



# SOCIAL ENGINEERING

Dress = \$300. Rented Tux = \$200.  
Bypassing Secret Service to meet the president inside the White House =  
Priceless!



# “Stratagem 1 "Deceiving the heavens to cross the sea”

## 瞒天过海

(Using the the 36 stratagems for Social Engineering)



Jayson E. Street, CISSP, C|EH,  
GSEC, GCIH, GCFA,  
IEM, IAM, ETC...

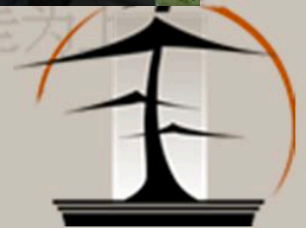


# Let go of my EGO

Who Am I?



THOTCON@f0rb1dd3n.com



# Hacker/Social Engineer

INFOSEC talk = slide like this ;-)

- Sun Wu (Tzu) “Ping-fa”(The Art of War)
- All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near. Hold out baits to entice the enemy. Feign disorder, and crush him.



# Contents

- INTRO
- History of the 36 Stratagems
- History of Social Engineering
- How S.E. differs between cultures
- The new OSI model
- Top 5 Stratagems relating to S.E.
- Discussion

請天過海 圍魏救趙 借刀殺人 以逸待勞  
擒賊擒王 李代桃僵 暗渡陳倉  
隔岸觀火 笑里藏刀 李代桃僵 順手牽羊  
打草驚蛇 借尸還魂 調虎離山 欲擒故縱  
圍魏救趙 擒賊擒王 釜底抽薪 渾水摸魚  
金蟬脫殼 羊門拐賊 遠交近攻 假道伐虢  
偷梁換柱 指桑罵槐 假痴不癲 上屋抽梯  
樹上開花 反客為主 美人計 空城計  
反間計 苦肉計 連環計 走为上



# The History of the 36 Stratagems

Cooking = France



Painting = Italy



Military Strategy = China



# The History of Social Engineering

From the beginning of time before it had a name it was being used as an effective form of attack.

Amenhotep III



The first Trojan attack



Bards masters of the (S.E.) craft



# How S.E. differs between cultures

Asia: Conformity Persuasion



Europe: Authority-Based Persuasion



North America: Need-Based Persuasion



South America: Reciprocation-Based Persuasion



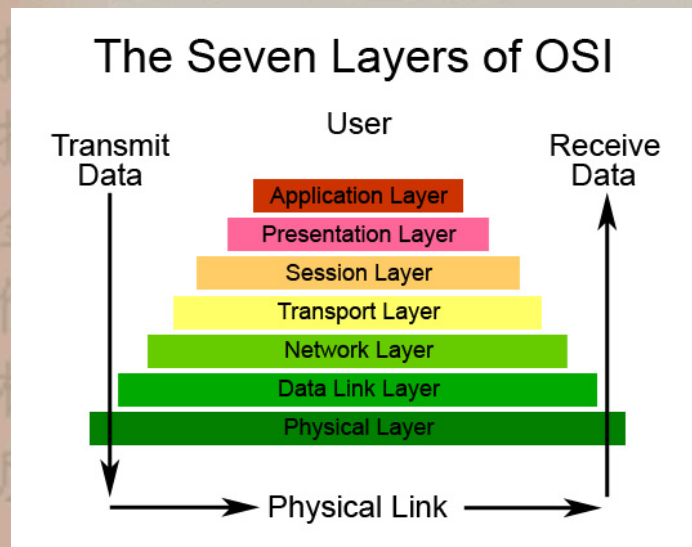


# The new OSI model

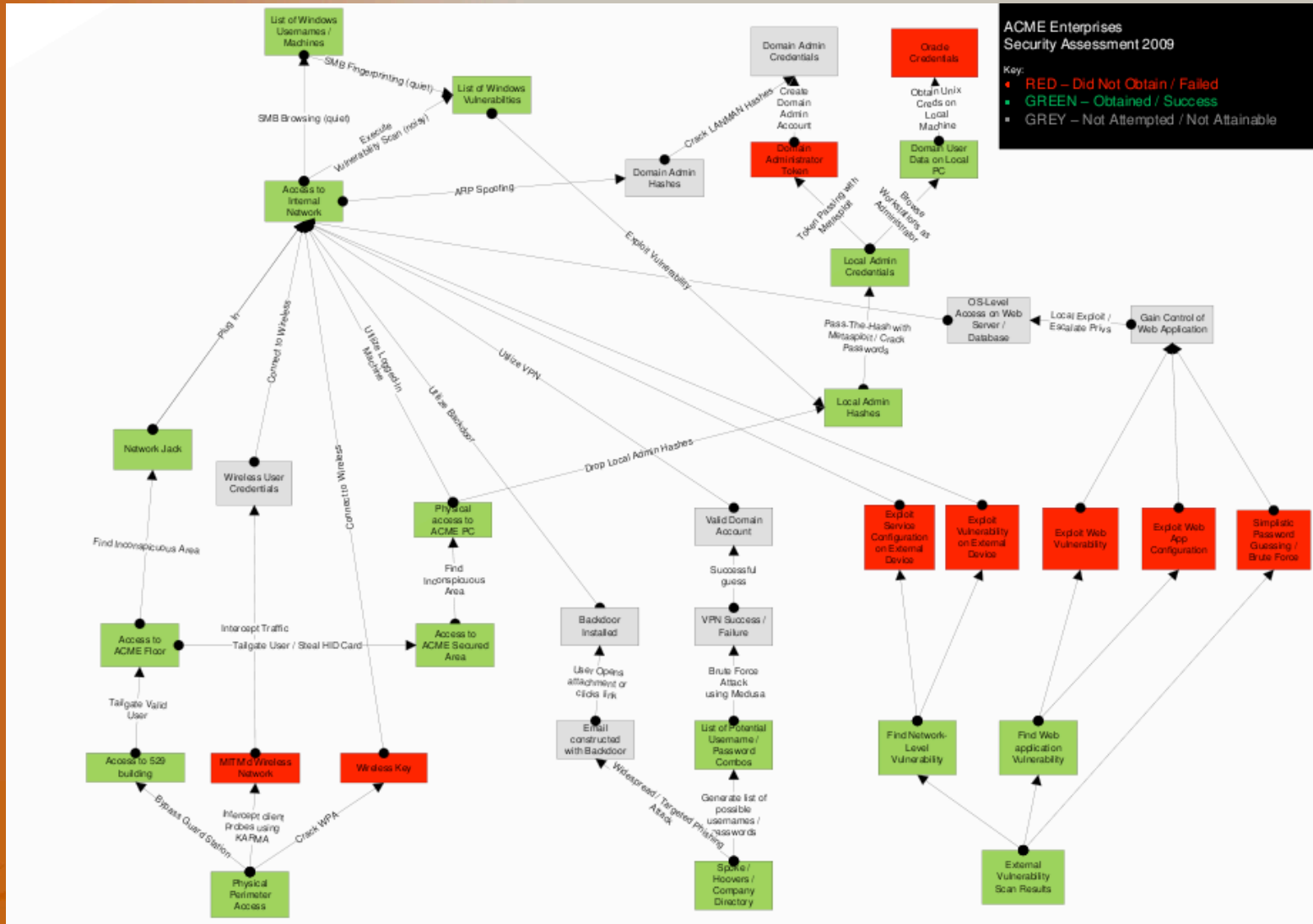
Layer 1-6 is over used time for a new vector.

Layer 7 good but getting better defended.

Layer 8 less guarded and can't be patched ;-)



# Why use Layer 8?



### 3. "Killing with a borrowed knife" 借刀杀人

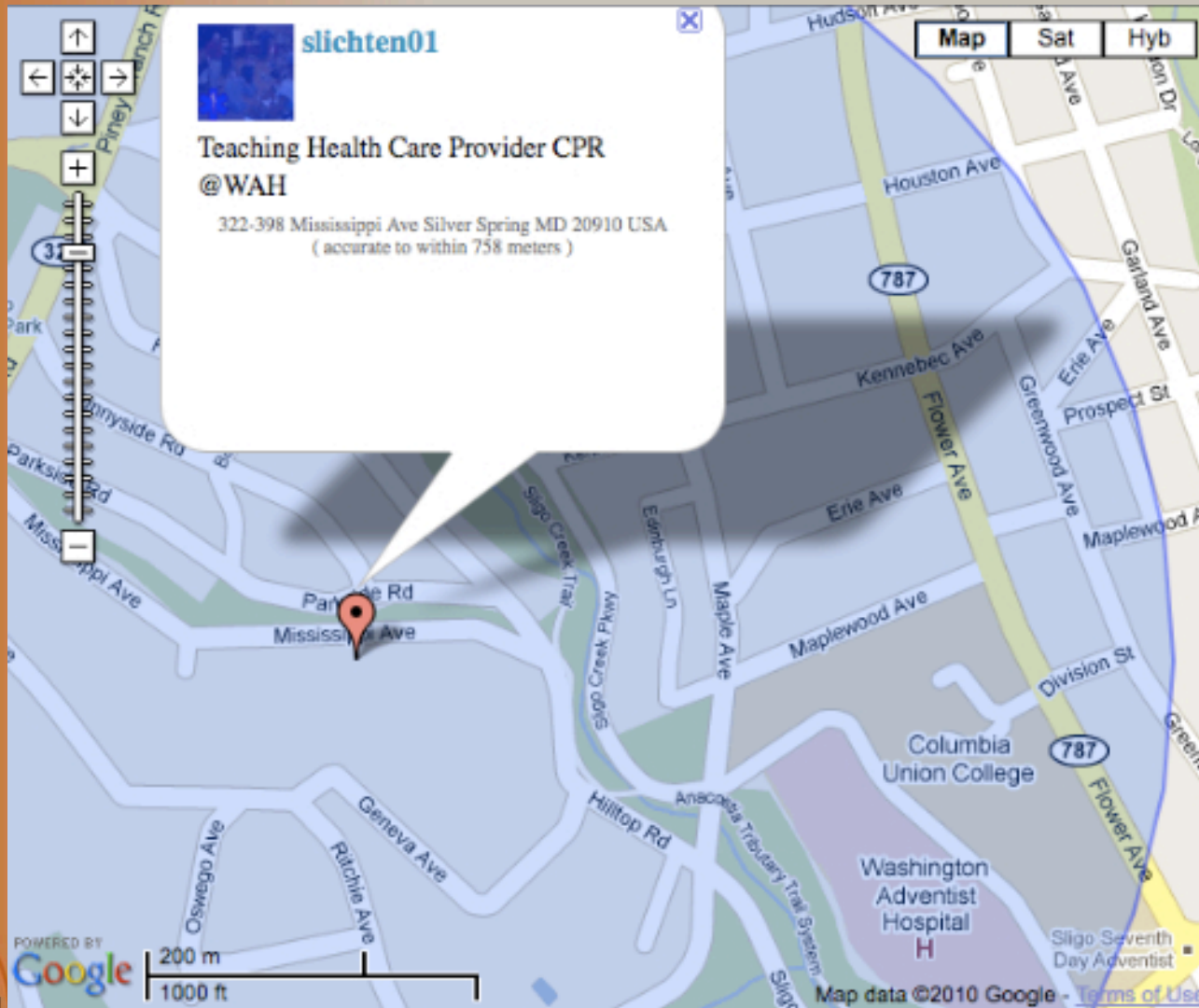
Turn an enemies asset against him  
(Let the employee be the attack vector)



### 3. "Killing with a borrowed knife"

借刀杀人

Cont...



逸待劳  
渡陈仓  
手牵羊  
擒故纵  
水摸鱼  
道伐虢  
屋抽梯  
城计



### 3. "Killing with a borrowed knife"

借刀杀人

Cont...

## Steven Lichtenberg

Washington D.C. Metro Area

**Current**

- volunteer EMT-B at GWGVFD
- Principal/consultant at Lichtenberg Associates
- VBOC Instructor at Montgomery County Volunteer Fire Rescue Association

1 more...


**Past**


- Consultant at Northrop Grumman Mission Systems
- independent consultant at innov8cs
- SR. Software Engineer at Jenark Business Systems

2 more...

**Education**

- University of Maryland College Park
- JFK High school

**Recommended**  2 people have recommended Steven

**Connections**  138 connections

**Industry** Health, Wellness and Fitness

---

### Steven Lichtenberg's Summary

A strong 20 year career in database design and development. I am now extremely interested in First Aid and Safety education and have participated in many training opportunities with both military and civilian agencies.

Instructor for CPR/AED/First Aid as well as an EMS instructor and EMT-B. Looking to expand this side of my life more.

Have taught IT and technical courses for community college and local independent training organizations.

以逸待劳  
暗渡陈仓  
顺手牵羊  
欲擒故纵  
浑水摸鱼  
假道伐虢  
上屋抽梯  
空城计  
走为上计



### 3. "Killing with a borrowed knife" 借刀杀人



待劳  
陈仓  
牵羊  
故纵  
摸鱼  
伐虢  
抽梯  
设计



### 3. "Killing with a borrowed knife"

借刀杀人

Cont...

#### Your Connections to OGE Energy Corp

To see how you're connected: [Join Now](#) or [Sign In](#)

#### Popular Profiles at OGE Energy Corp

[Amy Wegner](#), Recruiting and Placement  
[Reid Nuttall](#), VP Information Technology, CIO  
[Scott Milanowski](#), Director Utility Transformation - Smart Grid  
[Duane Kenyon](#), Dir, Business Systems  
[Randall Moss](#), Global Master Scheduler

#### New Hires and Recent Promotions at OGE Energy Corp

[Scott Milanowski](#), Director Utility Transformation - Smart Grid was Strategic Planner - 4 months ago  
[Donnie Jones](#), Director of Operations was Director Business Performance - 4 months ago  
[Lisa Cochran](#), Sr. Deployment Analyst was Sr. Process Designer - last month  
[Bill Busch](#), Manager HR Business Partners was OD Consultant - 4 months ago  
[Sandra Longcrier](#), Marketing/Message Management was Corporate Communications Supervisor - 3 months ago

To see more new hires & promotions: [Join Now](#) or [Sign In](#)

#### Jobs at OGE Energy Corp

Job Title	Location	Hiring Manager
-----------	----------	----------------

#### Key Statistics about OGE Energy Corp

**Top Locations**

- Oklahoma City, Oklahoma Area (238)
- Tulsa, Oklahoma Area (7)

Headquarters	Oklahoma City, Oklahoma Area
Industry	Utilities
Type	Public Company
Company Size	5,000 employees
Website	<a href="http://www.oge.com">http://www.oge.com</a>

**Common Job Titles**

Manager	4%
Project Manager	4%
Application Support Coordinator	3%
Executive Assistant	3%

**Top Schools**

Univ. of Oklahoma	14%
Oklahoma St. Univ.	11%
Oklahoma City Univ.	8%
Univ. of Central Oklahoma	6%
Univ. of Central Oklahoma - Coll. of Bus. Administration	5%

**Median Age** 37 years

**Gender**

Male	61%
Female	39%

待劳  
陈仓  
牵羊  
故纵  
摸鱼  
伐虢  
抽梯



## 5. "Looting a house on fire" 趁火打劫

Bad economy creates the proper kind of chaos  
for a subtle attack.



瞒天过海 围魏救赵 借刀杀人 以逸待劳  
趁火打劫 声东击西 无中生有 暗渡陈仓  
隔岸观火 笑里藏刀 借尸还魂 羊从鱼虎  
擒贼擒王 关门捉贼 指桑骂槐 弟  
树上开花 反客为主 美人计 空城计  
反间计 苦肉计 连环计 走为上

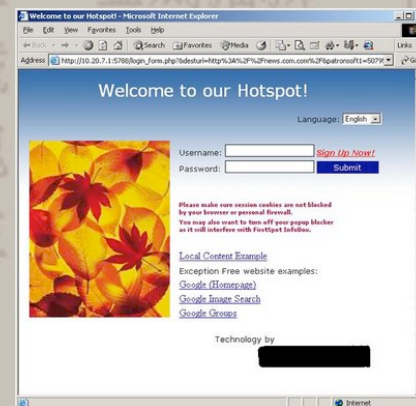
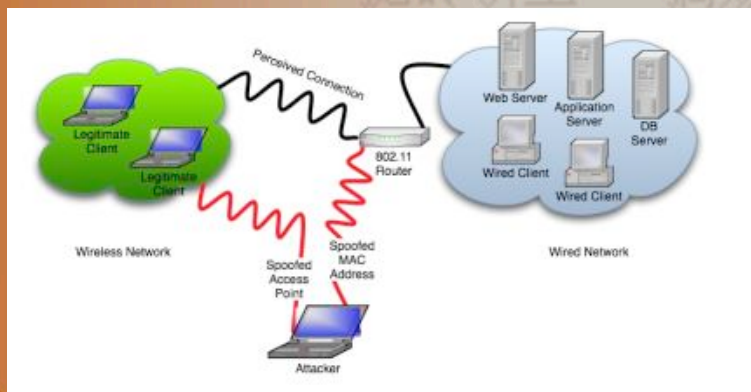




# 15. "Luring a tiger from its lair in the mountain" 调虎离山

Wait for the worker to take his network (laptop) to you.

```
aircrack-ng 1.2.3 - Aircrack-ng  
Aircrack-ng - A rogue AP setup utility.  
-  
The Shooop Group  
-  
Creating airod.conf... Done.  
Building the captive portal... Done.  
Setting the wireless parameters... Done.  
Done.  
Setting the IP address and default route... Done.  
Internet System Consortium DHCP Server 3.0.6  
Copyright 2004 ISC Internet Systems Consortium.  
All rights reserved.  
For info, please visit http://www.isc.org/dhcp/  
dhcpd 3.0.6: starting DHCP.  
Listening on IPv4 interface eth0:0.0.0.0:67,68:192.168.1.1  
Listening on IPv6 interface eth0:0.0.0.0:67,68:192.168.1.1  
No subnet declaration for eth0:192.168.1.100!  
** Ignoring request on eth0:192.168.1.100: not what  
you want: please write a subnet declaration  
in your dhcpd.conf file for the network segment  
to which interface eth0 is attached. **  
-  
Binding on socket /tmp/aircrack-ng/backnet  
Usage: Could not fully describe the server's fully qualified domain name, using 127.0.0.1 for ServerName  
Warning: Ignoring request on eth0:192.168.1.100:  
starting local DHCP responder:  
Starting DHCP server to broadcast DHCP... Done.  
Creating listening sockets for v.4 & v.6...  
Creating UDP socket for v.4 & v.6 - done.  
Creating UDP socket for v.4 & v.6 - done.  
Waiting for connections...  
Waiting for connections...  
Waiting for connections...  
Waiting for connections...
```



15. "Luring a tiger from its lair in the mountain"  
调虎离山



人有僵山薪攻癩  
以逸待劳  
暗渡陈仓  
顺手牵羊  
欲擒故纵  
浑水摸鱼  
假道伐虢  
上屋抽梯  
空城计  
走为上



## 17. "Tossing out a brick to get a jade" 抛砖引玉

\$15.00 USB could return an investment of  
\$5,000,000. If cast out to the right "lucky" person



## 36. "Escape - the best scheme" 走为上

Every plan should have an exit strategy in case the attack fails (especially if you are doing it in the "real world").



以逸待劳  
暗渡陈仓  
顺手牵羊  
欲擒故纵  
浑水摸鱼  
假道伐虢  
上屋抽梯  
空城计  
走为上



# Okay now what can we do?



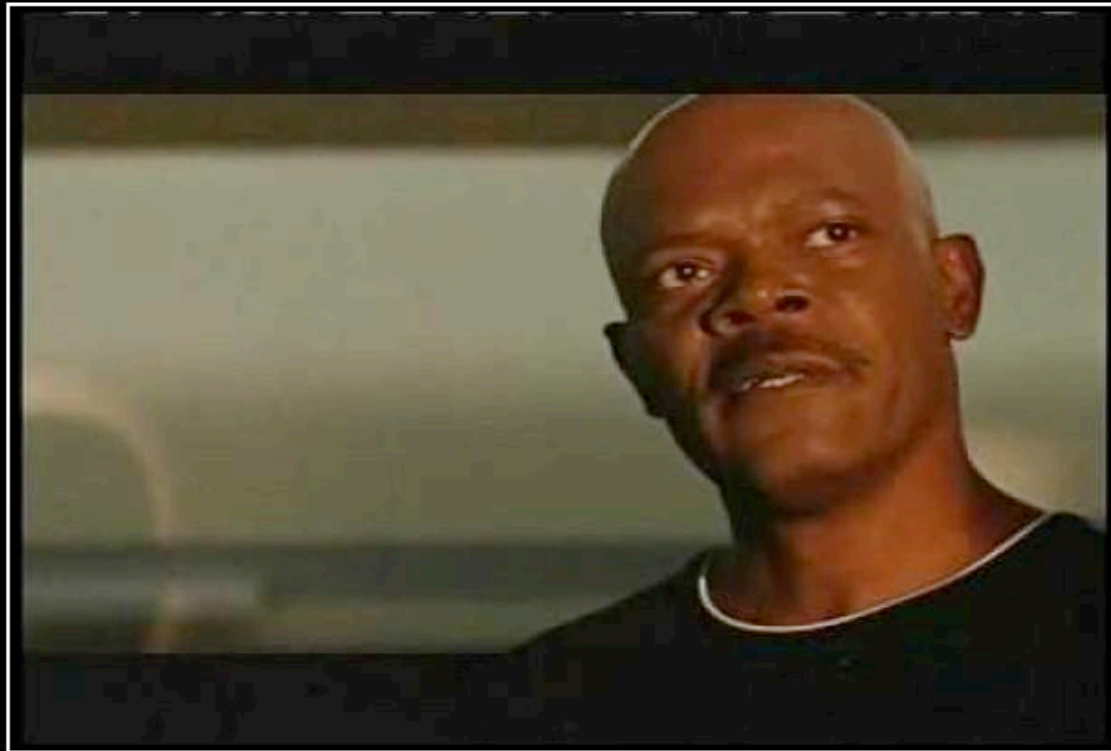
IT ONLY TAKES  
**20**  
SECONDS.

Less than 20 seconds after a Windows PC is connected to the internet, someone, somewhere will hack it.

 Fight Back. Use a firewall.



# Okay now what can we do?



## SECURITY AWARENESS

I'm tired of these Motha FSCKing Users!  
With Motha FSCKing easy to guess passwords!

待劳  
陈仓  
牵羊  
故纵  
摸鱼  
伐虢  
抽梯  
计



STRATAGE

"DEFENSE THROUGH DISCOVERY"

# Okay now what can we do?

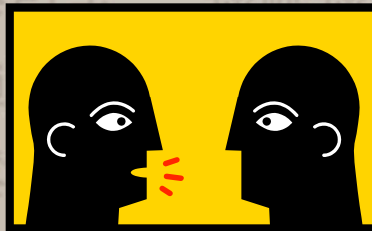
- Without understanding where the opponent's weaknesses are you cannot borrow their strength to use against them. (Cheng Man Ching)
- <http://www.dissectingthehack.com>
- <http://f0rb1dd3n.com>
- <http://headhacker.net>
- <http://www.social-engineer.org/>
- <http://netragard.com>
- <http://isc.sans.org>
- @jaysonstreet on Twitter

瞒天过海 围魏救赵 借刀杀人 以逸待劳  
趁火打劫 声东击西 无中生有 暗渡陈仓  
隔岸观火 笑里藏刀 李代桃僵 顺手牵羊  
打草惊蛇 借尸还魂 调虎离山 欲擒故纵  
此致引玉 擒贼擒王 釜底抽薪 浑水摸鱼  
金蝉脱壳 关门捉贼 远交近攻 假道伐虢  
偷梁换柱 指桑骂槐 假痴不癫 上屋抽梯  
树上开花 反客为主 美人计 空城计  
反间计 苦肉计 连环计 走为上



# Now let's learn from others

- Discussion and Questions????
- Or several minutes of uncomfortable silence it is your choice.



• This concludes my presentation Thank You





# Those Links Again

- <http://www.dissectingthehack.com>
- <http://f0rb1dd3n.com>
- <http://headhacker.net>
- <http://www.social-engineer.org/>
- <http://netragard.com>
- <http://isc.sans.org>
- @jaysonstreet on Twitter

請天過海 圍魏救趙 借刀殺人 以逸待勞  
趁火打劫 聲東擊西 無中生有 暗渡陳倉  
隔岸觀火 笑里藏刀 李代桃僵 順手牽羊  
打草驚蛇 借尸還魂 調虎離山 欲擒故縱  
拋磚引玉 擒賊擒王 釜底抽薪 渾水摸魚  
金蟬脫壳 關門捉賊 遠交近攻 假道伐虢  
偷梁換柱 指桑罵槐 假痴不癲 上屋抽梯  
樹上開花 反客為主 美人計 空城計  
反間計 苦肉計 連環計 走为上

