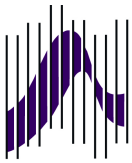
Hochschule
Ravensburg-Weingarten



Hochschule
Ravensburg-Weingarten
Technik | Wirtschaft | Sozialwesen

Erstellung eines automatisierten Phishing-Mailgenerators

Bachelorarbeit

Social Engineering

im Studiengang Angewandte Informatik

an der Hochschule Ravensburg - Weingarten

von

Marco Lang Matr.-Nr.: 27416

Abgabedatum : 5. November 2018

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit mit dem Titel

Generierung eines personalisierten Mail-Generators

selbststandig angefertigt, nicht anderweitig zu Pruefungszwecken vorgelegt, keine anderen als die angegebenen Hilfsmittel benutzt und woertliche sowie sinngemaesse Zitate als solche gekennzeichnet habe.

Weingarten, 5. November 2018

Autor Name

_____

Inhaltsverzeichnis

Kurzfassung

Abstract

Danksagung

Vorwort

1 Einleitung

1.1 Motivation

In der heutigen Zeit wird das Thema Informationssicherheit immer wichtiger. Systeme werden immer komplexer und Firewalls immer besser. Doch laut dem Bundeskriminalamt hat sich die Zahl der Cyberkriminalität mit einem klaren Trend nach oben entwickelt. [Bun18]
Eine häufig verwendetet Technik von Cyberkriminalität ist das E-Mail-Phishing. Hier wird der Mensch als Schwachstelle des Systems genutzt. In den neusten Fällen von Phishing-Attacken zeigt die Verbraucherzentrale Nordrhein-Westfalen, dass diese meist direkt an eine Person adressiert sind. Beispielsweise wird man in den gefälschten DSGVO-E-Mails, im Namen der Sparkasse, persönlich mit Namen angesprochen. [NW18]
Im Rahmen dieser Abschlussarbeit wird gezeigt, mit welchem Aufwand solche Angriffe verbunden sind und wie die Suche nach privaten Informationen im Internet aussieht.

1.2 Problem

Leser Problem komplett erklären, weiterführende Motivation

1.3 Eigene Leistung

Was werd ich neues Erfinden/Schaffen?!!!!

In dieser Arbeit wird ein Phishing-Mailgenerator erstellt. Dieser liest automatisiert Informationen von der Webseite www.fupa.net heraus und erstellt potentiellen Opferprofile. Zusätzlich wird mit dieser Information und einem Web-Crawler das Internet nach weiteren Informationen

durchstöbert. Mit dem Vornamen, Nachnamen und dem Geburtsjahr werden die E-Mail-Adressen generiert. Die gefundenen Informationen werde automatisch in eine personalisierte Phishing-E-Mail eingebaut. Für einen höheren Erfolg werden E-Mail-Muster erstellt.

1.4 Aufbau der Arbeit

Beispielsweise in Kapitel 3 finden sie das und in Kapitel 4 das.

Meine Arbeit gliedert sich in zwei Teile. Einem theoretischen und einem praktischen Teil. In der Theorie wird auf das Thema Social Engineering eingegangen. Speziell auf das Thema E-Mail Phishing. In dem praktische Teil wird der Phishing-Mailgenerator erzeugt und beschrieben. Der hier enthaltene Suchalgorithmus und die verbundene Verwaltung der Information, sowie die E-Mail-Generierung wird der Forschungsaspekt sein.

2 Grundbegriffe

2.1 Social Engineering

Definition

Die Definition von Social Engineering (SE) ist nicht eindeutig. Es gibt sehr verschiedene Ansichten von der Definition. Die Idee von Social Engineering ist, eine Ziel so zu manipulieren, damit das Ziel eine für den Angreifer bessere Entscheidung trifft. In dem Buch Social Engineering - The Art of Human Hacking, von Christopher Hadnagy, ist Social Engineering definiert als “social engineering is the act of manipulating a person to take an action that may or may not be in the “target’s“ best interest“ [Had11]. Die Definition in dem Buch von Kevin D. Mitnick lautet:“Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology“ [Mit01].
!!!!!!!!!!Umschreiben!!!!!!!!!!
Wie bereits erwähnt, nutzt ein Social Engineer menschliche Wünsche, Ängste und verbreitete Verhaltensmuster aus, um seine Opfer zu manipulieren. [uDsiNe15]

SE im Alltag

SE wird einem von Geburt an beigebracht und begegnet einem beinahe jeden Tag. Schon ein Baby muss wissen wie es die Eltern manipulieren kann damit man Dinge wie Essen, Zuneigung, o.ä. bekommt. Darüber hinaus ist SE in vielen Berufen ein täglicher Bestandteil. Beispielsweise manipulieren Ärzte viele Patienten mit einer Placebo-Behandlung. Bei dieser Behandlung wird dem Patient ein wirkstoff-freies Medikament verschrieben. Nur durch die Manipulation des Patienten und den sogenannten Palzebo-Effekt können Erfolge erzielt

werden.

SE in der Informationssicherheit

Im Bereich der Informationssicherheit spricht man von Social Engineering wenn man durch Manipulierung bzw. das Hacken von Menschen Passwörter, Zugänge zu Systemen oder vertrauliche Information bekommt. Die bekanntesten Angriffsmethoden sind Phishing, Pretexting, Baiting und Quad Pro Quo. Bei dieser Arbeit wird aber hauptsächlich auf das Thema Phishing eingegangen.

2.1.1 Social Engineering Angriffe

Aufbau eine SE-Angriffzykluses

Der Aufbau eines Social-Engineering-Angriffes ist definiert in mehrere Phasen. Das wohl bekannteste Modell für einen Social Engineering-Angriffszyklus ist in dem Buch von Kevin D. Mitnicks - The art of deception: controlling the human element of security [Mit01] definiert. Dieser Zyklus besteht aus den 4 Phasen Research, Developing rapport and trust, Exploiting trust und Utilize information. In der Research-Phase geht es um die Informationsbeschaffung, bei der der Angreifer möglichst viel Informationen über das Ziel herausfindet. Die Developing rapport and trust Phase beschreibt den aufbau für einen guten Kontakt, da der Angreifer ein leichteres Spiel hat wenn das Ziel dem Angreifer vertraut. Das nun erzeugte Vertrauen wird in der Exploitung trust Phase ausgenutzt. Hier will der Angreifer die eigentlich Information vom Opfer herausfinden. Dies geschieht einerseits durch bestimmtes nachfragen oder Manipulation. Utilize information ist die letzte Phase. Dort wird die gewonnene Information genutzt um das eigentliche Ziel des Angreifers zu erreichen.

!!!!!!!!BILD EINFÜGEN!!!!

SE Attack Framework

Leider sind die Phasen in dem Buch von Mintnick [Mit01] nicht sehr detailliert beschrieben. Aus diesem Grund haben die Autoren von der Publikation "Social Engineering Attack Framework" [FM14] ein Framework erstellt, was eine Erweiterung von Mitnick's Angriffszykluses darstellt.

!!!!!!!!BILD EINFÜGEN!!!!

Phishing

Das Wort Phishing wird von dem Wort "fishing" abgeleitet, da die Angreifer nach Informationen fischen. Das "Ph" kommt von "sophisticated" und meint damit, dass die Angreifer ausgeklügelte Techniken verwenden um an Informationen heranzukommen. [Jam05]
Phishing ist ein Angriffsmethode, bei dem ein Angreifer glaubwürdige E-Mails versendet, um von einem Opfer Informationen zu erhalten. Die sogenannten E-Mails enthalten meist eine Aufforderung einen Link zu öffnen und sehen täuschend echt aus. Zum Beispiel könnten der Angreifer ein Layout von Amazon verwenden und Sie auffordern, den Link zu öffnen, wegen einem Authentifizierungsproblem. Nachdem Sie auf den Link geklickt haben müssen Sie sich anmelden. Hier könnten die Angreifer Ihre Anmeldedaten abgreifen, nachdem Sie sie eingeben haben. Sobald Sie die Anmeldedaten haben könnten Sie mit der Meldung :"Hoppla, ein Fehler ist aufgetreten, melden Sie sich bitte neu an!" auf die originale Seite weitergeleitet werden. Durch diesen Vorgang hätten die Angreifer ihre Anmeldedaten bekommen.
Für diese Methode benötigt der Angreifer nicht nur Social Engineering Fähigkeiten sonder auch technische. [CH15]

Spear-Phishing

Spear-Phishing ist im Prinzip die gleiche Angriffsmethode wie Phishing. Nur dass hier anstatt einer anonymen E-Mail eine persönliche Mail gesendet wird. Beispielsweise wird man hier mit einem Namen angesprochen oder man bekommt Mails mit Inhalten die einen interessieren. Aus diesem Grund benötigt man hier Zeit für die Informationsbeschaffung. Dennoch ist der Erfolg hier sehr vielversprechender als beim normalen Phishing. Desweitern ist Spear-Phishing oft mit E-Mail-Spoofing verbunden. 91% der APT Angriffe auf Firmen beginnen mit einer

Spear-Phishing-E-Mail. Advanced Persistent Threat (APT). Die Schadsoftware wir meisten als Remote Access Trojans (RATs) in einem Zip-Datei überliefert.

Pretexting

Als Polizist verkleiden, etwas vortäuschen

Baiting

ähnelt Phishing, wie Trojanisches Pferd aber mit physischen Gegenständen. Gier und Neugier werden ausgenutzt. Beispielsweise USB-Stick liegen lassen mit Malware und warten bis ihn jemand findet und öffnet.

Quad Pro Quo

Etwas geben dafür etwas bekommen. Werben für einen Service. Kostenlose Musik für Anmeldedaten.

2.2 Webtools

2.2.1 Web-Crawler

Suchmaschine

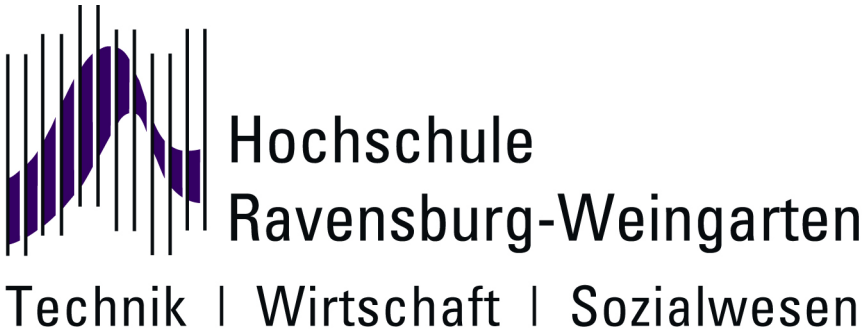


Bild 2.1: Logo der HS – oder nicht?

Tabelle 2.1: Verwendete Matrizen

Matrix	Dimension	Symbol
Systemmatrix	$n \times n$	$\mathbf{A}$
Ausgangsmatrix	$m \times n$	$\mathbf{C}$

2.2.2 Web-Scraper

2.2.3 E-Mail

SMTP

2.3 Sprachen

2.3.1 HTML

2.3.2 CSS

2.3.3 JavaScript

2.3.4 Python

2.3.5 SQL

Und es gibt auch ein Beispiel für eine Tabelle.

Man beachte: Bilder haben Bild**unter**schriften, Tabellen haben Tabellen**über**schriften.

Für jedes Kapitel sollte ein neues TEXFile erstellt und eingebunden werden.

Ein Symbol wie π Kann mathematisch korrekt dargestellt werden. Auch Glossareintrag zu Abkürzungen wie Active Directory (AD) können in LATEXbehandelt werden. Zum Demonstrieren wird hier noch eine Webseite von Microsoft zitiert [Maj09], und noch eine Stelle [Maj09]

3 Anforderungsanalyse und Priorisierung

3.1 Anforderungsanalyse

Unter anderem soll die Arbeit Antworten auf folgende Fragen finden:
Wie kann die Webseite www.fupa.net am effizientesten ausgelesen werden?
Welche zusätzlichen Webseiten liefern die meisten Informationen zu potentiellen Opfern?
Wie und wo lässt sich ein Opferprofil erstellen bzw. speichern? (z.B. mySQL-Datenbank)
Wie soll nach Informationen gesucht werden?
Gibt es bereits einen Algorithmus der mit Hilfe von Vorname, Nachname und Geburtsjahr eine E-Mail-Adresse generiert?
Wie können die Phishing-E-Mails möglichst auf einzelne Personen zutreffend erstellt werden?
Ist es sinnvoll E-Mail-Muster zu erstellen?

3.1.1

3.2 Priorisierung

4 Lösungsvorschläge

4.1 Test

4.1.1

5 Auswahl der Lösung anhand Anforderungen

5.1 Test

5.1.1

6 Hauptteil

6.1 Hauptteil

6.1.1

7 Hauptteil

7.1 Hauptteil

7.1.1

8 Hauptteil

8.1 Hauptteil

8.1.1

9 Hauptteil

9.1 Hauptteil

9.1.1

10 Hauptteil

10.1 Hauptteil

10.1.1

11 Hauptteil

11.1 Hauptteil

11.1.1

12 Schlussbemerkungen und Ausblick

A Ein Kapitel des Anhangs

Glossar

Active Directory

Active Directory ist in einem Windows Server 2000, Windows Server 2003, oder Windows Server 2008-Netzwerk der Verzeichnisdienst, der die zentrale Organisation und Verwaltung aller Netzwerkressourcen erlaubt. Es ermöglicht den Benutzern über eine einzige zentrale Anmeldung den Zugriff auf alle Ressourcen und den Administratoren die zentral organisierte Verwaltung, transparent von der Netzwerktopologie und den eingesetzten Netzwerkprotokollen. Das dafür benötigte Betriebssystem ist entweder Windows Server 2000, Windows Server 2003, oder Windows Server 2008, welches auf dem zentralen Domänencontroller installiert wird. Dieser hält alle Daten des Active Directory vor, wie z.B. Benutzernamen und Kennwörter. 3

Glossareintrag

Erweiterte Informationen zum einem Wort oder einer Abkürzung, ähnlich einem Eintrag im Duden. 3

AbkÃ¼rzungsverzeichnis

AD Active Directory 3

Symbolverzeichnis

π	Die Kreiszahl. 3

Literatur

[Bun18] Bundeskriminalamt: *Polizeilich erfasste Fälle von Cyberkriminalität im engeren Sinne* in Deutschland von 2004 bis 2017*. https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalität-im-engeren-sinne-in-deu 2018. Abrufdatum: 29.10.2018.

[CH15] Christopher Hadnagy, Michele Fincher: *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails*. 2015.

[FM14] Francois Mouton, Mercia M. Malan, Louise Leenen H.S. Venter: *Social Engineering Attack Framework*. 2014.

[Had11] Hadnagy, Christopher: *Social Engineering: The Art of Human Hacking*. 2011.

[Jam05] James, Lance: *Phshing Exposed: Uncover Secrets from the Dark Side*. 2005.

[Maj09] Major, Scott D. Applegate: *Social Engineering: Hacking the Wetware!* Information Security Journal: A Global Perspective, 18(1):40?46, 2009.

[Mit01] Mitnick, Kevin D.: *The art of deception:controlling the human elemnet of security*. 2001.

[NW18] Nordrhein-Westfalen, Verbraucherzentrale: *Phishing-Radar: Aktuelle Warnungen*. https://www.verbraucherzentrale.nrw/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059, 2018. Abrufdatum: 29.10.2018.

[uDsiNe15] Netz e.V., DATEV und Deutschland sicher im: *Verhaltensregeln zum Thema "Social Engineering"*. 2015.