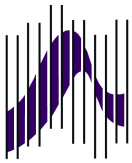
Hochschule
Ravensburg-Weingarten



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 : 20. 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, 20. 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

Persönliche Informationen werden im Internet immer leichter zugänglich gemacht. !!!ZITAT!!! Es gibt viele Webseiten die persönliche Information von Menschen bereitstellt. Eine davon ist auch www.fupa.net. Hier können persönliche Informationen ohne Anmeldung ausgelesen werden. Diese Art von Webseite ist eine perfekte Informationsquelle für Angreifer.
Im Bereich von Social Engineering Angriffen wird diese Information oft genutzt um ein Opfer zu manipulieren. Das hier beschriebene Problem zeigt dass der Zugang für persönliche Information durch das Internet für viele Menschen einfacher gemacht wird. Es soll gezeigt werden wie einfach es ist, personenbezogene Daten aus dem Internet herauszulesen, analysieren und für einen Phishing-Angriffe zu verwenden. !!!!ZITATE HINZUFÜGEN!!! statista z.B.

1.3 Eigene Leistung

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

Die Arbeit gliedert sich in einem theoretischen und praktischen Teil auf. Der Theorie-Teil beginnt im zweiten Kapitel und beschreibt die Grundbegriffe im Bereich Social Engineering, Webtools, E-Mails und Programmiersprachen. Im nächsten Kapitel befindet sich die Anforderungsanalyse. Hier werden die Anforderungen an die Arbeit festgelegt. Darauf folgen die Lösungsvorschläge im Kapitel vier und die ausgewählte Lösung anhand den Anforderungen im Kapitel 5. Anschließend wird bei der Umsetzung auf den Praktischen Teil eingegangen.Am Ende befindet sich das Fazit, der Ausblick und der Anhang.

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].

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.
Grundsätzlich werden bei einem Social Engineering Angriff menschliche Wünsche, Ängste und verbreitete Verhaltensmuster verwendet um ein Opfer zu manipulieren. [uDsiNe15]

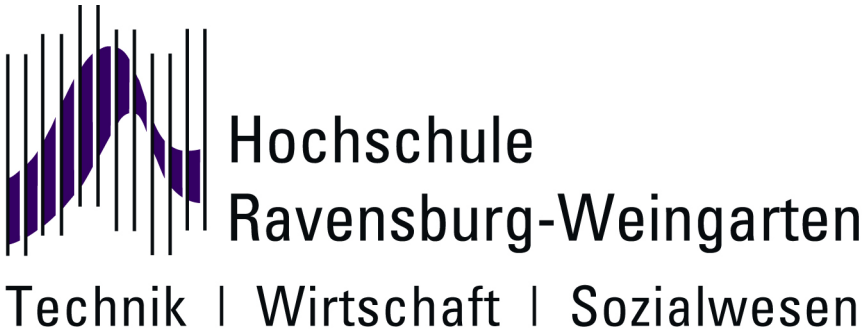


Bild 2.1: Logo der HS – oder nicht?

!!!!!!!!RICHTIGES BILD von ZYKLUS 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.

!!!!!!!!RICHTIGES BILD von FRAMEWORK 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 E-Mail gesendet wird. In einer Spear-Phishing-E-Mail wird ein Opfer beispielsweise mit einem Namen angesprochen oder es sind E-Mails mit Inhalten die das Opfer interessieren könnten. 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 Advanced Persistent Threat (APT) Angriffe auf Firmen beginnen mit einer Spear-Phishing-E-Mail. Die Schadsoftware wir meisten als Remote Access Trojans (RATs) in einem Zip-Datei überliefert. [Cal13]

2.2 Webtools

2.2.1 Web Scraping

Definition

In der Theorie bedeutet web scraping die Informationsbeschaffung im Internet mit unterschiedlichsten Mitteln. [Mit15]

Funktionsweise

Meist wird dies mit einem automatisierten Programm realisiert, das Daten von einem Webserver anfragt, bekommt, analysiert und auswertet. In der Praxis gibt es ein großes Feld von Programmiertechniken und Einsatzmöglichkeiten. Mit Hilfe von web scraping ist es möglich große Datenmengen zu erfassen und verarbeiten. [Mit15]

2.2.2 Web Crawling

Definition

Beim Web Crawling werden Webinhalte geladen und nach Hyperlinks durchsucht. Diesen wird wieder gefolgt und der Prozess beginnt von vorne. Das ist die Grundfunktion einer Suchmaschine. ???? Crawler. [Mit15]

Funktionsweise

Die Funktionsweise besteht darin, dass in den meisten Fällen ein automatisiertes Programm, Web Crawler, erstellt wird. Der Web Crawler lädt Webinhalte runter und durchsucht diese nach Hyperlinks bzw. URLs. Den gefundenen Hyperlinks werden wieder gefolgt, um neue Webseiten mit weiteren URLs zu laden. So hangelt sich ein Web Crawler von Link zu Link durch das Internet. [Mit15]

2.3 E-Mail

2.3.1 Aufbau einer E-Mail

Jede E-Mail besteht aus einem Header-Bereich und einem Body-Bereich. Im Header-Bereich befinden sich Informationen zum Absender. Im Body-Bereich befindet sich der eigentliche Text der E-Mail.

2.3.2 SMTP-Protokoll

E-Mails werden über das Protokoll SMTP (Simple Mail Transfer Protocol) versendet.

2.3.3 IMAP/POP3

IMAP und POP3 sind Protokolle, welche für die Kommunikation zwischen Webserver und Client zuständig ist. Hier wird das herunterladen von E-Mails bereitgestellt.

3 Anforderungsanalyse und Priorisierung

3.1 Anforderungsanalyse

Wie muss Lösung aussehen? must - should - could

Anforderungen:

Informationsbeschaffung:

- Mit Hilfe eines Web-Crawlers soll das Internet nach personenbezogenen Daten suchen
- Es soll durch web scraping personenbezogen Daten gewonnen werden

Datenverwaltung/-speicherung:

- Die Spieler- bzw. Opferinformationen sollen in einer gut übersichtlichen Struktur gespeichert werden. Informationen müssen erweiterbar sein.

E-Mail erzeugung:

- Es sollen E-Mail-Muster erstellt werden. Diese Muster sollen kategorisiert werden, damit für alle Opferinformationen ein passendes Muster vorhanden ist.
- Die Phishing-E-Mails sollen automatisiert erstellt werden und die personalisierte Opferinformation verwenden.

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 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

Priorisierungstabelle.

Tabelle 3.1: Priorisierung der Anforderungen

Anforderung	Priorisierung (A-C)	must-should-could
Anforderung 1	*A*	*must*
Anforderung 2	*B*	*should*

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

4 Lösungsvorschläge

4.1 Informationsbeschaffung

- Es soll durch Web Scraping die Internetseite www.fupa.net durchsucht werden. Persönliche Spielerinformationen werden ausgelesen und gespeichert.
  - Vorname, Nachname, Spitzname, Geburtsjahr, Verein (must)
  - Bild (could)
- Es soll ein Web Crawler erstellt werden der mit der vorhandenen Information nach weiteren Informationen im Internet sucht.

5 Auswahl der Lösung anhand Anforderungen

5.1 Test

5.1.1

6 Umsetzung

6.1 Informationsbeschaffung von der Website www.fupa.net

6.1.1 Erstellung eines Web Crawlers

Anforderung

Der Web Crawler soll die komplette Webseite www.fupa.net durchgehen und Links mit Spielerinformationen speichern. Die Funktionsweise des Web Crawlers besteht darin, dass das Programm auf der Startseite von Fupa.net beginnt nach links zu suchen und diesen folgt.

Probleme

1. Python hat einen verkürzten und erkennbaren Standard http-Header. Dieser wird von vielen Administratoren geblockt und mit der Fehlermeldung 451 erkennbar gemacht. 451 for legal reason
2. Honeypots gewollt oder ungewollt, hier Kalender darstellung mit links zu neuen Jahren die eine sehr hohe bis überhaupt keine Begrenzung haben.
3. Rekursion erreicht schnell die Maximale tiefe von 1500.
4. Zu langsamer Algorithmus

Lösungen

1. http-Header selber konfigurieren
2. Links mit möglichen Honeypots nicht beachten
3. Stack Klasse schreiben damit keine Rekursion benötigt wird
4. Algorithmus anpassen auf fupa-Webseite

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.

[Cal13] Caldwell, Tracey: *Spear-phishing: how to spot and mitigate the menace*. Computer Fraud & Security, 2013(1):11–16, 2013.

[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.

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

[Mit15] Mitchell, Ryan: *Web Scraping with Python: Collecting Data from the Modern Web*. 2015.

[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.