Projekthandbuch

AI in der Security

1

Version 1.0
Projektleiter/in: Sebastian Lipp
Datum: 12.04.2020

Inhalt

Änderungsverzeichnis

Versions-nummer	Datum	Änderung	Ersteller
0.1	11.04.2020	Aktualisieren des PHB aus dem WS: Allgemeine Projektbeschreibung, Projektauftrag, Projektzieleplan, Beschreibung Vorprojekt- und Nachprojektphase, Projektmeilensteinplan, Projektrisikonanalyse Integration des Dokuments ‚MCS-SS2020-PRJ2_Projektplanung.pdf' in das PHB	Wech Maximilian
0.2	12.04.2020	Projektstrukturplan, Projektbalkenplan, Projektzeitplan	Wech Maximilian

Ansprechpartner

Name	**Organisations-einheit**	**Rolle im Projekt**	**Telefon** (Büro, Mobil, Privat, …)	**e-mail**
Dipl.-Ing. Dr. Gerd Holweg	FH-Technikum Wien	Projektauftraggeber	0650 1234567	gholweg@technikum-wien.at
Bernhard Gally	FH-Technikum Wien - IT-Security	Projektteammitglied	0650 1234561	cs19m023@technikum-wien.at
Sebastian Lipp	FH-Technikum Wien - IT-Security	Projektleiter	0650 1234562	cs19m032@technikum-wien.at
Damir Marijanovic	FH-Technikum Wien - IT-Security	Projektteammitglied	0650 1234563	cs19m031@technikum-wien.at
Boris Stampf	FH-Technikum Wien - IT-Security	Projektteammitglied	0650 1234565	cs19m006@technikum-wien.at
Maximilian Wech	FH-Technikum Wien - IT-Security	Projektteammitglied	0650 1234566	cs19m020@technikum-wien.at

1 Projektpläne

1.1 Allgemeine Projektbeschreibung

Ein Thema, welches die Wissenschaft nach wie vor beschäftigt, ist die automatisierte und zeitnahe Erkennung schadhafter Angriffe auf Rechnersysteme. Um erhebliche Schäden zu vermeiden werden für diesen Zweck in Unternehmen oft Intrustion Dection Systeme (IDS) auf Basis von Anomalie-, Signaturerkennung, etc. eingesetzt. Ein relativ neuartiger Ansatz zur Erkennung von Angriffsmustern ist die Verwendung von künstlicher Intelligenz, also Machine Learning-Algorithmen. In einem Vorprojekt wurden öffentliche verfügbare Testdaten genutzt, um neuronale Netzwerke hinsichtlich der Erkennung von Anomalien zu trainieren. Dabei konnten vielversprechende Ergebnisse erzielt werden.

Ziel dieses Projekts ist es einen Datensatz zu erstellen, welcher für Supervised-Machine Learning in Form von neuronalen Netzen zur Erkennung von bösartigem Netzwerkverkehr eingesetzt werden kann. Dies soll auf Basis bestimmter Charakteristika im Datensatz möglich sein. Somit ist der Zweck des Projekts einen Beitrag zur automatisierten und verlässlichen Erkennung von schadhaften Angriffen auf Rechnersysteme zu leisten. Um das Ziel dieses Projekts zu erreichen, muss ein entsprechender Netzwerkverkehr simuliert, aufgezeichnet und weiterverarbeitet werden. Letztlich wird der erzeugte Datensatz mit dem neuronalen Netz aus dem Vorprojekt getestet und ein Performance-Vergleich durchgeführt.

Die Ergebnisse werden in zwei wissenschaftlichen Arbeiten dokumentiert.

1.2 Projektauftrag

projekthandbuch 001	PROJEKT- AUFTRAG

Projektstartereignis:	**Projektstarttermin:**
• Projekt-Kickoff	• 18.02.2020
Projektendereignis:	**Projektendtermin:**
• Abgabe der zwei wissenschaftlichen Paper und der Projektdokumentation	• 30.06.2020
Projektziele: • Erstellung eines Datensatzes, welcher für Supervised Machine Learning (neuronales Netz) zur Erkennung von bösartigem Netzwerkverkehr eingesetzt werden kann. • Verfassung von zwei wissenschaftlichen Paper zur Beschreibung der Resultate und der Vorgehensweise in diesem Projekt	**Nicht-Projektziele:** • Performance testen mit anderen Modellen/Machine Learning Algorithmen • Unsupervised Learning Ansätze für Intrusion Detection testen • Zusätzliche Paper zu dieser Thematik erstellen

Hauptaufgaben (Projektphasen):
- Detailplanung
- Aufbau der Infrastruktur
- Durchführen und Aufzeichnen von Angriffen
- Feature Extraction, Label-Vergabe
- Performance Vergleich der Datensätze mit Modell (neuronalem Netz) aus Vorjahr
- Durchführen einer Präsentation
- Erstellung wissenschaftlicher Paper

ProjektauftraggeberIn:	**ProjektleiterIn:**
• Dipl.-Ing. Dr. Gerd Holweg	• Sebastian Lipp

Projektteam:
- Bernhard Gally
- Damir Marijanovic
- Boris Stampf
- Maximilian Wech

Vorname Nachname, (ProjektauftraggeberIn)	*Vorname Nachname*, (ProjektleiterIn)

1.3 Projektzieleplan

projekthandbuch 001	PROJEKTZIELE- PLAN
Zielart	**Projektziele**
Ziele	• Erstellung von zwei wissenschaftlichen Paper zur Erläuterung der Ergebnisse und der Vorgehensweise, bis 30.06.2020 • Erstellung eines Proof of Concepts (Durchführung eines Angriffes, entsprechende Aufzeichnung und Weiterverarbeitung) zum Beweis, dass die Projektumsetzung wie geplant funktioniert, bis 01.05.2020 • Erstellung eines Datensatzes, welcher für Supervised-Machine Learning in Form von neuronalen Netzen zur Erkennung von bösartigem Netzwerkverkehr eingesetzt werden kann (= Durchführung, Aufzeichnung und Verarbeitung weiterer Angriffe), bis 01.06.2020 • Performance-Vergleich des neu erstellten Datensatz mit jenem des Vorjahrs unter Verwendung des erstellten Modells, bis 09.06.2020 • Erstellung einer Präsentation zur Erläuterung der Projektinhalte für die MCS-Studenten, am 16.06.2020 • Erstellung einer ausführlichen Dokumentation, welche die Arbeitsdurchführung und die gewonnenen Erkenntnisse vollständig enthält (= Projekthandbuch), bis 30.06.2020
Nicht-Ziele	• Nutzung jenes Netzwerkverkehrs, welcher eine Firewall durchläuft • Performance mit anderen Machine Learning-Algorithmen testen (nur Neuronales Netz zulässig) • Verwenden eines Unsupervised Learning Ansatzes zur Intrusion Detection • Zusätzliche Paper zu dieser Thematik verfassen

1.4 Beschreibung Vorprojekt- und Nachprojektphase

projekthandbuch

001

BESCHREIBUNG VORPROJEKT- UND NACHPROJEKTPHASE

1) Beschreibung von Ergebnissen der Vorprojektphase

Das Projekt betreffende Entscheidungen/Ereignisse. Wie ist es zu dem Projekt gekommen?

- Im Vorprojekt wurde auf Basis eines neuronalen Netzes und einem bereits existierenden Datensatz ein Intrusion Detection System aufgebaut
- Dabei konnte gezeigt werden, dass der Einsatz von AI-Algorithmen in diesem Kontext sinnvoll ist
- Im WS19/20 wurde ein Überblick über verschiedene Angriffsarten, Tools, Infrastruktur, Aufzeichnung und Verarbeitung des Netzwerkverkehrs gegeben

Für das Projekt relevante Dokumente (zB „Protokoll mit ...", „Besprechung mit …", Inhalt der Dokumente ist hier nicht gefragt, NUR die Dokumente!)

- SS19: Setup & Infrastructure: A Neural-Network Approach for an Intrusion Detection System
- SS19: A Neural-Network Approach for an Intrusion Detection System
- WS18/19: Introduction to data gathering methods in an AI-supported IDS context
- WS18/19: Survey on recent neural network research and approaches for intrusion detection
- WS19/20: Network packet generation for Artificial Intelligence
- WS19/20: Network Data Collection for Artifical Intelligence

Erfahrungen aus ähnlichen Projekten

- Im Vorprojekt wurden acht verschiedene Angriffsarten und gutartiger Traffic vom neuronalen Netz mit einer Genauigkeit von mindestens 99,85% erreicht.
- Es ist eine hohe Rechenleistung notwendig, um ein neuronales Netz zu betreiben
- Der Netzwerkverkehr wurde mit tcpdump aufgezeichnet, für die Feature Extraction wurde CIC Flow Meter verwendet.

2) Beschreibung von Ergebnissen der Nachprojektphase

Was wird nach dem Projekt passieren (Folgeaktivitäten, -projekte, etc.)?

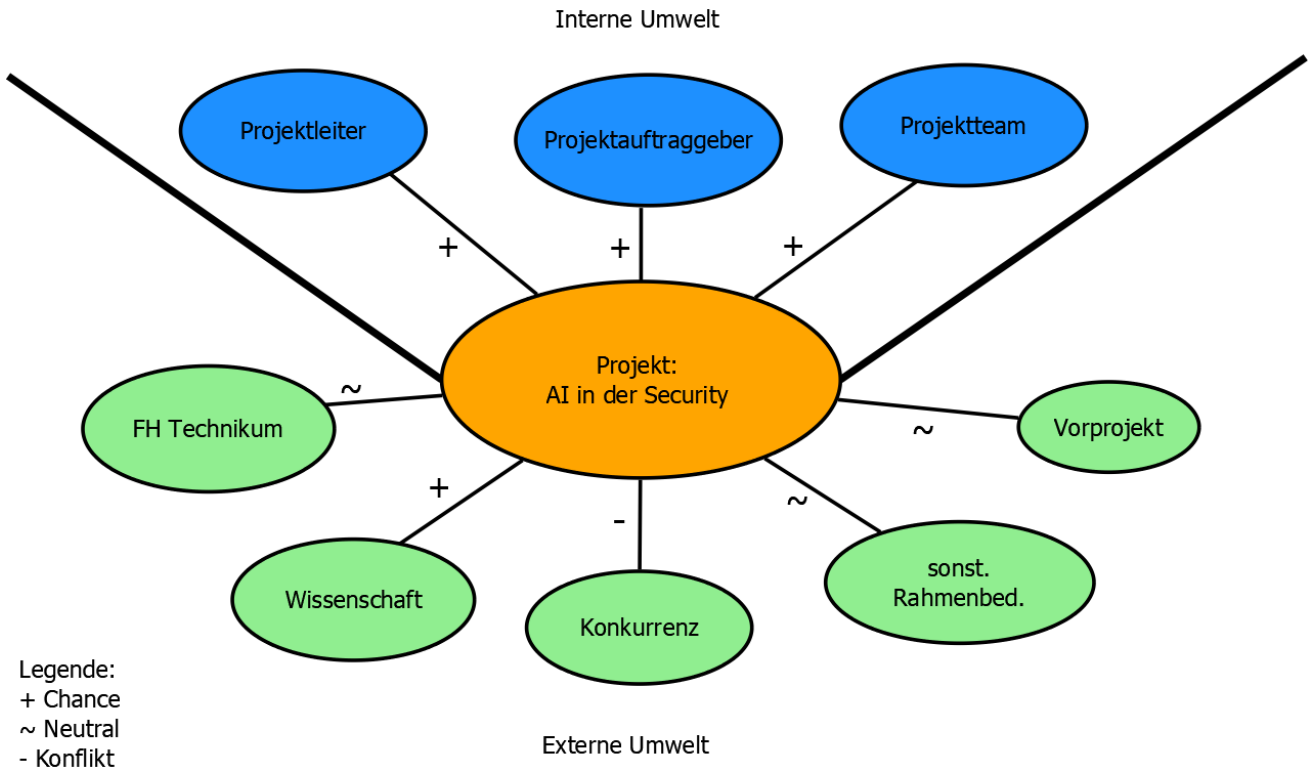
- Einbeziehen weiterer Angriffsarten
- Erweiterung des Datasets, um zusätzliche relevante Features
- Verwendung eines anderen Machine Learning Algorithmus und Durchführen eines Performance Vergleichs

1.5 Projektumwelt-Analyse

projekthandbuch

001

PROJEKTUMWELTEN-GRAPHIK



projekthandbuch

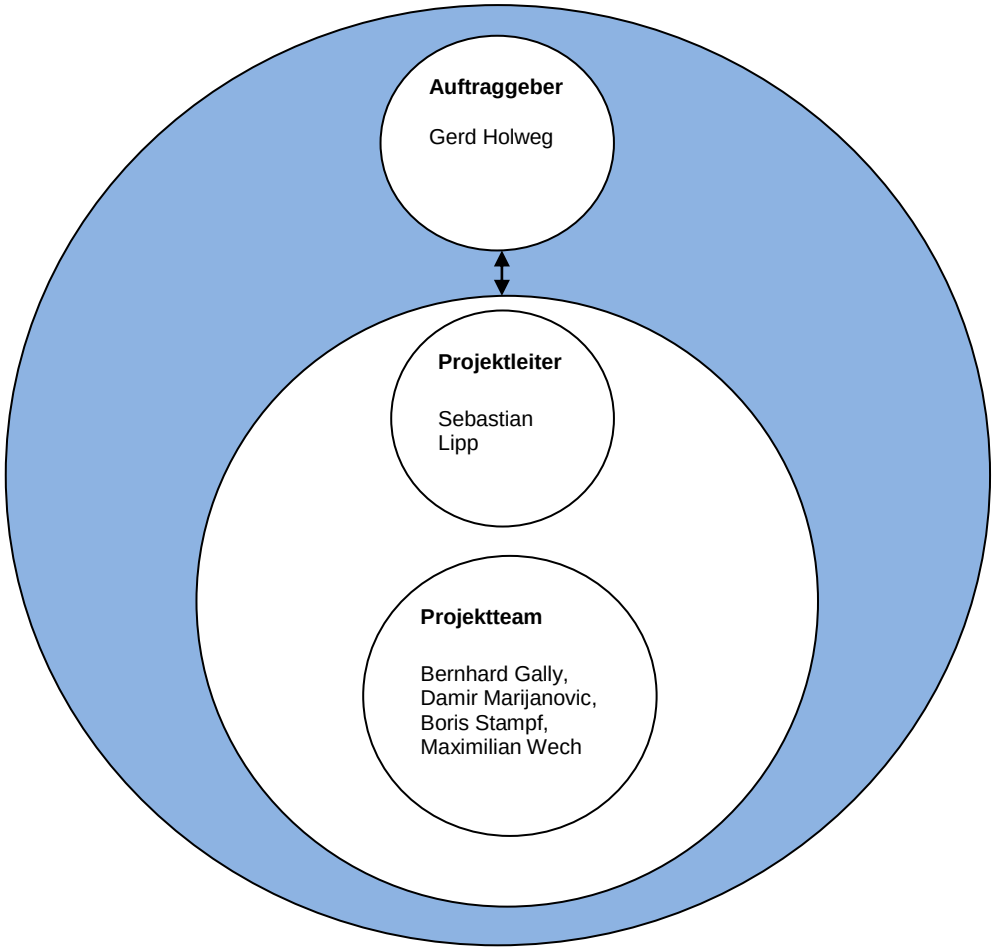
001

PROJEKTUMWELTEN-BEZIEHUNGEN

Umwelten	**Beziehung** (Potential/Konflikt)	**Maßnahmen**	**Who/When**
Projektleiter	Potential • gute Teamleitungsfähigkeit • Spaß an der Arbeit • fachliche Kompetenzen in sehr vielen Bereichen	• Evt. Prämie am Projektende • vollste Unterstützung durch Projektauftraggeber	Sebastian Lipp 03.07.2020

Projektteam	Potential ● Spaß an der Arbeit ● viel Projekterfahrung ● gutes Konfliktmanagement	● Förderung in allen Belangen ● Durchführung von Workshops um noch besseren Zusammenhalt zu erlangen ● eventuell Zusatzleistungen	Bernhard Gally Damir Marijanovic Boris Stampf Maximilian Wech laufend
Projektauftraggeber	Potential ● Hohes Interesse am Projekterfolg ● Kann wichtigen Input liefern	● Laufendes Reporting und Projektcontrolling ● Informieren über Erfolge und Hemmnisse ● Eskalation von Problemen vermeiden ● Miteinbeziehen bei wichtigen Entscheidungen	Dipl.-Ing. Dr. Gerd Holweg laufend
FH Technikum	Neutral ● Hohes Interesse an erfolgreichen Projekten ● Muss Infrastruktur bereitstellen	● Frühes Abklären wie Serverinfrastruktur aufgebaut werden kann (Selbsterstellung / Nutz von Bestehendem)	Sebastian Lipp Anfang März
Wissenschaft	Potential ● Viele Beiträge vorhanden mit ausreichend Information für ein Projekt in diesem Kontext	● Detaillierte Recherche um das benötigte Know-how zu erlangen ● Vergleich unterschiedlicher Literatur und Sammeln der Relevantesten	Bernhard Gally Damir Marijanovic Boris Stampf Maximilian Wech Sebastian Lipp Februar bis März
Konkurrenz	Konflikt ● Rivalität zwischen den Projektteams; jedes will das beste Team sein	● Konsequent und Effizient Arbeiten ● Gute Planung ● Viel Zeit investieren ● Periodischer Vergleich des eigenen Fortschrittes mit der Konkurrenz	Sebastian Lipp laufend
Sonst. Rahmenbed.	Neutral ● evtl. Ausfälle von Teammitglieder ● Zeitmangel ● Hohe Arbeitslast	● Mehrere Teams erstellen ● Aufgaben gut verteilen ● Detaillierte Planung	Sebastian Lipp Februar
Vorprojekt	Neutral ● Viele wichtige Erkenntnisse ● Diese müssen entsprechend genützt werden ● Dokumentation mangelhaft	● Nachvollziehen was im Vorprojekt genau geleistet wurde ● Die Erfahrungen nutzen ● Auf dieser Basis aufbauen	Bernhard Gally Damir Marijanovic Boris Stampf Maximilian Wech Sebastian Lipp laufend

1.6 Projektorganigramm



projekthandbuch

001

PROJEKT-ORGANISATION

Projektrolle	Aufgabenbereiche/Skills	Name
ProjektauftraggeberIn	Gibt die Rahmenbedingungen vor, Nimmt Projekt ab	Dipl.-Ing. Dr. Gerd Holweg
ProjektleiterIn	Koordination, Leitung der Meetings	Sebastian Lipp
Projektteam-mitgliederInnen	Teilnahme an Meetings, Erfüllung der Arbeitspakete	Bernhard Gally, Damir Marijanovic, Boris Stampf, Maximilian Wech

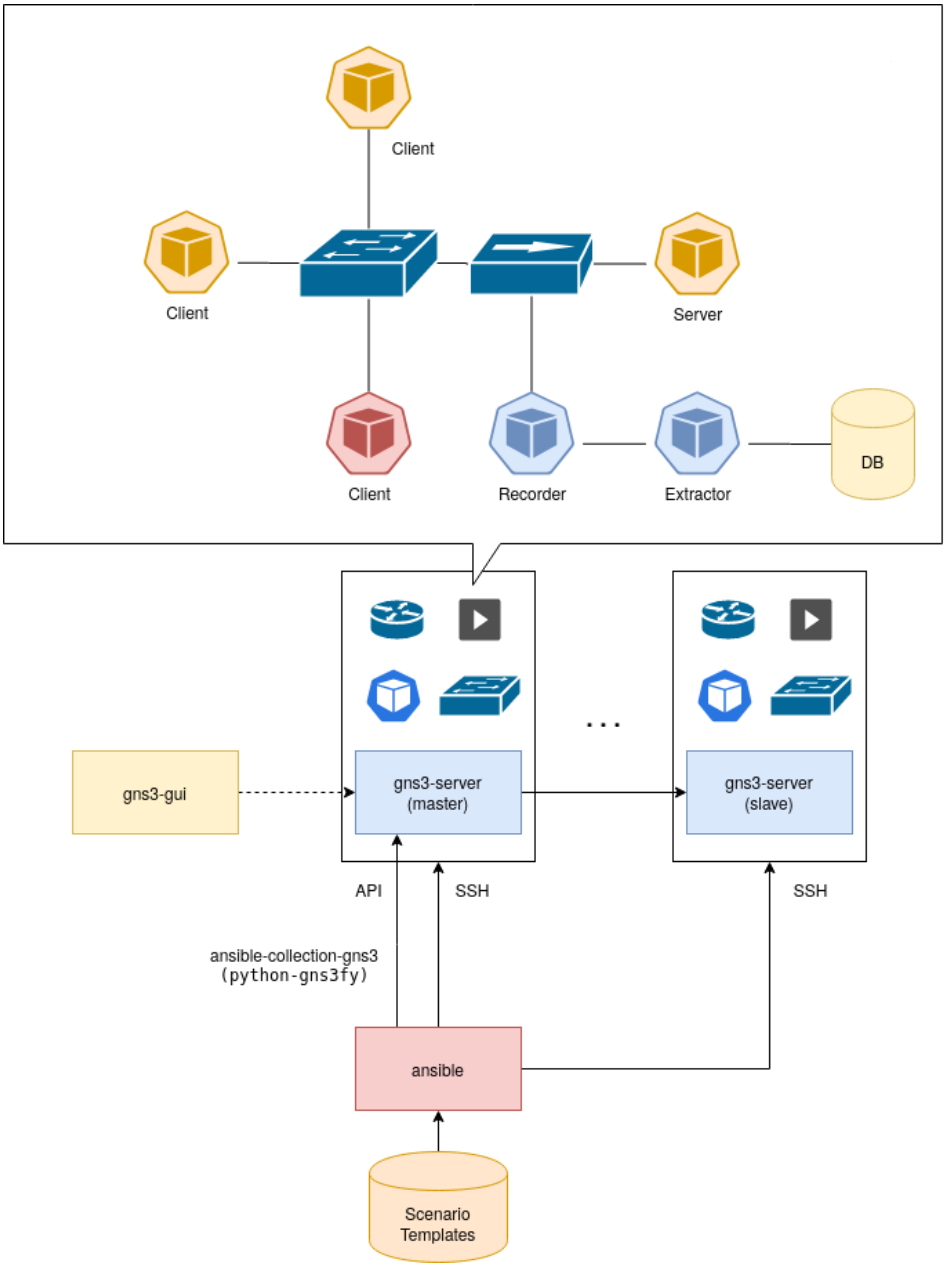
1.7 Technisches Konzept

Um den Netzwerkverkehr zu erzeugen wird der Netzwerksimulator GNS3 verwendet. Dieser verfügt über eine API, mit welcher es möglich ist Netzwerktopologien (für Angriffe und normalen Netzwerkverkehr) zu erstellen. Darüber hinaus können Container und virtuelle Maschinen in die Simulation integriert werden, wodurch die Weiterleitung des Netzwerkverkehrs an einen Recorder (zum Aufzeichnen des Verkehrs) und einen Extractor (zum Extrahieren relevanter Features) bewerkstelligt werden kann. Um den Netzwerksimulator in einer virtuellen und skalierbaren Umgebung zu betreiben wird Vagrant verwendet. Für das Deployment kommen Ansible Playbooks zum Einsatz, welche zum Definieren des Host-Setups und der verschiedenen Netzwerktopologien dienen. Der Simulations-Workflow beginnt somit bei der Eingabe des gewünschten Netzwerkszenarios. Daraufhin erfolgt das Deployment (von Host-System, Netzwerktopologie, Extractor, Recorder). Die extrahierten Features werden letztlich in einer zentralen Datenbank abgespeichert.

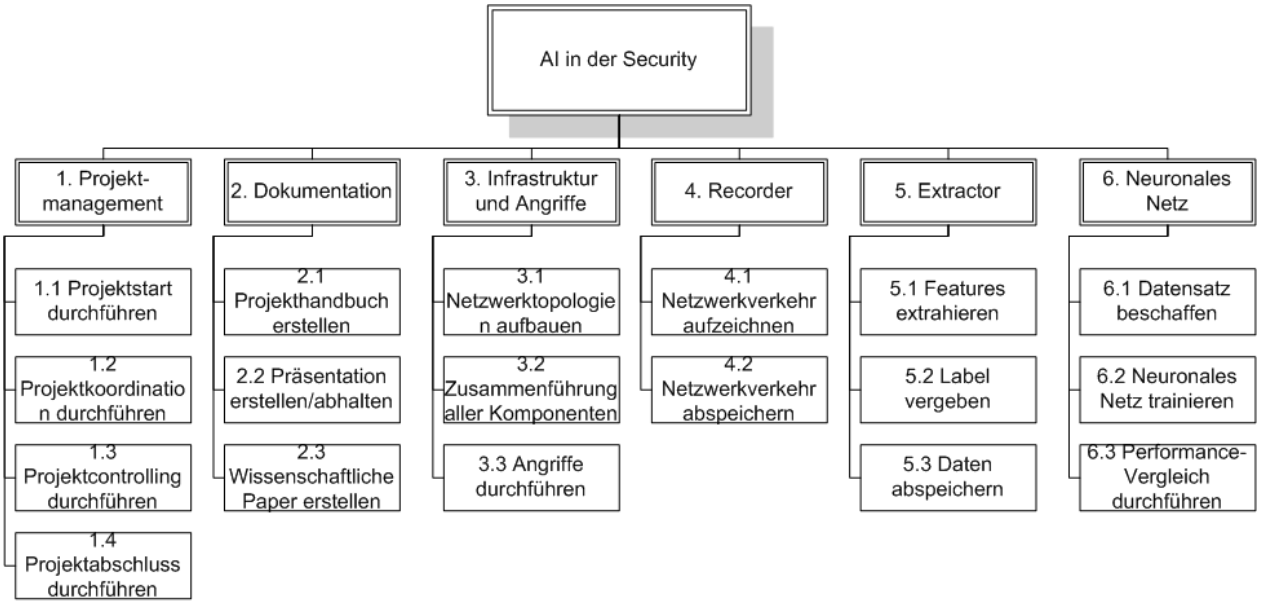
Konkret wird Folgendes durchgeführt:

- Aufbau mehrerer GNS3 Server mittels Ansible Playbooks
- Bereitstellung von GNS3 Netzwerken mittels dem gns3fy Ansible Modul über die GNS3 API. Ein GNS3 Netzwerk beinhaltet eine Netzwerktopologie (Angriff und normaler Netzwerkverkehr), sowie Recorder und Extractor.
- Verschiedene Szenarien können bereitgestellt und getestet werden mittels Ansible Playbooks (samt Parameter zum Extrahieren von Features).
- Features werden erzeugt und in einer Datenbank abgespeichert (genaue Position der Datenbank wird noch definiert).

Die folgende Abbildung zeigt eine grafische Darstellung des technischen Konzepts:



1.8 Projektstrukturplan



Der Projektmanagementblock trägt insgesamt dazu bei, einen zeitgerechten und erfolgreichen Projektabschluss zu bewerkstelligen. Es soll der laufend der Fortschritt gemessen und bei Bedarf steuernd eingegriffen werden.

Die Dokumentation besteht aus mehreren Komponenten. Es soll ein ausführliches und vollständiges Projekthandbuch erstellt werden, welches eine detaillierte Projektplanung enthält. Die Ergebnisse des Projekts werden im Rahmen einer Präsentation vorgeführt und in zwei wissenschaftlichen Papers erläutert.

Der Infrastruktur- und Angriffsteil wird mit einem Netzwerksimulator simuliert und beinhaltet den Aufbau einer entsprechenden Netzwerktopologie, bei welcher mehrere Komponenten (wie Clients, Server, etc.) zusammengeschalten werden. Dabei erfolgt eine Durchführung verschiedener Angriffsarten (z.B. SSH Brute Force).

Die nächsten zwei Bereiche beschäftigen sich mit dem Aufzeichnen des Netzwerkverkehrs (mittels tcpdump), der Extrahierung relevanter Features (mittels CIC-Flowmeter) und der Vergabe von Labels. Die extrahierten Daten werden in einer Datenbank abgespeichert.
Der letzte Teil inkludiert die Thematik des neuronalen Netzes. Dabei soll ein Performance-Vergleich mit dem im Vorprojekt erzeugten Modell durchgeführt und die Eignung unterschiedlicher Datensätze geprüft werden.

1.9 Arbeitspaket-Spezifikationen (veraltet)

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 1.1 Projektstart durchführen	**AP-Inhalt** Kickoff-Meeting • Projektinhalt/-ziele festlegen (→ Projektauftrag) • Rahmenbedingungen ermitteln und niederschreiben • Projektvorgehensmodell auswählen • Projektorganisation und –kommunikation regeln
	AP-Nicht-Inhalte • Mit der Projektplanung beginnen • Abarbeiten von Arbeitspaketen
	AP-Ergebnisse • Klar definierte Ziele • Motivation geschaffen • Projektmitglieder werden auf denselben Informationsstand gebracht • Zusammenarbeit geregelt
	AP-Leistungsfortschrittsmessung • Kickoff-Meeting abgehalten / nicht abgehalten • Am Ende des Meetings überprüfen, ob Projektmitglieder alles verstanden haben

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 1.2 Projektcontrolling durchführen	**AP-Inhalt** • Sicherstellen, dass Projektziele erreicht werden • Projektfortschritt messen • Planabweichungen erkennen (z.B. Soll/Ist Vergleich) • Gegebenenfalls steuernde Maßnahmen einleiten
	AP-Nicht-Inhalte • Controllingverfahren nicht explizit festlegen • Nichtumsetzbare Vorgaben an Projektmitglieder erteilen • Datenbeschaffung vernachlässigen
	AP-Ergebnisse • Abweichungen vom Plan erkannt • Projektfortschritt ermittelt • Steuernde Maßnahmen rechtzeitig eingeleitet
	AP-Leistungsfortschrittsmessung • Soll/Ist Vergleich • Meilensteintrendanalyse • Kennzahlen

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 1.3 Projektkoordination durchführen	**AP-Inhalt** • Sicherung des Projektfortschrittes • Konflikte lösen • Risikomanagement durchführen • Technische und personelle Ressourcen steuern
	AP-Nicht-Inhalte • Maßnahmen mangelhaft kommunizieren • Unklare Verantwortungsbereiche definieren • Arbeitsprozesse nicht regelmäßig überprüfen
	AP-Ergebnisse • Kommunikation im Projekt festgelegt • Verantwortungsbereiche eindeutig festgelegt • Optimale Ressourcenverteilung
	AP-Leistungsfortschrittsmessung • Überprüfen, ob Deadlines eingehalten werden • Berichte

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 1.4 Projektabschluss durchführen	**AP-Inhalt** • Überprüfen, ob alle Ziele erreicht wurden • Wissen und Erfahrungen dokumentieren • Feedbackgespräche • Abschlussbericht erstellen • Projektabschlussfeier
	AP-Nicht-Inhalte • Auf Abschlussbericht verzichten • Verbesserungspotentiale nicht definieren
	AP-Ergebnisse • Projektnachbereitung durchgeführt • Lessons Learned dokumentiert • Projektdokumentation vervollständigt
	AP-Leistungsfortschrittsmessung Ermitteln, ob • Dokumentation vervollständigt ist • alle Ziele erreicht sind

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 2.1 Wissenschaftliche Paper WS erstellen	**AP-Inhalt** • Literaturrecherche durchführen zur Erstellung einer Grobkonzeption • Überblick über das Themengebiet schaffen • Basis für die Feinkonzeption im SS20 erstellen
	AP-Nicht-Inhalte • Detailplanung des Sommersemesters • Zusätzliche Paper weit über das Themengebiet hinaus erstellen
	AP-Ergebnisse • Wissenschaftliche Paper zum Einstieg in das Themengebiet fertiggestellt • Auf Basis der Paper kann mit Detailplanung begonnen werden
	AP-Leistungsfortschrittsmessung • Laufendes Reporting des aktuellen Stands an den Projektleiter • Überprüfung: Paper fertig / nicht fertig; fristgerechte Einhaltung der Deadline

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 2.2 Konzept f. Aufbau d. Infrastruktur erstellen	**AP-Inhalt** • Bedarfsermittlung: welche (Server-)Infrastruktur wird gebraucht (zur Durchführung der Angriffe) • Planen, wie die notwendigen Komponenten beschafft werden können (FH Technikum?) • Skizzieren des Aufbaues • Literaturrecherche
	AP-Nicht-Inhalte • Bereits mit dem praktischen Aufbau beginnen • Über Planungsschritte hinausarbeiten
	AP-Ergebnisse • Genau definierter Plan, welche Komponenten benötigt werden, wie diese beschafft werden und wie diese aufgebaut wird
	AP-Leistungsfortschrittsmessung • Laufendes Reporting des aktuellen (Planungs-)Stands an den Projektleiter • Überprüfung: Konzept fertig / nicht fertig; fristgerechte Einhaltung der Deadline

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 2.3 Planung d. Angriffsmethoden und -ziele	**AP-Inhalt** • Festlegen, welche Tools eingesetzt werden (zum Durchführen der Angriffe) • Definieren, welche Arten von Angriffen ausgeführt werden (DOS, SQL-Injection, etc…) • Angriffsziele festlegen (was soll angegriffen werden) • Literaturrecherche
	AP-Nicht-Inhalte • Praktische Ausführung der Angriffe • Alles, was über die Planung hinausgeht
	AP-Ergebnisse Vollständiges Konzept mit • Auflistung der auszuführenden Angriffe • Auflistung der zu verwendenden Tools • Beschreibung, worauf die Angriffe abzielen
	AP-Leistungsfortschrittsmessung • Laufendes Reporting an den Projektleiter (samt Erläuterung: was wurde bereits getan / fehlt noch, etc.) • Planung abgeschlossen / nicht abgeschlossen, Deadline eingehalten / nicht eingehalten

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 2.4 Data Gathering planen	**AP-Inhalt** • Spezifizieren, wie ausgeführte Angriffe bzw. gutartiger Traffic aufgezeichnet werden sollen • Festlegen, welche Tools für diesen Zweck eingesetzt werden sollen • Definieren, wo und wie die aufgezeichneten Informationen abgespeichert werden sollen • Literaturrecherche
	AP-Nicht-Inhalte • Über die Planungsphase hinausgehen • Feature Extraction planen
	AP-Ergebnisse • Konzept, wie das Mitschneiden des Netzwerktraffics erfolgt • Spezifizieren von einzusetzenden Tools / Speicherort
	AP-Leistungsfortschrittsmessung • Laufendes Reporting an den Projektleiter • Data Gathering Konzept fertig / nicht fertig, Deadline eingehalten / nicht eingehalten

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 2.5 Datenverarbeitung/-aufbereitung planen	**AP-Inhalt** • Festlegen, welche Features aus dem Datensatz relevant für Machine Learning sind • Festlegen, nach welchen Kriterien klassifiziert werden soll (z.B. DOS, gutartiges Datenpaket, etc.) • Planen wie Daten für das neuronale Netz aufbereitet und verarbeitet werden sollen • Literaturrecherche
	AP-Nicht-Inhalte • Schritte, welche über die Planung hinausgehen • Praktische Durchführung der Datenverarbeitung /-aufbereitung
	AP-Ergebnisse • Vollständiges Konzept, wie die Daten aufbereitet und verarbeitet werden sollen (Feature Extraction, Kriterien, etc.) • Abschluss der Planungsphase
	AP-Leistungsfortschrittsmessung • Reporting an den Projektleiter; bei Fertigstellung dem Projektauftraggeber mitteilen, dass Planungsphase beendet ist • Überprüfen, ob Deadline eingehalten wurde

projekthandbuch 001	ARBEITSPAKET-SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 3.1 Infrastruktur aufbauen	**AP-Inhalt** • Gemäß der in 2.2 erstellten Planung soll nun die Infrastruktur beschaffen und aufgebaut werden • Zusammenstellen der Komponenten zum Aufbau der Infrastruktur
	AP-Nicht-Inhalte • Bereits Angriffe auf Knoten des Systems durchführen • Nicht an die in 2.2 erstellte Planung halten
	AP-Ergebnisse • Vollständig aufgebaute Infrastruktur • Bereit für das Durchführen der Angriffe auf Knoten des Systems
	AP-Leistungsfortschrittsmessung • Reporting an den Projektleiter (was ist bereits erledigt, was nicht) • Infrastruktur erfolgreich aufgebaut / nicht erfolgreich aufgebaut

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 3.2 Angriffe durchführen	**AP-Inhalt** • Anhand der in 2.3 erstellten Planung, sollen nun die Angriffe auf Knoten des Systems durchgeführt werden (ggf. unter Verwendung von Tools) • Dabei sollen verschiedene Arten von Angriffen ausgeführt werden • Unterschiedliche Angriffsziele angreifen bzw. Schwachstellen ausnützen
	AP-Nicht-Inhalte • Nicht geplante Angriffsarten ausführen • Andere Angriffsziele, als jene die geplant sind, angreifen
	AP-Ergebnisse • Es wurden gezielt Angriffe auf Knoten des Systems mit der Serverinfrastruktur ausgeführt • Auch legitimer Traffic findet statt
	AP-Leistungsfortschrittsmessung • Reporting an den Projektleiter (was fehlt noch, was ist erledigt..) • Anzahl Angriffe durchgeführt durch Anzahl aller Angriffe • Angriffe durchgeführt / nicht durchgeführt

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 3.3 Data Gathering durchführen	**AP-Inhalt** • Gemäß der in 2.4 erstellten Planung: Aufzeichnen des Netzwerktraffics • Angriffe (und Angriffsarten) entsprechend kennzeichnen • Einsatz von Tools
	AP-Nicht-Inhalte • Nur bestimmte Features aufzeichnen (Feature Extraction erfolgt später) • Nicht plangemäß vorgehen
	AP-Ergebnisse • Traffic erfolgreich mitgeschnitten • Datenpakete entsprechend gekennzeichnet
	AP-Leistungsfortschrittsmessung • Reporting des aktuellen Status an den Projektleiter • Data Gathering fertiggestellt / nicht fertiggestellt; an Deadline halten

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 3.4 Datenverarbeitung / -aufbereitung durchführen	**AP-Inhalt** • Reduzierung der aufgezeichneten Daten auf relevante Features (→Feature Extraction) gemäß der Planung aus 2.5 • Verarbeitung und Aufbereitung der Daten für das neuronale Netz
	AP-Nicht-Inhalte • Nicht an die Planung halten • Daten mangelhaft aufbereiten / verarbeiten
	AP-Ergebnisse • Aufbereitete Daten, anhand denen ein neuronales Netz trainiert werden kann • Bereitstellung der Daten
	AP-Leistungsfortschrittsmessung • Reporting an den Projektleiter • Datenverarbeitung -aufbereitung fertig / nicht fertig

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 3.5 Performance-Vergleich Neuronales Netz durchführen	**AP-Inhalt** • Es soll ein Performance-Vergleich (unter Verwendung neuronaler Netze) der öffentlich verfügbaren Testdaten aus dem Vorprojekt, mit dem in diesem Projekt erstellten Datensatz durchgeführt werden. • Ergebnisse entsprechend dokumentieren
	AP-Nicht-Inhalte • Weitere Datensätze testen • Andere Machine Learning Algorithmen für diese Thematik ausprobieren
	AP-Ergebnisse • Ergebnis, welche Klassifizierungsgenauigkeit mit dem erstellten Datensatz und neuronalen Netzen möglich ist • Erkenntnis welcher Datensatz besser für diese Thematik geeignet ist
	AP-Leistungsfortschrittsmessung • Reporting an den Projektleiter • Performance-Vergleich durchgeführt / nicht durchgeführt

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 4.1 Projekthandbuch finalisieren	**AP-Inhalt** • Vervollständigen der Projektdokumentation • Aktualisieren von veralteten Inhalten • Zusammenfassen der Projektergebnisse
	AP-Nicht-Inhalte • Andere Tätigkeiten außer dem Dokumentieren
	AP-Ergebnisse • Vollständig ausgefülltes Projekthandbuch • Wesentliche Projektergebnisse und Erkenntnisse dokumentiert
	AP-Leistungsfortschrittsmessung • Überprüfen, wie weit das Projekthandbuch ausgefüllt ist • Reporting an den Projektleiter • Projekthandbuch vollständig / nicht vollständig

projekthandbuch 001	ARBEITSPAKET- SPEZIFIKATIONEN
PSP-Code, AP-Bezeichnung 4.2 Wissenschaftliche Paper SS erstellen	**AP-Inhalt** • Zwei wissenschaftliche Paper erstellen, um einen Überblick über die Thematik zu erhalten (WS 19/20) • Zwei wissenschaftliche Paper erstellen, um die wesentlichen Ergebnisse und Erkenntnisse der Projektausführung zu dokumentieren (SS 20)
	AP-Nicht-Inhalte • Zusätzliche Paper zu dieser Thematik erstellen • Plagiate aus bereits existierenden Arbeiten
	AP-Ergebnisse • Vollständige wissenschaftliche Paper die das Themengebiet und die praktische Durchführung abdecken
	AP-Leistungsfortschrittsmessung • Laufende Überprüfung des Status der Vollständigkeit • Deadlines eingehalten / nicht eingehalten

ARBEITSPAKET-SPEZIFIKATIONEN

PSP-Code, AP-Bezeichnung 4.3 Projektergebnisse präsentieren	**AP-Inhalt** • Schreiben des Projektabschlussberichtes • Präsentieren der wesentlichen Ergebnisse • Erkenntnisse und Erfahrungen für zukünftige Projekte weitergeben
	AP-Nicht-Inhalte • Bereits zukünftige Projekte zu dieser Thematik vorstellen
	AP-Ergebnisse • Projektauftraggeber und relevante Stakeholder wurden im Rahmen der Abschlusspräsentation über die wesentlichen Ergebnisse und Erkenntnisse der Projektausführung informiert
	AP-Leistungsfortschrittsmessung • Status Abschlussbericht überprüfen • Abschlusspräsentation zeitgerecht abgehalten / nicht abgehalten

1.10 Projektmeilensteinplan

projekthandbuch 001	PROJEKT- MEILENSTEINPLAN		
Meilenstein	**Basis-termine**	**Aktuelle Plantermine**	**Ist Termine**
Projektkickoff durchgeführt	18.02.2020	18.02.2020	18.02.2020
Projektplanung erstellt	03.04.2020	03.04.2020	03.04.2020
Proof of Concept erstellt • Erste Netzwerktoplogie umgesetzt • Eine Angriffsart wurde durchgeführt • Anfallender Netzwerkverkehr aufgezeichnet • Entsprechende Features extrahiert • Labels vergeben	01.05.2020	01.05.2020	
Datensatz fertiggestellt • Wie bei Proof Of Concept; weitere Szenarien durchgeführt	01.06.2020	01.06.2020	
Neuronales Netz – Performance Vergleich durchgeführt • Erzeugter Datensatz wird mit den neuronalen Netz aus dem Vorprojekt getestet • Vergleich der Performance	09.06.2020	09.06.2020	
Projektpräsentation durchgeführt • Präsentation wesentlicher Projektergebnisse und der Vorgangsweise durchgeführt	16.06.2020	16.06.2020	
Projektabnahme durchgeführt • Wissenschaftliche Paper erstellt • Wesentliche Projektmaterialien (Source Code, Datensatz, etc.) und Projekthandbuch an den Projektauftraggeber übergeben	30.06.2020	30.06.2020	

1.11 Projektzeitplan

Grundlegende Information:

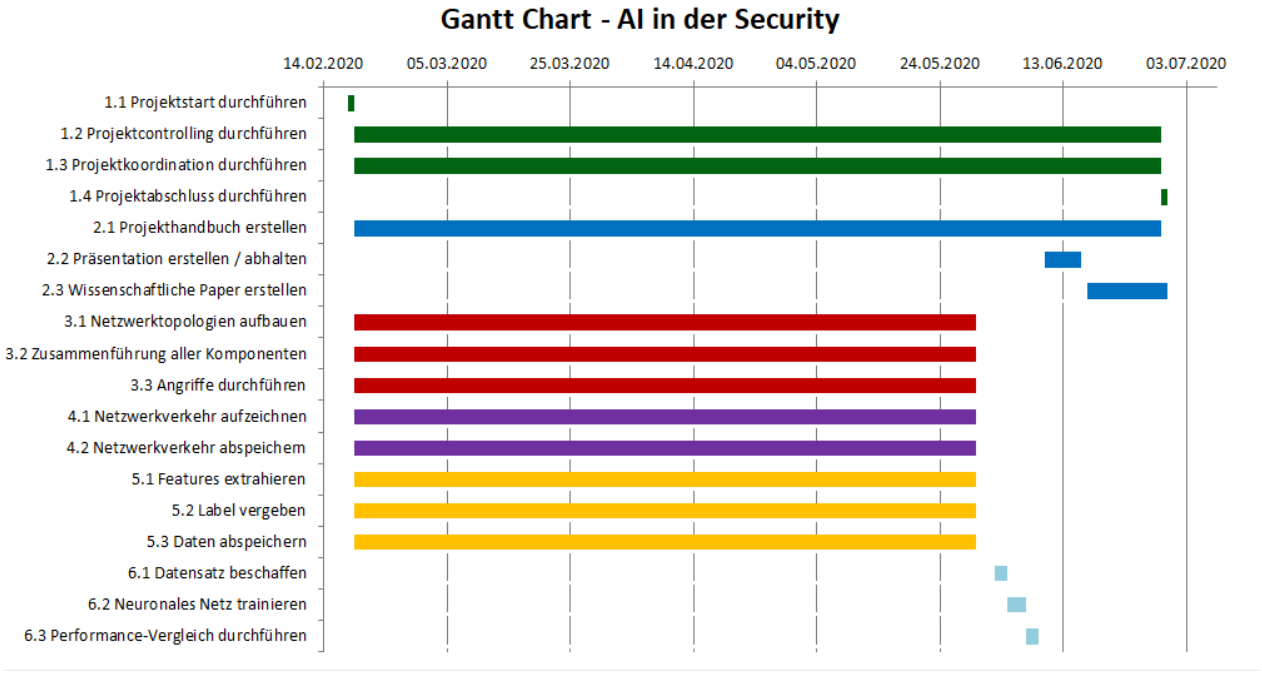
Semester	ECTS	ECTS in h	FH-Präsenzzeit in h	Anzahl Mitglieder	Gesamtaufwand aller Mitglieder in h
SS 20	4,5	112,5	22,5	5	562,5

Geplante Zeitaufteilung im SS20:

Aufgabe	Zeitdauer in h
LV-Anwesenheit	21 * 5 = 105
Planung	8 * 5 = 40
Einarbeiten in GNS3/notwendige SW	4 * 5 = 20
Netzwerktopologie(n) inkl. Angriffe aufbauen	50
Recorder erstellen	40
Extraktor erstellen	40
Zusammenführung der Komponenten	50
Performance-Vergleich NN	27,5
Abschlusspräsentation (+Vorbereitung)	6 * 5 = 30
Projektdokumentation und -management	60
Erstellen der wissenschaftlichen Paper	20 * 5 = 100

1.12 Projektbalkenplan

Arbeitspaket-Name	Start	Ende	Dauer (Tage)
1.1 Projektstart durchführen	18.02.2020	19.02.2020	1
1.2 Projektcontrolling durchführen	19.02.2020	29.06.2020	131
1.3 Projektkoordination durchführen	19.02.2020	29.06.2020	131
1.4 Projektabschluss durchführen	29.06.2020	30.06.2020	1
2.1 Projekthandbuch erstellen	19.02.2020	29.06.2020	131
2.2 Präsentation erstellen / abhalten	10.06.2020	16.06.2020	6
2.3 Wissenschaftliche Paper erstellen	17.06.2020	29.06.2020	13
3.1 Netzwerktopologien aufbauen	19.02.2020	30.05.2020	101
3.2 Zusammenführung aller Komponenten	19.02.2020	30.05.2020	101
3.3 Angriffe durchführen	19.02.2020	30.05.2020	101
4.1 Netzwerkverkehr aufzeichnen	19.02.2020	30.05.2020	101
4.2 Netzwerkverkehr abspeichern	19.02.2020	30.05.2020	101
5.1 Features extrahieren	19.02.2020	30.05.2020	101
5.2 Label vergeben	19.02.2020	30.05.2020	101
5.3 Daten abspeichern	19.02.2020	30.05.2020	101
6.1 Datensatz beschaffen	02.06.2020	04.06.2020	2
6.2 Neuronales Netz trainieren	04.06.2020	07.06.2020	3
6.3 Performance-Vergleich durchführen	07.06.2020	09.06.2020	2



1.13 Projektkommunikationsstrukturen

projekthandbuch 001	PROJEKT- KOMMUNIKATION			
Bezeichnung	**Ziele, Inhalte**	**Teilnehmer**	**Termine**	**Ort**
Management-Sitzung	• Diskussion Projektstatus, Abweichungen im Projekt • Entscheidungsfindung auf Basis der Projektcontrolling-Sitzung • Freigabe Projektfortschrittsbericht	Projektauftraggeber, Projektleiter	Monatlich, am ersten Mittwoch	Microsoft Teams
Projektcontrolling-Sitzung	• Projektstatus • Controlling Leistungsfortschritt, Termine und Ressourcen • Controlling der Umweltbeziehungen • Soziales Projektcontrolling • Diskussion übergeordneter Problemstellungen • Entscheidungsaufbereitung für Projektauftraggeber-Sitzung	ProjektleiterIn, Projektteam, Projektcoach	Wöchentlich, am Dienstag	Microsoft Teams
Projektteambesprechung	• Besprechung aktueller Probleme • Besprechung weitere Vorgehensweise • Aufgabeneinteilung • Konfliktlösung	Projektleiter, Projektteam	Wöchentlich, am Montag	Microsoft Teams

1.14 Projektrisikoanalyse

PROJEKT-RISIKOANALYSE							
Risiko-beschreibung, Ursache	Priorität	Risiko-kosten	Eintritts-wahrschein-lichkeit	Risiko-budget	Ver-zögerung	Präventive und korrektive Maßnahmen	Risiko-minimierungs-kosten
(Text)	*(Auswahl)*	*(Euro)*	*(Prozent)*	*(Euro)*	*(Wochen)*	*(Text)*	*(Euro)*
Ausfall eines Teammitgliedes	m	/	40	/	2	Arbeit gut aufteilen und rechtzeitig reagieren	/
Netzwerksimulator stellt sich als ungeeignet dar	m	/	10	/	2	Rechtzeitig ausprobieren und versuche Proof of Concept umzusetzen	/
Schwierigkeiten beim Aufzeichnen des Traffics	l-m	/	15	/	1	Anderes Tool verwenden, Frühzeitig Testen	/
Tools zum Durchführen der Angriffe ungeeignet	m	/	25	/	3	Weitere Tools recherchieren und ausprobieren	/
Probleme beim Zusammenführen von Recorder, Extraktor, Topologie entstehen	m	/	15	/	2	Kontrolle der Durchführung, Zeitpolster einplanen	/
Zu komplizierte Netzwerktopologien geplant	m	/	25	/	2	Review durch andere Kollegen, Schnelle Reaktion	/
Finden aussagekräftiger Features schwierig	l	/	15	/	1	Ausprobieren und Testen weiterer Features	/
Source Code aus dem Vorprojekt nicht lauffähig	l	/	10	/	1	Debuggen und versuchen das Problem rechtzeitig zu lösen	/
Anforderungen verändern sich erheblich	h	/	3	/	5	Regelmäßiges Feedback des Projektauftraggebers einholen	/
Meilensteine können nicht eingehalten werden	l-m	/	20	/	2-3	Regelmäßige Fortschrittskontrolle	/

1.15 Projektdokumentation

Bereich	Beschreibung
Ablage	Die im Zuge des Projekts erstellten Dokumente müssen am Projektserver der FH Technikum Wien abgespeichert werden. Zusätzlich erfolgt eine Versionsverwaltung mittels git.
Zugriffs-berechtigung	Auf die entstehenden Dateien dürfen nur der Projektauftraggeber, der Projektleiter, sowie die Projektteammitglieder Lese- und Schreibzugriff haben.
Namenskonvention	Die Benennung der im Laufe des Projekts entstehenden Dateien muss klar und eindeutig erfolgen. Anhand des Dateinamen soll der Ersteller bzw. der Titel (z.B. Projekthandbuch) des Dokuments, ersichtlich sein.
Spielregeln	Die durchgeführten Arbeiten beziehungsweise die gewonnen Erkenntnisse müssen zeitnah und verständlich dokumentiert werden.