Warning – Disclaimer - Upozorenje
Warning – Disclaimer - Upozorenje

Neither Cisco or the presentor encourages the use of any methods and/or tools mentioned within this presentation without the expresses approval 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 unauthorised usage of the aforementioned tools and/or methods could lead to legal prosecution and severe penalties.
First – words of wizdom
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.
A glimmer of hope?

The world economy and the perils of optimism
Dow Jones Index: 1929-1940 vs. 2007-today (20/05/09) - www.dickreuter.com
StockJock-e says: Bear market rallies are always exciting! But for those who catch the tops... not so much.

- 381.7
- Yeah! we are rocking now!
  +50% off the lows!
- 294.07
- 242.88 Next stop 360!
- 189.66 Nice! This was the new bull market!
- 157.51
- This is the bottom for sure!
- 152.66 This time the rally will hold!
- 121.70
- That's ok, just a little lower.
- 112.01 Things are different this time!
- 105.48
- Dot is always a bad month.
- 86.48
- 79.93 Sell it all!!!
- 41.22
- Aww F#$%^@#$@#$
- The stock market sucks! I'm never investing again!
Back to IT security ;-)}
Economic crisis 'could drive IT professionals to cybercrime'

March 24, 2009

Job losses and bonus cuts could push security gurus to the dark side

By Jeremy Kirk, IDG News Service

 Enterprises feel their employees will are increasingly willing to steal data or sell insider knowledge due to the poor economy, according to an annual security survey conducted by KPMG.

Sixty-six percent of respondents felt that out-of-work IT workers would be tempted to join the criminal underground, driven in part by threats to bonuses, job losses and worthless stock options.

The E-crime Survey 2009, presented at the E-Crime Congress in London on Tuesday, surveyed 307 private companies, government organisations and law enforcement agencies.

In the survey, KPMG said that fraud committed by managers, employees and customers tripled compared to 2007, which
Economic crisis 'to boost cyber crime': Microsoft

Denholm Barnetson
April 17, 2009

The global financial crisis threatens to spark a rise in cyber crime as computer experts lose their jobs and resort to illegal ways to earn a living, a senior official of Microsoft said Thursday.

"Today these (cyber) attacks are not about vandalism any more, today it's about cash," said Roger Halbheer, Microsoft's chief security advisor for Europe, the Middle East and Africa.

"Cyber crime has gone from cool to cash. And this will definitely grow in the future," he told AFP on the sidelines of an international conference on terrorism and cyber security.

It is "one of the things that scares me about the economic downturn because I'm expecting cyber crime will grow."

He said the crisis had meant people with good knowledge of the industry were being laid off. "They then have time and they don't have money," he said.

"At the moment we are still at the cool side. But I'm expecting it to move to the cash side."

He referred to the Conficker worm, believed to have burrowed into millions of computers around the world in the last few
Cyberspies hack into U.S. fighter project: report

WASHINGTON, Apr. 21, 2009 (Reuters) — Computer spies have repeatedly breached the Pentagon's costliest weapons program, the $300 billion Joint Strike Fighter project, The Wall Street Journal reported on Tuesday.

The newspaper quoted current and former government officials familiar with the matter as saying the intruders were able to copy and siphon data related to design and electronics systems, making it potentially easier to defend against the plane.

The spies could not access the most sensitive material, which is kept on computers that are not connected to the Internet, the paper added.

Citing people briefed on the matter, it said the intruders entered through vulnerabilities in the networks of two or three of the contractors involved in building the fighter jet.

Workers prepare a F-35 joint strike fighter four days before the opening of the 47th Paris Air Show at Le Bourget airport near Paris, June 14, 2007. REUTERS/Pascal Rossignol

Related Topics
- Armed Forces
- Military and Defense Policy
- Political Policy
- Science and Technology
- Technology

Related Articles
- Lockheed Martin 1Q Net Falls 8.8%, Raises Full-Year EPS View
  Apr. 21, 2009 (Wall Street Journal) — Lockheed Martin Corp.’s (LMT) first-quarter net income fell 8.8% on higher pension-related expenses, though the defense contractor raised its ...
- Hackers Break Into Pentagon's Fighter Jet Project
  Apr. 21, 2009 (CIO Magazine) — Hackers broke into U.S. Department of Defense computers and downloaded terabytes of data containing design information about the Joint Strike ...
- Lockheed Profit Falls 8.8% on Rising Pension Costs; 2009 Forecast Raised
  Apr. 21, 2009 (Bloomberg) — Lockheed Martin Corp., the world's largest defense company, said first-quarter profit fell 8.8 percent as rising pension costs offset increased ...
- Wanted: Nerds to byte into U.S. hacker battle
  Apr. 20, 2009 (Boston Herald) — The feds are
Black Hats
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

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

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).
Blackjacking - Owning the Enterprise via the Blackberry

Presented at Defcon 14 - Las Vegas, NV 2006

Jesse D’Aguanno
jesse [at] praetorian.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

Blackberry Attack Toolkit (Including BBProxy)

NOTE: This link is now active!
Blackjacking –
Owing the Enterprise via Blackberry

Jesse ‘x30n’ D’Aguanno
x30n@digrev.org
jesse@praetoriang.net

Defcon 14 - Las Vegas, NV USA 2006
Summary

This is a proof of concept exploit for Apache,

This code exploit multipart/form-data POST requests bug. This code only crash
apache deamon, not open any shell or execute code in the remote server.

PHP supports multipart/form-data POST requests (as described in RFC1867)
Attack by web sites
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.
Attack by web sites

Attackers turn Bank of India site into malware bazaar

By Dan Goodin in San Francisco → More by this author
Published Saturday 1st September 2007 00:11 GMT

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.q, 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 ed more 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 Script Injection or cross-site scripting, which is proving to be resilient against but brutal because there is no single...
Attack by web sites

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 nationwidepercyw.com, the Mercury music awards site (which is sponsored by building society Nationwide), and UK law firm

© 2007 Cisco Systems, Inc. All rights reserved.
WELCOME TO DARK MARKET
<table>
<thead>
<tr>
<th>Thread / Thread Starter</th>
<th>Rating</th>
<th>Last Post</th>
<th>Replies</th>
<th>Views</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sticky: e-gold exchange still available</strong></td>
<td></td>
<td>Yesterday 10:50 PM</td>
<td>5</td>
<td>126</td>
</tr>
<tr>
<td><strong>rbc logins</strong></td>
<td></td>
<td>Today 01:19 AM</td>
<td>12</td>
<td>190</td>
</tr>
<tr>
<td><strong>Tipper And Embosser For Sale</strong></td>
<td></td>
<td>Yesterday 06:46 PM</td>
<td>4</td>
<td>158</td>
</tr>
<tr>
<td><strong>Couple of hacked unix servers for SCAM</strong></td>
<td></td>
<td>10-17-2006 03:37 PM</td>
<td>5</td>
<td>106</td>
</tr>
<tr>
<td><strong>100 usa valid fullz for sale</strong></td>
<td></td>
<td>10-17-2006 01:07 PM</td>
<td>7</td>
<td>215</td>
</tr>
<tr>
<td><strong>Full infos with Bank account numbers</strong></td>
<td></td>
<td>10-17-2006 06:45 AM</td>
<td>1</td>
<td>79</td>
</tr>
<tr>
<td><strong>Halifax UK Logins</strong></td>
<td></td>
<td>10-17-2006 06:01 AM</td>
<td>10</td>
<td>177</td>
</tr>
<tr>
<td><strong>Zombie Computers</strong></td>
<td></td>
<td>10-15-2006 06:14 PM</td>
<td>5</td>
<td>258</td>
</tr>
<tr>
<td><strong>Need JCB cards, any country</strong></td>
<td></td>
<td>10-15-2006 02:14 AM</td>
<td>2</td>
<td>42</td>
</tr>
<tr>
<td><strong>Need CVV2'S of this county</strong></td>
<td></td>
<td>10-14-2006 12:47 PM</td>
<td>6</td>
<td>81</td>
</tr>
<tr>
<td><strong>canada banks</strong></td>
<td></td>
<td>10-14-2006 01:15 AM</td>
<td>0</td>
<td>26</td>
</tr>
<tr>
<td><strong>Need Bank logins of this county</strong></td>
<td></td>
<td>10-12-2006 07:39 AM</td>
<td>2</td>
<td>57</td>
</tr>
<tr>
<td><strong>Selling comcast and optonline accounts</strong></td>
<td></td>
<td>10-12-2006 07:39 AM</td>
<td>4</td>
<td>81</td>
</tr>
</tbody>
</table>
DarkPimp offline
Member

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.
Agree to use escrow service, buyer pay fees.
The passport expires in 2010 year.
Anyone interested PM with offers.
Will send a scan too.
matrix001 Offline
Reviewed Vendor (CC Templates & Custom Graphics)

3 European Amex Centurion Dumps

dumps sold.

Last edited by matrix001 : 08-14-2006 at 03:20 PM.
hi ppl
I am selling hacked hosts, available 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
Dark Market – The Bazaar

Thursday, November 5, 2009

 DDS SERVICE

04-18-2006, 06:34 PM

18 Offline
Trial Vendor (ddos service)

DDoS SERVICE

I offer services DDoS'.
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.
I have all this logins from UK:

Comes with DOB/SecurityNumber/ID

These are the accounts and prices, prices are negotiable and if you're buying more than one I can make better deals. Escrow is of course always accepted.
Have any questions you can email me at 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
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

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

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

19 - Personal - 1200 - 10GBP
20 - Personal - 5000 - 125GBP
21 - Personal - 6000 - 135GBP
22 - Business - 2700 - 50GBP
23 - Personal - 9000 - SOLD
24 - Personal - 5500 - 130GBP
25 - Personal - 2700 - 40GBP
Drax Offline
Verified Vendor (BANK LOGIN)
DM Reviewer
Canadian Moderator
Donator

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

19 - Personal - 1200 - 10GBP
20 - Personal - 5000 - 125GBP
21 - Personal - 6000 - 135GBP
22 - Business - 2700 - 50GBP
23 - Personal - 9000 - SOLD
24 - Personal - 5500 - 130GBP
25 - Personal - 2700 - 40GBP
Bluetooth
New antenna ups Bluetooth range to 30 Kilometers

Posted by Joshua Karp on Jul 2, 2007 10:11 am

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
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

---

© 2007 Cisco Systems, Inc. All rights reserved.

Thursday, November 5, 2009
# About SPA

<table>
<thead>
<tr>
<th>Unified Communications SPA</th>
<th>Web Application SPA</th>
<th>“Leak Test”</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assessment Description</strong></td>
<td><strong>Assessment Description</strong></td>
<td><strong>Assessment Description</strong></td>
</tr>
<tr>
<td>On-site assessment</td>
<td>In-depth review of web app(s)</td>
<td>Locate unauthorized Internet access</td>
</tr>
<tr>
<td>Trusted insider perspective</td>
<td>Black-box and white-box testing</td>
<td>Collector - injector architecture</td>
</tr>
<tr>
<td>Identify VoIP / IPT vulnerabilities</td>
<td>Integrate into development lifecycle</td>
<td>On-site assessment</td>
</tr>
<tr>
<td><strong>Value Proposition</strong></td>
<td><strong>Value Proposition</strong></td>
<td><strong>Value Proposition</strong></td>
</tr>
<tr>
<td>Proprietary tools</td>
<td>Proprietary tools</td>
<td>Proprietary tools</td>
</tr>
<tr>
<td>Industry leading expertise</td>
<td>Industry leading expertise</td>
<td>Industry leading expertise</td>
</tr>
<tr>
<td><strong>Impact</strong></td>
<td><strong>Impact</strong></td>
<td><strong>Impact</strong></td>
</tr>
<tr>
<td>Protect intellectual capital</td>
<td>Protect intellectual capital</td>
<td>Protect intellectual capital</td>
</tr>
<tr>
<td>Meet compliance requirements</td>
<td>Meet compliance requirements</td>
<td>Meet compliance requirements</td>
</tr>
<tr>
<td>Mergers and acquisitions</td>
<td>Harden web applications</td>
<td>Mergers and acquisitions</td>
</tr>
</tbody>
</table>
# About SPA

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

- Things will get worse before they get better!
- Who said things would get better?? 😊
Ehermans Corollary to Ginsberg’s Theorem

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

Thursday, November 5, 2009
Conclusion...

I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.