

The logo for SpecialOps Security features the word "SPECIALOPS" in a large, bold, green-to-white gradient font. Below it, the word "SECURITY" is written in a smaller, white, spaced-out font. The logo is centered on a black background that is part of a larger graphic design with yellow and grey elements.

SPECIALOPS
SECURITY

Network Strike Team!

Erik Pace Birkholz CISSP
PRESIDENT

NETWORK STRIKE TEAM



SPECIALOPSSECURITY.COM

Copyright © 2002-2005 Special Ops Security, Inc
All Rights Reserved • No duplication without explicit permission

888-R-U-OWNED

SLIDE 2

Introduction to Special Ops

Why start Special Ops Security, Inc.?

NETWORK STRIKE TEAM

- ▶ **Specialized security firms Foundstone, @Stake and Guardent were acquired in late 2004 by large, *product* vendors McAfee, Symantec, and VeriSign.**
- ▶ **This created a void for independent, well known security assessment and penetration testing players in the industry.**

Special Ops Security, Inc. is born!!!

NETWORK STRIKE TEAM

- ▶ **COSTA MESA, California--January 1, 2005--Special Ops Security, Inc., a network security training and consulting corporation, announced today the formal launch of the company with headquarters in Orange County, California.**

Where is Special Ops HQ?

NETWORK STRIKE TEAM



SPECIAL OPS
SECURITY

2727 NEWPORT BLVD :: SUITE 210
NEWPORT BEACH :: CALIFORNIA :: 92663

SPECIALOPSSecurity.COM

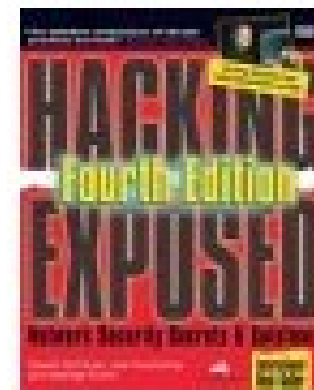
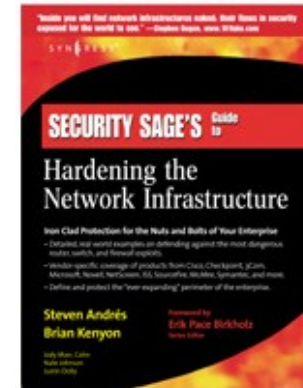
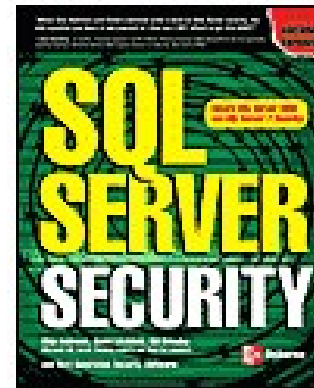
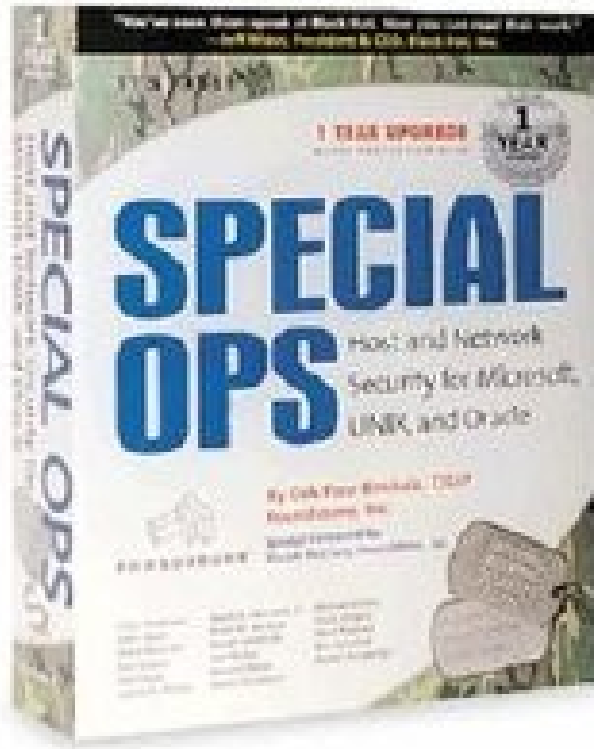
Copyright © 2002-2005 Special Ops Security, Inc
All Rights Reserved • No duplication without explicit permission

888-R-U-OWNED

SLIDE 6

Our team has authored 14 books

NETWORK STRIKE TEAM



SPECIALOPSSecurity.COM

Copyright © 2002-2005 Special Ops Security, Inc
All Rights Reserved • No duplication without explicit permission

888-R-U-OWNED

SLIDE 7

Security Assessment

NETWORK STRIKE TEAM

- ▶ **Security assessment can be thought of as incident prevention.**
 - ▷ Incidents are prevented by way of identification and remediation of vulnerabilities before they are exploited.

The Challenge

NETWORK STRIKE TEAM

- ▶ **The identification of new vulnerabilities, the introduction of changes to network architecture, and the deployment of new applications all make security a moving target.**

Security Assessment

NETWORK STRIKE TEAM

- ▶ **Why defensive security through offensive security assessment?**
 - ▷ Offensive security assessment allows organizations to understand their risk then make educated decisions about what and when to remediate.

A Moment of Clarity

NETWORK STRIKE TEAM

- ▶ **You need to make a decision, here and now. Are you willing to admit that your network wasn't secure yesterday and get proactive to increase your defenses for tomorrow?**
- ▶ **Forget *zero day*, we must begin planning for tomorrow by dealing with the negligence of yesterday.**
- ▶ **Perimeters, infrastructure devices, operating systems, applications and data must be assessed and appropriately fortified to mitigate the risks that threaten your organization.**

The Time is Now!

NETWORK STRIKE TEAM

- ▶ **Security professionals need to fight internally for money and resource allocation.**
- ▶ **Special Ops goal is to help our customers win the fight for budget and resources by identifying vulnerabilities and misconfigurations then documenting their potential impact on the business.**

What is Network Negligence?

NETWORK STRIKE TEAM

- ▶ **In my opinion, an organization should be considered negligent unless they have**
 - ▷ Assessed their current state of their security (posture)
 - ▷ Dealt with the high severity vulnerabilities, misconfigurations and architectural design flaws.
 - ▷ Implemented auditable procedures with accountability to reduce ongoing vulnerabilities and security misconfigurations. (or are in the process of doing so)

Why Assess Network Security?

NETWORK STRIKE TEAM

▶ **Some historical reasons for this focus**

- ▷ MS02-039 SQL UDP Resolution Buffer Overflow
 - ▲ Slammer
- ▷ MS03-026 RPC DCOM Buffer Overflow
 - ▲ Blaster
- ▷ MS04-011 LSASS Buffer Overflow
 - ▲ Sasser
- ▷ MS05-039 Plug and Play Buffer Overflow
 - ▲ Zobot

Bob Sapp's got my back and it is time to fight network negligence

NETWORK STRIKE TEAM



SPECIALOPSSECURITY.COM

Copyright © 2002-2005 Special Ops Security, Inc
All Rights Reserved • No duplication without explicit permission

888-R-U-OWNED

SLIDE 15

Hacking for the Masses!

NETWORK STRIKE TEAM

HACKING FOR THE MASSES



SPECIALOPSSSECURITY.COM

Copyright © 2002-2005 Special Ops Security, Inc
All Rights Reserved • No duplication without explicit permission

888-R-U-OWNED

SLIDE 17

www.Metasploit.com

NETWORK STRIKE TEAM



Metasploit Project

```
C:\ MSFConsole
# # ##### ##### ## #### ##### # ##### # #####
## ## # # # # # # # # # # # # # # #
# # # ##### # # # ##### # # # # # # #
# # # # # ##### # ##### # # # # #
# # # # # # # # # # # # # # # # #
# # ##### # # # ##### # ##### ##### # #

+ -- --=[ msfconsole v2.5 [105 exploits - 75 payloads]
msf > _
```

msfconsole v2.5
[105 exploits – 75 payloads]

Released 10/18/05
Includes 32 new exploits!

888-R-U-OWNED

SPECIALOPSSECURITY.COM

Copyright © 2002-2005 Special Ops Security, Inc
All Rights Reserved • No duplication without explicit permission

NETWORK STRIKE TEAM

The screenshot displays the Immunity Canvas application interface. At the top, there are tabs for Action, Helium, Listeners, Logging, Network Dump, and Hosts. The 'Listeners' tab is active, showing a table of exploits and a 'Listener Shell' window.

Name	Description
cam	cam.exe stack overflow.
emailsender	Sends email via SMTP
eznet	EZNet stack overflow
fp30reg	FP30REG.DLL Chunked Heap Overflow
harborlisten	Harbor Listen.exe
icecast	ICECAST exploit
iis5asp	IIS 5.0 .asp Heap Overflow
iis5ida	IIS 5.0 .ida Overflow
iis5mediaservices	IIS 5.0 Media Services Stack Overflow (nsis
iis5nsislog2	MX_STATS_LogLine IIS 5.0 Media Services S
iis5printer	IIS 5.0 .Printer Overflow
iis5webdav	IIS 5.0 WebDav Overflow
iisphonebook	Stack overflow vulnerability in the URL proc
imap4imap	imap4 stack overflow in Login field
ipswitch_cal	ipswitch calendar directory traversal
lssrv	License Logging Service Buffer Overflow
locator	MSRPC Locator Stack Overflow (runs only o
lsass	LSASRV.DLL LSASS.EXE stack overflow

The 'Listener Shell' window shows a list of actions: Download, Upload, cd, Spawn Process, Dir, pwd, Piped Command, and unlink. The 'Piped Command' field contains 'ipconfig'. Below the actions, network information is displayed:

```
Connection-specific DNS Suffix . :  
IP Address. . . . . : 10.10.10.60  
Subnet Mask . . . . . : 255.255.255.0  
IP Address. . . . . : 10.10.10.50  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.10.10.1
```

The status bar at the bottom shows a list of active listeners with their status and information:

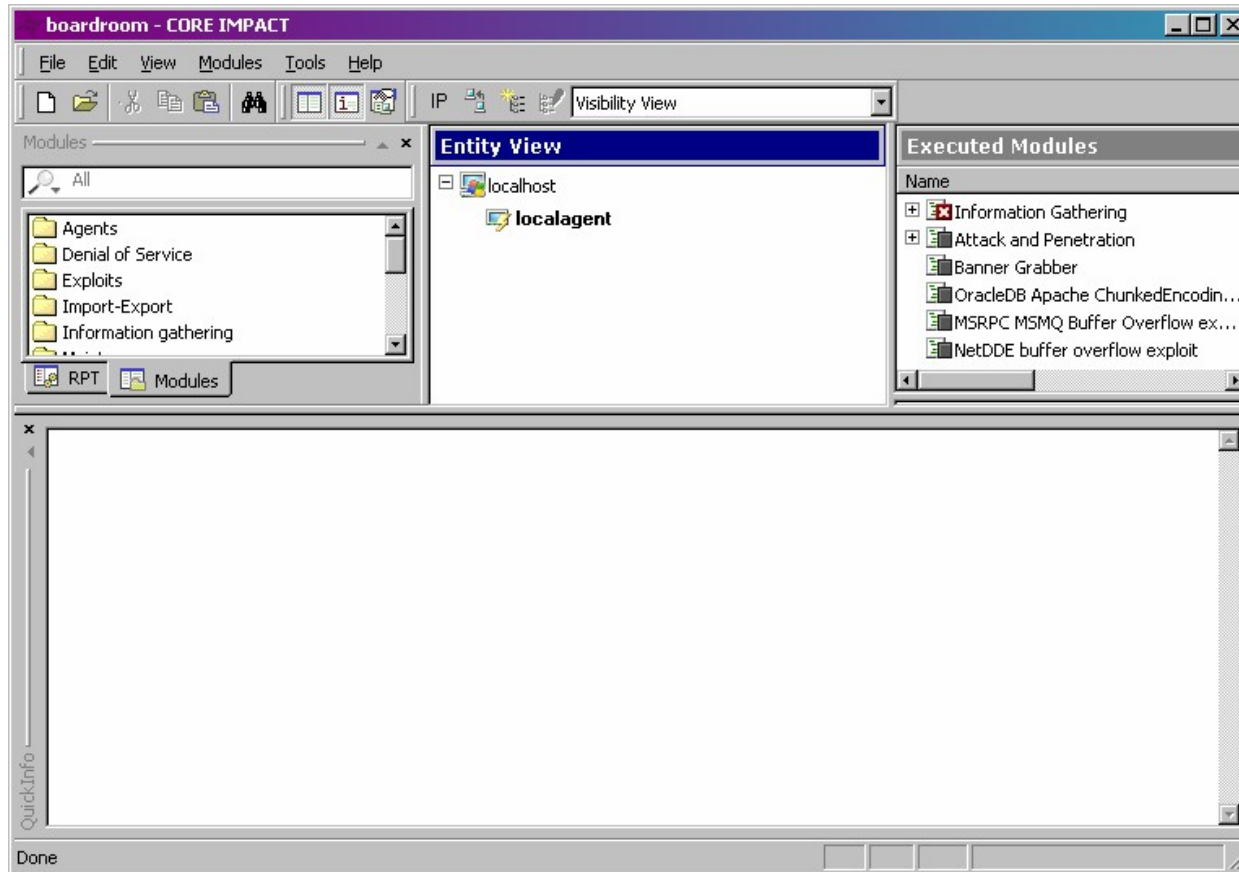
ID	Status	Information
5	██████	iis5webdav attacking 10.10.10.50:80
7	██████	iis5webdav attacking 10.10.10.30:80
8	██████	LSASRV.DLL LSASS.EXE DsRoleLogPrintRoutine() exploit attacking 10.10.10.50:135 (succeeded!)

The taskbar at the bottom shows the Start button and several open applications: MetaSploitExploits..., Shortcut to CMD..., Immunity Canvas..., Listener Shell, and untitled - Paint. The system clock shows 2:33 PM.

888-R-U-OWNED

CORE Impact – www.CoreSecurity.com

NETWORK STRIKE TEAM



888-R-U-OWNED

SPECIALOPSSECURITY.COM

Copyright © 2002-2005 Special Ops Security, Inc
All Rights Reserved • No duplication without explicit permission

SLIDE 20

Attacking Windows

NETWORK STRIKE TEAM

▶ **LSASS**

- ▷ MS04-007

▶ **Plug and Play**

- ▷ MS05-039

▶ **WINS**

- ▷ MS04-045

▶ **RPC DCOM**

- ▷ MS03-026

Attacking Microsoft IIS

NETWORK STRIKE TEAM

▶ IIS

▷ HTTP

- ▲ MS03-007 - IIS 5.0 WebDAV ntdll.dll Overflow

▷ HTTPS

- ▲ MS04-011 – SSL PCT Vulnerability

Attacking Microsoft SQL Server

NETWORK STRIKE TEAM

► SQL

▷ TCP: 1433

- ▲ Pre-authentication: MS02-056 – SQL Hello Overflow
- ▲ Brute Force Authentication

▷ UDP: 1434

- ▲ MS02-039 – SQL UDP Resolution

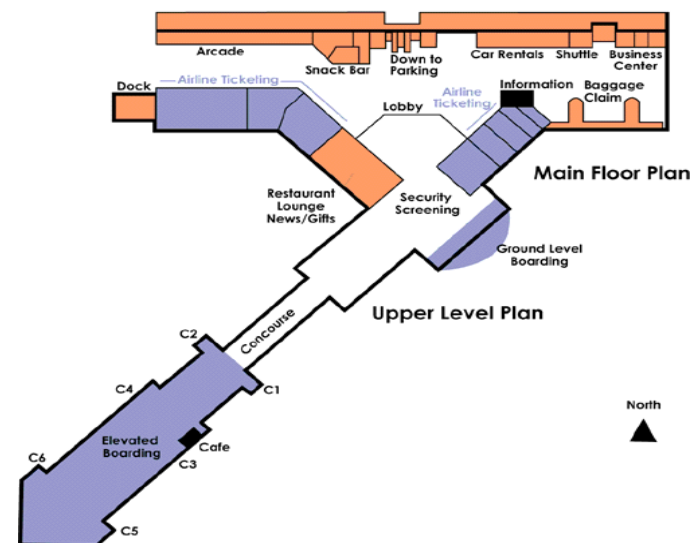
Asset Centric Security: Airport Model

Airport Model

NETWORK STRIKE TEAM

- ▶ Airport mitigates risk to its critical assets (**airplanes**) by implementing security zones (**terminals**) with multiple defensive layers

- ▶ Defense in Depth

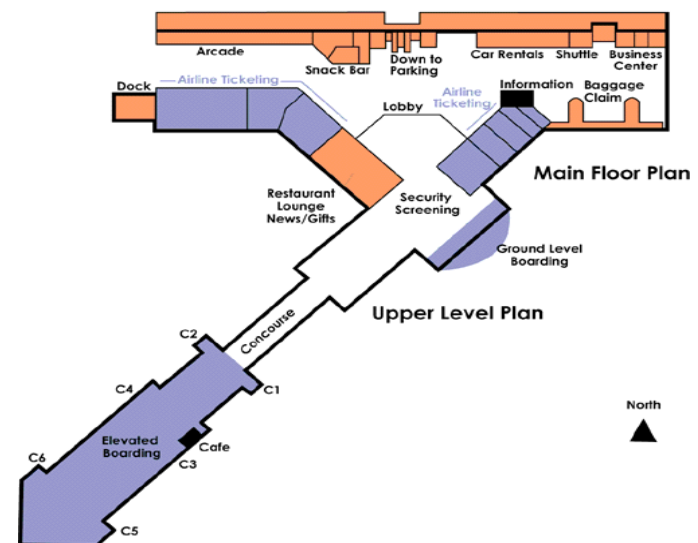


Airport Model

NETWORK STRIKE TEAM

- ▶ **Additionally, using diverse security mechanisms for each defensive layer risk is reduced further**

- ▶ **Defense in Diversity**



Airport Model

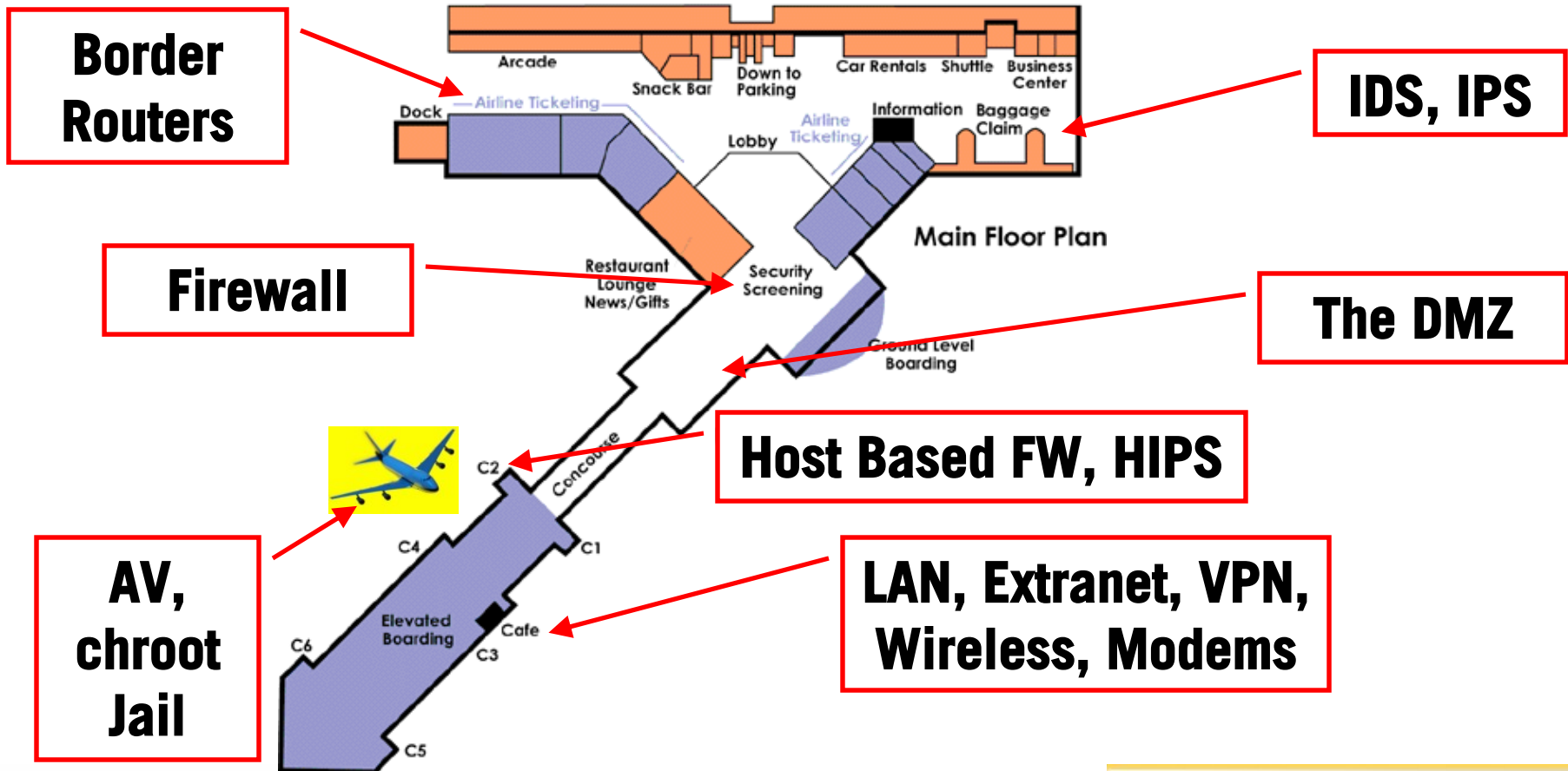
NETWORK STRIKE TEAM

▶ Multiple layers of protection can be applied to a Security Zone:

- ▷ The Check-in/Ticketing Area: **Border Routers**
- ▷ Security Screening: **Firewalls, Logging**
- ▷ The Concourse: **The DMZ**
- ▷ The Gates: **LAN, Extranets, VPN, Wireless, Modems**
- ▷ Baggage Handlers (x-ray, dogs, search): **IDS, IPS**
- ▷ Gate Agents: **Host Based (personal) Firewalls, HIPS**
- ▷ Reinforced Cockpit Doors: **AV, Chroot Jail**
- ▷ Airplanes and Passengers: **Assets**

Airport Model

NETWORK STRIKE TEAM



888-R-U-OWNED

SPECIALOPSSECURITY.COM

Copyright © 2002-2005 Special Ops Security, Inc
All Rights Reserved • No duplication without explicit permission

Questions & Answers

Thank you for attending!

Special Ops Security, Inc.

NETWORK STRIKE TEAM

Delivering tactical and strategic solutions that protect the people, processes and technology of our customers.

Erik Pace Birkholz, CISSP, IASSP, MCSE

erik@SpecialOpsSecurity.com

888.R.U.OWNED x187

www.SpecialOpsSecurity.com