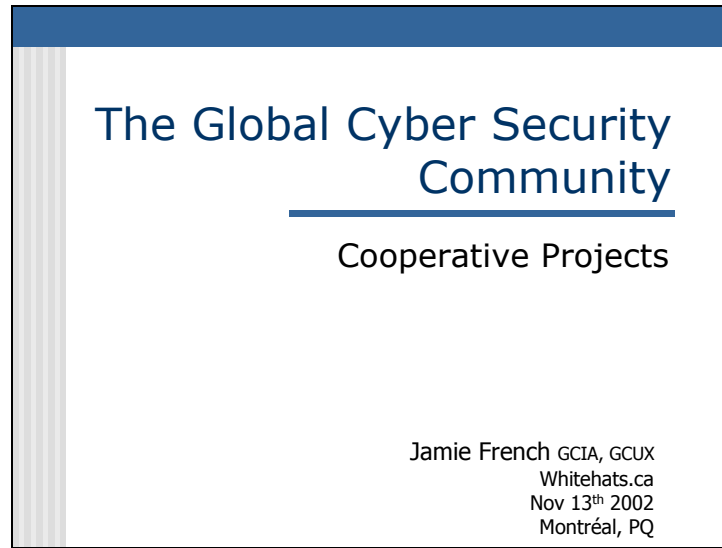


Slide 1



The Global Cyber Security
Community

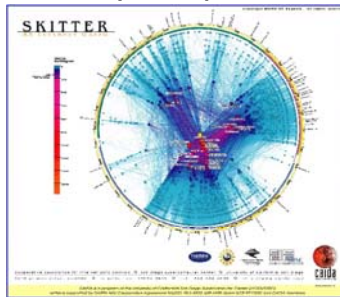
Cooperative Projects

Jamie French GCIA, GCUX
Whitehats.ca
Nov 13th 2002
Montréal, PQ

Slide 2

There are no borders!

- Don't be fooled, there are no borders in cyberspace



<http://www.caida.org/>

What drives the bad guys?

- Access to crime scene made easy
- Low risk
 - Good chance of not being caught
 - If caught, likely won't be prosecuted
 - No guard dog or security is going to physically shoot the bad guy through his monitor
- High profit
 - Transfer more money than you could physically carry
 - Mass exposure, more damage caused or profit to be taken

Do they work together?

- You bet they do!
 - <http://dmoz.org/Computers/Hacking/Groups/>
 - <http://packetstormsecurity.com.ar/mag/>
 - IRC channels
 - [.evil.]
 - basehack
 - <http://www.xgoogle.org/index2> (explicit content)
 - <https://www.team-teso.net/about.php>
- Take a look at exploit source code for sh0utz!

Why security pros don't work together

- Confidentiality
- Reputation
- Fear/Paranoia
- Policy
- Not aware




<http://www.ratbastards.org/scrapbook4.html>

Is there a comfort zone? Confidentiality

- Confidentiality (of your organization)
 - Sanitize Data
 - Share with those you trust
 - Orgs with Non-disclosure agreements (NDA's)
 - Eg. FIRST, CERT/CC, CANCERT
 - Anonymization Projects
 - <http://freenetproject.org/cgi-bin/twiki/view/Main/WhatIs>
 - <http://www.freehaven.net/related-comm.html>
 - Encryption
 - Protect your confidential information in transit

Is there a comfort zone? Reputation - Professional

- Reputation
 - Your professional reputation



OR

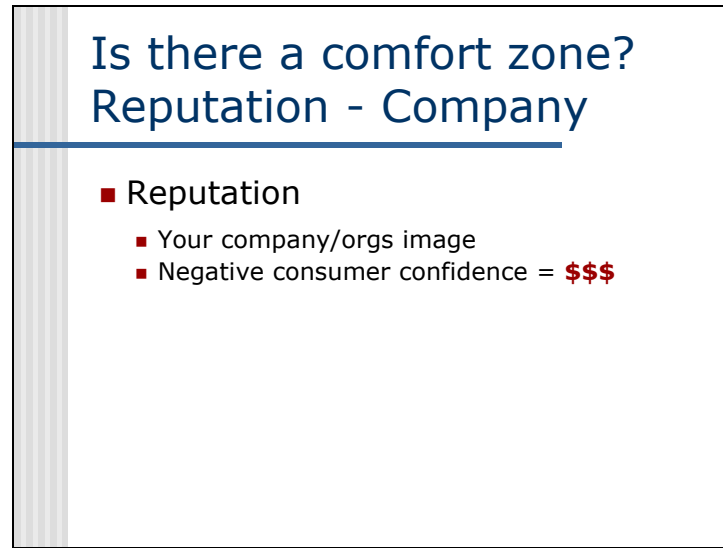
<http://www.ourcharacter.com/behavioral.html>

Your professional reputation

Don't hoard information, you become the weak link and single point of failure. This should not be a trait of security minded persons. If your too good to need help from others you should be offering help to those that need it, otherwise your in the wrong place right now.

Your companies image

Reasonable challenge. If the impact of disclosure of information is deemed to be severe, you'll have to keep your lips sealed. Weigh the cost of not dealing with the problem or not knowing if you've dealt with the problem appropriately against the impact of dealing with it using help from others you trust.



Is there a comfort zone?
Reputation - Company

- Reputation
 - Your company/orgs image
 - Negative consumer confidence = \$\$\$

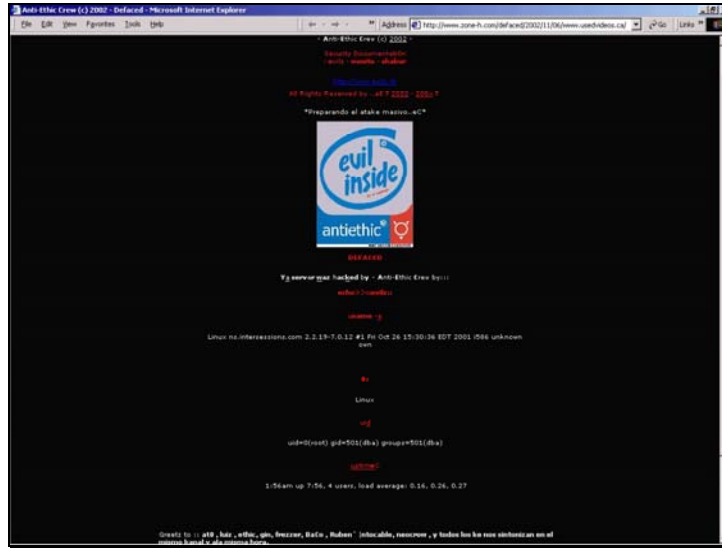
Your professional reputation

Don't hoard information, you become the weak link and single point of failure. This should not be a trait of security minded persons. If your too good to need help from others you should be offering help to those that need it, otherwise your in the wrong place right now.

Your companies image

Reasonable challenge. If the impact of disclosure of information is deemed to be severe, you'll have to keep your lips sealed. Weigh the cost of not dealing with the problem or not knowing if you've dealt with the problem appropriately against the impact of dealing with it using help from others you trust.

Slide 9



Is there a comfort zone? Fear/Paranoia

- Human behavioural issue
- Not everybody is out to get you!
Seriously!!!
- Info Sharing is done by many orgs
- Weigh benefit vs cost
Objectively

Is there a comfort zone? Policy

- Up to management to decide
- Show them the pros and cons
= **Informed Policy Decision**
- When event arises, review policy


Is there a comfort zone? Not Aware

- The goal of this presentation is to introduce some cooperative projects and raise **AWARENESS**.



SANS Institute

- Leadership in field
- Sponsors many projects
- GIAC Certification Program
- Ear to the ground – new research, threats, survey of cyberscape, and consensus (S.C.O.R.E.)
- <http://www.sans.org>
- <http://rr.sans.org>
- <http://www.sans.org/SCORE/>



HoneyNet Project

- Raise Awareness
- Teach and Inform
- Research
- <http://project.honeynet.org/>

Raise awareness. To raise awareness of the threats and vulnerabilities that exist in the Internet today. We raise awareness by demonstrating real systems that were compromised in the wild by the blackhat community. Many people believe it can't happen to them. We hope to change their mind.

Teach and inform. For those in the community who are already aware and concerned, we hope to give you the information to better secure and defend your resources. Historically, intelligence about attackers has been limited to the tools they use. The Project intends on providing additional information, such as their motives in attacking, how they communicate, when they attack systems and their actions after compromising a system.

Research To provide the technology and methods of information gathering. Organizations, such as universities, may be interested in developing their own ability to research threats or adversaries.

DeepSight Analyzer Security Focus


DeepSight™ Analyzer

- Submit logs from many devices
- Correlation of data from many others
- Adds value and aids in analysis
- Quickly identify new threats

IDS	Version	Platform
Cisco Secure	All current shipping versions	UNIX (Any version which supports current shipping version), Windows (Any version which supports current shipping version)
Enterasys Dragon IDS Sensor	4.x	FireHOLD (4.x), FireHOLD (3.x), HPX 11.0, Linux, OpenHSD, Solaris-Sparc, Solaris-x86
ISS RealSecure	3.1-6.3	Windows NT 4 SP2 (or above), Windows 2000
ISS BlackICE	Any version	Windows NT 4.0 (Service Packs 4, 5, 6, or 6a), Windows 95, Windows 98, Windows 2000 Server (Pack 1)
Snort Open Source Network IDS	1.6 - 1.8.6	UNIX (Any version which Snort will build on), Win32 (Any version which Snort will build on)
Covariant	1.1.7.0	Appliance based
Symantec NetProwler	3.5	Windows NT 4.0


- <http://analyzer.securityfocus.com/>
- <http://analyzer.securityfocus.com/Documents/dp.pdf>

<http://analyzer.securityfocus.com/>
<http://analyzer.securityfocus.com/FAQ.asp>
<http://analyzer.securityfocus.com/Documents/dp.pdf>



Center for Internet
Security

- Non-profit
- Provide guidance on how to secure systems
- Templates and audit checklists
- <http://www.cisecurity.org/>



Common Vulnerabilities and Exposures

- Standardized vulnerability names
 - Very important for quickly and accurately addressing a problem
- Consensus driven and presided over by a board of representatives
- <http://mitre.cve.org>
- <http://icat.nist.gov>

A list of standardized names for vulnerabilities and other information security exposures - CVE aims to standardize the names for all publicly known vulnerabilities and security exposures.

A Community-Wide Effort - The content of CVE is a result of a collaborative effort of the CVE Editorial Board. The Editorial Board includes representatives from numerous security-related organizations such as security tool vendors, academic institutions, and government as well as other prominent security experts. The MITRE Corporation maintains CVE and moderates Editorial Board discussions.



DSHield

- Collects logs
- Correlate logs and spot new trends and threats
- Fight back program
- <http://www.dshield.org>
- <http://www.dshield.org/search.php>

DShield.org is an attempt to collect data about cracker activity from all over the internet. This data will be cataloged and summarized. It can be used to discover trends in activity and prepare better firewall rules.

Right now, the system is tailored to simple packet filters. As firewall systems that produce easy to parse packet filter logs are now available for most operating systems, this data can be submitted and used without much effort.

More complex patterns, such as are used by application level firewalls may be handled in the future.

InternetStormCenter


Internet Storm Center

- Trend analysis on log submissions (thru Dshield)
- Intrusions Mailing List
 - intrusions-subscribe@incidents.org
- <http://isc.incidents.org>
- <http://isc.incidents.org/trends.html>



Whitehats.ca

- Port Database
- Research
- Some tools for InfoSec
- Member contributions
- <http://www.whitehats.ca>



Whitehats.com

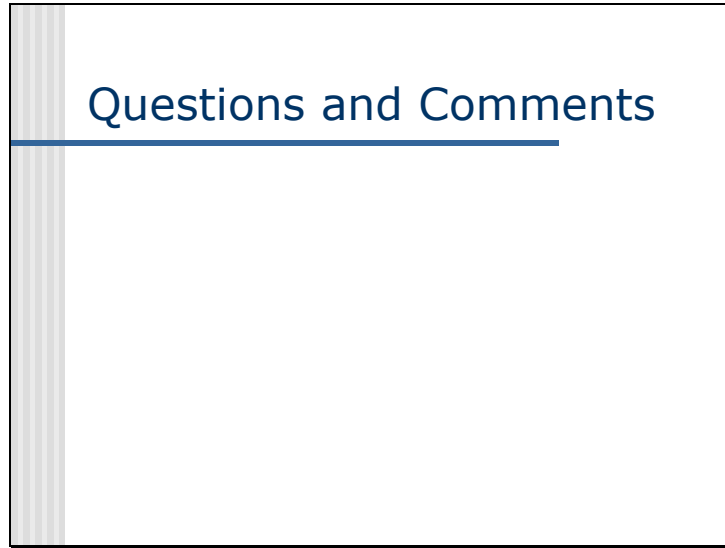
- arachNIDS Signature Database
 - Much more than just a collection of signatures
- Discussion Forums
- Tools
- Research
- <http://www.whitehats.com>

Taking from the community

The message is simple!

Use these cooperative projects to help secure your networks, if possible try to give something back.

The "uber hax0rs" work together (for a reason), shouldn't we?



Questions and Comments

Thank you!

This presentation is available online at

http://www.whitehats.ca/main/members/Malik/malik_coop_projects.htm

or

http://www.whitehats.ca/main/members/malik/malik_coop_projects.pdf

Jamie French
j.french@whitehats.ca
Jamie.French@nrms.ca