HACKING HUMANS:
Social Engineering with Real-Life Methods, Models, and Theories

Social Engineering
Building a More Secure World Thru Innovative Use of the Truth
HACKING HUMANS:
Social Engineering with Real-Life Methods, Models, and Theories

Introduction to the Dark Side

➳What is Social Engineering?
Wikipedia (www.wikipedia.org) defines social engineering as: *1) the practice of obtaining confidential information by manipulating users. 2) the practice of using psychological manipulation tactics to help or harm others.* This is a good definition, but it's only a start.

Many techies look down on Social Engineering, and consider it to be mere child's play, low-level, script-kiddy mind tricks. In fact, SE is both the easiest and the most difficult hack, depending upon how you go about it.

➳Sanitized stories

➳How to guard against it

➳Resources
What is Social Engineering?

●Why use it:
●Criminals—no l33+ $k1lz required
●Formal penetration testing teams
●Getting things done at work (privilege escalation)
●Improving interpersonal relations

➳Hacking humans

●Goal(s)—what do you want?
Why Do People Fall for It?

●Stupid?

●Gullible?

●Lazy?

●Exploitable!
How to Hack Humans
/** Pwn$ {u}

●Penetration Testing

●Control resources

●Leave backdoor

●Cover tracks
Services & Ports
Human and machine networks are same (just quirkier)
●Humans
•Self-esteem
•Apathy
•Sadness
•Happiness
•Gregariousness
•Ego / self-interest
•Benefit to self
•Commonalities
•Helpfulness
•Belonging

•Ex.: Bar pickup vs. wives (Bastion host in DMZ vs. standalone PKI root CA)
●Hosts
•telnet
•ftp
•sftp
•IpSec

HumInt
The Hidden Element
KNOW YOURSELF!!!
IPX/SPX vs. TCP/IP
Exploit Vulnerabilities
●Brain firewalls & content filters
●Finesse / Elicitation
●PKI model

HumInt
●**DON'T**
●Run an MS Office exploit against a BSD OS
●Keep hammering a port you can tell is closed (SSH ain't running on :8080 . . .)
•will get you blacklisted
•script kiddy vs. l33+ h@x04 (your neighbor's kid vs. Kevin Mitnik)

●**DO!**
●Know your target!

●Background
●Motivators
●Likes/dislikes
●Proceed with caution
●Finesse vs. not brute force (Hacker Ethic, don't leave it worse than you found it) ;)
Ex: Hammurabi village & corn
Sanitized Stories – irl 'spl01+$
●USB drives

●South American NOC service technicians

●Root-level CA and registrar server co-opt

●Fortune 100 datacenter badging / geometry

●Fortune 100 server heist w/ guards

Human IDS / IPS
How to Guard Against It
●Remain vigilant

●**ALWAYS** follow policies, baselines, and guidelines to the letter!
Questions?