mobile business

A Structured Comparison of Social Engineering Intelligence Gathering Tools

Kristian Beckers, Daniel Schosser, Sebastian Pape and Peter Schaab

TECHNISCHE UNIVERSITÄT MÜNCHEN

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Aug 30th / 31th, 2017 TrustBus 2017 Lyon, France

mobile business

Agenda

1	Social Engineering
2	Method & Criteria
3	Tools
4	Summary and Conclusion

Introduction: Social Engineering

Source: cybertec-security.com

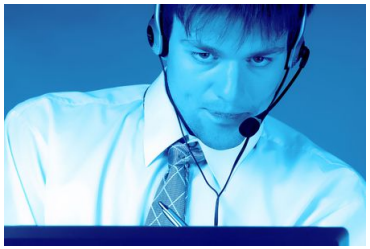
Breach vectors leading to compromise:

Source: PWC Information Security Breaches Survey 2017

Social Engineering Process

- Pre Engagement Interactions
- Intelligence Gathering
- Pretexting
- Exploitation
- Post-Exploitation




[26] Milosevic. Introduction to Social Engineering, 2013.

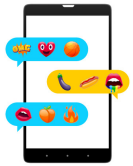
Communication Channels

User Credentials

Locations

Job Positions

Company Lingo



Personal Information

Information Needs

Phishing

- Communication channels
- Company knowledge

Baiting

- Locations (walking routes)
- Company knowledge

Impersonation

- Information about a single person
- Company knowledge

Agenda

1. Social Engineering
2. Method & Criteria
3. Tools
4. Summary and Conclusion

Method

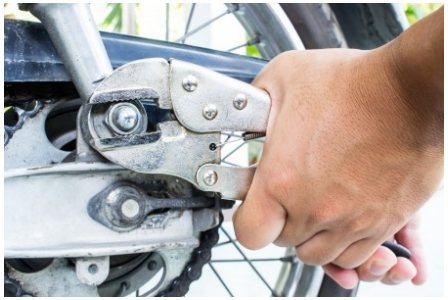
- Input
  - Google Search ”social engineering and tool or application or script or webpage”
  - List by Hadnagy [17]
  - Consents of 3 researchers
- Analysis
  - General Overview of Tool
- Mapping to Attack Types
  - Output of tools’ information types
  - Mapped information types to Attack types (Phishing, Baiting, Impersonation)
  - Mapped Tools to Attack Types

[17] C. Hadnagy. Social engineering: The art of human hacking. John Wiley & Sons, Indianapolis, 2010.

Tool Applicability

Purpose

Price

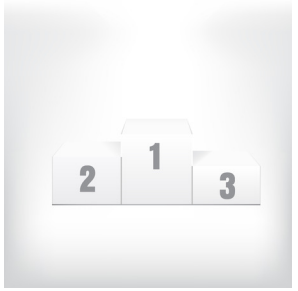


Usability

Counter Measures

Input Parameters

Output Visualisation



Sorting & Ranking

Mapping of SE Characteristics to Attack Types

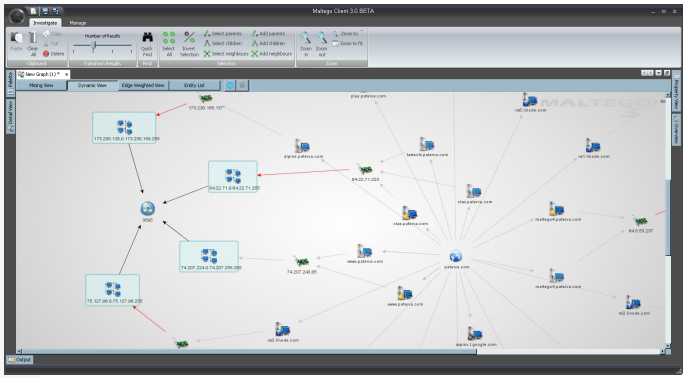
		Attack Type		
		Phishing	Baiting	Impersonation
Communication	Telephone Number	x		
	Friends	x		x
	Personal Information	x		x
	Private Locations	x		x
	EMail	x		
	Instant Messenger	x		
	Co-Workers: Communication			x
Company Knowledge	Co-Workers: New Employee			x
	Co-Workers: Hierarchies			x
	Lingo	x		x
	Facilities: Security-Measures		x	x
	Facilities: Company Location		x	x
	Websites	x		
	Policies: Software		x	
	Policies: Network		x	
	Policies: Organization		x	

Agenda

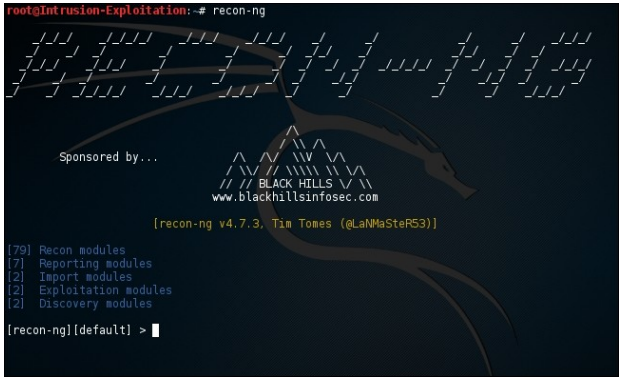
1. Social Engineering
2. Method & Criteria
3. Tools
4. Summary and Conclusion

mobile business

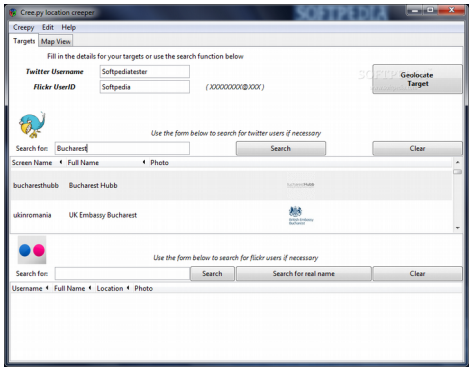
Social Engineering Tools



Maltego

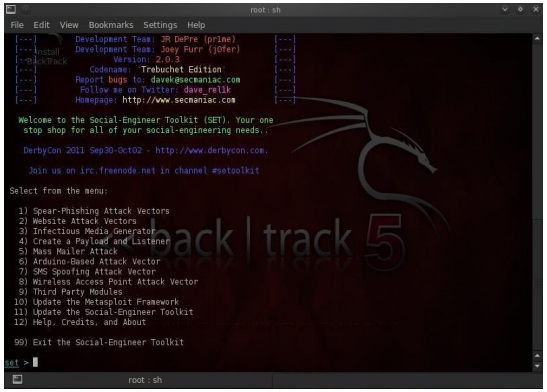


Recon-ng

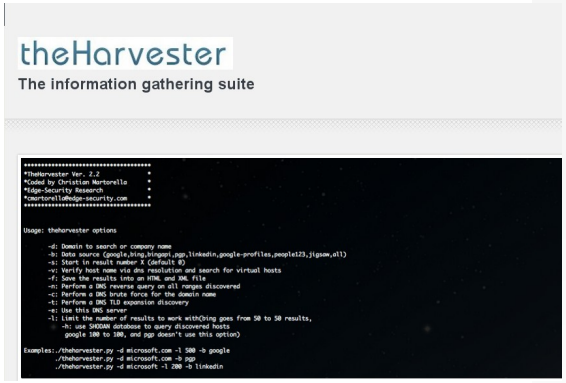


Cree.py

Spokeo

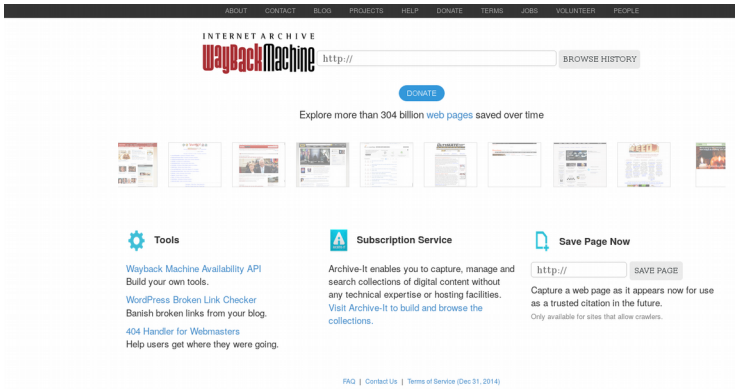


SET



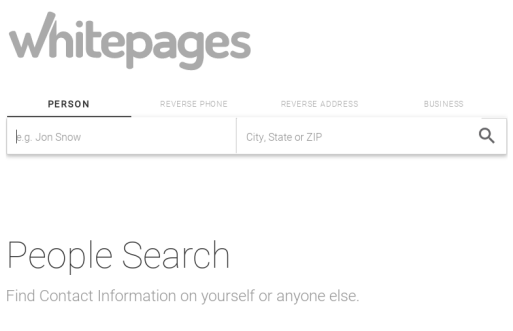
theHarvester

Social Engineering Webpages + X



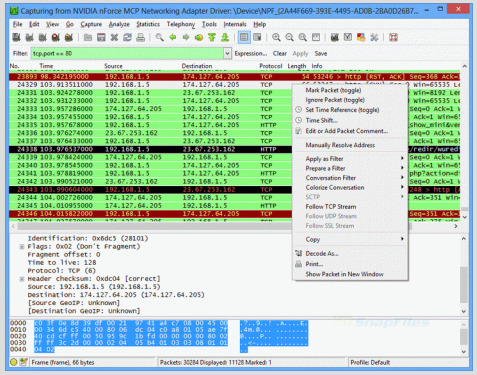
Wayback Machine

Background Checks



Whitepages

- Tax Records (e.g. US, Sweden)
- Company Related Information



Wireshark

Social Engineering Attack Potential

	SET	Maltego	Recon-ng	Cree.py	Spokeo	Wayback Machine	theHarvester	knowem.com	Whitepages	Instant Checkmate	freebackgroundcheck.org
Search by Person/ Company	o	++	++	++	++	++	++	+	++	++	++
Retrieve E-Mail Address	o	++	++	o	o	o	++	o	o	o	o
Retrieve Username/ Password	o	o	++	o	o	o	o	o	o	o	o
Retrieve Job-Title	o	o	++	o	o	o	o	o	o	++	++
Retrieve Locations	o	+	+	++	+	o	o	o	++	++	++
Retrieve Personal Data	o	o	o	o	++	o	o	+	+	++	++
Usability	+	+	+	++	++	++	+	++	++	++	++
Visualize Output	+	++	+	++	++	++	+	++	++	++	++
Retrieve Company Lingo	o	o	o	o	o	o	o	o	o	o	o
Free to use	++	++	++	++	o	++	++	++	++	o	o

Tool Coverage of Communication Channels

	Cree.py	Gitrob	KnowEm	LinkedIn	Maltego	Namechk	Recon-ng	Spokeo	theHarvester	Wayback Machine	Wireshark	Xing
Telephone Number							x					x
EMail				x	x		x		x			x
Instant Messenger			x		x	x		x				x
Friends			x	x	x	x						x
Personal Information	x		x	x		x		x				x
Private Locations	x							x				x

Tool Coverage of Company Data

	Cree.py	Gitrob	KnowEm	LinkedIn	Maltego	Namechk	Recon-ng	Spokeo	theHarvester	Wayback Machine	Wireshark	Xing
Company Locations	x			x			x	x	x			x
Company Lingo												
Special Knowledge				x	x		x					x
New Employees				x	x							x
Hierarchies				x	x							x
Websites					x		x		x	x		
Facility Security Measures		x									x	
Security Policies		x							x		x	
Software Policies		x					x				x	

Tools Mapped to Attacks

	Cree.py	Gitrob	KnowEm	LinkedIn	Maltego	Namechk	Recon-ng	Spokeo	theHarvester	Wayback Machine	Wireshark	Xing
Telephone Number							P					P
Friends			P,I	P,I	P,I	P,I						P,I
Personal Information	P,I		P,I	P,I		P,I		P,I				P,I
Private Locations	P,I							P,I				P,I
E-Mail				P	P		P		P			P
InstantMessenger			P		P	P		P				P
Co-Workers: NewEmployee				I	I							I
Co-Workers: Hierarchies				I			I					I
Lingo												
Facilities: Security-Measures		B,I									B,I	
Facilities: Company Location	B,I			B,I			B,I	B,I	B,I			B,I
Websites					P		P		P	P		

Agenda

1. Social Engineering
2. Method & Criteria
3. Tools
4. Summary and Conclusion

Summary and Conclusion

- Variety of tools exist
  - Allow non-experts to gather information
  - Company Lingo not covered
- None of the tools refers to countermeasures
  - Risk Assessment of available information
  - Propose policies depending on outcome
- Outlook
  - More tools
  - More data

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Dr. Sebastian Pape
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4
60629 Frankfurt, Germany

Phone +49 (0)69 798 34668
Fax +49 (0)69 798 35004

E-Mail: sebastian.pape@m-chair.de
WWW: www.m-chair.de