

The IED defense

Using improvised cyber-weapons
against system intruders

R.Pompon

My goal is to change your thinking about defense:
Stop being passive,
Put yourself in the attacker's shoes,
and then mess with their heads.

DISCLAIMER

- ▶ The opinions expressed in this talk are my own personal opinions and do not represent HCL in any way.
- ▶ Some of the techniques shown today may or may not be present in some form on HCL systems.

What is the problem?

Blind hacker baffles FBI

<http://www.wired.com/politics/law/news/200...>



SHARE THIS

After a succession of hoaxed phone calls detailing both murders and hostage crises, A US federal Joint Terrorism Task Force eventually uncovered a nasty 'hacking' technique known as 'swatting,' which was quickly spreading across the United States.

One example of this type of call came in the shape of a supposed suicidal gunman threatening:

"I will shoot, I'm not afraid. I will shoot, and then I will kill myself, because I don't care."

After over an hour of searching the suspected location, no gunman was found, nor any suspects, but just a baffled family, who had absolutely no idea of what was going on. After much investigation the task force located that the swatting calls were coming from a computer user in Colorado. The 17-year-old East Boston kid is known as "Li'l Hacker," but Lil'Hacker has one difference from most other hackers; he is blind from birth.

RUSSIAN COMPUTER HACKER SENTENCED TO THREE YEARS IN PRISON

John McKay, United States Attorney for the Western District of Washington, and Charles E. Mandigo, Special Agent in Charge, Seattle Division, Federal Bureau of Investigation, announced today that Chief United States District Judge John C. Coughenour has sentenced VASILY GORSHKOV, age 27, of Chelyabinsk, Russia, to serve 36 months in prison for his convictions at trial last year on 20

Our servers get popped
Cops are pretty much helpless to stop it
Even when they finally catch someone, it's a wrist slap
Nothing to do but pray your defenses hold

Deception

Improvised Electronic Deception



Let's look at a military counter intelligence response
Operation Fortitude, Ali's rope-a-dope, exploding dye packs

Booby trap your network with deception
We're talking more than honey pots (tho a good start)
You want to draw enemy fire
Deceive, confuse and harass attackers
Waste their resources - be an asshole

This is not a new idea



theScamBaiter     

Fighting Scammers Worldwide for Fun and Justice

ScamBaiting - (Scam Baiting) involves tricking internet scammers into believing you are a potential victim

Below is only 1 of the many videos that Scammers make for us

AnusLaptops.com Commercial ★★★★★



- Cliff Stoll - and the SDI bait
- Fred Cohen - Practical work
- Neil Rowe - Academic analysis
- Scambaiters - hilarious example of messing with people
- MarkMonitor and their "dilution" techniques

In fact

Red Teaming Experiments with Deception Technologies

Fred Cohen, Irwin Marin, Jeanne Sappington, Corbin Stewart, and Eric Thomas*
Draft of November 12, 2001

- Fred Cohen: Fred Cohen & Associates, University of New Haven, Sandia National Laboratories
- Irwin Marin: The Emblematics Corporation
- Jeanne Sappington: The Emblematics Corporation
- Corbin Stewart: Sandia National Laboratories
- Eric Thomas: Sandia National Laboratories

This research was sponsored by the United States Department of Defense under MIPR1CDOEJG102 2112040 162-3825
P633D06 255X 633006.247.01.DD.00 JGBZZ.1 JOAN 1JG8CA

Analysis

The first and perhaps most important thing to notice in the summary of results is that when deception is enabled, attackers never get as far toward the truth as they do when deception is disabled. In other words, deception works. Furthermore, it works very well. When deception is turned on, attackers almost uniformly go down the deception parts of the attack graphs rather than down the real parts of the attack graph. In cases other than blatant dazzlement, they are convinced that they are going down real paths for a substantial time. In some cases, attackers were so convinced that they had won when they were actually deceived, that they declared victory and walked away early. In some dazzlement cases, people got so frustrated that they gave up early. These results verify the previous anecdotal data from the Honeynet project [6] and Deception ToolKit [7].

PROVEN TO WORK

- Actually proven effective for short periods of time
- Quote from Fred Cohen's Red Team tests

In fact

Red Teaming Experiments with Deception Technologies

Fred Cohen, Irwin Marin, Jeanne Sappington, Corbin Stewart, and Eric Thomas*
Draft of November 12, 2001

- Fred Cohen: Fred Cohen & Associates, University of New Haven, Sandia National Laboratories
- Irwin Marin: The Emblematics Corporation
- Jeanne Sappington: The Emblematics Corporation
- Corbin Stewart: Sandia National Laboratories
- Eric Thomas: Sandia National Laboratories

This research was sponsored by the United States Department of Defense under MIPR1CDOEJG102 2112040 162-3825
P633D06 255X 633006.247.01.DD.00 JGBZZ.1 JOAN 1JG8CA

Analysis

“In other words, deception works. Furthermore, it works very well.”

The first and perhaps most important thing to notice in the summary of results is that when deception is enabled, attackers never get as far toward the truth as they do when deception is disabled. **In other words, deception works. Furthermore, it works very well.** When deception is turned on, attackers almost uniformly go down the deception parts of the attack graphs rather than down the real parts of the attack graph. In cases other than blatant dazzlement, they are convinced that they are going down real paths for a substantial time. In some cases, attackers were so convinced that they had won when they were actually deceived, that they declared victory and walked away early. In some dazzlement cases, people got so frustrated that they gave up early. These results verify the previous anecdotal data from the Honeynet project [6] and Deception ToolKit [7].

PROVEN TO WORK

- Actually proven effective for short periods of time
- Quote from Fred Cohen's Red Team tests

But wait, you say?



INTERNATIONAL
STANDARD

**ISO/IEC
17799**

Second edition
2005-06-15



Security
Standards CouncilTM

<http://iedtalk.com>

Why is this not more prevalent? Why can't you get funding?
Complaints: Ops and IT get confused by the deception
Deception is useless for audits
Legal risk - blowback - liability?
Your boss "You wasted time on this?"
Deception is hard when there are a lot of information channels

Use it anyway



<http://iedtalk.com>

Okay, we can't count on it for assurance
Which means you won't get funding - you need to DIY
Deception is passive so legal risk is minimal
Maybe if it was used more, it would be acceptable in audit

Anatomy of an attack

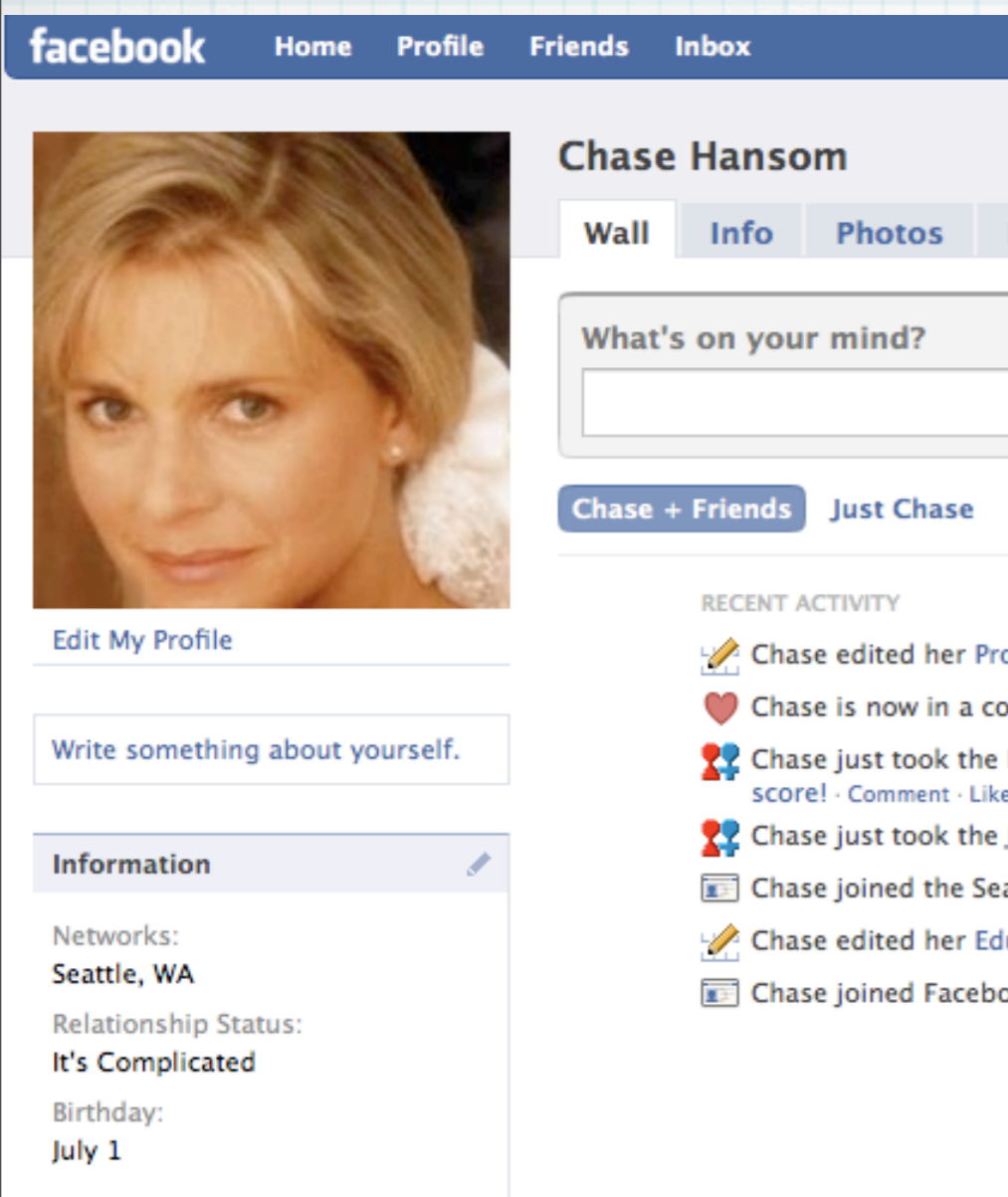
1. Passive recon
2. Active recon
3. Initial compromise / Beachhead
4. Elevation and invasion
5. Theft and extraction

<http://iedtalk.com>

Lets follow a typical attack
Watch improvised deception defenses
Key is the I in IED - each deception must be unique
Try to learn something while doing it

Passive recon

“Entice the tiger to leave it’s mountain lair”



facebook Home Profile Friends Inbox

Chase Hansom

Wall Info Photos

What's on your mind?

Chase + Friends Just Chase

RECENT ACTIVITY

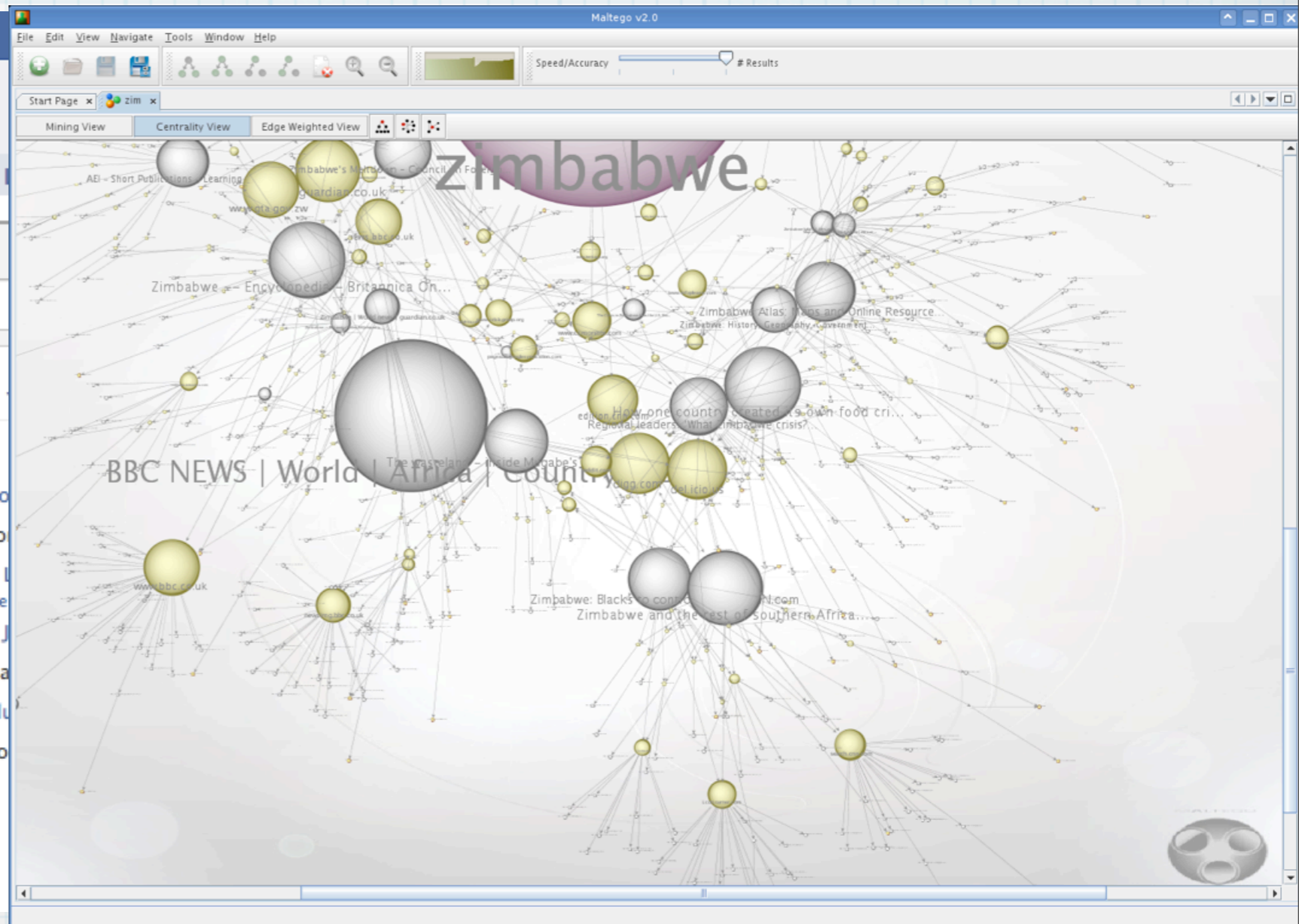
- Chase edited her Profile
- Chase is now in a couple
- Chase just took the IQ score! · Comment · Like
- Chase just took the IQ
- Chase joined the Sea
- Chase edited her Edu
- Chase joined Facebo

Information

Networks:
Seattle, WA

Relationship Status:
It's Complicated

Birthday:
July 1



<http://iedtalk.com>

Run Maltego against yourself, then add something for it to find
Create social network bait to give you early warning for attack campaigns
Use fake names and have the email come back to you "out of band"
Forum/mail-list "help" posts with
- fake diagrams, IPs that point to your honeypots
Remember - Improvise! (free)

Active recon

“Pretend inferiority and encourage his arrogance.”

```
$sudo nc -k -l 80 > web.txt
```

```
# robots.txt  
User-agent: *  
Disallow: /admin/  
Disallow: /cgi-bin/  
Disallow: /login.html
```



<http://iedtalk.com>

Fake DNS entries that go to honeypots, tripwires, traps
The old unplugged wifi - waste their time
Spider-loops on websites - redirects that sent web scrapers in circles
robots.txt with fake admin pages
Hidden passwords in HTML comments that don't work

Initial compromise / Beachhead

“Borrow a corpse to resurrect a soul”

LaBrea - The Tarpit

LaBrea is a program that creates a tarpit or, as some have called it, a "sticky honeypot". LaBrea takes over unused IP addresses on a network and creates "virtual machines" that answer to connection attempts.



The screenshot shows the Outlook Web Access login interface. It features a Microsoft logo in the top right corner. The main heading is "Microsoft Office Outlook Web Access" with the subtext "Provided by Microsoft Exchange Server 2003". On the left side, there is a large, stylized graphic of a key. The login form includes two input fields: "Domain\user name:" and "Password:". To the right of the password field is a "Log On" button. Below the login fields is a "Security" section with two radio button options: "Public or shared computer" (which is selected) and "Private computer". A red warning message is displayed below the "Private computer" option, stating: "Warning: By selecting this option you acknowledge that the computer complies with your organization's security policy." At the bottom of the page, there is a disclaimer: "To protect your account from unauthorized access, Outlook Web Access automatically closes its connection to your mailbox after a period of inactivity. If your session ends, refresh your browser, and then log on again."

<http://iedtalk.com>

Tarpits, Fake proxies & dead ends
Put fake sites up on your perimeter
Repurpose old hardware w/booting Linux CD/DVDs
Fake websites with logins - log what they attempt
Why not make OWA lookalike? See which accounts have been stolen.
REMEMBER - Use out of band communication
Honeypots at the DMZ

Elevation and invasion

“Inflict injury on one’s self to win an enemy’s trust”



Oracle Database 10g Express Edition

Free to develop, deploy, and distribute

Oracle Database 10g Express Edition (Oracle Database XE) is an entry-level, small-footprint database based on the Oracle Database 10g Release 2 code base that's free to develop, deploy, and distribute; fast to download; and simple to administer. Oracle Database XE is a great starter database for:

<http://iedtalk.com>

On the inside - have a few fake IP ranges that are alarmed
Put decoys near the critical server to distract
How about a decoy database server?
Strategic use of honey pots
Default route on DMZ boxes that point to Honeypots

Theft and extraction

“Let the enemy’s own spy sow discord in the enemy camp”

Name	Birth	Death	Last Residence	Last Benefit	SSN	Issued
MARY HOFFMAN	03 Dec 1883	Feb 1976	02360 (Plymouth, Plymouth, MA)	(none specified)	001-01-2177	New Hampshire
MAURICE HOFFMAN	01 Mar 1902	Jan 1974	98122 (Seattle, King, WA)	(none specified)	001-01-2638	New Hampshire
MARION HOFFMAN	06 Jul 1916	Feb 1968	03103 (Manchester, Hillsborough, NH)	(none specified)	001-03-6184	New Hampshire
EDWARD L HOFFMAN	14 Jul 1916	20 Nov 1990	(not specified)	(none specified)	001-09-2765	New Hampshire
LOUIS HOFFMAN	17 Jan 1875	Nov 1965	(New Hampshire)	(none specified)	001-09-2798	New Hampshire
WILLIAM C HOFFMAN	25 Feb 1918	23 Oct 2005 (V)	06042 (PE)	(none specified)	001-09-3819	New Hampshire

Mastercard

5401760969923823
 5300460008932529
 5377886486724954
 526352453257 5198
 5101979844612855
 5403827460035130
 5247945492510142
 5274367114117725
 51 55525089005209
 5501072124391600

VISA 16 digit

4556696675770981
 4813343504210173
 4996822841975415
 4539452554334685
 4 556272269092933
 4916932077333861
 4716708717901495
 4024007128366035
 4449249 489722276
 4929175014412183

VISA 13 digit

4539520870257
 4182833088117
 4556253330366
 4904298597310
 4532754167821

American Express

344653559563755
 343596788996547
 372543008464322
 347969229997794
 374 126380681537

<http://iedtalk.com>

Zip bombs for bad guys to download and examine
 Honeyfiles - the network equivalent of a dye pack
 Provide them PANs that already marked for fraud
 Use the Top 10 most wanted SSNs
 This also works great for catching insiders

Judo

“One of the most startling effects is that teams suffer from self-deception. For example, the two teams that were not being deceived believed that they were being deceived at various times and acted on those self-deceptions.”

<http://iedtalk.com>

In the end, use their strength against them
Advanced deception - the old honey pot double fake out
Use reverse psychology
Lots of bad Honeypots
Honeypot detectors - examine how they work
Make the real thing will look like honeypot
Some malware will detect VMs and try to avoid forensic environments.
Can you fake a VM to throw them off?

Remember

“All warfare is based on deception.”

- ▶ **Part of your defense in depth**
- ▶ **DIY or die**
- ▶ **Think dirty**
- ▶ **Offer the unexpected**
- ▶ **Work out of band**

<http://iedtalk.com>



www.planetheidi.com

Heidi, Geek Girl Detective, says "Paranoia is my lifestyle. And it should be yours too."