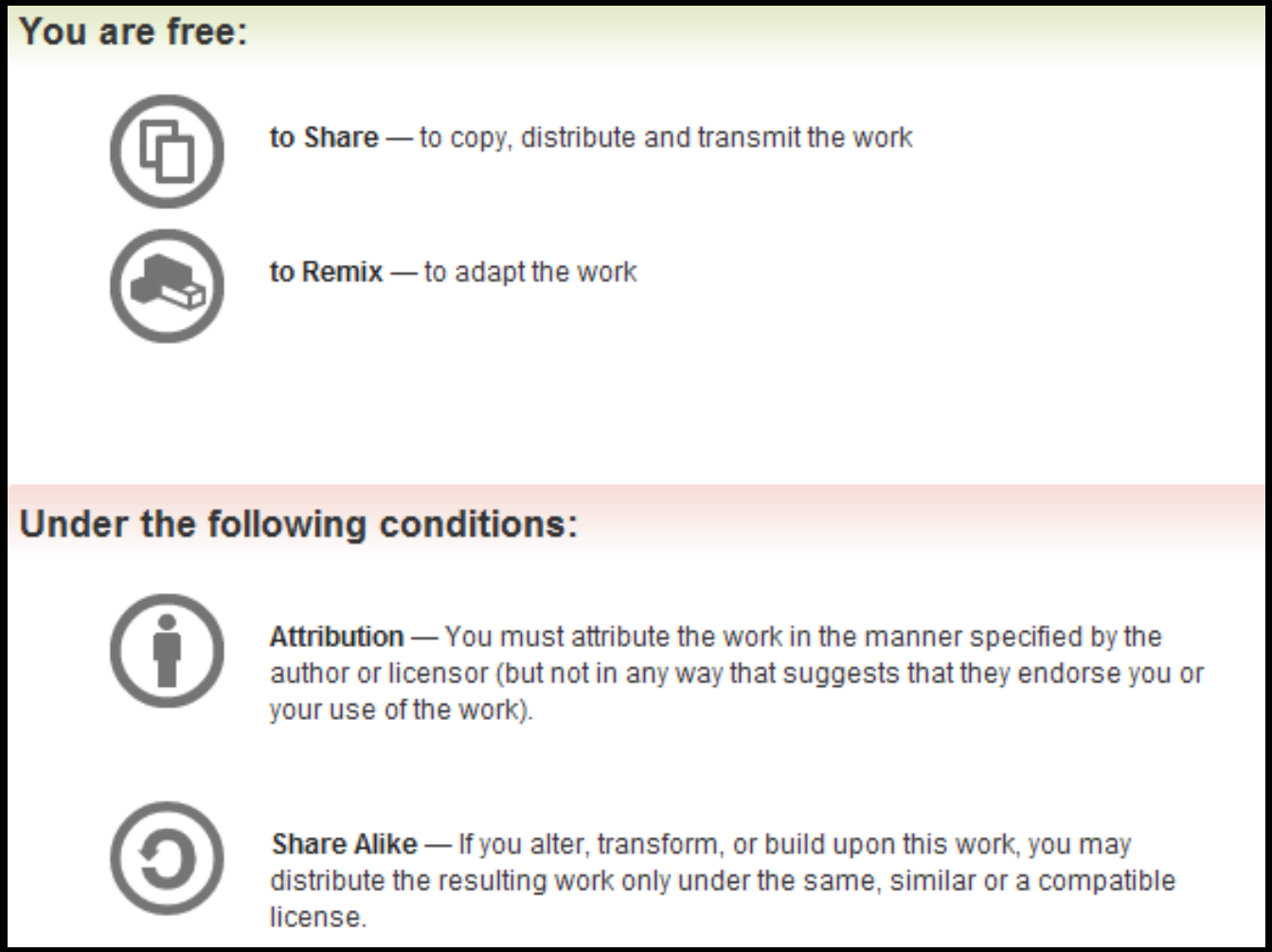
Hacking Techniques & Intrusion Detection

Ali Al-Shemery
arabnix [at] gmail

All materials is licensed under a Creative Commons "Share Alike" license.

- http://creativecommons.org/licenses/by-sa/3.0/



whoami

- Ali Al-Shemery
- Ph.D., MS.c., and BS.c., Jordan
- More than 14 years of Technical Background (mainly Linux/Unix and Infosec)
- Technical Instructor for more than 10 years (Infosec, and Linux Courses)
- Hold more than 15 well known Technical Certificates
- Infosec & Linux are my main Interests

Welcome

Please introduce yourself:

- Name:
- Work:
- Why Infosec degree?
- Any Technical Background?

Social Engineering

Kickstarting Notes

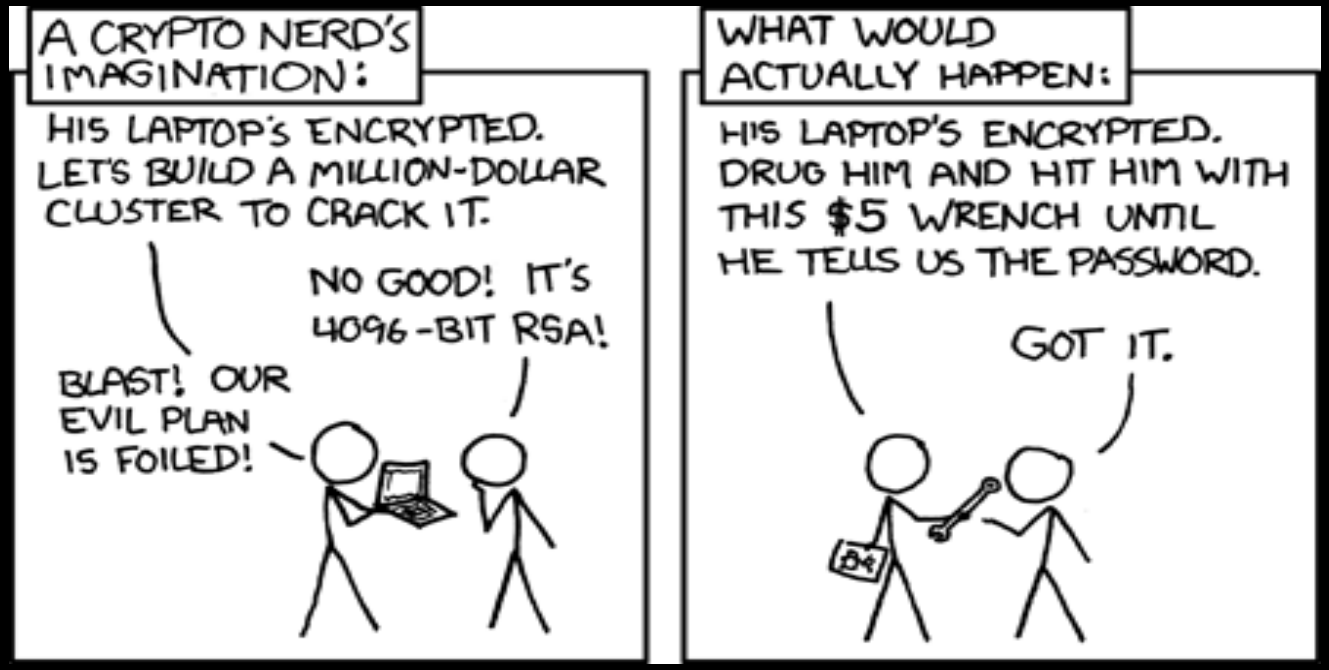
- The course will cover different topics from an offensive point of view,
- Mitigation and remediation steps will be provided for each subject of the course,
- Backtrack Linux is used to perform the attacks,
- Don’t depend on the course’s slide notes!

Outline - Social Engineering

- Intro.
- Information Gathering
- Elicitation
- Pretexting: How to Become Anyone!
- Mind Tricks: Psychological Principles Used in Social Engineering
- Tools Used

Why Start the course with Social Engineering

?



"You could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain vulnerable to old-fashioned manipulation."

Kevin Mitnick

Definition SE

"The act of manipulating a person to take an action that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action."

– Christopher Hadnagy

Why Attackers Might Use Social Engineering?

- No technology in the world can prevent social engineering!
- Because there is no patch for *human stupidity*!
- People are the largest vulnerability in any network or security chain!
- Path of Least Resistance
  - Why spend hours, days, weeks to crack a password when you can just ask for it?
- On The Rise
  - Phishing attacks are rising 26% per month!

Categories of Social Engineers

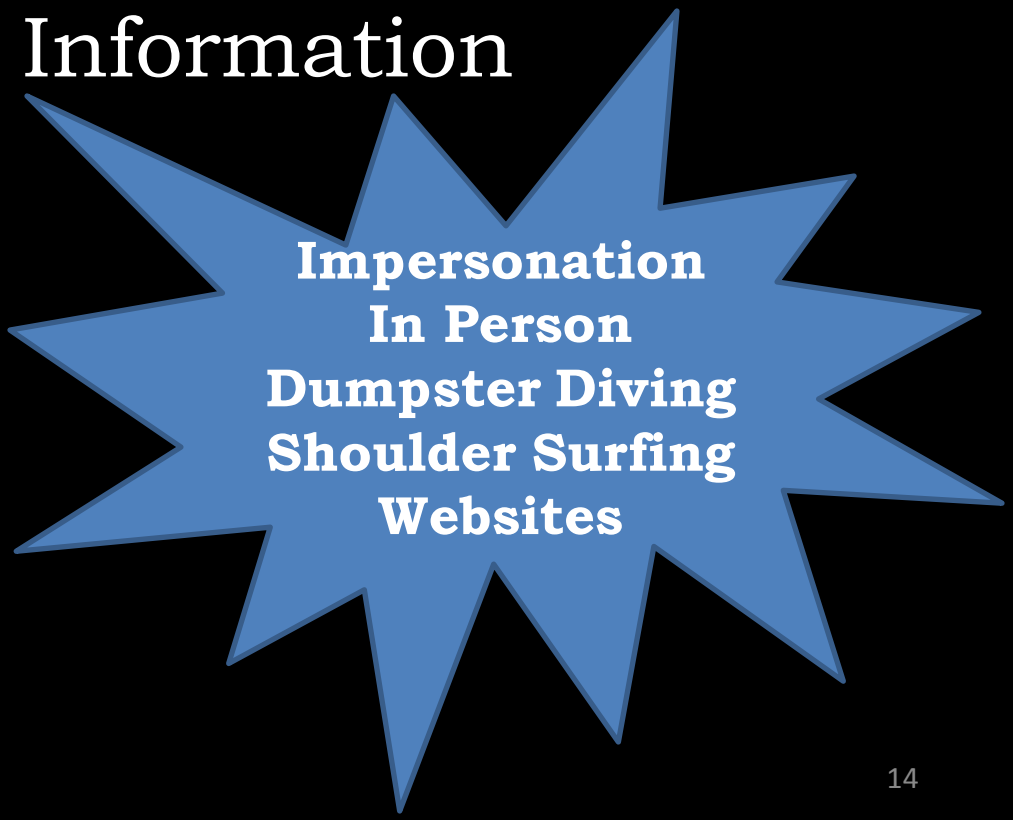
- Hackers
- Penetration Testers
- Spies or Espionage
- Identity Thieves
- Disgruntled Employees
- Information Brokers
- Scam Artists
- Executive Recruiters
- Sales People
- Governments
- Everyday People

Typical Goals of a Social Engineer

- Dr. Max Kilger (Honeynet Project) identified six motivations for non-ethical computer activity:
  - Money, Entertainment, Ego, Cause, Entrance into a social group, and Status within that social group
- Other key motivations:
  - knowledge, revenge and curiosity.
- Social Engineering as a Protection

Classic Social Engineering Attacks

- Username / Password Information
- Credit Information
- Name & Address Information
- Procedures
- PIN Codes



Real World Social Engineering Examples

- Playing the Part
- Opposite Sex
- Confidence Men (Con Men)
- Phishing (*more on this coming*)
- Politicians

Phishing

In the field of computer security:

- “Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication".
- Examples:
  - URL and Email Manipulation
    - A URL like (http://www.company.com) looks almost identical to (http://www.cornpany.com)
  - Spear Phishing
  - Penetration Testers and Social Engineers

Information Gathering

- Human Intelligence (HUMINT)
- Signals Intelligence (SIGINT)
- Open Source Intelligence (OSINT)
- Imagery Intelligence (IMINT)

– Will be discussed next week.

ELICITATION

"Elicitation is the process of extracting information from something or someone."

– NASA

Elicitation Goals

- Elicitation is used to get to know people better.
- Used to make mental judgments of **IF** and **HOW** to develop a relationship with a person.
- In the case of an individual or group of people, this is something we do everyday by talking, listening, and asking questions.

Elicitation Preloading

- Preloading is influencing subjects before the event.
- Think about a movie's pre-release trailers.
- They use desired outcome words such as "The best film you have ever seen!"
- This technique works great when introducing anything.

Becoming a Successful Elicitor

- Understand how to communicate with people.
- Must learn to be adaptive (communication must be made to fit the environment and situation).
- Build a bond or relationship with the potential "target".
- Communications should match your pretext, otherwise you might seem out of place to the people your communicating with. *If your pretext is a member of the IT staff then you need to know, understand, and be able to effectively communicate enough technical information to appear convincing.*
- You must know how to ask intelligent questions that will force a response. *Questions that can be answered with a simple "Yes" or "No" are not good questions at all.*

Types of Questions

- Open Ended
- Close Ended
- Neutral
- Leading
- Assumptive

Key Points

- Important key points in mind:
  - Too many questions can shut down the interaction
  - Too little may make the person uncomfortable
  - Ask only one question at a time, too many will cloud the answer you get
  - Use a narrowing approach to questions to gain the most information

i.e. Neutral Questions -----> Open Ended -----> Closed Ended -----> Highly Directed

PRETEXTING:
How to Become Anyone!

"True social engineering is not just believing you are playing a part, but for that moment you are that person, you are that role, it is what your life is."

– Chris Nickerson

Definition

- Pretexting is a social engineering technique wherein a hacker uses false pretenses to engage with his/her intended victim in order to get information from that target.
- Basically it's a lie with a made-up story to go along with it. Pretexting is often used to gain trust, and when trust is gained by the pretexter, data and privacy are in danger.

"Honesty is the key to a relationship. If you can fake that, you're in."

- —Richard Jeni

Importance of Pretexting

- One of the most important aspects of social engineering is trust. *If you cannot build trust you will most likely fail.*
- A solid pretext is an essential part of building trust.
- If your alias, story, or identity has holes or lacks credibility or even the perception of credibility the target will most likely catch on.

Pretexting Principles and Planning

- A crucial aspect of using pretexting as a social engineering tactic is proper planning.
- If proper planning is not taken, the percentage of your social engineering attempts that will succeed will be few to none.
  - Basic Principles
  - Planning and Using Pretexts
  - Character Creation
    - Trust Relationships

Basic Principles

- The more research that is done the better chance of success
- Careful planning is required for success
- Practicing dialects or expressions that will be familiar to your target is essential
- Just because the pretext is over the phone does not minimize the research effort
- The simpler the pretext the better chance of success
- Your pretext should appear spontaneous
- Your pretext should seem accurate or have aspects that are not susceptible to verification
- You must know the intelligence and type of person you will be contacting

Planning and Using Pretexts

- Pretexting has been hailed as one of the quickest ways to obtain information.
- Utilized by federal and local law enforcement, private detectives, reporters, interrogators and many other types of people.

- While selecting your pretext it is imperative to consider a few key questions:
  - What problem am I trying to solve?
  - What questions am I trying to answer?
  - What information do I seek?
  - The nature of the person whom we will be contacting

Character Creation

- When you're developing a pretext you are essentially creating a character.
- The complexity of that character is determined by the planned depth of interaction with people at the target site.
- A pretext can be as simple as just being friendly to someone during a conversation or as complicated as a full blown fake identity complete with ID's, public records, and all the trappings of a normal person's life (social networking pages, blog postings, and other things searchable via the Internet).
- The process of character development is well documented and practiced by the acting community.

Mind Tricks

Psychological Principles Used in Social Engineering

PSYCHOLOGICAL PRINCIPLES

"Simply confirming your nonverbal behavior to the client, using language from the client's preferred representational system and matching speech volume, tone and area of speech often overcomes client reluctance to communicate."

– *Subtle Skills for Building Rapport, FBI*

Modes of Thinking

- To alter someone's way of thinking you must understand the way people think and in what modes they think.
- A basic question will come in mind "How do I figure out a target's dominant mode of thinking?"
  - The Senses
  - Micro-Expressions
  - Neurolinguistic Programming (NLP)

The Three Main Modes of Thinking

- Although we have five senses, the modes of thinking are associated with only three of them:
  - Sight, or a visual thinker
  - Hearing, or an auditory thinker
  - Feeling, or a kinesthetic thinker

Micro-Expressions

- Anger
- Disgust
- Fear
- Joy
- Sadness
- Surprise

Anger

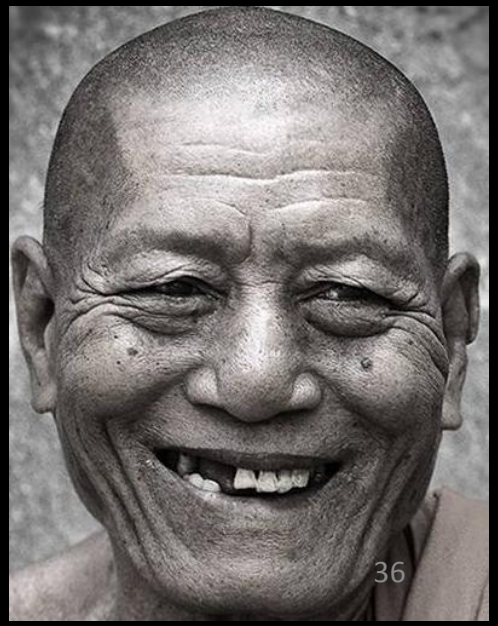
Disgust

Fear

Contempt

Sadness

Happiness



Training Yourself to See Microexpressions

- Replay expression videos to see how each part of the face is involved.
- Perform the ME yourself using a mirror.

Benefits of ME Training

- Combine the skill with:
  - interrogation tactics,
  - body language skills,
  - and elicitation skills to not only figure out what targets are thinking, but also to lead them down the path you want.

You're not a Mind Reader!

- The expression is linked to an emotion, but the *expression doesn't tell you why the emotion is being displayed*.

How to Use ME as a Social Engineer

- Eliciting or causing an emotion
- Detecting deception
  - Contradictions
  - Hesitation
  - Changes in behavior
  - Hand gestures

Neurolinguistic Programming (NLP)

- "a model of interpersonal communication chiefly concerned with the relationship between successful patterns of behavior and the subjective experiences (esp. patterns of thought) underlying them,"
- and "a system of alternative therapy based on this which seeks to educate people in self-awareness and effective communication, and to change their patterns of mental and emotional behavior."

– Oxford English Dictionary

How to Use NLP as a Social Engineer

- Many of the scripts and principles of NLP tend to lean toward hypnosis and similar avenues.
- Even though you will not use hypnosis to social engineer a target, you can use many of the principles of NLP as a social engineer.
- For example, NLP can teach you how to use your voice, language, and choice of words to guide people down the path you want.

SOCIAL ENGINEERING TOOLS

Physical Tools

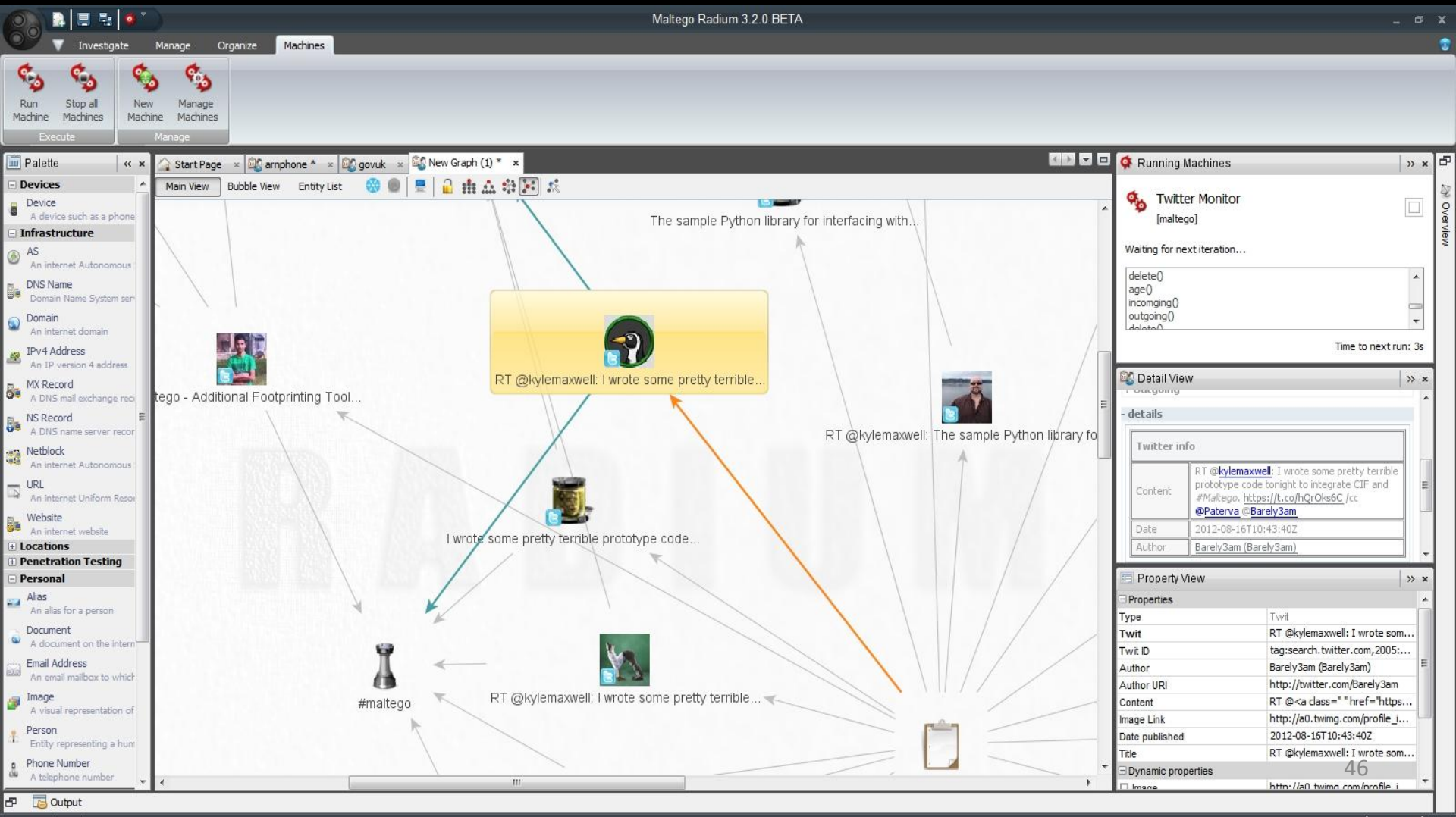
- Lock Picking and Shims
- (Shove Knife,
- Bump Keys,
- Shims)
- Snap Gun.

Physical Tools – Cont.

- Cameras (Small/Compact, Cell Phones, Covert, Qik)
- GPS Tracker (SpyHawk, SuperTrack)
- Pen Recorder
- RF Bug Kits

Computer Based Tools

- Maltego



Computer Based Tools – Cont.

- Social Engineer Toolkit (SET)
- Common User Passwords Profiler (CUPP)
- Who's Your Daddy Password Profiler (WYD)
- Dradis, BaskKet – Information Gathering

Phone Based Tools

- Caller ID Spoofing
  - SpoofCard
  - Asterisk
  - SpoofApp
  - Voicemail

Social Engineering

- Countermeasure
- Mitigation
- Remediation

?

SUMMARY

- How hackers manipulate people to reach information using Social Engineering techniques,
- Who are Social Engineers,
- The Tools used by Social Engineers,
- Countermeasures, Mitigation, and Remediation for Social Engineering.

References

[-] Social Engineering Framework, http://www.social-engineer.org/framework/

[-] Chris Nickerson, a well-known social engineer from the TV series Tiger Team

[-] Dr. Max Kilger, motivations, http://www.social-engineer.org/wiki/archives/TypicalGoals/TypicalGoals-rdodge.pdf

[-] Social Engineering: The Art of Human Hacking, Chris Hadnagy

[-] NASA SE definition, http://social-engineer.org/wiki/archives/Elicitation/Definition_of_Elicitation.htm