Social Engineering on Rails

Presenter: Anthony Valente
A+, CCNA, CEH, BA Network Security.
Phone: 347-586-9386
E-mail: Anthony@NetworkDefenseSolutions.com
Site: http://www.NetworkDefenseSolutions.com

Social Engineering on Rails

Social Engineering:

Why Social Engineering is Important

Commonly Abused by low-level attackers and high level attackers as a wild card.

Groups Like Anonymous are doing it to cause panic and fear (pin numbers, etc)

There is a need for it! You can find out a lot of information by innocent innocuous conversation than by nmap... and.. because people are stupid!

What can Social Engineering Glean?

Configurations

Passwords

Names of key people

Locations of key people

What to say to the next poor slob you get on the phone

Who should you target?

Social Engineering on Rails

Keeping Track of Lies & The Gender gap P1

Keeping track of lies is like tracking money in congress

More than half the time you will forget your lies. Software wont!

One slip of information in LEO status or a versed individual this can cost you a client, or worse.

If you are acting as a team, centralized methodologies can assist in 10x

Reverse engineering on the social front is easy. Learning the technologies aren't!

Social Engineering on Rails (Because typos can give you up!)

Our tool kit allows you to set parameters of what words will have replacements for your profile.

Profile creation is assisted, you won't have to do anything except think of a personality, user and a target!

Text statistics, and profile creation are some of the aspects that will be incorporated. Did you know...

Social Engineering on Rails

The Gender Gap is Real

Women have their own way to speak

You can identify a woman by how she types and speaks through text delivery methods (SMS, Facebook, Instant Messaging [Really?!])

Sometimes emotocons can be utilized as a metric to pinpoint women from men.

Conversation type and context also plays into identifying genders behind a screen

Men Don't Dabble They Smear!

The same things said for women can also be applied here for men

Emotocons and slang will differ from men and women

Men are more inclined to discuss things like mechanics, and other things women find useless (go figure)

Social Engineering on Rails

If You Thought Gender Gap Was Bad Enough....

Sexes and Geographic Location

Each location, demographic and race has their own slang. You'll need to know this

The easiest place to start is over-seas... It's rather simple

Religious factors also play a role but rather minute

Males and Their scams... How cute!

Over-seas comma, and periods are used differently within pricing schematics (U.S.: 1,340.00. Other: 1.340,00) Notice anything different?!

Trapped in the Philippines and need you monies grandma!

Social Engineering on Rails

Catfish Me Not! Your text says You're a dude!

The conversation is blah. Are you a he she with a she-wee?

How can we determine if we are talking to a woman or a guy?
(It's in the use of nouns and pronouns)

What about assistance? Can someone please help us?!

Resources: http://www.hackerfactor.com/GenderGuesser.php#Analyze

What can you obtain from instant conversations?

Some types of information include but are not limited to secret reset questions, innocent requests for such answers, and other contact information.

Validate the secret information rather quickly and in near real-time

Social Engineering on Rails

Reverse Engineering Humans:

What Goes into Reverse Engineering?

You will need to be an expert in something! Blind firing will get you just over the saddle of the door, and out the next one.

Reverse engineering with the job process or when selling a product

With reverse engineering also holds the risk of reverse mapping!

Why Should you Know Reverse Engineering?

Much harder to detect if it's done in the right tone.

People love pictures. Forging business cards and other material is enough "authentication" and you should know how to do this.

Find a person and play the emotional strings (love, hate, lust, etc.)

Places of abusing trust through images: FedEx Kinkos, Photoshop, Gimp and your imagination (vista prints, overnight prints, etc.)

Social Engineering on Rails

Low Level Training of SE/RE

What Are The Current Problems With Available Toolkits?

Training can cause some problems if you don't know se/re you may compromise the effectiveness of the test

Internal training can sometimes be an issue, and with software applications these hurtles may be overcome.

What can Angreifer Unbekannt do That others Can't?

Team Collaboration

Multiple targets, and target tracking through the software.

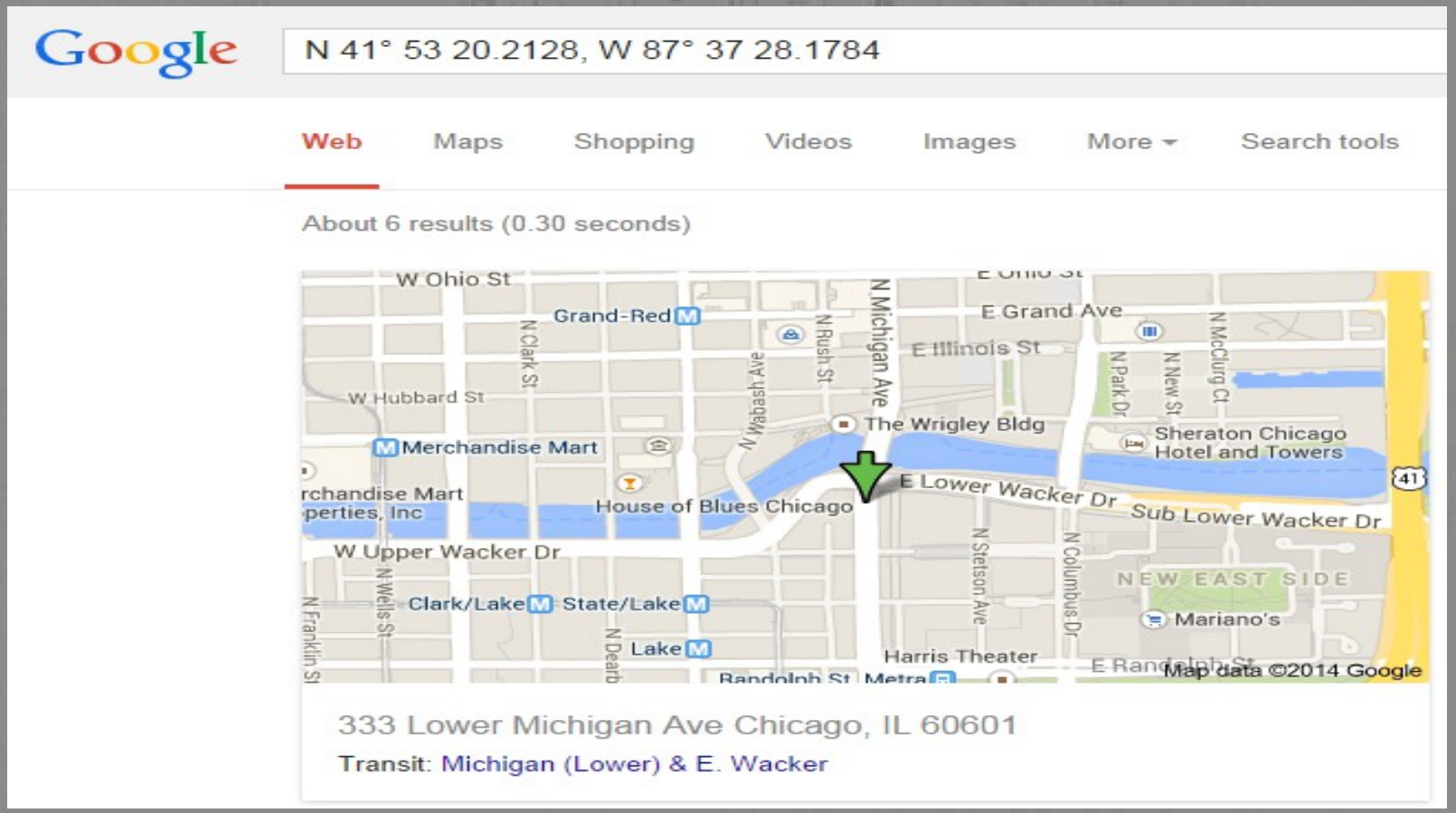
Updates can be cloud, network, internal, or external. Update once update everyone!

Statistics on what has worked (call home, etc) and what has not

Social Engineering on Rails

Combining Attacks

Using Pix!ti



Social Engineering on Rails

Presenter: Anthony Valente
A+, CCNA, CEH, BA Network Security.
Phone: 347-586-9386
E-mail: Anthony@NetworkDefenseSolutions.com
Site: http://www.NetworkDefenseSolutions.com