SANS

Network Security 2015

Caesars Palace

Las Vegas, NV

September 12-21, 2015

PROGRAM GUIDE

@SANSInstitute #SANSNetworkSecurity

SANS OnDemand Bundle

Add an OnDemand Bundle to your course to get an additional four months of intense training!
OnDemand Bundles are just $629
when added to your live course, and include:

- Four months of OnDemand access to our custom e-learning platform
- Quizzes
- Labs
- MP3s and videos of lectures
- Subject-matter expert support

OnDemand Bundle is available for these courses.

SEC301 – $629	SEC575 – $629	FOR518 – $629
SEC401 – $629	SEC579 – $629	FOR526 – $629
SEC501 – $629	SEC617 – $629	FOR572 – $629
SEC503 – $629	SEC642 – $629	FOR585 – $629
SEC504 – $629	SEC660 – $629	FOR610 – $629
SEC505 – $629	AUD507 – $629	ICS410 – $629
SEC506 – $629	DEV522 – $629	LEG523 – $629
SEC511 – $629	DEV541 – $629	MGT414 – $629
SEC542 – $629	DEV544 – $629	MGT512 – $629
SEC560 – $629	FOR408 – $629	MGT514 – $629
SEC566 – $629	FOR508 – $629	MGT525 – $629

Three ways to register!

Visit the registration desk in the Promenade Foyer
Call (301) 654-SANS
Write to ondemand@sans.org

TABLE OF CONTENTS

CORE NETWARS TOURNAMENT

Hosted by Jeff McJunkin
Thursday, September 17 and Friday, September 18
6:30-9:30pm | Roman II/IV

DFIR NETWARS TOURNAMENT

Hosted by Jake Williams & Philip Hagen
Thursday, September 17 and Friday, September 18
6:30-9:30pm | Roman III

All students who register for a 4-6 day course will be eligible to play NetWars for FREE. Register Now!
sans.org/event/network-security-2015/schedule

Are You Interested in Being a SANS Instructor?

If you have exceptional security skills with lots of hands-on experience, like to give back to the security community, and enjoy helping others learn, then we want to talk to you about being a Mentor which is the first step in becoming a SANS instructor. Come visit us Tuesday, September 15th at the information table near the SANS Registration desk to learn more about this great opportunity!

GENERAL INFORMATION

Registration & Courseware Pick-up Information

Location: Promenade Foyer

Sunday, September 13 (Welcome Reception)	5:00-7:00pm
Monday, September 14	7:00am-5:30pm
Tuesday, September 15 - Saturday, September 19	8:00am-5:00pm
Saturday, September 20 (Short Courses Only)	8:00-9:00am

Internet Café *(WIRED & WIRELESS)*

Location: Promenade Foyer

Monday, September 14	Opens at noon – 24 hours
Tuesday, September 15 - Friday, September 18	Open 24 hours
Saturday, September 19	Closes at 2:00pm

Course Times

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

Course Breaks

7:00-9:00am – Morning Coffee

10:30-10:50am – Morning Break

12:15-1:30pm – Lunch (On your own)

3:00-3:20pm – 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 **8:15-8:45am** on **Monday, September 14** at the **General Session** in ***Florentine I-IV***.

GENERAL INFORMATION

Dining Options

We have assembled a short list of dining suggestions you may like to try during lunch breaks. See page 28 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.

Twitter

Join the conversation on Twitter and use the hashtag **#SANSNetworkSecurity** for up-to-date information from fellow attendees!

Wear Your Badge

To make sure you are in the right place, the SANS door monitors will be checking your badge for each course and evening event 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 Promenade 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)

SEC401: Security Essentials Bootcamp Style

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

MGT414: SANS Training Program for CISSP® Certification

Extended Hours:

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

SEC560: Network Penetration Testing and Ethical Hacking

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

HOSTED: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Training Seminar

COURSE SCHEDULE

START DATE: **Monday, September 14**

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

SEC301: Intro to Information Security
Instructor: Keith Palmgren. . . . . .Location: Octavius 15/16

SEC401: Security Essentials Bootcamp Style
Instructor: Dr. Eric Cole . . . . .Location: Milano VII/VIII
Bootcamp Hours: 5:00-7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials – Enterprise Defender
Instructor: Paul A. Henry . . . . .Location: Neopolitan III

SEC503: Intrusion Detection In-Depth
Instructor: Mike Poor. .Location: Milano II

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

SEC505: Securing Windows with PowerShell and the Critical Security Controls
Instructor: Jason Fossen. . . . . .Location: Octavius 9/10

SEC506: Securing Linux/Unix
Instructor: Hal Pomeranz. . . . . Location: Octavius 13

SEC511: Continuous Monitoring and Security Operations
Instructor: Eric Conrad . . . . .Location: Roman IV

SEC542: Web App Penetration Testing and Ethical Hacking
Instructor: Seth Misenar . . . . .Location: Pompeian III

SEC550: Active Defense, Offensive Countermeasures and Cyber Deception
Instructor: Bryce Galbraith . . . . Location: Anzio

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

SEC561: Immersive Hands-On Hacking Techniques
Instructor: Kevin Fiscus . . . . Location: Octavius 6

SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise
Instructor: Tim Medin . . . . Location: Octavius 14

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
Instructor: James Tarala . . . . .Location: Octavius 17/18

SEC573: Python for Penetration Testers
Instructor: Mark Baggett . . . . Location: Octavius 19

SEC575: Mobile Device Security and Ethical Hacking
Instructor: Joshua Wright. . . . . Location: Neopolitan IV

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

COURSE SCHEDULE

SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses
Instructor: Larry Pesce . . . . Location: Messina

SEC642: Advanced Web App Penetration Testing and Ethical Hacking
Instructor: Justin Searle . . . . Location: Milano VI

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Instructors: James Lyne, Stephen Sims . . . . . . Location: Octavius 5
Bootcamp Hours: 5:15pm-7:00pm (Course days 1-5)

DEV522: Defending Web Applications Security Essentials
Instructor: Johannes Ullrich, Ph.D. . . . . .Location: Pompeian I

DEV541: Secure Coding in Java/JEE: Developing Defensible Apps
Instructor: Gregory Leonard . . . . .Location: Salerno

DEV544: Secure Coding in .NET: Developing Defensible Apps
Instructor: Eric Johnson . . . . Location: Octavius 3

FOR408: Windows Forensic Analysis
Instructor: Rob Lee . . . . Location: Roman III

FOR508: Advanced Digital Forensics and Incident Response
Instructor: Chad Tilbury . . . . Location: Milano I

FOR518: Mac Forensic Analysis
Instructor: Sarah Edwards. . . . . Location: Capri

FOR526: Memory Forensics In-Depth
Instructors: Jake Williams . . . . Location: Pompeian II

FOR572: Advanced Network Forensics and Analysis
Instructors: Philip Hagen . . . . .Location: Octavius 7/8

FOR585: Advanced Smartphone Forensics
Instructors: Heather Mahalik. . . . . Location: Neopolitan II

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Instructor: Lenny Zeltser . . . . Location: Octavius 11

MGT414: SANS Training Program for CISSP® Certification
Instructor: Jonathan Ham . . . . .Location: Pompeian IV
Bootcamp Hours: 8:00-9:00am (Course days 2-6) & 5:00-7:00pm (Course days 1-5)

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

MGT514: IT Security Strategic Planning, Policy and Leadership
Instructor: Frank Kim . . . . Location: Milano V

MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep
Instructor: Jeff Frisk . . . . .Location: Octavius 1/2

COURSE SCHEDULE

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems
Instructor: David Hoelzer . . . . Location: Milano III

LEG523: Law of Data Security and Investigations
Instructor: Benjamin Wright . . . . Location: Octavius 20

ICS410: ICS/SCADA Security Essentials
Instructor: Matthew Luallen . . . . .Location: Octavius 21/22

HOSTED: (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Training Seminar
Instructor: Mano Paul . . . . Location: Octavius 23
Extended Hours: 5:00-6:00pm (Course Days 1-5)

START DATE: Thursday, September 17

CORE NetWars Tournament
Host: Jeff McJunkin . . . . Location: Roman II/IV
Hours: 6:30-9:30pm

DFIR NetWars Tournament
Hosts: Rob Lee & Chad Tilbury . . . . Location: Roman III
Hours: 6:30-9:30pm

START DATE: Sunday, September 20

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

SEC440: Critical Security Controls: Planning, Implementing, and Auditing
Instructor: Randy Marchany . . . . Location: Octavius 3

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Instructor: Pieter Danhieux . . . . .Location: Octavius 1/2

MGT305: Technical Communication and Presentation Skills for Security Professionals
Instructor: David Hoelzer . . . . Location: Octavius 13

MGT415: A Practical Introduction to Cyber Security Risk Management
Instructor: James Tarala . . . . Location: Octavius 5

MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program
Instructor: Lance Spitzner . . . . Location: Octavius 6

MGT535: Incident Response Team Management
Instructor: Christopher Crowley . . . . .Location: Octavius 7/8

HOSTED: Health Care Security Essentials
Instructor: Greg Porter . . . . .Location: Octavius 9/10

HOSTED: Physical Penetration Testing
Instructor: The CORE Group . . . . Location: Octavius 11

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

Bundle GIAC certification with SANS training and SAVE $320!

In the information security industry, certification matters. The Global Information Assurance Certification (GIAC) program offers skills-based certifications that go beyond high-level theory and test true hands-on and pragmatic skill sets that are highly regarded in the InfoSec industry.

Save $320 when you bundle your certification attempt with your SANS training course. Simply stop by Registration in the Promenade Foyer and add your certification option before the last day of class.

Find out more about GIAC at www.giac.org or call (301) 654-7267.

SANS Technology Institute

The SANS Technology Institute transforms the world's best cybersecurity training and certifications into a comprehensive, rigorous, graduate education experience.

Master's Degree Programs:

- M.S. in Information Security Engineering
- M.S. in Information Security Management

Specialized Graduate Certificates:

- Penetration Testing & Ethical Hacking
- Incident Response
- Cybersecurity Engineering (Core)
- Cyber Defense Operations

Learn more at www.sans.edu | info@sans.edu

Congratulations to the SANS Technology Institute Class of 2015

Master of Science in Information Security Engineering

Carrie Roberts	James Tarala
Courtney Imbert	Josh Johnson
George Khalil	Kiel Wadner

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, SEPTEMBER 13

SPECIAL EVENT

Registration Welcome Reception

Sun, Sept 13 | 5:00-7:00pm | Location: Promenade Foyer

Register early and network with your fellow students!

MONDAY, SEPTEMBER 14

SPECIAL EVENT

General Session – Welcome to SANS

Speaker: Dr. Eric Cole

Mon, Sept 14 | 8:15-8:45am | Location: Florentine I-IV

Join us for a 30-minute overview to help you get the most out of your SANS training experience. You will receive event information and learn about programs and resources offered by SANS. This brief session will answer many questions and get your training experience off to a great start. This session will be valuable to all attendees but is highly recommended for first time attendees.

SPECIAL EVENT

Women in Technology Meet and Greet

Speaker: Deanna Boyden

Mon, Sept 14 | 6:15pm - 7:15pm | Location: Genoa

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.

SPECIAL EVENTS

KEYNOTE

WHY?

Speaker: Dr. Eric Cole

Mon, Sept 14 | 7:15-9:15pm | Location: Florentine I-IV

Cybersecurity breaches have become a norm and people are no longer surprised when they hear about them on the news, but WHY? Organizations continue to spend a significant amount of money and buy lots of product, however it seems to make little, if any, difference, but WHY? Despite the fact that people are talking more about security and are more aware of the threats, there is little impact on security, but WHY? Startups are creating new technologies, venture capitalist firms continue to dump significant money into this area, and attacks continue, but WHY? In this solution-based talk, Dr. Cole, a world-renowned security expert, will get to the heart of the problem and address WHY the current approach to security is not working. Once the problem is dissected, systematic, provable methods for properly addressing security will be provided. This talk will provide an actionable roadmap to help prepare the next generation of Cyber Defenders to tackle the problems that need to be addressed.

Based on experience gained from responding to many high-profile incidents and engaging with many customers, Dr. Cole will cover solutions that Cyber Defenders can use to increase their security and gain better visibility into what is happening within their organization. Topics include crypto-free zones, outbound proxies, network segmentation, and defending a compromised network. If your organization has not detected an attack in the last six months you need to attend this talk. In most cases if you have not detected an attack it is not because it is not happening, but because you are not looking in the right area. This talk will change your vantage point to better understand how to prevent, detect, and respond to advanced attacks. Are you ready to become a Cyber Defender? Are you ready to take a proactive stance against the adversary? Are you ready to take the Dr. Cole Challenge?

TUESDAY, SEPTEMBER 15

LUNCH & LEARN

Want to be a SANS Instructor?

Speaker: Eric Conrad
Tue, Sept 15 | 12:30-1:15pm | Location: Pompeian II

Have you ever wondered what it takes to be a SANS instructor and how you can rise to the top to demonstrate the talents necessary to be part of the SANS faculty? Attend this informative session and hear how SANS Principal instructor Eric Conrad accomplished his goal and learn how you can start your own journey to be part of the amazing SANS Faculty. Have a small team to train? Mentor @Work is a great option for training teams of 3-10. You can learn more about this option in Eric's presentation.

MASTER'S PRESENTATION

eAUDIT: Designing a Generic Tool to Review Entitlements

Speaker: Francois Begin – Master's Degree Candidate
Tue, Sept 15 | 7:15-7:55pm | Location: Messina Room

SANS@NIGHT

Evolving Threats

Speaker: Paul A. Henry
Tue, Sept 15 | 7:15-8:15pm | Location: Florentine I

For nearly two decades, defenders have fallen into the "Crowd Mentality Trap." They have simply settled on doing the same thing everyone else was doing, while at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and upon attempting to outwit attackers' delivery methods. This leaves us woefully exposed and according to a recent Data Breach Report, it has resulted in 3,765 incidents, 806 million records exposed, and $157 billion in data breach costs in only the past six years.

SANS@NIGHT

Playing with SCADA's Modbus Protocol

Speaker: Justin Searle
Tue, Sept 15 | 7:15-8:15pm | Location: Florentine II

Join Justin for a peek into one of SCADA's oldest and most deployed TCP/IP protocols. He'll take you through the modbus network protocol standard and walk you through some hands-on exercises, including analyzing modbus network captures, configuring modbus endpoint simulators, generating your own modbus traffic to query PLCs, and a primer on fuzzing modbus endpoints. If you want to follow along on your own laptop, download the latest version of SamuraiSTFU (www.SamuraiSTFU.org) and have it running in VMware before we start!

SANS@NIGHT

Using an Open Source Threat Model for Prioritized Defense

Speaker: James Tarala
Tue, Sept 15 | 7:15-8:15pm | Location: Florentine III

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.

MASTER'S PRESENTATION

Coding for Incident Response: Solving the Language Dilemma

Speaker: Shelly Giesbrecht – Master's Degree Candidate
Tue, Sept 15 | 8:15-8:55pm | Location: Messina Room

SANS@NIGHT

What's New in Windows 10 and Server 2016?

Speaker: Jason Fossen
Tue, Sept 15 | 8:15-9:15pm | Location: Florentine I

Windows 8 was a flop, so will the second try be the charm? Microsoft intends Windows 10 to be a universal platform (PCs, tablets, phones, etc.) to run universal apps. The graphical interface of Windows 8 made that OS undeployable, so will users prefer the Windows 10 desktop over Windows 7? This session will lay out what's new in Windows 10, with an emphasis on security and enterprise management, such as Windows Hello, Passport, Cortana, and running LSASS.EXE in a separate virtual machine. The speaker, Jason Fossen, is a SANS Institute Fellow and author of the SANS Securing Windows course (http://sans.org/SEC505). Windows Server 2016 will also soon be available, so we'll also cover what's new and interesting on the server side too, such as Virtual TPM chips in Hyper-V client VMs. There is a lot more to Windows 10 than just the return of the Start Menu, so come see!

SANS@NIGHT

Card Fraud 101

Speaker: G. Mark Hardy

Tue, Sept 15 | 8:15-9:15pm | Location: Florentine II

Ever get a call from your bank saying your credit card was stolen, but it was still in your wallet? What's going on here? Card fraud costs $16 billion annually, and it's not getting better. Target, PF Chang's, Michaels, Home Depot, who's next? Find out how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and why Apple Pay is trivial to compromise. See if your bank even bothers to use the security protections it could – we'll have a mag stripe card reader so you can really see what's in your wallet. Certified SANS Instructor G. Mark Hardy is the CEO and founder of CardKill Inc., a start-up that helps banks preemptively kill stolen cards BEFORE they are used in fraud.

SANS@NIGHT

A History of ATM Violence

Speaker: Erik Van Buggenhout

Tue, Sept 15 | 8:15-9:15pm | Location: Florentine III

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. With the continuous rise in cyber criminality, these cash-filled computers are more and more becoming an interesting target for cyber-attacks. The Ploutus malware and Carbanak attack are only two recent examples where cyber-attacks against ATMs were mounted. During Erik's talk, he will focus on the typical design and architecture of current ATMs. He will then further focus on possible areas for attack and provide some advice to help increase the ATM's cybersecurity posture. Lastly, his presentation will include a live demonstration of an ATM malware sample deployed on a current ATM.

WEDNESDAY, SEPTEMBER 16

SANS@NIGHT

DLP FAIL!!! Using Encoding, Steganography, and Covert Channels to Evade DLP and Other Critical Controls

Speaker: Kevin Fiscus

Wed, Sept 16 | 7:15-8:15pm | Location: Florentine I

It's all about the information! Two decades after the movie Sneakers, the quote remains as relevant, if not more so. The fact that someone hacks into an environment is interesting but not that relevant. What is important is what happens after the compromise. If the data is destroyed or modified, organizations are negatively impacted but the benefits to an attacker for destruction or alteration are somewhat limited. Stealing information, however, is highly profitable. Identity theft, espionage, and financial attacks involve the exfiltration of sensitive data. As a result, organizations deploy tools to detect and/or stop that data exfiltration. While these tools can be extremely valuable, many have serious weaknesses; attackers can encode, hide, or obfuscate the data, or can use secret communication channels. This session will talk about and demonstrate a range of these methods.

SANS@NIGHT

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

Speaker: Josh Wright

Wed, Sept 16 | 7:15-8:15pm | Location: Florentine II

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

The Crazy New World of Cyber Investigations: Law, Ethics, and Evidence

Speaker: Ben Wright

Wed, Sept 16 | 7:15-8:15pm | Location: Florentine III

Increasingly, employers and enterprises are engaged in cyber investigations. The explosion of cyber evidence (email, text, meta data, social media, etc.) about every little thing that anyone does or says creates a massive need for HR departments, IT departments, internal audit departments, and other investigators to find and sift through this evidence. These cyber investigations are guided, motivated, and restricted by a blizzard of new laws and court cases. Increasingly enterprises need professionals with backgrounds in cyber forensics, cyber law, and computer privacy.

MASTER'S PRESENTATION

Finding Evil in the Whitelist

Speaker: Josh Johnson – Master's Degree Candidate

Wed, Sept 16 | 7:15-7:55pm | Location: Messina Room

SPECIAL EVENT

Death from Above: Hands-On Drone and IoT Hacking

Speakers: Josh Wright, Tim Medin, James Lyne, and Steve Sims
Wed, Sept 16 | 7:30-9:30pm | Location: Roman IV

Join Josh, Tim, James, and Steve in this ***"limited-seating"*** SANS special event. Somewhere along the line product developers thought it would be a good idea to connect things like pet food dispensers and automated plant-watering devices to the Internet and smartphone apps. What could go wrong? We will have a collection of "things" for you to try and find vulnerabilities. We will walk through an introduction of how to extract and analyze firmware, and the types of bugs that are most commonly found. That's not all! In tandem we will be running a "Hack the Drone" challenge where your goal will be to break and pivot through a series of systems, ultimately reaching one that controls a drone (or two) that will be sitting in the room awaiting your hacking instructions for live take-off. Helmets optional. First one to reach the drone will receive a SEC660 challenge coin! So how do you gain entry? We will have a limited number of passes available. There will be four instructors from whom you can get a pass:

Josh Wright in SEC575 | **Tim Medin** in SEC562
Stephen Sims or **James Lyne** in SEC660.

What do you need to bring? A laptop with a modern Debian Linux VM.

SANS@NIGHT

Smartphone and Network Forensics Goes Together Like Peas and Carrots

Speakers: Heather Mahalik and Phil Hagen
Wed, Sept 16 | 8:15-9:15pm | Location: Florentine III

Although two distinct and critical forensic disciplines, there are strong ties between the smartphone and network aspects of the forensic process. Smartphone investigations cover myriad devices, operating systems, applications, and data storage mechanisms but a great deal of their functionality involves a single common technology – TCP/IP communications. On the other hand, hunting an attacker's network activities within your environment often identifies endpoints including smartphones as relevant to the investigation, which need in-depth device analysis. In this talk, Heather Mahalik, will address the smartphone side of this investigative coin as covered in SANS FOR585: Advanced Smartphone Forensics. Phil Hagen will look at things from the network side as covered in SANS FOR572: Advanced Network Forensics and Analysis. As often identified in the forensic process, a comprehensive approach is necessary to conduct a thorough investigation.

MASTER'S PRESENTATION

Live Long and Prosper by Protecting SPoC!

Speaker: David Belangia – Master's Degree Candidate
Wed, Sept 16 | 8:15-8:55pm | Location: Messina Room

SANS@NIGHT

Meterpreter without Meterpreter

Speaker: Mark Baggett
Wed, Sept 16 | 8:15-9:15pm | Location: Florentine I

Metasploit's meterpreter is an extremely powerful attack payload. It is often the tool of choice for post-exploitation pillaging by today's professional penetration tester. But end point security products such as anti-virus can make meterpreter bitter sweet. What do you do when end point protection prevents you from using meterpreter? Come join Mark Baggett for this presentation on "meterpreter without meterpreter" and he'll show you.

SANS@NIGHT

Hacking Back, Active Defense, and Internet Tough Guys

Speaker: John Strand
Wed, Sept 16 | 8:15-9:15pm | Location: Florentine II

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.

THURSDAY, SEPTEMBER 17

CORE NETWARS TOURNAMENT

Host: Jeff McJunkin
Thu, Sept 17 & Friday, Sept 18 | 6:30-9:30pm | Location: Roman II/IV

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.

DFIR NETWARS TOURNAMENT

Hosts: Jake Williams and Phil Hagen
Thu, Sept 17 & Friday, Sept 18 | 6:30-9:30pm | Location: Roman 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.

SANS@NIGHT

Debunking the Complex Password Myth

Speaker: Keith Palmgren
Thu, Sept 17 | 7:15-8:15pm | Location: Florentine II

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

Malware Analysis Essentials using REMnux

Speaker: Lenny Zeltser
Thu, Sept 17 | 8:15-9:15pm | Location: Florentine I

The REMnux distro allows malware analysts to examine many aspects of malicious software in a lightweight Linux environment. This practical session will show you how to get started with this powerful toolkit and demonstrate some of the most useful tools installed as part of the REMnux environment. Lenny Zeltser, who teaches SANS' reverse-engineering malware course FOR610, will share how you can use the utilities installed on REMnux to:

- Study network interactions of malicious programs
- Analyze malicious websites and obfuscated JavaScript
- Examine malicious document files
- Explore important aspects of suspicious Windows executables

If you haven't experimented with Linux-based tools for malware analysis, you've been missing out. And if you've been meaning to begin exploring the field of malware analysis, this talk will help you get started.

FRIDAY, SEPTEMBER 18

SANS@NIGHT

Making Awareness Stick

Speaker: Lance Spitzner
Fri, Sept 18 | 7:15-8:15pm | Location: Florentine I

One of the most common, long-term challenges faced by any awareness program is getting it to stick. How do you create an engaging program that people want to listen to, teaches them more, and ultimately changes behaviors? In this talk, Lance Spitzner will explain what organizations are effectively doing around the world to emotionally engage and communicate to their employees. Key points you will learn include:

- Behavior modeling
- Defining your culture
- Developing your engagement strategy
- Self-education
- Ambassador/Champion programs

SANS@NIGHT

Securing The Kids

Speaker: Lance Spitzner
Fri, Sept 18 | 8:15-9:15pm | Location: Florentine I

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, Lance Spitzner will 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.

VENDOR EVENTS

Vendor Solutions Expo

Wed, Sept 16 | 12:00-1:30pm | 5:30-7:30pm
Location: Octavius 24/25

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, Sept 16 | 5:30-7:30pm | Location: Octavius 24/25

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, Sept 16 | 12:00-1:30pm | Location: Octavius 24/25

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:

BeyondTrust
Bradford Networks
Centrify
Cisco
Datacom Systems
EiQ Networks
Fidelis Cybersecurity
Forescout Technologies
LightCyber
LogRhythm
Lookingglass Cyber Solutions
Palo Alto Networks
PhishMe
Pwnie Express
Qualys
Splunk
Symantec
ThreatSTOP
Threatstream
Triumfant
Vectra Networks
VSS Monitoring

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.

ForeScout
Access ability.

LUNCH AND LEARN

An Architecture for Continuous Monitoring and Mitigation

Speaker: Robert McLean, Systems Engineer
Tue, Sept 15 | 12:30-1:15pm | Location: Roman IV

This session examines a reference architecture for continuous monitoring and mitigation, based on next-generation network access control, and a standards-based architecture to share information between and among legacy security systems.

EiQ Continuous Security Intelligence™

LUNCH AND LEARN

Achieving Continuous Security with Your Limited Resources

Speaker: Dick Faulkner, Vice President of Worldwide Sales
Tue, Sept 15 | 12:30-1:15pm | Location: Roman I

In this session we will discuss the novel approach of using a combination of People, Process, and Technology delivered as a service by EiQ to achieve a continuous security environment. A large number of customers across a variety of industries are leveraging EiQ's SOCVue service to cost-effectively gain visibility into their security posture on a 24x7 basis and are leveraging EiQ's trained product and SOC professionals to proactively identify weak links in their security landscape as well as potential incidents and obtain remediation guidance before it's too late.

beyondtrust®
Beyond Traditional Security

LUNCH AND LEARN

Aligning Vulnerability and Privilege Management in the Context of Business Risk

Speaker: Morey Haber, Vice President of Technology
Tue, Sept 15 | 12:30-1:15pm | Location: Roman II

Despite gigantic investments in IT security, many organizations still struggle to identify real, critical risks buried within massive amounts of data. CISOs need new strategies for assessing, prioritizing and addressing both internal and external risks in business context. Join our conversation to discuss how aligning vulnerability management and privilege management programs can shed new light on risk in terms of compliance, asset integrity, data confidentiality, and other unique business requirements, while enabling IT and security teams to efficiently collaborate on risk reduction efforts enterprise-wide.

LIGHTCYBER

LUNCH AND LEARN

Breach Detection 101: What do Attackers Actually do in a Network, and how can You Catch Them?

Speaker: DT Thompson, Sr. Director Product Management
Tue, Sept 15 | 12:30-1:15pm | Location: Florentine I

This session will discuss the role of active breach detection, including new research from the SANS Analyst Program about review of the LightCyber Magna Platform™. Attendees will be among the first to receive this new SANS whitepaper that new techniques in breach detection.

tenable
network security

LUNCH AND LEARN

A Practitioner and Manager's Guide to Optimizing Enterprise Vulnerability Management

Speaker: Jack Daniel, Product Manager
Tue, Sept 15 | 12:30-1:15pm | Location: Pompeian IV

During the session you will also learn how the "vulnerability workbench" capabilities in Tenable SecurityCenter Continuous View support a more efficient and effective vulnerability management practice.

SOPHOS
Infogressive, Inc.
Aggressive Information Security

LUNCH AND LEARN

Prevent – Detect – Respond

Speaker: Will Tipton, Security Engineer
Thu, Sept 17 | 12:30-1:15pm | Location: Florentine I

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

CISCO™

LUNCH AND LEARN

Raising the Security Bar with Integrated Threat Defense

Speaker: Steve Passarelli and William Young, Cisco
Tue, Sept 15 | 12:30-1:15pm | Location: Roman III

In this talk, we will look at how threat intelligence and enterprise visibility becomes the cornerstone for integrating your security technologies, automating your security practice where it makes sense for your environment, and improving the business outcome of your security program.

Centrify®

LUNCH AND LEARN

Identity is the New Perimeter

Speaker: Dean Thompson
Tue, Sept 15 | 12:30-1:15pm | Location: Florentine II

We will discuss how identity security is really the only thing that can protect your company. Explore how to provide single Active Directory or cloud-based login to corporate resources, PCs and Macs, mobile devices, and cloud apps like Office 365, Salesforce.com, and WEbEx and Discover how a secure web portal can provide one-click web access, as well as self-service account management, so your company can embrace bring-your-own (BYO) initiatives, without sacrificing security policy.

LOOKINGGLASS

LUNCH AND LEARN

Making Threat Intelligence Work Better for Security Operations Teams

Speaker: Allan Thomson, Chief Technology Officer
Tue, Sept 15 | 12:30-1:15pm | Location: Florentine III

Getting the most out of threat intelligence is complicated. In this session, we will discuss how to take threat intelligence and act upon it in your organization to make more effective use of threat intelligence.

FIDELIS CYBERSECURITY

LUNCH AND LEARN

Turn on the Lights! Case Studies of Malware in Memory

Speaker: Tyler Halfpop, Threat Researcher
Tue, Sept 15 | 12:30-1:15pm | Location: Florentine IV

The purpose of this session is to demonstrate, via a case-studies approach, the wealth of information that can be obtained from memory to better detect and understand malware in order to improve incident response and digital forensics capabilities.

ThreatSTOP

LUNCH AND LEARN

Hackers are Equal Opportunity Businessmen: Everyone's a Target

Speaker: John Thompson, Director, Systems Engineering
Thu, Sept 17 | 12:30-1:15pm | Location: Florentine IV

Hackers are now running like any business, with consistent outbound forays into finding new targets (victims). They are using the cloud and other broad-reaching tools to launch automated attacks looking for vulnerable network entry points. It is not personal, it is not a guy at a keyboard. The attackers launch methodical scans looking for unprotected endpoints—anything online. They just need a beachhead, be it a printer or a laptop. More often than not, a close look into a network for malware will turn up a surprising amount of undetected threats. Learn best practices for deflecting attacks, and preventing malware on your network from stealing data.

PHISHME

LUNCH AND LEARN

Change the Game – Fight Those Who Fight You

Speaker: Ronnie Ronnie Tokazowski, Senior Research Engineer
Thu, Sept 17 | 12:30-1:15pm | Location: Florentine II

Over the years, attackers of all affiliations have broken into corporations and stolen documents, pilfered bank accounts, or attempted to social engineer our employees. One thing that many forget is that the attackers are human too, and are susceptible to the same techniques they are using. This session will present several use-cases and ideas in order to make life more difficult for the attackers you are facing.

paloalto networks

LUNCH AND LEARN

Crack the Code: Defeat the Advanced Adversary

Speaker: Richard Porter, Systems Engineer
Thu, Sept 17 | 12:30-1:15pm | Location: Florentine III

Cybersecurity can sometimes feel like a puzzle, a code to crack. This isn't how it should be. Adversaries don't need to win. Stopping them doesn't require endless time and resources because most just take the path of least resistance for the easiest win. Your objective as a security practitioner is to raise the total cost of a successful attack, to make your organization a less appealing target. Join Palo Alto Networks for a detailed look at real attacks and how you can crack the code to defend your organization

QUALYS® CONTINUOUS SECURITY

LUNCH AND LEARN

Tackling Application Security Challenges Through Progressive Scanning

Speaker: Michael M. Class, Web Application Security Subject Matter Expert
Thu, Sept 17 | 12:30-1:15pm | Location: Pompeian I

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

TRIUMFANT

LUNCH AND LEARN

Anomaly Detection: Boots on the Ground for 21st Century Cyber Warfare

Speaker: Greg Wessel, COO
Thu, Sept 17 | 12:30-1:15pm | Location: Pompeian IV

Today, if you're unprepared for a breach – or unaware that one has occurred – the adversary will take advantage. Therefore, you need to put "boots on the ground" in the face of 21st century cyber warfare. How is that possible? Anomaly Detection. Learn how Triumfant's AtomicEye solution closes the breach detection gap with rapid response and remediation.

Symantec.

LUNCH AND LEARN

#SecurityisaMyth

Speaker: Jeff Guilfoyle, Principal SE
Thu, Sept 17 | 12:30-1:15pm | Location: Pompeian III

Cyber attacks – it is not a matter of "if" but "when". Hardly a day goes by without another report of hacker attacks, data leaks or espionage. As the volume and sophistication of attacks increases, we need a better game plan. . Attend for a discussion on intelligence-driven security, including an overview of recent attack campaign trends, key elements of a proactive security posture, and how to respond quickly and effectively when incidents occur.

VECTRA™
Security that thinks.™

LUNCH AND LEARN

A Methodology for Real-Time Automated Threat and Cyber Attack Detection

Speaker: Pablo Garcia, Sales Engineer
Thu, Sept 17 | 12:30-1:15pm | Location: Pompeian II

Over the past year, cyber attacks have gone from being a worst-case scenario for security teams to a real-world certainty. Yet for all the recent investment and focus on cybersecurity, attackers continue to succeed at stealing or destroying our most valued assets. In this discussion, we will deconstruct recent cyber attacks to see what is working in security and where the industry still has gaps. Then we will go beyond the search for simplistic silver bullets, and propose new models of defense-in-depth that can apply generically to detecting today's most sophisticated attacks.

VENDOR EVENTS

THREATSTREAM®

LUNCH AND LEARN

Social Threat Intelligence (STI)

Speaker: Trevor Welsh, Principal Security Strategist
Thu, Sept 17 | 12:30-1:15pm | Location: Roman I

Social has changed many aspects of information security. Fascinatingly, enterprise has been slow to embrace community sourcing security intelligence. Trevor Welsh of ThreatStream will present on Social Threat Intelligence (STI). This talk will detail how STI exists today, and how it might exist tomorrow. Trevor will also detail how enterprise can best take advantage of STI in a sensible, secure way.

FUTURE EVENT

SANS
Network Security 2016

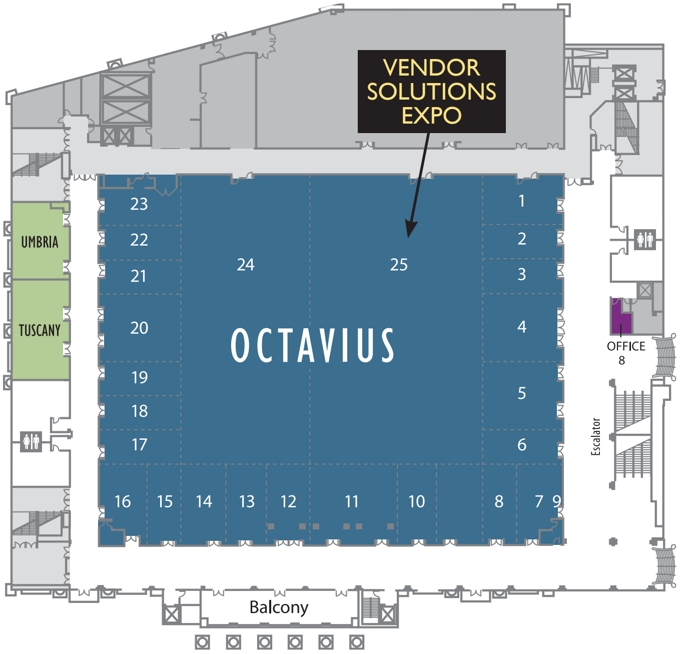
At Caesars Palace

SEPT 12-17, 2016

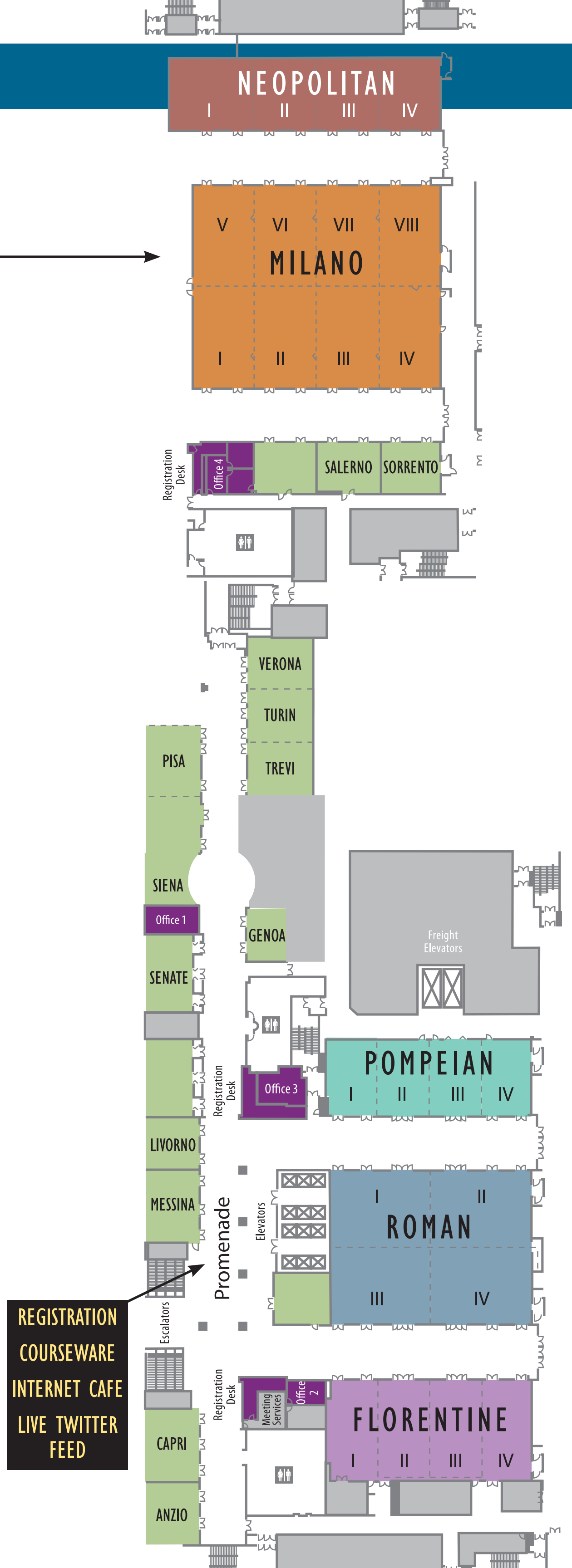
Save the Date!

HOTEL FLOORPLAN

PROMENADE SOUTH



PROMENADE LEVEL



DINING OPTIONS

BACCHANAL BUFFET
Bacchanal Buffet features more than 500 items prepared by a team of master chefs in nine globally-inspired open kitchens.

UPSCALE ITALIAN

RAO'S
Come experience simple, honest, home cooking at Rao's at Caesars Palace, voted one of the best Italian restaurants in Las Vegas.

UPSCALE JAPANESE

NOBU
The ideal destination to be seen, socialize, and enjoy the unique cuisine of celebrated Chef Nobu Matsuhisa.

UPSCALE STEAKHOUSE

OLD HOMESTEAD STEAKHOUSE
Old Homestead Steakhouse at Caesars Palace offers fine dining in a Las Vegas restaurant inspired by the original Old Homestead, one of NYC's most historic restaurants.

UPSCALE FRENCH

PAYARD PATISSERIE & BISTRO
The Payard Patisserie & Bistro at Caesars Palace, unique among Las Vegas restaurants, contains an upscale bistro as well as a chocolate and pastry shop.

RESTAURANT GUY SAVOY
Restaurant Guy Savoy at Caesars Palace has been called the best restaurant in Las Vegas, serving elegant French Cuisine in a fine dining environment.

UPSCALE CONTEMPORARY SOUTHWESTERN

MESA GRILL
Brought to Caesars Palace Las Vegas by celebrity chef Bobby Flay, Mesa Grill Southwestern Restaurant features bold flavors and specialty margaritas.

UPSCALE CHINESE

EMPRESS COURT
Dine on authentic Cantonese seafood at the Empress Court Chinese Restaurant, a premium Las Vegas restaurant at Caesars Palace Las Vegas.

CASUAL CHINESE

BEIJING NOODLE NO. 9
Beijing Noodle No. 9 offers Northern Chinese cuisine in a friendly, casual atmosphere. The best restaurants in Las Vegas can only be found at Caesars.

CASUAL AMERICAN

MUNCHBAR
Come take a break at Munchbar, a Las Vegas restaurant and pub where you can find all your favorite comfort foods on a menu created by renowned Chef Bryan Ogden.

SERENDIPITY 3
Serendipity 3, one of the great Las Vegas restaurants at Caesars Palace, serves fun and whimsical entrees and delectable desserts.

CENTRAL BY MICHEL RICHARD
At Central, Chef Michel Richard serves American food with a French twist in a casual dining environment. For all the best restaurants in Las Vegas, try Caesars Palace.

CASUAL CAFE/VARIETY

GORDON RAMSAY PUB & GRILL
Gordon Ramsay Pub & Grill is the neighborhood restaurant conceptualized by the award-winning chef. The 290 seat restaurant is the most authentic English pub experience in Las Vegas, as only a native UK chef can provide.

CYPRESS STREET MARKETPLACE
Casual dining at Cypress Street Marketplace offers a wide variety of cuisines and specialty food. Find all the best Las Vegas restaurants at Caesars Palace.

Future SANS Training Events

SANS **Baltimore** 2015
Baltimore, MD | Sept 21-26

SANS **Cyber Crime** SUMMIT & TRAINING
Dallas, TX | Sept 21-26

SANS **Seattle** 2015
Seattle, WA | Oct 5-10 | #SANSSeattle

SANS **Tysons Corner** 2015
Tysons Corner, VA | Oct 12-17 | # SANSTysonsCorner

SANS **Cyber Defense San Diego** 2015
San Diego, CA | Oct 19-24 | #CyberDefSD

SANS **South Florida** 2015
Fort Lauderdale, FL | Nov 9-14

SANS **Pen Test Hackfest** SUMMIT & TRAINING 2015
Alexandria, VA | Nov 16-23

SANS **San Francisco** 2015
San Francisco, CA | Nov 30 - Dec 5

SANS **Security Leadership** SUMMIT & TRAINING 2015
Dallas, TX | Dec 3-10

SANS **Cyber Defense Initiative** 2015
& **4th Annual Tournament of Champions**
Washington DC | Dec 14-19

SANS **Las Vegas** 2016
Las Vegas, NV | Jan 9-14

SANS **Security East** 2016
New Orleans, LA | Jan 25-30

SANS **Scottsdale** 2016
Scottsdale, AZ | Feb 8-13

SANS **McLean** 2016
McLean, VA | Feb 15-20

SANS **ICS** SUMMIT & TRAINING 2016
Orlando, FL | Feb 16-23

SANS **Anaheim** 2016
Anaheim, CA | Feb 22-27

SANS **Philadelphia** 2016
Philadelphia, PA | Feb 29 - Mar 5

SANS 2016
Orlando, FL | Mar 12-21

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