



# RED TEAM TESTING

CHRIS NICKERSON

LARES

# Agenda

Who Are You?

Why should we do Red Team Testing

Methodology

- Gather Information
- Scan for Vulnerabilities
- Plan The Attack
- Execute
- Dig for Data

# A Little about me . . . .

## Chris Nickerson

### Employment History:

- Founder, Lares
- Director ,Security Services Alternative Technology
- Team Lead, KPMG
- Lead Security Architect /Compliance Mgr., Sprint
- Sr. Security Architect, Shook Hardy & Bacon
- US NAVY

### Professional Certifications:

- CISSP
- CISA
- ISO 17799
- NSA IAM
- CCNA

### Security Stuff

- Created Risk Management and CSO structure for many fortune 500
- Created Global Compliance /Penetration testing practices
- Contributor to Social-Engineer.org
- InformIT,Ethical Hacker.net
- Exotic Liability Podcast / Site
- Other media whoring...



# Why do SE Testing/Red Teaming?

---

Military tactics are like unto water; for water in its natural course runs away from high places and hastens downwards.

Water shapes its course according to the nature of the ground over which it flows; the soldier works out his victory in relation to the foe whom he is facing.

He who can modify his tactics in relation to his opponent and thereby succeed in winning, may be called a heaven-born captain.

The five elements (water, fire, wood, metal, earth) are not always equally predominant; the four seasons make way for each other in turn.

---

-Sun Tzu

# *Red Team Testing:*

The term originated within the military to describe a team whose purpose is to penetrate security of "friendly" installations, and thus test their security measures. The members are professionals who install evidence of their success, e.g. leave cardboard signs saying "bomb" in critical defense installations, hand-lettered notes saying that "your codebooks have been stolen" (they usually have not been) inside safes, etc. Sometimes, after a successful penetration, a high-ranking security person will show up later for a "security review," and "find" the evidence. Afterward, the term became popular in the computer industry, where the security of computer systems is often tested by tiger teams.

**How do you know you can put up a fight if you have never taken a punch?**

# Why should I do it?

- It goes Beyond compliance
- It simulates the REAL WORLD attacks
- Hackers don't have scopes.... Why should a test?
- Do you really think testing .1% of your assets makes the COMPANY secure?
- You never know the value of what you have till its gone.

# Why traditional Testing is Dead

- It does not focus risk on Business, but on exposure of vulnerability
- Testing that replicates an attacker (sparring partner) has its hands tied.
- The perimeter is DEAD (give it up... its over.....srsly..... For really realz... ok? Please?)
- I gotta stop ranting.. Look at the stats!



# It's Just the beginning

- Industry data points to significant increase in the prevalence and criticality of client-side vulnerabilities
- A "shift" towards finding vulnerabilities in client-side software is occurring (SANS and Symantec security threat reports)
- 8 out of 20 categories in SANS Top 20 report relate directly to client-side vulnerabilities
- High profile incidents taking advantage of vulnerabilities in client-side software
- Feb 09 Adobe oday
- Feb 09 MS09-002 via .doc
- Chinese malware drive-by iframe autopwn sites

# Some Stats

**From Websense security Labs™: State of Internet Security, Q3 – Q4, 2008:**

Top 10 Web Attack Vectors in 2nd Half of 2008:

1. **Browser vulnerabilities**
2. **Rogue antivirus/social engineering**
3. SQL injection
4. **Malicious Web 2.0 components (e.g. Facebook apps, third-party widgets and gadgets, banner ads)**
5. **Adobe Flash vulnerabilities**
6. DNS Cache Poisoning and DNS Zone file hijacking
7. **ActiveX vulnerabilities**
8. **RealPlayer vulnerabilities**
9. **Apple QuickTime vulnerabilities**
10. **Adobe Acrobat Reader PDF vulnerabilities**

[http://securitylabs.websense.com/content/Assets/WSL\\_ReportQ3Q4FNL.PDF](http://securitylabs.websense.com/content/Assets/WSL_ReportQ3Q4FNL.PDF)

No more Stats, Let's talk how to!

# How to steal a company

---

# #1 YOU GOTTA HAVE STYLE

**External Direct**

Server / App Attack

**External Indirect**

Client Side / Phishing / Phone Calls

**Internal Indirect**

Key/CD Drops / Propaganda

**Internal Direct**

Social / Electronic / Physical / Blended

**Exotic Attacks**

# Process

Figure Out What  
the Company  
Thinks is Important



Steal it !





# The METHOD

**THE METHOD:** Take the EASY way in.

Gather Intelligence



Scan for Vulnerabilities



Plan Attack



Exploitation and Execution



Dig for the GOLD!

# Gathering Electronic Intel

© 2006 United States Electronic Intelligence





# DIDN'T YOU WATCH GATES?

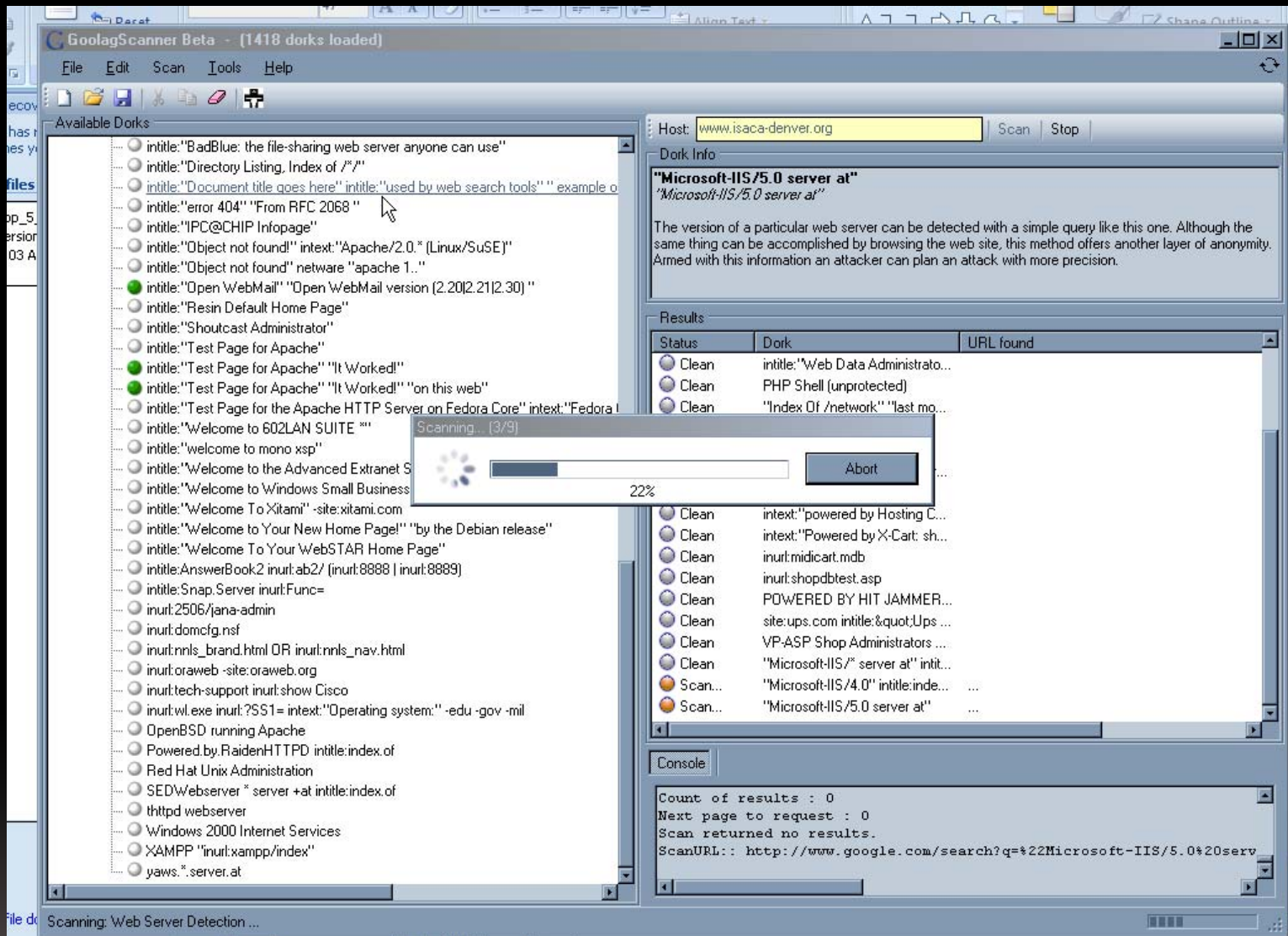


# Offsite Information Gathering



# Stuff To Find

- Email Addresses
- Server Addresses
- Websites
- Business names
- Partners
- Physical Address
- Phone Numbers
- Documents
- BluePrints
- Maps
- Local Utilities
- Service Companies
- DNS
- Banners
- Ports
- Vulnerabilities
- Net Block
- AS Name
- Employee Info
- Social Network Information Leakage



# GOOLAG

Finding Information for fun and Profit:  
The new google for analysts and hackers alike.

- Clez.net (External Profiling)
- CentralOps.net (Network Profiling)
- Robtex (Server profiling)
- Touchgraph (Show business relationships and links)
- ServerSniff (Get Tons of webserver specific info and verification)
- Netcraft ( usage info)
- DomainTools (Domain info)
- MySpace / Friendster / Twitter (know ya enemy)
- And SOOOOO many more

The Twitter logo, featuring the word "twitter" in a light blue, rounded, lowercase font.The ZoomInfo logo, featuring a sunburst icon to the left of the text "zoominfo" in orange and blue, with the tagline "find people and companies" below it.The Spock BETA logo, featuring the word "spock" in orange and "BETA" in blue below it.The Flickr logo, featuring the word "flickr" in blue and pink.The Plaxo logo, featuring a blue circular icon with a white "P" and the word "plaxo" in black.The Zabasearch logo, featuring the word "ZABASEARCH" in a bold, blue, uppercase font.The Myspace.com logo, featuring a blue icon of two people and the text "myspace.com" in white, with the tagline "a place for friends" below it.The Google logo, featuring the word "Google" in its multi-colored font.The LinkedIn logo, featuring the word "LinkedIn" in white on a blue background.

TouchGraph Navigator - Senate 110.xls

File Settings Edit View Tools Help

Settings Connected Components:  All  Single  Degrees of Separation

Zoom:  Spacing:

**Senator**

id: 0000167  
 name: Barack Obama  
 sex: male  
 state: IL  
 party: Democrat  
 born: Thu Aug 03 1961  
 religion: United Church of Christ  
 webpage: http://obama.senate.gov/  
 Bill #: 383

Senator Bill Relation Senator Co-oc

Group By: state Search

state / Senator	state	party	Bill #	Senator #
DE				2
MA				2
NM				2
OR				2
IL				2
Durbin	IL	Democrat	537	
Obama	IL	Democrat	383	
WA				2
KY				2
MN				2
OH				2
GA				2
LA				2
VA				2
SC				2

powered by TouchGraph

TOUCHGRAPH FOR INTERWEBS:  
 TOUCHGRAPH FOR FACEBOOK  
<http://www.youtube.com/watch?v=YOsbWWvWdjA>

NOT!

**Social Networks Are yer Frnd!**

---

## Philippe Bogaerts <sup>1st</sup>

Senior Field Systems Engineer F5 Networks /  
co-organizer **BruCON** (<http://www.brucon.org>)

Namur Area, Belgium | Internet



Philippe Bogaerts back at work @F5 Networks and shifting gear to BruCON a big success !!! 1 month ago

- Current**
- Senior Field Systems Engineer at F5 Networks
  - Co-organizing BRUCON at Brucon
  - Founder, consultant and trainer at RADARSEC SECURITY SERVICES

- Past**
- International Technical Manager at BeeWare
  - Technical Manager at Risc Technology Belgium
  - Trainer / Team Leader at Telindus High-Tech Institute

[see all...](#)

- Education**
- Groep T - Leuven Hogeschool
  - Koninklijke School voor Onderofficieren
  - K.A.T

**Recommendations** 14 people have recommended Philippe

**Connections** 421 connections

- Websites**
- My Website
  - My Company
  - My Blog

**Public Profile** <http://www.linkedin.com/in/xxradar>

## Benny Ketelslegers <sup>2nd</sup>

IT Security Officer at Retail Belgium

Belgium | Information Technology and Services

- Current**
- IT Security Officer at Retail Belgium

- Past**
- Information Security Consultant at Asure
  - Network & Security Engineer/Team Leader at VanGenechten Packaging
  - Network Design Engineer at Proximus

[see all...](#)

- Education**
- Centrum voor Levende Talen
  - Solvay Business School (ISC<sup>2</sup>)

[see all...](#)

14 people have recommended Benny

9 connections

<http://www.linkedin.com/in/bketelslegers>



## Filip Waeytens <sup>1st</sup>

Co-Founder / Boardmember at **Brucon** VZW

Gent Area, Belgium | Computer & Network Security

- Current**
- Co-Founder / Boardmember at Brucon VZW
  - Senior Technical Consultant Applications Security at Telindus Belgacom ICT
  - team-member at Remote-Exploit

- Past**
- IT/Network Security Specialist at Belgacom
  - IT security Manager at Esselte
  - Senior Security Engineer at Scanit

[see all...](#)

- Education**
- Coloma
  - HEMACO

**Recommendations** 19 people have recommended Filip

**Connections** 171 connections

- Websites**
- Remote Exploit
  - My Website







# Linked IN Anyone?



# FACEBOOK

**View Guest List**

Attending **Maybe** Declined Not Yet Responded

	<b>Sonia Auger</b>	<a href="#">Add as Friend</a>
	<b>B-art Degroote</b>	<a href="#">Add as Friend</a>
	<b>Filip Verlaeckt</b>	<a href="#">Add as Friend</a>
	<b>Roger Sels</b> Belgium	<a href="#">Add as Friend</a>
	<b>Philippe Bogaerts</b> F5 Networks	<a href="#">Add as Friend</a>
	<b>Brice Mees</b> Belgium	<a href="#">Add as Friend</a>

[Close](#)

**Events**

**Web Results**

**Brucon**  
What sta...  
do a Bru...  
blog.bru...

**Brucon**  
Want to...  
stickers as a bonus. Here is another sample of the Hex Challenge ...  
blog.brucon.org/?widgetType...

**Brucon (brucon) on Twitter**  
Belgian Security Conference ... Hey there! brucon is using Twitter. Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent ...  
twitter.com/brucon

Results by Bing [View All Web Results](#)

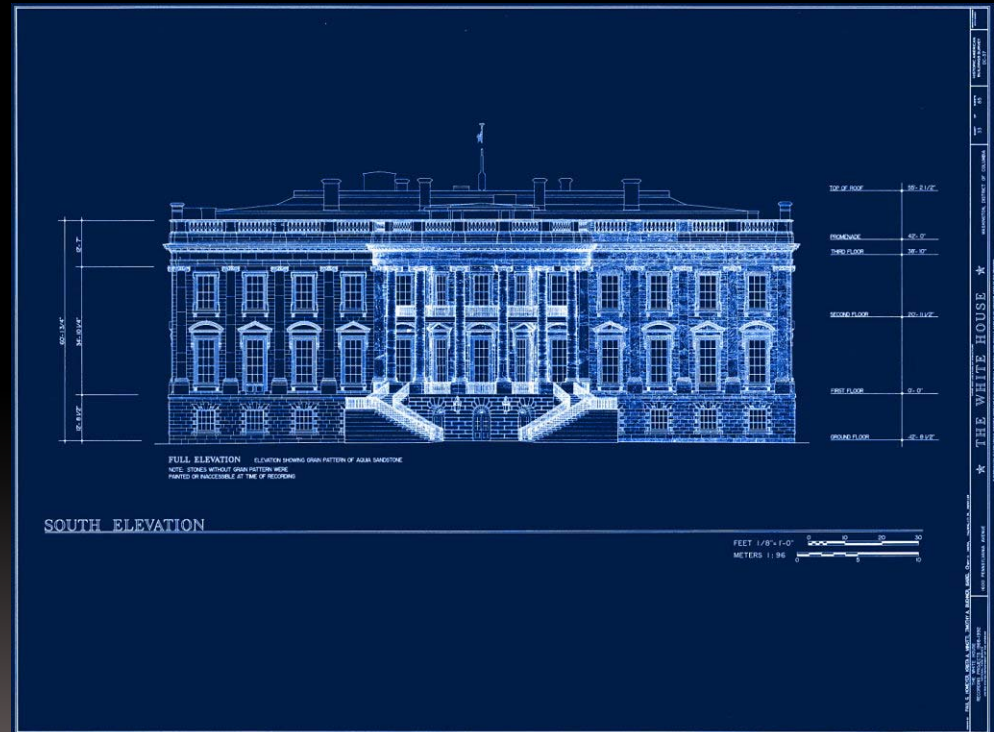
# Gathering Physical Intel Onsite



# Perimeter Assessment

What do you see when you are walking up to the target?

- Cameras?
- Door locks?
- What vendors do they use?
- What do their uniforms look like?
- Hours of business?
- Security guards?
- Gates?
- Uniforms?
- Smoking area?
- Parking lot?
- How do they communicate?



# TOOLBAG for onsite work

- Costumes
- ID Cards
- Paperwork
- Lock Picks
- Laptop
- Bag
- Phones ( to leave behind)
- Leave behinds
- Biz Cards
- Candy
- Smokes
- A lighter
- A CAMERA or Video Recorder
- A Giant set of B@LL\$
- Mylar Balloons
- A Blow Up Doll (not just for breaks on the job)
- String/Twine
- Helium
- Cell Jammer
- Appropriate Cables
- Lineman's set
- Something to record audio
- Grappling hook and rope

# Costuming

- Goodwill is the best costume department ever



I'm sorry, I don't speak your language!





# Remote Observation



# Facility Recon and Remote Resource Copying





# Badge Cloning

# Dumpster Diving

- An extremely useful source of information.
- Most companies don't shred
- Tells you about customers, employees, vendors, products, and distributors.

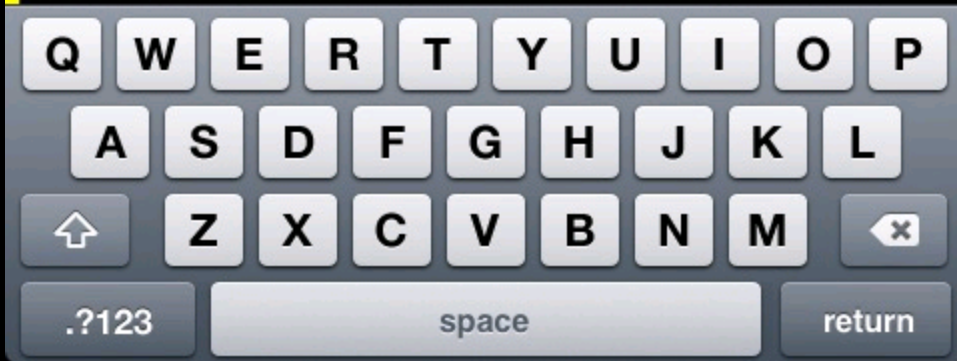


# Parking Lot Shopping



... AT&T 7:49 PM

```
iate stager for over-sized stage... (89 bytes)
[*] Sending stage (2834 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (81931 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (192.168.2.108:4444 -> 192.168.2.113:1039)
```



Brooke 2:55 PM

## Who Are You?

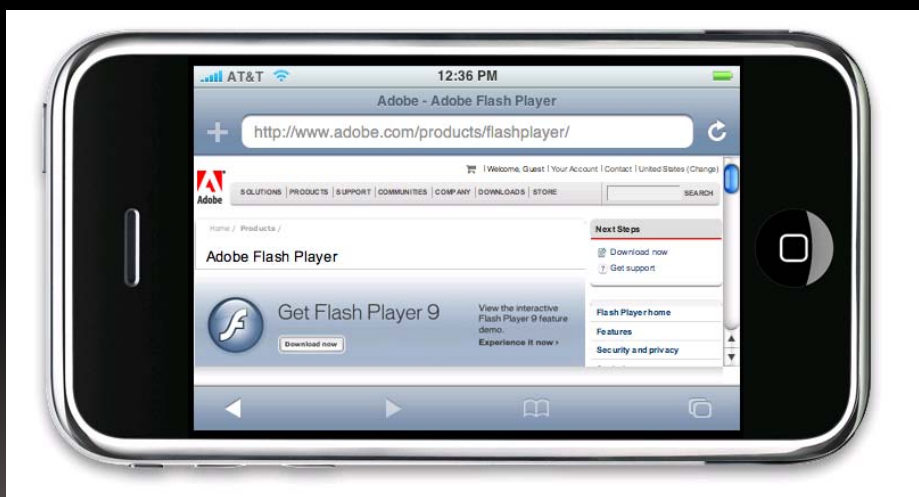
Not all of the packages available via Cydia are designed to be used by all users. Please categorize yourself so that Cydia can apply helpful filters.

This choice can be changed from "Settings" under the "Manage" tab.

User (Graphical Only)

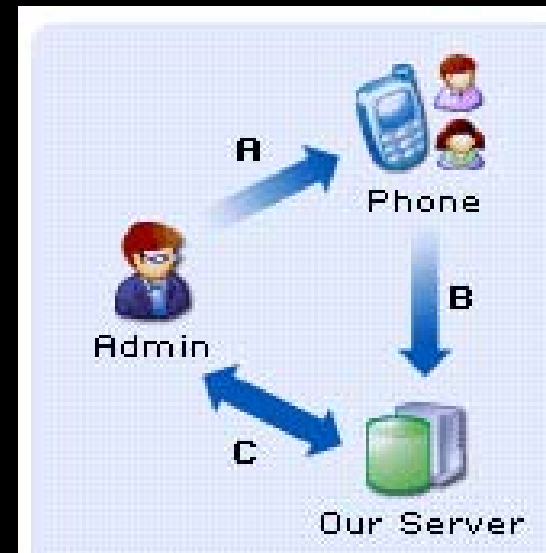
Hacker (Command Line)

Developer (No Filters)



iPWN

<b>NEW FLEXISPY - PRO - X</b>			<b>FLEXISPY - PRO</b>		
<b>PRO-X</b>	<a href="#">FULL DETAILS</a>	<a href="#">Supported Phones</a>	<b>PRO</b>	<a href="#">FULL DETAILS</a>	<a href="#">Supported Phones</a>
<b>TOP OF THE RANGE SPYPHONE</b>			<b>MID RANGE SPYPHONE</b>		
<ul style="list-style-type: none"> <li>Listen to actual phone calls</li> <li>Use as a secret mobile gps tracker</li> <li>Includes all PRO features</li> <li>Change phones as often as you like</li> <li>For <a href="#">Symbian</a> and <a href="#">Windows Mobile</a></li> </ul>			<ul style="list-style-type: none"> <li>Spyphone to bug a room or person</li> <li>Read their SMS, EMAIL and Call Logs</li> <li>BUY NOW for Instant Download</li> <li>Change phones as often as you like</li> <li><a href="#">Symbian</a>, <a href="#">Windows</a> and <a href="#">Blackberry</a></li> </ul>		
<b>ORDER NOW: €250</b> (per year) <a href="#">Convert this currency to USD</a>			<b>ORDER NOW: €150</b> (per year) <a href="#">Convert this currency to USD</a>		
<a href="#">LEARN ABOUT SPYPHONE FEATURES HERE</a>			<a href="#">ALL YOUR QUESTIONS ANSWERED HERE</a>		
<a href="#">Buy Now</a>			<a href="#">Buy Now</a>		
<b>FLEXISPY - LIGHT</b>			<b>FLEXISPY - BUG</b>		
<b>LIGHT</b>	<a href="#">FULL DETAILS</a>	<a href="#">Supported Phones</a>	<b>BUG</b>	<a href="#">FULL DETAILS</a>	<a href="#">Supported Phones</a>
<b>BASIC SPY PHONE</b>			<b>PHONE BUG</b>		
<ul style="list-style-type: none"> <li>Read their SMS, EMAIL and Call Logs</li> <li>BUY NOW for Instant Download</li> <li><a href="#">Symbian</a>, <a href="#">Windows Mobile</a>, <a href="#">Blackberry</a></li> </ul>			<ul style="list-style-type: none"> <li>Spyphone to bug a room or person</li> <li>Remote Listening Only</li> <li>SIM Change SMS Notification</li> </ul>		
<b>ORDER NOW: €100</b> (per year) <a href="#">Convert this currency to USD</a>			<b>ORDER NOW: €100</b> (one time) <a href="#">Convert this currency to USD</a>		
<a href="#">Buy Now</a>			<a href="#">Buy Now</a>		

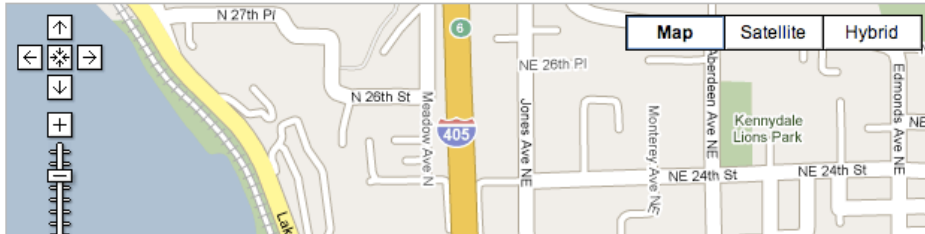


# Cell phone Bugging

## Features

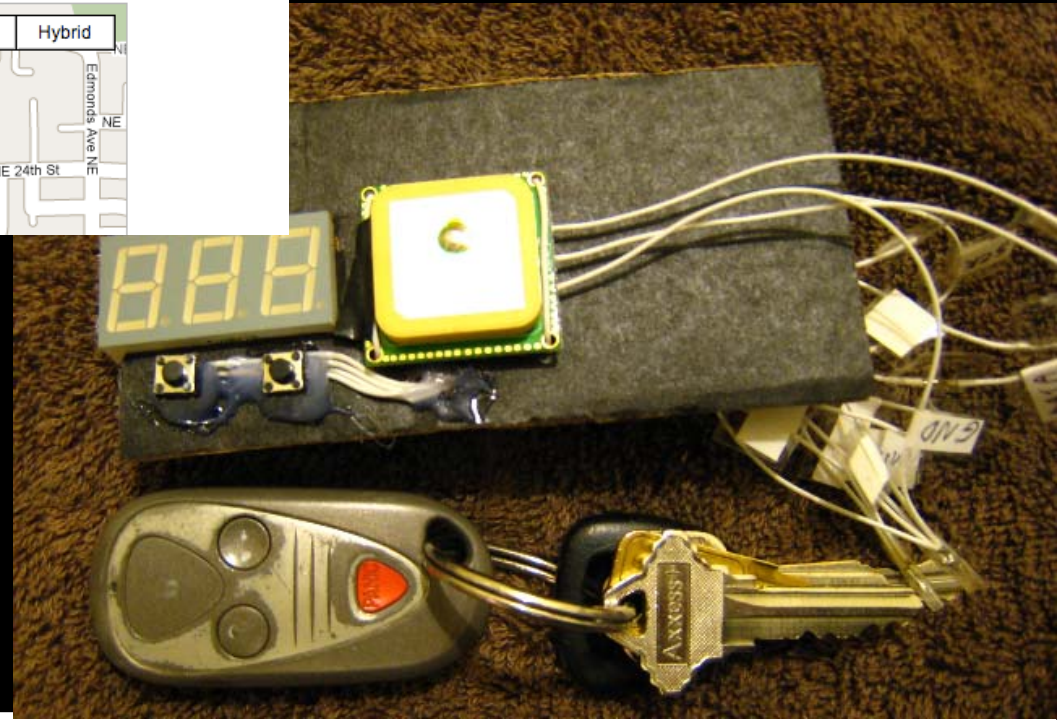
### True real-time tracking

With InstaMapper, the object you track is [a moving dot on a map](#). Positions are updated as often as every 5 seconds.



[www.opengpstracker.com](http://www.opengpstracker.com)

[www.instamapper.com](http://www.instamapper.com)



# Cell phone tracking

# Scanning for vulnerabilities



# If you hack a person, they are harder to reboot!

- Manipulations points
- Interests
- Habits
- Leverage areas
- Points of similarity
- Date Specific events (social events, etc)
- Ability to manipulate
- Old OS/Server Types
- Vulnerable Apps
- Vulnerable Services
- 3rd Party app usage
- Free Sensitive Data
- Templates
- Stuff to Copy (Corporate Communication Tone/Look/Feel)



Plan your attack

# Get ready, Get Set...

- Time and Date
- Character
- Costume
- Methods
- Memorizing Data
- Entrance Strategy
- Exit Strategy
- Plan B (and C,D,E,F,G....)

This is not a good example of how you should get there.



failblog.org

**COVERT FAIL**

# Making Copies

- The power of observation is not always as it seems



# Magic of a copy center...

- Like Disneyland only for Social Engineering
- Everything you need to forge anything is in here
- Lamination
- Color copier
- Cardstock
- Cutters
- Color Printer
- Photoshop



# Badge Forgery

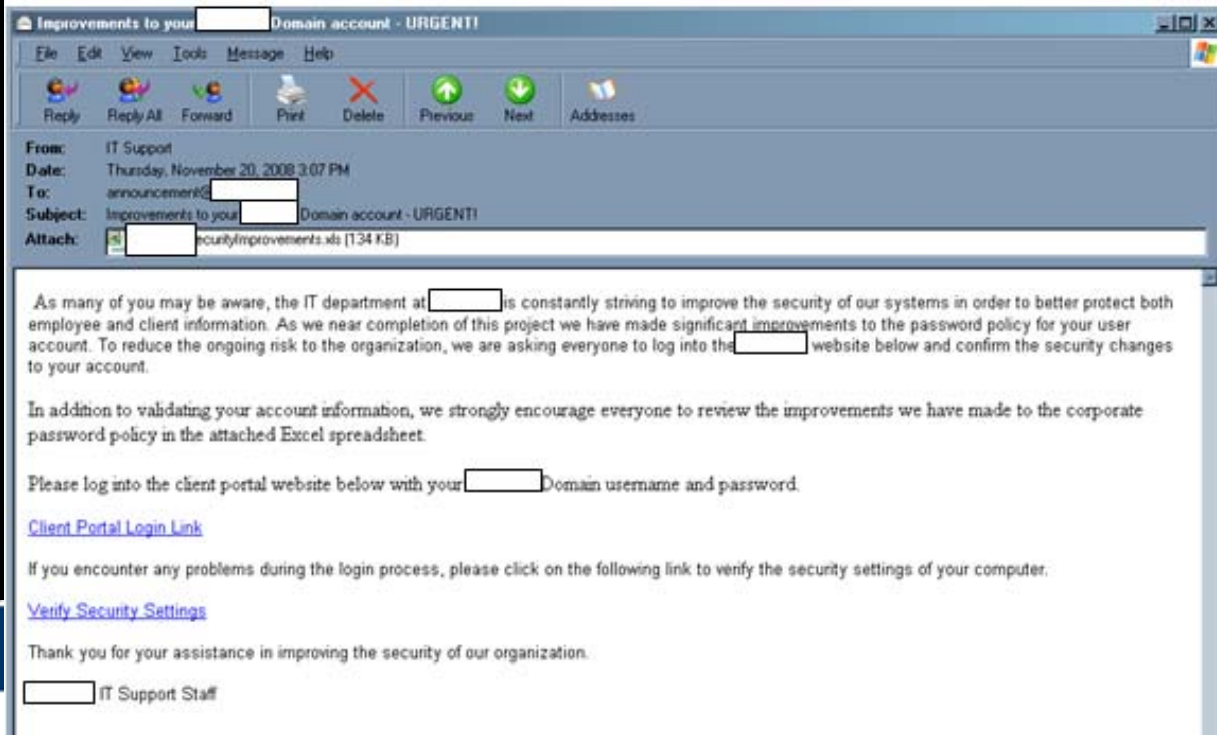
- RFID
- Digital camera pictures
- Color copier
- ..and also, don't scan your badge and put it up on flickr, I will find it....



Execute



# Phishing



Sign On

To access your Account...  
Login to the Client Website

Username:

Password:

Login

Forgot your password?  
Having trouble logging in?

This site has been optimized for Internet Explorer 5.5 or Netscape 7.0. The latest versions of these browsers can be downloaded free from Microsoft and Netscape if you have any questions or need assistance upgrading your browser, please contact your client service representative.

[Privacy Policy](#) | [Terms & Conditions](#)

To protect the privacy of your portfolio information, [redacted] is committed to using advanced technology, both on our corporate computer by using firewalls and by encrypting all data. We ask you to help in this process by keeping your password private and by maintaining the security of your personal computer so that others cannot access your financial information. Please note, however, that Internet security technology is continually refined and enhanced.

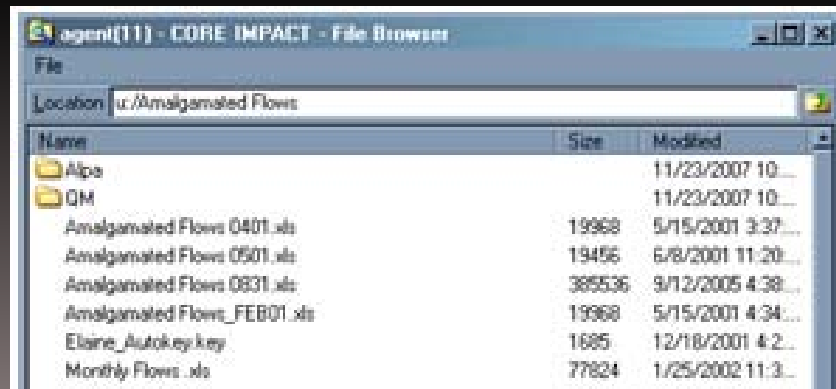
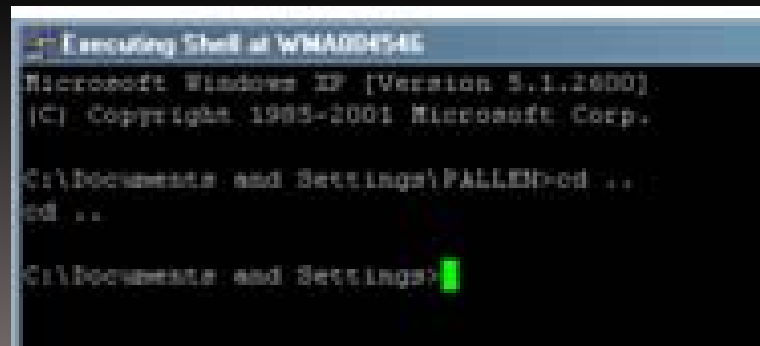
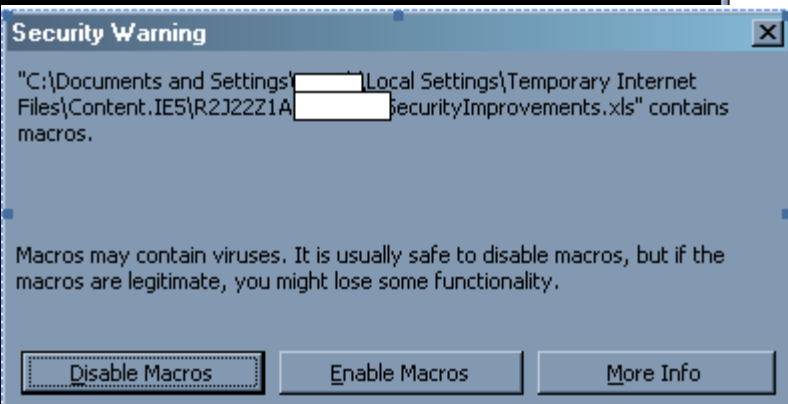
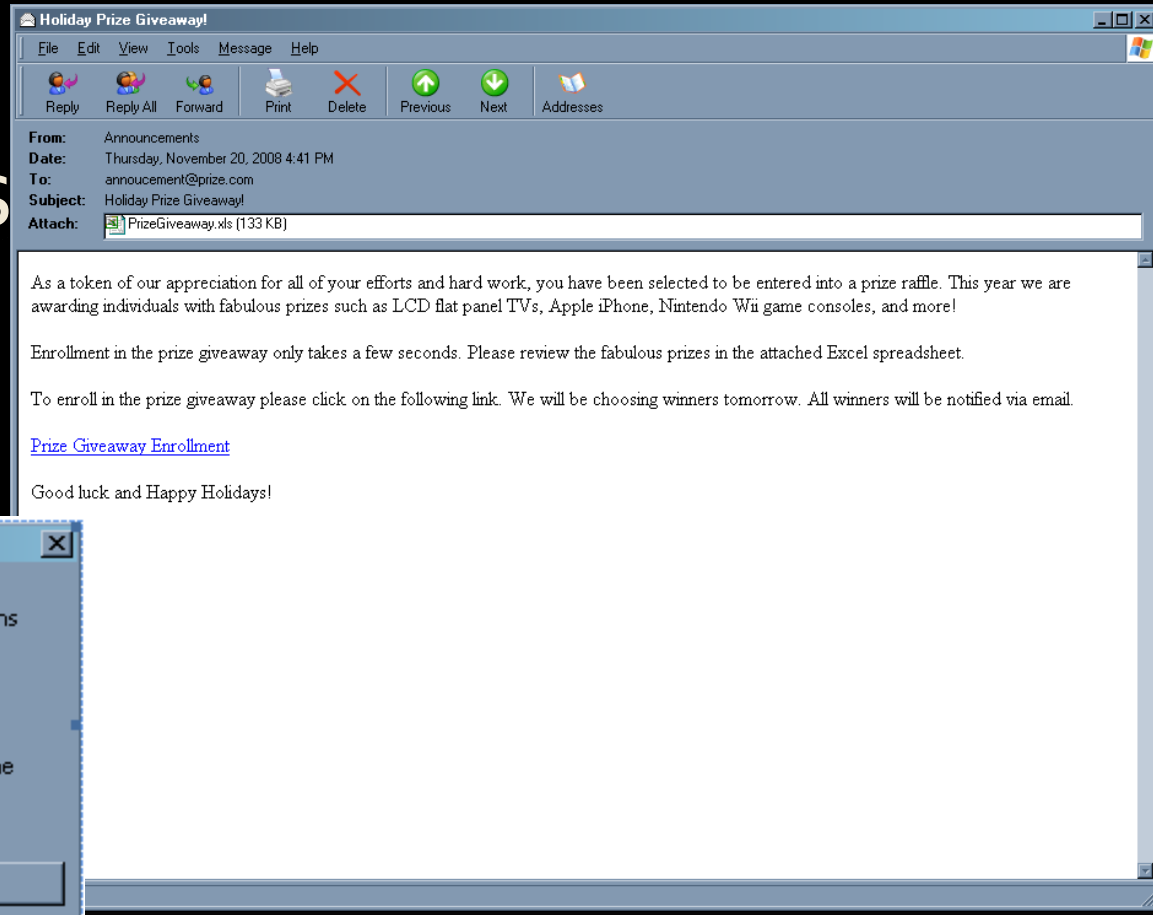
Use of this Web site involves the electronic transmission of encrypted portfolio information. Using this site is consent to such transmission of this information; such consent is in effect at all times when using this site.

Copyright © 2003 [redacted] All Rights Reserved.

- Tax Forms
- Health / Benefits Change
- Corporate Parties
- Holiday events
- IT Department
- Manager / Authority Figures
- Discounts
- Travel / Product Deals



# Client Side Attacks



# Phone a Friend



## THE PHONE CALL

An interactive forum theater play where **YOU** determine the outcome!



# RIST

*remote intelligence and surveillance technology*

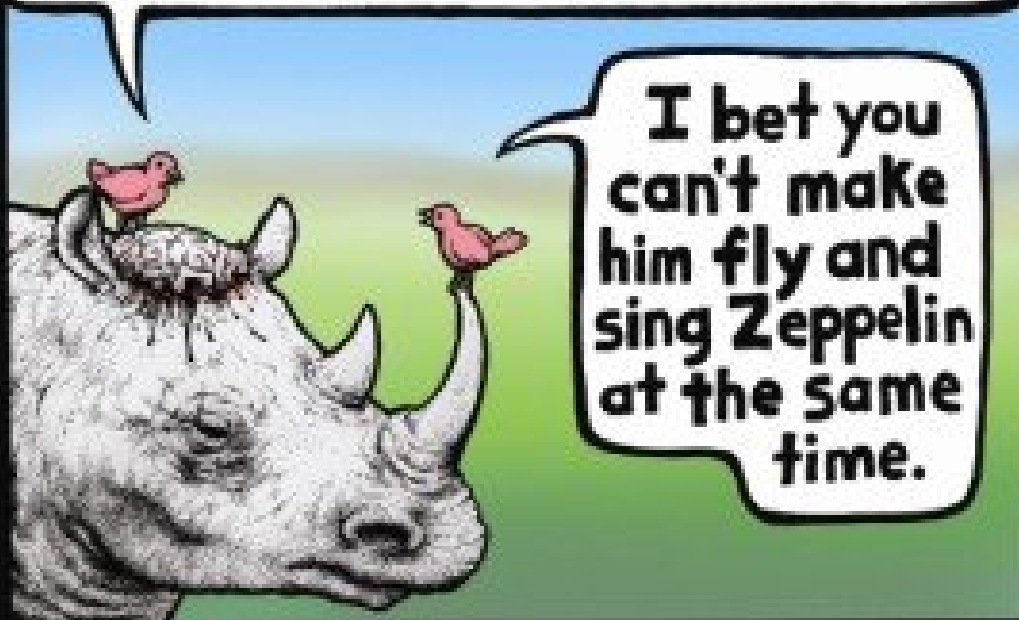
Don't pick up every little bit of trash you find and think it's your's.

- CDs
- USB Keys
- Flyers
- Promo Items



# In Person

**By incessantly pecking this rhino's head, I've broken through to the brain. By manipulating the surface, I can make him do anything I want.**



**I bet you can't make him fly and sing Zeppelin at the same time.**

- NLP
- Breathing Techniques
- Touch
- Psychosomatic Presence
- Magic
- Hypnotism
- Ekman Coding
- Facial Feedback
- Temperature Reading
- Communication Stances
- Satir Comm. Models
- Classic Con's

# Please don't call it SE unless it's ENGINEERED

**KEVIN MITNICK**

BRAND



**WARNING:**

Not for use in corporate settings.  
Use of this product may cause  
unexpected results on your network,  
social engineering , and other undesired  
activity. Use with caution.

Serving Size ..... 1 can  
Calories ..... 1337  
Calories from BS .... 250%

Percentages based on  
8 hour work day

**INGREDIENTS**

31337 sauce, elb juice, extract of  
p0wn, lametree fruit concentrate,  
high fructose corn syrup, caffiene

**ENERGY DRINK**

**For 31337 energy all day long!**

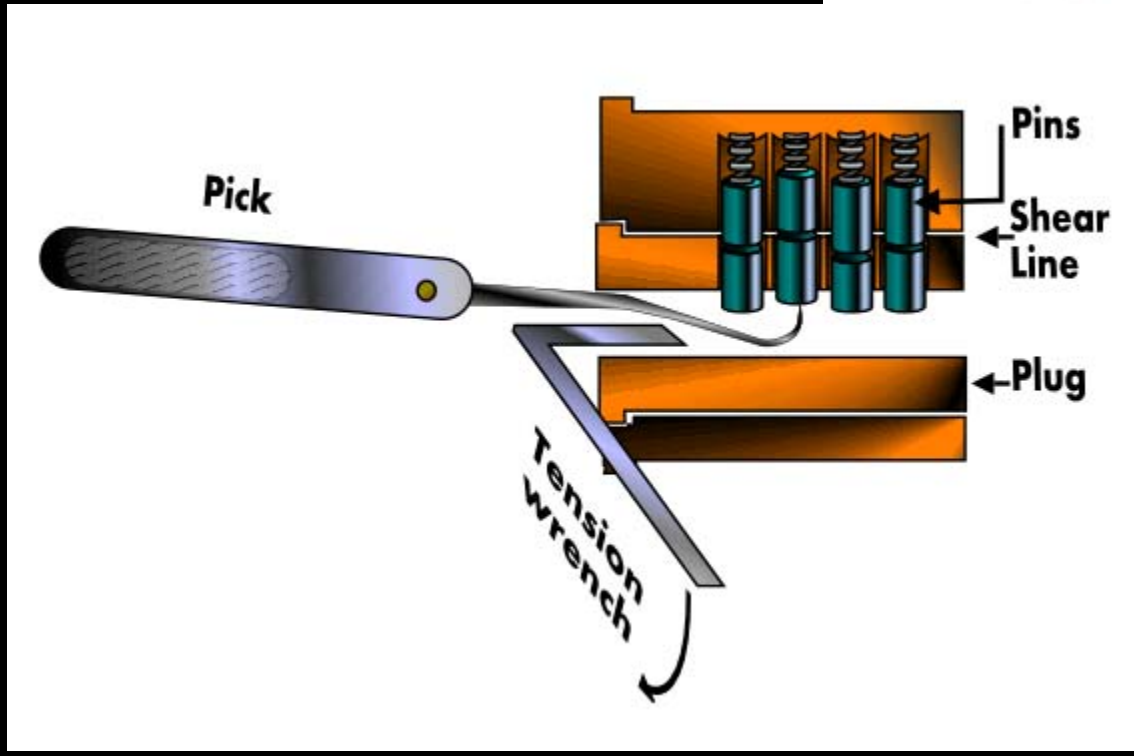
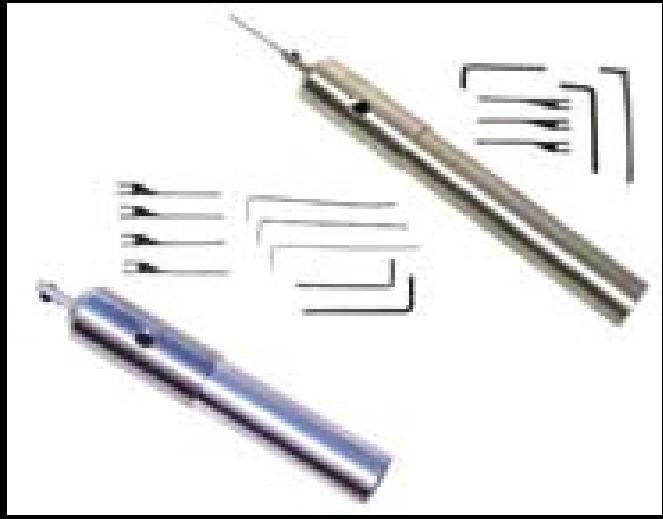
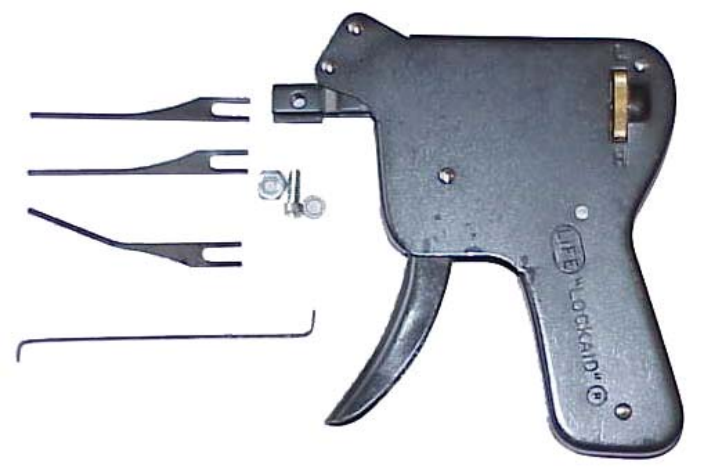
A pack of smokes and a lighter will get you  
anywhere...

Smoking areas are one of the most insecure  
places

Offer a smoke, you just made a new friend  
BS with them about their day, they may start  
telling you unexpected secrets

They may even hold the  
door for you





# Lock Picking



Go for the Gold  
Or Start over!



Reservations	In Europe:
Guest Services	00800 228 0
Meeting/Event Services	
Hertz discount number	Hertz or visit <a href="http://www.hertz.com">www.hertz.com</a>

If you are unable to reach our Elite Guest Services numbers listed below, please use the toll-free numbers:

U.S./Canada: 801-468-4000  
 Brazil: 55 11 3069 2307  
 Latin America: 52 55 110 221 21  
 Europe, UK and Middle East: 44 (0) 20 7012 7312

(60) 3 2688 8080  
 Australia: 61 2 950 86492  
 Hong Kong: 852 2346 5279  
 China: 86 21 340 9618  
 Japan: 81 3 405 1513  
 India: 91 142 877

Earn rewards at Marriott Hotels & Resorts, JW Marriott Hotels & Resorts, Courtyard by Marriott, Fairfield Inn by Marriott, TownePlace Suites by Marriott and Marriott Vacations Worldwide International.

Photo on front: Robert Rodriguez

5/9/06

801-468-4000  
 55 11 3069 2307  
 52 55 110 221 21  
 44 (0) 20 7012 7312  
 61 2 950 86492  
 852 2346 5279  
 86 21 340 9618  
 81 3 405 1513  
 91 142 877





TO ACCESS THE CONSOLE  
PRESS SCROLL LOCK 2X

USER NAME: USER  
NO PASSWORD





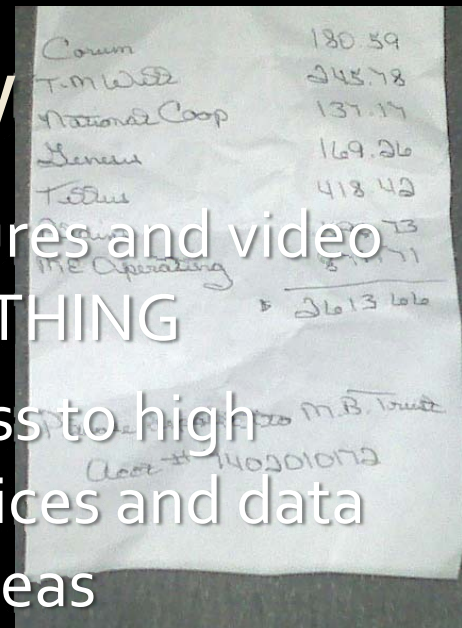
# How to Find Sensitive Data

- Look in the good Spots
  - Connected Ports/Services
  - TNS/SQL Listeners
  - NFS Mounts
  - Shared Drives
  - MY Docs
  - Home Directory
  - /FINANCE
  - Search is your friend
  - Portal
  - Windows Temp
  - IE/FF Cookie Dir
  - Bookmarks
  - Stored PW's
  - History
  - ERP Systems

# Use What YOU Know

- Exploit
- Review and Record Paper documentation
- Check out all network traffic

- Take Pictures and video of EVERYTHING
- Gain access to high profile offices and data storage areas



Think like the Business NOT Like a hacker!

# The SEXY way

- Automated Tools
  - Spyder (Thanks Cornell)
  - Vericept
  - Any other DLP Solution
  - Power Shell Search
  - Nessus
  - GREP (make regex then.. `grep -cEHilrs -f patterns /directory/to/search`)
  - [dbDataFinder](#)
  - FileHunter
  - PowerGREP
  - WindowsGREP



---

**Questions?.....**  
**Concerns?.....**  
**Comments?.....**  
**Time to RUN?**