Scuola universitaria professionale della Svizzera italiana
Dipartimento tecnologie innovative

SUPSI

Social Engineering Techniques and The Human Factor

Studente
Bovino Cristian

Relatore
Consoli Angelo

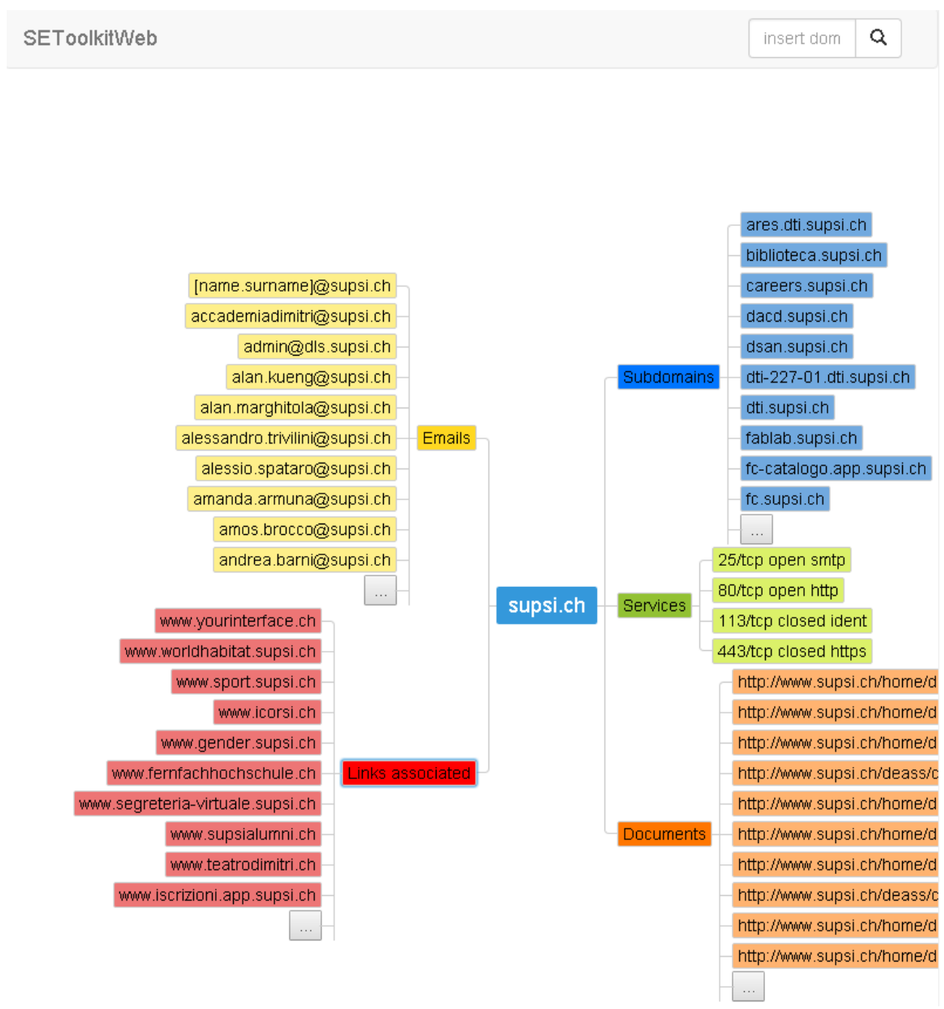
Correlatore
Schiavoni Fabio

Corso Bachelor
Ingegneria informatica

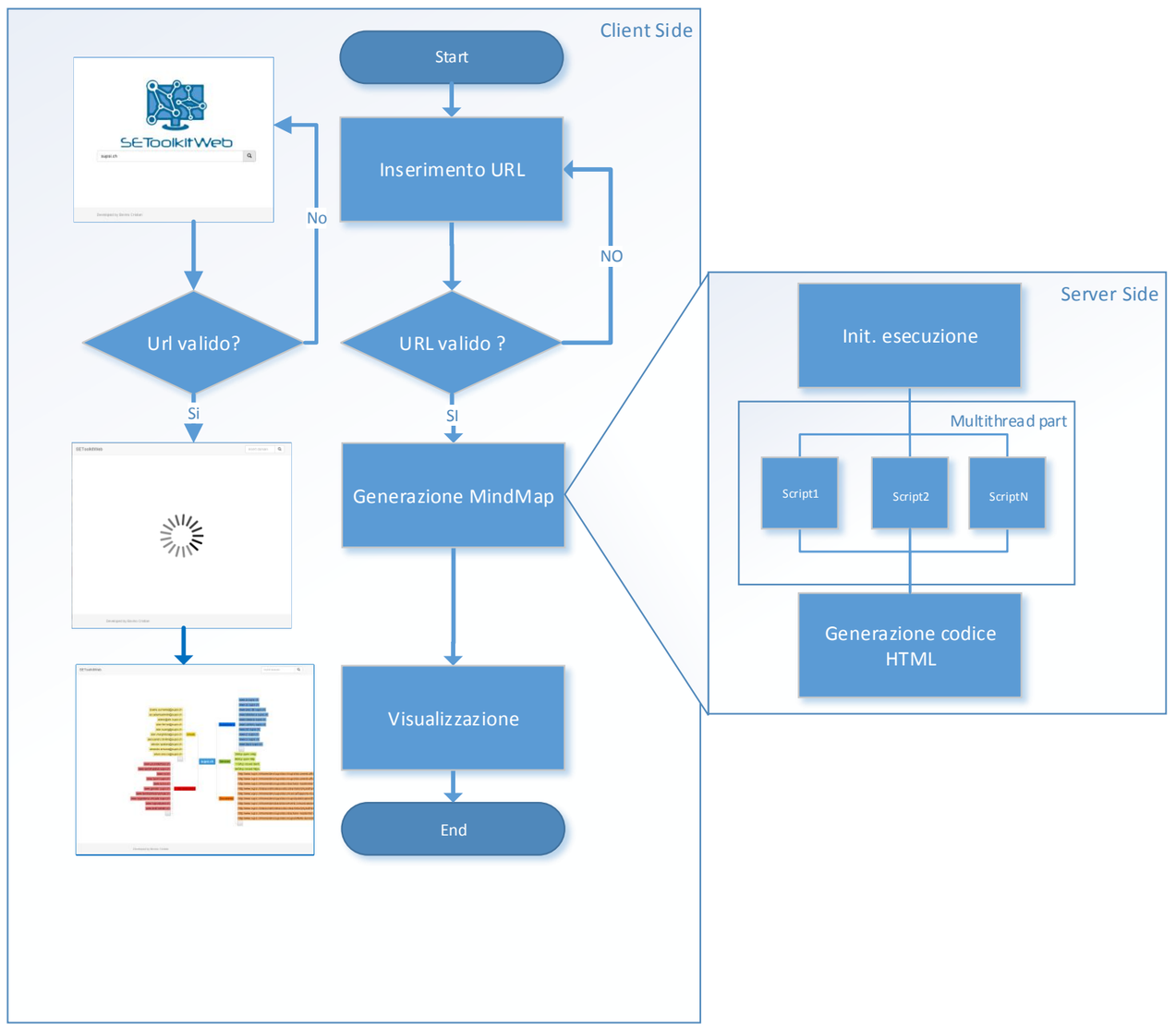
Modulo
Progetto di diploma

Anno
2015/2016

Data
09.12.2015



Mindmap view



Schema di funzionamento del servizio

STUDENTSUPSI

Abstract
Il numero di attacchi informatici è in costante aumento, come anche le numerose tecnologie che fungono da contromisure per contrastarli. Avendo questo aumento di sicurezza si sono sviluppate tipologie di attacco che non agiscono più sulla violazione diretta dei sistemi, ma si occupano di fare leva su un altro fattore, ovvero quello umano. Si tenta infatti di ingannare la persona per fargli compiere delle azioni tali da compromettere la sicurezza del sistema.

L'ingegneria sociale (SE) è una delle principali minacce per le informazioni, di ogni tipo, che sono proprie di un'azienda, un'istituzione o di privati cittadini. Le reti sociali amplificano l'esposizione a questi rischi in modo esponenziale.
La praticità di diversi strumenti (es. gli smartphones e le applicazioni di sharing che li caratterizzano) contribuiscono a nascondere i rischi all'utenza, che tende a sottovalutare la propria esposizione.

Descrizione progetto
Il progetto assegnato ha vari obiettivi da raggiungere, primo tra i quali un'analisi di quali sono le tecniche utilizzate dagli hacker per effettuare questo genere di attacchi e con quali mezzi vengono effettuati. Un altro importante obiettivo da raggiungere è quello di cercare una serie di attacchi avvenuti realmente e catalogarli per tipologia.

Parte del progetto riguarda anche la realizzazione di una parte pratica. Per svolgere questo punto, il lavoro è iniziato cercando dei software, script o siti che fanno parte della categoria OSINT(Open Source INTelligence) ovvero software che estraggono tipologie di informazioni pubblicate online. Successivamente viene richiesto di realizzare una web application che metta insieme le risorse trovate precedentemente e che sia in grado di mostrare, tramite una *mindmap,* delle informazioni chiave che appartengono al sito web. Questo consentirà di valutare quanto il sito in questione sia esposto ad attacchi di Social Engineering e la quantità di informazioni pubbliche che è possibile reperire senza alcuna violazione di privacy.

Obiettivi
Raccogliere casi di attacchi recenti che hanno fatto uso di SE e classificarli. Studiare i programmi sul mercato che permettono di operare attività di tipo OSINT, prestando particolare attenzione a quelli open source e classificandoli in base al linguaggio di programmazione sul quale si basano. Testare tutte le possibili fonti per la raccolta di dati di diversa natura. Sviluppare un toolkit che combini diverse librerie disponibili per accedere a informazioni. Raccogliere dati e analizzarli. Studiare un modo per attaccare una vittima scelta tra quelle di cui si sono raccolte informazioni. Classificare le tipologie di attacco in base al loro costo, cioè in base a quanto sforzo è necessario per raggiungere la vittima e farla cadere in un attacco di SE.

Conclusione
Sono molto soddisfatto dei risultati ottenuti da questo lavoro di bachelor in quanto mi ha permesso di andare ad analizzare il tema del Social Engineering da più punti di vista. Questo é un problema per la sicurezza nel mondo del web. Il progetto serve a rendersi conto della quantità di informazioni che vengono esposte in internet e di conseguenza la pericolosità che può generare esporle.