INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Digital Deception:
Raising the Stakes on Hackers

Dan Houser, CISM, CISSP, ISSAP

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Overview

- **Changes in hacker space**
- **Weather & early warning systems**
- **Dirty deeds done dirt cheap**
- **Big freakin' haystack introduction**
  - **Emulation of 16 million node network**
  - **Intrusion Management network**
- **What next?**
- **Q&A**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Goals…

- **Use of Digital Deception**
- **Confuse, Harass, Confound the enemy**
- **Dramatically, drastically, overwhelmingly increase the economic cost of system scanning and worm target acquisition**
- **Make script kiddy and worms infeasible**
- **Force a paradigm shift**

We are locked in a cold-war arms race, where only the arms dealer wins.

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Internet attacks have changed…

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Old school attack

- **Lone interloper targets major firm**
- **Studies publicly available information**
- **Hangs out at local pub, befriends sales team**
- **Dumpster dives to obtain manuals, phone lists**
- **Uses war-dialer to find modems & remote hosts**
- **Uses social engineering to obtain passwords**
- **Dials up hosts, logs in, mayhem & mischief**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

"Modern" attack

- **Lone interloper targets IP range**
- **Downloads script kiddy tools**
- **Scans IP range looking for vulnerable hosts**
- **Port scans hosts looking for exploitable services**
- **Uses exploit tool, mayhem & mischief**

Target selection now a target of opportunity… indiscriminate attack

INFORMATION SECURITY DECISIONS

Hosted by

Confuse and harass attackers

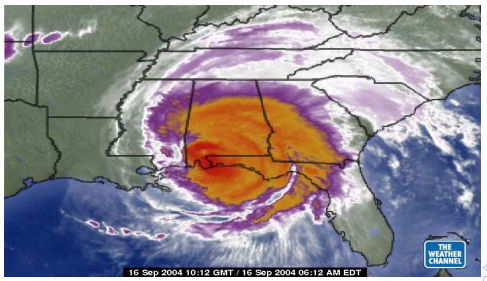
Make your real servers look bogus

- **Save all .ASP code as .CGI files, perl as .ASP**
- **Configure responses from Apache that mimic IIS**
- **Open dummy NetBIOS ports on Unix servers**
- **Open bogus 21, 23, 25, 80 & 443 ports on all servers, with netcat listening on the bogus ports**
- **Call your database server "Firewall"**
- **Route bogus traffic to IDS network**

INFORMATION SECURITY DECISIONS

Hosted by

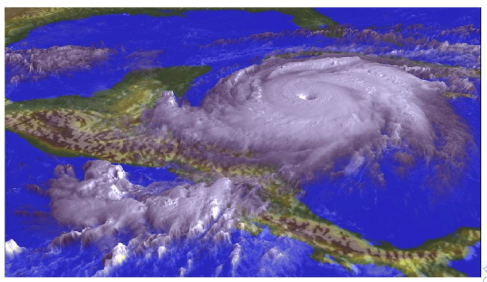
Worms hit 10,000 networks at once…



INFORMATION SECURITY DECISIONS

Hosted by

What we need is early warning



INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Hide in the open: Big freakin' haystack

- **Virtual honeynets + Intrusion Management**
- **Create server that emulates address range: 10.x.x.x**
- **Open tons of ports: 20, 21, 23, 25, 37, 42, 43, 49, 67, 68, 69, 80, 109, 110, 137-139, 389, 443, 666, 6667**
- **Emulate good hosts: MS-Exchange, Solaris/Oracle, MS-SQL, RedHat/Apache/Tomcat, WinXP Pro**
- **Emulate bad boxes: botnet servers, Warez server, trojaned workstations, Win95 workstation, backdoor**
- **Honeyd likely tool, or at least a starting point**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

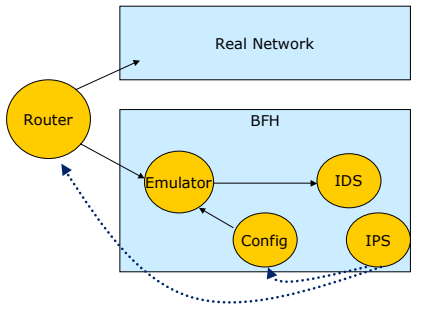
Hide in the open: Big freakin' haystack

- **Convert unused address space into decoy tripwire nets - 16,320,000 decoys to 200 "real" servers**
- **Stop swallowing packets: route unreachable hosts to the virtual honeynet**
- **190,000 decoys per "real" server = 99.9995% detection**
- **Any hits are malicious – route to IDS / IPS**
  - **Research attack profile**
  - **Throttle attack / drop packets**
  - **Block attackers for 1 hour, 2 hours, 24 hours, 1 week**
- **You've gained breathing room to respond to real attacks**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Hide in the open: Big freakin' haystack



INFORMATION SECURITY DECISIONS

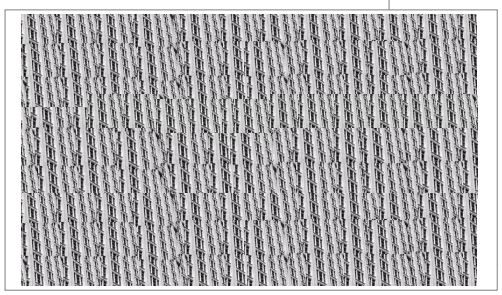
Hosted by SECURITY SearchSecurity.com

Security through obscurity?

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Hide in the open



INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

The fun has just begun…

LaBrea: SYN/ACK, TCP Window size = 0 (wait)

- **Use Tarpit to freeze a scan, run on random port**
- **Freezes Windows-based scanners up to 4 minutes**
- **Change window size to vary randomly, 0-15**
- **Scanning 10,000 hosts takes 27 days.**
- **Detecting 100 unpublished hosts in Class B network would take approximately 110 days**
- **Detecting 100 unpublished hosts in Class A would take approximately 112 years**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

The fun has just begun…

Storm Surge Mode**: active re-configuration**

- **Suppose your "standard" BFH net emulates:**
  - **25% Apache/Tomcat on RedHat 7**
  - **25% Win2003 / SQL-Server**
  - **25% Lotus Notes/Domino on Win2k Server**
  - **25% Oracle 9i on Solaris**
- **IDS telemetry reports spike in Win2k attacks**
- **BFH configuration changes:**
  - **30% Win2000 / SQL 6.5**
  - **30% Win2000 / Exchange**
  - **30% Win2000 / IIS**
  - **10% Allocated among 30 other server/workstation images**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

The fun has just begun…

- **Virtual honeynets: Make legitimate servers look like bogus servers**
- **Make all servers (fake & real) look identical**
- **BFH in your internal network**
  - **Malware outbreaks see your network with 16 million hosts**
  - **Ability to detect worms while slowing spread by 600x**
- **Simulate sendmail open relays – Death to spam!!**
- **If all Class A, B & C networks ran BFH:**
  - **Emulation of 12,493,209,429,306 bogus hosts**
  - **Port scans & profiling a thing of the past**
- **Worms and script kiddies would be economically infeasible**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Where do we go from here?

- **Tactical changes**
- **Strategic changes**
- **Open source vs. commercial**
- **Platform**
- **Network changes?**
  - **Firewall, router, switch, smart-switch, blades**
- **Unintended consequences: little guys get beat up**
- **Interactive, collaborative BFHnet**
- **Do we even NEED a firewall anymore, with BFH?**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

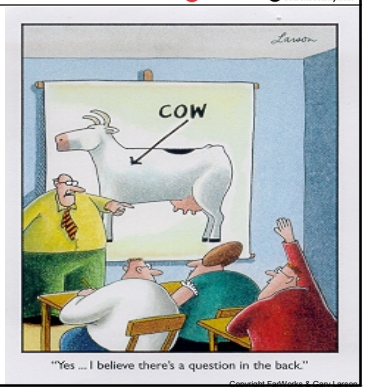
Summary

- **Stop script kiddies for $30k, seems like reasonable ROI**
- **Imagine if every class A, B & C network ran BFH**
  - **Emulation of 12,493,209,429,306 bogus hosts**
  - **Port scanning infeasible, profiling a moot point**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Q&A



INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Contact Information

Contact info: guru@xota.net

Further info:

"Submarine Warfare", August 2003 issue of Information Security Magazine:

http://infosecuritymag.techtarget.com

Big Freakin' Haystack Initiative:
http://sourceforge.net/projects/bfhi

Some images courtesy of The Weather Channel, NASA.
Trogdor the BURNiNATOR image courtesy homestarrunner.com