



GWAVA

Solutions for GroupWise



GWAVA

February 3, 2009

**David Balcar**  
Chief Security Officer

Network Design & Integration  
[dbalcar@networkdesign.net](mailto:dbalcar@networkdesign.net)



There is no security on this earth, there is only opportunity - General Douglas MacArthur

# Surviving a Security Attack

## Why are we here?

- When your security perimeter fails what do you do?
- When your internal security fails what do you do?
- How do you mitigate your risks if you've been the victim of a penetration of your IT Security?

I know, DEMO!



# Just the Facts

On December 23, RBS Worldpay, a subsidiary of Citizens Financial Group Inc., said a breach of its payment systems may have affected more than 1.5 million people.

In March 2008, Hannaford Brothers Co. disclosed that a breach of its payment systems -- also aided by malicious software -- compromised at least 4.2 million credit and debit card accounts.

In early 2007, TJX Companies Inc., the parent of retailers Marshalls and TJ Maxx said a number of breaches over a three-year period exposed more than 45 million credit and debit card numbers.

In 2005, a breach at payment card processor CardSystems Solutions jeopardized roughly 40 million credit and debit card accounts

**A data breach last year at Princeton, N.J., payment processor Heartland Payment Systems may have compromised tens of millions of credit and debit card transactions, the company said today.**



**190+ MILION.....**

# Surviving a Security Attack

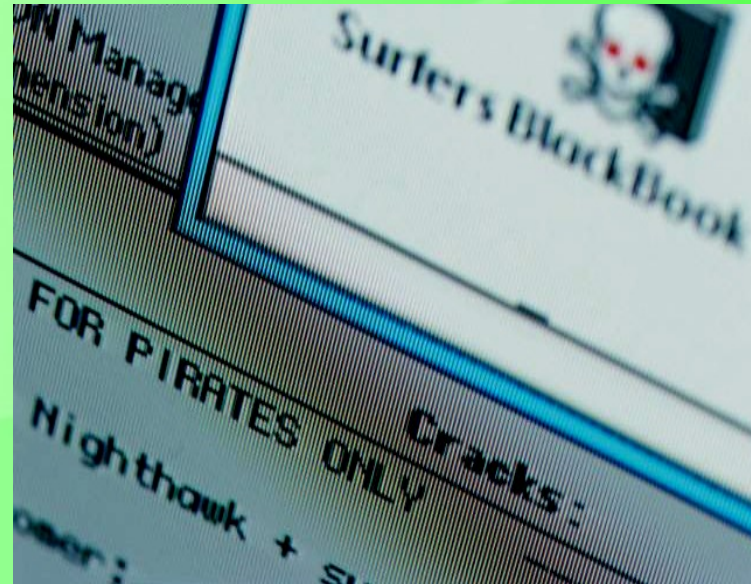
## Today's Reality

- Too many customers focus on Perimeter security
  - “AV and Firewalls will keep me secure”
- Most people think only of keeping the bad guys out
- 90% of break-ins are the result of mis-configuration
- 70% are break-ins are from the inside



# Surviving a Security Attack

Viruses      Malware  
Spyware    Cybercrime  
Disgruntled employees  
Espionage/Hacktivism/etc.



**Anti-Virus / Firewalls are not enough!**



# Surviving a Security Attack



## Who's watching your Network?



# Surviving a Security Attack

Information Gathering (Port scanning)

Denial of Service - (DOS/DDOS)

Information Theft - Credit Card Numbers  
Financial Information



# Surviving a Security Attack

- Stay calm
- Assess the damage
- Notify pertinent staff in your organization; i.e., executive management, help desk, etc.
- Secure your backups



# Surviving a Security Attack

- Document the hack—Someone needs to write documentation of everything that happened. *Who, what, where, and when* are the operative words.
- Who...Names of people who discovered discrepancies or problems.
- What...Exact descriptions of what was discovered.
- Where...What servers, networks, Web pages, etc. were affected?
- When...Report all events in chronological order.



# Surviving a Security Attack

- Know your baseline.
- If you're not planning to identify the intruder, then you should disconnect the entire internal network from the Internet immediately. This will prevent the intruder working against you while you clean up the mess, and prevent further infection or data loss while you find a resolution.



# Surviving a Security Attack

Security perimeter fails:

Start by following your Security response plan.

**If you don't have one get one! :-)**

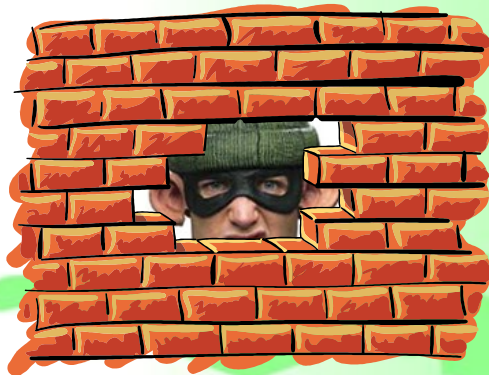
On production systems: (General guidelines)

- 1) Start a journal of the event.
- 2) Remove the system from the network.
- 3) Get a snapshot image of the system.
- 4) Consult a Security professional.



# Surviving a Security Attack

## Mitigating Your Attack Profile



- The edge of the Network
  - Managed Endpoint / Malware Protection
  - Patch Remediation
- Wireless
  - Integrate tight authentication (802.1x)
  - Map it, and reign in those wifi signals!
- Gateways/Guest Network Access
  - UTM: Unified Threat Management
- Network Infrastructure
  - IPS, network monitoring
- Authentication
  - Biometrics, Tokens, SmartCards, etc...



# DEMO

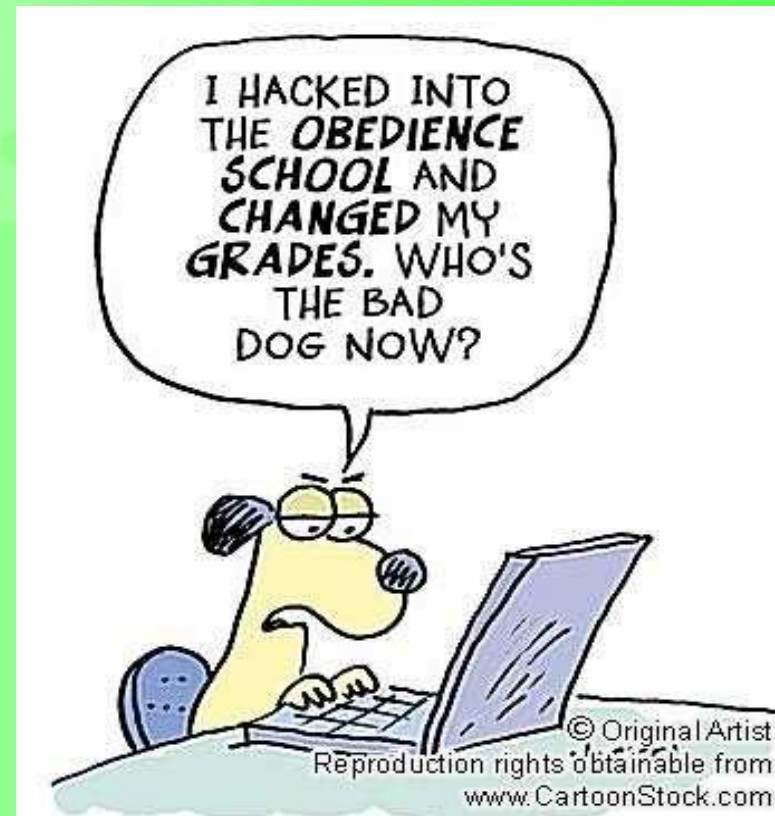
- Backtrack
- [www.remote-exploit.org/backtrack.html](http://www.remote-exploit.org/backtrack.html)

- NMAP

- <http://nmap.org/>

- CAIN / ABLE

- [www.oxid.it/cain.html](http://www.oxid.it/cain.html)



# DEMO

- GFI LANGuard Security Scanner
- [www.gfi.com/lannetscan](http://www.gfi.com/lannetscan)

# Interesting URL's

<http://ha.ckers.org/>

[Ciseek.com](http://Ciseek.com)

<http://ophcrack.sourceforge.net/>

<http://www.aircrack-ng.org/doku.php>

<http://www.wigle.net/>

[www.insecure.org](http://www.insecure.org)

[www.sans.org](http://www.sans.org)

[www.cert.org](http://www.cert.org)

[secunia.com](http://secunia.com)

# Quotes

“If you spend more on coffee than on Information Technology security, then you will be hacked. What’s more, you deserve to be hacked.”

Richard Clarke, Special Advisor to the President on CyberSecurity

“64 percent of organizations in the United States have experienced unauthorized use of computer systems and information in the past year.”

FBI and the Computer Security Institute

27% of Fortune 500 companies have battled harassment claims related to employee misuse and abuse of corporate e-mail

“Attacks on cyberspace – through worms, viruses, hacking, identity theft, fraud, extortion and industrial espionage – continue to rise exponentially in frequency, severity and financial cost. Last year alone, cyber attacks cost the U.S. financial sector nearly \$1 billion”

BITS, a nonprofit financial services industry consortium



# Trivia

Message from discussion What would you like to see most in minix?

View parsed - Show only message text

Path: gmdzi!unido!fauern!ira.uka.de!sol.ctr.columbia.edu!zaphod.mps.ohio-state.edu!wupost!uunet!mcsun!news.funet.fi!hydra!klaava!torvalds  
From: torva...@klaava.Helsinki.FI (Linus Benedict Torvalds)  
Newsgroups: comp.os.minix  
Subject: What would you like to see most in minix?  
Summary: small poll for my new operating system  
Keywords: 386, preferences  
Message-ID: <205708.9541@klaava.Helsinki.FI>  
Date: **25 Aug 91 20:57:08 GMT**  
Organization: University of Helsinki  
Lines: 20

Hello everybody out there using minix -

I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) among other things).

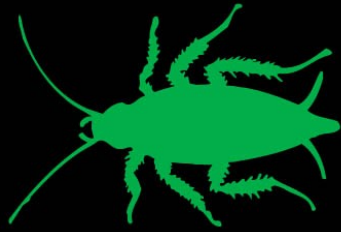
I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want. Any suggestions are welcome, but I won't promise I'll implement them :-)

Linus (torva...@kruuna.helsinki.fi)

PS. Yes - it's free of any minix code, and it has a multi-threaded fs. It is NOT protable (uses 386 task switching etc), and it probably never will support anything other than AT-harddisks, as that's all I have :-).



Thank You!



**GWAVA**



### **Unpublished Work of Beginfinite, Inc. All Rights Reserved.**

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Beginfinite, Inc. Access to this work is restricted to Beginfinite employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Beginfinite, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

### **General Disclaimer**

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. Beginfinite, Inc., makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Beginfinite, Inc., reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Beginfinite marks referenced in this presentation are trademarks or registered trademarks of Beginfinite, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.