



# 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?



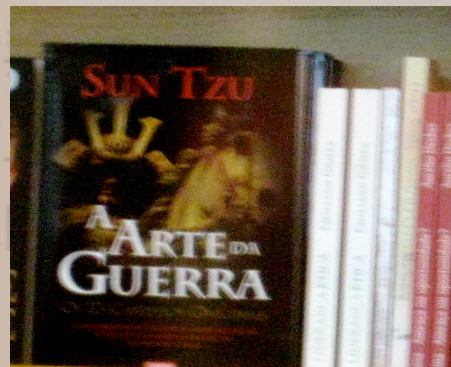
defcon18@f0rb1dd3n.com



# 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



# The History of the 36 Stratagems

Cooking = France



Painting = Italy



Military Strategy = China



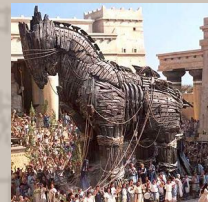
# The History of Social Engineering

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: Save face = Losing secrets



Europe: Command = Control



North America: Do unto others = Before they do to you



South America: Mutual benefit = An uneven outcome





# The new OSI model

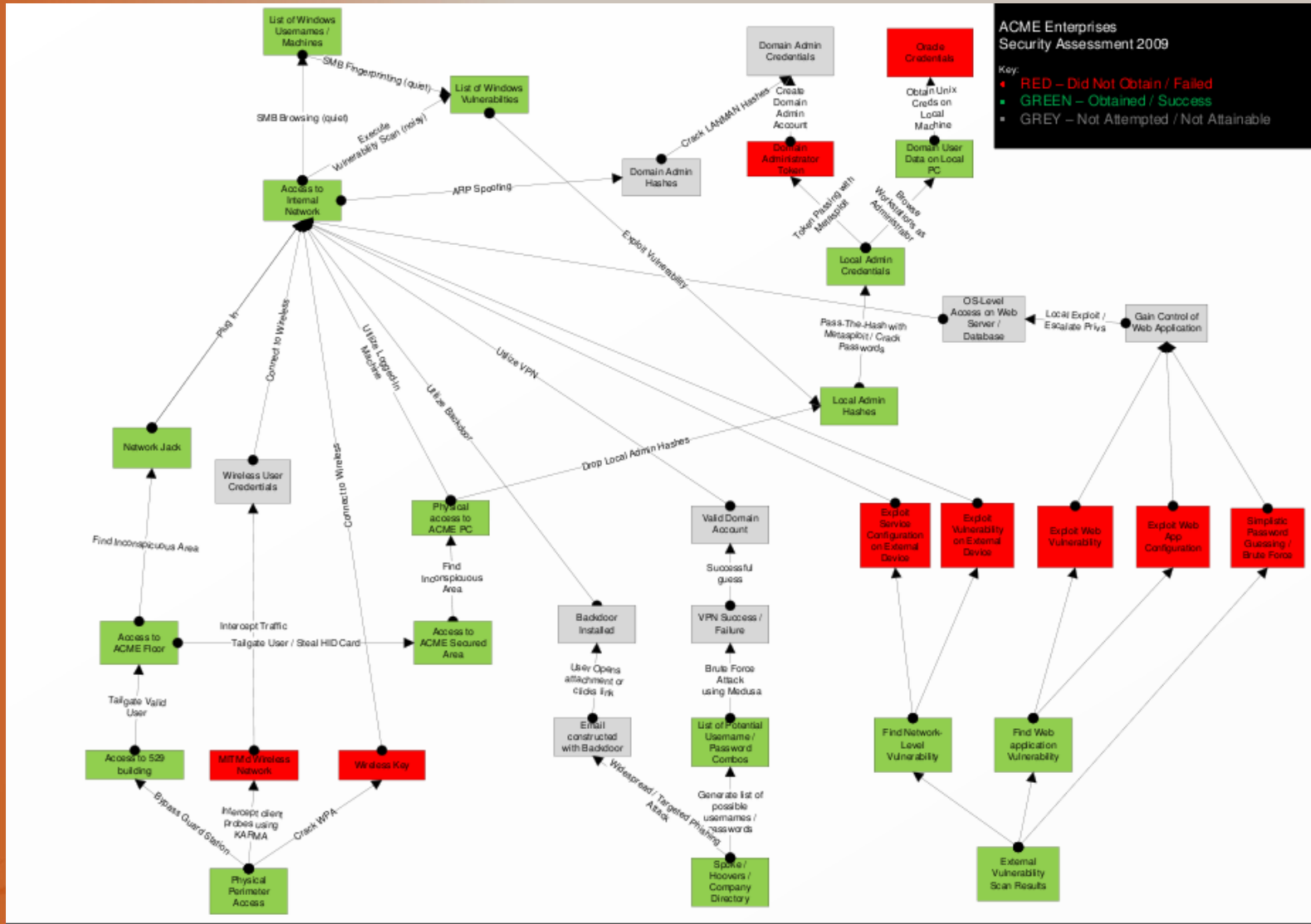
Layer 1-6 is over used time for a new vector.

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...

**User Profile**  
@haxorthematrix  
PaulDotCom Podcast & Blog, dedicated to providing the latest information security news, and information about hacking, research, vulnerabilities.  
Providence, RI  
Friend  
<http://www.pauldotcom.com>  
Twitter page

1816 Followers 1783 Following 2000 Tweets Lists

@jafolkerts Yes, that's the one I meant. An initial look made it look like Mercedes was on that house.....  
1813  
haxorthematrix, [+] Tue 09 Feb 13:24 via TweetDeck in reply

@jafolkerts Never heard of it, but now adding to the arsenal!  
1813  
haxorthematrix, [+] Tue 09 Feb 13:10 via TweetDeck in reply

@jafolkerts Nice find. I bet that the house across the street with the pick with ladder and Mercedes SUV is your winner.  
1813  
haxorthematrix, [+] Tue 09 Feb 13:02 via TweetDeck in reply

RT @donttrythis: <http://twitpic.com/128p1b> - Now it's off to work in my beast. <---thanks to exiftool, we know where you live.  
1812  
haxorthematrix, [+] Tue 09 Feb 10:34 via TweetDeck

Anyone know of a way to grap existing contents of the Windows Security log form 90+ machines easily? Filter by event type would be nice too  
1812  
haxorthematrix, [+] Tue 09 Feb 10:16 via TweetDeck

Yes, yes I did eat half a can of Tactical Bacon (<http://tinyurl.com/yahyz4t>) at the podcaster's meetup at #shmoocon. Also took mv statin!  
1803

Remaining API: 62/150 Resets: 22:01  
**User Profile**  
Joel  
@jafolkerts  
Developer, forensics, security, student  
Iowa

Twitter page

86 Followers 176 Following 227 Tweets Lists

@haxorthematrix Looks like it one house east (open garage door)  
86  
jafolkerts, [+] Tue 09 Feb 13:21 via TweetDeck

@haxorthematrix If you analyze at the interior pic (<http://twitpic.com/128l7d>), it's also grabbed the GEO Coords (<http://bit.ly/b15PVk>)  
86  
jafolkerts, [+] Tue 09 Feb 13:20 via TweetDeck in reply to...

@haxorthematrix Ever heard of Google Earth PhotoTag? (<http://bit.ly/cBmr8O>) Too easy...  
86  
jafolkerts, [+] Tue 09 Feb 13:08 via TweetDeck in reply to...

@haxorthematrix Look familiar? <http://bit.ly/bg9HDV> (Google Maps Street View of .donttrythis's house)  
86  
jafolkerts, [+] Tue 09 Feb 12:59 via TweetDeck

@haxorthematrix Good catch! :)  
86  
jafolkerts, [+] Tue 09 Feb 11:32 via TweetDeck in reply to...


RT @Mandiant: MANDIANT is hiring Security Consultants and Associates <http://bit.ly/dbAzzz>  
86  
jafolkerts, [+] Tue 09 Feb 11:21 via TweetDeck

@LanceUlanoff Great commercial up to that



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

Cont...



twitpic  
share photos on twitter

Twitter username: .....  
 Remember me **Login**

Rotate photo View full size

Posted on February 9, 2010 by dontrythis

More photos by dontrythis

Put this photo on your website

Views 13,592  
Tags

Report Image

Now it's off to work in my beast. Wait... How'd that DOG get in there?

Login to leave a comment

prbowman on February 10, 2010  
Ever catch air in that vehicle? :-)

denniifloss on February 10, 2010  
Driving in style!!

Pirelli on February 9, 2010  
YEAH! Nice wheels!!!

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

Cont...



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

借刀杀人

Cont...

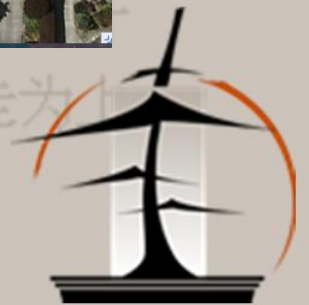


反间计

苦肉计

连环计

走为上计



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

Cont...

The screenshot shows a web browser window displaying the website "I Can Stalk U". The browser's address bar shows the URL "http://icanstalku.com/". The website header includes the title "I Can Stalk U" and the tagline "Raising awareness about inadvertent information sharing". Below the header are navigation links for "Home", "How", "Why", "About Us", and "Contact Us". The main content area is titled "What are people *really* saying in their tweets?" and lists several tweets, each with a profile picture, name, and location data (Latitude and Longitude). The tweets are as follows:

- 1andreas:** I am currently nearby Latitude: 52.3743, Longitude: 4.88467 (less than a minute ago)
- FLAREmagazine:** I am currently nearby Latitude: 43.6692, Longitude: -79.3857 (less than a minute ago)
- alielayus:** I am currently nearby Latitude: 35.2652, Longitude: -116.075 (less than a minute ago)
- Scentsational:** I am currently nearby 4130 S Normandie Ave Los Angeles CA (2 minutes ago)
- champagne\_ste:** I am currently nearby Latitude: 53.5857, Longitude: -2.53317 (1 minute ago)
- kyledoherty:** I am currently nearby Santa Clarita CA (3 minutes ago)
- BarelyBlind:** I am currently nearby Eastex Fwy Houston TX (3 minutes ago)
- philsnews:** I am currently nearby I- 44 Oklahoma City OK (4 minutes ago)
- brianfeldman:** I am currently nearby 117 Semoran Blvd Casselberry FL (8 minutes ago)
- elliottbay\_beer:** I am currently nearby 385 SW 152nd St Burien WA (7 minutes ago)

On the right side of the page, there is a "Links" section with a list of organizations: Mayhemic Labs, PaulDotCom, SANS ISC, Electronic Frontier Foundation, and Center for Democracy & Technology. Below the links is a section titled "How did you find me?" with a sub-section "Did you know that a lot of smart phones encode the location of where pictures are taken? Anyone who has a copy can access this information." and a "read more" link. At the bottom of this section is "Help me fix this!" with a sub-section "Disabling Geo-Tagging on your phone is easy. Check our list of common phones." and a "read more" link.

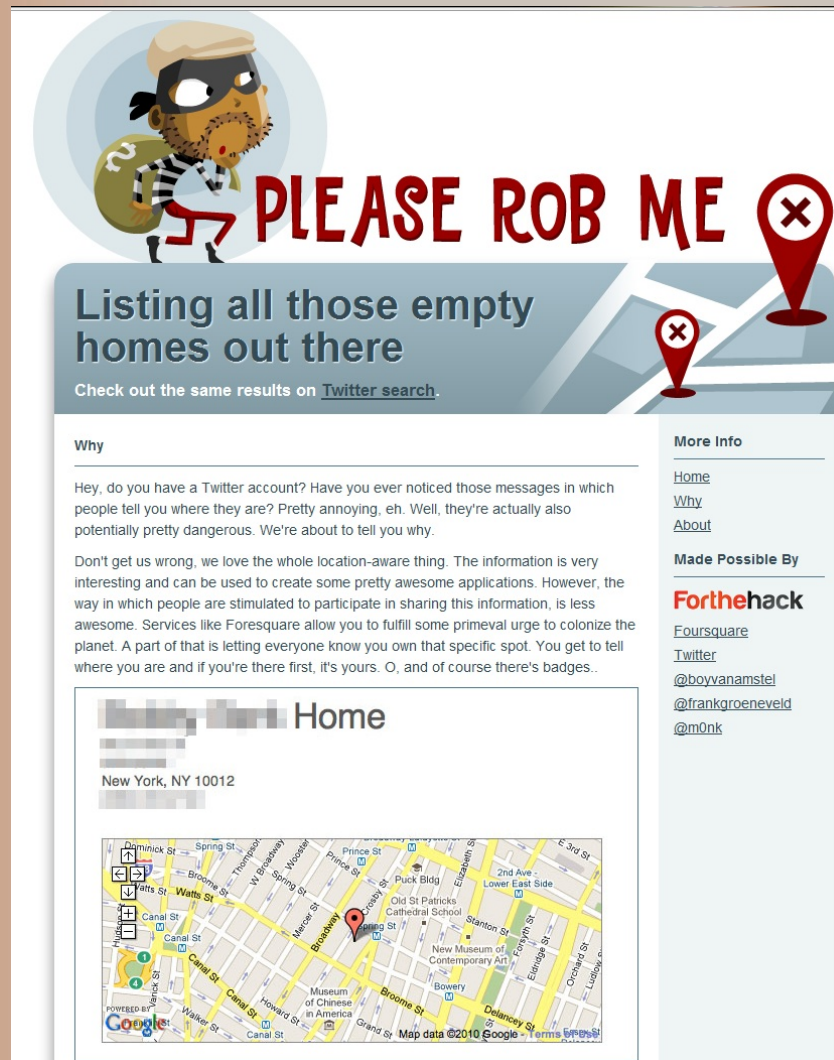




### 3. "Killing with a borrowed knife"

借刀杀人

Cont...



**PLEASE ROB ME**

Listing all those empty homes out there

Check out the same results on [Twitter search](#).

**Why**

Hey, do you have a Twitter account? Have you ever noticed those messages in which people tell you where they are? Pretty annoying, eh. Well, they're actually also potentially pretty dangerous. We're about to tell you why.

Don't get us wrong, we love the whole location-aware thing. The information is very interesting and can be used to create some pretty awesome applications. However, the way in which people are stimulated to participate in sharing this information, is less awesome. Services like Foursquare allow you to fulfill some primeval urge to colonize the planet. A part of that is letting everyone know you own that specific spot. You get to tell where you are and if you're there first, it's yours. O, and of course there's badges..

**More Info**

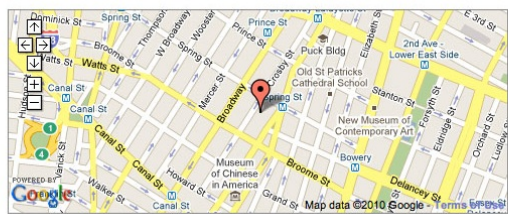
[Home](#)  
[Why](#)  
[About](#)

**Made Possible By**

**Forthefhack**  
[Foursquare](#)  
[Twitter](#)  
[@boyvanamstel](#)  
[@frankgroeneveld](#)  
[@m0nk](#)

**Home**

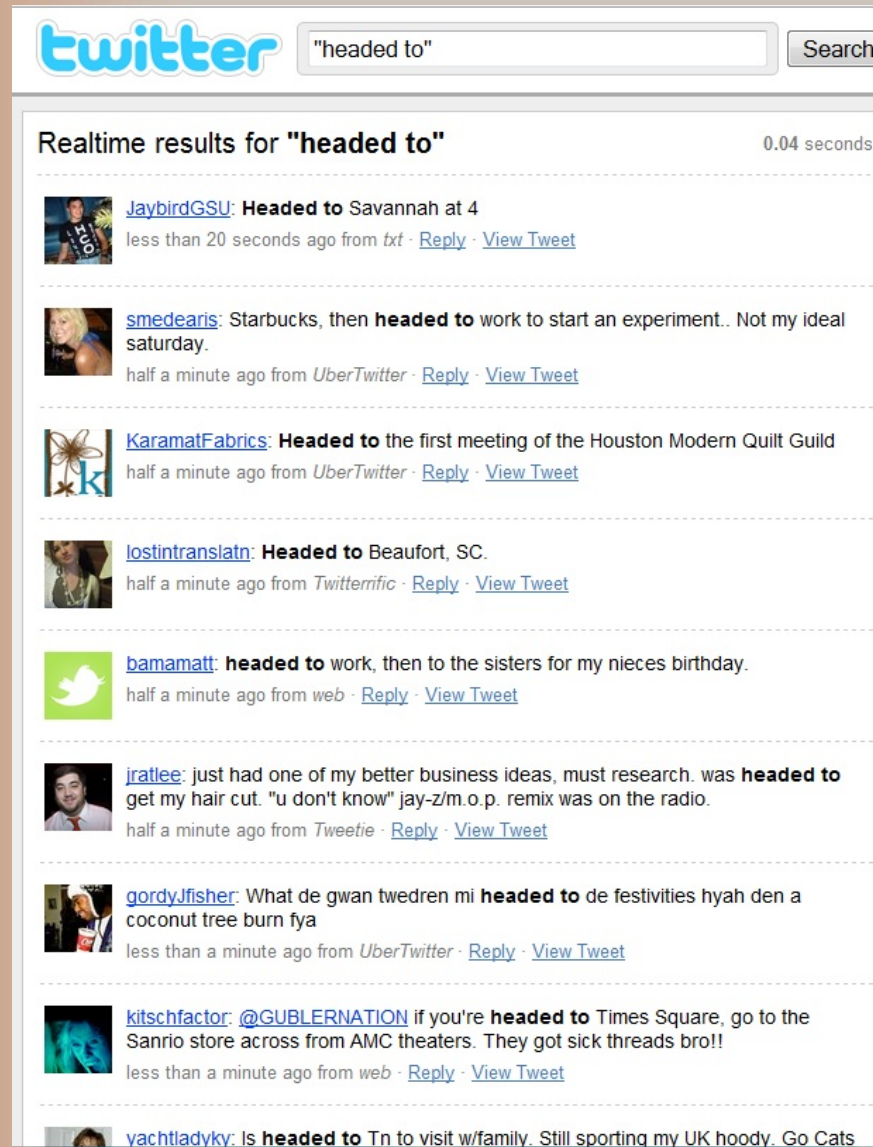
New York, NY 10012



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  
走为上计



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



The screenshot shows a Twitter search interface with the query "headed to". The search results are displayed in a list format, showing real-time tweets from various users. Each tweet includes the user's profile picture, name, and the text of the tweet. The tweets are separated by horizontal dashed lines. The search bar at the top contains the text "headed to" and a "Search" button. The results are titled "Realtime results for 'headed to'" and show a search time of "0.04 seconds".

twitter "headed to" Search

Realtime results for "headed to" 0.04 seconds

- JaybirdGSU:** Headed to Savannah at 4  
less than 20 seconds ago from txt · Reply · View Tweet
- smedearis:** Starbucks, then headed to work to start an experiment.. Not my ideal saturday.  
half a minute ago from UberTwitter · Reply · View Tweet
- KaramatFabrics:** Headed to the first meeting of the Houston Modern Quilt Guild  
half a minute ago from UberTwitter · Reply · View Tweet
- lostintranslatn:** Headed to Beaufort, SC.  
half a minute ago from Twitterrific · Reply · View Tweet
- bamamatt:** headed to work, then to the sisters for my nieces birthday.  
half a minute ago from web · Reply · View Tweet
- iratlle:** just had one of my better business ideas, must research. was headed to get my hair cut. "u don't know" jay-z/m.o.p. remix was on the radio.  
half a minute ago from Tweetie · Reply · View Tweet
- gordyJfisher:** What de gwan twedren mi headed to de festivities hyah den a coconut tree burn fya  
less than a minute ago from UberTwitter · Reply · View Tweet
- kitschfactor:** @GUBLERNATION if you're headed to Times Square, go to the Sanrio store across from AMC theaters. They got sick threads bro!!  
less than a minute ago from web · Reply · View Tweet
- yachtladyky:** Is headed to Tn to visit w/family. Still sporting my UK hoody. Go Cats

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 Cont...

Network Diagram Tool  
Produce Up-to-date Network Diagrams with Topology & Configuration-Fast

Free Network Diagram  
Map & Discover Your Entire Network with Qualys Free Map!

Ads by Google

---

HOME LAST LOGGED IN VIEW COMMENTS MEMBER SEARCH LOST PASSWORD SITE FAQ CONTACT US

Network Documentation

Worst 0 1 2 3 4 5 6 7 8 9 10 Awesome!

click diagram for a clear full size view

**SCTCS Network/Server Diagram**  
Enoree Building, Synergy Business Park

IP Addresses and other miscellaneous information has been removed. My supervisors would be quite unhappy with me if I posted the full version.

**SignUpNow!**

**Rate Network Diagrams**

- » Rate Large Networks
- » Rate Small Networks
- » Rate Home Networks
- » Rate Network Racks
- » Rate Funny Diagrams
- » Rate All

**Large Networks**

- » Cthistle 7.9316
- » Bobdonkey 7.5661
- » 24567920 7.0292

**Small Networks**

- » Ijoy 8.9457
- » Hodgesbo 6.6030
- » Suicideboy 6.5566

**Home Networks**

- » Dmessana 8.5250
- » Luser 8.1453
- » Stverschoof 7.8942

**Network Racks**

- » Layer1guy 7.3596
- » Networkguy 6.7924
- » Nsteam 6.5891

**Funny Diagrams**

- » Joeholden 9.6162
- » Gavo 6.7943
- » Mindrue 6.1022

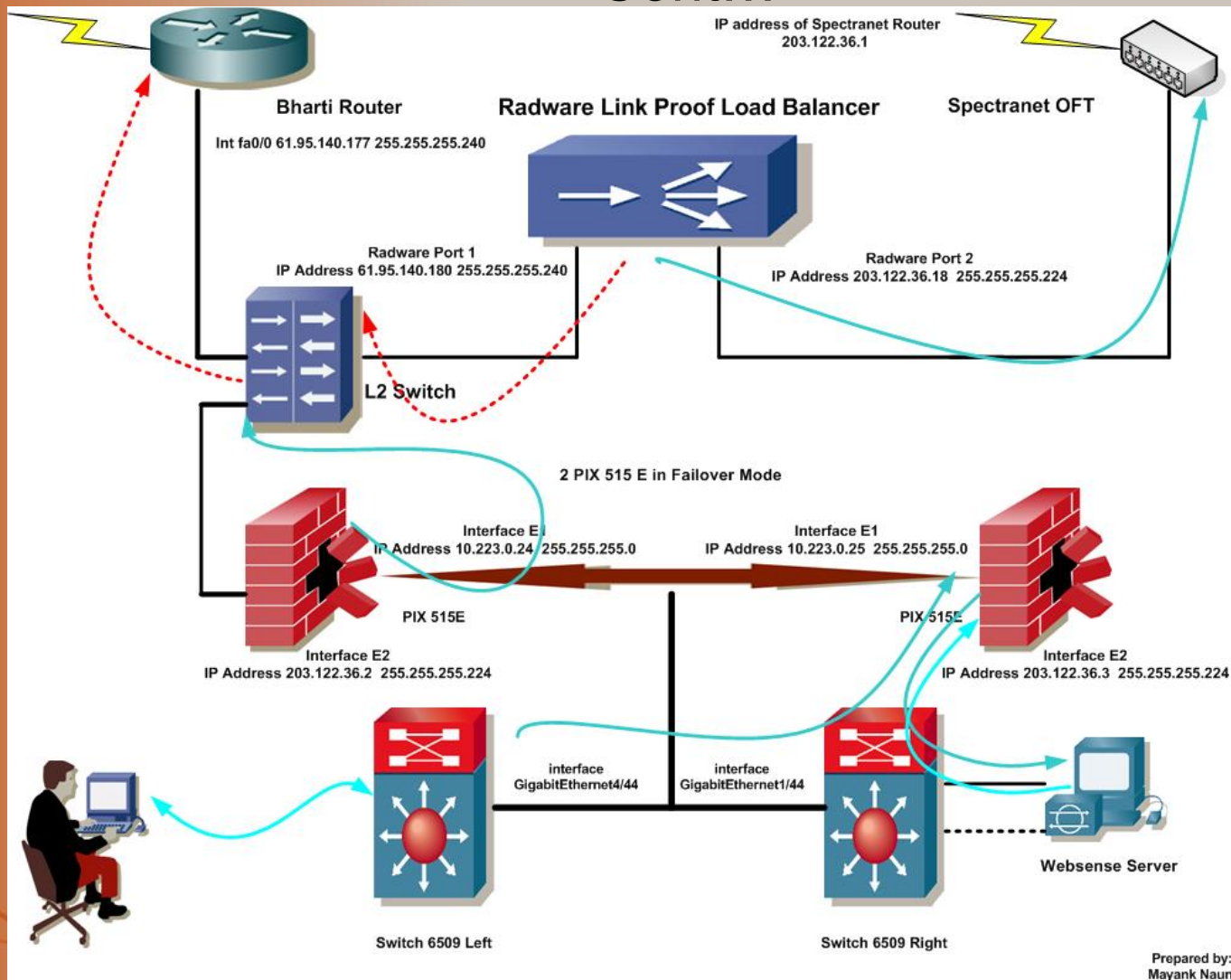
以逸待劳  
暗渡陈仓  
顺手牵羊  
欲擒故纵  
浑水摸鱼  
假道伐虢  
空城计  
走为上计



### 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  
为上



Prepared by:  
Mayank Nauri

## 5. "Looting a house on fire" 趁火打劫

Lay offs / acquisitions create the proper kind of chaos for a subtle attack.

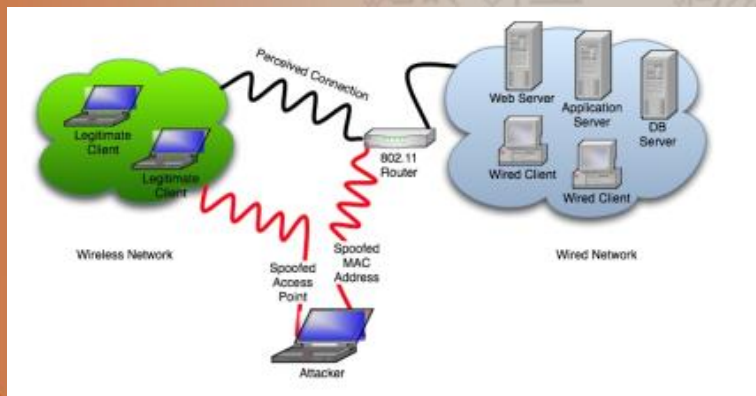
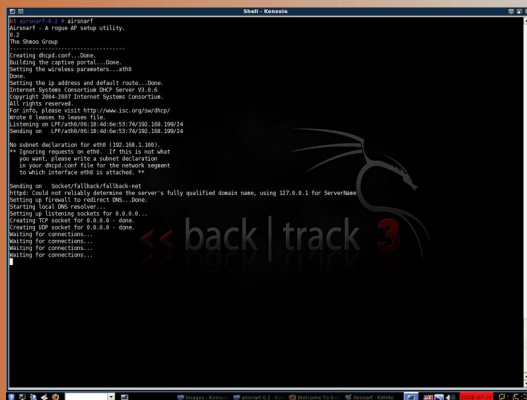


瞒天过海 围魏救赵 借刀杀人 以逸待劳  
趁火打劫 声东击西 无中生有 暗渡陈仓  
隔岸观火 笑里藏刀 借尸还魂 羊从鱼虎  
擒贼擒王 关门捉贼 指桑骂槐 弟  
树上开花 反客为主 美人计 空城计  
反间计 苦肉计 连环计 走为上计



# 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.



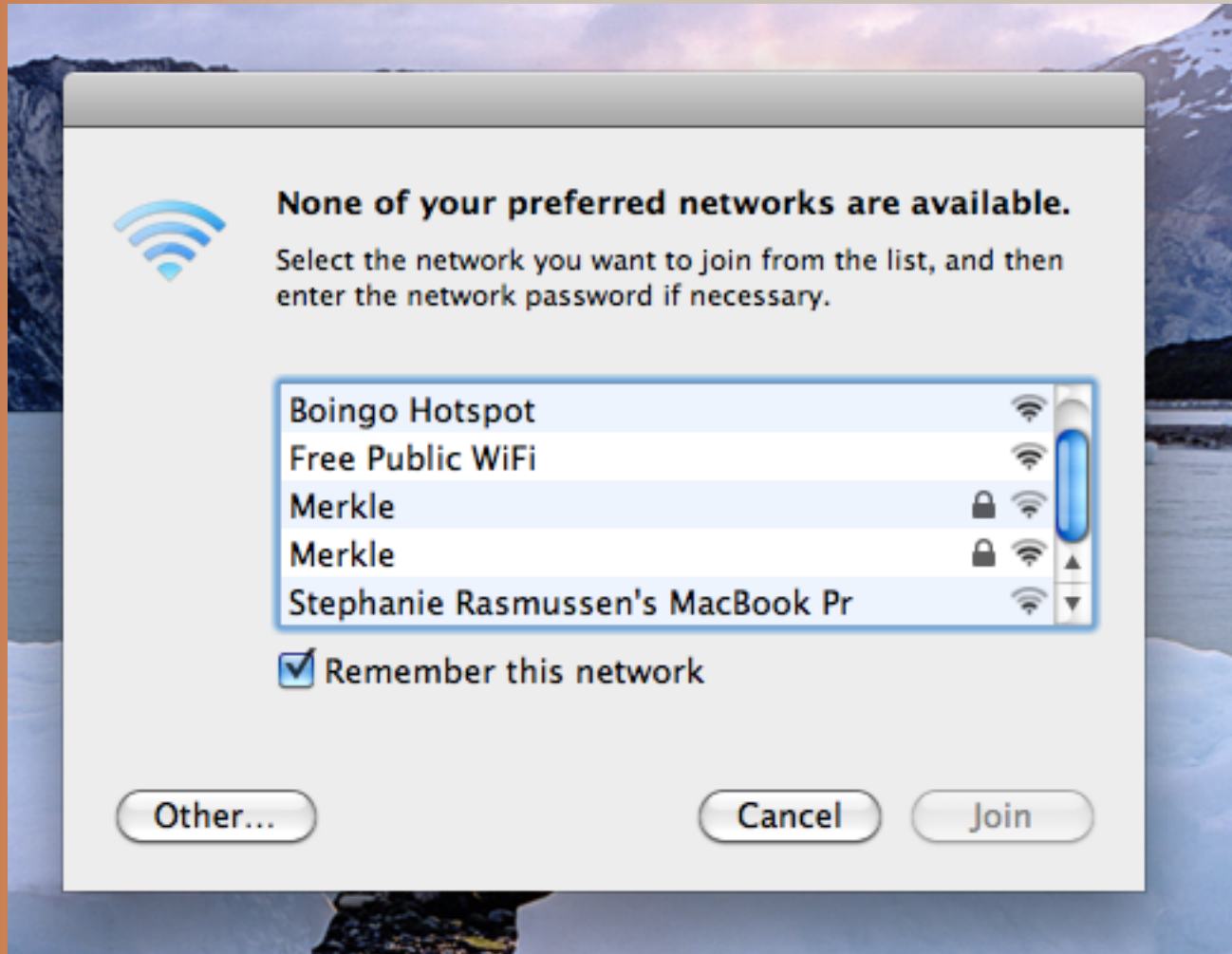
15. "Luring a tiger from its lair in the mountain"  
调虎离山



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  
走为上计



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



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





# 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

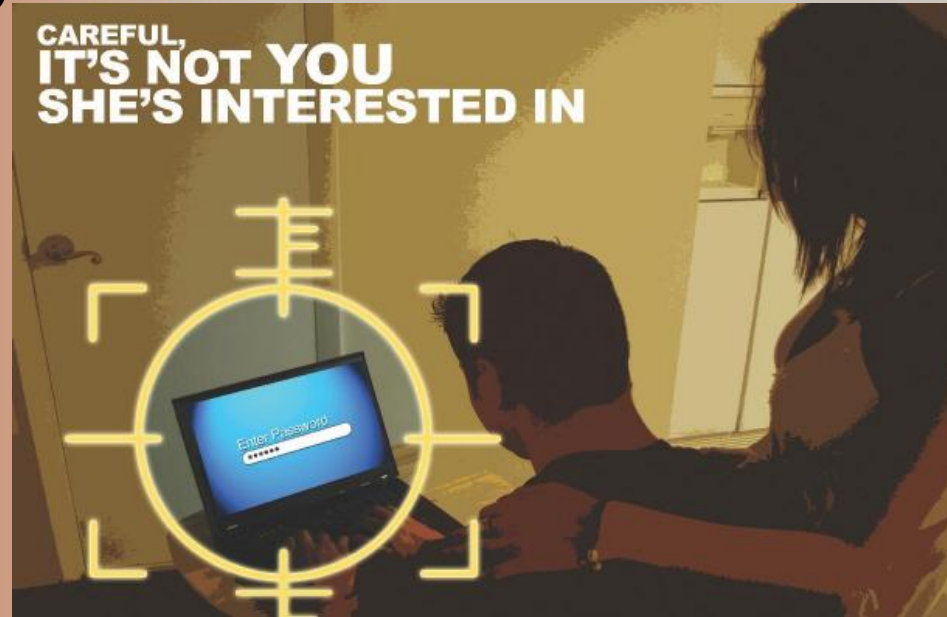
Every plan should have an exit strategy in case the attack fails (especially if you are doing it in the "real world").



瞒天过海 围魏救赵 借刀杀人 以逸待劳  
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?



以逸待劳  
暗渡陈仓  
顺手牵羊  
欲擒故纵  
浑水摸鱼

抛砖引玉 擒贼擒王 釜底抽薪

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?



## PHYSICAL COMPROMISE

Yeah it's just like them.

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



**STRATAGEM 1 SOLUTIONS**  
"DEFENSE THROUGH DISCOVERY"

# Okay now what can we do?



## APT

There are people smarter than you, they have more resources than you,  
and they are coming for you. Good luck with that.

待劳  
陈仓  
牵羊  
故纵  
摸鱼  
伐虢  
抽梯  
计



**STRATAGEM 1 SOLUTIONS**  
"DEFENSE THROUGH DISCOVERY"

Thanks to @0ph3lia

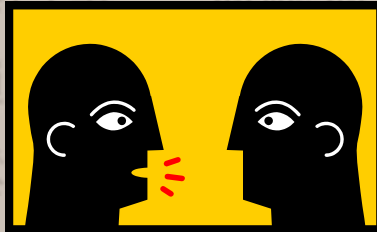
# Okay now what can we do?

- 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



# 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

請人過海 圍魏救趙 借刀殺人 以逸待勞  
趁火打劫 戶東擊西 無中生有 暗渡陳倉  
隔岸觀火 笑里藏刀 李代桃僵 順手牽羊  
驚蛇草動 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  
金蟬脫殼 閉門捉賊 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 走為上計

