

Social-Engineer, Inc.



Advanced Practical Social Engineering

SYLLABUS

IMPORTANT

**** EACH NIGHT YOU WILL BE ASSIGNED TO DO LIVE HOMEWORK ENGAGEMENTS****

You will be placed in a team and sent out on engagements

More details given in class

Table of Contents

Social Engineering for Penetration Testers Introduction 6

Before We Begin..... 7

- i. Legal Stuff7
- ii. How To Approach This Course.....7
- iii. Reporting7
- iv. Social Engineering Pentest Methodology8

Section I: Know Yourself to Know Others 10

Module 1: Introduction to Social Engineering 10

- 1.1: Social Engineering Defined..... 11
- 1.2: Why Does Social Engineering Work..... 11
- 1.3: Identify Your Communication Style 12
 - 1.3 Exercise 1:..... 12
- 1.4: Story Telling Time..... 13
- 1.5: DISC Assessment..... 13
 - 1.5 Exercise 1:..... 16
 - 1.5.2 Exercise 2:..... 16
- 1.6: Strengths To the Extreme..... 17
- 1.7: DISC Engagement Action Plan..... 18
 - 1.7 Exercise: DISC Writing Exercise 27
- 1.8: Construct Your Own DISC Engagement Plan..... 27
- Module 1 Conclusion:..... 30

Module 2: Advanced Approach Techniques 30

- 2.1: The 10 Steps To Developing Rapport 31
 - 2.1.1: Establish Artificial Time Constraints..... 31
 - 2.1.2: Accommodating Nonverbals..... 32
 - 2.1.3: Slower Rate of Speech 32
 - 2.1.4: Sympathy or Assistance Theme 33
 - 2.1.5: Ego Suspension..... 33
 - 2.1.6: Validate Others 34
 - 2.1.7: Ask...How? When? Why? 34
 - 2.1.8: Connect with Quid Pro Quo..... 35
 - 2.1.9: Reciprocal Altruism aka Gift Giving..... 35
 - 2.1.10: Manage Expectations 36
- 2.1: Props..... 36
- Module 2 Conclusion:..... 37

Module 3: Elicitation..... 38

- 3.1: Mastering Elicitation 38
 - 3.1.1: Be Natural..... 39
 - 3.1.2: Be Educated..... 39
 - 3.1.3: Don't Be Greedy..... 39
- 3.2: The Principles Behind Elicitation 40
 - 3.2.1: Preloading..... 40

IMPORTANT

**** EACH NIGHT YOU WILL BE ASSIGNED TO DO LIVE HOMEWORK ENGAGEMENTS****

You will be placed in a team and sent out on engagements

More details given in class

3.2.2: <i>Appealing to Ones Ego</i>	41
3.2.3: <i>Mutual Interest</i>	43
3.2.4: <i>Deliberate False Statements</i>	43
3.2.5: <i>Assumed Knowledge</i>	45
3.2.6: <i>Alcohol</i>	45
3.3: <i>The Effective Use of Questions</i>	46
3.3.1: <i>Open-Ended Questions</i>	46
3.3.2: <i>Close-Ended Questions</i>	47
3.3.3: <i>Leading Questions</i>	48
3.3.4: <i>Assumptive Questions</i>	48
Home Work Session 1	49
Section II: Preparation & Information	50
Module 4: <i>Information Gathering</i>	51
4.1: <i>No Tech Information Gathering</i>	52
4.1.2: <i>Dumpster Diving</i>	52
4.1.3: <i>Shoulder Surfing</i>	53
4.1.4: <i>Physical Security</i>	55
4.1.5: <i>Badge Surveillance</i>	57
4.1.6: <i>Vehicle Surveillance</i>	59
4.1.7: <i>Cameras and Listening Devices</i>	61
4.2: <i>Technology Based Information Gathering</i>	64
4.2.2: <i>Corporate Web Sites</i>	64
4.2.3: <i>Search Engines</i>	65
<i>Google Dorking</i>	67
4.2.3: <i>Exercise</i>	75
4.2.4: <i>Public Reporting Systems</i>	75
4.2.6: <i>Misc. Information Sources</i>	81
4.2.7: <i>Maltego</i>	81
4.2.8: <i>ECHOSEC</i>	86
Module 4: <i>Exercise</i>	87
Section III: Advanced Preparation Tactics	88
Module 5: Pretexting	88
5.1: <i>Principles of Successful Pretexting</i>	89
5.1.1: <i>Research Equals Success</i>	89
5.1.2: <i>Involve Personal Interests</i>	89
5.1.3: <i>Practice Dialects or Expressions</i>	90
5.1.4: <i>Phone Skills Should Not Be Lacking</i>	91
5.1.5: <i>Keep It Simple</i>	92
5.1.6: <i>Spontaneity is the Spice</i>	92
5.1.7: <i>Provide a Follow Through</i>	94
Module 5: <i>Exercise</i>	95
Homework Session 2:	96
Module 6: <i>Influence and Manipulation</i>	97

IMPORTANT

**** EACH NIGHT YOU WILL BE ASSIGNED TO DO LIVE HOMEWORK ENGAGEMENTS****

You will be placed in a team and sent out on engagements

More details given in class

6.1: The Eight Aspects of Highly Effective Influence.....	97
6.1.1 Reciprocation	97
6.1.2 Obligation.....	99
6.1.3 Concession.....	100
6.1.4 Scarcity.....	101
6.1.5 Authority.....	101
6.1.6 Commitment and Consistency.....	102
6.1.7 Liking.....	103
6.1.8 Social Proof.....	104
6.2: Using Influence in your scenario.....	105
6.3: Manipulation	105
6.3.1: Increasing Susceptibility.....	106
6.3.2: Environmental Control.....	106
6.3.3: Forced Reevaluation.....	107
6.3.4: Make them feel powerless.....	107
6.3.5: Punishment.....	107
6.3.6: Intimidation.....	108
Section IV: Psychology and the Social Engineer	109
Module 7: Framing.....	109
7.1: Framing.....	109
7.1.1 Frame Bridging.....	110
7.1.2 Frame Amplification.....	110
7.1.3 Frame Extension.....	110
7.1.4 Frame Transformation.....	111
Framing Rule #1: Everything You Say Evokes a Frame.....	111
Framing Rule #2: Words that are defined within a frame evoke the frame.....	112
Framing Rule #3: Negating the Frame.....	113
Framing Rule #4: Causing the target to think about the frame reinforces the frame.....	114
Framing Conclusion.....	114
Homework Session 3:	114
Module 8: Nonverbal Communication	115
Lie Detection Exercise Analysis.....	115
Baselines.....	115
8.2: Digging Deep into Nonverbal Communications.....	116
8.2.0: Emotions vs. Feelings.....	116
8.2.1: The Seven Emotions.....	117
What Governs Nonverbal Communication.....	118
8.2.2.: Facial Expressions.....	118
8.2.3: Body Language.....	126
8.2.4: Verbal Style & Content.....	130
8.2.5: Body Language Queues.....	131
8.2 Exercises.....	137
Homework Session 4:	138
8.3: Nonverbal Human Hacking (aka Amygdala Hijacking).....	139

IMPORTANT

**** EACH NIGHT YOU WILL BE ASSIGNED TO DO LIVE HOMEWORK ENGAGEMENTS****

You will be placed in a team and sent out on engagements

More details given in class

8.3.1: Amygdala Hijacking The Basics	139
8.3.2: Using as a Social Engineer.....	139
Module 9: Attack Vectors.....	141
9.1: Developing Your Attack Vector	141
9.2: Executing Your Attack Vector	144
9.2.1: In Person Attacks.....	144
9.2.2: Phone Social Engineering Attacks	145
9.2.3: Phishing / Email Attacks.....	146
END OF THE LIVE COURSE	148
Section V: On the Pentest	148
Module 10: Reporting and Legalities	148
10.1: What to Report	149
10.2: What Not to Report.....	150
10.3: Get Out of Jail Free Card.....	150
How to use this course.....	151
Social Engineering Pentest Certification	151
Final Remarks	152

All rights reserved to Social-Engineer, Inc., 2017

©

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distance learning, in any form or by any means such as any information storage, transmission, or retrieval system, without prior written permission from the author.

Social Engineering for Penetration Testers Introduction

Dear Student,

Social Engineering has become a very hot topic in the recent years. With the multitude of attacks that have occurred in the market many are now focusing their efforts on trying to prepare for the threats that social engineering poses.

Just a few years ago searching the web for the term “social engineering” offered up a little more than how to get free pizza or “pick up chicks”. While there is some merit in these skills, these are a far cry from what is being used to infiltrate Fortune 500 companies.

That was one of our motivations for developing the world’s first online framework for social engineering found at www.social-engineer.org. This resource along with my books, Social Engineering: The Art of Human Hacking & Unmasking the Social are the basis for this course.

Our motto is “Security Through Education” and we feel that it is impossible to be truly secure without truly understanding all the methods, tools and tricks that are used by the “bad guys”. To do that we have prepared an in-depth, fast paced, comprehensive course that will prepare you to begin mastering the skills needed to become a true social engineer and to get into their minds.

Our goal is that at the end of this course you will have a new arsenal of tools and skills to use that will help you defend yourself, your families and your companies against these malicious attacks.

Course Overview

To truly understand others, to truly be able to influence others and to truly be able to be a good social engineer you first need to understand yourself. Through a series of self-analysis tools you will begin to see what type of a personality you have, how you can master your own style and what power lies behind this knowledge.

The next part of the course will be a rollercoaster ride through the skills that make up the professional social engineer. This course is not meant to be a short-term course just for a week and then done, but part of a lifetime of learning. It has been designed to help you focus on the skills, start you on a path and give your foundation needed to truly become a Social Engineering Professional.

Sincerely,

