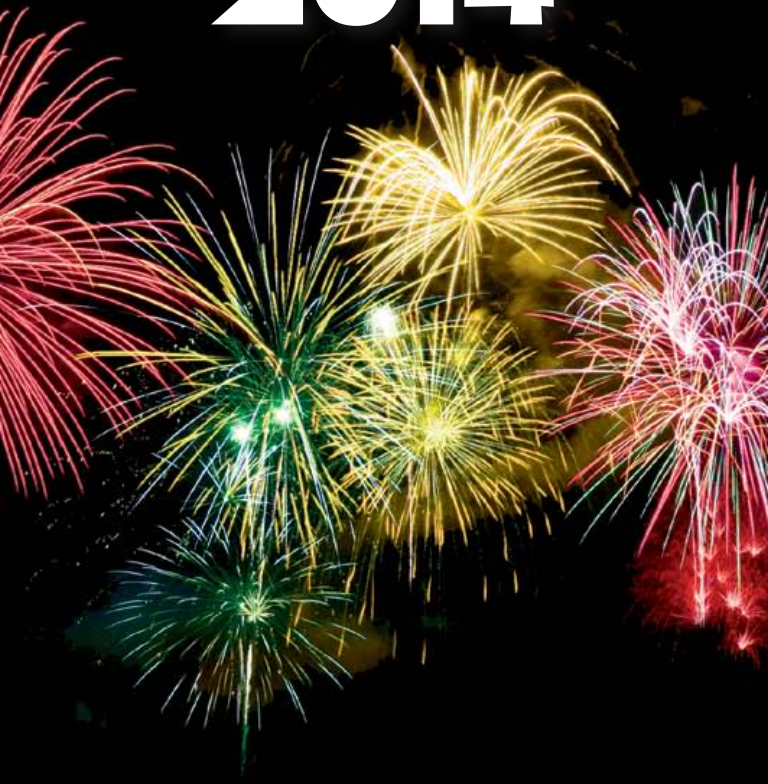
SANS 2014



PROGRAM GUIDE

April 5-14, 2014

Walt Disney World Dolphin

Orlando, FL

TABLE OF CONTENTS

NETWARS TOURNAMENTS

All students who register for a 5- or 6-day course will be eligible to play NetWars for FREE.

Register Now!
www.sans.org/event/sans-2014/schedule

SANS DFIR

Hosted by Rob Lee
Thursday, April 10 and Friday, April 11
6:30pm - 9:30pm | Southern Hemisphere Salon III

CORE NETWARS TOURNAMENT

Hosted by Ed Skoudis & Tim Medin
Thursday, April 10 and Friday, April 11
6:30pm - 9:30pm | Southern Hemisphere Salon II

GENERAL INFORMATION

Registration and Courseware Pick-up Information

Location: Northern Hemisphere Foyer

Saturday, April 5 (Short Courses Only) . . . . . 8:00am - 9:00am
Sunday, April 6 (Short Courses Only) . . . . . 8:00am - 9:00am
Sunday, April 6 (Welcome Reception) . . . . . 5:00pm - 7:00pm
Monday, April 7 . . . . . 7:00am - 5:30pm
Tuesday, April 8 - Saturday, April 12 . . . . . 8:00am - 5:30pm
Sunday, April 13 . . . . . 8:00am - 9:00am
Monday, April 14 . . . . . 8:00am - 9:00am (Closes)

Internet Café *(WIRED & WIRELESS)*

Location: Southern Foyer

Printer will be available for students' use

Monday, April 7 . . . . . Opens at noon - 24 hours
Tuesday, April 8 - Friday, April 11 . . . . . Open 24 hours
Saturday, April 12 . . . . . Closes at 2:00pm

Course Times

All full-day courses will run 9:00am - 5:00pm (unless noted)

Course Breaks

10:30am - 10:50am – Morning Break
12:15pm - 1:30pm – Lunch (On your own)
3:00pm - 3:20pm – Afternoon Break

First Time at SANS?

Please attend our ***Welcome to SANS*** briefing designed to help newcomers get the most from your SANS training experience. The talk is from **8:15am-8:45am** on **Monday, April 7** at the General Session in **Northern Hemisphere Salon B**.

GENERAL INFORMATION

Dining Options

We have assembled a short list of dining suggestions you may like to try during lunch breaks. See page 23 of this booklet.

Feedback Forms and Course Evaluations

The SANS planning committee wants to know what we should keep doing and what we need to improve – but we need your help! Please take a moment to fill out an evaluation form after each course and drop it in the evaluation box.

Social Board

You can post open invites to lunch, dinner or other outings. Located on the Bulletin Board near the Registration Desk.

Wear Your Badge and Course Ticket Daily

To make sure you are in the right place, the SANS door monitors will be checking your badge and course tickets for each course you enter. For your convenience, please wear your badge and course ticket at all times.

Lead a BoF! (Birds of a Feather Session)

Whether you are an expert or just interested in keeping the conversation going, sign up and suggest topics at the BoF board near registration. If you have questions, leave a message with your contact information with someone at the registration desk in the Convention Foyer.

Bootcamp Sessions and Extended Hours

The following classes have evening bootcamp sessions or extended hours. For specific times, please refer to pages 4-6.

Bootcamps (Attendance Mandatory)

MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam

SEC401: Security Essentials Bootcamp Style

SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking

Extended Hours:

MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™

SEC504: Hacker Techniques, Exploits & Incident Handling

SEC560: Network Penetration Testing and Ethical Hacking

COURSE SCHEDULE

START DATE: **Saturday, April 5**

Time: 9:00am - 5:00pm (Unless otherwise noted)

SEC434: Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting
Instructor: Jake Williams . . . . . .Location: Oceanic 5

SEC546: IPv6 Essentials
Instructor: Dr. Johannes Ullrich . . . . . .Location: Oceanic 6

MGT433: Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program
Instructor: Lance Spitzner . . . . . .Location: Oceanic 8

START DATE: **Sunday, April 6**

Time: 9:00am - 5:00pm (Unless otherwise noted)

MGT305: Technical Communication and Presentation Skills for Security Professionals
Instructor: G. Mark Hardy . . . . . Location: Europe 4

MGT415: A Practical Introduction to Risk Assessment
Instructor: James Tarala. . . . . Location: Europe 5

MGT535: Incident Response Team Management
Instructor: Alissa Torres . . . . . Location: Europe 6

START DATE: **Monday, April 7**

Time: 9:00am - 5:00pm (Unless otherwise noted)

SEC301: Intro to Information Security
Instructor: Fred Kerby . . . . . Location: Asia 2

SEC401: Security Essentials Bootcamp Style
Instructor: Dr. Eric Cole . . . . . Location: S. H. Salon I
Bootcamp Hours: 5:00pm - 7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials - Enterprise Defender
Instructor: Paul A. Henry . . . . . Location: N. H. Salon E4

SEC502: Perimeter Protection In-Depth
Instructor: Bryce Galbraith . . . . . .Location: Oceanic 7

SEC503: Intrusion Detection In-Depth
Instructor: Mike Poor. . . . . Location: Americas Seminar

SEC504: Hacker Techniques, Exploits, and Incident Handling
Instructor: John Strand. . . . . .Location: N. H. Salon D
Extended Hours: 5:00pm-6:30pm (Course Day 1 only)

SEC505: Securing Windows with the Critical Security Controls
Instructor: Jason Fossen. . . . . .Location: Oceanic 6

SEC542: Web App Penetration Testing & Ethical Hacking
Instructor: Seth Misenar . . . . . .Location: N. H. Salon C

COURSE SCHEDULE

SEC560: Network Penetration Testing and Ethical Hacking
Instructor: Ed Skoudis . . . . . .Location: S. H. Salon II
Extended Hours: 5:00pm-6:30pm (Course Day 1 only)

SEC561: Intense Hands-on Pen Testing Skill Development
Instructor: Tim Medin . . . . . .Location: Oceanic 8

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
Instructor: James Tarala . . . . . Location: Asia 3

SEC575: Mobile Device Security and Ethical Hacking
Instructor: Joshua Wright. . . . . Location: Australia 3

SEC579: Virtualization and Private Cloud Security
Instructor: Dave Shackleford . . . . . .Location: Oceanic 5

SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses
Instructor: Larry Pesce . . . . . Location: N. H. Salon A3

SEC642: Advanced Web App Penetration Testing and Ethical Hacking
Instructor: Justin Searle . . . . . Location: N. H. Salon A1

SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking
Instructor: Stephen Sims . . . . . Location: Asia 1
Bootcamp Hours: 5:15pm-7:00pm (Course days 1-5)

DEV522: Defending Web Applications Security Essentials
Instructor: Dr. Johannes Ullrich . . . . . Location: N. H. Salon A4

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
Instructor: Gregory Leonard . . . . . Location: Europe 4

DEV544: Secure Coding in .NET: Developing Defensible Applications
Instructor: Eric Johnson . . . . . Location: Europe 5

FOR408: Windows Forensic Analysis
Instructor: Ovie Carroll . . . . . Location: S. H. Salon III

FOR508: Advanced Computer Forensic Analysis and Incident Response
Instructor: Rob Lee . . . . . Location: S. H. Salon IV

FOR526: Memory Forensics In-Depth
Instructor: Alissa Torres. . . . . Location: Australia 2

FOR572: Advanced Network Forensics and Analysis
Instructors: Philip Hagen, George Bakos. . . . . Location: N. H. E3

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Instructor: Lenny Zeltser . . . . . .Location: S. H. Salon V

COURSE SCHEDULE

START DATE: **Monday, April 7** (CONTINUED)
Time: 9:00am - 5:00pm (Unless otherwise noted)

MGT414: SANS® +S™ Training Program for the CISSP® Cert Exam
Instructor: Eric Conrad . . . . . Location: N. H. Salon E2
Bootcamp Hours: 8:00am – 9:00am (Course days 2-6) &
5:00pm - 7:00pm (Course days 1-5)

MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™
Instructor: G. Mark Hardy . . . . . Location: Asia 5
Extended Hours: 5:00pm – 6:00pm (Course days 1-4)

MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep
Instructor: Jeff Frisk . . . . . Location: N. H. Salon E1

AUD444: Auditing Security and Controls of Active Directory and Windows
Instructors: Tanya Baccam, Bryan Simon. . . . . Location: Europe 3

AUD507: Auditing Networks, Perimeters, and Systems
Instructor: David Hoelzer. . . . . Location: N. H. Salon A2

LEG523: Law of Data Security and Investigations
Instructor: Benjamin Wright . . . . . Location: Asia 4

HOSTED: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program
Instructor: EJ Jones . . . . . Location: Europe 6

START DATE: **Thursday, April 10**
Time: 9:00am - 5:00pm (Unless otherwise noted)

AUD445: Auditing Security and Controls of Oracle Databases
Instructors: Tanya Baccam, Bryan Simon. . . . . Location: Europe 3

DFIR NetWars Tournament
Host: Rob Lee . . . . . Location: S. H. Salon III
Hours: 6:30pm - 9:30pm

Core NetWars Tournament
Hosts: Ed Skoudis, Tim Medin . . . . . Location: S. H. Salon II
Hours: 6:30pm - 9:30pm

START DATE: **Sunday, April 13**
Time: 9:00am - 5:00pm (Unless otherwise noted)

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Instructor: Eric Conrad . . . . . Location: Oceanic 5

HOSTED: Physical Penetration Testing – Introduction
Instructor: Deviant Ollam. . . . . Location: Oceanic 6

SPECIAL EVENTS

Enrich your SANS experience!

Morning and evening talks given by our faculty and selected subject matter experts help you broaden your knowledge, get the most for your training dollar, and hear from the voices that matter in computer security.

SUNDAY, APRIL 6

Registration Welcome Reception

Sunday, April 6 | 5:00pm - 7:00pm | Location: Convention Foyer

Register early and network with your fellow students!

STI MASTER'S PRESENTATION

Building and Managing a PKI Solution for a Small and Medium-Size Business

Speaker: Wylie Shanks — Master's Degree Candidate

Sunday, April 6 | 7:30pm - 8:10pm | Location: Asia 3

Microsoft Windows, Mac OS X, open source, and third-party (cloud) PKI solutions are analyzed for their ease of installation, use, management, and overall cost to operate for small to medium size businesses.

MONDAY, APRIL 7

General Session - Welcome to SANS

Speaker: Rob Lee

Monday, April 7 | 8:15am - 8:45am | Location: N. H. Salon B

SANS Technology Institute Open House

Speaker: Alan Paller

Monday, April 7 | 6:00pm - 7:00pm | Location: Asia 4

SANS Technology Institute Master of Science degree programs offer candidates an unparalleled opportunity to excel in the two aspects of security that are most important to the success of their employer and their own careers: management skills and technical mastery.

SANS Online Training Pool Party

Monday, April 7 | 6:15pm - 7:15pm | Location: Swan Lap Pool Terrace

Join us poolside for fun, prizes, and of course, some talk about SANS' fantastic four online training formats. The basics and benefits of taking vLive, OnDemand, Simulcast, or SelfStudy courses will be the relaxed focus, presented by a top SANS instructor with the backdrop of a warm Florida sunset. It's your pre-keynote party — don't miss it!

SPECIAL EVENTS

KEYNOTE

APT Attacks Exposed: Network, Host, Memory, and Malware Analysis

Speakers: Rob Lee, Ovie Carroll, Alissa Torres, Phil Hagen, and Lenny Zeltser

Monday, April 7 | 7:15pm - 9:15pm | Location: N. H. Salon B

For many years, professionals have been asking to see real APT data in a way that shows them how the adversaries compromise and maintain presence on our networks. Now you can experience it first hand – using real data. The SANS Digital Forensics and Incident Response team will take you through an end-to-end investigation similar to briefs that are supplied to C-level executives who want to understand how their network was compromised and how these adversaries think, act, and move around their enterprise.

This talk is perfect for those in the trenches or for those in management who really want to understand how a response team identifies and responds to these adversaries. What is it they are after? How did they get in? How did our systems fail to detect them? These questions and more will be answered in this one-of-a-kind keynote.

TUESDAY, APRIL 8

ICS Cybersecurity in an Interconnected World

Speaker: Wally Magda

Tuesday, April 8 | 12:30pm - 1:15pm | Location: Americas Seminar

Industrial Control Systems, such as SCADA, are the "brains" of critical infrastructure, providing the vital functions of control and monitoring necessary to operate the Bulk Electric System. Since they were designed for functionality and performance, cybersecurity was not a primary consideration. During this session, we will discuss SCADA threat vectors, possible consequences, and some horror stories. Many of the actions presented to protect the utility and its customers can be applied to all Industrial Control Systems.

Space is limited and registration is required. Lunch is provided.

How to Become a SANS Instructor

Speaker: John Strand

Tuesday, April 8 | 12:30pm - 1:15pm | Location: N. H. Salon D

Have you ever wondered what it takes to teach for SANS? Would you like to train others in your own organization or local community? Join us for a lunch and learn where we'll share with you what it takes to become a Certified SANS Instructor. John Strand started as a Mentor and will be sharing his own story along with some "behind the scenes" stories that are sure to make you laugh.

Space is limited and registration is required. Lunch is provided.

SPECIAL EVENTS

Women in Technology Meet and Greet

Speaker: Karen Fioravanti | Tuesday, April 8 | 6:15pm - 7:15pm
Location: Crescent Terrace – Walt Disney World Swan

From Jean Jennings Bartik to Diane Greene, women have always been a driving force in the field of information technology. Their experiences have been filled not only with stories of overcoming challenges but also ones of innovation and inspiration. Join us to hear some of these stories and come share your own. After the discussions, stay and network with other conference attendees.

STI MASTER'S PRESENTATION

RapidTriage: An Automated Approach to System Intrusion Discovery

Speaker: Trenton Bond – Master's Degree Candidate
Tuesday, April 8 | 7:15pm - 7:55pm | Location: Asia 3

Effective system intrusion discovery is a critical component of the information security incident handling process. The SANS Institute publishes system intrusion discovery cheat sheets that are invaluable guides to help identify indicators of compromise. We'll look at how the RapidTriage Python tool can automate system data collection based on these guides, speeding up the initial triage and ensuring consistency across multiple systems and platforms.

SANS@NIGHT

Effective Phishing that Employees Like

Speaker: Lance Spitzner
Tuesday, April 8 | 7:15pm - 8:15pm | Location: N. H. Salon D

One of the toughest challenges in establishing a high-impact security awareness program is measuring the impact. Are you changing behavior and reducing risk? Phishing assessments are a powerful way to measure such change, while addressing one of the most common human risks. As more organizations use phishing assessments, many of them are doing it wrong, not only negatively impacting their metrics but generating resentment among employees. In this short presentation, learn how to create a fun, engaging phishing program that not only effectively measures and reinforces key behaviors, but is also truly enjoyed by employees.

STI MASTER'S PRESENTATION

A Hands-on XML External Entity Vulnerability Training Module

Speaker: Carrie Roberts – Master's Degree Candidate
Tuesday, April 8 | 8:15pm - 8:55pm | Location: Asia 3

Many web applications that accept and respond to XML requests are vulnerable to XML External Entity (XXE) attacks due to default XML parser settings. This vulnerability can be exploited to read arbitrary files from the server. This presentation will describe the issue and introduce a freely downloadable training module. The training module virtual machine image can be used to provide engaging, hands-on XXE training for developers and intrusion analysts. I will demonstrate exploitation tools and techniques for reading the sample applications sensitive configuration files and describe a simple method for removing the vulnerability. Network analysis of an attack will also be shown.

SPECIAL EVENTS

SANS@NIGHT

An Introduction to PowerShell for Security Assessments

Speaker: James Tarala
Tuesday, April 8 | 8:15pm - 9:15pm | Location: N. H. Salon C

With the increased need for automation in operating systems, every platform now provides a native environment for automating repetitive tasks via scripts. Since 2007, Microsoft has gone all in with their PowerShell scripting environment, providing access to every facet of the Microsoft Windows operating system and services via a scriptable interface. Administrators can completely administer and audit not only an operating system from this shell, but most all Microsoft services, such as Exchange, SQL Server, and SharePoint services as well. In this presentation James Tarala of Enclave Security will introduce students to using PowerShell scripts for assessing the security of these Microsoft services. Auditors, system administrators, penetration testers, and others will all learn practical techniques for using PowerShell to assess and secure these vital Windows services.

SANS@NIGHT

Securing The Kids

Speaker: Lance Spitzner
Tuesday, April 8 | 8:15pm - 9:15pm | Location: N. H. Salon D

Technology is an amazing tool. It allows our kids to access a tremendous amount of information, meet new people, and communicate with friends around the world. In addition, for them to be successful in the 21st century, they have to know and understand how to leverage these new tools. However, with all these capabilities come a variety of new risks – risks that as parents you may not understand or even be aware of. In this one-hour presentation, we cover the top-three risks to kids online and the top-five steps you can take to protect them. This course is based on the experiences and lessons learned from a variety of SANS top instructors who not only specialize in security, but are parents just like you. This talk is sponsored and delivered by SANS Securing The Human program.

SANS@NIGHT

Social Engineering for Pentesters

Speaker: Dave Shackleford
Tuesday, April 8 | 8:15pm - 9:15pm | Location: Americas Seminar

As more advanced enterprise pen testing teams assess their organizations' security posture, most discover over time that the weakest link in their security is in fact the end users. In numerous high-profile breaches reported in the last several years, social engineering of end users played a pivotal role in the attackers' success. To properly emulate the threats we face today, pen testers need to perform social engineering attacks, as well, with the goal of identifying current vulnerabilities in user behavior and helping educate the organization on how attackers can take advantage of people. In this presentation, Dave will discuss the need for social engineering in pen testing programs and engagements, how social engineering fits into a larger security program, and various tools and tactics pen testers can use to better assess security awareness through targeted social engineering.

WEDNESDAY, APRIL 9

Vendor Solutions Expo

Wednesday, April 9 | 12:00pm - 1:30pm | 5:00pm - 7:00pm
Location: N. H. Salon B

All attendees are invited to meet with established and emerging solution providers as they reveal the latest tools and technologies critical to information security. The SANS Vendor Expo showcases product offerings from key technology providers in the commercial tools and services market. Vendors arrive prepared to interact with a technically savvy audience. You'll find demonstrations and product showcases that feature all the best that the security industry has to offer!

SANS@NIGHT

RTC Security

Speaker: Jason Ostrom
Wednesday, April 9 | 7:15pm - 8:15pm | Location: Americas Seminar

RTC (real-time communications) is an acronym the industry is adopting for communication applications that have a real-time requirement for media. This includes not only VoIP and unified communications, but also a new kid in town: WebRTC. WebRTC is an open and free project that uses Javascript APIs enabling web browsers to do peer-to-peer media sessions, such as VoIP, IM, and HD Video chat sessions – all with zero plugins. Supporting Google Chrome, Firefox, and Opera in desktop and Android versions, this effectively renders a media engine in the web browser. With WebRTC, the user must explicitly opt-in for the web application to take control of their microphone and camera streams. This is exciting and promises many benefits, yet it raises some serious security considerations for web application security. This presentation will discuss RTC Security. Key takeways will be remote SIP trunk architectures and security issues to assess. The presentation will also introduce WebRTC and its security architecture.

STI MASTER'S PRESENTATION

Security Static Vulnerable Devices

Speaker: Chris Farrell – Master's Degree Candidate
Wednesday, April 9 | 7:15pm - 7:55pm | Location: Asia 3

Many computing devices today are deployed with a static configuration that cannot be modified due to governance restrictions (i.e., FDA-Approved Medical Devices). This excludes these devices from operating system, anti-virus, and exploit signature updates that would normally be used to protect these devices. As a result, these critical devices are more vulnerable to compromise. Since most of these devices have to communicate with other production systems, segmentation has had limited success in protecting them. Due to advances in next-generation firewalls, we should no longer leave these devices unprotected. It is now possible to protect them while still maintaining the static configuration. If properly configured for virtual networks (VLANS), thousands of previously-insecure devices can be granted the same protections given to modifiable devices.

SANS@NIGHT

Analyzing a Second-Hand ATM (Automated Teller Machine)

Speaker: Erik Van Buggenhout
Wednesday, April 9 | 7:15pm - 8:15pm | Location: N. H. Salon D

ATMs are the main component of self-servicing banking functions used by millions of banking customers worldwide. In Europe alone, as of 30 June 2013, 400,000 ATM devices were deployed and this number is expected to further increase in the next few years. We did our part and also purchased an ATM device in early 2014! During this talk, we will summarize our approach and the initial results of our research activities.

SANS@NIGHT

Windows Exploratory Surgery with Process Hacker

Speaker: Jason Fossen
Wednesday, April 9 | 7:15pm - 8:45pm | Location: N. H. Salon C

In this talk we'll rummage around inside the guts of Windows while on the lookout for malware, using a free tool named Process Hacker (similar to Process Explorer). Understanding processes, threads, drivers, handles, and other OS internals is important for analyzing malware, doing forensics, troubleshooting, and hardening the OS. If you have a laptop, get Process Hacker from SourceForge.net and together we'll take a peek under the GUI to learn about Windows internals and how to use Process Hacker for combating malware. http://processhacker.sourceforge.net

SANS@NIGHT

Pillage the Village!

Speaker: Mike Poor
Wednesday, April 9 | 8:15pm - 9:15pm | Location: N. H. Salon D

Many Penetration testers worry so much about pwn'ing this and getting domain admin on that, that they forget to pillage the boxes and networks they compromise. From hacking in-flight entertainment systems, web applications and hardware, we will go through examples from penetration tests where the hidden tidbits we found made the test.

SANS@NIGHT

How I Learned to Stop Worrying and be Agile!

Speaker: James Leyte-Vidal
Wednesday, April 9 | 8:15pm - 9:15pm | Location: Americas Seminar

How do you put security in and around an environment that deploys every two weeks, every week, every day, or even multiple times a day? We've faced it and you can too. Join James Leyte-Vidal to talk about some of the opportunities Agile presents for today's information security team.

STI MASTER'S PRESENTATION

The Security Onion Cloud Client: Network Security Monitoring for the Cloud

Speaker: Joshua Brower – Master's Degree Candidate

Wednesday, April 9 | 8:15pm - 8:55pm | Location: Asia 3

With "cloud" servers continuing to become ever more popular, along with typical off-site servers (VPS & Dedicated), Network Security Monitoring (NSM) practitioners struggle to gain insight into these devices, as they usually don't have the ability to tap the network traffic flowing to and from these servers. To solve this problem, I propose designing a cross platform NSM client that would integrate with Security Onion, a NSM-centric Linux distribution. Essentially, the NSM client would copy traffic (near real time) to the Security Onion Sensor, which would then process the data as it would any other network tap. This would allow NSM practitioners the visibility they need into their off-site servers that are not in a setting where a typical NSM setup would suffice.

THURSDAY, APRIL 10

GIAC Program Overview

Speaker: Jeff Frisk

Thursday, April 10 | 6:00pm - 6:45pm | Location: N. H. Salon D

GIAC is the leading provider and developer of Information Security Certifications. GIAC tests and validates the ability of practitioners in information security, forensics, and software security. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by government, military, and industry to protect the cyber environment.

SANS DFIR NETWARS TOURNAMENT

Host: Rob Lee

Thu, April 10 & Fri, April 11 | 6:30pm - 9:30pm | Location: S. H. Salon III

SANS DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges covering host forensics, network forensics, and malware and memory analysis. It is developed by incident responders and analysts who use these skills daily to stop data breaches and solve crimes. Sharpen your team's skills prior to being involved in a real incident.

CORE NETWARS TOURNAMENT

Hosts: Ed Skoudis & Tim Medin

Thu, April 10 & Fri, April 11 | 6:30pm - 9:30pm | Location: S. H. Salon II

Core NetWars is a computer and network security challenge designed to test a participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars OnSites to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you'll build a wide variety of skills while having a great time.

SANS@NIGHT

Continuous Ownage: Why you Need Continuous Monitoring

Speakers: Seth Misenar and Eric Conrad

Thursday, April 10 | 7:15pm - 8:15pm | Location: N. H. Salon D

Repeat after me, I will be breached. Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending Seth Misenar and Eric Conrad's new course: SEC511: Continuous Monitoring and Security Operations.

SANS@NIGHT

How the West was Pwned

Speaker: G.Mark Hardy

Thursday, April 10 | 7:15pm - 8:15pm | Location: N. H. Salon C

Can you hear it? The giant sucking sound to the East? With it are going more than just manufacturing jobs – it's our manufacturing know-how, intellectual property, military secrets, and just about anything you can think of. If we're so technologically advanced, how are the People's Republic of China (PRC) and others able to continue to pull this off? Why do we keep getting pwned at our own game?

There has been much talk about "cyberwar," but there may not be a war. If a victor can extract tribute from the vanquished, war isn't necessary. Today, intellectual capital is a proxy for tribute. We'll look at some specifics, including documents that outline the plan of attack, details about what operations have been run against us, and progress in efforts to create an international legal framework for when the bits start flying.

SANS@NIGHT

The Law of Offensive Countermeasures, Active Defense, or Whatever You Wanna Call It

Speaker: Benjamin Wright

Thursday, April 10 | 7:15pm - 8:15pm | Location: N. H. Salon D

The range of steps that a good guy might take relative to a bad guy is limited only by imagination. As our imagination invents new steps, we use metaphors like 'honeypot,' 'sinkhole' and 'hacking back' to describe what's going on. But when we try to fit these metaphors into law, confusion erupts. This presentation will only compound the confusion. Come join the raucous discussion.

SANS@NIGHT

Introduction to IDA Pro and Debugging

Speaker: Stephen Sims

Thursday, April 10 | 8:15pm - 9:15pm | Location: N. H. Salon C

In this presentation, Stephen will discuss the most commonly used features and plugins for IDA Pro and WinDbg from an exploitation perspective. You will learn about IDA navigation, IDAPython and IDC scripting, remote debugging, and Kernel debugging. The presentation will be 50% lecture and 50% demonstration. Feel free to bring a demo or licensed version of IDA and WinDbg to play along.

SANS@NIGHT

Hacking Back, Active Defense, and Internet Tough Guys

Speaker: John Strand

Thursday, April 10 | 8:15pm - 9:15pm | Location: N. H. Salon D

In this presentation John Strand will demonstrate the Active Defense Harbinger Distribution, a DARPA funded, free Active Defense virtual machine. He will debunk many of the myths, outright lies, and subtle confusions surrounding taking active actions against attackers. From this presentation, you will not only know how to take action against attackers, you will learn how to do it legally.

FRIDAY, APRIL 11

SANS@NIGHT

Evolving VoIP Threats

Speaker: Paul A. Henry

Friday, April 11 | 7:15pm - 8:15pm | Location: N. H. Salon C

VoIP is thriving in an otherwise down economy – VoIP implementations are growing, driven by cost savings. Cost is typically the only consideration in the implementation of VoIP – it is all about saving money. Security, if considered at all, is clearly an afterthought. Too many still dismiss VoIP threats as theoretical. VoIP can afford significant costs savings while not sacrificing an organization's security. Recognizing the threats and implementing the compensating and technical controls can make all the difference in a successful VoIP implementation.

SANS@NIGHT

What is bWAPP? Web Application Penetration Testing with bWAPP

Speaker: Malik Mesellem

Friday, April 11 | 7:15pm - 8:15pm | Location: N. H. Salon D

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP prepares one to conduct successful web application penetration testing and ethical hacking projects.

What makes bWAPP so unique? Well, it has over 60 web vulnerabilities! It covers all major known web bugs, including all risks from the OWASP Top 10 project.

Defense is needed...superbees are wanted!

SANS@NIGHT

There's *GOLD* in Them Thar Package Management Databases!

Speaker: Phil Hagen

Friday, April 11 | 8:15pm - 9:15pm | Location: N. H. Salon C

There is a lot of useful file metadata stored in package management databases for popular Linux distributions. The RedHat Package Manager (RPM) and Debian's dpkg are two examples. We'll focus on how to leverage RPM in forensic investigations, as it can provide a quick and effective way to find changed files that warrant more in-depth analysis. We'll also discuss potential shortfalls to consider in using this method.

SANS@NIGHT

How to Spy on your Employees with Memory Forensics

Speakers: Jacob Williams and Alissa Torres

Friday, April 11 | 8:15pm - 9:15pm | Location: N. H. Salon D

Many companies can't afford employee endpoint monitoring software such as SpectorPro, and yet still have the need to figure out how a rogue employee is spending his time on the job. Consider a cheaper solution for employee spying- one that makes use of native Windows services and an investigator's ninja memory analysis skills. Whether it be creating a scheduled task to send a machine to hibernate or instantiating an unsuspected memory dump, targeted employee spying can be done on the cheap. Through process enumeration, browsing history reconstruction and memory-mapped file extraction, watch as your presenters piece together what our trusted insider was doing on their company computer, unbeknownst to his boss. Even if you don't have the need to covertly investigate a rogue employee (yet), this talk will arm you the knowledge to know what is within the realm of the possible.

VENDOR EVENTS

Vendor Solutions Expo

Wednesday, April 9 | 12:00pm - 1:30pm | 5:00pm - 7:00pm
Location: N. H. Salon B

All attendees are invited to meet with established and emerging solution providers as they reveal the latest tools and technologies critical to information security. The SANS Vendor Expo showcases product offerings from key technology providers in the commercial tools and services market. Vendors arrive prepared to interact with a technically savvy audience. You'll find demonstrations and product showcases that feature all the best that the security industry has to offer!

Vendor Welcome Reception: PRIZE GIVEAWAYS!!! – Passport to Prizes

Wednesday, April 9 | 5:00pm - 7:00pm | Location: N. H. Salon B

This informal reception allows you to visit exhibits and participate in some exciting activities. This is a great time to mingle with your peers and experience firsthand the latest in information security tools and solutions with interactive demonstrations and showcase discussions. Enjoy appetizers and beverages and compare experiences with other attendees regarding the solutions they are using to address security threats in their organization. Attendees will receive a Passport to Prizes entry form. Visit each sponsor to receive a stamp, and then enter to win exciting prizes.

Vendor-Sponsored Lunch Session

Wednesday, April 9 | 12:00pm - 1:30pm | Location: N. H. Salon B

Sign-up at SANS Registration to receive a ticket for a free lunch brought to you by sponsoring vendors. Please note, by accepting a lunch ticket your badge will be scanned and your information shared with the sponsoring vendors. Join these sponsoring vendors and others on the expo floor for an introduction to leading solutions and services that showcase the leading options in information security. Take time to browse the show floor and get introduced to providers and their solutions that align with the security challenges being discussed in class.

Luncheon sponsors are:

Alephcloud
Aramco Services Company
Beyond Trust
EiQNetworks
Emulex
FireEye
Forescout
General Dynamics Fidelis Cybersecurity
PhishMe
Qualys

VENDOR EVENTS

Vendor-Sponsored Lunch & Learns

Since SANS course material is product neutral, these presentations provide the opportunity to evaluate vendor tools in an interactive environment to increase your effectiveness, productivity, and knowledge gained from the conference. These sessions feature a light meal or refreshments provided by the sponsor. Sign-Up Sheets for the events below are located on the Community Bulletin Board at Student Registration.

LUNCH AND LEARN

Enabling Secure Cloud Storage: Moving from Perimeter to Object-Based Protection

Speaker: Gregory Breeze, Principal SE
Tuesday, April 8 | 12:30pm-1:15pm | Location: N. H. A4

The adoption of cloud storage has been hampered by the security shortcomings/tradeoffs of traditional, perimeter-based security models. In order to gain the cost and agility benefits of the cloud, enterprises and service providers need to leverage an object-based security model to facilitate secure data sharing across trust boundaries. What's needed is a trustworthy platform for comprehensive protection of information assets – regardless of where the content is stored. Such a platform should provide federated key management and mediation using a Zero Knowledge methodology, enabling controlled access and content life cycle management, while eliminating the need for any central security authority or "trusted" third party.

LUNCH AND LEARN

The Power of Lossless Packet Capture (1G-100G) and Real-Time Netflow

Speaker: Andrew Weisman, Senior Sales Engineer
Tuesday, April 8 | 12:30pm-1:15pm | Location: N. H. Salon C

With network speeds of 10G, 40G, and even 100G now deployed in many production environments, organizations are finding it harder than ever to maintain the level of network visibility they were used to seeing at 1G. Furthermore, many commercial and open source network & security tools do not scale well at these higher data rates. Finding the root cause problem to security and network issues is now taking longer and incident response times are increasing, not decreasing. This Endace presentation will cover the benefits of a security architecture that incorporates a high-speed loss-less packet capture fabric and the generation of real-time Netflow data to improve network visibility, decrease incident response time, and better aid in the identification of root cause issues many organizations are facing today.

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

LUNCH AND LEARN

The Power of Metadata

Speaker: Mike Nichols, Senior Technical Product Manager
Tuesday, April 8 | 12:30pm-1:15pm | Location: N. H. A3

The term 'metadata' has been top of the news cycle lately, but what exactly is it and what can one accomplish through the it's analysis. In the Fidelis XPS Collector, metadata is netflow on steroids, providing rich attribute extraction of network and content level information. Using this data we can detect advanced threats through the behavior of their techniques, instead of relying upon signatures of their tactics we can and empower the network defender by automating the hunt for malicious activity. Learn how you can utilize full network visibility to speed the time of detection and remediation with Fidelis XPS.

FireEye™

LUNCH AND LEARN

World War C Threat Landscape – A Look At The Threats of Yesterday, The Trends Today, and What's to Come Tomorrow

Speaker: Mark Stanford, Senior Sales Engineering Manager
Tuesday, April 8 | 12:30pm-1:15pm | Location: N. H. A2

The threat landscape is ever-changing…polymorphic in its nature, just as the the attacks themselves are. Year over year, the statistics grow in favor of the attacker, showing the capabilities, resources and determination that continues to grow on the attacker's behalf. In this session, Mark Stanford will cover some high profile attacks across several verticals, the strengths and weaknesses of them, and how attacks are being constructed today and into the future. Tools will be discussed that can help combat these advanced threats (and opportunistic ones) across all vectors, and how to operationalize procedures to help secure your enterprise, your brand and give you piece of mind.

ForeScout
Access ability.

LUNCH AND LEARN

Continuous Monitoring & Mitigation

Speaker: Doug Laughlin, Account Manager – GA/FL/Caribbean
Tuesday, April 8 | 12:30pm-1:15pm | Location: N. H. A1

You've already invested in multiple kinds of security systems, but are they working together effectively? Do they share intelligence? Do they coordinate their responses? Are all your remediations automated? This session examines a reference architecture for continuous monitoring and mitigation, based on next-generation network access control and open standards-based information sharing architecture.

FORTINET® Infogressive, Inc. *Aggressive Information Security*

LUNCH AND LEARN

Fortinet Next Generation Firewalls

Speaker: Justin Kallhoff, CEO
Tuesday, April 8 | 12:30pm-1:15pm | Location: N. H. E4

Infogressive, a Fortinet platinum partner, will discuss next generation firewall technology. Learn how Fortinet products can improve your organization's security and simplify your network for a fraction of the cost of other manufacturers.

QUALYS® Continuous Security

LUNCH AND LEARN

Why use Continuous Monitoring?

Speaker: Jonas Kelly, Technical Account Manager
Thursday, April 10 | 12:30pm-1:15pm | Location: N. H. E4

Traditionally we ran scans, disseminated reports and waited in some cases 30 days or more for remediation activities to occur. CM compresses this time frame drastically and immediately alerts on the most important events so that problems are fixed, faster. The Attack Use Case: using CM can detect dangerous attacks as they happen by identifying, malicious hosts or new software on the perimeter. The Change Control Use Case: Identify unauthorized changes to ports and services on your perimeter, by alerting on those that are unauthorized. Verify the Change Control process works. The Compliance Use Case: Substantiate controls for audits with CM, it shows that the controls you have in place are working and are effective.

EiQ
Simplified Security Intelligence

LUNCH AND LEARN

Continuous Security Intelligence with the SANS Critical Security Controls

Speaker: Brian Mehlman, Senior Director of Product Management
Thursday, April 10 | 12:30pm-1:15pm | Location: N. H. D

Organizations of all sizes, and across almost every industry, face significant challenges protecting critical IT assets from an exponentially increasing threat landscape. And, of course, serious vulnerabilities continue to be discovered in both legacy and emerging IT systems. Implementing effective security controls has been shown to significantly reduce the risk of information breach. In this session, Brian Mehlman, Senior Director of Product Management, at EiQ Networks, will discuss an approach for delivering continuous security intelligence through the intersection of the right people, process, and technology. He will also provide a case study on how EiQ's flagship solution, SecureVue®, can increase information security, improve operational efficiency, and lower cost for an organization through automation of many of the top Critical Security Controls recommended by SANS.

VENDOR EVENTS

tenable network security

LUNCH AND LEARN

Tenable, the SANS 20 Critical Security Controls, And You; The Basics and Beyond

Speaker: Jack Daniel, Technical Product Manager

Thursday, April 10 | 12:30pm-1:15pm | Location: N. H. A4

Version 5 of the SANS' 20 Critical Security Controls has just been released, and the controls are being adopted across enterprises and government agencies. This presentation explores the evolving controls as well as some of the challenges and roadblocks to their implementation. Learn how Tenable Network Security can help you reach your security goals through discovery, assessment, and audit of your environment.

beyondtrust®

Beyond Traditional Security

LUNCH AND LEARN

Retina Vulnerability Management: The Best-Kept Secret in Security

Speaker: Morey J. Haber - Sr. Director, Program Management

Thursday, April 10 | 12:30pm-1:15pm | Location: N. H. C

Some vendors expend a lot of energy on, well, being loud. At BeyondTrust, we focus on R&D, making Retina one of the fastest, most complete vulnerability management solutions available (and you have to see the reports). Come have lunch on us, and see a secret weapon thats been deployed hundreds of thousands of times since 1998.

PHISHME

LUNCH AND LEARN

Phishing Your Employees – Lessons Learned From Phishing 5 Million People

Speaker: Jim Hansen, Executive VP

Thursday, April 10 | 12:30pm-1:15pm | Location: America's Seminar

Cyber crime and electronic espionage, most commonly, initiate with an employee clicking a link to a website hosting malware, opening a file attached to an email and laden with malware, or just simply giving up corporate credentials when solicited via phishing websites. Phishing has been used to hijack online brokerage accounts to aid pump n' dump stock scams, compromise government networks, sabotage defense contracts, steal proprietary information on oil contracts worth billions, and break into the world's largest technology companies to compromise their intellectual property. Technical controls presented as silver bullets provide false hope and a false sense of security to employees, promoting dangerous behaviors. Learn how to build a scalable and effective program to educate your staff and change behavior from experts at PhishMe.

DINING OPTIONS

WALT DISNEY WORLD SWAN AND DOLPHIN RESORT

YOUR TABLE IS READY

SIGNATURE DINING

TODD ENGLISH'S bluezoo *

Enjoy coastal cuisine from Celebrity Chef Todd English, incorporating an innovative selection of fresh seafood in an energetic and vibrant atmosphere. AAA Four Diamond Award recipient and multi-award winner of *Wine Spectator's* Award of Excellence. Open for dinner.

Dolphin - Lower Level

SHULA'S STEAK HOUSE *

Shula's serves the best beef money can buy, The SHULA CUT®, in addition to the freshest seafood, and 3-5 lb. live Maine lobsters. Critics choice for Orlando's Best High-End Steak House and multi-award winner of *Wine Spectator's* Award of Excellence. Open for dinner.

Dolphin - Lobby Level

IL MULINO NEW YORK TRATTORIA *

Traditional Italian cuisine from the Abruzzi region of Italy, served in a dynamic rustic trattoria. Features a diverse offering of exciting and bountifully presented dishes, prepared from original Italian recipes. Open for dinner.

Swan - Lobby Level

KIMONOS

Experience the art of sushi, nightly karaoke, and an intimate atmosphere in our authentic Japanese sushi restaurant. Open for dinner.

Swan - Lobby Level

CASUAL DINING

FRESH MEDITERRANEAN MARKET

Savor fresh, made-to-order menu items from our Mediterranean-style market. Open for breakfast and lunch.

Dolphin - Lower Level

THE FOUNTAIN

Crisp salads, custom grilled burgers, and a delectable array of sandwiches and desserts. Take away homemade or soft serve ice cream. Open for lunch and dinner.

Dolphin - Lower Level

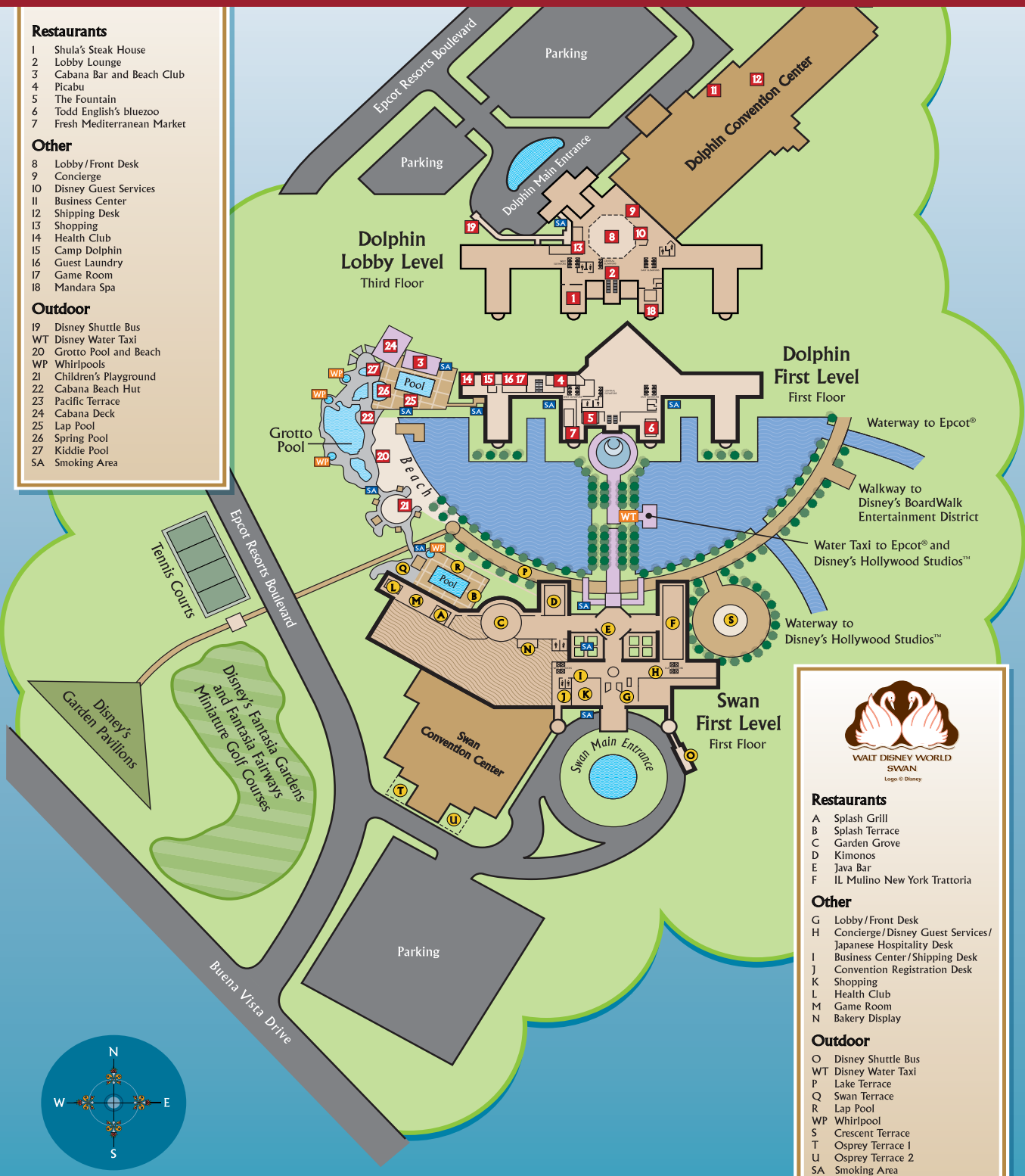
CABANA BAR AND BEACH CLUB

Sleek and contemporary, with a hint of South Beach Style, this is the perfect place for lunch or dinner. Then transition into evening with specialty cocktails at the illuminated bar. Open seasonally.

Dolphin - Poolside

**Reservations accepted*

HOTEL FLOORPLAN



Restaurants

1 Shula's Steak House
2 Lobby Lounge
3 Cabana Bar and Beach Club
4 Picabu
5 The Fountain
6 Todd English's bluezoo
7 Fresh Mediterranean Market

Other

8 Lobby/Front Desk
9 Concierge
10 Disney Guest Services
11 Business Center
12 Shipping Desk
13 Shopping
14 Health Club
15 Camp Dolphin
16 Guest Laundry
17 Game Room
18 Mandara Spa

Outdoor

19 Disney Shuttle Bus
WT Disney Water Taxi
20 Grotto Pool and Beach
WP Whirlpools
21 Children's Playground
22 Cabana Beach Hut
23 Pacific Terrace
24 Cabana Deck
25 Lap Pool
26 Spring Pool
27 Kiddie Pool
SA Smoking Area

WALT DISNEY WORLD SWAN
Logo © Disney

Restaurants

A Splash Grill
B Splash Terrace
C Garden Grove
D Kimonos
E Java Bar
F IL Mulino New York Trattoria

Other

G Lobby/Front Desk
H Concierge/Disney Guest Services/ Japanese Hospitality Desk
I Business Center/Shipping Desk
J Convention Registration Desk
K Shopping
L Health Club
M Game Room
N Bakery Display

Outdoor

O Disney Shuttle Bus
WT Disney Water Taxi
P Lake Terrace
Q Swan Terrace
R Lap Pool
WP Whirlpool
S Crescent Terrace
T Osprey Terrace 1
U Osprey Terrace 2
SA Smoking Area

Future SANS Training Events

US Cyber Crime Conference
Leesburg, VA | April 27-28

SANS **Austin** 2014
Austin, TX | April 28 - May 3

SANS **Security Leadership Summit** 2014
Boston, MA | April 29 - May 7

SANS **Security West** 2014
San Diego, CA | May 8-17

Digital Forensics & Incident Response Summit
Austin, TX | June 3-10

SANS **Rocky Mountain** 2014
Denver, CO | June 9-14

SANSFIRE 2014
Baltimore, MD | June 21-30

SANS **Capital City** 2014
Washington, DC | July 7-12

SANS **San Francisco** 2014
San Francisco, CA | July 14-19

ICS Security Training – Houston
Houston, TX | July 21-25

SANS **Boston** 2014
Boston, MA | July 28 - August 2

SANS **San Antonio** 2014
San Antonio, TX | August 11-16

SANS **Virginia Beach** 2014
Virginia Beach, VA | August 18-29

SANS **Chicago** 2014
Chicago, IL | August 24-29

SANS **Crystal City** 2014
Crystal City, VA | September 8-13

SANS **Albuquerque** 2014
Albuquerque, NM | September 15-20

SANS **Baltimore** 2014
Baltimore, MD | September 22-27