SANS 2015

PROGRAM GUIDE

April 11-18, 2015

Walt Disney World Swan and Dolphin

Orlando, FL

@SANSInstitute | #SANS2015

TABLE OF CONTENTS

NETWARS TOURNAMENTS

All students who register for a 4-6 day course will be eligible to play NetWars for FREE.

Register Now!
sans.org/event/sans-2015/schedule

DFIR NETWARS TOURNAMENT

Hosted by Rob Lee and Phil Hagen
Thursday, April 16 and Friday, April 17
6:30pm - 9:30pm | Pelican 1 (SWAN)

CORE NETWARS TOURNAMENT

Hosted by Jeff McJunkin
Thursday, April 16 and Friday, April 17
6:30pm - 9:30pm | Swan 5 (SWAN)

GENERAL INFORMATION

Registration & Courseware Pick-up Information

Location: Swan Foyer (SWAN)

Saturday, April 11 (Short Courses Only) . . . . . 8:00am - 9:00am
Sunday, April 12 (Short Courses Only) . . . . . 8:00am - 9:00am
Sunday, April 12 (Welcome Reception) . . . . . 5:00pm - 7:00pm
Monday, April 13 . . . . . 7:00am - 5:30pm
Tuesday, April 14 - Friday, April 17 . . . . . 8:00am - 5:00pm
Saturday, April 18 . . . . . 8:00am - noon

Internet Café *(WIRED & WIRELESS)*

Location: Swan Foyer (SWAN)
Printer will be available for students' use

Monday, April 13 . . . . . Opens at noon - 24 hours
Tuesday, April 14 - Friday, April 17 . . . . . Open 24 hours
Saturday, April 18 . . . . . Closes at 2:00pm

Course Times

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

Course Breaks

7:00am - 9:00am – Morning Coffee
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 13** at the ***General Session*** in **Swan 5** (SWAN).

GENERAL INFORMATION

Dining Options

We have assembled a short list of dining suggestions you may like to try during lunch breaks. See page 21 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

To make sure you are in the right place, the SANS door monitors will be checking your badge for each course you enter. For your convenience, please wear your badge 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 Swan Foyer (SWAN).

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)

SEC401: Security Essentials Bootcamp Style
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
SEC760: Advanced Exploit Development for Penetration Testers
MGT414: SANS Training Program for CISSP Certification®

Extended Hours:

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
FOR408: Windows Forensic Analysis
FOR585: Advanced Smartphone Forensics
SEC560: Network Penetration Testing and Ethical Hacking
MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™

COURSE SCHEDULE

START DATE: **Saturday, April 11**

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

SEC440: Critical Security Controls: Planning, Implementing, and Auditing
Instructor: Randy Marchany . . . . . Location: Europe 6 (DOLPHIN)

SEC524: Cloud Security Fundamentals
Instructor: Dave Shackleford . . . . . Location: Oceanic 5 (DOLPHIN)

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Instructor: Eric Conrad . . . . . Location: Oceanic 4 (DOLPHIN)

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

HOSTED: Health Care Security Essentials
Instructor: Greg Porter . . . . . Location: Oceanic 6 (DOLPHIN)

HOSTED: Physical Penetration Testing
Instructor: The CORE Group. . . . . Location: Europe 7 (DOLPHIN)

START DATE: **Sunday, April 12**

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

MGT305: Technical Communication and Presentation Skills for Security Professionals
Instructor: Seth Misenar . . . . . Location: Toucan 1/2 (SWAN)

MGT415: A Practical Introduction to Risk Assessment
Instructor: G. Mark Hardy . . . . . Location: Pelican 1 (SWAN)

MGT535: Incident Response Team Management
Instructor: Christopher Crowley. . . . . Location: Pelican 2 (SWAN)

START DATE: **Monday, April 7**

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

SEC301: Intro to Information Security
Instructor: Keith Palmgren. . . . . Location: Swan 10 (SWAN)

SEC401: Security Essentials Bootcamp Style
Instructor: Dr. Eric Cole . . . . . Location: Asia 1 (DOLPHIN)
Bootcamp Hours: 5:00pm - 7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials – Enterprise Defender
Instructor: Paul A. Henry . . . . . Location: Swan 9 (SWAN)

SEC503: Intrusion Detection In-Depth
Instructor: Mike Poor. . . . . Location: Swan 1 (SWAN)

SEC504: Hacker Tools, Techniques, Exploits & Incident Handling
Instructor: John Strand. . . . . Location: Swan 5 (SWAN)
Extended Hours: 5:00pm - 7:15pm (Course Day 1 only)

COURSE SCHEDULE

SEC505: Securing Windows with the Critical Security Controls
Instructor: Jason Fossen. . . . . Location: Oceanic 7 (DOLPHIN)

SEC511: Continuous Monitoring and Security Operations
Instructor: Eric Conrad . . . . . Location: Osprey Ballroom 1 (SWAN)

SEC542: Web App Penetration Testing and Ethical Hacking
Instructor: Seth Misenar . . . . . Location: Swan 7 (SWAN)

SEC560: Network Penetration Testing and Ethical Hacking
Instructor: Ed Skoudis . . . . . Location: Pelican 1 (SWAN)
Extended Hours: 5:00pm - 7:15pm (Course Day 1 only)

SEC561: Intense Hands-on Pen Testing Skill Development (with SANS NetWars)
Instructor: Tim Medin . . . . . Location: Europe 5 (DOLPHIN)

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
Instructor: James Tarala . . . . . Location: Asia 2 (DOLPHIN)

SEC573: Python for Penetration Testers
Instructor: Mark Baggett . . . . . Location: Europe 7 (DOLPHIN)

SEC575: Mobile Device Security and Ethical Hacking
Instructor: Joshua Wright. . . . . Location: Parrot (SWAN)

SEC579: Virtualization and Private Cloud Security
Instructor: Dave Shackleford . . . . . Location: Pelican 2 (SWAN)

SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses
Instructor: Larry Pesce . . . . . Location: Europe 8 (DOLPHIN)

SEC642: Advanced Web App Penetration Testing and Ethical Hacking
Instructor: Justin Searle . . . . . Location: Mockingbird 2 (SWAN)

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Instructor: James Lyne . . . . . Location: Oceanic 6 (DOLPHIN)
Bootcamp Hours: 5:15pm-7:00pm (Course days 1-5)

SEC760: Advanced Exploit Development for Penetration Testers
Instructor: Stephen Sims . . . . . Location: Egret (SWAN)
Bootcamp Hours: 5:15pm - 7:00pm (Course days 1-5)

DEV522: Defending Web Applications Security Essentials
Instructor: Dr. Johannes Ullrich . . . . . Location: Macaw (SWAN)

DEV544: Secure Coding in .NET: Developing Defensible Apps
Instructor: Eric Johnson . . . . . Location: Oceanic 8 (DOLPHIN)

FOR408: Windows Forensic Analysis
Instructor: Rob Lee . . . . . Location: Swan 2 (SWAN)
Set up time: 8:00am - 9:00am (Course Day 1 only)

COURSE SCHEDULE

FOR508: Advanced Digital Forensics and Incident Response
Instructor: Chad Tilbury . . . . . Location: Mockingbird 1 (SWAN)

FOR572: Advanced Network Forensics and Analysis
Instructors: Philip Hagen . . . . . Location: Oceanic 5 (DOLPHIN)

FOR585: Advanced Smartphone Forensics
Instructors: Heather Mahalik. . . . . Location: Dove (SWAN)
Set up time: 8:00am - 9:00am (Course Day 1 only)

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Instructor: Lenny Zeltser . . . . . Location: Toucan 1/2 (SWAN)

MGT414: SANS Training Program for CISSP Certification®
Instructor: Jonathan Ham . . . . . Location: Swan 8 (SWAN)
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: David Hoelzer . . . . . Location: Swan 4 (SWAN)
Extended Hours: 5:00pm - 6:00pm (Course days 1-4)

MGT514: IT Security Strategic Planning, Policy and Leadership
Instructor: G. Mark Hardy . . Location: Osprey Ballroom 2 (SWAN)

MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep
Instructor: Jeff Frisk . . . . . Location: Swan 3 (SWAN)

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems
Instructor: Tanya Baccam . . . . . Location: Oceanic 4 (DOLPHIN)

LEG523: Law of Data Security and Investigations
Instructor: Benjamin Wright . . . . . Location: Europe 6 (DOLPHIN)

HOSTED: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program
Instructor: Frank Shirmo . . . . . Location: Heron (SWAN)

START DATE: **Thursday, April 16**

DFIR NetWars Tournament
Hosts: Rob Lee and Phil Hagen . . . . . Location: Pelican 1 (SWAN)
Hours: 6:30pm - 9:30pm

CORE NetWars Tournament
Host: Jeff McJunkin . . . . . Location: Swan 5 (SWAN)
Hours: 6:30pm - 9:30pm

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 network and computer security.

SUNDAY, APRIL 12

Registration Welcome Reception

Sun, April 12 | 5:00pm - 7:00pm | Location: Swan Foyer (SWAN)

Register early and network with your fellow students!

MONDAY, APRIL 13

General Session – Welcome to SANS

Speaker: Dr. Eric Cole

Mon, April 13 | 8:15am - 8:45am | Location: Swan 5 (SWAN)

SANS Technology Institute Open House

Speaker: Bill Lockhart

Mon, April 13 | 5:30pm - 7:00pm | Location: Swan 6 (SWAN)

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.

Visit our Open House and learn more!

KEYNOTE

Understanding the Offense to Build a Better Defense

Speaker: Dr. Eric Cole

Mon, April 13 | 7:15pm - 9:15pm | Location: Swan 5 (SWAN)

Many organizations do not perform proper threat modeling and understand what the adversary is capable of. The only way to be good at the defense is to understand the offense. Understanding how the threat targets and attacks a system can provide insight into implementing a proper security program. In this talk, the attacker killer chain will be examined as will specific steps organizations can take to properly defend themselves.

SPECIAL EVENTS

TUESDAY, APRIL 14

LUNCH & LEARN

How to Become a SANS Instructor

Speaker: Eric Conrad

Tue, April 14 | 12:30pm - 1:15pm | Location: Swan 4 (SWAN)

Have you ever wondered what it takes to become a SANS instructor? SANS Principal instructor Eric Conrad will share his experiences and show you how to become part of the SANS top-rated instructor team.

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

Women in Technology Meet and Greet

Speaker: Deanna Boyden

Tue, April 14 | 5:30pm - 6:30pm | Location: Crescent Terrace (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 attendees.

Online Pool Party

Speaker: Steve Peterson

Tue, April 14 | 6:15pm - 7:15pm | Location: Pool Terrace (SWAN)

Join the Online Training team for an hour of poolside fun, fresh air, and networking!

Cyber Leadership Reception

Speaker: Frank Kim

Tue, April 14 | 7:15pm - 8:15pm | Location: Osprey Terrace 2 (SWAN)

Cyber leaders, managers, and aspiring leaders are cordially invited to attend the Cyber Leadership reception compliments of the SANS Management curriculum. Join us for cocktails and hors d'oeuvres while you network with industry leaders. Hear from industry experts on how you can make the most of your career with cyber security leadership training.

SANS@NIGHT

Self-Education: Using the Pull Method for Security Awareness Training

Speaker: Lance Spitzner

Tue, April 14 | 7:15pm - 8:15pm | Location: Osprey Ballroom 1 (SWAN)

Traditionally security awareness training has used a push method, from pushing out CBT training to mandatory workshops. Organizations are now trying a different approach, the pull method. This is when employees are encouraged to actively seek out training on their own. Learn how organizations are effectively building and promoting pull training and the successes they are seeing.

SANS@NIGHT

Using an Open Source Threat Model for Prioritized Defense

Speaker: James Tarala

Tue, April 14 | 7:15pm - 8:15pm | Location: Osprey Ballroom 2 (SWAN)

Threat actors are not magic and there is not an unlimited, unique list of threats for every organization. Enterprises face similar threats from similar threat sources and threat actors – so why does every organization need to perform completely unique risk assessments and prioritized control decisions? This presentation will show how specific, community-driven threat models can be used to prioritize an organization's defenses – without all the confusion. In this presentation James Tarala will present a new, open, community-driven threat model that can be used by any industry to evaluate the risk that faces them. Then he will show how to practically use this model to prioritize enterprise defense and map to existing compliance requirements facing organizations today. Whether you are in the Department of Defense or work for a small mom-and-pop retailer, you will be able to use this model to specifically determine a prioritized defense for your organization.

SANS@NIGHT

The 13 Absolute Truths of Security

Speaker: Keith Palmgren

Tue, April 14 | 7:15pm - 8:15pm | Location: Swan 5 (SWAN)

Keith Palmgren has identified 13 "Absolute Truths" of security – things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these 13 absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the 13 absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

SANS@NIGHT

Preparing for PowerShellmageddon – Investigating Windows Command Line Activity

Speaker: Chad Tilbury

Tue, April 14 | 8:15pm - 9:15pm | Location: Swan 5 (SWAN)

There is a reason hackers use the command line, and it isn't to impress you with their prowess. Throughout the history of Windows, the command line has left far fewer forensic artifacts than equivalent operations via the GUI. To make matters worse, the transition to Windows 7 and 8 has spread PowerShell throughout the enterprise. While it makes our lives easier as defenders, it does the same for our adversaries. Every time you marvel at the capabilities of PowerShell, you should fear how your adversaries may use that power against you.

This talk will demonstrate how incident responders are countering the command line threat with real-world examples. Learn to identify when it is in play, extract command history, and see what is new on the horizon from Microsoft to make tracking command line and PowerShell activity easier.

SPECIAL EVENTS

SANS@NIGHT

iOS Game Hacking: How I Ruled the Worl^Hd and Built Skills For AWESOME Mobile App Pen Tests

Speaker: Josh Wright

Tue, April 14 | 8:15pm - 9:15pm | Location: Osprey Ballroom 2 (SWAN)

I am a terrible video game player. I lack the skills to competitively arrange words with colleagues, crush jelly beans, or achieve a high score arranging numbers by threes. However, what I lack in video game competition, I make up for in iOS app hacking. In this talk, we'll explore the profitable market of iOS games, looking at several techniques that are used to cheat, hack, or even steal from iOS game developers. You'll be able to apply these techniques to give yourself a leg up on your next gaming experience. Most importantly, each and every technique we'll discuss is also directly applicable to penetration testing and assessing the security of the iOS apps your organization uses each and every day. Learn to pwn games while becoming a better app pen tester! What's not to like?

SANS@NIGHT

Securing The Kids

Speaker: Lance Spitzner

Tue, April 14 | 8:15pm - 9:15pm | Location: Osprey Ballroom 1 (SWAN)

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.

SPECIAL EVENTS

WEDNESDAY, APRIL 15

SANS@NIGHT

Malware Analysis for Incident Responders: Getting Started

Speaker: Lenny Zeltser

Wed, April 15 | 7:15pm - 9:15pm | Location: Swan 5 (SWAN)

Knowing how to analyze malware has become a critical skill for incident responders and forensic investigators. A good way to get started with such efforts involves examining how malicious software behaves in a controlled laboratory environment. In this two-hour seminar briefing, Lenny Zeltser demonstrates key aspects of this process, walking you through behavioral analysis of a malware specimen by using several free tools and even peeking into the world of code analysis. You will see practical techniques in action and understand how malware analysis will help you to triage the incident to assess key capabilities of the malicious software. This seminar will help you start learning how to turn malware inside out.

SANS@NIGHT

Gone In 60 Minutes

60 Minutes From Discovery Through Exploitation – How Fast is Your Patching Process?

Speaker: David Hoelzer

Wed, April 15 | 7:15pm - 8:15pm | Location: Osprey Ballroom 2 (SWAN)

In this fast-paced talk, David Hoelzer will walk you through the process a hacker might go through to discover a flaw, engineer a working proof of concept, and then convert that into a working Metasploit exploit module... All in 60 minutes. If you're not a technical person, don't worry. There's still plenty to take away from this talk. If you are a technical person come along and see if there's a trick or two that you can use!

SANS@NIGHT

Windows Exploratory Surgery with Process Hacker

Speaker: Jason Fossen

Wed, April 15 | 7:15pm - 8:45pm | Location: Osprey Ballroom 1 (SWAN)

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**

SPECIAL EVENTS

SANS@NIGHT

It's Time To Make a Case

Speaker: Moses Hernandez

Wed, April 15 | 7:15pm - 8:15pm | Location: Pelican 1 (SWAN)

We live in some interesting times, not because we have a negative or positive viewpoint of the times, but because we are truly at the beginning of an interesting journey. When we look far into the future, we should ask "What can we be doing today to really push forward the conversation?" I provide a few stories to show you that there is a path forward. I also provide our STI students with a potentially new project that they can really use to make a difference, not just for us, but for the whole of society.

GIAC Program Overview

Speaker: Jeff Frisk

Wed, April 15 | 8:15pm - 9:15pm | Location: Swan 4 (SWAN)

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@NIGHT

Enterprise PowerShell for Remote Security Assessment

Speaker: James Tarala

Wed, April 15 | 8:15pm - 9:15pm | Location: Osprey Ballroom 2 (SWAN)

As organizations assess the security of their information systems, the need for automation has become more and more apparent. Forensic analysts, incident handlers, penetration testers, and auditors all regularly find themselves in situations where they need to remotely assess a large number of systems through an automated set of tools. Microsoft's PowerShell scripting language has become the defacto standard for many organizations looking to perform this level of distributed automation. This presentation will describe to students the enterprise capabilities PowerShell offers and show practical examples of how PowerShell can be used to perform large scale Windows security assessments.

SANS@NIGHT

Hacking Back, Active Defense, and Internet Tough Guys

Speaker: John Strand

Wed, April 15 | 8:15pm - 9:15pm | Location: Mockingbird 1 (SWAN)

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.

SPECIAL EVENTS

THURSDAY, APRIL 16

Hosts: Rob Lee and Phil Hagen
Thu, April 16 & Friday, April 17 | 6:30pm - 9:30pm
Location: Pelican 1 (SWAN)

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.

Host: Jeff McJunkin
Thu, April 16 & Friday, April 17 | 6:30pm - 9:30pm
Location: Swan 5 (SWAN)

SANS 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 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

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

Speaker: Benjamin Wright
Thu, April 16 | 7:15pm - 8:15pm | Location: Osprey Ballroom 1 (SWAN)

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.

SPECIAL EVENTS

SANS@NIGHT

Debunking the Complex Password Myth

Speaker: Keith Palmgren
Thu, April 16 | 7:15pm - 8:15pm | Location: Osprey Ballroom 2 (SWAN)

Perhaps the worst advice you can give a user is "choose a complex password." The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves and even for their children.

SANS@NIGHT

Let's Face It, You Are Probably Compromised. What Next?

Speaker: Joff Thyer
Thu, April 16 | 8:15pm - 9:15pm | Location: Osprey Ballroom 2 (SWAN)

In this talk, we will discuss changing philosophy away from the, near impossible, 100% successful defense to one of accepting that compromise has likely occurred. While layers of defense are absolutely necessary, as an industry, we know that this approach is not always successful. If we collectively accept that compromise has likely occurred, some resources can be refocused on finding macro-level indicators of compromise in order to successfully hunt down and eliminate bad actors within our computing environments. The discussion will touch on techniques that can be used to identify and correlate information from firewall, proxy, and DNS server log analysis.

SANS@NIGHT

Defense Needed, Superbees Wanted (WebApp Pentesting with bWAPP)

Speaker: Malik Mesellem
Thu, April 16 | 8:15pm - 9:15pm | Location: Osprey Ballroom 1 (SWAN)

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application developed by Malik Mesellem. It helps security enthusiasts, developers, and students to discover and to prevent web vulnerabilities. bWAPP prepares one to conduct successful penetration testing and ethical hacking projects. "A security testing framework made for educational purposes." What makes bWAPP so unique? Well, it has over 100 different web vulnerabilities and issues! It covers all major known web bugs, including all risks from the OWASP Top 10 project. Defense is needed... superbees are wanted!

VENDOR EVENTS

Vendor Solutions Expo

Wed, April 15 | 12:00pm - 1:30pm | 5:30pm - 7:30pm
Location: Swan 6 (SWAN)

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

Wed, April 15 | 5:30pm - 7:30pm | Location: Swan 6 (SWAN)

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

Wed, April 15 | 12:00pm - 1:30pm | Location: Swan 6 (SWAN)

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:

Invincea	PhishMe	ThreatSTOP
ThreatStream	Qualys	Splunk
Rapid7	Bit9 & Carbon Black	Centrify
CloudPassage	F5 Networks	Alert Logic
Pwnie Express	EiQ Networks	Sophos/Infogressive
Palo Alto Networks	General Dynamics Fidelis Cybersecurity	Lookingglass

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.

THREATSTREAM®

LUNCH AND LEARN

Fight Cyber Adversaries with Controlled Collaboration

Speaker: Trevor Welsh, Cyber Engineering Architect
Tue, April 14 | 12:30pm-1:15pm | Location: Swan 5 (SWAN)

In the war for information, the adversary has one key advantage... collaboration. There's no barrier preventing cyber criminals from joining forces to attack organizations. With bot army's and sophisticated malware RATs, the enemies' resources are limitless. It's time to take control and turn the tables by enabling our own community. Real-time threat indicator sharing is now a possibility. Join other like-minded security professionals to create a collective defense grid by sharing threat intelligence. Learn how to mitigate cyber attacks by enabling controlled collaboration.

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

LUNCH AND LEARN

Advanced Threats Need Comprehensive Defense

Speaker: Anubhav Arora
Tue, April 14 | 12:30pm-1:15pm | Location: Swan 1 (SWAN)

Today's threat actors are organized, well funded, and more sophisticated than ever; with the goal of stealing or destroying sensitive data for profit. Advanced threats are risks to a business with transactions conducted over the network by sophisticated actors exploiting known and publicly unknown system vulnerabilities. The network transactions are usually obfuscated and deeply embedded inside content. Dedicated security teams are charged with preparing organizations for the most advanced of attacks. Unfortunately, if your security team can't see advanced threats over your network, they definitely can't detect or prevent data theft. Learn about

- Why do enterprises need comprehensive defense against advanced threats? The current threat landscape and approaches to advanced threat defense.
- How does a security product detect advanced threats?
- How you can empower the security analysts to detect and prevent threats across the network with actionable visibility over your network.

ThreatSTOP™

LUNCH AND LEARN

Protecting the Things, Including the Ones You Already Have (and don't know about)

Speaker: Tom Byrnes, CEO and Founder
Tue, April 14 | 12:30pm-1:15pm | Location: Swan 7 (SWAN)

The Internet Of Things is already here. Printers, Medical Devices, Cameras, Alarm systems; and more ALREADY connect to the network, and are Pwned. These systems typically are deployed and managed by people with little to no understanding of security, and are almost never patched. In this session we will show actual infections, and demonstrate protection that works for the Things on your network.

paloalto networks®

LUNCH AND LEARN

Expose the Underground: Prevent Advanced Persistent Threats

Speaker: Mike Milholland, Network Security Engineer, Palo Alto Networks
Tuesday, April 14 | 12:30pm-1:15pm | Location: Swan 9 (SWAN)

Advanced Persistent Threats (APTs) are being used to compromise organizations around the globe with increasing sophistication, persistence, and evasive attack methods. Join Palo Alto Networks® for a lunch and learn that will take you straight to the heart of the cyber underground. This event will cover:

- Today's threat landscape – analysis of breaking attacks: what they did, how they got in, and their lifecycle
- How current solutions for enterprise security fail, with key considerations on how to protect your organization
- How to combat APTs now and in the future with a fundamentally different approach.

EiQ

Simplified Security Intelligence

LUNCH AND LEARN

Continuous Security Intelligence with the SANS Critical Security Controls

Speaker: Justin Pennock, North America Sales Leader, EiQ Networks
Tue, April 14 | 12:30pm-1:15pm | Location: Swan 8 (SWAN)

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, Justin Pennock 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 solutions 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.

LOOKINGGLASS

LUNCH AND LEARN

The Power of Threat Intelligence in Your Cybersecurity Program

Speaker: Jason McEachin, Director, Sales Engineering, Lookingglass
Tue, April 14 | 12:30pm-1:15pm | Location: Mockingbird 1 (SWAN)

Cybersecurity attacks dominate the headlines everyday, with large and small organizations alike being breached and impacted. Organizations need a more effective threat intelligence management capability to quickly prioritize and enrich events to enable robust response to attacks. During this presentation, we will discuss how:

- Harnessing the power of threat intelligence collection, aggregation, ingestion, and automation for full threat intel integration into your cybersecurity defense lifecycle
- Adding global context to internal and external threat intel sources enables decision support both within and outside the enterprise perimeter
- Aggregating disparate threat information supports improved analysis and confidence

ALERT LOGIC®
Security. Compliance. Cloud.

LUNCH AND LEARN

ANATOMY OF AN ATTACK: It takes an Expert to Stop Attackers

Speaker: Stephen Coty, Chief Security Evangelist
Thu, April 16 | 12:30pm-1:15pm | Location: Swan 5 (SWAN)

Attacks have advanced far beyond the early threats of tech-savvy kids wreaking havoc on computer networks. Today's attackers are fast, well funded and organized. Our discussion will take you into the world of cybercrime and give you an insider's look into how attackers operate and what you can do to protect your information in the cloud.

QUALYS®
CONTINUOUS SECURITY

LUNCH AND LEARN

Tackling Application Security Challenges Through Progressive Scanning

Speaker: Frank Catucci, Director of Web Application Security, Qualys
Thu, April 16 | 12:30pm-1:15pm | Location: Swan 8 (SWAN)

Welcome to the 'Age of the App.' Whether it's consuming news and entertainment, communicating with friends, or taking care of business, there's an app for it. With all of these actions taking place via apps, security is becoming a big concern. The web has become the dominant vector for cyber attacks, as hackers are focusing their efforts to find new ways to penetrate our defenses via web applications, as underscored with the recent Shellshock vulnerability. As a result, manual testing falls short to discover and efficiently scan large number of web apps making automated, progressive scanning a necessity to address this problem at scale. This session will provide a brief overview of today's most pressing challenges in the web application security market, and highlight how progressive scanning can help solve some of these challenges by streamlining the web application testing process.

VENDOR EVENTS

CloudPassage

LUNCH AND LEARN

Rapid visibility and compliance with CloudPassage Halo

Speakers: Ryan Thomas, Director of Product & Chad Gasaway, Sr. Sales Engineer
Thu, April 16 | 12:30pm-1:15pm | Location: Swan 9 (SWAN)

Join CloudPassage to learn clear steps to securing cloud environments, and how to get there with CloudPassage Halo - the agile security solution that provides instant visibility and the fastest time to compliance available.

PHISHME

LUNCH AND LEARN

Reverse Engineering Emails for Threat Indicators

Speaker: Ronnie Takazowski, Senior Research Engineer, PhishMe
Thu, April 16 | 12:30pm-1:15pm | Location: Swan 7 (SWAN)

Although enterprises receive high volumes of phishing emails daily, many still lack the ability to effectively analyze them. Performing reverse engineering allows companies to quickly answer questions about phishing emails they receive. This session will detail new reverse engineering techniques that show how to parse and pivot on metadata within an email, use custom signatures to detect malicious logic, and provide general visibility into phishing emails. Performing these techniques will provide answers to questions, such as "Have the bad guys ever used this domain against us?" that will allow organizations to proactively respond to phishing attacks.

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

LUNCH AND LEARN

Bit9 Connect IR Partner Enablement

Speaker: James Darby, Director of IR/MSSP Operations
Thu, April 16 | 12:30pm-1:15pm | Location: Swan 4 (SWAN)

What are the benefits of becoming a Bit9 Connect Partner? We'll cover the benefits of being in the program and the process followed to get a partner fully enabled on the best Incident Response tool on the market. We'll highlight how the tool will benefit your existing process and reduce the kill chain from detection to resolution. We're building a better tool for the IR first responders with the goal of enabling teams to identify and eradicate malware in record time.

SOPHOS Infogressive, Inc. *Aggressive Information Security*

LUNCH AND LEARN

Prevent - Detect - Respond

Speaker: Justin Kallhoff, Founder, COO, Infogressive
Thu, April 16 | 12:30pm-1:15pm | Location: Swan 1 (SWAN)

We all want to prevent 100% of attacks, however most SANS attendees know that isn't realistic given today's threat landscape. We will discuss technologies and services that increase prevention rates, help with detection when your defenses fail, and how we respond when it really hits the fan. #BOOM

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

SANS Shuttle Service
Wyndham Hotel ⟶ Swan

April 13-18

PICK-UP TIMES (EVERY HALF HOUR):
6:30am - 11:30am

SANS Shuttle Service
Swan ⟶ Wyndham Hotel

SHUTTLE WILL DEPART FROM SWAN HOTEL – TOUCAN FOYER ENTRANCE

April 13-17

PICK-UP TIMES (EVERY HALF HOUR):
4:30pm - 10:00pm

April 18

PICK-UP TIMES (EVERY HALF HOUR):
1:30pm - 6:30pm

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

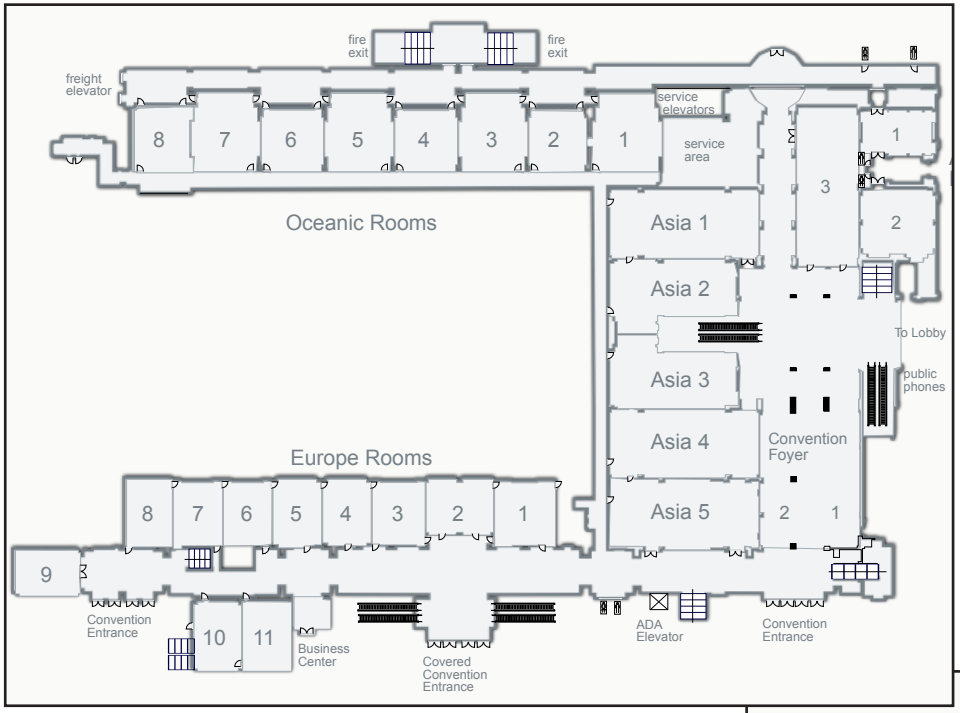
G Lobby/Front Desk
H Concierge/Disney Guest Services/ Japanese Hospitality Desk
I Business Center/Shipping Desk
J Convention Registration Desk
K Shopping
L Health Club
M Game Room
N Bakery Display

Outdoor

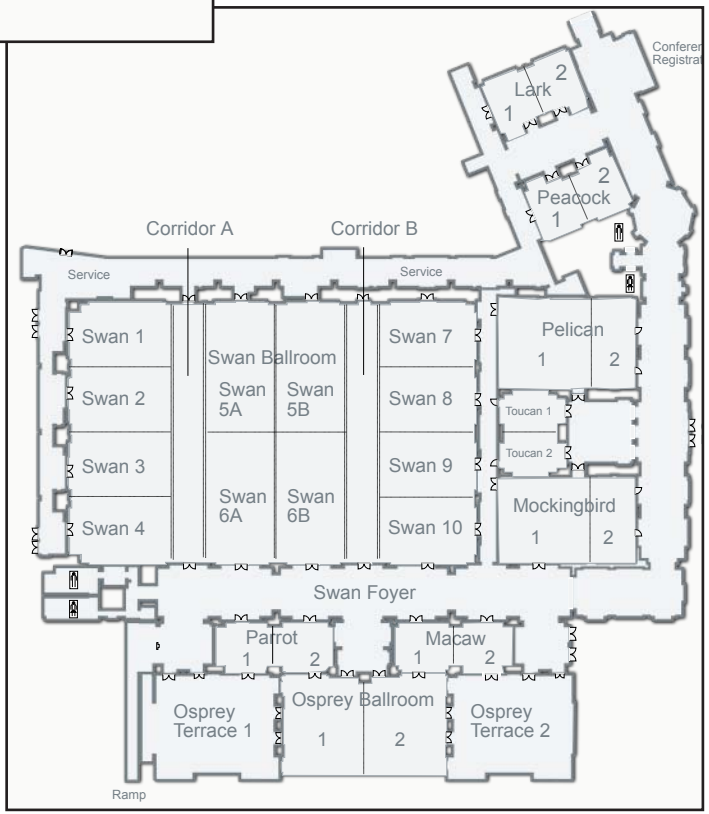
O Disney Shuttle Bus
WT Disney Water Taxi
P Lake Terrace
Q Swan Terrace
R Lap Pool
WP Whirlpool
S Crescent Terrace
T Osprey Terrace 1
U Osprey Terrace 2
SA Smoking Area

HOTEL FLOORPLAN

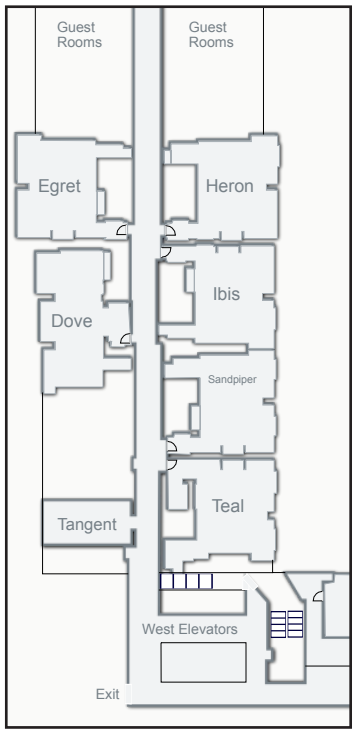
Dolphin – Lobby Level



Swan – Ground Level



Swan – 2nd Level



Future SANS Training Events

SANS **Security Operations Center** SUMMIT & TRAINING
Washington, DC | April 24 - May 1 | #SOCSummit

SANS **Security West** 2015
San Diego, CA | May 3-12 | #SecurityWest

SANS **Pen Test Austin** 2015
Austin, TX | May 18-23 | #PenTestAustin

SANS **ICS Houston Security Training** 2015
Houston, TX | June 1-5 | #SANSHouston

SANSFIRE 2015
Baltimore, MD | June 13-20 | #SANSFIRE

SANS **Rocky Mountain** 2015
Denver, CO | June 22-27 | #SANSRockyMtn

SANS **Capital City** 2015
Washington, DC | July 6-11 | #SANSCapitalCity

SANS **Digital Forensics & Incident Response** SUMMIT
Austin, TX | July 7-14 | #DFIRSummit

SANS **San Jose** 2015
San Jose, CA | July 20-25 | #SANSSJ

SANS **Minneapolis** 2015
Minneapolis, MN | July 20-25 | #SANSmpls

SANS **Boston** 2015
Boston, MA | August 3-8 | #SANSBoston

SANS **Cyber Defense** SUMMIT & TRAINING
Nashville, TN | August 11-18 | #CyberDefenseSummit

SANS **San Antonio** 2015
San Antonio, TX | August 17-22 | #SANSSATX

SANS **Virginia Beach** 2015
Virginia Beach, VA | August 24 - Sept 4 | #SANSVaBeach

SANS **Chicago** 2015
Chicago, IL | August 30 - September 4 | #SANSChicago

SANS **Crystal City** 2015
Crystal City, VA | September 8-13 | #SANSCrystalCity

SANS **Network Security** 2015
Las Vegas, NV | September 12-19 | #SANSNetworkSecurity

Information on all events can be found at
sans.org/security-training/by-location/all