

© Whitepaper is supplement to the Cisco Press publication – *The ISP Essentials* by Barry Raveendran Greene, and Philip Smith. Materials can be used with the permission of the authors and Cisco Press.

SP Security Empowerment Materials

DRAFT 1.0

The following materials will help SPs, Hosting Centers, and Operators of any large network get details on a wide range of SP Security techniques. Many of these techniques are taking advantage of technologies that already exist in the network – it just takes a bit of time to empower yourself and deploy them. Many of the links are to materials with a Video on Demand (i.e. the NANOG Sessions and Cisco Powersessions). These help you hear from people who are doing the technique and/or created the technique – many from large networks themselves.

Questions

Feel free to ask questions via the following Cisco alias:

sp-security-questions@cisco.com

Location of this List

You can hyperlink to the follow FTP sites to gain access to this document:

<http://www.ispbook.com>

<ftp://ftp-eng.cisco.com/cons/isp/essentials/>

New Materials

Protecting Your Core: Infrastructure Protection Access Control Lists

Wednesday, January 11, 2006

ISP Essentials Supplement

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Infrastructure Protection on Cisco IOS Software-based Platforms

(Giving Lots of Hardware Examples)

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper0900aecd802b8f21.shtml

WHERE TO START

Public On-Line ISP Security Bootcamp - Singapore Summer 2003

<http://www.getitmm.com/bootcampflash/launch.html>

Sign-On:

<http://palomar.getitmm.com/bootcamp/>

Much of the materials presented in the ISP Security Bootcamp builds on and assumes a basic understanding of the principles in the ISP Essentials materials. This whitepaper is now a book - ISP Essentials which can be purchased through Cisco Press (<http://www.ciscopress.com/>) or through another on-line book store. The supplements for the book along with the tutorials, workshops, and bootcamps presented by Philip and I are at:

<ftp://ftp-eng.cisco.com/cons/>

or

<http://www.ispbook.com>

TEAM CYMRU Templates and Tools

Team CYMRU provides configuration templates, security templates, and other services to help make the Internet a safer place to network. These can be found at:

Cisco Systems, Inc.
170 West Tasman Drive.
San Jose, CA 95134-1706
Phone: +1 408 526-4000
Fax: +1 408 536-4100

<http://www.cymru.com/>

The Original Backscattered Traceback and Customer Triggered Remote Triggered Black Hole Techniques

<http://www.secsup.org/Tracking/>
<http://www.secsup.org/CustomerBlackHole/>

What is a BOTNET?

One of the best write ups is from a freeware tool gone commercial (I guess so they can scale).

<http://swatit.org/bots/index.html>

COMMUNITIES OF PEOPLE WORKING TOGETHER TO MITIGATE MISCREANT ACTIVITIES

+ Distributed Detection Systems Individuals and Organizations can Participate:

Dshield - www.dshield.org
My Netwatchman - www.mynetwatchman.com

NANOG SP SECURITY SEMINARS AND TALKS

The NANOG Coordination Committee actively works to product sessions and seminars to help foster security on the Internet. All sessions are taped and converted to VOD for all to use for their personal education. Over time, this effort has generated a valuable On-Line Tutorial for engineers and organizations seeking to learn more about running a more secure network.

NANOG Security Tutorial Series

Tutorial: Implementing a Secure Network Infrastructure (Part I)

<http://www.nanog.org/mtg-0310/kaeo.html>

Tutorial: ISP Security - Real World Techniques I - Remote Triggered Black Hole Filtering and Backscatter Traceback.

<http://www.nanog.org/mtg-0110/greene.html>

Tutorial: ISP Security - Real World Techniques II - Secure the CPE Edge

<http://www.nanog.org/mtg-0210/ispsecure.html>

Tutorial: ISP Security: Deploying and Using Sinkholes

<http://www.nanog.org/mtg-0306/sink.html>

Tutorial: Deploying IP Anycast

<http://www.nanog.org/mtg-0310/miller.html>

NANOG Security Sessions

Options for Blackhole and Discard Routing

<http://www.nanog.org/mtg-0410/soricelli.html>

ISP Security Toolkits

<http://www.nanog.org/mtg-0410/battles.html>

Botnets

<http://www.nanog.org/mtg-0410/kristoff.html>

What Will Stop Spam?

<http://www.nanog.org/mtg-0410/stiles.html>

DNSSEC Deployment: Big Steps Forward; Several Steps to Go

<http://www.nanog.org/mtg-0410/crocker.html>

Tracking Global Threats with the Internet Motion Sensor

<http://www.nanog.org/mtg-0410/bailey.html>

Implications of Securing Backbone Router Infrastructure

<http://www.nanog.org/mtg-0405/mcdowell.html>

Wednesday, January 11, 2006

ISP Essentials Supplement

Preparing RIR Allocation Data for Network Security Analysis Tasks

<http://www.nanog.org/mtg-0405/trammell.html>

Integrated Security for SNMP-Based Management

<http://www.nanog.org/mtg-0405/hardaker.html>

Watching Your Router Configurations and Detecting Those Exciting Little Changes

<http://www.nanog.org/mtg-0310/rancid.html>

Building a Web of Trust

<http://www.nanog.org/mtg-0310/abley.html>

The Relationship Between Network Security and Spam

<http://www.nanog.org/mtg-0310/spam.html>

Simple Router Security, What Every ISP Router Engineer Should Know and Practice

<http://www.nanog.org/mtg-0310/routersec.html>

Flawed Routers Flood University of Wisconsin Internet Time Server

<http://www.nanog.org/mtg-0310/plonka.html>

Trends in Denial of Service Attack Technology

<http://www.nanog.org/mtg-0110/cert.html>

Recent Internet Worms: Who Are the Victims, and How Good Are We at Getting the Word Out?

<http://www.nanog.org/mtg-0110/moore.html>

DoS Attacks in the Real World

<http://www.nanog.org/mtg-0110/irc.html>

Diversion & Sieving Techniques to Defeat DDoS

<http://www.nanog.org/mtg-0110/afek.html>

DNS Damage - Measurements at a Root Server

<http://www.nanog.org/mtg-0202/evi.html>

Protecting the BGP Routes to Top Level DNS Servers

<http://www.nanog.org/mtg-0206/bush.html>

BGP Security Update

<http://www.nanog.org/mtg-0206/barry.html>

Wednesday, January 11, 2006

ISP Essentials Supplement

Industry/Government Infrastructure Vulnerability Assessment: Background and Recommendations

<http://www.nanog.org/mtg-0206/avi.html>

A National Strategy to Secure Cyberspace

<http://www.nanog.org/mtg-0210/sachs.html>

How to Own the Internet in Your Spare Time

<http://www.nanog.org/mtg-0210/vern.html>

ISP Security BOF I

<http://www.nanog.org/mtg-0210/securebof.html>

The Spread of the Sapphire/Slammer Worm

<http://www.nanog.org/mtg-0302/weaver.html>

ISP Security BOF II

<http://www.nanog.org/mtg-0302/securebof.html>

The BGP TTL Security Hack

<http://www.nanog.org/mtg-0302/hack.html>

Security Considerations for Network Architecture

<http://www.nanog.org/mtg-0302/avi.html>

Lack of Priority Queuing on Route Processors Considered Harmful

<http://www.nanog.org/mtg-0302/gill.html>

Interception Technology: The Good, The Bad, and The Ugly!

<http://www.nanog.org/mtg-0306/schiller.html>

The NIAC Vulnerability Disclosure Framework and What It Might Mean to the ISP Community

<http://www.nanog.org/mtg-0306/duncan.html>

Inter-Provider Coordination for Real-Time Tracebacks

<http://www.nanog.org/mtg-0306/moriarity.html>

ISP Security BOF III

<http://www.nanog.org/mtg-0306/securitybof.html>

S-BGP/soBGP Panel: What Do We Really Need and How Do We Architect a Compromise to Get It?

Wednesday, January 11, 2006

ISP Essentials Supplement

<http://www.nanog.org/mtg-0306/sbgp.html>

BGP Vulnerability Testing: Separating Fact from FUD

<http://www.nanog.org/mtg-0306/franz.html>

BGP Attack Trees - Real World Examples

<http://www.nanog.org/mtg-0306/hares.html>

NRIC Best Practices for ISP Security

<http://www.nanog.org/mtg-0306/callon.html>

RIPE SP SECURITY PRESENTATIONS

RIPE-46 BoF: NSP-SEC (Hank Nussbacher)

<http://www.ripe.net/ripe/meetings/ripe-46/presentations/ripe46-nspbof-nsp-sec.pdf>

IRT Object in the RIPE Database (Ulrich Kiermayr)

<http://www.ripe.net/ripe/meetings/ripe-46/presentations/ripe46-nspbof-irt.pdf>

Operational Security Requirements (George M. Jones)

<http://www.ripe.net/ripe/meetings/ripe-46/presentations/ripe46-techsec-ops-security.pdf>

Infrastructure Security (Nicholas Fischbach)

<http://www.ripe.net/ripe/meetings/ripe-46/presentations/ripe46-nspbof-fischbach.pdf>

MPLS-Based Traffic Shunt PDF (Nicholas Fischbach)

<http://www.ripe.net/ripe/meetings/ripe-46/presentations/ripe46-eof-fischbach.pdf>

Address Space and AS Number Hijacking (Leslie Nobile, Leo Vegoda)

<http://www.ripe.net/ripe/meetings/ripe-48/presentations/ripe48-eof-nobile-vegoda.pdf>

Managing a DoS Attack (Vincent Gillet, Jean-michel Valey)

<http://www.ripe.net/ripe/meetings/ripe-48/presentations/ripe48-eof-gillet.pdf>

ETSI & Lawful Interception of IP Traffic (Jaya Baloo)

<http://www.ripe.net/ripe/meetings/ripe-48/presentations/ripe48-eof-etsi.pdf>

Securing a Core Network: Tutorial (Michael Behringer)

<http://www.ripe.net/ripe/meetings/ripe-49/presentations/ripe49-eof-security-tutorial.pdf>

CISCO SP SECURITY POWERSESSION SERIES

Service Providers Power Session in Dulles, Virginia, on October 20 and 21, 2004

<http://www.ciscotmme.com/go/securitypowersession/presentations.lasso>

Powersession on Core Security (4-6 May 2004)

<http://www.ciscoeventreg.net/go/networkers/agenda9.lasso>

CPN Summit SP Security Materials (April 2004)

<ftp://ftp-eng.cisco.com/cons/isp/security/CPN-Summit-2004/>

CISCO SP SECURITY MATERIALS

BGP 'Attack Tree' - Realities of BGP Security: Cisco's CIAG Team moves beyond the armchair hypothesizing of BGP Security Risk and runs test against the industry's multiple implementations of BGP

<http://www.in-people.cisco.com/sean/ciag-bgp-blackhatv2.pdf>