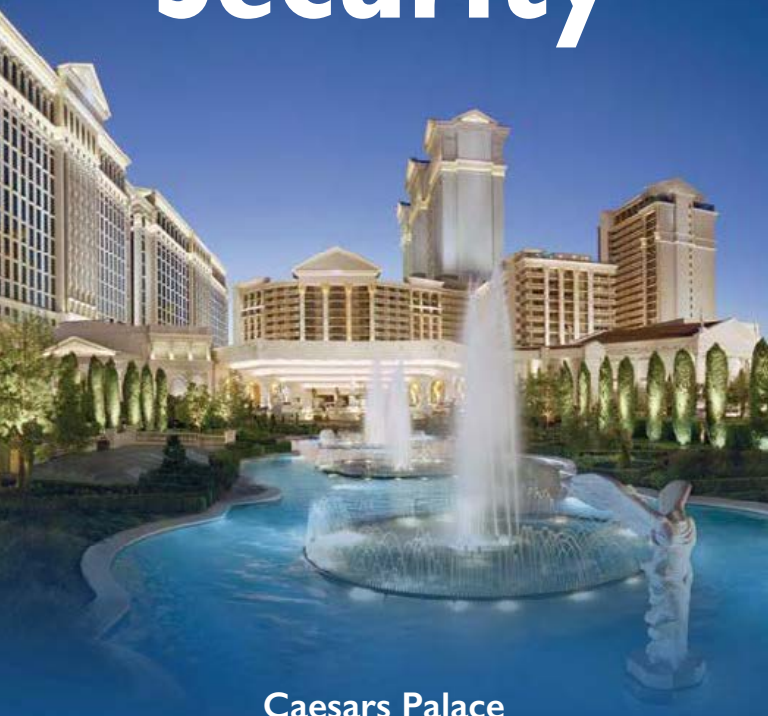
SANS Network Security 2016



Caesars Palace

Las Vegas, NV

September 10-19, 2016

PROGRAM GUIDE

@SANSInstitute #SANSNetworkSecurity

TABLE OF CONTENTS

SANS NETWARS EXPERIENCE

(FREE with any 4-6 Day SANS Course Registration)

Stop by the Registration Desk for more information.

CORE NETWARS EXPERIENCE

Hosted by Jeff McJunkin
Thursday, September 15 and Friday, September 16
6:30pm - 9:30pm | Roman I & II

DFIR NETWARS TOURNAMENT

Hosted by Rob Lee & Chad Tilbury
Thursday, September 15 and Friday, September 16
6:30pm - 9:30pm | Roman III & IV

GENERAL INFORMATION

Registration & Courseware Pick-up Information

Location: Promenade Foyer

Saturday, September 10 (Short Courses Only) . . . . 8:00am - 9:00am
Sunday, September 11 (Welcome Reception). . . . . 5:00pm - 7:00pm
Monday, September 12. . . . . 7:00am - 9:00am
Tuesday, September 13 - Saturday, September 17 9:00am - 5:00pm

Location: Siena Room

Sunday, September 18 . . . . . 8:00am - 9:00am

Internet Café *(WIRELESS)*

Location: Imperial Boardroom

Monday, September 12. . . . . Opens at noon - 24 hours
Tuesday, September 13 - Friday, September 16 . . . Open 24 hours
Saturday, September 17 . . . . . 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 **8:00am - 8:30am** on **Monday, September 12** at the ***General Session*** in **Florentine I/II**.

GENERAL INFORMATION

Photography Notice

SANS may take photos of classroom activities for marketing purposes. SANS Network Security attendees grant SANS all rights for such use without compensation, unless prohibited by law. Those who wish not to be photographed onsite should notify the photographer.

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 day and evening session and drop it in the evaluation box.

Wear Your Badge

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

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

SEC511: Continuous Monitoring and Security Operations

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

SEC560: Network Penetration Testing and Ethical Hacking

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

COURSE SCHEDULE

START DATE: **Saturday, September 10**
Time: 9:00am - 5:00pm

SEC440: Critical Security Controls: Planning, Implementing, and Auditing
Chris Christianson . . . . . LOCATION: Anzio

SEC567: Social Engineering for Penetration Testers
Dave Shackleford . . . . . LOCATION: Capri

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
Eric Conrad . . . . . LOCATION: Pompeian IV

MGT415: A Practical Introduction to Cyber Security Risk Management
James Tarala . . . . . LOCATION: Pompeian III

MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program
Lance Spitzner . . . . . LOCATION: Pompeian II

MGT535: Incident Response Team Management
Christopher Crowley . . . . . LOCATION: Pompeian I

DEV544: Secure Coding in .NET: Developing Defensible Apps
Aaron Cure . . . . . LOCATION: Salerno

HOSTED: Physical Penetration Testing
The CORE Group . . . . . LOCATION: Messina

START DATE: **Monday, September 12**
Time: 9:00am - 5:00pm (Unless otherwise noted)

SEC301: Intro to Information Security
Keith Palmgren . . . . . LOCATION: Octavius 17/18

SEC401: Security Essentials Bootcamp Style
Paul A. Henry . . . . . LOCATION: Milano VII/VIII
Bootcamp Hours: 5:00pm - 7:00pm (Course days 1-5)

SEC501: Advanced Security Essentials – Enterprise Defender
Bryan Simon . . . . . LOCATION: Neopolitan III

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

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

SEC505: Securing Windows and PowerShell Automation
Jason Fossen . . . . . LOCATION: Octavius 9/10

SEC506: Securing Linux/Unix
Hal Pomeranz . . . . . LOCATION: Capri

SEC511: Continuous Monitoring and Security Operations
Seth Misenar . . . . . LOCATION: Milano I
Bootcamp Hours: 5:15pm-7:00pm (Course days 1-5)

COURSE SCHEDULE

SEC542: Web App Penetration Testing and Ethical Hacking
Micah Hoffman . . . . . LOCATION: Pompeian III

SEC550: Active Defense, Offensive Countermeasures and Cyber Deception
Bryce Galbraith . . . . . LOCATION: Octavius 6

SEC560: Network Penetration Testing and Ethical Hacking
Ed Skoudis . . . . . LOCATION: Neopolitan I
Extended Hours: 5:00pm - 7:15pm (Course Day 1 only)
*Extended hours will be led by John Strand in the SEC504 Classroom – Roman II

SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
James Tarala . . . . . LOCATION: Octavius 15/16

SEC573: Python for Penetration Testers
Jonathan Thyer . . . . . LOCATION: Octavius 19

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

SEC579: Virtualization and Private Cloud Security
Dave Shackleford . . . . . LOCATION: Anzio

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

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

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

SEC760: Advanced Exploit Development for Penetration Testers
Stephen Sims . . . . . LOCATION: Octavius 3
Bootcamp Hours: 5:15pm-7:00pm (Course days 1-5)

FOR408: Windows Forensic Analysis
Chad Tilbury . . . . . LOCATION: Roman III

FOR508: Advanced Digital Forensics and Incident Response
Rob Lee . . . . . LOCATION: Roman IV

FOR518: Mac Forensic Analysis
Sarah Edwards . . . . . LOCATION: Octavius 13

FOR526: Memory Forensics In-Depth
Alissa Torres . . . . . LOCATION: Pompeian II

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

FOR578: Cyber Threat Intelligence
Jake Williams . . . . . LOCATION: Sorrento

FOR585: Advanced Smartphone Forensics
Heather Mahalik . . . . . LOCATION: Neopolitan II

COURSE SCHEDULE

FOR610: REM: Malware Analysis Tools and Techniques
Lenny Zeltser . . . . . .LOCATION: Octavius 1 I

MGT414: SANS Training Program for CISSP® Certification
Eric Conrad. . . . . LOCATION: Pompeian IV
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™
G. Mark Hardy . . . . . LOCATION: Milano IV
Extended Hours: 5:00pm - 6:00pm (Course days 1-4)

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

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

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

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

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

ICS410: ICS/SCADA Security Essentials
Eric Cornelius . . . . . LOCATION: Octavius 21/22

ICS515: ICS Active Defense and Incident Response
Robert M. Lee, Mark Bristow . . . . . .LOCATION: Octavius 23

START DATE: **Wednesday, September 14**
Time: 9:00am - 5:00pm

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

START DATE: **Thursday, September 15**

CORE NetWars Tournament
Jeff McJunkin . . . . . .LOCATION: Roman I/II
Hours: 6:30pm - 9:30pm

DFIR NetWars Tournament
Rob Lee, Chad Tilbury . . . . . LOCATION: Roman III/IV
Hours: 6:30pm - 9:30pm

START DATE: **Sunday, September 18**
Time: 9:00am - 5:00pm

MGT305: Technical Communication and Presentation Skills for Security Professionals
David Hoelzer. . . . . LOCATION: Salerno

HOSTED: Health Care Security Essentials
Greg Porter. . . . . LOCATION: Sorrento

PMP is registered mark of the Project Management Institute, Inc.

SPECIAL EVENTS

Enrich your SANS experience!

Morning, lunchtime, 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 11

SPECIAL EVENT

Registration Welcome Reception

Sunday, September 11 | 5:00pm - 7:00pm
Location: Promenade Foyer

Register early and network with your fellow students!

SANS@NIGHT

Securing Your Kids

Speaker: Lance Spitzner
Sunday, September 11 | 7:00pm - 8:00pm | Location: Milano V

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 steps you can take to protect them.

MONDAY, SEPTEMBER 12

SPECIAL EVENT

General Session – Welcome to SANS

Speaker: Bryan Simon
Monday, September 12 | 8:00am - 8:30am | Location: Florentine I/II

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 EVENTS

SPECIAL EVENT

Women's CONNECT Event

Monday, September 12 | 6:15pm - 7:15pm | Location: Genoa

Joins SANS and ISSA International Women In Security Special Interest Group (WIS SIG) as we partner with local association chapters and groups to foster an evening of connections, both by having their members attend and having group representatives on hand to discuss their group, its activities and benefits of membership.

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 as well as the various groups who will be featured at the event.

This reception is free of charge, but space is limited. Register at www.sans.org/event/network-security-2016/bonus-sessions

KEYNOTE

An Interactive Look at Cyber Crime and Today's Threat Landscape

Speakers: James Lyne & Stephen Sims
Monday, September 12 | 7:15pm - 9:15pm | Location: Roman I

Let's take a journey through the most common attack trends, malicious software, and techniques used by adversaries today. Cyber criminals closely monitor the landscape for changes, actively responding to these changes and remaining one step ahead of our efforts to maintain an acceptable level of security. It is critical for our defenders to keep up with these forever-changing techniques. Surprisingly, the success of cyber-criminals often depends on basic mistakes still made by users. Join James and Stephen as they energetically perform several demonstrations of exploiting both publicly and privately disclosed vulnerabilities involving applications such as Internet Explorer, Microsoft Office, and Skype.

SPECIAL EVENTS

TUESDAY, SEPTEMBER 13

SANS@NIGHT

GIAC Program Presentation

Speaker: Jeff Frisk

Tuesday, September 13 | 6:15pm - 7:15pm | Location: Florentine I

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. Join us for an informational presentation along with a Q and A session. We'll cover everything from why you should get certified, what testing looks like, how to keep certifications current and more. GIAC staff will be present to answer your questions before and after the presentation.

SANS@NIGHT

Naked and Afraid Starring Windows 10 Memory

Speaker: Alissa Torres

Tuesday, September 13 | 7:15pm - 8:15pm | Location: Florentine III

We are in a cybersecurity arms race with our PSR (Primitive Survival Rating) as incident responders hinge on our "surthrivability," that is, our ability to effectively and efficiently detect and contain malicious actors inside our environment. Better lean in and advance your memory forensics skills for what is expected to be the most rapidly adopted enterprise Windows version of all time. Find out what is new in Windows 10 memory management and how the memory forensic frameworks are keeping up. With a current adoption rate of 10% and growing, it is only a matter of time before this OS version will make up the majority of your digital forensics and incident response casework. This presentation will provide insight into the significant changes introduced with Windows 10 and how they will affect your investigative process.

SANS@NIGHT

Everything They Told Me About Security Was Wrong

Speaker: John Strand

Tuesday, September 13 | 7:15pm - 8:15pm | Location: Roman I

If you were to believe the vendors and the trade shows, you would think everything was OK with IT security. You would think AV works. You would think plug and play IDS was effective. You would think that Data Loss Prevention would prevent data loss. Why then is it that organizations with very large budgets and staff still get compromised in advanced and persistent ways? Something is very wrong in this industry. Let's talk about it.

SPECIAL EVENTS

SANS@NIGHT

Using an Open-Source Threat Model for Prioritized Defense

Speaker: James Tarala

Tuesday, September 13 | 7:15pm - 8:15pm | Location: Florentine II

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 actors, so why does every organization need to perform completely unique risk assessments and prioritize its 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. James Tarala will present a new, open, community-driven threat model that can be used by any industry to evaluate the risk it faces. Then he will show how to practically use this model to prioritize enterprise defense and map to existing compliance requirements. Whether you work for the Department of Defense or a mom-and-pop retailer, you will be able to use this model to specifically identify a prioritized defense for your organization.

STI MASTER'S DEGREE PRESENTATION

Automated Intrusion Detection and Response on AWS

Speaker: Teri Radichel, STI Master's Degree Candidate

Tuesday, September 13 | 7:15pm - 7:55pm | Location: Florentine I

IInitially companies thought moving to the cloud was not a secure option. Over time, companies are starting to believe that the benefits gained from cloud platforms outweigh the risk. In fact, some argue that AWS is a more secure environment when properly configured. Amazon Web Services provides built-in inventory, logging, and tools that facilitate automated response to events. By monitoring network logs and detecting unwanted behavior, an event can trigger an automated backup of a misbehaving host followed by termination of the host and instantiation of a new one with a clean configuration stored in a source control system. Come hear an overview of AWS networking and resources. See a demonstration of automated intrusion detection response using source code you can run yourself with little or no knowledge of AWS.

SPECIAL EVENTS

SANS@NIGHT

CISO Success Strategies

Speaker: Frank Kim

Tuesday, September 13 | 8:15pm - 9:15pm | Location: Roman I

The increased importance and visibility of cybersecurity as a vital component of business growth make it critical that security leaders understand how to connect with senior executives and business leaders. Join Frank Kim, seasoned security leader and CISO, as he explains three things that will make you a more effective security business leader.

SANS@NIGHT

How to Commit Card Fraud

Speaker: G. Mark Hardy

Tuesday, September 13 | 8:15pm - 9:15pm | Location: Florentine I

Well, we're not going to show you how to commit fraud, but we will show you how the bad guys do it and how you can protect yourself and your business. We'll take a look into the "dark web" and see how these big card heists are pulled off, why chip-and-pin won't solve the fraud problem, and why payment technologies like Apple Pay pose new risks. You'll learn the ecosystem of fraud, and how it's become a big business that costs banks and merchants over $16 billion annually. We'll have a mag stripe card reader so you can really see what's in your wallet.

SANS@NIGHT

Security Awareness: Understanding and Managing Your Top Seven Human Risks

Speaker: Lance Spitzner

Tuesday, September 13 | 8:15pm - 9:15pm | Location: Florentine II

A key step to managing your human risk is first identifying and then prioritizing those risks and then focusing on the top ones. After working with hundreds of organizations, Lance Spitzner will discuss what are the seven most common human risks he finds in organizations and what you can do to effectively manage and measure those specific risks. Key points you will learn include:

- Concepts of "cognitive overload" and how every behavior has a cost
- Key elements in a human risk analysis
- Determining the key behaviors that will mitigate your top human risks
- How to effectively communicate and measure those behaviors

SPECIAL EVENTS

WEDNESDAY, SEPTEMBER 14

SPECIAL EVENT

SANS Pen Test Reception

Wednesday, September 14 | 6:00pm - 7:00pm | Location: Florentine IV

Please join Ed Skoudis, SANS pen test instructors, and your fellow pen test students for a reception on Wednesday, September 14 from 6pm until 7pm for a chance to network together and the possibility to win some cool prizes. This is open to all SANS students who have taken or are currently taking a SANS pen test course or are interested in taking a pen test course in the future.

SANS@NIGHT

Quality Not Quantity: Continuous Monitoring's Deadliest Events

Speaker: Eric Conrad

Wednesday, September 14 | 7:15pm - 8:15pm | Location: Florentine III

Most Security Operations Centers (SOCs) are built for compliance, not security. One well-known retail firm suffered the theft of over a million credit cards, and 60,000 true positive events were reported to its SOC during that missed breach, but they were lost in the noise of millions. If you are bragging about how many events your SOC handles each day, you are doing it wrong. During this talk, we will show you how to focus on quality instead of quantity, and provide an actionable list of the deadliest events that occur during virtually every successful breach.

SANS@NIGHT

Running Away from Security: Web App Vulnerabilities and OSINT Collide

Speaker: Micah Hoffman

Wednesday, September 14 | 7:15pm - 8:15pm | Location: Florentine II

Lately it seems like more and more of our lives are being sucked into the computer world. There are wrist sensors for tracking our steps, phone apps that plot our workouts on maps, and sites to share our healthy eating and weight-loss progress. When people sign up for these sites, they usually use pseudonyms or the sites give them a unique numbered ID to keep their information "private." How hard would it be to connect a person's step counting, diet history, and other info on these health sites to their real lives? Are businesses using these sites for non-fitness purposes? This talk will show weaknesses in several web applications used for health and exercise tracking and reveal (spoiler alert) how trivial it is to find the real people behind the "private" accounts.

SPECIAL EVENTS

SANS@NIGHT

Smartphone and Network Forensics Goes Together Like Peas and Carrots

Speaker: Heather Mahalik and Phil Hagen

Wednesday, September 14 | 7:15pm - 8:15pm | Location: Florentine I

There are strong ties between the smartphone and network aspects of the forensics process. In this talk, Heather Mahalik will address the smartphone side of this investigative coin and Phil Hagen will look at things from the network side. As often identified in the forensics process, a comprehensive approach is necessary to conduct a thorough investigation.

STI MASTER'S DEGREE PRESENTATION

Sleeping Your Way Out of the Sandbox

Speaker: Hassan Mourad, STI Master's Degree Candidate

Wednesday, September 14 | 7:15pm - 7:55pm | Location: Milano III

With over a million new malware samples per day, traditional signature-base detection is failing to catch up. This created a huge demand on the security industry to offer unconventional ways to address the rising threat. One of the offered solutions was file-based sandboxing. Sandboxes were marketed as the solution for solving your malware problems, yet it is becoming trivial to evade sandbox detection. In this presentation, we will discuss several ways to evade sandboxes and introduce a couple of new techniques. Our goal is to figure out if, where, and how the sandbox can fit in your overall security defense and how the currently offered solutions can be enhanced to add real value to your defense strategy.

SANS@NIGHT

The Control Things Platform and its Little Minion

Speaker: Justin Searle

Wednesday, September 14 | 8:15pm - 9:15pm | Location: Florentine II

SamuraiSTFU was a great start to help electric utilities do penetration testing of their DCS and SCADA networks, but it just wasn't enough. SamuraiSTFU has expanded its goals to include all control systems and IoT devices, thus requiring a name change and a complete rebuild of the pentest distribution. Come check out the new Control Things Platform and its new open-source hardware companion, the Control Things Minion!

SPECIAL EVENTS

SANS@NIGHT

Analyzing the Cyber Attack on the Ukrainian Power Grid

Speaker: Robert M. Lee

Wednesday, September 14 | 8:15pm - 9:15pm | Location: Florentine I

On December 23, 2015 a cyber attack caused a power outage that affected 230,000 people in Ukraine. The SANS Industrial Control Systems team immediately began investigating and reporting on the case. In this presentation the attack will be broken down with lessons learned and takeaways for organizations to secure their infrastructure.

SANS@NIGHT

The iOS of Sauron: How iOS Tracks Everything You Do

Speaker: Sarah Edwards

Wednesday, September 14 | 8:15pm - 9:15pm | Location: Florentine III

iOS devices have the ability to track everything the user does – how many steps the user takes, where the user has been, and keeps track of how they use their devices. This presentation will dive into some of the protected files that keep track of every detail of a user's life that iOS tracks. These databases and files can be used to correlate user activity down to the smallest detail. Methods of analysis as well as some scripts will be shown to help analyze these files.

THURSDAY, SEPTEMBER 15

LUNCH & LEARN

How to Become a SANS Instructor

Speaker: Eric Conrad

Thursday, September 15 | 12:30pm - 1:15pm | Location: Pompeian IV

Have you ever wondered what it takes to become a SANS instructor? How does your SANS instructor rise to the top and demonstrate the talents to become part of the SANS faculty? Attend this session and learn how to become part of the faculty and learn the steps to make that goal a reality. SANS Principal instructor Eric Conrad will share his experiences and show you how to become part of the SANS top-rated instructor team.

This presentation is free of charge, but space is limited to the first 40 registrations. Please register using the bulletin board for lunch and learn sign ups.

SPECIAL EVENTS

SANS@NIGHT

Digital Investigations: Leveraging the Multitude of Records

Speaker: Ben Wright

Thursday, September 15 | 7:15pm - 8:15pm | Location: Florentine I

Owing to advancing technologies like the cloud, smartphones, and the Internet of Things, the quantity of records relevant to any official investigation is expanding beyond imagination. There are SO MANY records in SO MANY places – emails, texts, photos, metadata, backups, social media, travel histories, deleted stuff – that traditional assumptions on how to advance an investigation or resolve a dispute have become obsolete. Today smart investigation teams are able to leverage the massive volume of records in new and surprising ways. The team does not necessarily need access to records in order to take advantage of their existence. This presentation teaches tips and strategies and tells war stories that simply were not applicable 10 years ago. These lessons help investigators and their employers reach more favorable outcomes in Human Resource disputes, potential lawsuits, forensic audits, regulatory inquiries, criminal proceedings and corporate espionage cases.

SANS@NIGHT

Debunking the Complex Password Myth

Speaker: Keith Palmgren

Thursday, September 15 | 7:15pm - 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

Inside the Defender's Sanctum

Speaker: Derek Harp

Thursday, September 15 | 8:15pm - 9:15pm | Location: Florentine III

Join host Derek Harp for a chat with security researcher and industry veteran Eric Cornelius on the highs and lows of protecting systems from malicious actors and human error alike. Learn what keeps this long-time defender moving forward in the face of an ever-changing threat landscape.

SPECIAL EVENTS

CORE NETWARS EXPERIENCE

Hosted by Jeff McJunkin

Thursday, September 15 and Friday, September 16

6:30pm - 9:30pm | Roman I & II

CORE NetWars Experience is a computer and network security challenge designed to test a participant's experience and skills in a safe environment. It is accessible to a broad level of player skill ranges and is split into separate levels so that advanced players may quickly move through earlier levels to the level of their expertise.

(FREE with any 4-6 Day SANS Course Registration)

DFIR NETWARS TOURNAMENT

Hosted by Rob Lee & Chad Tilbury

Thursday, September 15 and Friday, September 16

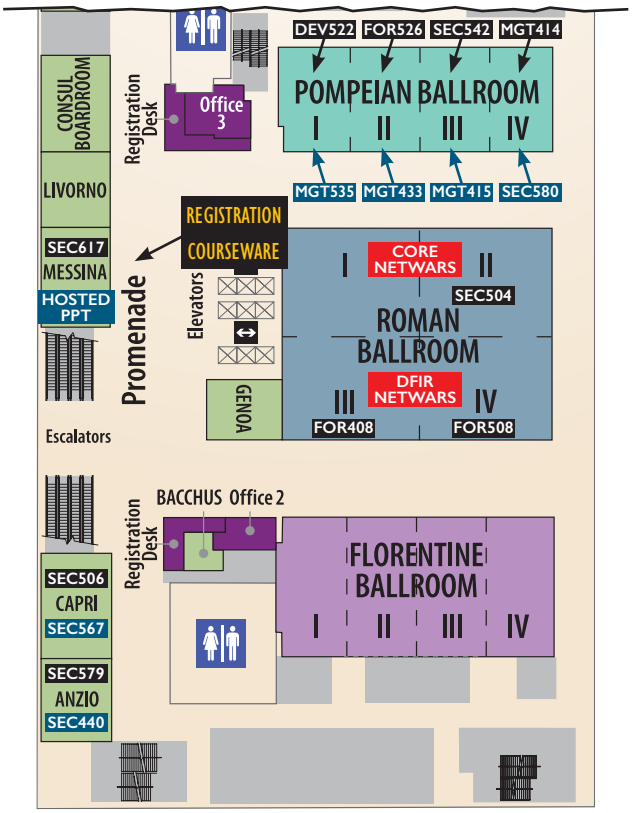
6:30pm - 9:30pm | Roman III & IV

DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges, for individual or team-based "firefights." It is developed by incident responders and forensic analysts who use these skills daily to stop data breaches and solve complex crimes. DFIR NetWars Tournament allows each player to progress through multiple skill levels of increasing difficulty, learning first-hand how to solve key challenges they might experience during a serious incident. DFIR NetWars Tournament enables players to learn and sharpen new skills prior to being involved in a real incident.

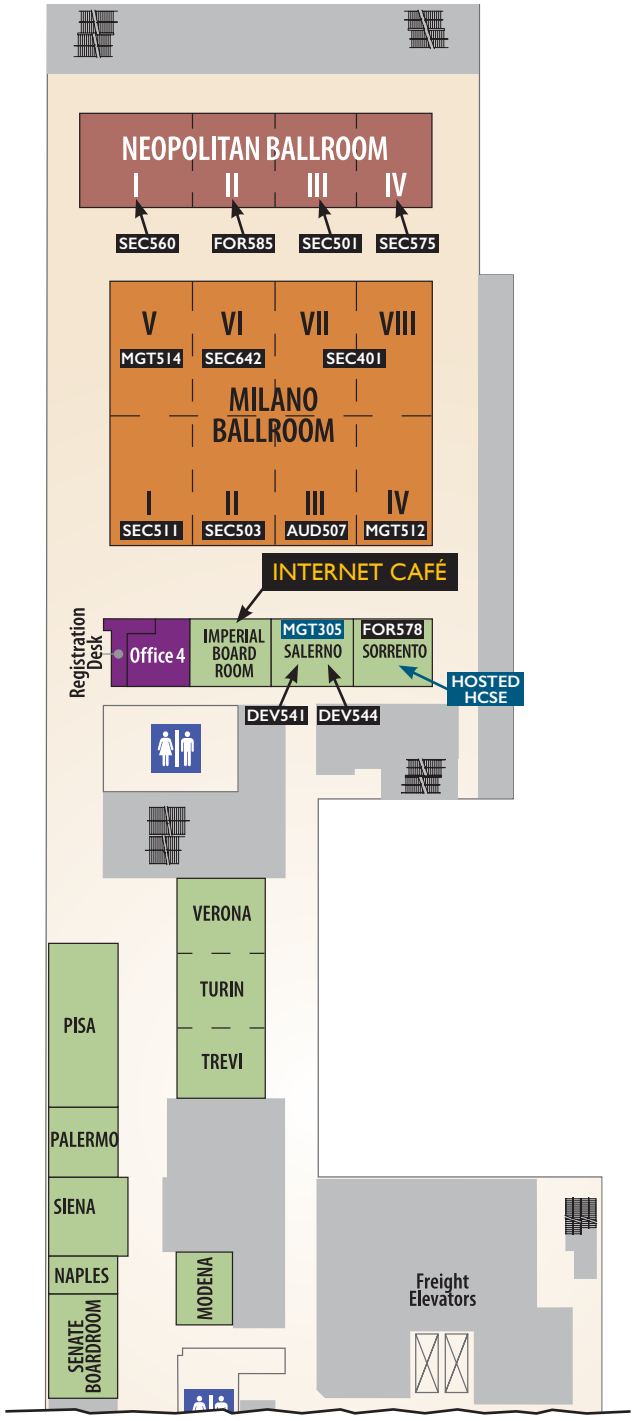
(FREE with any 4-6 Day SANS Course Registration)

PROMENADE SOUTH

PROMENADE LEVEL (CONTINUED)



PROMENADE LEVEL



VENDOR EVENTS

Vendor Solutions Expo

Wednesday, September 14 | 12:00pm-1:30pm | 5:30pm - 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

Wednesday, September 14 | 5:30pm-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

Wednesday, September 14 | 12:00pm-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:

A10 Networks	Datacom Systems	Qualys
Anomali	Drawbridge Networks	Sift Security
Bradford Networks	Forescout Technologies	Sophos
BugCrowd	InfoArmor	ThreatQuotient
Centrify	Kaspersky	Tripwire
CrossMatch	Leidos	VSS Monitoring
Cyberbit	LightCyber	Watchguard
Cylance	LogRhythm	WireX
	PwnieExpress	

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
LUNCH AND LEARN

Supporting CIS Critical Security Controls with ForeScout

Speaker: Sandeep Kumar, Director Product Marketing
Tuesday, September 13 | 12:30pm-1:15pm | Location: Pompeian III

The Center for Internet Security has defined required controls for effective cyber defense (CIS Critical Security Controls). How do they relate to your security initiatives, and why is endpoint security and control such a major focal point of SANS security? Join ForeScout Director, Product Marketing, Sandeep Kumar, as he discusses how ForeScout CounterACT® can help you create an effective cyber defense system. Discover how agentless cybersecurity technology and ForeScout's See, Control and Orchestrate solution can accelerate this process

leidos
LUNCH AND LEARN

Metadata Matters

Speaker: Kurt Silberberg, Cyber Intel Analyst, Leidos Cyber
Tuesday, September 13 | 12:30pm-1:15pm | Location: Pompeian I

Today's networks create an abundance of data – this can be good and bad for security analysts. More data gives defenders more visibility and more opportunities to detect malicious traffic. However, an avalanche of data can be overwhelming to analyze and costly to store. This talk will demonstrate how email metadata can be collected and leveraged to better defend the enterprise.

VENDOR EVENTS

Centrify

LUNCH AND LEARN

Stepwise Security: A Planned Path to Reducing Risk

Speaker: Chris Webber, Security Strategist

Tuesday, September 13 | 12:30pm-1:15pm | Location: Pompeian IV

Attackers are making major headway into our businesses with simple tactics that exploit our weakest points. It's clear that we need to bolster our defenses, but prioritization can seem daunting. Join Chris Webber, Security Strategist form Centrify, as he walks through some proven practices for prioritizing a risk mitigation strategy, starting with the easy gaps that most often lead to data breach, and moving to sophisticated and comprehensive control.

SOPHOS

LUNCH AND LEARN

Solving Today's Top Problems with Firewalls

Speaker: Ofer Elzam, Director of Product Management, Sophos

Tuesday, September 13 | 12:30pm-1:15pm | Location: Pompeian II

Advanced attacks are more coordinated than ever before – your defenses can be too. Join Ofer Elzam, Sophos' Director of Product Management, to learn how web filtering can provide quick and easy business application protection, instant and automatic incident response, and simple and affordable sandboxing protection.

CYLANCE

LUNCH AND LEARN

Beyond IOCs: Pragmatic Attacker Identification

Speaker: Eric Cornelius, Consulting Director, ICS

Tuesday, September 13 | 12:30pm-1:15pm | Location: Neopolitan III

This talk will focus on fundamental attacker techniques that are common among many sophisticated threat actors and the techniques that can be used to detect them without the need for IOCs.

VENDOR EVENTS

QUALYS® CONTINUOUS SECURITY

LUNCH AND LEARN

Keep Calm and Prioritize: Five Requirements for Streamlining Vulnerability Remediation

Speaker: Jimmy Graham, Director of Product Management, AssetView and ThreatPROTECT

Thursday, September 15 | 12:30pm-1:15pm | Location: Neopolitan II

In this presentation, you'll learn the five key elements for successfully prioritizing vulnerability remediation, then learn best practices for using tools that allow you to take full control of evolving threats by correlating active threats against your vulnerabilities, so you know which vulnerabilities to remediate first.

ANOMALI™

LUNCH AND LEARN

Fraud Threat Detection

Speaker: Kris Palmer, Senior Security Engineer

Thursday, September 15 | 12:30pm-1:15pm | Location: Neopolitan III

In this discussion, we will talk about fraud in efforts to use threat intelligence solutions for detection, automation and analyzing fraudulent observables in centralized arena for defense practices. We will also talk about understanding the threats and where tomorrow leads in effective threat detection capabilities for fraud based attacks.

wirex

LUNCH AND LEARN

Network Forensics as a Key Element in Intelligence-Driven SOC Journey

Speakers: Uriel Cohen, Director of Products,WireX Systems and Ondrej Krehel, CEO and Founder, LIFARS LLC

Thursday, September 15 | 12:30pm-1:15pm | Location: Milano V

We've seen many innovations to improve threat detection and alert prioritization, but the SOC's true bottleneck still resides in the manual process of performing actual investigations. What are your current forensics limitations and how can you overcome it? Join us to discuss.

VENDOR EVENTS

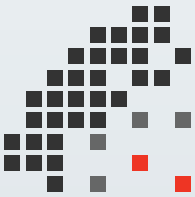
bugcrowd

LUNCH AND LEARN

If You Can't Beat 'Em, Join 'Em

Speaker: Grant McCracken, Application Security Engineer
Thursday, September 15 | 12:30pm-1:15pm | Location: Pompeian 1

Having a bug bounty program is one of the most efficient methods of finding security vulnerabilities today. But, as anyone who has tried to run a bug bounty program knows, it's not a trivial undertaking. As professionals who have helped to manage hundreds of bug bounty programs, we're uniquely positioned to provide advice on how to succeed. Whether you're already running a bug bounty program, are looking to run a bug bounty program, or are a researcher, this talk aims to deepen your knowledge of the subject.



SIFTSECURITY

LUNCH AND LEARN

Leveraging Graph Analytics for Incident Response and Threat Hunting

Speaker: Colin Estep, Chief Security Officer
Friday, September 16 | 12:30pm-1:15pm | Location: Pompeian 1

Modern security teams are not only reacting to known incidents, but must also actively hunt for adversaries that have already compromised defenses. Whether you're a SOC analyst, Incident Responder, or Threat Hunter, you must have the right tools to discover malicious activity on infrastructure that's constantly changing within your enterprise.

Future SANS Training Events

SANS **Security Leadership** SUMMIT & TRAINING 2016
Dallas, TX | Sep 27 - Oct 4 | #SANSSecLeadership

SANS **Seattle** 2016
Seattle, WA | Oct 3-8 | #SANSSeattle

SANS **Baltimore** 2016
Baltimore, MD | Oct 10-15 | #SANSBaltimore

SANS **Tysons Corner** 2016
Tysons Corner, VA | Oct 22-29 | #SANSTysons

SANS **San Diego** 2016
San Diego, CA | Oct 19-24 | #SANSSanDiego

SANS **Pen Test HackFest** SUMMIT & TRAINING 2016
Crystal City, VA | Nov 2-9 | #HackFestSummit

SANS **Miami** 2016
Miami, FL | Nov 7-12 | #SANSMiami

SANS **Healthcare CyberSecurity** SUMMIT & TRAINING 2016
Houston, TX | Nov 14-21 | #SANSHealthcareSummit

SANS **San Francisco** 2016
San Francisco, CA | Nov 27 - Dec 2 | #SANSSanFran

SANS **Cyber Defense Initiative** 2016
Washington DC | Dec 10-17 | #SANSCDI

SANS **Security East** 2017
New Orleans, LA | Jan 9-14 | #SANSSecurityEast

SANS **Las Vegas** 2017
Las Vegas, NV | Jan 23-28 | #SANSLasVegas

SANS **Cyber Threat Intelligence** SUMMIT & TRAINING 2017
Arlington, VA | Jan 25 - Feb 1 | #CTISummit

SANS Southern California – **Anaheim** 2017
Anaheim, CA | Feb 6-11 | #SANSAnaheim

SANS **Scottsdale** 2017
Scottsdale, AZ | Feb 20-25 | #SANSScottsdale

SANS **Dallas** 2017
Dallas, TX | Feb 27 - Mar 4 | #SANSDallas

SANS **San Jose** 2017
San Jose, CA | Mar 6-11 | #SANSSanJose

SANS **Tysons Corner Spring** 2017
Tysons Corner, VA | Mar 20-25 | #SANSTysons

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

Mark Your Calendar for Next Year's

SANS Network Security 2017

Save the Date!

September 9-18, 2017

LOCATION:

Caesars Palace – Las Vegas, NV