Vorläufiges Thema

Bachelorarbeit
zur Erlangung des Grades *Bachelor of Science*

an der
Hochschule Niederrhein
Fachbereich Elektrotechnik und Informatik
Studiengang *Informatik*

vorgelegt von
Robert Hartings
Matrikelnummer: 1164453

Datum: 19. Mai 2020

Prüfer: Prof. Dr. Jürgen Quade
Zweitprüfer: Prof. Dr. Jürgen Quade

Eidesstattliche Erklärung

Name: Robert Hartings
Matrikelnr.: 1164453
Titel: Vorläufiges Thema

Ich versichere durch meine Unterschrift, dass die vorliegende Arbeit ausschließlich von mir verfasst wurde. Es wurden keine anderen als die von mir angegebenen Quellen und Hilfsmittel benutzt.

Die Arbeit besteht aus _____ Seiten.

_____ _____

Ort, Datum Robert Hartings

Inhaltsverzeichnis

1 Einleitung

Das Thema IT Sicherheit ist besonders in den letzten Jahren relevant geworden. Viele Firmen suchen Experten[1], welche die bestehen und neue designeten Systeme auf Sicherheitslücken prüfen und Lösungsvorschläge zur deren Behebung präsentieren. Auch werden Experten gesucht, welche die im Unternehmen bestehenden Prozesse prüfen und neue Prozesse zum Umgang mit Sicherheitslücken entwerfen.

Einen Mangel an IT-Security in privat und öffentlich Unternehmen beziehungsweise ein fehlendes Konzept zur Vorbeugung, Erkennung und Abwendung von Sicherheitslücken sieht man auch in jüngster Vergangenheit deutlich, nachdem beispielsweise diverse Universitäten wie Gießen, Maastricht und Bochum Ende 2019 Ziele von Hackerangriffen geworden sind. Aber nicht nur Universitäten sind betroffen, so ist neben Gerichten, Stadtverwaltungen und Krankenhäusern bereits der Deutsche Bundestag von Hackern angegriffen und kompromittiert worden.

In der Studie „Wirtschaftsschutz in der digitalen Welt“ vom 06. November 2019 des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. Bitkom wird die aktuelle Bedrohungslage durch Spionage und Sabotage für deutsche Unternehmen untersucht. Aus dieser Studie geht hervor, dass im Jahr 2019 von Datendiebstahl, Industriespionage oder Sabotage 75% der befragten Unternehmen[1] betroffen und 13% vermutlich betroffen waren. Die Zahlen der betroffenen Unternehmen ist steigend. Im Jahre 2015 waren „nur“ 51% betroffen und 28% vermutlich betroffen. Die Unternehmen beziffern den Schaden auf 102,9 Milliarden Euro pro Jahr.[2]

Das dieses auch im Lehrbetrieb angekommen ist, sieht man an neu startenden Studiengängen wie dem Bachelorstudiengang Cyber Security Management der Hochschule Niederrhein, welcher zum kommenden Wintersemester 2020/21 startet.[3]

Aber es ist zu erwähnen, dass die Hochschulen sich bereits mit dem Thema auseinandersetzen. So beschäftigt sich an der Hochschule Niederrhein das Institut für Informationssicherheit Clavis besonders mit Themen rund um das Informationssicherheitsmanagement, gestaltet aber auch Inhalte zur Vulnerabilität von (kritischer) Infrastruktur und Hacking. Das Ziel von Clavis ist die Erhöhung der Informationssicherheit von Organisationen im regionalen Umfeld der Hochschule. [4] Auch hat die Hochschule Niederrhein das Thema IT-Sicherheit bereits in

[1] Die Grundlage der Studie sind 1070 (2019) und 1074 (2015) befragte Unternehmen

Ihren Lehrplan für die Studiengänge Informatik und Elektrotechnik am Fachbreich 03 Elektrotechnik und Informatik aufgenommen. So werden dort im fünften Semester in der Veranstaltung IT-Security grundlegenden Kompetenzen zum Thema IT-Sicherheit vermittelt, welche einem allgemeinen Anspruch genügen.[5]

1.1 Motivation

Neben diversen Meldung zu erfolgreichen Angriffen auf Unternehmen und öffentliche Körperschaften, bin ich durch die Veranstaltung IT-Security im fünften Semester, besonders herauszuheben sind hier die Praktika[2], auf das Thema IT Sicherheit aufmerksam geworden.

Im Anschluss an das erfolgreiche Absolvieren des zweiten Praktikums „Catch me, if you can“ habe ich die Betreuer gefragt, ob es eine Übersicht gibt, welche das Abschneiden der verschiedenen Gruppen über das Semester darstellt. Diese Ansicht hätte ich mir aus verschiedenen Backups erstellen können. Hier hätte ich mir ein generierte Übersicht gewünscht.

Auch bin ich der Meinung, dass es zum heutigen Stand bessere Möglichkeiten gibt, die Darstellung (Web Oberfläche) und Funktionsweise zu realisieren.

Da ich an dem Praktikum sehr viel Spaß hatte und ich mich für Web-Entwicklung interessiere, möchte ich im Rahmen meiner Bachelorarbeit, das mittlerweile 10 Jahre alte System modernisieren, überarbeiten und erweitern.

1.2 Aufgabenstellung

Begleitend zu der Veranstaltung IT-Security für die Studiengänge Bachelor Informatik und den Bachelor Elektrotechnik des Fachbereichs 03 Elektrotechnik und Informatik der Hochschule Niederrhein werden 3 Praktika durchgeführt. Diese sollen den Studierenden praktisch Erfahrungen ermöglichen.

Das zweite Praktikum „Catch me, if you can“ stellt einen Vergleichswettbewerb dar. An diesem Wettbewerb nehmen mehrere Teams teil, welche sich alle in einem gemeinsamen Netzwerk befinden. Die Aufgabe der Teams besteht darin, festgelegte IT-Dienste (abgesichert) bereit zustellen, geheime Informationen sowohl auf dem eigenen Rechner als auch auf den Rechnern der anderen Teams zu finden und zu verhindern, dass andere Teams an die eigenen geheimen Informationen gelangen.[6, S. 2] Die geheimen Informationen sind logisch gesehen Passwörter oder private Bilder und werden durch sogenannte Flags repräsentiert. Eine Flag ist ein gehashter Zeichenfolge und hat immer die gleiche Länge.

[2] Praktikum ist hierbei mit einer Pflichtübung vergleichbar

Das Praktikum wird durch ein Auswertungs- und Überwachungssystem überwacht - anderes Wort -, welches eine objektiv nachvollziehbare Bewertung vornehmen kann und die in den Bewertungsprozess eingeflossenen Parameter dokumentiert.[6, S. 2]

Ziel meiner Arbeit ist die Modernisierung und Verbesserung dieses Auswertungs- und Überwachungssystems.

In der einführenden Betrachtung (Kapitel 2) wird der aktuelle Stand des Systems, Schnittstellen zwischen Server und Client sowie der Begründung für die Veränderung dargelegt.

Aus dieser einführenden Betrachtung werden dann im Kapitel 3 Entwurf Anforderungen abgeleitet und Entwürfe für die verschieden Komponenten des Servers erstellt.

An Hand der abgeleiteten Anforderungen und des Entwurfs der verschiedenen Komponenten wird im Kapitel 4 Technologien verschiedene Technologien diskutiert und passende Technologien ausgewählt.

Die Implementierung des Entwurfs mit den gewählten Technologien wird im Kapitel 5 Realisierung beschrieben.

Eine kritische Auseinandersetzung mit dem Ergebnis dieser Arbeit folgt und es werden Aussichten für mögliche Veränderungen und Verbesserungen gegeben.

2 Analyse

In diesem Kapitel werden die Voraussetzungen im Labor vorgestellt, die derzeitige Implementierung des Auswertungs- und Überwachungssystems beleuchtet und kurz auf einen überwachten Client sowie dessen Schnittstellen zum System eingegangen.

Die Lehrveranstaltung „IT-Sicherhiet“ der Hochschule Niederrhein beschäftigt sich mit den Gefährdungszielen Integrität von Daten, Nutzbarkeit von Systemen und der (digitalen) Privatsphäre vertraut machen.[7]

Die Lehrveranstaltung ist in Vorlesung, Übung und Praktikum untergliedert. Durch die Praktika sollen sich die Studierende praktisch mit dem Thema beschäftigen und beweisen, dass sie die in der Lehrveranstaltung vermittelten Themen verstanden haben.

Das Praktikum „Catch me, if you can“ ist das zweite von drei Praktika, welches die Studierenden als Voraussetzung für die Klausurteilnahme erfolgreich absolvieren müssen.

Bevor die Studierenden am Praktikum teilnehmen können, müssen diese ein sogenanntes Hackit[1] lösen und das erhalte Passwort zum nächsten Termin mitbringen. Ohne dieses Passwort ist die Teilnahme am Praktikum nicht möglich.

2.1 Ausstattung Labor

Das Praktikum wird im Labor für Echtzeitsysteme (EZS Labor) der Hochschule Niederrhein durchgeführt.

Das Labor ist mit acht Gruppenarbeitsplätzen für Studenten sowie Arbeitsplätzen für die Betreuer und Mitarbeiter ausgestattet. Ein Arbeitsplatz der Betreuer kann zu einem neunten Gruppenarbeitsplatz umfunktioniert werden.

An einem Gruppenarbeitsplatz können 2 Studierende gleichzeitig arbeiten, da diese mit einem leistungsfähigem Desktop-PC und einem Raspberry Pi[2] sowie den dazugehörigen Peripheriegeräten (Maus, Tastatur & Monitor) ausgestattet sind. Auf den Desktop-PCs ist Ubuntu[3] und auf den Raspberry Pis ist Raspbian[4] als Betriebssystem installiert.

[1] Aufgabe aus dem Bereich IT-Security / Hacking
[2] Einplatinencomputer mit der Größe einer Kreditkarte
[3] Ubuntu ist eine freie Linux Distribution auf Basis von Debian
[4] Abwandlung von Debian für den Raspberry Pi

Auf den Desktop-PCs ist die Software VirtualBox der Firma Oracle installiert. Diese Software ermöglicht es auf dem Rechner einen weiteren Rechner zu virtualisieren. Dieser weitere PC wird Guest genannt und kann den Host, den Rechner auf dem die Software VirtualBox läuft, nicht schädigen oder beeinflussen. Sollte auf dem Guest ein Virus aktiv werden, kann dieser nicht den Host angreifen. Hierbei sollte beachtet werden, dass die Software VirtualBox Fehler haben kann oder der Nutzer Einstellungen getroffen hat, sodass der Host doch angreifbar ist.

Neben diesen Rechner steht ein Linux Server zur Verfügung, auf welchem das Auswertungs- und Überwachungssystem läuft.

Alle Rechner, auch die Guest System der Studentengruppe, sind untereinander via Ethernet verbunden.

Auch steht ein Beamer zur Verfügung auf dem die aktuelle Spielübersicht dargestellt werden kann.

2.2 Systemkomponenten

2.2.1 Komponenten des Servers

Im folgenden werden die verschiedenen Komponenten des Auswertungs- und Überwachungssystems in der derzeitigen Implementierung untersucht. Dabei werden Rückschlüsse auf Anforderungen gezogen sowie Schwachstellen und Verbesserungsmöglichkeiten herausgearbeitet.

Scanner

Der Scanner prüft in regelmäßigen Abständen, welcher beim Start des Spieles in der Web Oberfläche eingestellt werden kann, die auf den Guest Systemen der Studierenden installierten Dienste und speichert das Ergebnis ab. Die folgenden Dienste werden pro Team geprüft.

ScanUp Die Aufgabe dieses Scanns besteht darin zu prüfen, ob das Guest System noch für den Server erreichbar ist. Sollte das Guest System nicht erreichbar sein wird hierfür ein Strafpunkt vergeben. Aus technischer Sicht wird das Linux Kommando *ping* verwendet. An Hand des Rückgabewertes kann nachvollzogen werden, ob der Server das Guest System erreichen konnte.

ScanBubble Auf dem Guest System läuft ein selbst programmierter Bubble Server, welcher Flags via Telnet bereitstellt. Nach dem eine Flag abgeholt worden ist, erfolgt ein Timeout, sodass für eine bestimmte Zeit keine weitere Flag abgeholt werden kann. Der Bubble Server nimmt Anfragen auf dem Port *12321* für unverschlüsselte Flags und Port *12322* für verschlüsselte Flags entgegen. Der Scanner überprüft, ob eine Telnet Verbindung zu Port *12321* möglich ist, in dem der Scanner eine Telnet Verbindung öffnet und prüft, ob die Verbindung erfolgreich war.

ScanWebUp Jedes Guest System stellt mit Hilfe eines Apache Web Servers und php-Dateien Webseiten und Daten bereit, welche mit Hilfe von Web Clients abgerufen werden können. Dazu muss auf Port *80* der HTTP- und auf Port *443* der HTTPS Dienst laufen. Dieses verifiziert der Scanner in dem dieser eine Socket Verbindung zu den Ports *80* und *443* öffnet und das Ergebnis prüft.

ScanSQLInjectUp Dieser Scanner prüft, ob das Team die SQL Injection bereits bei sich durchgeführt hat. Dazu wird geprüft ob die Datei, welche nach der erfolgreichen SQL Injection angelegt wird, bereits angelegt worden ist. Damit die Studierenden die Datei nicht per Hand anlegen können, wird geprüft ob die Datei mit einem mitgegebenen Nutzernamen und Passwort erfolgreich eine SQL Abfrage stellen kann. Das Ergebnis wird dann mit dem erwarteten Ergebnis verglichen.

ScanSQLInjectSave Wie bei ScanSQLInjectUp (2.2.1) wird geprüft ob die angelegte Datei das erwartet Ergebnis zurück liefert. Besonderheit hierbei ist, dass statt einer validen Kombination aus Nutzernamen und Passwort eine SQL Injection im Nuterznamen übergeben wird. So kann geprüft werden, ob das Team die SQL Injection abgesichert hat.

ScanXSSSave Dieser Scanner prüft, ob der auf dem Guest System mögliche XSS Angriff behoben worden oder weiterhin möglich ist. Dazu wird die Webseite mit Payload, welches einen XSS Angriff darstellt, aufgerufen. In der Rückgabe wird geprüft, ob der Payload ungefilter auf der Webseite zu finden ist. Sollte diese der Fall sein, ist der XSS Angriff möglich und nicht oder unzureichend von den Studierenden abgesichert worden.

ScanSQLSave Bei diesem Scan wird geprüft, ob die Verbindung mit dem auf allen System voreingestellten Passwort *toor* auf dem Root Account der SQL Datenbank *root* möglich ist. Oder ob die Studierenden dieses unsichere Passwort geändert haben.

ScanFTPSave Auf dem Client System läuft ein FTP Server, welcher ohne Login (Nutzername & Passwort) Daten bereitstellt. Der Scanner prüft, ob ein sogenannter Anonymous Login möglich ist, in dem eine sFTP Verbindung ohne Login aufgebaut wird. Sollte die Verbindung erfolgreich sein, ist der Anonymous Login immer noch möglich.

ScanTelnetSave Ein Telnet Server wartet auf Verbindungen auf Port *23*. Da dieser Dienst nicht benötigt wird, sollen die Studierende diesen Dienst abschalten oder deinstallieren. Der Scanner prüft, ob eine Verbindung via Telnet auf Port *23* möglich ist, in dem dieser eine Verbindung via Telnet zu Port *23* aufbaut und prüft ob die Verbindung erfolgreich war.

Generierung von Flags

Derzeitig erfolgt die Generierung der Flags sowohl auf den Clients als auch auf dem Server. Dies ist in sofern notwendig, da der Server sonst nicht prüfen könnte, ob die von den Studierenden abgegebenen Flags gültig sind. Für die Generierung wird folgender Algorithmus verwendet.

```
function generate($ip,$anzahl,$filename,$SALT){
        ...
        for($i=0;$i<$anzahl;$i++) {
                $seed=$SALT.$ip."Aufgabe".$i;
                $string.=md5($seed);
                $string.=";";
        }
        ...
}
```

Listing 2.1: Algorithmus zur Generiung der Flags

Webserver

Abgabe von Flags

2.2.2 Komponenten des Clients

Da sich die Bachelorarbeit mit der Modernisierung des Auswertungs- und Überwachungssystem beschäftigt, sind nur die wichtigen Komponenten des Clients beschrieben.

Webserver des Clients

2.3 Schnittpunkte zwischen Server und Clients

2.4 Abgeleitete Anforderungen

3 Entwurf

4 Technologien

5 Realisierung

6 Ergebnis

7 Zusammenfassung & Aussicht

Anhang

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

Literatur

[1] it-daily.net. (3. März 2019). IT-Security-Experten Werden Händeringend Gesucht - It-Daily.Net, Adresse: https://www.it-daily.net/analysen/20773-it-security-experten-werden-haenderingend-gesucht (besucht am 16. 05. 2020).

[2] A. Berg und M. Niemeier, „Wirtschaftsschutz in der digitalen Welt," S. 13, 11. Juni 2019.

[3] Hochschule Niederrhein. (7. Feb. 2020). Hackern die rote Karte zeigen - Neuer Studiengang Cyber Security Management, Adresse: https://www.hs-niederrhein.de/startseite/news/news-detailseite/?tx_news_pi1%5Bnews%5D=18990&cHash=e849d260ecd92cf53fc9c98f6dc9edaa (besucht am 16. 05. 2020).

[4] ——, *Flyer Institut Clavis*. Adresse: https://www.hs-niederrhein.de/fileadmin/dateien/Institute_und_Kompetenzzentren/Clavis/Flyer_Institut_Clavis__5_.pdf (besucht am 16. 05. 2020).

[5] ——, *Modulhandbuch Vollzeit BA Informatik*, 9. Dez. 2019. Adresse: https://www.hs-niederrhein.de/fileadmin/dateien/FB03/Studierende/Bachelor-Studiengaenge/PO2013/modul__bi.pdf (besucht am 16. 05. 2020).

[6] A. Sosna, „Konzeption und Realisierung eines modular aufgebauten Auswertungs- und Überwachungssystems zur Durchführung von IT-Sicherheitsschulungen.," Bachelor Arbeit, Hochschule Niederrhein, Juni 2010, 98 S.

[7] J. Quade, *Was Sie schon immer über IT-Security wissen sollten... Eine praxisorientierte Einführung in die Rechner- und Netzwerksicherheit*. 18. Sep. 2019, Bd. 2.0, Version 2.0.