



# Days Of Thunder



**MSc. Ivica Ostojic CISSP, CISM**

# **Warning – Disclaimer - Upozorenje**

## **Warning – Disclaimer - Upozorenje**

**Neither Cisco or the presenter 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.**

# **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 wisdom

# 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.**





# **COUPLE FACTS FROM THE REAL LIFE**



- Quick Jump -

**Reg Hardware**

**Reg Developer**

**Channel Register**

**Reg Research**

**News Tools**

[Newsletters & Feeds](#) 

[Reg Mobile](#)

[DeskTop News Alerts](#)

[US Edition](#) 

**Reg Shops**

[Reg Merchandise](#)

[Reg Books](#)

[Mobile Gadgets](#)

[Hosting](#)

**Top Stories**

[Google developing eavesdropping software](#)

[PSP crackers break console 'wide open'](#)

[Trusted computing a shield against worst attacks?](#)

[MPAA to serve lawsuits on BitTorrent servers](#)

[The Register](#) » [Management](#) » [IT Director](#) »

## Cybercrime costs biz more than physical crime



Lock up your servers, thar be hackers about

By [John Leyden](#) → [More by this author](#)

Published Thursday 16th March 2006 12:16 GMT

**White Papers - Download them for free from Reg Research**

Cybercrime is more costly to businesses than physical crime, according to a recent IBM survey of 600 US businesses. Lost revenue, wasted staff time dealing with IT security attacks and damage to customer goodwill were rated as a bigger problem than conventional crime by 57 per cent of firms in the healthcare, financial, retail and manufacturing industries. Respondents in the US finance industry (71 per cent) were the most concerned about the threat of cybercrime.

Almost three-quarters (74 per cent) of the US CIO (chief information officer) respondents to IBM's telephone poll reckon the threat of information security attacks originating from insiders is a significant risk. Most (84 per cent) reckon technically sophisticated criminal groups are replacing lone hackers as their principle adversaries. Businesses tend to put more responsibility on law enforcement agencies (61 per cent) to combat organised crime than consumers. A recent IBM consumer survey revealed that 53 per cent of Americans hold themselves most responsible for protecting themselves from cybercrime, while just 11 per cent felt it was the job of federal law enforcement agencies. Only four per cent of consumers held local law enforcement agencies responsible.

### SPONSORED LINKS

[NEC Computers, your accredited Catalist IT supplier](#)

[Technology White Papers - Download them for free from Reg Research](#)

According to the IBM survey, 83 per cent of US organisations believe they have safeguarded themselves against organised cybercrime but most concentrated on upgrading virus software (73 per cent), improving firewall defences (69 per cent) and implementing patch management systems (53 per cent).

IBM said these procedures are a necessary first step but fail to



# Cybercrime Profits Outpace Drug Trafficking



By Jennifer LeClaire  
TechNewsWorld  
11/29/05 7:43 AM PT

[Print Version](#)  
[E-Mail Article](#)  
[Digg It](#)  
[Reprints](#)

The good news is cybercrimes targeting businesses are at their lowest level ever, according to the Computer Security Institute (CSI). The annual CSI/FBI Computer Crime and Security Survey noted that the average loss per cybercrime incident in 2005 was about US\$250,000.

advertisement

## [Free Security Software](#)

Get the tools you need to stop adware and viruses from these expert resources.

One visit to the Computer Crime and Intellectual Property Section of the U.S. Department of Justice's Web site offers an eye-opening glimpse into the world of cybercrime.

Case after case details how the Feds are cracking down on cyber-criminals, defendants are pleading guilty, and the judged are being sentenced to prison.

## Out of Control

Despite aggressive law enforcement efforts, however, experts say cybercrime is growing at a rampant pace; a pace that rivals drug trafficking.

Cybercrime includes such illegal activities as child pornography, stock manipulation, software piracy, and extortion -- and security experts expect those activities to multiply as [technology](#) becomes more pervasive in developing countries.

"Last year was the first year that proceeds from cyber crime were

Meet  
Google  
Checkout.

[Find out what](#)





**So, who are they?**

# Small introduction to general population

# Small introduction to general population



# Ian Murphy AKA Captain Zap

# Ian Murphy AKA Captain Zap



# Black Hats





## East European gangs in online protection racket

Blackmail by DDoS

By [John Leyden](#)

Published Wednesday 12th November 2003 20:45 GMT

**Security White Papers - Download them free from Reg Research**

Eastern European crime syndicates are using threats of computer hacking to extort pay-offs from UK online businesses.

Organised criminals are using distributed denial of service (DDoS) attacks to force online bookmakers, retailers and payment providers into protection rackets, according to the lead story in today's *Financial Times*. The *FT* reports that the attacks have cost the companies involved "millions of dollars in lost business" and exposed them to extortion.

### SPONSORED LINKS

[Technology White Papers - Download them for free from Reg Research](#)

[Free spyware scan to find out whats lurking on your PC](#)

[NEC Computers, your accredited Catalyst IT supplier](#)

[UK IT recruitment specialists - Jobsite](#)

[At Packman, Webre built to handle](#)

Britain's National Hi-Tech Crime Unit (NHTCU) is investigating a case where one betting firm was brought down by an attack prior to receiving a threat that it would be attacked again "unless tens of thousands of pounds were paid", according to the *FT*. The gang behind the threats are believed to be based in Eastern Europe.

Ian Morris, founder of security integrator Equip Technology, told the *FT* that it



# Researchers hack Wi-Fi driver to breach laptop

One of many flaws found allowed them to take over a laptop by exploiting a bug in an 802.11 wireless driver

By Robert McMillan, IDG News Service  
June 21, 2006

E-mail Printer Friendly Reprints Slashdot It!

Security researchers have found a way to seize control of a laptop computer by manipulating buggy code in the system's wireless device driver.

## Free IT resource

Free White Papers, Trialware and more

Sponsored by Symantec

## Free IT resource

InfoWorld Podcast: Interview with log management expert Dominique Levin.

Sponsored by LogLogic

The hack will be demonstrated at the upcoming Black Hat USA 2006 conference during a presentation by David Maynor, a research engineer with Internet Security Systems and Jon Ellch, a student at the U.S. Naval postgraduate school in Monterey, California.

Device driver hacking is technically challenging, but the field has become more appealing in recent years, thanks in part to new software tools that make it easier for less technically savvy hackers, known as script kiddies, to attack wireless cards, Maynor said in

an interview.

The two researchers used an open-source 802.11 hacking tool called LORCON (Loss of Radio Connectivity) to throw an extremely large number of wireless packets at different wireless cards. Hackers use this technique, called fuzzing, to see if they can cause programs to fail, or perhaps even run unauthorized software when they are bombarded with unexpected data.

Using tools like LORCON, Maynor and Ellch were able to discover many examples of wireless device driver flaws, including one that allowed them to take over a laptop by exploiting a bug in an 802.11 wireless driver. They also examined other networking technologies including Bluetooth, Ev-Do (Evolution-Data Only), and HSDPA (High Speed Downlink Packet Access).

The two researchers declined to disclose the specific details of their attack before the August 2 presentation, but they described it in



Navigation bar and browser interface showing the URL <http://www.praetoriang.net/presentations/blackjack.html>. The interface includes a search bar, weather forecasts for various days, and a list of browser tabs including "Presentation - Bla..." and "BlackBerry".

Header section featuring the Praetorian Global logo (a stylized face) and the text "PRAETORIAN GLOBAL proven information security". A navigation menu on the right lists: About us, Services, Solutions, Projects, and Contacts. The background of the header is a world map.

## Blackjacking - Owning the Enterprise via the Blackberry

Presented at Defcon 14 - Las Vegas, NV 2006

Jesse D'Aguanno  
jesse [at] praetoriang.net

### Abstract:

Research in Motion's Blackberry technology has quickly become the defacto standard for executives and technical personnel alike to maintain unteathered remote access to critical data. Often regarded as inherently secure, most administrators deploy this solution without a full understanding of the technology or risks involved.

This presentation will demonstrate how an attacker could utilize many typical corporate blackberry deployments to directly attack machines on the internal network—behind your perimeter defenses! The tools and source code presented will be available for attendees. Techniques for reducing the risks associated with this technology will also be presented.

### Materials:

#### Presentation Slides

[Download](#)

#### Blackberry Attack Toolkit (Including BBProxy)

[Download](#)

**NOTE: This link is now active!**

including Bluetooth, Ev-Do (Evolution-Data Only), and HSDPA (High Speed Downlink Packet Access).

The two researchers declined to disclose the specific details of their attack before the August 2 presentation, but they described it in



# Blackjacking – Owning the Enterprise via Blackberry



Jesse 'x30n' D'Aguanno  
•x30n@digrev.org  
•jesse@praetoriang.net



Defcon 14 - Las Vegas, NV USA 2006

including Bluetooth, Ev-Do (Evolution-Data Only), and HSDPA (High Speed Downlink Packet Access).

The two researchers declined to disclose the specific details of their attack before the August 2 presentation, but they described it in



Folder	New	Total				From	To	Subject
+ @ Ivica		240						
	310	13711						
Inbox	310	314						
Outbox		0						
Sent		0						
Trash		5						
Prebaceno		4502						
Vazno		270						
Arhiva		8620						
+ @	347	14221						

**From** [redacted] **4,256 b**  
**Reply-To** [redacted]  
**To** [redacted]  
**Subject** Apache Proof of Concept Exploit



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 daemon, not open any shell or execute code in the  
 remote server.  
 PHP supports multipart/form-data POST requests (as described in  
 RFC1867)

apache.c

including Bluetooth, Ev-Do (Evolution-Data Only), and HSDPA (High Speed Downlink Packet Access).

The two researchers declined to disclose the specific details of their attack before the August 2 presentation, but they described it in



Total attacks: 5023 of which 1775 single ip and 7250 mass defacements

#### POLLS

Should Zone-H continue mirroring defacements? (floods will be purged)

☐ Yes, it's useful

☐ No, it's useless

Vote

Results

#### MAIN MENU

Home

Digital Warfare

Geopolitics

ITsec News

ITsec Advisories

Test Drive

360°

Digital Attacks Archive

Zone-H events

Publications

Zone-H Friends/Partners

Contact Us

Search

Download Area

Zone-H forum

About this website

Scotland Yard careers web site defaced

Chinese cyberwarriors on the rise?

## WEB DEFACEMENTS 2007 IN SHARP DECREASE (-37%). IS IT A GOOD NEWS OR BAD NEWS?

User Rating: / 13

Poor Best Rate

Written by Roberto Preatoni

Friday, 21 March 2008



We recently published the **2007 statistics** based on the data collected by Zone-H. One of the most interesting fact is the sharp decrease (-37%) of the attacks compared to the attacks reported the previous year. In fact, while in year 2006 we filed 752,361 attacks, in year 2007 the reported attacks were "only" 480,905. Since the end of the 90s, when the first mirror archives (Alldas, Safemode, Attrition) started to track website defacements, this is the first time ever that the trend is showing a negative figure.

Usually from year to year, we were used to see an average increment of about 30% (in year 2005 the reported attacks were 493,840).

Is this a good news or a bad news? Certainly website defacements are loosing popularity. A few years ago a Microsoft defacement would have hit the news, today there's no more hype among journalists in reporting such fact. We just got used to it, period.

The interesting question is: if the Internet user-base is getting larger and larger and if the systems are getting weaker and weaker, why the website defacements are decreasing by strong figures?

We do have an answer and to explain it to you we have to go back with our memories in year 2005...

At that time and before, website defacement was mainly a Brazilian business where hundreds of Brazilian crackers groups were causing havoc to the web. They were all coordinating between each other using the most famous Brazilian IRC network, called Brasnet. One day in year 2005, the Brazilian police seized the logs of the conversations between the Brazilian defacers and started to distribute punishments to some of them. The reaction was quite immediate: most of the crews quit their own IRC Brasnet channels, some of them decided to quit defacing and some of them moved to different servers, trying to look for "secrecy" on private IRC servers.

Regardless, the path was already traced, defacing was maybe something funny to do for Brazilians but more interesting activities were profiling at the horizon, such scamming, phishing, carding and banking. From hacking for fun, soon the Brazilians efforts were targeted to hacking for money. So much that today, there is no more activity in regards of defacements coming from Brazil. Sure, the Turks inherited the defacing business from Brazilians, nowadays most of the website defaces are coming from the land of Ata Turk.



(votes will be purged)

☐ Yes, it's useful

☐ No, it's useless

Vote

Results

## MAIN MENU

Home

Digital Warfare

Geopolitics

ITsec News

ITsec Advisories

Test Drive

360°

Digital Attacks Archive

Zone-H events

Publications

Zone-H Friends/Partners

Contact Us

Search

Download Area

Zone-H forum

About this website

Staff Members

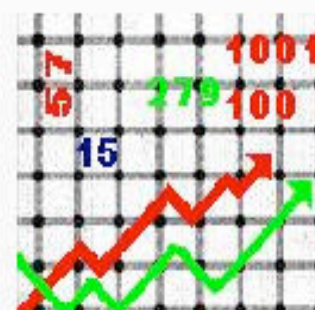
## USER MENU

Your Details

Mailing list subscription

Logout

Wednesday, 05 March 2008



Every year, Zone-H publishes stats of registered attacks.

In the early months of Zone-H, we received an average of 2.500 notifications per month, last year this average jumped to 37.915 monthly attacks. In order to have better idea of the attacks number, during January 2007, 62.092 attacks were validated, and in the month of June - when a DDoS cyberwar in **Russia** paralyzed thousands of web sites, Zone-H included - we validated 17.797 defacements. The record occurred in the month of August 2006, with 130.645 registered attacks.

In the past the most attacked operating system was Windows, but many servers were migrated from Windows to Linux...

Therefore the attacks migrated as well, as Linux is now the most attacked operating system with 1.485.280 defacements against 815.119 in Windows systems (numbers calculated from 2000).

Attacks by month	Year 2005	Year 2006	Year 2007
Jan	45.929	43.585	62.092
Feb	47.059	37.061	52.697
Mar	41.175	38.630	54.842
Apr	48.995	43.007	40.919
May	41.735	86.135	41.410
Jun	43.870	51.888	17.797
Jul	41.469	95.461	56.763
Aug	41.917	130.645	38.362
Sep	31.853	69.643	29.236
Oct	40.724	52.421	31.681
Nov	35.000	50.940	31.925
Dec	34.114	52.945	23.181
<b>Total</b>	<b>493.840</b>	<b>752.361</b>	<b>480.905</b>



# FUCK TO ADMIN...



we are [ [  
[ D1G\_D1G ]

] contact [  
[ [d1g\\_d1g@hackermail.com](mailto:d1g_d1g@hackermail.com) ]

] irc [  
[ [irc.brasnet.org](http://irc.brasnet.org) - #virtualhell ]

] greetz [  
[ [ Interactive, phRoZen, TriaX, BHS, Attacked SOul, cr1m3 0rg4n1z4d0



## LAST WEEK ATTACKS

O.S.	Def.	%
Linux	5536	61.34%
Win 2003	3090	34.24%
Win 2000	250	2.77%
FreeBSD	114	1.26%
Unknown	12	0.13%
Other	23	0.25%

Total attacks: **9025** of which  
**1775** single ip and **7250** mass  
defacements

## MAIN MENU

- Home
- Digital Warfare
- Geopolitics
- ITsec News
- ITsec Advisories
- Test Drive
- 360°
- Digital Attacks Archive
  - ▶ Attacks Archive
  - ▶ Attacks Archive
  - ▶ Attackers Top List
  - ▶ Attackers Top List ★
  - ▶ Attack Notification
  - ▶ Attacks On Hold
- Zone-H events
- Publications

## ATTACKERS TOP LIST

This is the list of the first 50 attackers...

NO	ATTACKER	SINGLE DEF.	MASS DEF.	TOTAL DEF.	HOMEPAGE DEF.	SUBDIR DEF.
1	<b>iskorpitx</b>	20700	174242	194942	70046	124896
2	<b>Fatal Error</b>	10792	22195	32987	26951	6036
3	<b>SPYKIDS</b>	8717	21750	30467	29488	979
4	<b>1923Turk</b>	7336	20467	27803	5231	22572
5	<b>Secrethackers.org</b>	7187	1424	8611	1876	6735
6	<b>Thehacker</b>	7080	35872	42952	37941	5011
7	<b>BeLa</b>	6604	4971	11575	6813	4762
8	<b>aLpTurkTegin</b>	6540	17023	23563	13977	9586
9	<b>GHoST61</b>	5824	7831	13655	5760	7895
10	<b>ir4dex</b>	5675	31159	36834	36672	162
11	<b>hackbsd crew</b>	5454	8396	13850	7581	6269
12	<b>Red Eye</b>	5240	31244	36484	36174	310
13	<b>Dengesiz Team</b>	4869	5465	10334	3708	6626
14	<b>AYYILDIZ</b>	4719	6671	11390	4201	7189
15	<b>SanalYargic</b>	4389	3512	7901	2140	5761
16	<b>core-project</b>	4372	9777	14149	14089	60
17	<b>TechTeam</b>	4333	32034	36367	36354	13
18	<b>uykusuz001</b>	4160	3907	8067	846	7221
19	<b>Yusuf</b>	4058	666	4724	684	4040
20	<b>r00t System</b>	4055	19218	23273	21043	2230



## LAST WEEK ATTACKS

O.S.	Def.	%
Linux	1736	54.92%
Win 2003	1162	36.76%
Win 2000	114	3.61%
FreeBSD	70	2.21%
Unknown	62	1.96%
Other	17	0.54%

Total attacks: **3161** of which **1168** single ip and **1993** mass defacements

## MAIN MENU

- Home
- Digital Warfare
- Geopolitics
- ITsec News
- ITsec Advisories
- Test Drive
- 360°
- Digital Attacks Archive
  - Attacks Archive
  - Attacks Archive
  - Attackers Top List
  - Attackers Top List ★
  - Attack Notification
  - Attacks On Hold
- Zone-H events
- Publications

## DIGITAL ATTACKS ARCHIVE: TODAY'S VERIFIED ATTACKS

[ **DISABLE FILTERS** ]

Apply Filters

ATTACKER: ALL DOMAIN: sk

DATE: ALL : 01 JANUARY 1999 SYSTEM: ALL

Total attacks: **4839** of which **914** single ip and **3925** mass defacements

**Legend:**

- H - Homepage defacement
- M - Mass defacement (click to view all defacements of this IP)
- R - Redefacement (click to view all defacements of this site)
- ★ - Special defacement (special defacements are important websites)























DATE	ATTACKER	FLAGS	DOMAIN	OS	VIEW
2008/05/15	AnonscorpAttackTeam	M	[REDACTED]	Linux	
2008/05/15	AnonscorpAttackTeam	M	[REDACTED]	Linux	
2008/05/15	AnonscorpAttackTeam	M	[REDACTED]	Linux	
2008/05/15	AnonscorpAttackTeam	M	[REDACTED]	Linux	
2008/05/15	AnonscorpAttackTeam	M	[REDACTED]	Linux	
2008/05/15	AnonscorpAttackTeam	M	[REDACTED]	Linux	
2008/05/15	AnonscorpAttackTeam	M	[REDACTED]	Linux	
2008/05/15	AnonscorpAttackTeam	M	[REDACTED]	Linux	
2008/04/30	AnonscorpAttackTeam	H M	[REDACTED]	Win 2003	
2008/04/30	AnonscorpAttackTeam	H M	[REDACTED]	Win 2003	
2008/04/30	AnonscorpAttackTeam	H M	[REDACTED]	Win 2003	



[Publications](#)[Zone-H Friends/Partners](#)[Contact Us](#)[Search](#)[Download Area](#)[Zone-H forum](#)[About this website](#)[Staff Members](#)**USER MENU**[Your Details](#)[Mailing list subscription](#)[Logout](#)**LOGIN FORM**

Hi, malimujo

[Logout](#)

2008/04/30	AnonscorpAttackTeam	H M	[REDACTED]	Win 2003	
2008/04/30	AnonscorpAttackTeam	H M	[REDACTED]	Win 2003	
2008/04/27	TGH	H M R	[REDACTED]	Linux	
2008/04/27	TGH	H M R	[REDACTED]	Linux	
2008/04/27	AnonscorpAttackTeam	M	[REDACTED]	Linux	
2008/04/27	AnonscorpAttackTeam	H M	[REDACTED].sk	Linux	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	
2008/04/25	TGH	H M	[REDACTED].sk	Win 2000	

# Attack by web sites



# Attack by web sites

Trojan intercepts bank tokens | The Register - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.theregister.co.uk/2006/03/24/trojan\_captures\_token/

Now: Partly Sunny, 21° C Sun: 6° C Mon: 23° C Mon: 8° C Tue: 24° C Tue: 13° C Wed: 19° C Wed: 7° C Thu: 2

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

The Register search results for "deutsche b... Trojan intercepts bank tokens | The ...

Search

– Quick Jump –

**Reg Hardware**

**Reg Developer**

**Channel Register**

**Reg Research**

**News Tools**

Newsletters & Feeds

Reg Mobile

DeskTop News Alerts

US Edition

**Reg Shops**

Reg Merchandise

Reg Books

Mobile Gadgets

Hosting

**Top Stories**

Linux patch becomes terminal pain

Are Google's glory days behind it?

MPAA to serve lawsuits on BitTorrent servers

Crypto browser plug-in aims for simplicity

## Trojan intercepts bank tokens

TAN marks exposed

By [Jan Libbenga](#)

Published Friday 24th March 2006 16:23 GMT

[Find your perfect job - click here for thousands of tech vacancies.](#)

A newly discovered Trojan is intercepting the TAN codes used as security tokens by customers of two major German banks, Postbank and Deutsche Bank, according to anti-virus experts.

Until now, TAN codes were pretty safe, in particular against phishing attacks, as these tokens are sent either through (snail) mail or by SMS. Phishing scammers would not only have to know a customer's login details and password to enter an online bank account, but also the token to enable transactions. For this reason, many European banks have adopted the system for online banking.

### SPONSORED LINKS

- [UK IT recruitment specialists - Jobsite](#)
- [A+ CERTIFICATION from the Register's training library](#)
- [Rackspace, The Managed Hosting Specialist - its all we do! - Click here to find out more](#)
- [Technology White Papers - Download them for free from Reg Research](#)

Trojan-Spy.Win32.Bancos.pw is changing the security landscape once again, as it is able to [intercept](#) HTTPS traffic and obtain the security token pass code. When the customer tries to enter a TAN code, an error message appears. Phishing scammers, if they are quick enough, can then enter the code themselves.

The Trojan isn't widespread yet, nor have there been any reports of victims

**REG WE**

**The Re**

SHO ON

SEN MA

NEE KNO

**GET THE REG WE NEWSLE**

*Too many to read during week? Let us sure you don't miss the important sign up for our day news roll [click here](#)*

Done 0 errors



# Attack by web sites

FT.com / World - Hackers attack 13% of big businesses - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.ft.com/cms/s/0/a755dc4c-0fe6-11dd-8871-0000779fd2ac.html?nclink\_check=1

ABAC@TRADE - Pregl... Abacus gledalica - pr... Currency Charts

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

SignupShield Fill-in Save Form 1-Click Sign-in

Zone-H.org - When security becomes ... Zone-H.org - War 2.0 FT.com / World - Hackers attack ...

## Hackers attack 13% of big businesses

By Maija Palmer  
Published: April 21 2008 23:45 | Last updated: April 21 2008 23:45

Computer hackers trying to steal confidential information have attacked more than one in 10 large UK businesses, a 10-fold increase compared with two years ago, according to a government report.

About 13 per cent of large companies have detected unauthorised outsiders in their networks, according to the study by the Department for Business, Enterprise and Regulatory Reform, to be published on Tuesday at the Infosecurity Europe show in London.

"Large corporations are being actively targeted by hackers, often working in cahoots with organised crime, and looking to steal confidential customer data which can be used for identity fraud," said Chris Potter, partner at PwC, which did the research.

The immediate financial impact of IT security problems has lessened, costing UK businesses about £6bn a year, compared with £10bn in 2006. This is because fewer businesses are falling victim to computer viruses, which have caused substantial financial losses in the past.

But confidential data loss was likely to have a more profound long-term effect in terms of reputational damage, Mr Potter warned.

The TJX Companies, the discount retailer that owns the TK Maxx stores in the UK, revealed in January last year it had suffered a breach of data security that compromised the credit and debit card payments of customers. TJX has agreed in the next few months to pay out tens of millions of dollars to settle lawsuits brought in

### EDITOR'S CHOICE

- Breaking into the US citadel was child's play - Apr-22
- I am online, therefore I am (whoever I say I am) - Mar-08
- A run for their money - Mar-09
- Security experts warn of internet threats - Feb-20
- Targeted attacks mean this time it's personal - Mar-07
- Computer misuse act is bound to snare the innocent - Nov-22

### HIGHLIGHT


#### MBA Rankings

See our annual rankings of top MBA, EMBA, Executive Education and Master in Management programmes.

[More](#)

FT Central and Eastern European country special reports ▶

sponsored by

 **Raiffeisen INTERNATIONAL**  
Member of RZB Group

We live in FINANCIAL TIMES®

Jobs Business for sale Contracts & tenders

SEARCH Enter keywords

[Ticketing Schemes Manager](#)  
Transport for London

**ALPHAVILLE**  
instant market insight



# Attack by web sites

IndiaTimes website 'attacks visitors' | The Register - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.theregister.co.uk/2007/11/10/india\_times\_under\_attack/

ABAC@TRADE - Pregl... Abacus gledalica - pr... Currency Charts

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

SignupShield Fill-in Save Form 1-Click Sign-in

Zone-H.org - When security becomes ... Zone-H.org - War 2.0 FT.com / World - Computer misuse act... The Register: Security News and View... IndiaTimes

## IndiaTimes website 'attacks visitors'

Targets multiple vulns, some new

By [Dan Goodin in San Francisco](#) → [More by this author](#)

Published Saturday 10th November 2007 01:47 GMT

[See what the experts have to say on attracting, retaining and developing IT talent](#)

Visitors to the *IndiaTimes* website are being bombarded by malware, some of which appear to target previously unknown vulnerabilities in Windows, a security researcher warns.

In all, the English-language Indian news site is directly or indirectly serving up at least 434 malicious files, many of which are not detected by antivirus software, according to Mary Landesman, a senior security researcher at ScanSafe. She said at least 18 different IP addresses are involved in the attack.

"The end result of the compromise is that the user, going through their normal course of activities, is subject to a really massive installation of malicious files," she told us. "Coupled with the low detection by antivirus vendors, it does put the end user in a very vulnerable position."

Visitors can be infected even if they have up-to-date systems and they don't fall victim to tricks to install software or browser add-ons, she said. She urged people to avoid the site until it's been cleaned up.

[Diwali](#), the Hindu festival of lights, is in full swing in India and Landesman is concerned webmasters for the site may be hard to reach over this holiday weekend.

"Our hope is they'll cut their holiday short and take care of this before Monday," she said.

She said most pages on the IndiaTimes site are clean. Those that are infected, however, contain a potent cocktail of downloader and dropper Trojans and other binaries. They contain a script that points to remote sites, some of which link to still other sites. The malicious files exploit multiple vulnerabilities, and some appear to be previously unknown flaws in Windows, according to Landesman, who used to be a security researcher for Microsoft.

### News Tools

[Newsletters & Feeds](#)

[Reg Mobile](#)

[Reg Desktop News Alerts](#)

### Reg Shops

[Reg Merchandise](#)

[Books/Online Learning](#)

### Top Stories

- MS patch system poses 'significant risk', say researchers
- YouTube has a little local difficulty in Arabia
- Standalone security industry dying, says guru
- Hidden card fraud taxes UK.biz
- Smut blocking? We're more bothered about

### Top Rated



# Attack by web sites

Attackers turn Bank of India site into malware bazaar | The Register - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.theregister.co.uk/2007/09/01/bank\_of\_india\_website\_takeover/

ABAC@TRADE - Pregl... Abacus gledalica - pr... Currency Charts

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

SignupShield Fill-in Save Form 1-Click Sign-in

Zone-H.org - When sec... Zone-H.org - War 2.0 FT.com / World - Comp... The Register: Security ... IndiaTimes website 'att... Attackers turn Bank...

## Attackers turn Bank of India site into malware bazaar

31 unique exploits served

By [Dan Goodin in San Francisco](#) → [More by this author](#)

Published Saturday 1st September 2007 00:11 GMT

[Test Drive Sun's Quad-Core Intel Xeon systems today](#)

Bank of India IT staff are mopping up the mess left by attackers who rigged the firm's website to feed malware to customers trying to access online services.

The bank managed to pry loose the rogue iframe responsible for the malware sometime early Friday morning California time. At time of writing, though, Bank of India's website was effectively cordoned off, bearing a terse notification saying: "This site is under temporary maintenance and will be available after 09:00 IST on 1.09.07."

The shuttering came a day after employees for security provider Sunbelt Software discovered someone had planted an iframe in the site that caused unpatched Windows machines to be infected with some of the most destructive pieces of malware currently in circulation. Sunbelt counted 31 separate pieces in all, including Pinch, a [powerful and easy-to-use Trojan](#) that siphons personal information from a user's PC. Other malware included Trojan.Netview, Trojan-Spy.Win32.Agent.ql, various rootkits and several spam bots.

Executives and IT administrators at US offices of Bank of India who were contacted Friday morning by IDG were initially unaware of the attack. A spokesman [later told the news service](#) that officials were aware of the problem and were working to correct it, but had no information concerning its severity or duration.

Some of the servers used to install the malware belonged to the notorious Russian Business Network, a group Spamhaus [says](#) is involved in child porn, phishing and other misdeeds. According to Verisign's iDefense unit, the RBN also played a hand in bringing us MPack, a powerful Trojan downloader that [infect edmore than 10,000 websites](#) in just three days.

In this case, the attackers appeared to use an exploit kit dubbed n404, according to [this post](#) by Dancho Danchev. It relies on a technique known as Fast-Flux, in which a server is constantly changing IP addresses to evade detection. However, there is no single

Search

Reg Hardware

Reg Developer

Channel Register

Whitepapers

**News Tools**

Newsletters & Feeds

Reg Mobile

Reg Desktop News Alerts

**Reg Shops**

Reg Merchandise

Books/Online Learning

**Top Stories**

**Top Rated**

- MS patch system poses 'significant risk', say researchers
- Modern 'primitive' could ease the pain of encrypting massive amounts of data
- Prime yourself for security on the web
- Microsoft: Finding flaws on our website is OK
- Apple gets into



# Attack by web sites

**Hackers load malware onto Mercury music award site | The Register - Mozilla Firefox**

File Edit View History Bookmarks Tools Help

http://www.theregister.co.uk/2007/06/07/dreamhost\_hack/

ABAC@TRADE - Pregl... Abacus gledalica - pr... Currency Charts

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

SignupShield Fill-in Save Form 1-Click Sign-in

Zone-H.org - When security b... Zone-H.org - War 2.0 FT.com / World - Computer mi... The Register: Security News ... IndiaTimes website 'attacks vi... Hack

## Hackers load malware onto Mercury music award site

### Security nightmare for DreamHost

By [John Leyden](#) → [More by this author](#)  
Published Thursday 7th June 2007 15:04 GMT

[Find out how to eradicate 99.7% of spam](#)

Hackers have been able to load malware onto the official Mercury music awards site, as well as hundreds of other sites, after breaking into the systems of US-based hosting firm DreamHost.

DreamHost blamed a security flaw in its web control panel software for an attack that allowed hackers to compromise a "very small subset" of user accounts. Affected customers have been notified by email. DreamHost said only web content - not credit card or billing information - was compromised.

In a [statement](#) published Wednesday, DreamHost said: "The security flaw allowed the attackers to log into our customer web control panel with the access privileges of another user. From our web panel they were able to access individual user password information. The attackers also attempted to gain access to our central database and billing information but were ultimately thwarted in that attempt. No credit card information or customer personal information was obtained."

DreamHost takes care of more than 500,000 domains, according to the firm. An email sent by DreamHost to its customers on 5 June, said approximately 3,500 separate FTP accounts were compromised by the hack. DreamHost has advised its customers to change their FTP account passwords immediately. The firm has promised to update concerned punters about the steps it is taking to prevent a repetition.

News of the attack followed just hours after DreamHost said it had upgraded its WebFTP systems. The timing of this announcement suggests this was more likely to have been part of DreamHost's efforts to put its house in order rather than the cause of its problems.

UK-based web security firm ScanSafe, which has been monitoring the attack, said attackers used the insecure web controls at DreamHost to load Trojan downloader malware onto well known and trusted sites. Confirmed targets of the attack include [nationwidemercurys.com](#), the Mercury music awards site (which is sponsored by building society Nationwide), and UK law firm

Search

Reg Hardware

Reg Developer

Channel Register

Whitepapers

**News Tools**

Newsletters & Feeds

Reg Mobile

Reg Desktop News Alerts

**Reg Shops**

Reg Merchandise

Books/Online Learning

**Top Stories**

**Top Rated**

- MS patch system poses 'significant risk', say researchers
- Modern 'primitive' could ease the pain of encrypting massive amounts of data
- Prime yourself for security on the web
- Microsoft: Finding flaws on our website is OK
- Apple gets into


























# **WELCOME TO DARK MARKET**




Administration (Administrator)

10-03-2006

		Thread / Thread Starter	Rating	Last Post	Replies	Views
		Sticky: <u>e-gold exchange still available</u> JiLsi		Yesterday 10:50 PM by JiLsi	5	126
		<u>rbc logins</u> (1 2) toss		Today 01:19 AM by toss	12	190
		<u>Tipper And Embosser For Sale..</u> wozney		Yesterday 06:46 PM by soufly	4	158
		<u>Couple of hacked unix servers for SCAM</u> Fake		10-17-2006 03:37 PM by Fake	5	106
		<u>100 usa valid fullz for sale</u> crimepays		10-17-2006 01:07 PM by ZDEVIL19	7	215
		<u>Full infos with Bank account numbers</u> Iceburg		10-17-2006 06:45 AM by underown	1	79
		<u>Halifax UK Logins</u> (1 2) qlegit		10-17-2006 06:01 AM by qlegit	10	177
		<u>Zombie Computers</u> DarkPimp		10-15-2006 06:14 PM by soufly	5	258
		<u>Need JCB cards,any country</u> ibatistuta		10-15-2006 02:14 AM by ibatistuta	2	42
		<u>Need CVV2'S of this county</u> Meki		10-14-2006 12:47 PM by Meki	6	81
		<u>canada banks</u> workerbee		10-14-2006 01:15 AM by workerbee	0	26
		<u>Need Bank logins of this county</u> esc		10-12-2006 07:39 AM by esc	2	57
		<u>Selling comcast and optonline accounts</u> esc		10-12-2006 07:39 AM by esc	4	81

DarkPimp offline  
Member

Join Date: Jul 2006  
Posts: 11

 **HIRING: Hacker, need to keylog someone**

I will supply you with IP, you will then get yourself in and install a keylogger.

Paying through egold and paypal.

PM me for full details and if you're willing to do this.

QUOTE




## Latvian M, 18 Passport For Sale

09-04-2006, 05:55 PM

#1

Brady offline  
Member

Join Date: Apr 2006  
Posts: 1

 Latvian M, 18 Passport For Sale

Agree to use escrow service, buyer pay fees.  
The passport expires in 2010 year.

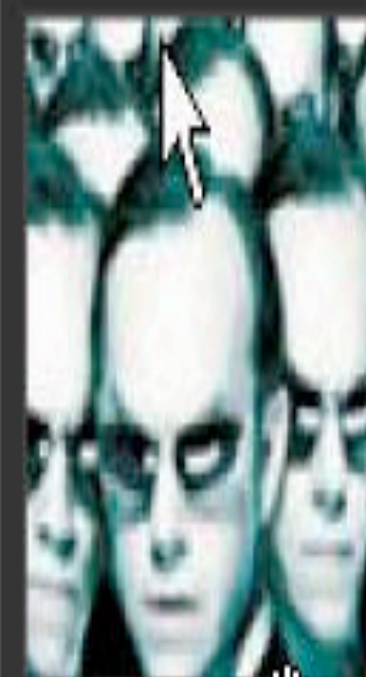
Anyone interested PM woth offers.  
Will send a scan too.

QUOTE

## 3 European Amex Centurion Dumps

08-07-2006, 12:48 PM

#1



**matrix001** Offline

Reviewed Vendor (CC Templates & Custom Graphics)

Join Date: Feb 200

Posts: 163



3 European Amex Centurion Dumps

dumps sold.

*Last edited by matrix001 : 08-14-2006 at 03:20 PM.*

QUOTE

08-13-2006, 09:17 AM

#1

qlegit offline

Member \*Use Escrow\*

Join Date: Mar 200

Posts: 35



## Hacked hosts

hi ppl  
I am selling hacked hosts, avaible for scams and mailers etc.

PHP is supported

CPanel is supported

SSH is supported,

price is : 20 \$ per host.

( if u need more hosts i can give you discount )

-----  
icq : 251-611-896

yahoo: azuraza001  
-----

[ i accept escrow ]

C ya

QUOTE

## DDos SERVICE

04-18-2006, 06:34 PM

#1

[is](#) Offline

Trial Vendor (ddos service)

Join Date: Mar 200

Posts: 4

### DDos SERVICE

I offer services DDos'a,  
The prices: from 30 \$ up to 50 \$.

----  
Preliminary check of service is possible. Anonymity of the order  
It is completely guaranteed.

----  
Contact icq: 112221111,  
Write in offline on all your questions  
There will be answers.

QUOTE



I have all this logins from UK.

Comes with DOB/SecurityNumber/ID

These are the accounts and prices, prices are negociable and if you're buying more than one i can make better deals. Escrow is ofcourse always accepted.

Have any questions you can email me at [draxdrax@safe-mail.net](mailto:draxdrax@safe-mail.net)

- 1 - Personal - 15 000 - 250GBP
- 2 - Personal - 3 000 - 50GBP
- 3 - Personal - 4 000 - 60GBP
- 4 - Personal - 1 000 - 20GBP
- 5 - Personal - 2 800 - 40GBP
- 6 - Personal - 2 000 - 30GBP
- 7 - Personal - 30 000 - 300GBP
- 8 - Personal - 1 000 - 20GBP
- 9 - Personal - 1 000 - 20GBP
- 10 - Personal - 800 - 10GBP
- 11 - Personal - 700 - 10GBP
- 12 - Personal - 3 600 - 55GBP
- 13 - Personal - 11 000 - SOLD
- 14 - Personal - 1 110 - 10GBP
- 15 - Personal - 500 - 10GBP
- 16 - Personal - 70 000 - 300GBP
- 17 - Personal - 13 000 - 250GBP
- 18 - Personal - 1 500 - 10GBP
- 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

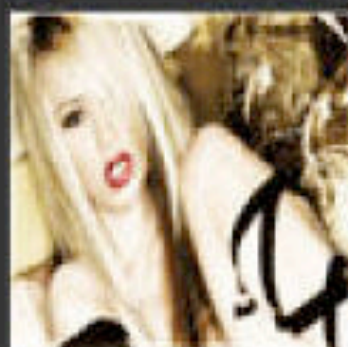
10-05-2006, 11:40 AM

#1



Join Date: Jul 200

Posts: 118

**Drax** Offline

Verified Vendor (BANK LOGIN)

DM Reviewer

Canadian Moderator

Donator

have some of this bank.  
In this format

Customer Number:  
Memorable Data:  
Pass Number:  
IP:

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



05-30-2006, 06:33 PM

#1

qlegit offline  
Member \*Use Escrow\*

Join Date: Mar 2006

Posts: 35



## UK logins

hi ppl  
i have ~~UK logins~~ and other UK logins  
msg me for deal  
price is 3 - 5 % from balance ..  
c ya 😊

QUOTE

Memorable Data:  
Pass Number:  
IP:

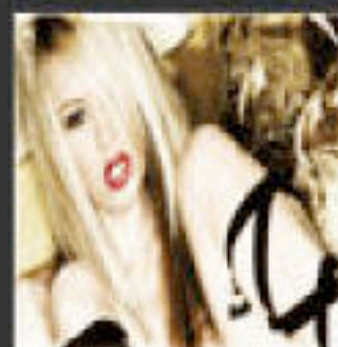
I have 3 accs with 10k+ , 11k, 50k, 220k. buy all for 750gbp or each for 300gbp  
also have many accs with 1k - 20gbp each acc

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

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 ~~capital one~~ ~~chase~~ ~~etc.~~ etc.,

pm me if u need anythin

P

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



# Google - A View To A Kill!



# Do you need printer?

Hackers use Google to access photocopiers - ZDNet UK News - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://news.zdnet.co.uk/communications/networks/0,39020345,39167848,00.htm

IBM Business Transf... IBM Internal Help Ho... IBM Standard Softw... Search the Web wit...

Disable CSS Forms Images Information Miscellaneous Outline Resize Validation View Source Options

Search MSD Text Search for

Google Search: google hackers Google a favorite among hackers, too | CNE... Hackers use Google to access photoc...

advertisement

POUR PARTICIPER, CLIQUEZ DÈS **MAINTENANT.** inmarsat Total Communications Network

Search: All of ZDNet SEARCH top search newsletters

News > Internet > Security Tuesday 28th September 2004

## Hackers use Google to access photocopiers

Dan Ilett  
ZDNet UK  
September 24, 2004, 15:50 BST

**Making copies of something important? Photocopiers are the latest networked devices to fall prey to hackers armed with nothing more than Google's search engine**

Hackers are using search engines to watch what people photocopy.

Using Google hacks — requests typed into the search engine that bring up...

Talkback Tell us your opinion

Also in News

- IDC raises sales for 2004
- Electronic voting again
- Are nanoparticles attack your fees
- Start-up brews for Java
- Microsoft opens
- Microsoft stands on downloads
- VIA secures market with on-chip encryption
- Dell tackles IT recycling push

BUSINESS FASH

# Do you need printer?

Jimmyneutron



Apprentice Google Hacker



Joined: Sep 05, 2004

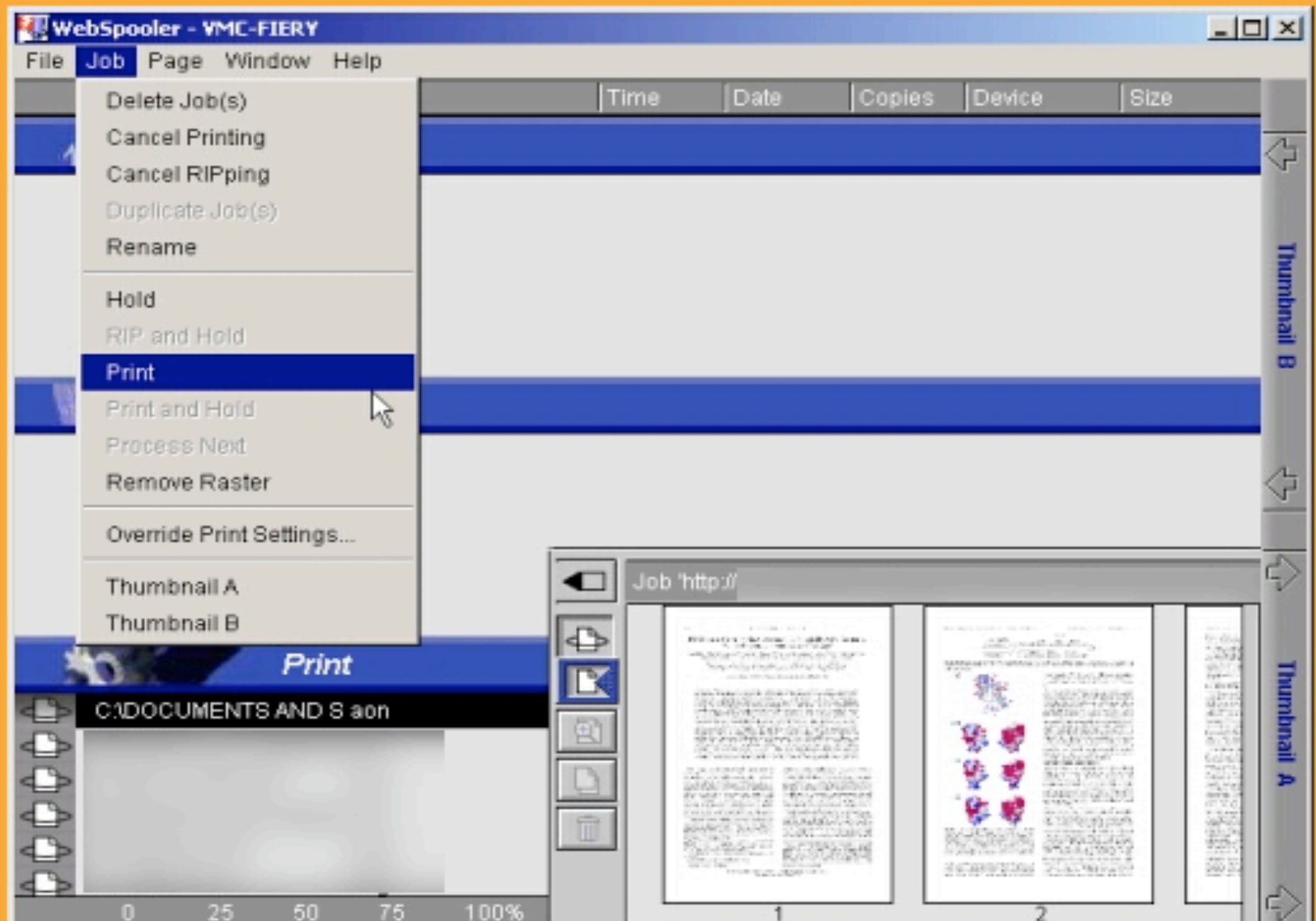
Posts: 158

Status: Offline

Posted: Sep 26, 2004 - 06:47 PM



This is how the admin app for Canon ImageRunner looks like:



# Do you need printer?

[Network Administration] - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://

IBM Business Transf... IBM Internal Help Ho... IBM Standard Softw... Search the Web wit...

Disable CSS Forms Images Information Miscellaneous Outline Resize Validation View Source Options

Search MSD Text Search for

Google S

# Konica

Main Page

Printer Status

Advanced Features

**Network Setup**

Printer Setup

Language Select

## Web Utilities

Model: IP-304

Network Card Serial Number:

REFRESH

System	Protocols	Others
<a href="#">Reset</a>	<a href="#">Setup NetWare</a>	<a href="#">Test Printer</a>
<a href="#">Factory Default</a>	<a href="#">Setup TCP/IP</a>	<a href="#">Configure Status Page</a>
<a href="#">Unit Status</a>	<a href="#">Setup AppleTalk</a>	
<a href="#">Network Address</a>		
<a href="#">Change Password</a>		



# Do you need printer?

Lantronix Web Manager - Mozilla Firefox

File Edit View Go Bookmarks Tools Help


http:

IBM Business Transf... IBM Internal Help Ho... IBM Standard Softw... Search the Web wit...

Disable CSS Forms Images Information Miscellaneous Outline Resize Validation View Source Options

Search MSD Text Search for OR Get

nny.ihackstuff.co...

**LANTRONIX**  
**MSS100**  
[TCP/IP](#)  
[Netware/IPX](#)  
[LAT](#)  
[Server Properties](#)  
[Port Properties](#)  
[Tech Support](#)  
[Home](#)  

Select from the menu above to modify server configuration.

**SERVER CONFIGURATION:**  
Server Name: MSS\_612591  
Boot Code Version: V1.6 (Sep 01, 2000)  
Firmware Version: Version V3.6/8(010807)  
Uptime: 15 Days 11:33  
Hardware Address: 00-80-a3-61-25-91  
IP Address: 192.168.1.200  
Subnet Mask: 255.255.255.0

**PORT:**  
1 Connected

**PROTOCOLS:**

TCP/IP	IPX	LAT
Enabled	Disabled	Enabled

# Do you need printer?

Remote UI:Top page - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

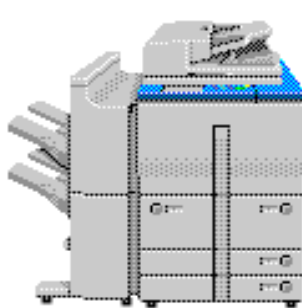
http://

IBM Business Transf... IBM Internal Help Ho... IBM Standard Softw... Search the Web wit...

Disable CSS Forms Images Information Miscellaneous Outline Resize Validation View Source Options

Search MSD Text Search for OR Get PDB:

## Remote UI



Remote UI  
Copyright CANON INC. 2003  
All Rights Reserved

Device Name : iR5000  
Product Name : iR5000  
Location :

Last Updated:09/28/2004 00:11:16

Printer Status: **Ready.**  
Scanner Status: **Ready.**

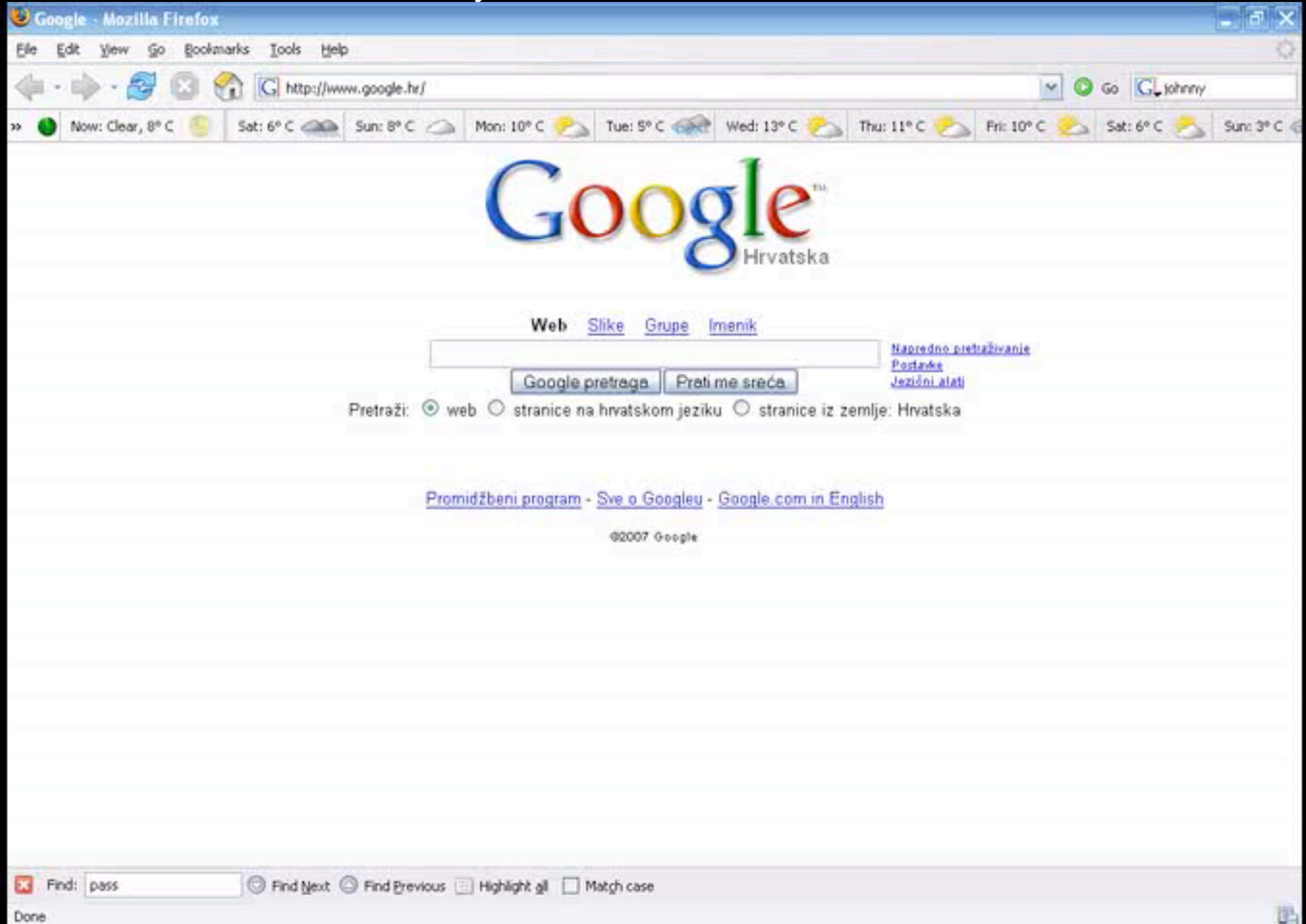
System Manager :  
Support :

[To Top page](#)  
[Device](#)  
[Job Status](#)  
[Add. Func.](#)  
[Send Mail](#)

# So, how it is done....



# So, how it is done....





# Something In The Air? ;-)



# Wardriving

# Wardriving



# Licence To Kill - Wireless



# Licence To Kill - Wireless

hr05686@dyn-9-157-161-22:~/war
File Edit View Terminal Go Help

**Network List** (Latest Seen desc)
(-) Up

Name	T	W	Ch	Pkts	Flags	IP Range	Size
vans.hr	A	Y	001	3		0.0.0.0	0B
SLAVE	A	N	011	36	A4	192.168.10.10	0B
Meeting_room	A	Y	007	5		0.0.0.0	0B
VIPonline.airlink	A	N	007	106		0.0.0.0	0B
VIPonline.airlink	A	N	001	3		0.0.0.0	0B
VIPonline.airlink_test	A	N	007	4	T4	212.91.118.22	0B
VIPonline.airlink_orinoco	A	N	007	1	T4	212.91.118.13	0B
<no ssid>	A	N	006	28		0.0.0.0	0B
17hnb09veza2002	A	Y	013	14		0.0.0.0	0B
zvbarhmo01	A	Y	006	952		0.0.0.0	300B
zvbarhmo01	A	Y	006	935		0.0.0.0	35k
bezicno	A	N	010	18	U3	192.168.0.0	324B
bezicno	A	N	004	2		0.0.0.0	0B
bezicno	A	N	002	4		0.0.0.0	0B
bezicno	A	N	008	6		0.0.0.0	0B
MEDVED	A	N	007	45	T	0.0.0.0	436B
nanobarh08	A	Y	002	899		0.0.0.0	55k
zvonimirova	A	Y	006	1		0.0.0.0	0B
<no ssid>	H	N	010	12		0.0.0.0	0B
privrvez	A	N	007	219	T4	172.19.10.75	29k
<no ssid>	H	N	010	16		0.0.0.0	0B
WiFiHR_Kvatric2	A	N	005	12	T4	10.14.0.5	13k
Hone	H	N	001	34		0.0.0.0	0B
<no ssid>	A	Y	005	195		0.0.0.0	25k
cenonarh07	A	Y	013	16		0.0.0.0	0B
traffico	A	N	011	1		0.0.0.0	0B

Ntwrks  
170  
Pckets  
94501  
Cryptd  
7733  
Weak  
3  
Noise  
538  
Discrd  
65187  
Pkts/s  
0  
  
prism2  
Ch: 7  
  
Discon

Lat 45.820 Lon 15.983 Alt 506.2f Spd 2.186m/h Hed 0.000 Fix NONE
64% (+) Down
02:09:44

**Status**

Found new network "linksys" bssid 00:06:25:4A:9B:17 WEP N Ch 11 @ 54.00 mbit  
Saving data files.  
Saving data files.  
localhost:2501 TCP error: socket returned EOF, server has closed the connection.

**Battery: AC charging 60% 0h0m0s**

# Licence To Kill - Wireless

hr05686@pingvin:/home/hr05686

File Edit View Terminal Go Help

Network List (Latest Seen desc) (-) Up Info

Name	T	W	Ch	Pkts	Flags	IP Range	Size
L1479	A	Y	009	8		0.0.0.0	0B
17hnb09veza2002	A	Y	013	1		0.0.0.0	0B
HTmobile	A	N	006	2		0.0.0.0	0B
hup	A	Y	007	746		0.0.0.0	0B
hup	A	Y	007	394		0.0.0.0	0B
default	A	N	006	59	F	192.168.0.1	0B
01knmasn	A	N	010	719		0.0.0.0	0B
<no ssid>	A	N	---	1		0.0.0.0	0B
Hendal	A	Y	006	363		0.0.0.0	0B
Apple Network f71690	A	N	010	17		0.0.0.0	0B
default	A	N	006	7	F	192.168.0.1	0B
hrsume.airlink	A	Y	006	104		0.0.0.0	0B
hrsume.airlink	A	Y	006	194		0.0.0.0	0B
hrsume.airlink	A	Y	006	77		0.0.0.0	0B
hrsume.airlink	A	Y	006	17		0.0.0.0	0B
<no ssid>	A	Y	008	7		0.0.0.0	0B
hrsume.airlink	A	Y	006	149		0.0.0.0	0B
HTmobile	A	N	006	276		0.0.0.0	0B
0707d	A	N	007	996		0.0.0.0	0B
ZagiW-Papirus	A	N	008	170	T3	192.168.3.0	1k
<zgw-trnje>	A	N	005	551	T2	10.5.0.0	98k
WaveLAN Network	A	N	010	5		0.0.0.0	0B
UcionicaWLAN	A	Y	010	1		0.0.0.0	0B
fsbwireless	A	Y	005	1		0.0.0.0	0B
<no ssid>	A	Y	007	11		0.0.0.0	0B
cvelba2	A	N	009	253	A4	172.29.31.1	740B

Info

Ntwrks 111

Pckets 112968

Cryptd 21

Weak 0

Noise 172

Discrd 60804

Pkts/s 0

prism2

Ch: 7

Elapsd 03:12:19

71% (+) Down

Status

Saving data files.

Saving data files.

Saving data files.

Saving data files.

Battery: AC charging 98% 0h0m0s

[root@pingv hr05686@p ?

The GIMP Layers, Cha --

Wed Feb 11 8:37:43 PM

# Licence To Kill - Wireless

hr05686@pingvin:/home/hr05686

File Edit View Terminal Go Help

**Network List (Latest Seen desc)** (-) Up Info (-) Up

**Network Details**

SSID : default  
+ Server : 127.0.0.1:2501  
BSSID : 00:0D:88:82:C8:67  
Carrier : IEEE 802.11b  
Manuf : D-Link  
Model : Unknown  
Matched : 00:0D:88:00:00:00/FF:FF:FF:00:00:00  
+ **FACTORY CONFIGURATION**  
Max Rate: 22.0  
First : Wed Feb 11 17:58:23 2004  
Latest : Wed Feb 11 17:58:43 2004  
Clients : 0  
Type : Access Point (infrastructure)  
Info :  
Channel : 6  
WEP : No  
Beacon : 100 (0.102400 sec)  
Packets : 59  
Data : 0  
LLC : 59  
Crypt : 0  
Weak : 0  
Dupe IV : 0  
Data : 0B  
Signal :  
Power : 17 (best 38)  
Noise : 6 (best 5)  
IP Type : Factory default  
IP Range: 192.168.0.1  
Min Loc : N/A

Saving data files.

Battery: AC charging 99% 0h0m0s

96% (+) Down

8

[root@pingv] hr05686@p ?  
The GIMP [Layers, Ch --

Wed Feb 11 8:50:23 PM



# Licence To Kill - Wireless

```
hr05686@dyn-9-157-161-22:~/war
File Edit View Terminal Go Help

Network List (Latest Seen desc) Info
Data Strings Dump All
Host: cgs.iskon.hr
Cookie: webmail=[REDACTED]@net.hr; __utma=222512899.3747715462.1053685438.1076583417.1076587475.1627; __utmb=2225
Accept: text/html, image/gif, image/jpeg, *:q=.2, */*;q=.2
Pragma: no-cache
Connection: Keep-Alive
messenger
hotmail
gxV>@
GET / HTTP/1.0
Via: 1.0 VENERA
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Hotbar 4.3.5.0)
Host: adopt.hotbar.com
Cookie: SDCU=10F28E0000513D; CTCI=00482008D20001200AA200Bp1000120032100001007BKh2nTqo.1Jc0100007e00000010Y0400Am00001E
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel,
Referer: http://adopt.hotbar.com/link.jsp?location_id=1450&acamp_id=2560&pcamp_id=2&creative_id=4121&dem=f.f.9.SI&href
Accept-Language: hr
Connection: Keep-Alive
DxV<@
5xV-A
GET /wutrack.bin?V=2&U=dd8145d8d5856d4d9f18fdf34f0ef727&C=iu&A=n&I=&D=&P=5.1.a28.2.100.1.0&L=en-US&S=s&E=00000000&M=&X
Accept: */*
User-Agent: Industry Update Control
Host: wustat.windows.com
Connection: Keep-Alive
fxV^@
USR 16 TWN I [REDACTED]@hc.htnet.hr
7V[@J
<xV<@
FxV>@
JxVB@

Found new network "<no ssid>" bssid 00:02:2D:09:CC:3D WEP N Ch 0 @ 0.00 mbit
Battery: 83% 0h58m0s
```

# Licence To Kill - Wireless

Kismet-Feb-12-2004-1.dump - Ethereal

File Edit View Capture Analyze Help

No.	Time	Source	Destination	Protocol	Info
83563	6104.597028	10.5.130.2	195.29.218.245	TCP	1146 > http [SYN] Seq=0 Ack=0 win=57344 Len=0 MSS
83564	6104.613907	10.5.130.2	195.29.218.245	TCP	1146 > http [SYN] Seq=0 Ack=0 win=57344 Len=0 MSS
84470	6160.307591	10.5.130.2	194.152.216.48	TCP	5222 > 24303 [ACK] Seq=0 Ack=0 win=58080 Len=0
84486	6160.871703	10.5.130.2	192.54.112.30	DNS	standard query A pleazerzoneprod.com
84629	6165.522572	10.5.130.2	202.103.190.99	DNS	standard query AAAA ns0.namelite.com
84674	6166.512334	10.5.130.2	64.156.186.90	DNS	standard query A pleazerzoneprod.com
84906	6176.539833	10.5.130.2	213.191.132.146	DNS	standard query A a1623.g.akamai.net
85167	6189.524903	10.5.130.2	195.29.218.245	TCP	1152 > 9899 [FIN, ACK] Seq=0 Ack=0 win=58400 Len=
86615	6225.255695	10.5.130.2	195.29.218.245	TCP	1160 > http [ACK] Seq=1 Ack=1 win=58400 Len=0
88025	6502.201472	10.5.130.2	213.191.132.146	TCP	22 > 4611 [SYN, ACK] Seq=0 Ack=1 win=57344 Len=0

Frame 95543 (174 bytes on wire, 174 bytes captured)

Arrival Time: Feb 12, 2004 19:51:44.283348000  
 Time delta from previous packet: 2.660893000 seconds  
 Time since reference or first frame: 7021.211782000 seconds  
 Frame Number: 95543  
 Packet Length: 174 bytes  
 Captured Length: 174 bytes

IEEE 802.11

0000	08 09 02 01 00 0b be 6a 2e 20 00 02 2d 32 f0 be	.....j . .-2..
0010	00 40 96 00 00 07 e0 f4 aa aa 03 00 00 00 08 00	.@..... .....
0020	45 00 00 8e 00 00 40 00 2e 11 5e 10 c0 29 a2 1e	E.....@. ..^..)
0030	0a 05 82 02 00 35 0f 39 00 7a fb fd da 9d 80 00	.....5.9 .z.....
0040	00 01 00 00 00 02 00 02 03 77 77 77 09 73 74 75	..... .www.stu
0050	64 69 6f 61 68 6d 03 63 6f 6d 00 00 01 00 01 c0	dioahm.c om.....
0060	10 00 02 00 01 00 02 a3 00 00 13 01 61 03 64 6e	..... .a.dn
0070	73 07 68 6f 73 74 77 61 79 03 6e 65 74 00 c0 10	s.hostwa y.net...
0080	00 02 00 01 00 02 a3 00 00 04 01 62 c0 31 c0 2f	..... .b.1./
0090	00 01 00 01 00 02 a3 00 00 04 42 71 81 f3 c0 4e	..... ..Bq...N
00a0	00 01 00 01 00 02 a3 00 00 04 40 1a 00 73	..... ..@..s

# Licence To Kill - Wireless

Studio AHM software pageplayer, pixxxgrabber, pixxxsafe - Mozilla Firefox

File Edit View Go Bookmarks Tools Help


http://www.studioahm.com/

Firefox Help Firefox Support Plug-in FAQ

STUDIO AHM CONVENIENCE SOFTWARE

Home | Company | Products | Buy | Support | Contact


TURN ANY WEB PAGE INTO A SLIDE SHOW



PagePlayer

PRESENTATION + FREE TRIAL


BATCH DOWNLOAD IMAGES AND VIDEO FROM THE WEB



PixxxGrabber


PRESENTATION + FREE TRIAL

HIDE & ENCRYPT YOUR IMAGE LIBRARY



PixxxSafe


PRESENTATION + FREE TRIAL

 PagePlayer

- Start a **zooming slide show** from **any web page** in Internet Explorer.

[Product information](#)


Available: Win

 PixxxGrabber

- Batch download image series and movie** collections from gallery sites.

[Product information](#)

Available: Win / Mac

 PixxxSafe

- Hide and encrypt** an image collection behind a password. View the picture series in your library as **animated side shows**.

[Product information](#)

Available: Win / Mac

NEWS

Feb. 01, 2004 New features:

PixxxGrabber 2.0 now downloads images, video, MP3, PDF, ... and shows large previews while you download

.....

Be the first to find out about our new releases: [register](#)



# Licence To Kill - Wireless

Kismet-Feb-12-2004-1.dump - Ethereal

File Edit View Capture Analyze Help

No.	Time	Source ^	Destination	Protocol	Info
95616	7023.896436	67.72.101.12	10.5.130.2	DNS	Standard query response CNAME sweetcuties.com A 4.78
95618	7023.908566	67.72.101.12	10.5.130.2	DNS	Standard query response CNAME sweetcuties.com A 4.78
95574	7023.789329	64.26.0.115	10.5.130.2	DNS	Standard query response
95584	7023.805793	64.26.0.115	10.5.130.2	DNS	Standard query response
95586	7023.813136	64.26.0.115	10.5.130.2	DNS	Standard query response
95589	7023.820067	64.26.0.115	10.5.130.2	DNS	Standard query response
95600	7023.853539	64.26.0.115	10.5.130.2	DNS	Standard query response
95602	7023.863259	64.26.0.115	10.5.130.2	DNS	Standard query response
95609	7023.870667	64.26.0.115	10.5.130.2	DNS	Standard query response
95610	7023.879568	64.26.0.115	10.5.130.2	DNS	Standard query response

Frame 95616 (221 bytes on wire, 221 bytes captured)

Arrival Time: Feb 12, 2004 19:51:46.968002000  
 Time delta from previous packet: 0.005295000 seconds  
 Time since reference or first frame: 7023.896436000 seconds  
 Frame Number: 95616  
 Packet Length: 221 bytes  
 Capture Length: 221 bytes

ETHER II, Src: Intel Wireless, Dst: 10.5.130.2, Protocol: DNS

```

0000  08 01 02 01 00 0b be 6a 2e 20 00 02 2d 32 f0 be  .....j . .-2..
0010  00 40 96 00 00 07 50 f8 aa aa 03 00 00 00 08 00  .@....P. ....
0020  45 00 00 bd 08 20 00 00 30 11 4d b5 43 48 65 0c  E.... ..0.M.CHe.
0030  0a 05 82 02 00 35 0f 39 00 a9 39 36 66 bd 84 80  ....5.9 ..96f...
0040  00 01 00 02 00 02 00 03 03 77 77 77 0b 73 77 65  .... .www.swe
0050  65 74 63 75 74 69 65 73 03 63 6f 6d 00 00 01 00  etcuties .com....
0060  01 c0 0c 00 05 00 01 00 00 0e 10 00 02 c0 10 c0  ....
0070  10 00 01 00 01 00 00 0e 10 00 04 04 4e 16 1a c0  .... .N...
0080  10 00 02 00 01 00 00 0e 10 00 15 03 6e 73 31 0b  .... .ns1.
0090  74 65 63 68 69 65 6d 65 64 69 61 03 6e 65 74 00  techieme dia.net.
00a0  c0 10 00 02 00 01 00 00 0e 10 00 06 03 6e 73 32  .... .ns2
00b0  c0 53 c0 4f 00 01 00 01 00 00 0e 10 00 04 04 4e  .S.O.... .N
00c0  16 09 c0 70 00 01 00 01 00 00 0e 10 00 04 43 48  ...p....CH
00d0  65 0c 00 00 29 10 00 00 00 00 00 00 00 00 00  e....)....
    
```

# Licence To Kill - Wireless

Kismet-Feb-12-2004-3.dump - Ethereal

File Edit View Capture Analyze Help

No.	Time	Source	Destination	Protocol	Info
73490	3700.862313	10.5.130.60	195.29.150.5	POP	Request: PASS Cm7mk8
73494	3700.979079	10.5.130.60	195.29.150.5	POP	Request: STAT

Contents of TCP stream

PASS Cm7mk8  
STAT

Frame 73490 (85 bytes)  
Arrival Time: Feb  
Time delta from previous capture: 0.000000  
Time since reference capture: 0.000000  
Frame Number: 73490  
Packet Length: 85  
Capture Length: 85  
Ether II, Src: Intel 802.11, Dst: Intel 802.11

0000 08 02 02 01 00 00 00  
0010 00 40 96 00 00 00 00  
0020 45 00 00 35 5d 11 00  
0030 c3 1d 96 05 04 a3 00  
0040 50 18 fb 13 8d c4 00  
0050 6d 6b 38 0d 0a 00 00

# Licence To Kill - Wireless

## Contents of TCP stream

```
POST [REDACTED] HTTP/1.0
Accept: image/gif, image/x-xpixmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us,hr;q=0.5
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; windows 98; DigExt)
Host: [REDACTED]
Content-Length: 38

Phone=38598[REDACTED]&Message=pacove jedan
```



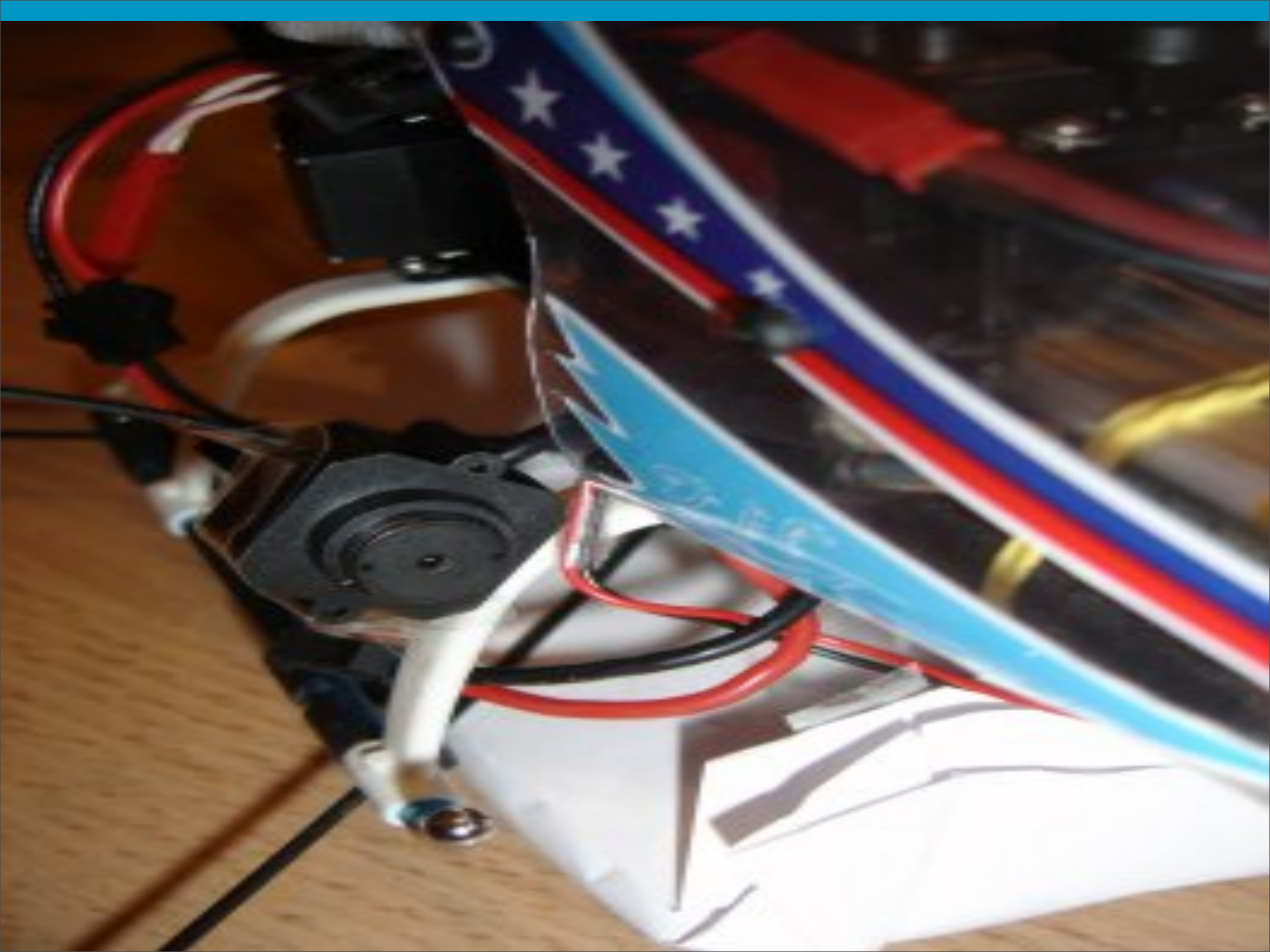






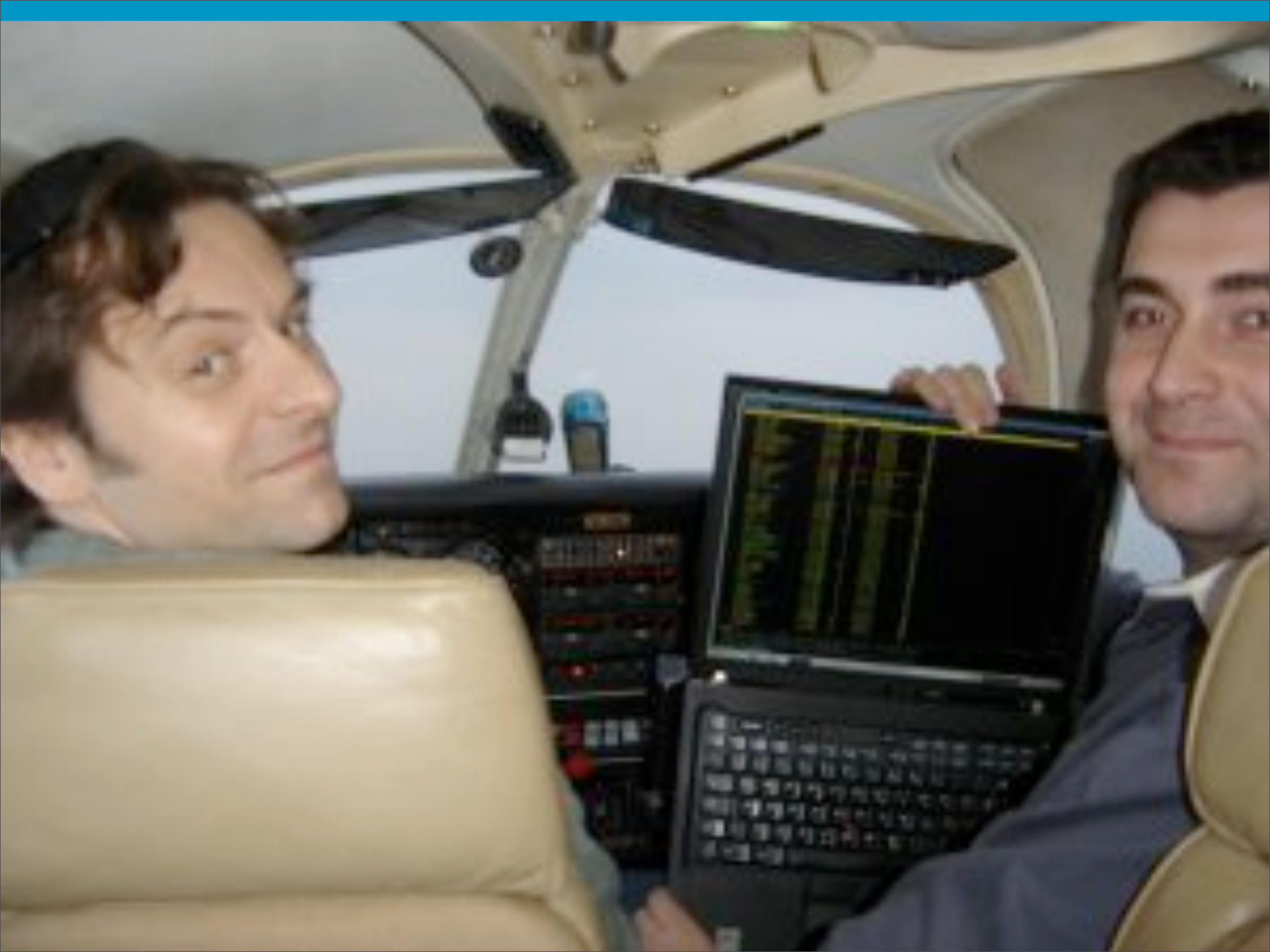














# Kismet in action - part one

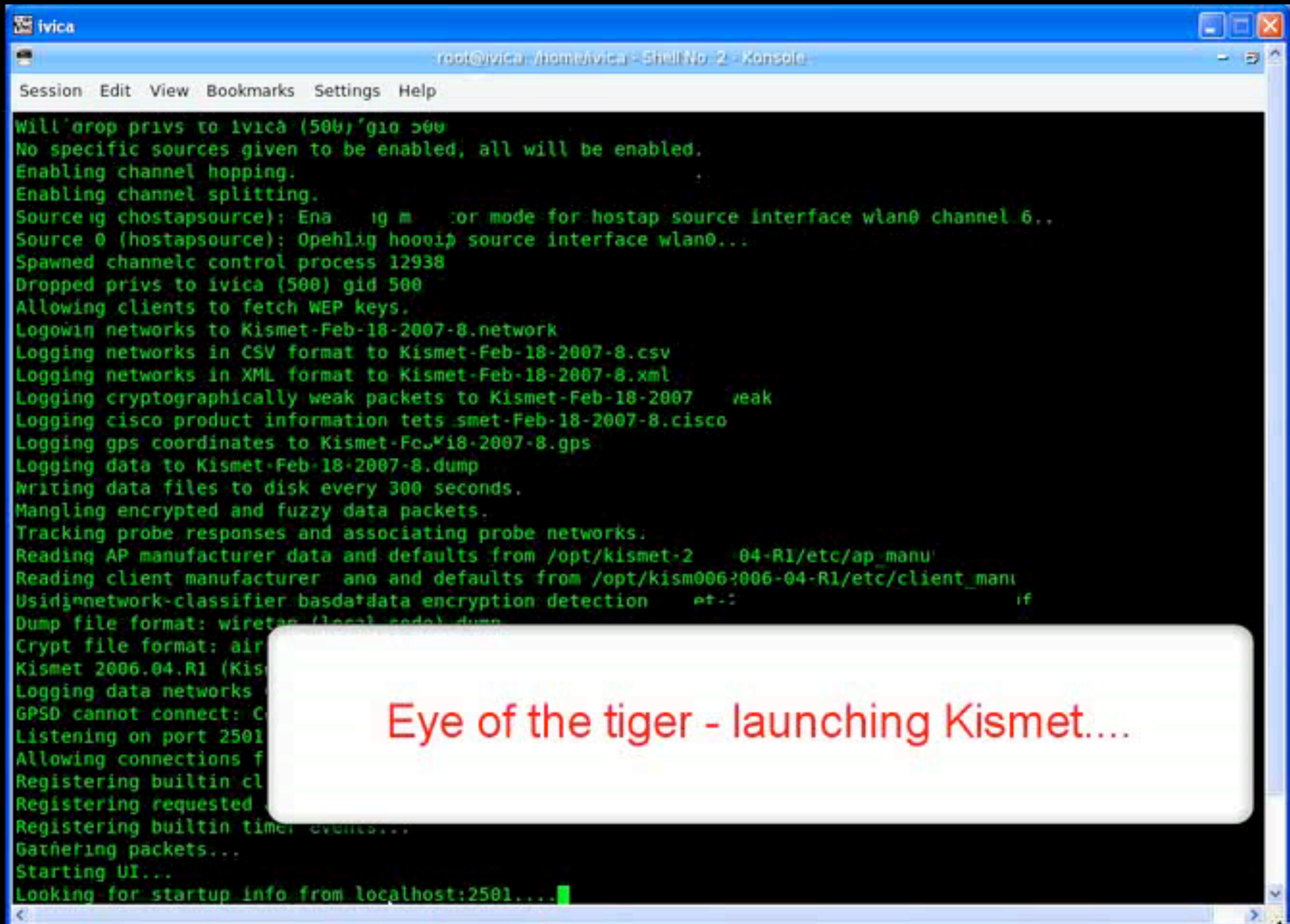
# Kismet in action - part one



# Kismet in action - part two



# Kismet in action - part two



The screenshot shows a terminal window titled 'ivica' with a menu bar (Session, Edit, View, Bookmarks, Settings, Help) and a status bar ('root@ivica: /home/ivica - Shell No. 2 - Konsole'). The terminal displays the following output:

```
Will drop privs to ivica (500) gid 500
No specific sources given to be enabled, all will be enabled.
Enabling channel hopping.
Enabling channel splitting.
Source 0 (hostapsource): Enabling monitor mode for hostap source interface wlan0 channel 6..
Source 0 (hostapsource): Opening hooop source interface wlan0...
Spawned channel control process 12938
Dropped privs to ivica (500) gid 500
Allowing clients to fetch WEP keys.
Logon networks to Kismet-Feb-18-2007-8.network
Logging networks in CSV format to Kismet-Feb-18-2007-8.csv
Logging networks in XML format to Kismet-Feb-18-2007-8.xml
Logging cryptographically weak packets to Kismet-Feb-18-2007-8.weak
Logging cisco product information to Kismet-Feb-18-2007-8.cisco
Logging gps coordinates to Kismet-Feb-18-2007-8.gps
Logging data to Kismet-Feb-18-2007-8.dump
Writing data files to disk every 300 seconds.
Mangling encrypted and fuzzy data packets.
Tracking probe responses and associating probe networks.
Reading AP manufacturer data and defaults from /opt/kismet-2-2006-04-R1/etc/ap_manu
Reading client manufacturer data and defaults from /opt/kismet-2-2006-04-R1/etc/client_manu
Using network-classifier based data encryption detection
Dump file format: wiretap (local code) dump
Crypt file format: air
Kismet 2006.04.R1 (Kismet)
Logging data networks
GPSD cannot connect: C
Listening on port 2501
Allowing connections from
Registering builtin client
Registering requested
Registering builtin timer events...
Gathering packets...
Starting UI...
Looking for startup info from localhost:2501....
```

Eye of the tiger - launching Kismet....



# Bluetooth



## New antenna ups Bluetooth range to 30 Kilometers

Posted by [Joshua Karp](#) on Jul 2, 2007 10:11 am

[2 Comments](#)

Filed in [News](#)



Yeah, you read that right. The newly announced AIRcable Host XR [Bluetooth USB Adapter](#) extends your average 3 meter Bluetooth range to just over 30 Kilometers. How far is that is America, you might ask? Roughly 19 miles. Whoa. Before you all get too excited, you should know that some level of "professional installation" is required to achieve the increased length. Without the pro-level tweaking you'll get 2 kilometers out of the box, which is still pretty impressive. Bluetooth range has been pushed to these lengths before, but the \$129 price point of this particular box makes it one of the first to be in range of the average consumer. Let the games begin!

[Read](#)

**AIRCABLE**

BLUETOOTH WITH RANGE!

PROGRAMMABLE, WIRELESS  
SENSOR INTERFACES &  
DATA LOGGERS WITH RANGE!

**Bluetooth®** WITH RANGE AS FAR  
AS THE EYE CAN SEE...

**UP TO  
30 KM!**

**AIRcable  
Host XR**  
LONG-RANGE  
BLUETOOTH  
"DONGLE"

**AIRcable  
Industrial XR**  
LONG-RANGE  
PROGRAMMABLE  
SENSOR INTERFACE

**AIRcable SMD**  
THE WIRELESS, PROGRAMMABLE  
MICRO-CONTROLLER (W-PLC)



All

Device Oriented Tree View

Device	Type	Address	Manufacturer	# o...	Note	First Seen	Last Seen	F	C	Auth
All Devices										
Computer										
(Local)	Desktop Workstation	00:02:72:C0:6B:49	CC&C Technologie...	2		09:58:00 05/20/2008	09:58:00 05/20/2008			
Phone										
N/A	Mobile phone	00:15:DE:93:EC:BA	Sage Instruments I...	0		09:58:06 05/20/2008	09:58:06 05/20/2008			
Fuzik SAMSU...	Mobile phone	00:17:D5:1B:E7:91		8		09:58:43 05/20/2008	10:04:13 05/20/2008			
K800i (Anomet)	Mobile phone	00:19:63:9D:AD:D6		14		10:02:51 05/20/2008	10:05:06 05/20/2008			
N/A	Mobile phone	00:1C:D6:7C:4B:89		0		10:00:35 05/20/2008	10:02:51 05/20/2008			
N/A	Mobile phone	00:1D:98:56:2A:7F		0		09:59:41 05/20/2008	10:05:06 05/20/2008			
N/A	Mobile phone	00:1E:45:2D:CD:54		0		10:04:13 05/20/2008	10:04:13 05/20/2008			
DuKe E60	Smart phone	00:12:D2:35:8D:99	Perception Digital ...	12		09:58:06 05/20/2008	10:05:06 05/20/2008			
Kuralkan e61i	Smart phone	00:12:D2:9E:AB:BE	Perception Digital ...	13		09:58:06 05/20/2008	10:05:06 05/20/2008			
Milan	Smart phone	00:19:2D:42:EA:01		11		09:58:06 05/20/2008	09:59:41 05/20/2008			
Pawel W/	Smart phone	00:1A:89:0D:1C:14		9		09:58:06 05/20/2008	10:01:17 05/20/2008			
Dodo N73	Smart phone	00:1C:35:66:E3:91		13		10:00:35 05/20/2008	10:01:50 05/20/2008			
Nokia N73	Smart phone	00:1C:35:6A:6A:3A		12		09:58:06 05/20/2008	10:05:06 05/20/2008			

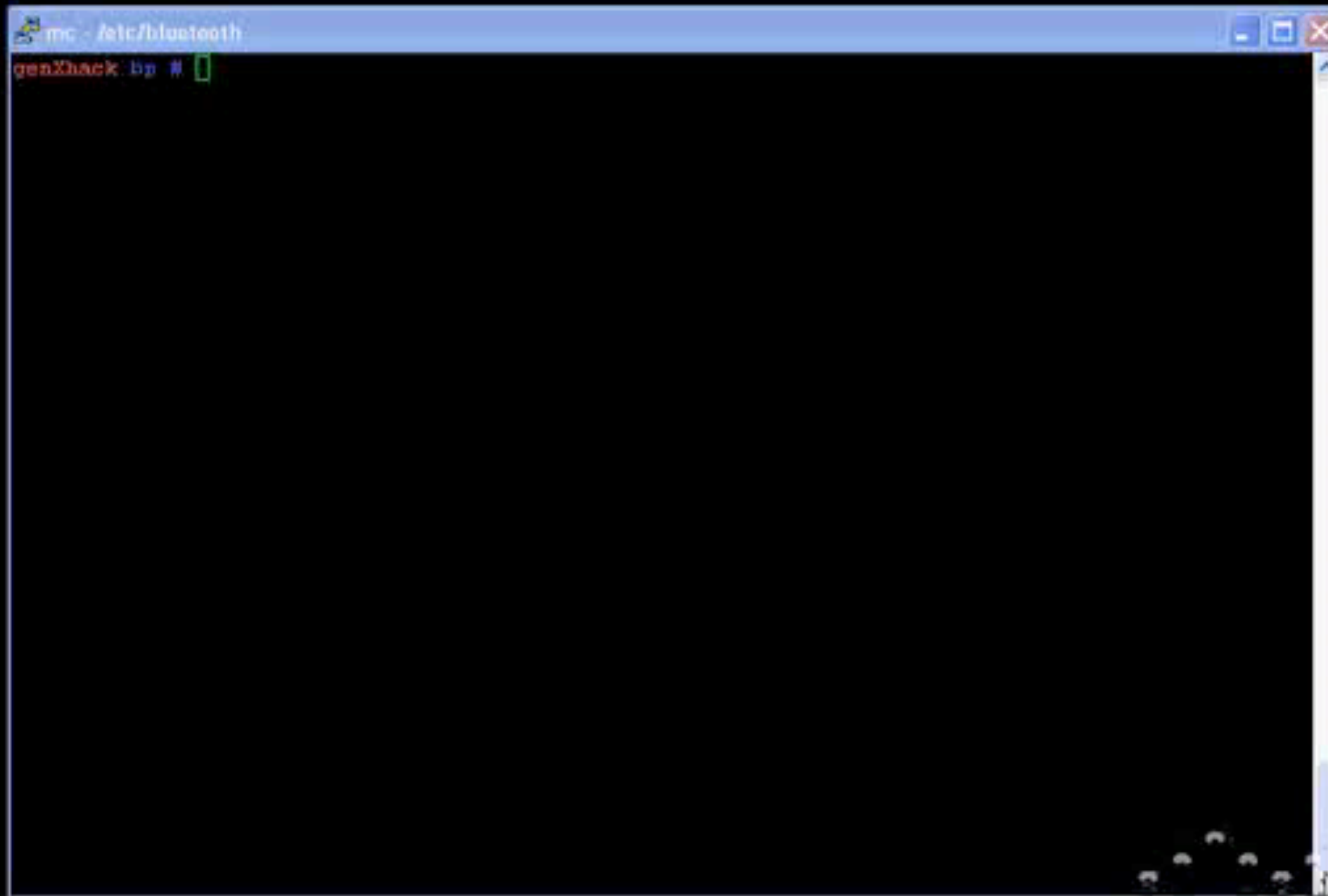
Device Note:

Service Name	Description	Service UUID	First Seen	Last Seen
Limited Service Discovery	SDP Server	0x1000	10:00:51 05/20/2008	10:01:59 05/20/2008
AV Remote Control Target	AVRCP TargetAudio Video ...	0x110C	10:00:51 05/20/2008	10:01:59 05/20/2008
Dial up Networking	Dial-Up Networking	0x1103	10:00:51 05/20/2008	10:01:59 05/20/2008
OBEX Object Push	OBEX Object Push	0x1105	10:00:51 05/20/2008	10:01:59 05/20/2008
Handsfree Audio Gateway	Hands-Free Audio Gateway	0x111F	10:00:51 05/20/2008	10:01:59 05/20/2008
Headset Audio Gateway	Headset Audio Gateway	0x1112	10:00:51 05/20/2008	10:01:59 05/20/2008
Audio Source	Audio Source	0x110A	10:00:51 05/20/2008	10:01:59 05/20/2008
Imaging Repsonder	Imaging	0x111B	10:00:51 05/20/2008	10:01:59 05/20/2008
Unknown	SyncMLClient	0x2	10:00:51 05/20/2008	10:01:59 05/20/2008
OBEX File Transfer	OBEX File Transfer	0x1106	10:00:51 05/20/2008	10:01:59 05/20/2008
Unknown	Nokia OBEX PC Suite Servic...	0x5005	10:00:51 05/20/2008	10:01:59 05/20/2008
Unknown	Nokia SyncML Server	0x5601	10:00:51 05/20/2008	10:01:59 05/20/2008
Unknown	SIM Access	0x112D	10:00:51 05/20/2008	10:01:59 05/20/2008

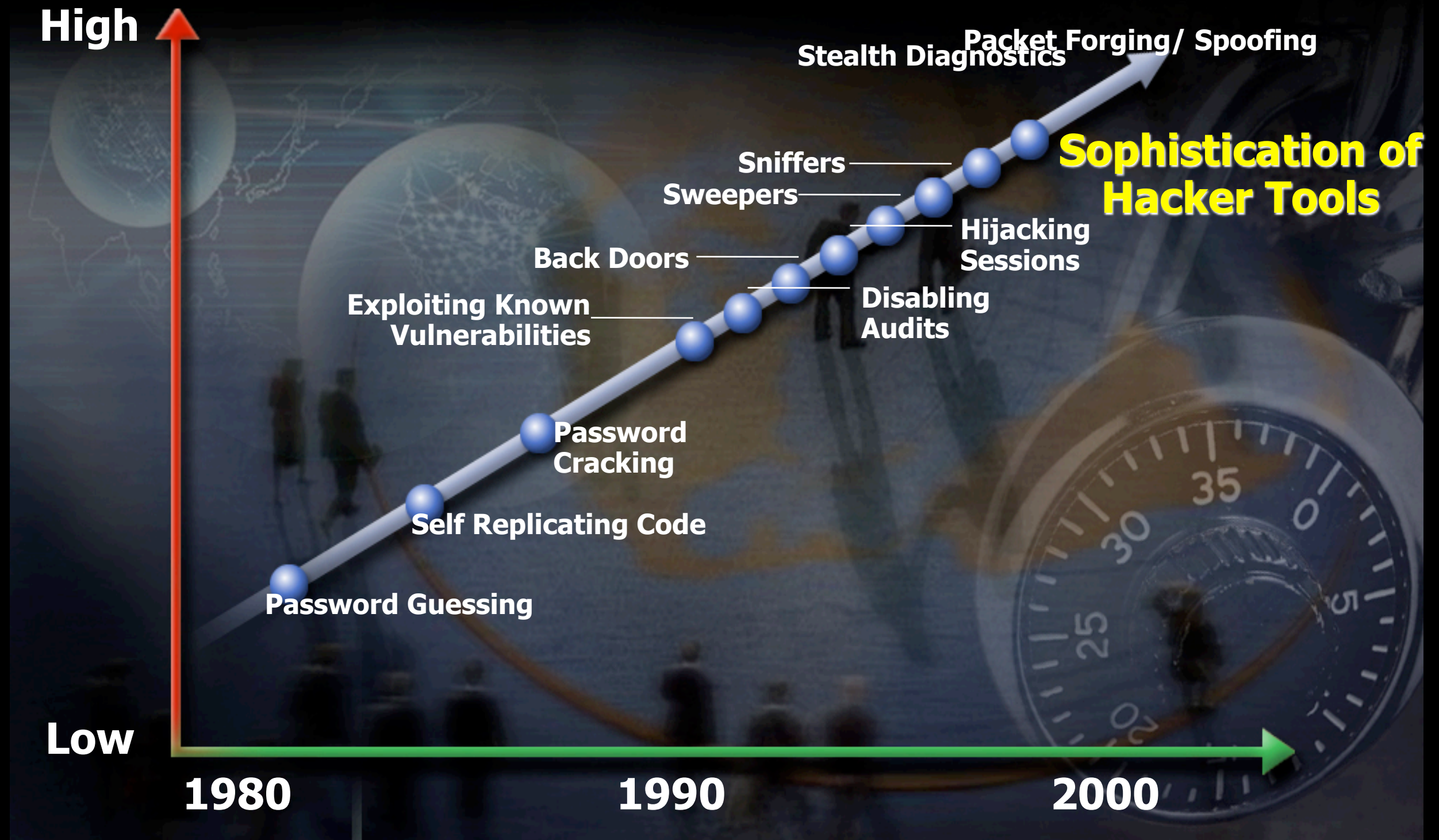


# Small bluetooth example

# Small bluetooth example

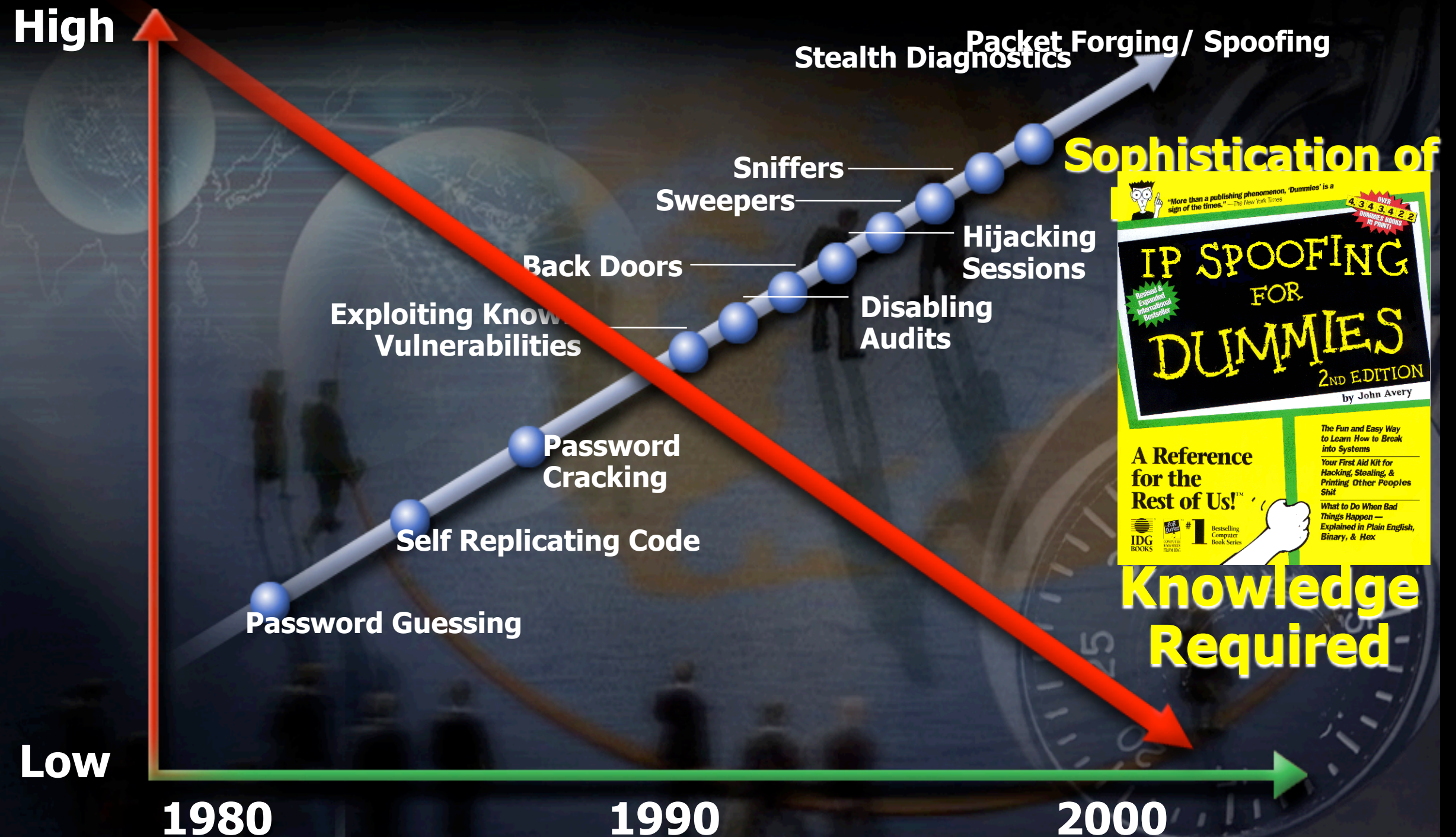


# Roadmap To Hell - Current situation





# Roadmap To Hell - Current situation





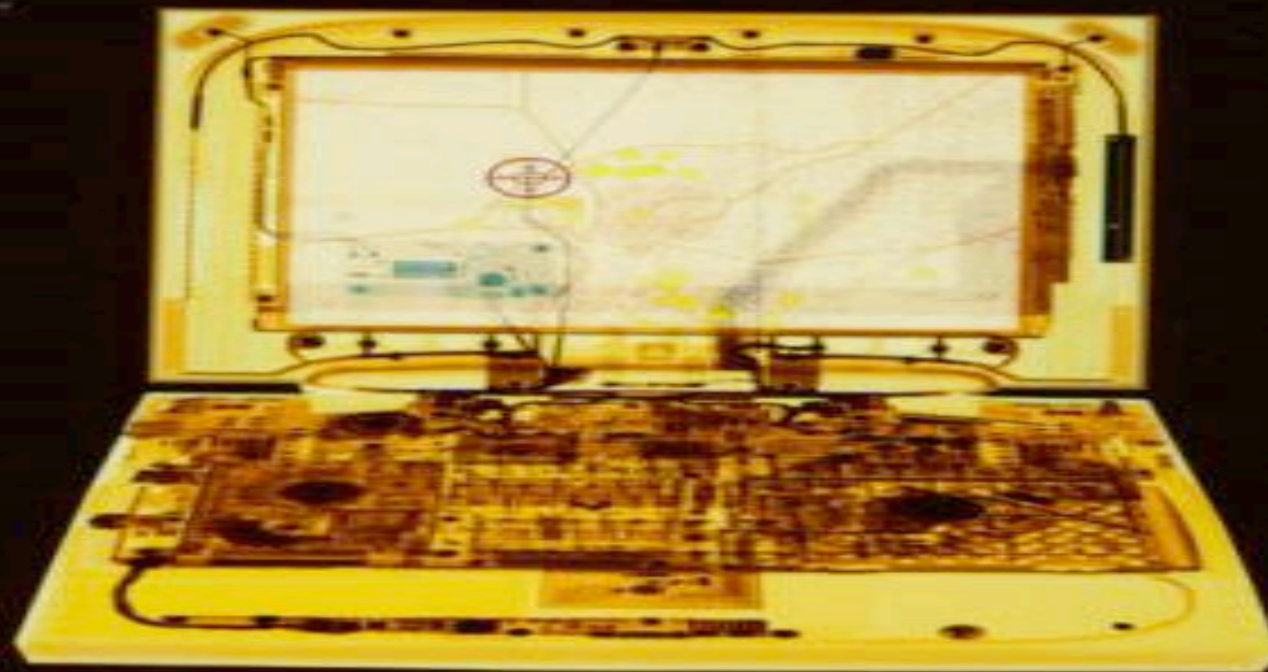
**AND IF YOU THINK THAT IS  
BAD CHECK THIS OUT...**



# The Spy Who Loved Me

Copyrighted Material

## Secrets of **Computer Espionage**



## Tactics and Countermeasures

Copyrighted Material

Joel McNamara



28 August 2005

This combines three lists of MI6 officers published here on [13 May 1999](#) (116 names), [21 August 2005](#) (74 names) and [27 August 2005](#) (121 names).

While none of the 311 names appeared on all three lists, these 35 names appeared on two lists, leaving 276 unique names (\* indicates names listed in the August 2005):

Named 13 May 1999

Named 21 August 2005

Named 27 August 2005

**James Lloyd Baxendale:** 94 Cairo (MECAS), 97 Amman; dob 1967.

**James Lloyd Baxendale:** dob 1967; 94 Cairo, 97 Amman, 99 Brussels, 04 Beirut (1 Sec).\*

**Richard Philip Bridge:** 86 Warsaw, 88 Moscow; dob 1959.

**Richard Philip Bridge:** dob 1959; 86 Warsaw, 89 Moscow, 98 New Delhi, 04 Geneva (Cllr).\*

**George Benedict Joseph P Busby:** 89 Bonn, 92 Belgrade; dob 1960; OBE.

**George Benedict Joseph Pascal Busby:** dob 1960; 89 Bonn, 92 Belgrade, 00 Vienna, 04 London.

**Martin Hugh Clements:** 86 Tehran, 90 Vienna; dob 1961.

**Martin Hugh Clements:** dob 1961; 86 Tehran, 90 Vienna, 98 Bonn, 99 Berlin, 04 Kabul (Cllr).\*

**Peter Salmon Collecot:** 80 Khartoum, 82 Canberra, 93 Jakarta; dob 1950.

**Peter Salmon Collecott:** dob 1950; 85 Khartoum, 82 Canberra, 89 Jakarta, 94 Bonn, 04 Brasilia.\*

**Sherard Louis Cowper-Coles:** 80 Cairo, 87 Washington; dob 1955; CMG, LVO.

**Sherard Louis Cowper-Coles:** dob 1955; 80 Cairo, 87 Washington, 97 Paris, 01 Tel Aviv, 03 Riyadh.\*

**John Martin Jamie Darke:** 88 Cairo, 96 Dubai; dob 1953.

**John Martin Jamie Darke:** dob 1953; 88 Cairo, 96 Dubai, 03 Lisbon (Cllr).\*

**Michael Hayward Davenport:** 89 Warsaw, 96 Moscow; dob 1961.

**Michael Hayward Davenport:** dob 1961; 90 Warsaw, 96 Moscow, 00 Warsaw, 04 Cairo (DHM).\*

**Robert Dominic Russell Fenn:** 85 Hague, 88 Lagos, 92 New York; dob 1962.

**Robert Dominic Russell Fenn:** dob 1962; 85 Hague, 88 Lagos, 92 New York, 97 Rome, 04 Nicosia (DHM).\*

**Kevin Andrew Garvey:** 81 Bangkok, 85 Hanoi, 92 Phnom Penh; dob 1960.

**Kevin Andrew Garvey:** dob 1960; 81 Bangkok, 85 Hanoi, 92 Phnom Penh, 93 Grand Turks, 01 Guatemala City (DHM).\*



# TIMESONLINE



“Dogs love whoever happens to feed them” Jeremy Clarkson

Send your views

NEWS COMMENT BUSINESS SPORT LIFE & STYLE ARTS & ENTERTAINMENT LUXX OUR PAPERS AUDIO / VIDEO JOBS & CLASSIFIEDS

MARKETS ECONOMICS INDUSTRY SECTORS COLUMNISTS MOVERS & SHAKERS MONEY LAW ENTREPRENEUR RELATED REPORTS

Where am I? Home Business Industry Sectors Technology

SEARCH

From The Times

SHOP MY PROFILE SITEMAP

December 1, 2007

## MI5 alert on China's cyberspace spy threat

Exclusive: director-general of MI5 sends letter to British companies warning systems are under attack from China



Jonathan Evans sent a confidential letter to 300 chief executives and security chiefs at banks, accountants and legal firms

Rhys Blakely, Jonathan Richards, James Rossiter and Richard Repton

### EXPLORE INDUSTRY SECTORS

- > BANKING & FINANCE
- > CONSTRUCTION & PROPERTY
- > CONSUMER GOODS
- > ENGINEERING
- > HEALTH
- > INDUSTRIALS
- > LEISURE
- > MEDIA
- > NATURAL RESOURCES
- > RETAILING
- > SUPPORT SERVICES

MOST READ

MOST COMMENTED

MOST CURIOUS

TODAY

- > Britons kidnapped in Iraq are 'held by...
- > Babies seized by Robert Mugabe's forces as...
- > Kim Jong-il builds...
- > Rich List reveals wealthy reap profits under...

TIMESONLINE

The Times Law 100:  
Britain's most  
powerful lawyers



Search

Reg Hardware

Reg Developer

Channel Register

Whitepapers

News Tools

Newsletters & Feeds

Reg Mobile

Reg Desktop News Alerts

Reg Shops

Reg Merchandise

Books/Online Learning

Top Stories

Top Rated

- Eye-o-Sauron™ border beam barrier tech too crap to keep
- Home Office defends 'dangerously misleading' Phorm thumbs-up
- Brain-plug weapons could provide war crime immunity
- UK Reaper drone wrecked in

[The Register](#) » [Public Sector](#) » [Government](#) »

# Department of Homeland Security website hacked!

Infected by massive attack sweeping the net

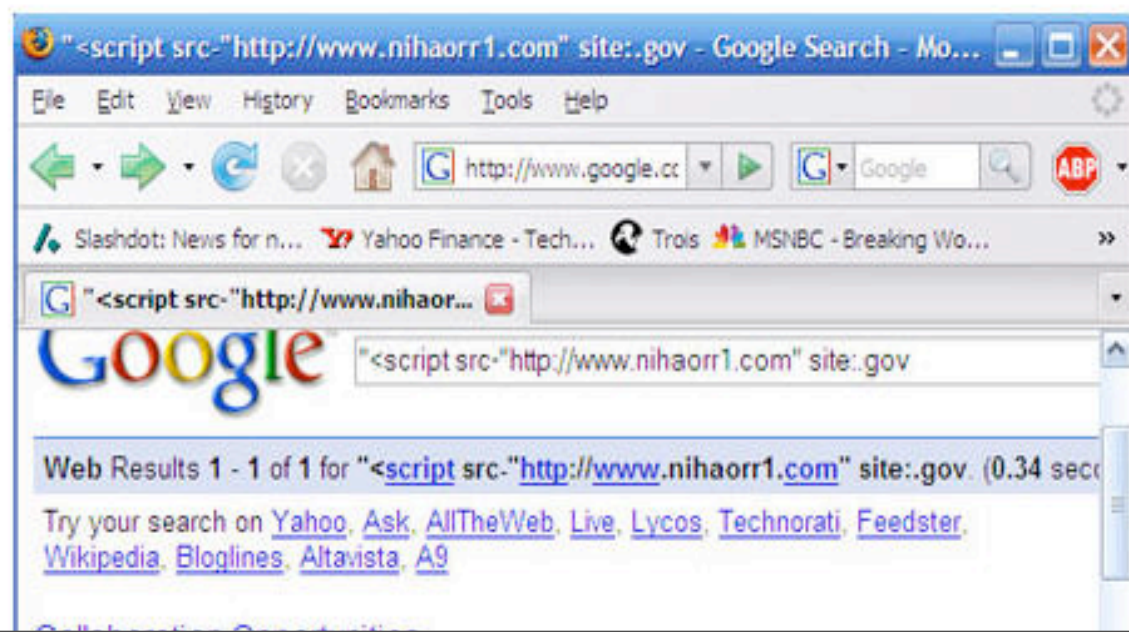
By [Dan Goodin](#) → [More by this author](#)

Published Friday 25th April 2008 18:57 GMT

[See what the experts have to say on attracting, retaining and developing IT talent](#)

The sophisticated mass infection that's injecting attack code into hundreds of thousands of reputable web pages is growing and even infiltrated the website of the Department of Homeland Security.

While so-called SQL injections are nothing new, this latest attack, which we [we reported earlier](#), is notable for its ability to infect huge numbers of pages using only a single string of text. At time of writing, Google searches [here](#), [here](#) and [here](#) showed almost 520,000 pages containing the infection string, though the exact number changes almost constantly. As the screenshot below shows, even the DHS, which is responsible for protecting US infrastructure against cyber attacks, wasn't immune. Other hacked sites include those belonging to the United Nations and the UK Civil Service.





# Web infection attacks more than 100,000 pages

UK Civil Service, UN and EPA among the plagued

By [Dan Goodin in San Francisco](#) → [More by this author](#)

Published Thursday 24th April 2008 00:51 GMT

[Find out how to eradicate 99.7% of spam](#)

Hackers have injected malicious code into hundreds of thousands of reputable web pages, turning them into launchpads for attacks that silently install malware on the machines of those who visit them. The UK's Civil Service and the United Nations were among those who had been hacked.

This [Yahoo search](#) returned 173,000 results for the term "nihaorr1," which is part of the address that uses a malicious javascript to attack end users. The rogue URL horns its way onto web pages through a SQL injection vulnerability in IIS and possibly other web servers, according to IT-related web forums.

Websense, which [wrote about the mass infection](#) Tuesday, said the attackers perpetrated a similar assault a few weeks ago on news and travel sites. Little is known about the group responsible, except that they're using the nihaorr1.com domain name, which [appears](#) on the surface to be registered to someone in Shanghai.

Users visiting an infected site will be redirected to a series of sites that eventually tries to exploit eight different vulnerabilities, all of which have been patched.

We've written plenty about vulnerabilities in browsers, media players and other types of software that are triggered only after the mark visits a website under the control of the attacker. Almost inevitably, a *Reg* reader comments that only a fool would be drawn to such a place. As mass infections like this one make clear, anyone who visits pages belonging to well-known news and travel sites, the United Nations or governmental agencies on either side of the Atlantic is susceptible.

So if you haven't patched that old version of iTunes or AIM in a while, now might a good time. ®



in-depth summary of Nation2Nation Cyber conflicts and developments I recommend you to read in case you're interested. It covers China, India, Iran, North Korea, Pakistan, and, of course, Russia. Some selected brief excerpts on China, Iran, and Russia :

## China

*"Beijing's intelligence services continue to collect science and technology information to support the government's goals, while Chinese industry gives priority to domestically manufactured products to meet its technology needs. The PLA maintains close ties with its Russian counterpart, but there is significant evidence that Beijing seeks to develop its own unique model for waging cyber warfare."*

## Iran

*"The armed forces and technical universities have joined in an effort to create independent cyber R & D centers and train personnel in IT skills; and second, Tehran actively seeks to buy IT and military related technical assistance and training from both Russia and India."*

## Russia

*"Russia's armed forces, collaborating with experts in the IT sector and academic community, have developed a robust cyber warfare doctrine. The authors of Russia's cyber warfare doctrine have disclosed discussions and debates concerning Moscow's official policy. "Information weaponry," i.e., weapons based on programming code, receives paramount attention in official cyber warfare doctrine."*

Technology as the next Revolution in Military Affairs (RMA) was inevitable

**Sun, Sep 2 2007 - 11:21 AM**

## Sick Kids doctor loses data on 3,300 patients

Six weeks after Ontarios privacy commissioner ordered the Hospital for Sick Children not to remove electronic health records from the hospital, a doctor lost an external hard drive containing such re...

**Sun, Sep 2 2007 - 11:06 AM**

## Electoral Page Linked To Pxxx Site

Residents who tried to sign up to an online electoral roll have instead been diverted to a "Wild Girls" pxxx site. Sedgemoor District Council in Somerset sent out letters to every household urging peo...

**Sun, Sep 2 2007 - 11:03 AM**

## State officials report theft of laptop containing personal informa...

Maryland officials say a laptop computer containing personal information on people with state licenses has been stolen. The Maryland Department of the Environment says the laptop was stolen from a veh...

**Sun, Sep 2 2007 - 11:02 AM**

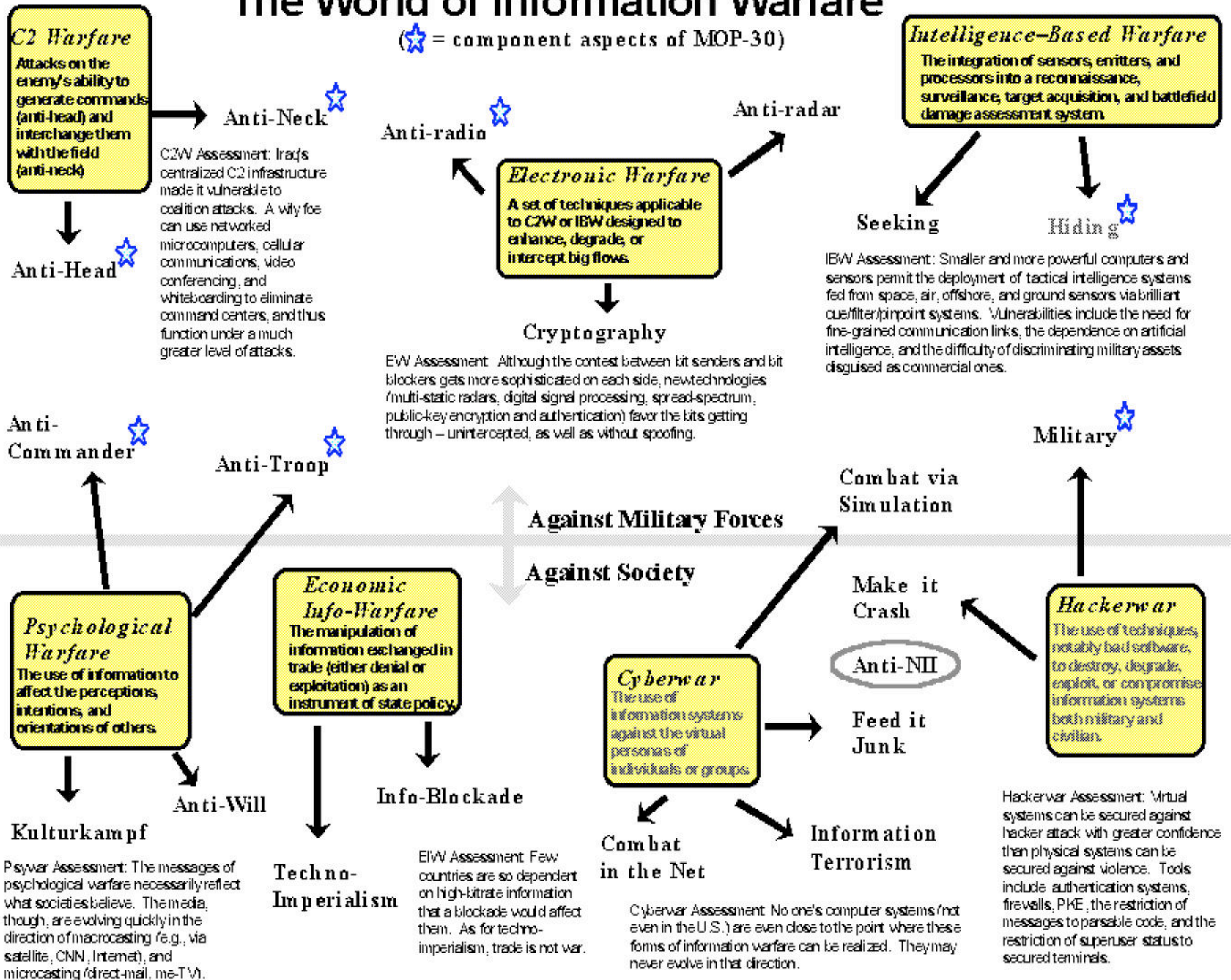
## Major Computer Viruses Over 25 Years

Major computer viruses over the last 25



# The World of Information Warfare

(★ = component aspects of MOP-30)





## In Pictures: America's Hackable Backbone

Read the full story [Andy Greenberg](#)

[E-mail](#) [Create Alerts](#)



Speed - +



© iStock

### Dams

In 2002, *The Washington Post* reported that a 12-year-old had unwittingly hacked into Arizona's Roosevelt Dam and gained full control over its systems. That report turned out to be almost completely apocryphal. In fact, IBM's Scott Lunsford says that a hacker in control of a major dam likely wouldn't be able to destroy the dam or cause major floods. But Lunsford does warn that an intruder could cut off the dam's relatively small supply of hydroelectric power or, more important, disrupt the flow of water the dam pumps from deep within reservoirs to cool reactors at other power plants.



## In Pictures: America's Hackable Backbone

Read the full story [Andy Greenberg](#)

[E-mail](#) [Create Alerts](#)



Speed - +



© Scott Olson/Getty Images

### Water Distribution

In 2000, 48-year-old Vitek Boden was arrested for hacking into the control systems of Hunter Watertech, an Australian water-treatment facility from which he'd been laid off. Boden was found to have gained control of the system 46 times, dumping sewage into parks and rivers so that the company would re-hire him to solve the problem. TippingPoint's Ganesh Devarajan imagines an even scarier water-based scenario, in which a dirty bomb is planted in a water supply and SCADA systems are hacked to prevent detection.



# In Pictures: America's Hackable Backbone

[Read the full story](#) [Andy Greenberg](#)

[E-mail](#) [Create Alerts](#)



Speed - +



© AP Photo/FirstEnergy Nuclear

## Power Plants

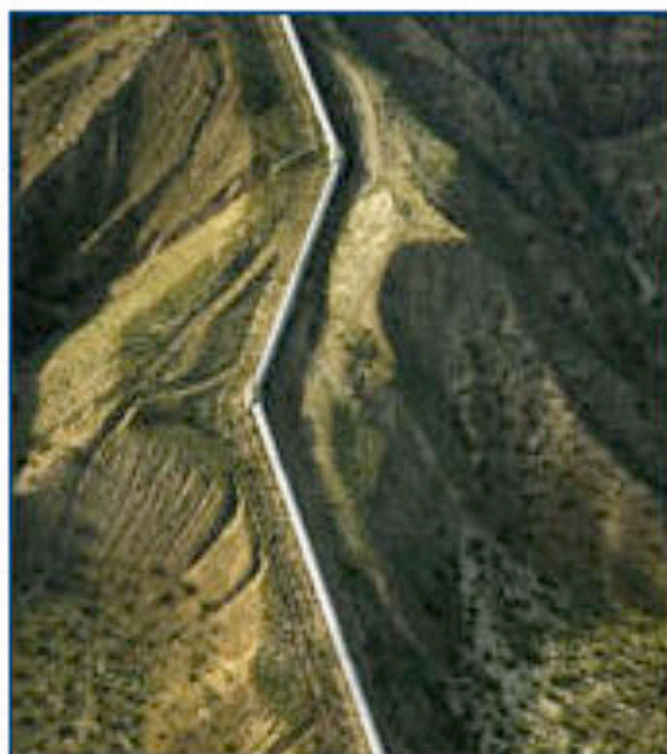
Scott Lunsford of IBM's Internet Security Systems argues that it would be nearly impossible to hack into a nuclear power plant and trigger a meltdown, thanks to certain safeguards. Causing a major blackout, however, is much easier. In fact, computer worms hamstrung SCADA power systems twice in 2003. In the first case, the Slammer worm infected computers at the Davis-Besse nuclear power plant in Ohio, causing millions to lose power. Seven months later, the Blaster worm was suspected of causing downtime in a power plant's detection systems, leading to prolonged blackouts in parts of New York State.



## Security

# America's Hackable Backbone

Andy Greenberg, 08.22.07, 6:00 PM ET



In Pictures: America's Hackable Backbone

By This Author

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.'"

[Make Forbes.com My Home Page](#) [Bookmarks](#)

[Find Free Wi-Fi Hotspots](#)

**News by E-mail** Get stories by E-Mail on this to

### Companies

☐ Siemens

☐ Rockwell Auto

☐ ABB

☐ COMS

### Topics

☐ Security

☐ Software

☐ SCADA

☐ Infrastructure

[Become a member FREE](#)

[Already a Member?](#)

Enter E-Mail Address

Select Your Title



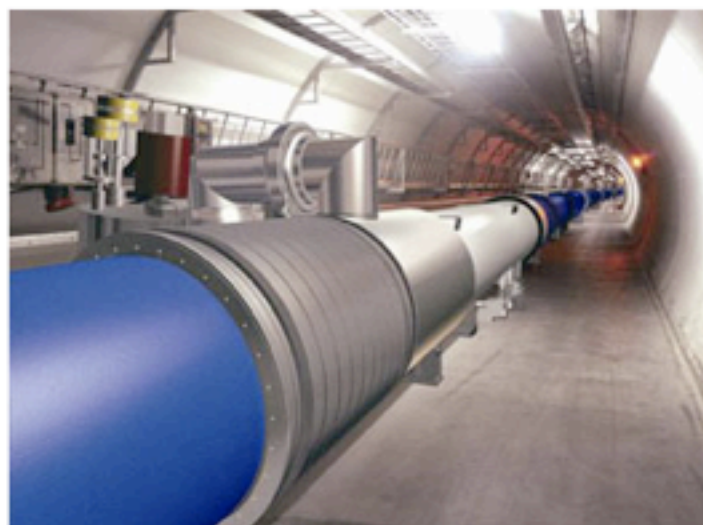


Sep 12, 2008 03:32 PM in [Physics](#) | [5 comments](#) | [Post a comment](#)

## Hackers attack Large Hadron Collider computers to prove they're vulnerable

[Larry Greenemeier](#)

SHARE 2 diggs [digg it](#) [NT](#) [b](#) [f](#) [ShareThis](#) EMAIL PRINT TEXT SIZE: - +



As the first particles began circulating in the [Large Hadron Collider](#) (LHC) this week, a group of hackers calling themselves the "Greek Security Team" penetrated computer systems inside [CERN's](#) Geneva, Switzerland, facility, where the world's biggest particle accelerator is housed, the [Telegraph.co.uk](#) reported today.

The hackers were reportedly targeting the Compact Muon Solenoid Experiment (CMS), a device in Cessy, France, built to [monitor a wide range of particles and phenomena](#) produced in high-energy collisions in the LHC. The 12,500-ton detector's different layers (weighing, according to CERN, as much as 30 jumbo jets or 2,500 African elephants) stop and measure the different particles, and use this data to form a picture of events at the heart of the collision. Scientists plan to use the info to help answer questions about what the

university is really made of and what forces act within it.

On Wednesday, as the LHC was revving up, CMS engineers searched computers for half a dozen files uploaded by the hackers. The interlopers accessed the computer that monitors the CMS software system as the CMS collects data during particle collisions.

CERN scientists says no harm was done but that the break-in raises security concerns, given that intruders were able to penetrate so close to the CMS's computer control system, according to the [Telegraph.co.uk](#). In other words, the hackers came *this* close to being able to switch off some CMS controls.

"We are 2600 - dont mess with us. (sic)," the group warned in a message to CERN engineers. The "2600" refers to a U.S. magazine published quarterly that appeals to the hackers worldwide by publishing technical information about

### ABOUT 60-SECOND SCIENCE

60-Second Science is Scientific American's news blog, offering reporting and analysis on science and technology. Write to us with tips or comments at [blog@sciam.com](mailto:blog@sciam.com).

We're also:

- ▶ A weekly video roundup: [The Monitor](#)
- ▶ A daily podcast: [60-Second Science](#)
- ▶ A weekly podcast: [60-Second Psych](#)
- ▶ A RSS feed [and](#) a Twitter feed

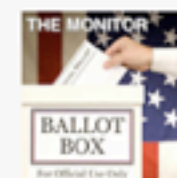
### 60-SECOND SCIENCE VIDEO

[VIEW VIDEO](#)



#### The Monitor: In the Dark about White Matter No More

A train that doesn't even stop in Willoughby; Extinction rock; and more...

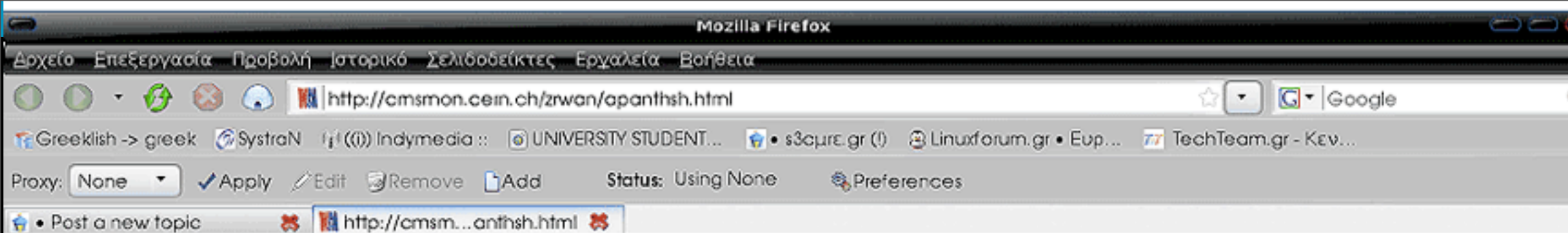


#### The Monitor: Episode 15

Voters who know their place; Chilling evidence of rapid climate meltdown; Humans to galaxy: "We're here!" via golden plaques and snack food; and DNA self-sequencing kit marketers parse "lab test"

Check out previous episodes of [The Monitor](#). Subscribe to this video podcast via [iTunes](#) or [RSS](#)





10/09/08 03:00

Αυτήν την ώρα γίνεται η απόπειρα πειράματος στο CERN.

Ο λόγος που διαλέξαμε αυτή τη σελίδα είναι για να σας θυμίζουμε μερικά πράγματα.

Δεν έγινε βάση κάποιας προσωπικής μας αντιπαράθεσης με την ομάδα διαχείρισης του CERN αλλά με βάση την μεγάλη επισκεψιμότητα που θα αποκτήσει τα επόμενα 24ωρα ο συγκεκριμένος διαδικτυακός τόπος λόγω του πειράματος.

Μερικά στοιχεία απ' τη βάση :

```
USERNAME USER_ID CREATED
SYS 0 2008-02-18 16:19:25.0
SYSTEM 5 2008-02-18 16:19:25.0
OUTLN 11 2008-02-18 16:19:28.0
DIP 19 2008-02-18 16:21:17.0
TSMSYS 21 2008-02-18 16:23:27.0
DBSNMP 24 2008-02-18 16:24:25.0
WMSYS 25 2008-02-18 16:24:53.0
EXFSYS 34 2008-02-18 16:27:55.0
XDB 35 2008-02-18 16:28:04.0
PDB_ADMIN 46 2008-02-18 17:26:32.0
GLEGE 49 2008-02-19 10:13:07.0
PDBMON 45 2008-02-18 17:25:24.0
BALYS 44 2008-02-18 17:25:24.0
USERMON 48 2008-02-18 17:59:26.0
..etc...etc....
```

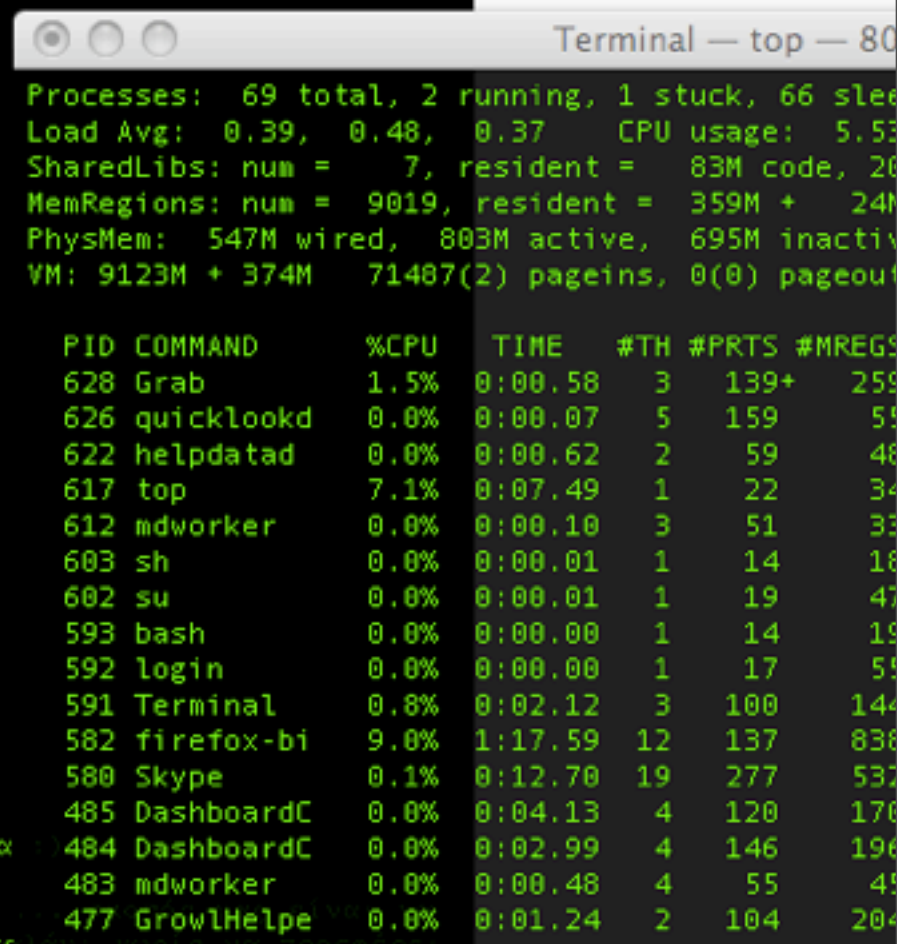
Μερικά emails :

burk\*\*t@fnal.gov  
zr\*\*n@fnal.gov

Τα \*\* απλά μπήκαν για να μην εκθέσουμε κόσμο ο οποίος δεν μας φταίει σε τίποτα

Όπως γράψαμε και στον πρόλογο δεν έχουμε σκοπό να χαλάσουμε το σύστημα ή να καταστρέψουμε το site  
δείξουμε την έμπρακτη αντίδραση μας σε πολλά μέλη της "ενεργής???" GHS η οποία έχει καθαλήσει το καλό...

Χαζές κλίκες απλά δημιουργούνται μόνο και μόνο για να τραμπουκίζουν λεκτικά ή με αποκλεισμούς από κανάλια του irc άτομα τα











# GONE IN 60 SECONDS

# GONE IN 60 SECONDS

What can be hacked and how?



# Traffic control?

# Traffic control?



# Bridge?



# Bridge?



# Train station?

# Train station?







92.168.2.16 - Remote Desktop

CPU Usage

2%

PF Usage

403 MB

CPU Usage History

Page File Usage History

Totals

Handles	12131
Threads	759
Processes	82

Physical Memory (K)

Total	2095536
Available	1564024
System Cache	542492

Commit Charge (K)

Total	413488
Limit	5080236
Peak	480076

Kernel Memory (K)

Total	100312
Paged	52204
Nonpaged	48108

Processes: 82    CPU Usage: 2%    Commit Charge: 403M / 4961M

root@ivica: /temp

[root@ivica temp]#

```

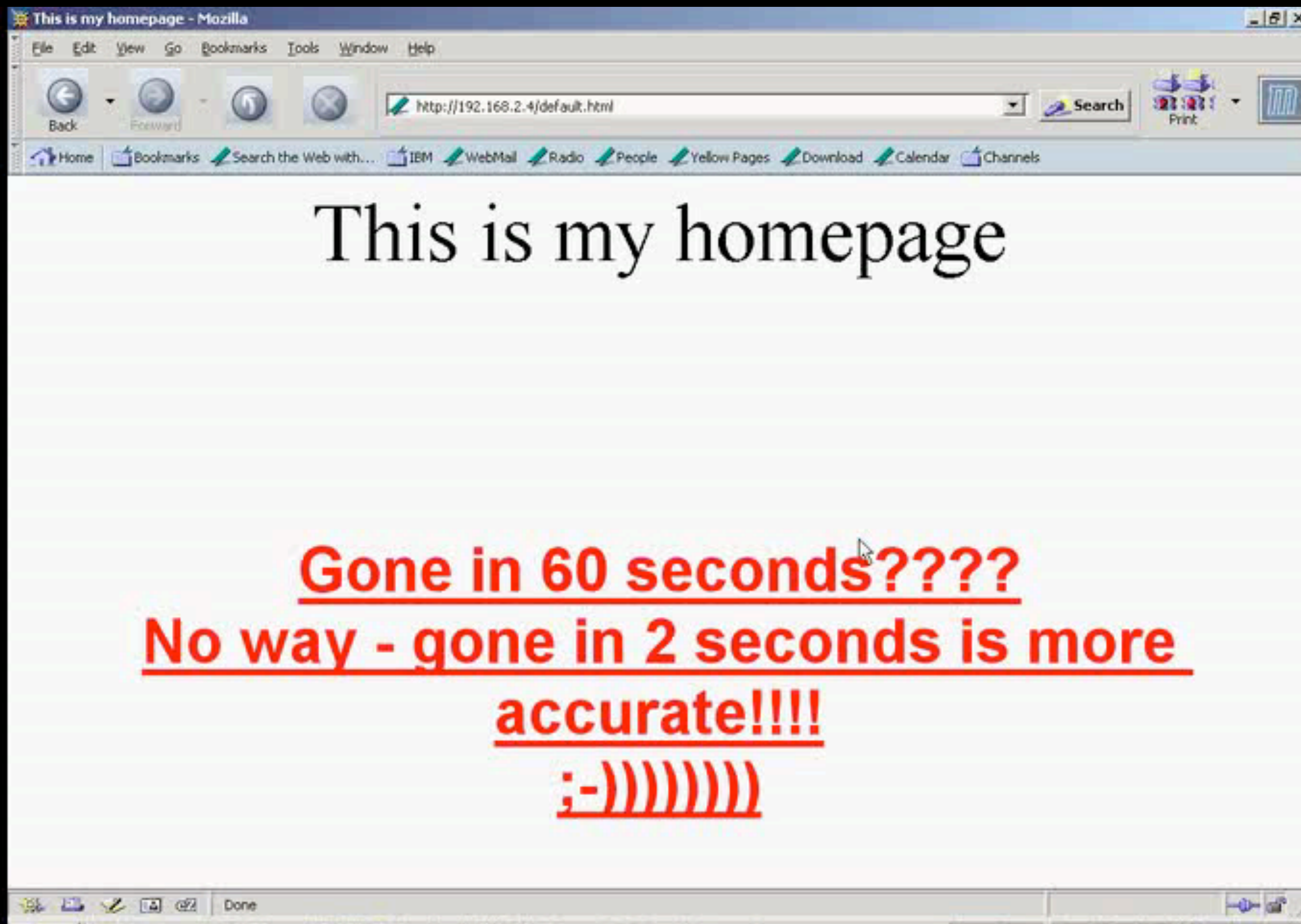
oly from 192.168.2.2: bytes=32 time<1ms TTL=128
Timestamp: 192.168.2.2 : 48087188
oly from 192.168.2.2: bytes=32 time<1ms TTL=128
Timestamp: 192.168.2.2 : 48088180
oly from 192.168.2.2: bytes=32 time<1ms TTL=128
Timestamp: 192.168.2.2 : 48089181
oly from 192.168.2.2: bytes=32 time<1ms TTL=128
Timestamp: 192.168.2.2 : 48090183
oly from 192.168.2.2: bytes=32 time<1ms TTL=128
Timestamp: 192.168.2.2 : 48091184
oly from 192.168.2.2: bytes=32 time<1ms TTL=128
Timestamp: 192.168.2.2 : 48092186
oly from 192.168.2.2: bytes=32 time<1ms TTL=128
Timestamp: 192.168.2.2 : 48093187

54 bytes from 192.168.2.16: icmp_seq=409 ttl=128 time=0.275 ms
54 bytes from 192.168.2.16: icmp_seq=410 ttl=128 time=0.203 ms
54 bytes from 192.168.2.16: icmp_seq=411 ttl=128 time=0.200 ms
54 bytes from 192.168.2.16: icmp_seq=412 ttl=128 time=0.266 ms
54 bytes from 192.168.2.16: icmp_seq=413 ttl=128 time=0.206 ms

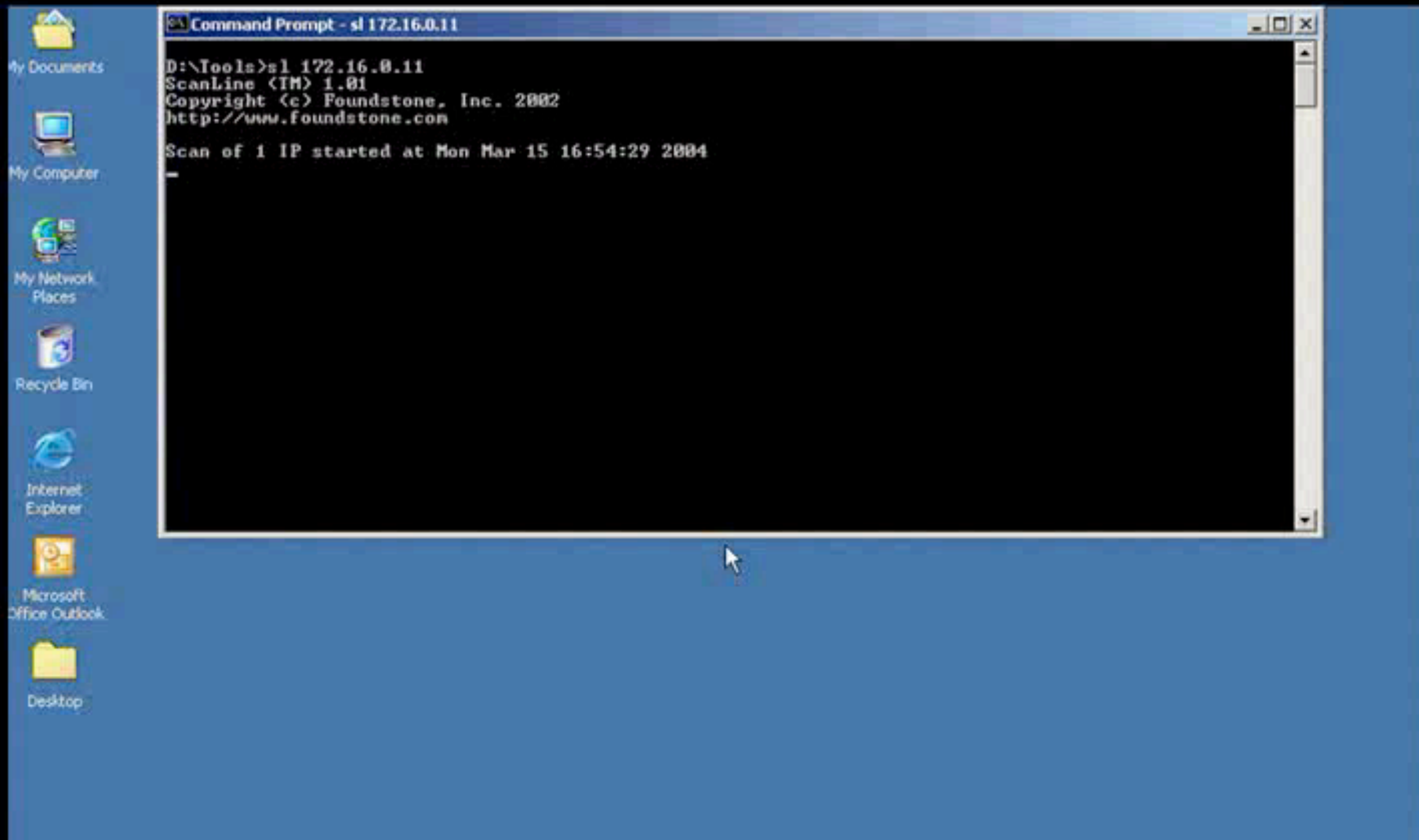
```





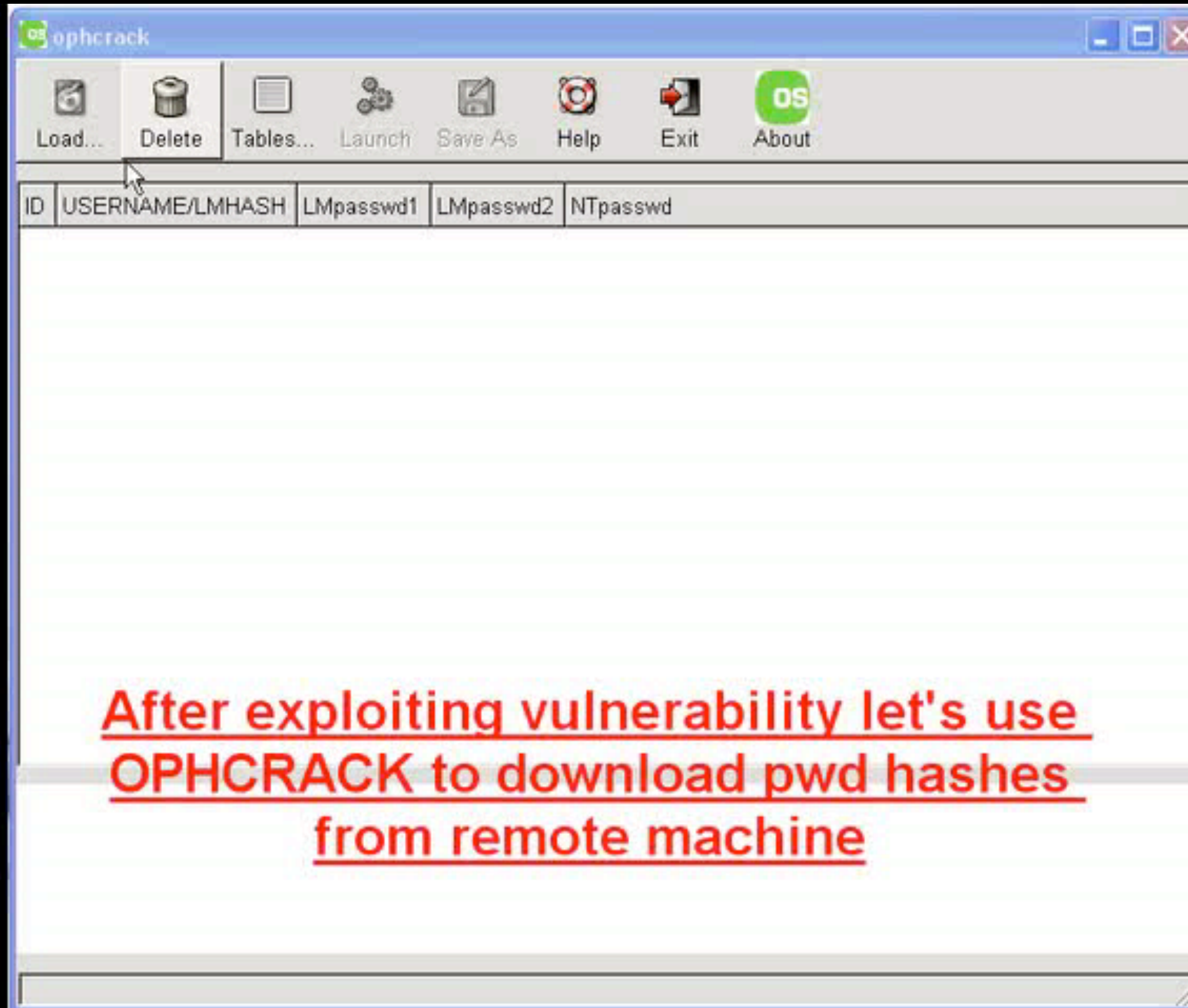












After exploiting vulnerability let's use  
OPHCRACK to download pwd hashes  
from remote machine





Metasploit Framework Web Console v2.3 - Mozilla Firefox












File Edit View Go Bookmarks Tools Help Partly Cloudy, 8°C 16°C 7°C 17°C 8°C 16°C 5°C 18°C 5°C 20°C 7°C

http://127.0.0.1:55555/ Go

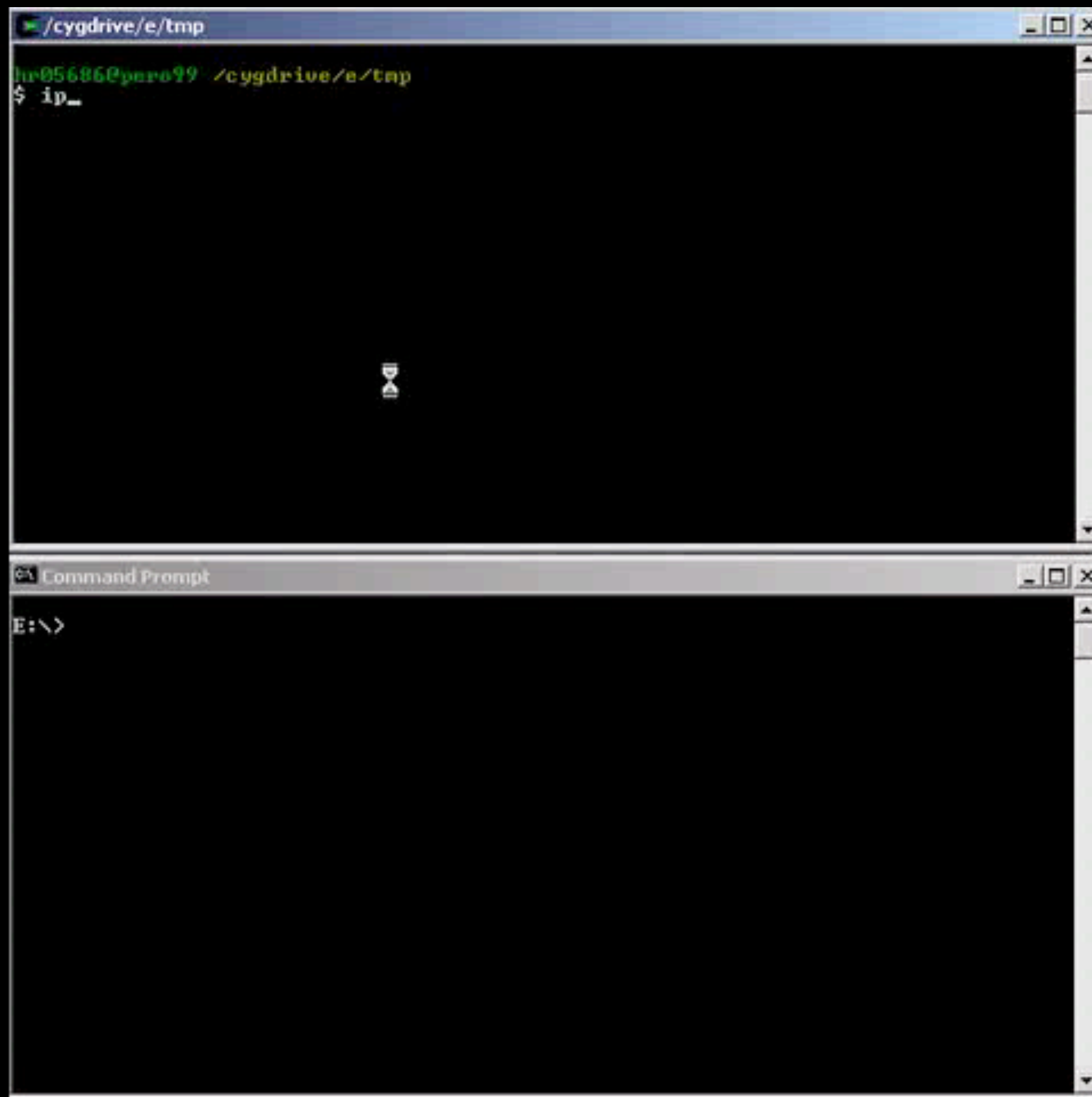
IBM Business Transf... IBM Internal Help Ho... IBM Standard Softw... Search the Web wit...

Disable CSS Forms Images Information Miscellaneous Outline Resize Validation View Source Options

— Architecture — Filter Modules

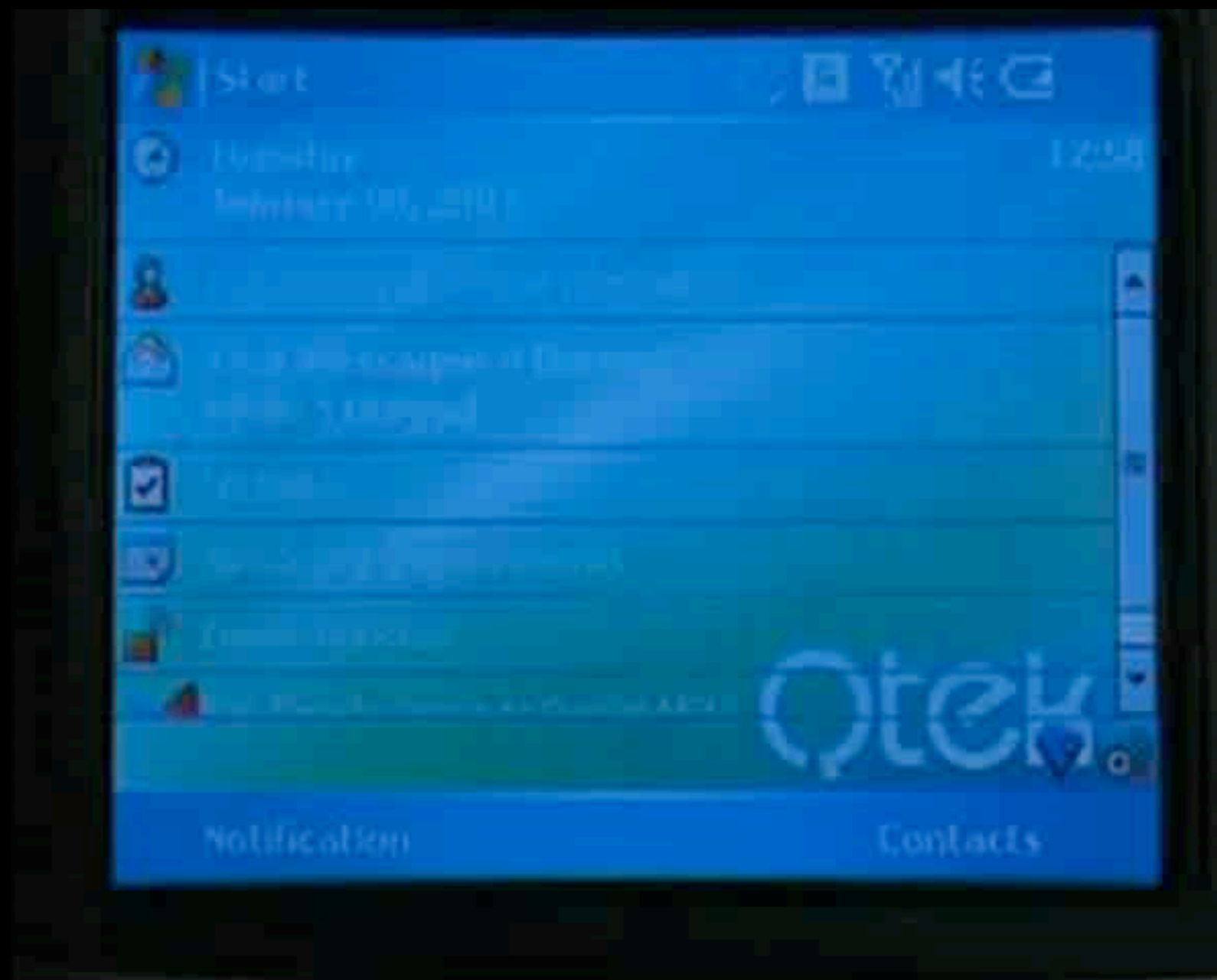
	3Com 3CDaemon FTP Server Overflow
	AOL Instant Messenger goaway Overflow
	Apache Win32 Chunked Encoding
	AppleFileServer LoginExt PathName Overflow
*	Arkeia Backup Client Remote Access
	Arkeia Backup Client Type 77 Overflow (Mac OS X)
	Arkeia Backup Client Type 77 Overflow (Win32)
	CA BrightStor Discovery Service Overflow
	CA BrightStor Discovery Service SERVICEPC Overflow
	CA BrightStor Universal Agent Overflow
	CA License Client GETCONFIG Overflow
	CA License Server GETCONFIG Overflow















Linux - [Ctrl-Alt-F1] - VMware Workstation

File Power Settings Devices View Help

Power Off Power On Suspend Reset Full Screen

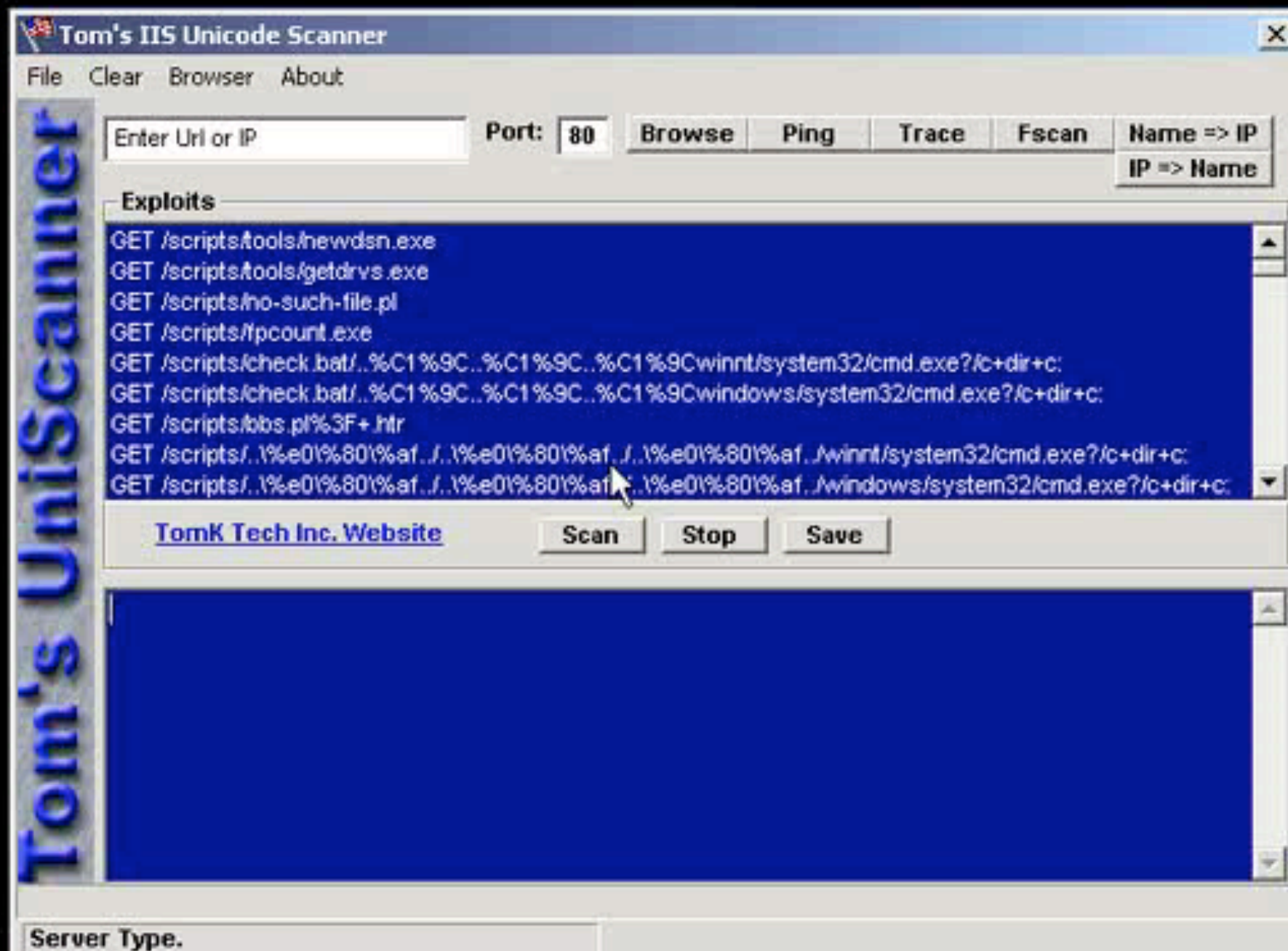
```
-- press any key>
--- Main Menu --- rcvpkt 3638, free/alloc 63/64 -----
l/w/r) list/watch/reset connections
u)      host up tests
a)      arp/simple hijack (avoids ack storm if arp used)
s)      simple hijack
d)      daemons rst/arp/sniff/mac
o)      options
x)      exit
->
hunt: possible ACK storm: 0) 10.0.0.101 [3293] --> 200.1.1.78 [23]
```





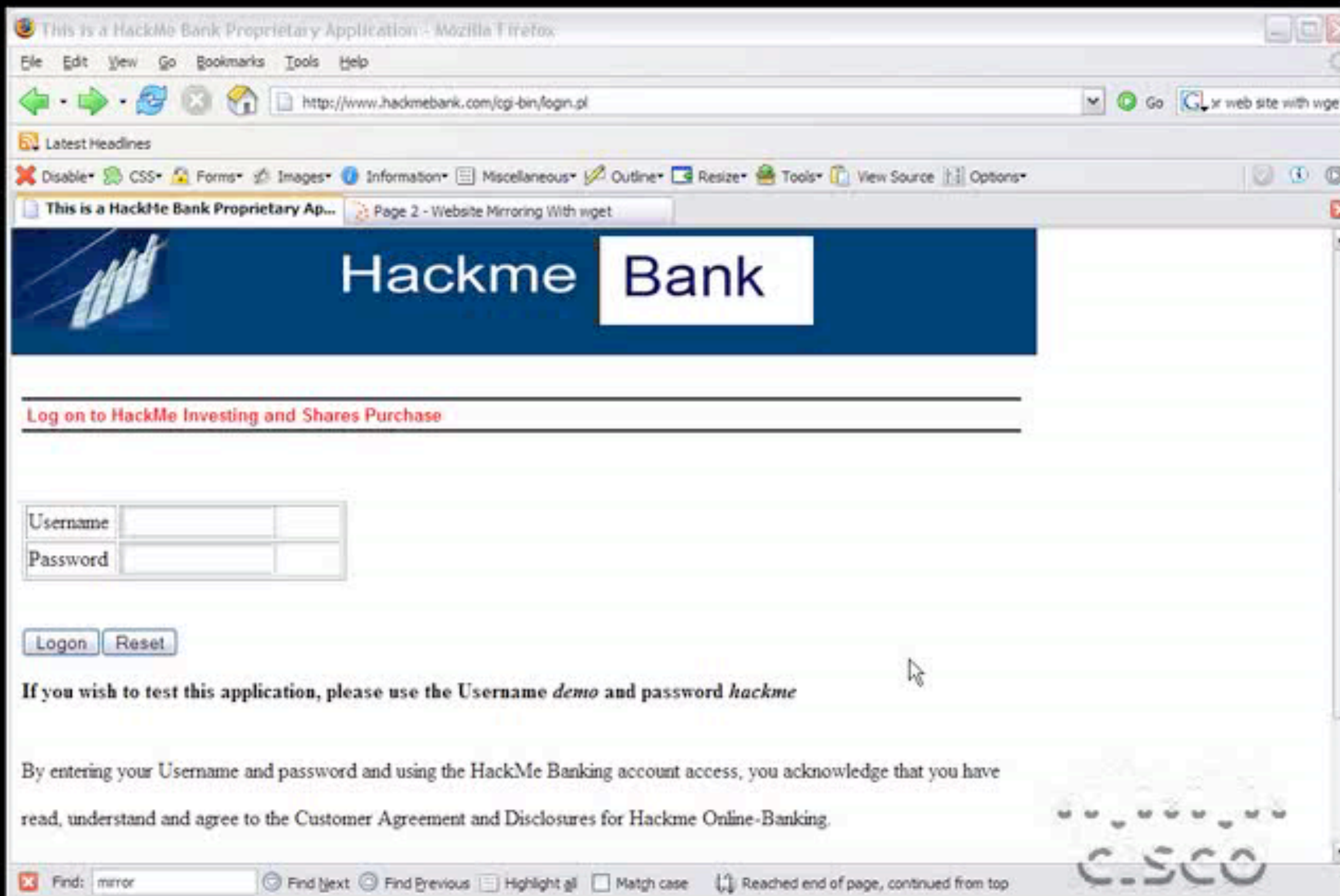














No account in bank??  
No problem! Justo open one with SQL  
injection... :-)

## HACKME BANK HOME BANKING

### Hackme Bank Login

#### Customer Access

Access to these pages is restricted.

The following pages are restricted to customers of Hackme Bank.

Username:

Password:

Done

Internet





Ok, but you are evil person and you want other people money? No problem - again! :-)

# HACKME BANK HOME BANKING

## Hackme Bank Login

### Customer Access

Access to these pages is restricted.

The following pages are restricted to customers of Hackme Bank.

Username:

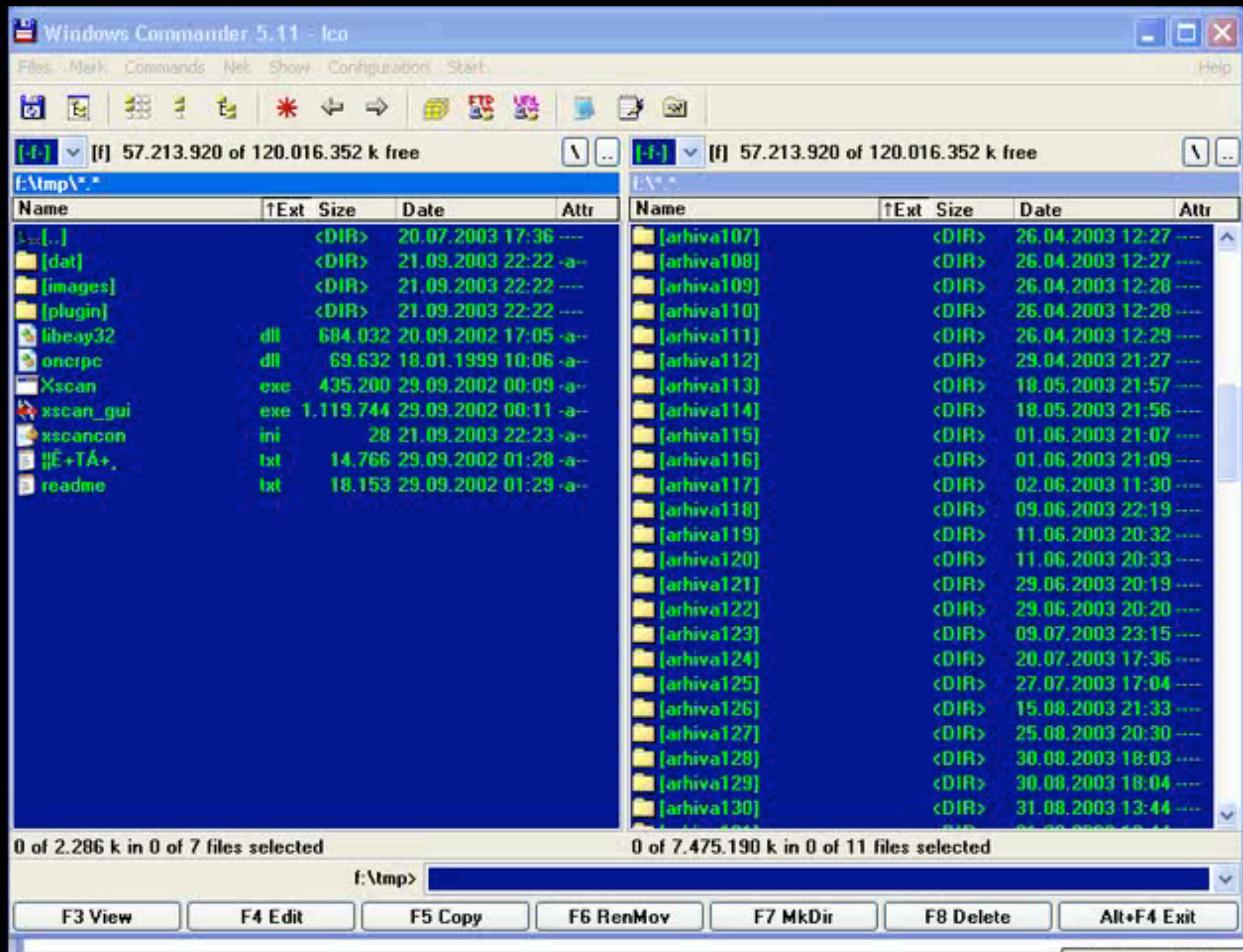
Password:

Done

Internet



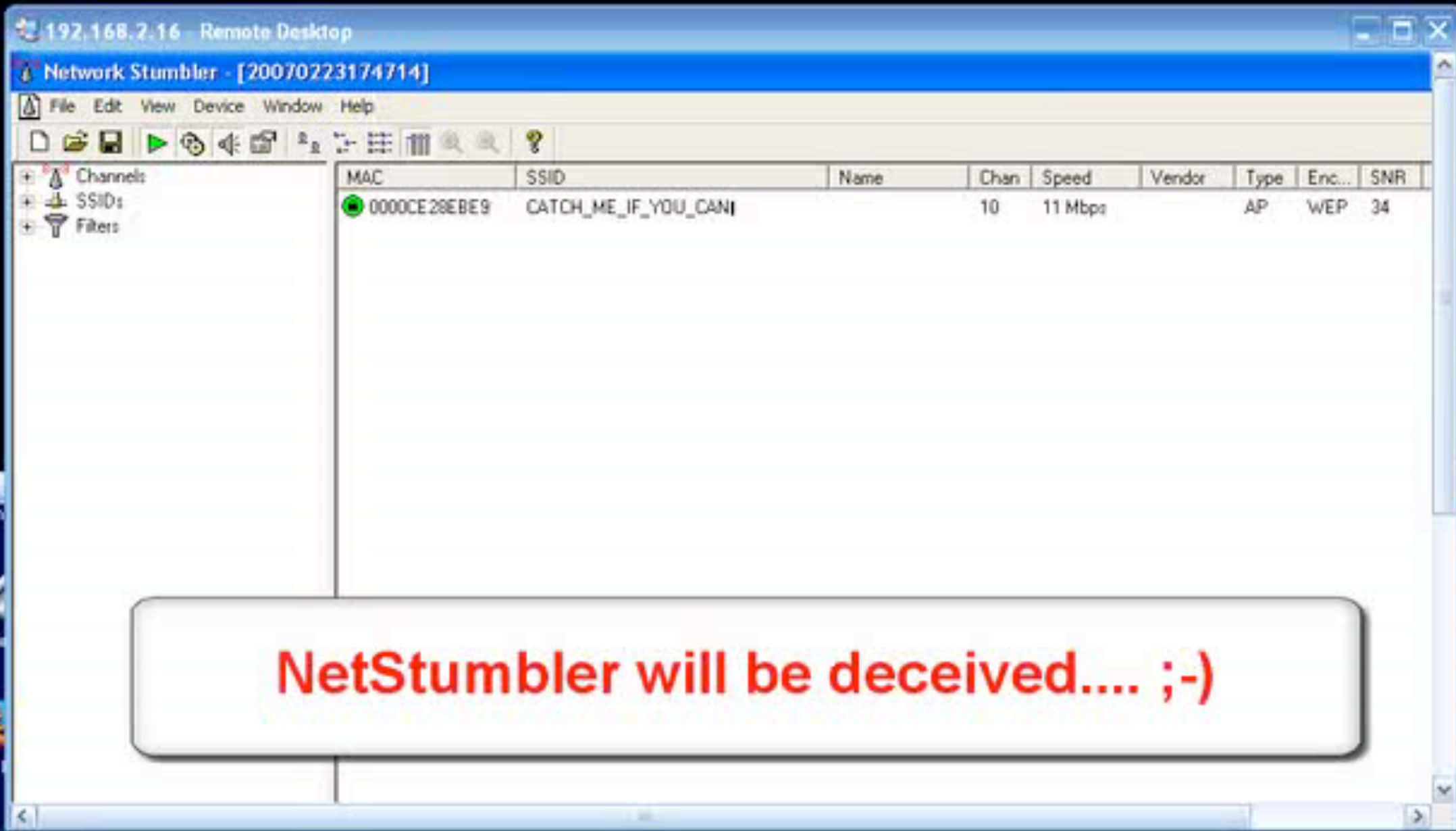






**Linux with fakeap will generate fake AP's**

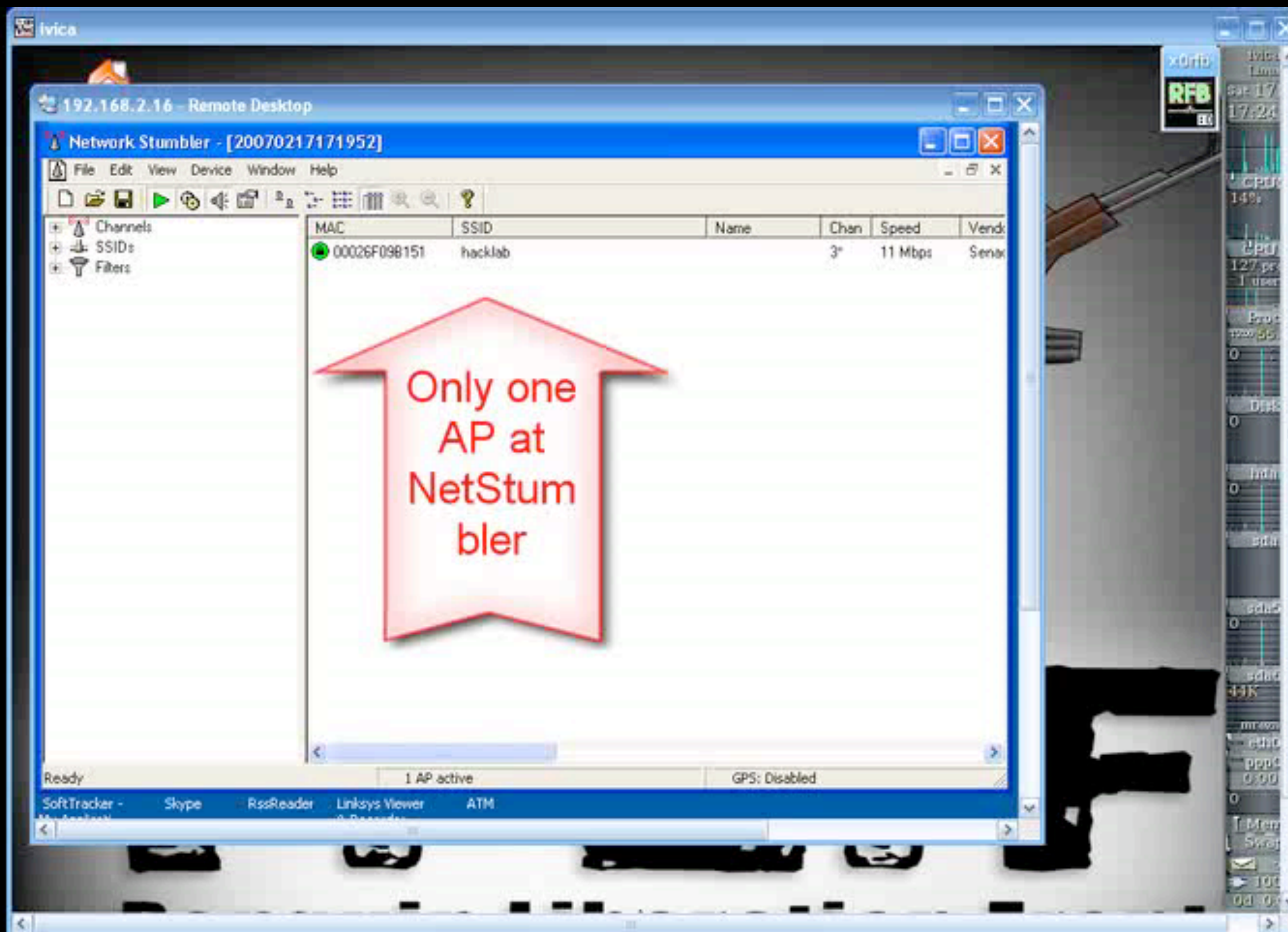
```
[root@ivica  
AP.txt      COPYING  CREDITS  fakeap.pl  INSTALL  lists/  README  
[root@ivica fakeap-0.3.2]# perl fakeap.pl --interface wlan0 --words AP.txt
```



**NetStumbler will be deceived.... ;-)**







# Security Posture Assessment



- About SPA
- Things We've Found



# About SPA

- SPA is a 'snap shot' of the current state of a network, identifying and detailing how the network can be compromised and so highlighting risk factors

A hybrid **penetration test** and **vulnerability assessment**

- Delivered using a combination of **commercial and proprietary tools**

The proprietary tools are developed and maintained in house with capabilities that extend beyond standard commercial tools, both in terms of efficiency and robustness

- SPA is available in two 'families':

**Vector-defined**: how unauthorised access is gained to a network

**Functional**: testing an aspect of network functionality

# About SPA

## External SPA

### Assessment Description

- Conducted from Cisco SOC
- Identify Internet visible vulnerabilities

### Value Proposition

- Mature service offering
- Proprietary tools
- Industry leading expertise

### Impact

- Protect intellectual capital
- Harden Internet perimeter



## Wireless SPA

### Assessment Description

- Locate rogue access points
- Review 802.11 security

### Value Proposition

- Joint NAR offering with WWWP
- Proprietary tools
- Industry leading expertise

### Impact

- Protect intellectual capital
- Locate and disable backdoors



## Internal SPA

### Assessment Description

- On-site inspection
- Trusted insider perspective

### Value Proposition

- Mature service offering
- Proprietary tools
- Industry leading expertise

### Impact

- Protect intellectual capital
- Meet compliance requirements
- Mergers and acquisitions





# About SPA

## Unified Communications SPA

### Assessment Description

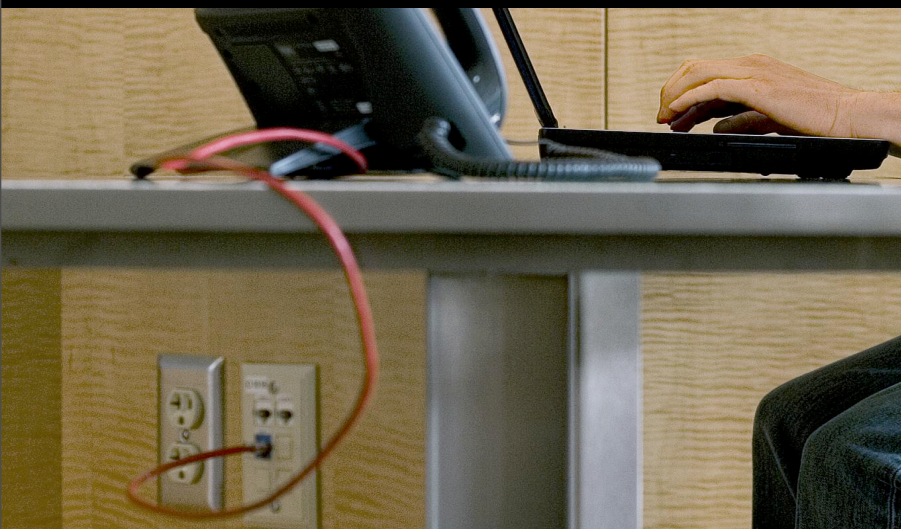
- On-site assessment
- Trusted insider perspective
- Identify VoIP / IPT vulnerabilities

### Value Proposition

- Proprietary tools
- Industry leading expertise

### Impact

- Protect intellectual capital
- Meet compliance requirements
- Mergers and acquisitions



## Web Application SPA

### Assessment Description

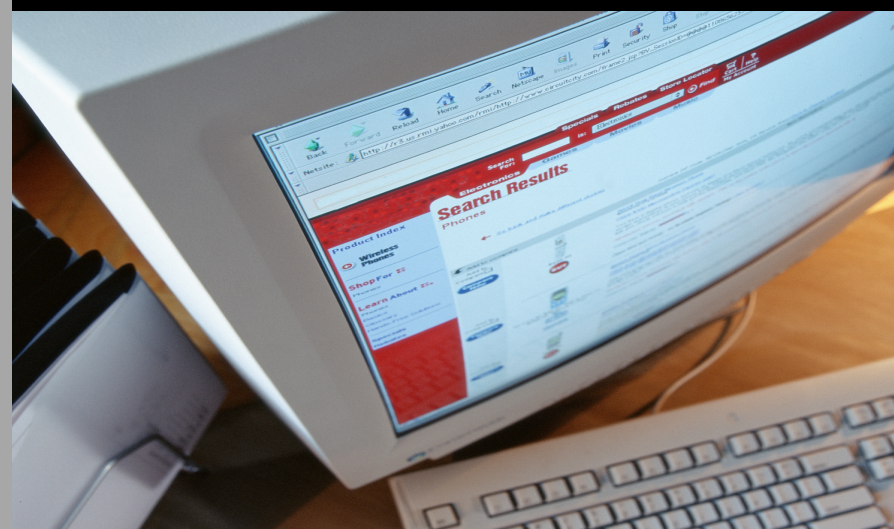
- In-depth review of web app(s)
- Black-box and white-box testing
- Integrate into development lifecycle

### Value Proposition

- Proprietary tools
- Industry leading expertise

### Impact

- Protect intellectual capital
- Meet compliance requirements
- Harden web applications



## “Leak Test”

### Assessment Description

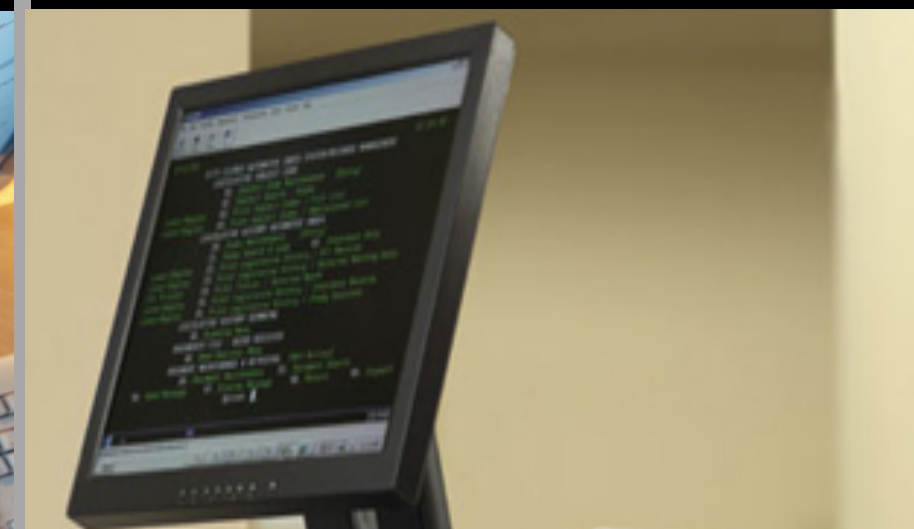
- Locate unauthorized Internet access
- Collector - injector architecture
- On-site assessment

### Value Proposition

- Proprietary tools
- Industry leading expertise

### Impact

- Protect intellectual capital
- Meet compliance requirements
- Mergers and acquisitions





# About SPA

Features	Managed vulnerability scan (e.g. Qualys)	Traditional penetration test	Cisco SPA (vector-defined)
Automated ICMP (ping) scan	✓	✓	✓
Full TCP and UDP scans for asset fingerprinting	✓	✗	✓
In-depth vulnerability scan	✓	✗	✓
Manual confirmation of vulnerabilities through secondary exploitation, so removing false positives	✗	✗	✓
Wireless Access Point configuration review, rogue AP detection and wireless authentication analysis	✗	✗	✓
Understand and prove how vulnerabilities on one system can be exploited to provide access to another	✗	✗	✓
Prove and report unauthorised system access	✗	✓	✓
Validate compliance against relevant parts of ISO27001 framework and industry best practices	✗	✗	✓
Formal report, including in-depth analysis specific to your network, by security experts	✗	✗	✓
Onsite report presentation / workshop	✗	?	✓

# About SPA

- Why is a vector-defined SPA different from a penetration test or vulnerability assessment service?

**Comprehensive approach** – we look for all ways into the network, not just a sampling of some IPs, attack vectors, etc.

**Confirm the presence of vulnerabilities on network** – leverage non-destructive exploits to gain root access, prove the risk

**Prioritize vulnerabilities** – all vulnerabilities are rated (low, medium or high) to help prioritise remediation efforts

**Perform secondary exploitation** – skilled security experts undertake a detailed analysis of how vulnerabilities can be used in combination to gain unauthorized access

# CONCLUSION – GINSBERG THEOREM



# CONCLUSION – GINSBERG THEOREM

- **You can't win!**

# CONCLUSION – GINSBERG THEOREM

- **You can't win!**
- **You can't break even!**

# CONCLUSION – GINSBERG THEOREM

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



# Ehrmans Corollary to Ginsberg's Theorem

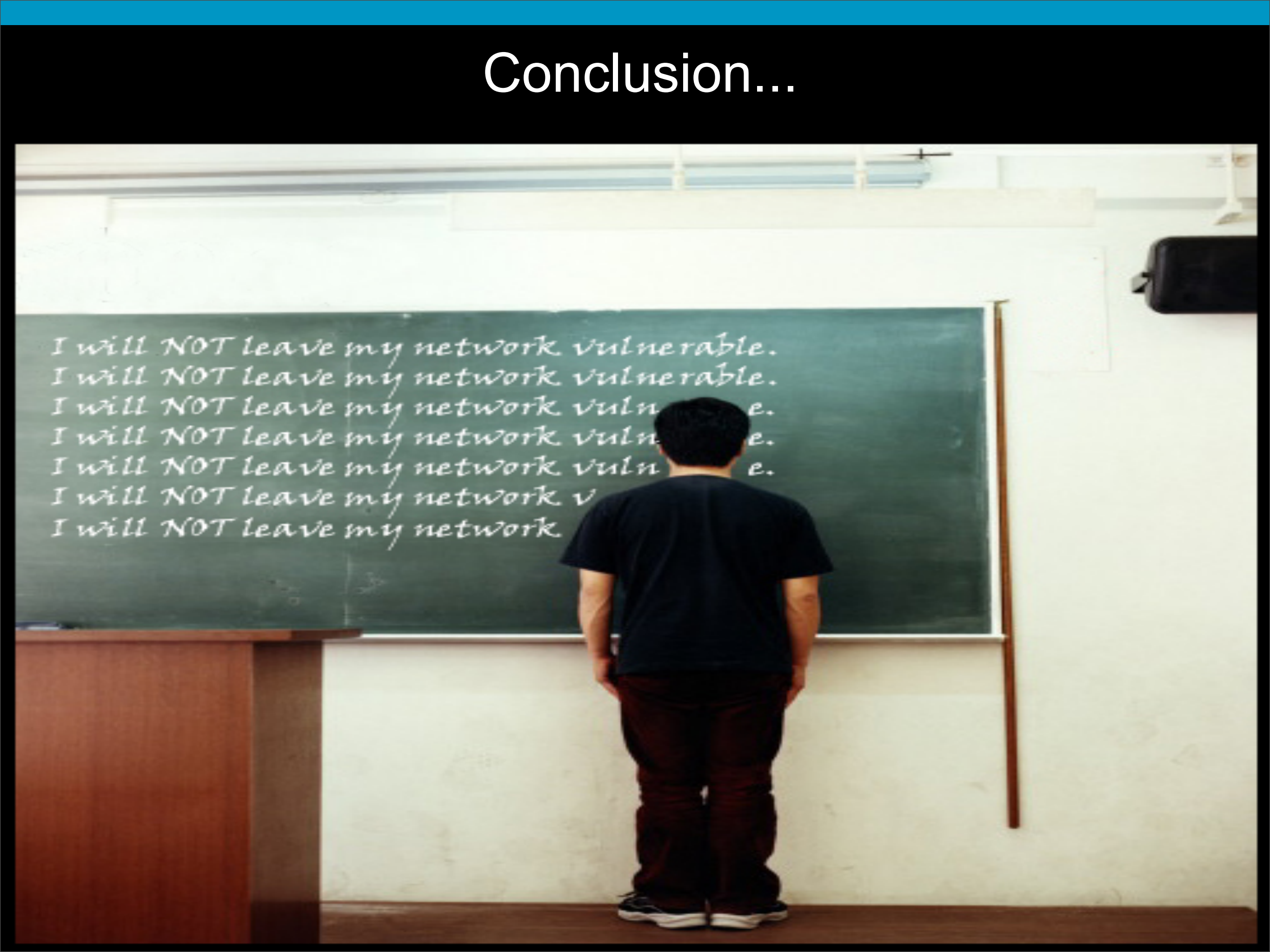
- Things will get worse before they get better!
- Who said things would get better??



# Ehrmans Corollary to Ginsberg's Theorem



# Conclusion...

A person with short dark hair, wearing a dark blue t-shirt and dark pants, stands with their back to the camera, looking at a green chalkboard. The chalkboard is mounted on a white wall and contains seven lines of text written in white chalk. The text is a repetitive phrase: "I will NOT leave my network vulnerable." The first two lines are complete, and the following five lines are partially obscured by the person's head and shoulders. To the left of the chalkboard is a wooden podium. To the right, a black rectangular object, possibly a projector or a sign, is mounted on the wall. The floor is a light brown color.

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



