encountered with making a honeypot

7) What are design conventions for online trading platforms that can be implemented in a honeypot for a more believable application?

8) What is a viable network infrastructure to successfully mimic a company

## **2.3 Project Scope**

The scope of this project is to be the creation and maintenance of a simulated environment for continuous monitoring. The focus is on gaining insights into the inner workings, identifying specific attacks if possible, and analyzing attack behaviors. Ultimately, the aim is to get a better understanding of real-world cybersecurity threats by actively monitoring and learning from the simulated environment. In the end deceive attackers into believing that they've gained access to the real system.

### **2.3a Project Objectives**

The main objective of the project are :

| Scope of Work | Outside of Scope |
| --- | --- |
| Designing and deploying a realistic honeypot network architecture. | Physical security measures for protecting the infrastructure hosting the honeypot network. |
| Developing backend functionalities using Python for data collection and analysis. | Development of custom hardware or software solutions beyond the defined objectives. |
| Implementing server-side logging on a Linux server for network emulation and simulation. | Implementation of advanced threat hunting techniques beyond the honeypot's data collection. |
| Continuously monitor the honeypot network using Python and log files to gather data on cybersecurity threats and attacker behaviour.  Develop strategies to deceive attackers into believing they have infiltrated a real system, enhancing the authenticity of the honeypot environment. | Forensic analysis of cybersecurity incidents outside the honeypot's scope. |
| Identify and analyze specific attack vectors, exploits, and/or malware used by hackers |  |
| Utilize honeypot data to gain insights into evolving intrusion techniques and threat landscapes. |  |

## **2.4 Project Team**

| **Name** | **Role/tasks** | **Availability** |
| --- | --- | --- |
| Ali, Khaled K. | Team member | Mon-Fri, 9:00 - 16:00 |
| Dooren, Reuel R. van | Team member | Mon-Fri, 9:00 - 16:00 |
| Fleetwood-Bird, Andrew A.T. | Team member | Mon-Fri, 9:00 - 16:00 |
| Kessels, Roan R.A.F. | Team member | Mon-Fri, 9:00 - 16:00 |
| Linden, Ben B.C.H. van der | Team member | Mon-Fri, 9:00 - 16:00 |
| Nikolov, Bogdan B.N. | Team member | Mon-Fri, 9:00 - 16:00 |
| Roijers, Stefan S.E. | Project Client | Email: Mon-Fri, 9:00 - 16:00  On-Location:  Mon 9:00 - 16:00 Wed 13:00 - 16:00 |
| Houkes-Linssen, Raoul R.W.W. | Project Coach | Email: Mon-Fri, 9:00 - 16:00  On-Location:  Mon 9:00 - 16:00 Wed 13:00 - 16:00 |

## **2.5 Sprint deliverables**

**Sprint 1: Identify (Week 4-6)**

Research and Selection:

* Research into honeypots, how they work exactly. Decide whether we want a low interaction honeypot or a high interaction honeypot
* Evaluate pros and cons and select the most suitable option.
* Interview stakeholders
* Setup Network infrastructure
* Setup already-existing honeypot
* Research monitoring software
* Basic website design

**Sprint 2: Protect (Week 7-9)**

* Research
* Design document
* Proof of concept honeypot
* Network diagram

**Sprint 3: Protect (Week 10-12)**

* Execute the design document by deploying the researched honeypot solution.
* Configure honeypot to selected option (low or high interaction).

**Sprint 4: Detect (Week 13-15)**

* implement monitoring software to track and analyse honeypot activity
* Configure alerts and notifications for suspicious activity detection.

**Sprint 5: Respond, Test and Final Delivery (Week 16-17)**

* Finalising implementation
* Test report/demo
* Presentation/Documentation

## **2.6 Stakeholder Communication/Wishes**

Communication between team members will be done in person and through a discord server. Meeting with the client and project coach will be scheduled through email, minor questions can be asked through Microsoft Teams but should be kept to a minimum. We also have plenty of opportunities to ask both coach and client questions in person.

## 

## **2.7 Work Delivery**

Delivery of the project will be done on a sprint by sprint basis through the pre-made assignments in Canvas. We will have at least one client meeting every sprint in which we will give a detailed demonstration of our progress and discuss expected progress for upcoming sprints. In the end, the completed work is bundled and submitted in a GitLab repository.

## **2.8 Risk assessment**

| **Resource Consumption**: Honeypots can consume significant resources such as bandwidth, storage, and computing power, especially if they are actively monitoring network traffic or emulating services. This can potentially impact the performance of the network or systems hosting the honeypot. (2-low)(2-Probability) |
| --- |
| **Solution:** Creating a conclusive plan such as listing all the resources that you will be using and creating a network diagram to plan out all the servers being used, this can help you manage and understand all the resources you'll be using and means you can create an educated assumption about the used resources. |
| **False Positives**: Honeypots may generate false positive alerts, leading to unnecessary investigations or actions by security teams. This can waste time and resources, diverting attention from real threats.(1-low)(3-Probability) |
| **Solution:** Creating a plan on what you're trying to track and the type of honeypot network you are creating will help streamline the kind of attacks you are looking for and creating a proper security structure allows you to streamline the route the attacker can take |
| **Maintenance Overhead**: Honeypots require ongoing maintenance and monitoring to ensure they remain effective and secure. This includes updating software, analyzing collected data, and adjusting configurations based on emerging threats.()() |
| **Solution:** Setting up the right team that is a very IT conscious team that makes sure to continuously monitor the system and create regular updates to software to ensure the integrity of the systems. |
| **Legal and Ethical Concerns**: Depending on the nature of the honeypot and the data it collects, there may be legal and ethical considerations to take into account. For example, capturing and storing network traffic could potentially violate privacy laws or organizational policies.(2-low)(3-medium) |
| **Solution:** Before deploying a honeypot, conduct a thorough review of relevant laws, regulations, and organizational policies. Engage with legal counsel and compliance teams to ensure compliance with privacy laws and internal policies. |
| **Environmental Leak:** When setting up a honeypot there are many configurations to take into account, such as a high interaction honeypot allowing the attacker to run commands. This allows the Possibility of the attacker being able to break out from the honey pot network into the production environment. |
| **Solution:** Setting up a correctly set Network with proper segmentation and traffic rules reduces the chance of the attacker finding out they are in a honeypot network. |

## **2.9 Project Constraints**

## **2.9.1 Time Constraints**

Time constraints are essential toward our successful project. Our project must adhere to the client’s and college’s time planning. Our project will use the Agile sprint method of keeping track of progress. That means that our project will have to complete a certain amount of tasks during those sprints. Each sprint is between 2 and 3 weeks.

## 

## 

## 

## 

## **2.9.2 Client Constraints**

This refers to the specific requirements, preferences, or limitations imposed on us by the client. These constraints could include constraints about limitations in the budget, or certain technological preferences or maybe compliance requirements. Thus, it is important to hold regular meetings or contact with the client for information and questions about those constraints and if our plans/project aligns with the client.

## **2.9.3 Scope Creeps**

Scope creep happens when additional features, functions, or requirements are added to the project beyond the initial defined scope. This can happen both by the client wanting to see more functionalities or by misalignment of our project with the idea that the client has. This can result in a more complex project or extended time needed to implement said functionalities. Therefore it’s important to establish it early on and set realistic expectations and proper time management.