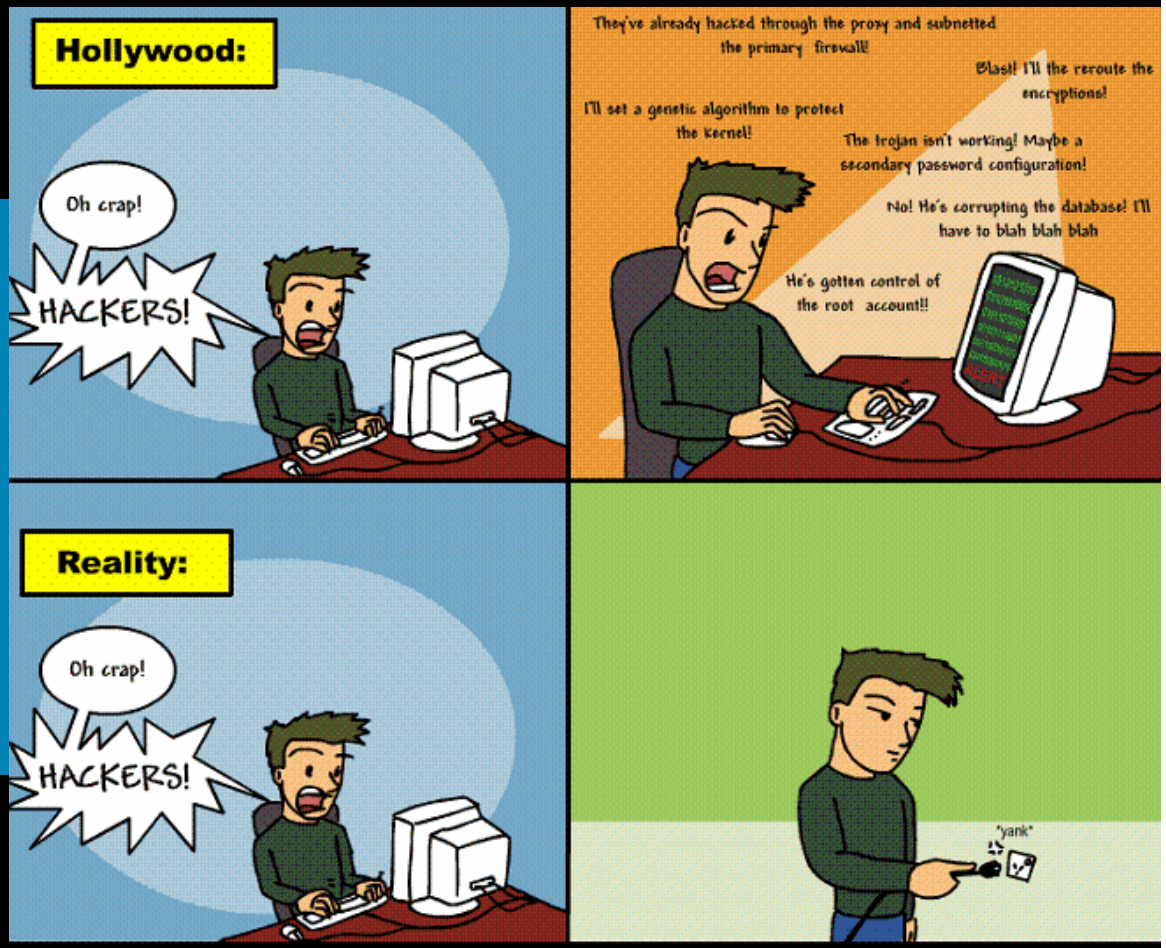
# Life of Ivica Ostojić

**security consultant engineer CEE region**

## *"Gone In 60 Seconds"*





**Goran Peteh**


**Dubrovnik, 20. ožujak 2008.**

# Warning – Disclaimer - Upozorenje

**Neither Cisco or the presentor encourages the use of any methods and/or tools mentioned within this presentation without the expresses aproval and signed agreement with the owner of the IT infrastructure in question.**

**The unathorised usage of the aforementioned tools and/or methods could lead to legal prosecution and severe penalties.**

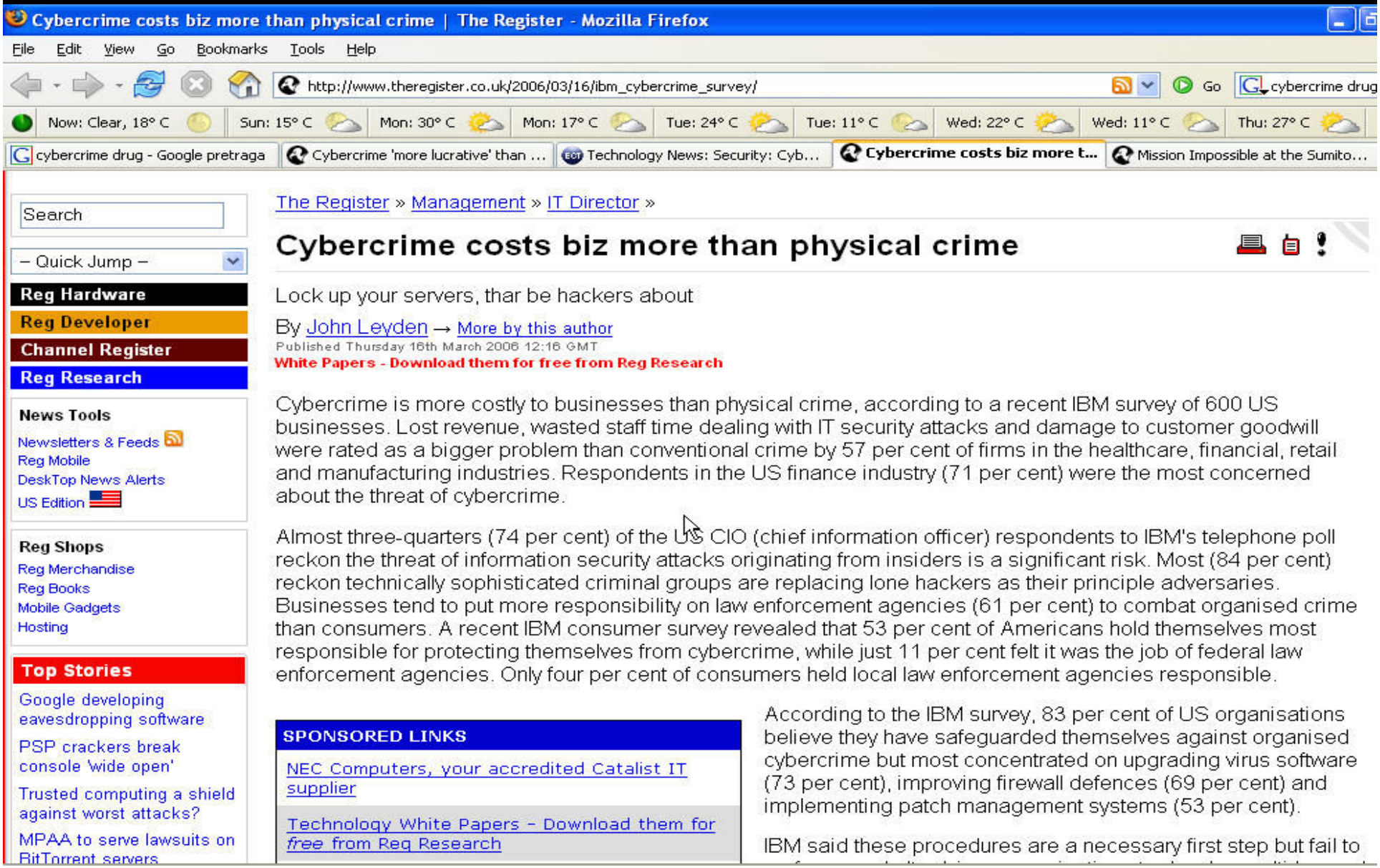
# First – words of wizdom

# SUN TZU

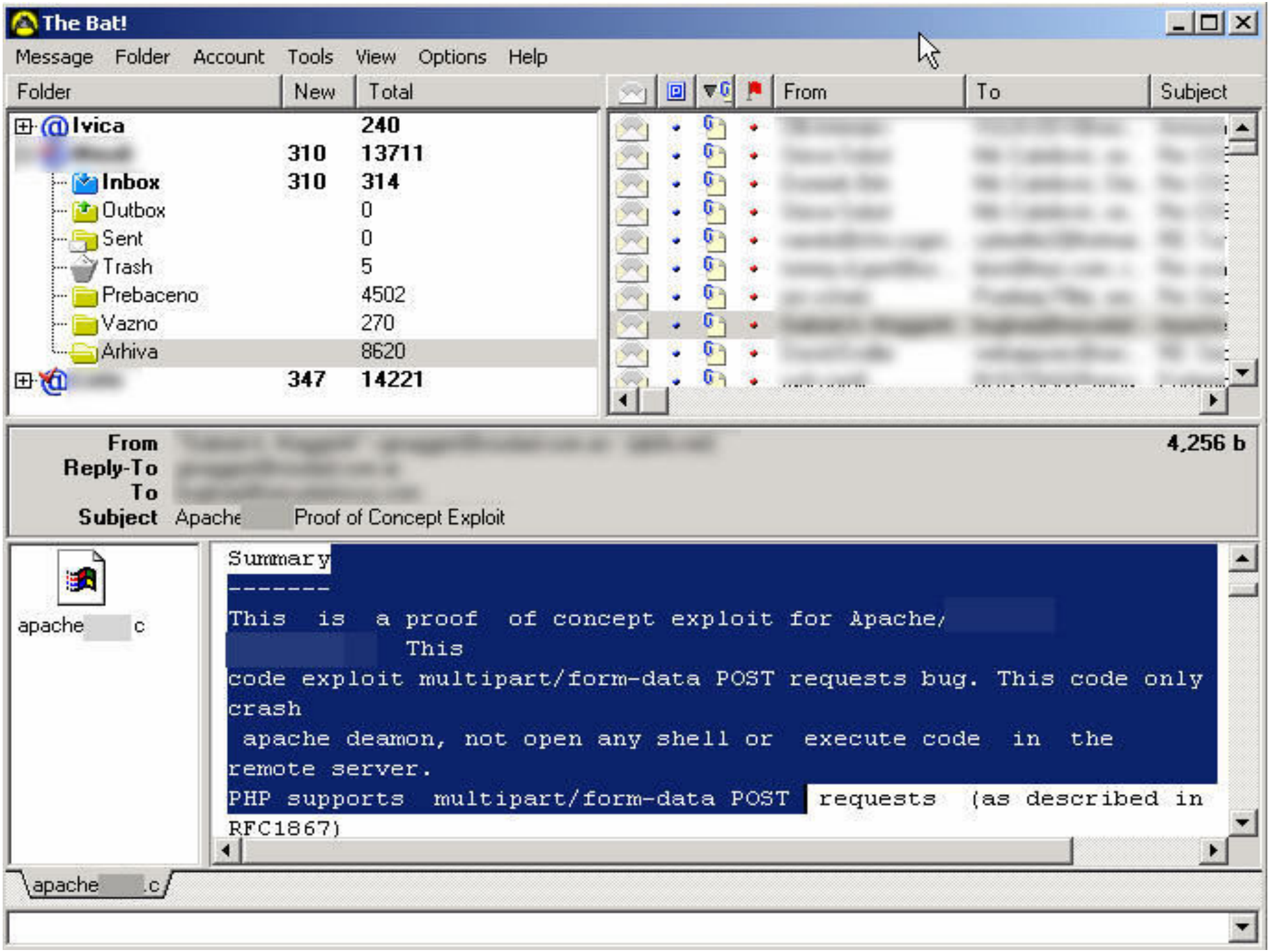
## THE ART OF WAR

**If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.**

# New way of doing business?



# COUPLE FACTS FROM THE REAL LIFE


The Bat!
Message Folder Account Tools View Options Help
Folder New Total
Ivica 240
310 13711
Inbox 310 314
Outbox 0
Sent 0
Trash 5
Prebaceno 4502
Vazno 270
Arhiva 8620
347 14221
From To Subject
From
Reply-To
To
Subject Apache Proof of Concept Exploit
4,256 b
apache c
Summary
-------
This is a proof of concept exploit for Apache/
This
code exploit multipart/form-data POST requests bug. This code only
crash
apache deamon, not open any shell or execute code in the
remote server.
PHP supports multipart/form-data POST requests (as described in
RFC1867)
apache .c

# DARK MARKET – MYTH OR FACT?

UK Logins

## various usa logs

09-14-2006, 03:06 PM #1

**Drax** Offline
Verified Vendor (BANK LOGIN)
DM Reviewer
Canadian Moderator
Donator

Join Date: Jul 2006
Posts: 118

**various usa logs**

i have various amounts of usa logs, only login/pass.

banks such as [redacted] etc..

pm me if u need anythin

IP:

QUOTE

I have 3 accs with 10k+ . 11k, 50k, 220k. buy all for 750gbp or each for 300gbp

also have many accs with 1k - 20gbp each acc

QUOTE

19 - Personal - 1 200 - 10GBP
20 - Personal - 5 000 - 125GBP
21 - Personal - 6 000 - 135GBP
22 - Business - 2 700 - 50GBP
23 - Personal - 9 000 - SOLD
24 - Personal - 5 500 - 130GBP
25 - Personal - 2 700 - 40GBP

# AND IF YOU THINK THAT IS BAD CHECK THIS OUT...

http://www.forbes.com/home/security/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html

SnagIt

Search Web

Mail

My Yaho

Attackers turn Bank of India ...

Hotmail hack punts person in ...

Hackers prowl for Trend Micr...

Zone-H.c

Security

# America's Hackable Backbone

Andy Greenberg, 08.22.07, 6:00 PM ET

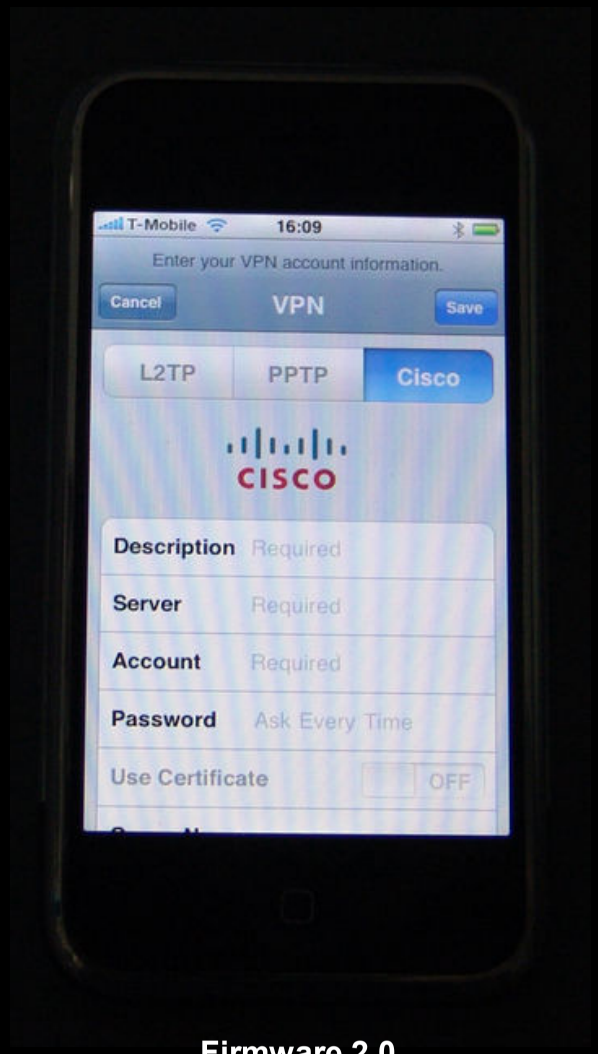
In Pictures: America's Hackable Backbone

The first time Scott Lunsford offered to hack into a nuclear power station, he was told it would be impossible. There was no way, the plant's owners claimed, that their critical components could be accessed from the Internet. Lunsford, a researcher for **IBM**'s Internet Security Systems, found otherwise.

"It turned out to be one of the easiest penetration tests I'd ever done," he says. "By the first day, we had penetrated the network. Within a week, we were controlling a nuclear power plant. I thought, 'Gosh. This is a big problem.'"

**By This Author**

# And now something different....


**Firmware 2.0**

# metasploit

OFFICIAL BLOG OF THE METASPLOIT PROJECT

TUESDAY, SEPTEMBER 25, 2007

## A root shell in my pocket (and maybe yours)

After the recent price drop and toolchain release, I bit the bullet and bought a shiny new iPhone. The first thing I did is bypass activation, run jailbreak, and install the AppTapp Installer. Using the installer, I added OpenSSH and a VT-100 Terminal to the phone. Once I had shell access, I made a few observations:

1) The processor is actually decent. Compare the iPhone (400Mhz*) with the Nokia n770 (233mhz) or the Nokia n800 (320Mhz) and the choice of a handheld hacking device is a no-brainer. The (mostly) working toolchain, large amounts of storage (8Gb), and ease of use make this a great candidate for almost any security researcher "on-the-go". If you tweak the networking preferences file, you can set the signal quality limit down to "1", turning the "join a WiFi network" screen into a primitive stumbler (or just install Stumbler via AppTapp).

* The media widely reported the processor speed as 620Mhz and I repeated it here. Dan Moniz suggested I check the output of ioreg for the actual CPU speed, which is reported as 400Mhz (0084d717 == 0x17d78400 == 400000000).

BLOGS

Halvar Flake
Matasano Chargen
nCircle Team
Arbor Networks
Technocrat
RISE Security

PREVIOUS POSTS

An easier way to create payload modules in 3.0
The Pwnie Awards: Winners Announced!
Black Hat USA: Tactical Exploitation
The Pwnie Awards: Nominate your favorites today!
April Codings Bring May Pwnings
HeapLib support added to Metasploit 3
Exploiting the ANI vulnerability on Vista

# The Metasploit Project

Metasploit provides useful information to people who perform penetration testing, IDS signature development, and exploit research. This project was created to provide information on exploit techniques and to create a useful resource for exploit developers and security professionals. The tools and information on this site are provided for legal security research and testing purposes only. Metasploit is a community project managed by Metasploit LLC.

**Tactical Exploitation Course**

Metasploit is partnering with Offensive Computing's Valsmith and the SANS Institute to offer an intensive two-day training class on Tactical Exploitation. Registration for this class starts NOW and only a limited number of seats are available. Please see the course description to sign up today!

**The Metasploit Web Site**

Welcome to the new web site of the Metasploit Project. The site was redesigned to focus on the active components of the project. If you run into trouble with the new site please contact us at msfdev[at]metasploit.com.

## Quick Links

- Framework Downloads
- Conference Materials
- Shellcode Generator

## External

- Books on Metasploit
- Blogs about Metasploit
- News about Metasploit

## The Metasploit Blog

Feb-08-2008 - RISE Security vs ASUS Eee PC (hdm)
Jan-28-2008 - METASPLOIT UNLEASHES VERSION 3.1 (hdm)
Oct-23-2007 - Reliable staging without a stager receive loop (skape)
Oct-22-2007 - Cracking the iPhone (part 3) (hdm)
Oct-16-2007 - Cracking the iPhone (part 2.1) (hdm)
Oct-15-2007 - Cracking the iPhone (part 2) (hdm)
Oct-12-2007 - Cracking the iPhone (part 1) (hdm)
Sep-26-2007 - A root shell in my pocket (and maybe yours) (hdm)

## Oct-12-2007 Cracking the iPhone (part 1) (hdm)

In my last post, I described the Apple iPhone in terms of being a security tool and a security target. At the time, I had just finished a first pass on iPhone shellcode. What I didn't realize was that a stock iPhone does not include a /bin/sh executable, nor any of the standard Unix command line tools. My shellcode would only be useful against iPhones which had been updated with the BSD environment package.

A few days later, Apple released the 1.1.1 update. This update removed any installed third-party packages and relocked unlocked phones. Fortunately for the iPhone development community, Apple shipped the iPhone with a vulnerable version of the libtiff library and didn't bother updating it for the 1.1.1 release. This vulnerability has already been used to run homebrew games on the Sony PSP and can be exploited through the MobileSafari web browser. Two of the Toc2rta.com members (Niacin and Dre) put together an impressive exploit for this flaw that jailbreaks the phone directly from the browser. This exploit prepares a gigantic stack frame and returns back to an address within the libSystem shared libary. After a ridiculous amount of chained returns, it manages to rename a file, create a symlink, and remount the root filesystem. A hell of a job, especially considering the state of the iPhone debugging tools.

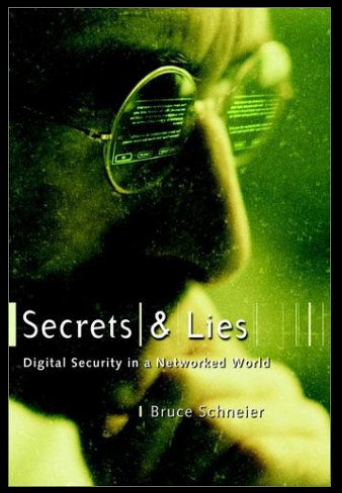
Using a security vulnerability to enable third-party development is nothing new, but in the case of iPhone, this can be a problem. The libtiff flaw can be triggered by both MobileSafari and MobileMail, two applications which are used heavily by many iPhone users. The tricky part is writing an exploit which is reliable and is not limited to calling existing functions within a shared library. One approach is to return to a memcpy() call, another is to find a bounce path through a system library, back to the heap. Technically, a heap fill attack could work as well, but only by using a large tiff file or through the use of javascript in MobileSafari.

The first step to writing a weaponized exploit for this flaw is to obtain a usable debugger. The weasel utility is a great start, but is missing a few useful features, such as memory search and command repetition. I hacked out a new version of weasel (hdm-0.1) tonight that provides a "v" command (dump the virtual memory mappings), a "f" command (search for an ascii or hex string inside process memory), and the ability to attach to a running process. While this code works, it is still ugly as sin, so try not to judge it too harshly (yes, there are scanf overflows in input parsing, no, I don't care). The following example shows the memory search command locating all instances of the word "Hello" in the MobileSafari process.

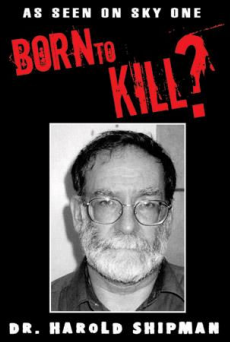
```
# ./weasel -p 259 /Applications/MobileSafari.app/MobileSafari
Read 4 symbols.
[$3008b224 weasel] f 0x0 Hello
009e2168 48 65 6c 6c 6f 3f 27 2c 48 74 6d 6c 55 72 6c 3a
02b2d158 48 65 6c 6c 6f 3f 27 2c 48 74 6d 6c 55 72 6c 3a
3134e113 48 65 6c 6c 6f 00 5f 53 53 4c 50 72 65 70 61 72
3134e179 48 65 6c 6c 6f 44 6f 6e 65 00 5f 53 53 4c 50 72
```

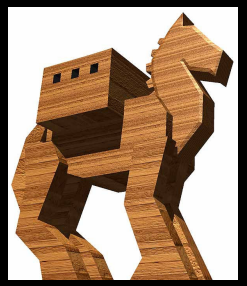
# CONCLUSION

# Secrets & Lies – Bruce Schneier




- Ask the doctor how to poison someone untraceable, and he can tell you (Dr. Harold Shipman).
- Ask someone who works in aircraft maintenance how to drop a 747 out of the sky without getting caught, and he'll know.
- Ask any internet security professional how to take down the Internet, permanently. I've heard about half a dozen different ways,...

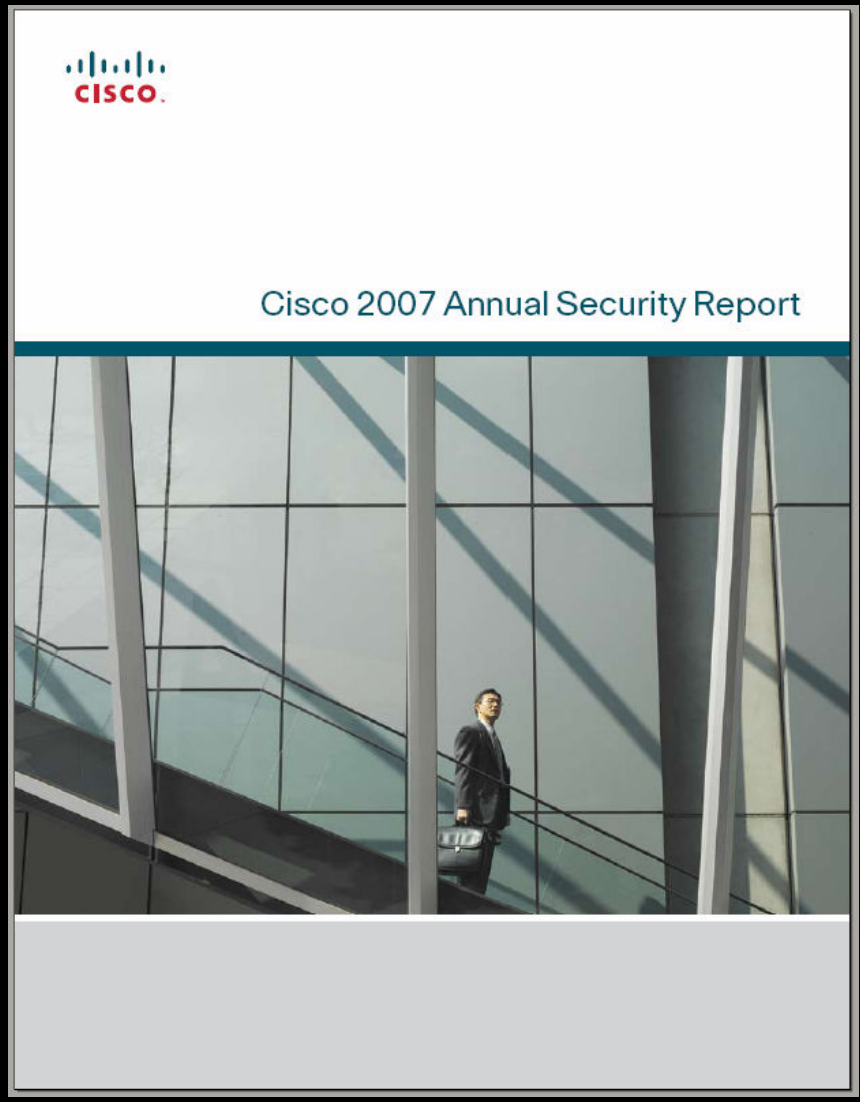



# WHAT ABOUT SOLUTION?

# SDN Solutions

- ASA Family Expansion – New entry and high performance appliances
- Cisco IOS Security Features – Application Inspection
- NAC Appliance – More scalable
- CSA – Simplified management
- New high performance IPS solutions
- MARS, Iron Port, Guard, etc...

*New Solutions for Building Self-Defending Networks*

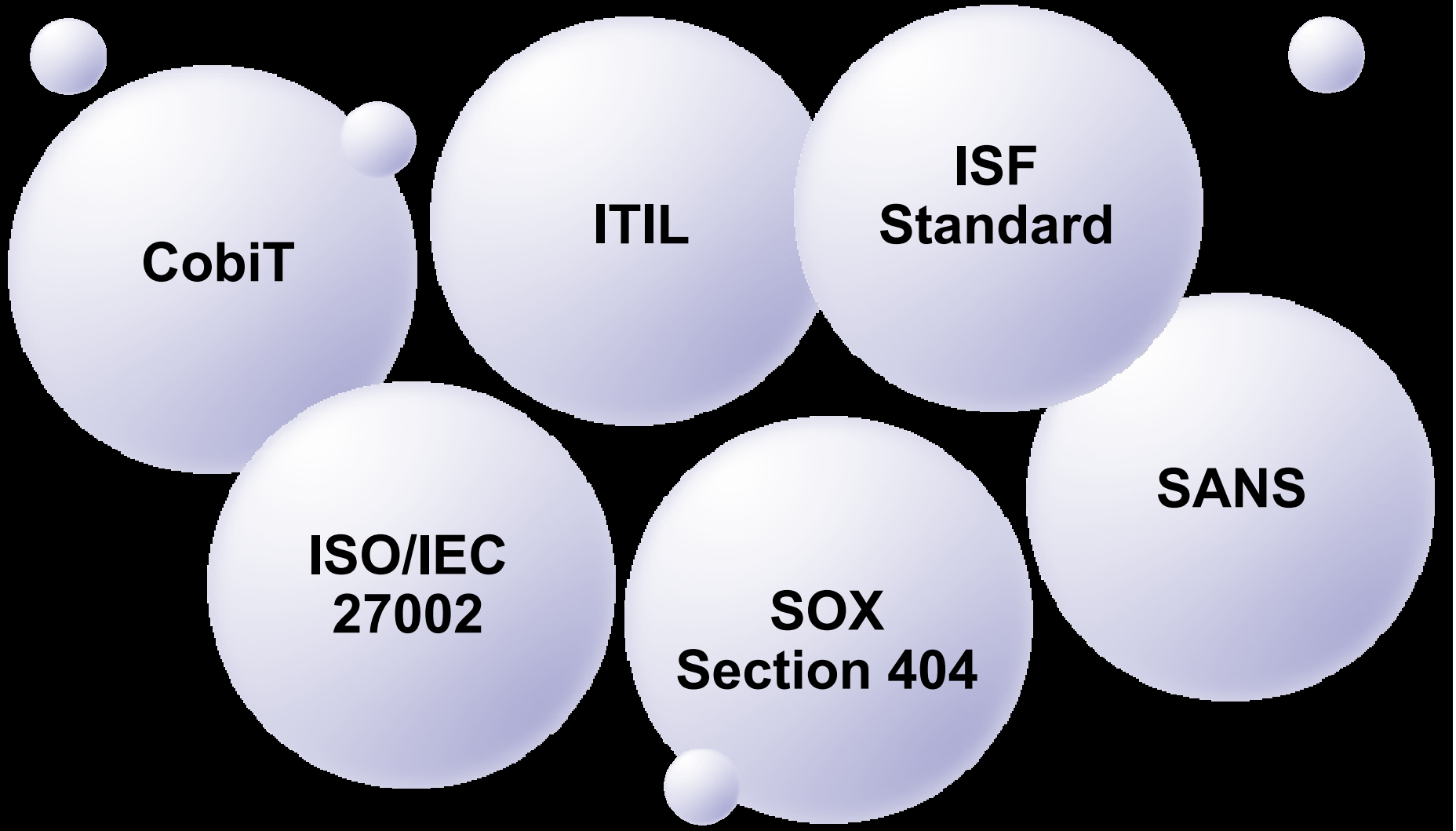



Contents

# Services Offering

- Cisco Security Unified Communications Services
- Security Posture Assessment
- Security Design
- Security Implementation
- Security Technology Planning
- Cisco Security Architecture Review
- Cisco Incident Readiness and Response Services
- Security incident control systems implementation service
- Cisco Security IntelliShield Alert Manager Service
- NAC, MARS, CSA implementation services

# Industry IT Frameworks and Security Best Practices – SDN3



# Education

- elementary school
- high school
- faculty
- government
- ....

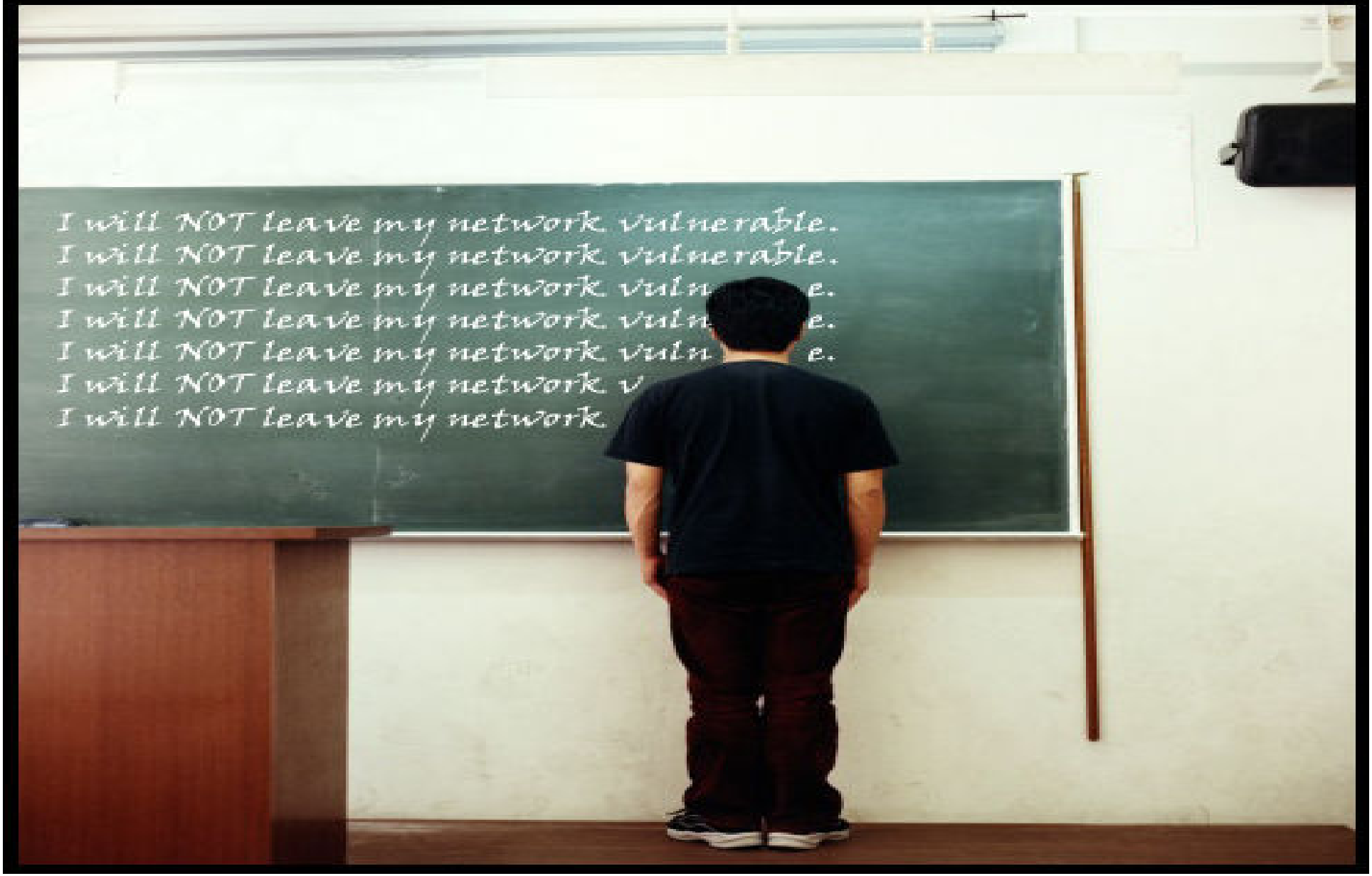
# AND IF NOT!

# CONCLUSION – GINSBERG THEOREM

- You can't win!
- You can't break even!
- You can't even quit the game!

# Ehermans Corollary to Ginsberg's Theorem

# Conclusion...


I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.
I will NOT leave my network vuln e.
I will NOT leave my network vuln e.
I will NOT leave my network vuln e.
I will NOT leave my network v
I will NOT leave my network