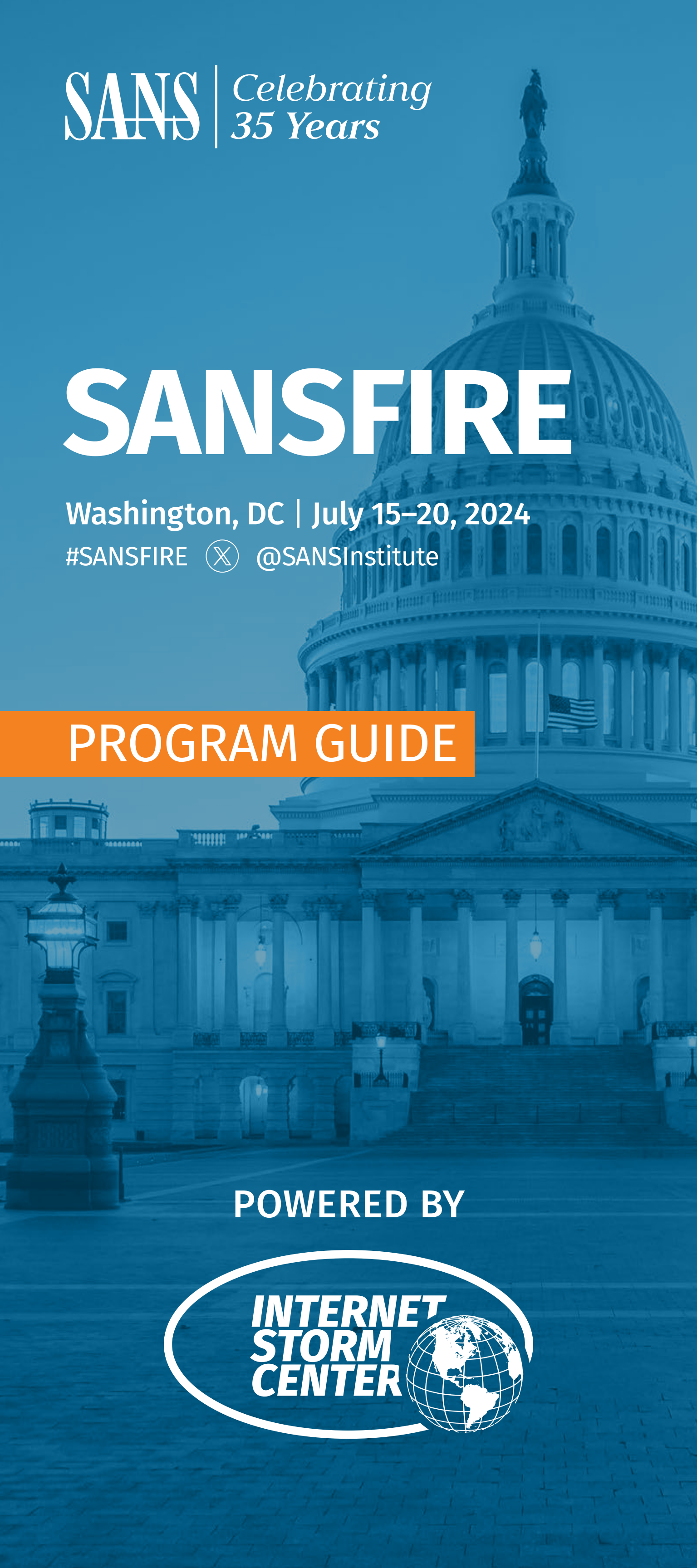
SANS | *Celebrating 35 Years*



SANSFIRE

Washington, DC | July 15–20, 2024

#SANSFIRE 𝕏 @SANSInstitute

PROGRAM GUIDE

POWERED BY

INTERNET STORM CENTER

SANSFIRE 2024

Welcome Reception

Monday, July 15 | 6:30–8:00 PM

LOCATION: **McClellan's Sports Bar & Patio** (LOBBY LEVEL)

Kick off your SANSFIRE 2024 experience at the Welcome Reception! Be part of this kickoff event and join the industry's most powerful gathering of cybersecurity professionals. Share stories, make connections, and learn how to make the most of your week in Washington, DC. Come join your instructors and fellow students for a fun, relaxed evening. Beverages (adult and otherwise) and small bites will be included.

SANS

CYBER RANGES

Develop and practice real-world skills
to be prepared to defend your environment.

NETWARS
CORE

Thursday, July 18 & Friday, July 19
6:30–9:30 PM | International Ballroom Center (CONCOURSE LEVEL)

NETWARS
CYBER DEFENSE

Thursday, July 18 & Friday, July 19
7:15–10:15 PM | International Ballroom East (CONCOURSE LEVEL)

All In-Person students who registered to attend a course at SANSFIRE 2024 are eligible to play NetWars for FREE.

Space is limited. Please register for NetWars through your SANS Account Dashboard.

Extend Your Training

SANS OnDemand

Add an OnDemand Bundle to your course.

Extend Your Training Experience with an OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter-expert support to help you increase your retention of course material

OnDemand Bundle price: $979

sans.org/ondemand/bundles

Validate Your Training

GIAC CERTIFICATIONS

Add a GIAC Certification attempt to your course.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt

GIAC Certifications Bundle price: $979

giac.org

GENERAL INFORMATION

Venue

Washington Hilton
1919 Connecticut Avenue N.W.
Washington D.C. 20009
Phone: 202-483-3000

Event Check-In | Badge & Courseware Distribution

LOCATION: Terrace Foyer (TERRACE LEVEL)

Sunday, July 14	4:00–6:00 PM
Monday, July 15	7:00–8:30 AM

Registration Support

LOCATION: International Terrace (TERRACE LEVEL)

Monday, July 15	7:00 AM–5:30 PM

Location: Albright Room (TERRACE LEVEL)

Tuesday, July 16–Friday, July 19	8:00 AM–5:30 PM
Saturday, July 20	8:00 AM–2:00 PM

Course Breaks

Morning Coffee	7:00–9:00 AM
Morning Break*	10:30–10:50 AM
Lunch (ON YOUR OWN)	12:15–1:30 PM
Afternoon Break*	3:00–3:20 PM

*Snack and coffee to be provided during these break times.

Parking

Self-parking is available at the prevailing rate of $56/day at the Washington Hilton. SANS does not have a negotiated parking discount with this venue.*

*Parking rates are subject to change.

Photography Notice

SANS may take photos of classroom activities for marketing purposes. SANSFIRE 2024 attendees grant SANS all rights for such use without compensation, unless prohibited by law.

Feedback Forms and Course Evaluations

SANS is committed to offering the best information security training, and that means continuous course improvement. Your student feedback is a critical input to our course development and improvement efforts. Please take a moment to complete the electronic evaluation posted in your class Slack channel each day.

Wear Your Badge

To confirm you are in the right place, SANS Work-Study participants 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)

LDR414:	SANS Training Program for CISSP® Certification
SEC401:	Security Essentials: Network, Endpoint, and Cloud
SEC540:	Cloud Security and DevSecOps Automation
SEC660:	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
SEC670:	Red Teaming Tools – Developing Windows Implants, Shellcode, Command and Control

Extended Hours:

SEC504:	Hacker Tools, Techniques, and Incident Handling

COURSE SCHEDULE

Time: 9:00 AM–5:00 PM (Unless otherwise noted)
NOTE: All classes begin at 8:30 AM on Day 1 (Monday, July 15)

FOR500: Windows Forensic Analysis (6-DAY COURSE)
Ovie Carroll . . . . Homestead East (LOBBY LEVEL)

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics (6-DAY COURSE)
Carlos Cajigas . . . . Columbia Hall 7 (TERRACE LEVEL)

FOR509: Enterprise Cloud Forensics & Incident Response (6-DAY COURSE)
Terrence Williams. . . . . Columbia Hall 5 (TERRACE LEVEL)

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (6-DAY COURSE)
Philip Hagen . . . . Oak Lawn (LOBBY LEVEL)

FOR578: Cyber Threat Intelligence (6-DAY COURSE)
Peter Szczepankiewicz. . . . . Columbia Hall 11 (TERRACE LEVEL)

FOR585: Smartphone Forensic Analysis In-Depth (6-DAY COURSE)
Domenica Crognale . . . . Holmead West (LOBBY LEVEL)

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques (6-DAY COURSE)
Xavier Mertens . . . . Columbia Hall 2 (TERRACE LEVEL)

ICS410: ICS/SCADA Security Essentials (6-DAY COURSE)
Justin Searle . . . . Int'l Ballroom Center (CONCOURSE LEVEL)

LDR414: SANS Training Program for CISSP® Certification (6-DAY COURSE)
Seth Misenar . . . . Columbia Hall 4 (TERRACE LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 8:00 AM–7:00 PM (Days 2–5)
8:00 AM–5:00 PM (Day 6)

LDR512: Security Leadership Essentials for Managers (5-DAY COURSE)
Frank Kim. . . . . Georgetown East (CONCOURSE LEVEL)

LDR514: Security Strategic Planning, Policy & Leadership (5-DAY COURSE)
Kim Jones. . . . . Georgetown West (CONCOURSE LEVEL)

LDR520: Cloud Security for Leaders (5-DAY COURSE)
Jason Lam . . . . Lincoln East (CONCOURSE LEVEL)

LDR553: Cyber Incident Management (5-DAY COURSE)
Steve Armstrong-Godwin . . . . Jefferson East (CONCOURSE LEVEL)

SEC301: Introduction to Cyber Security (5-DAY COURSE)
Doc Blackburn. . . . . Lincoln West (CONCOURSE LEVEL)

SEC401: Security Essentials: Network, Endpoint & Cloud (6-DAY COURSE)
Ross Bergman . . . . Columbia Hall 3 (TERRACE LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

SEC450: Blue Team Fundamentals: Security Operations and Analysis (6-DAY COURSE)
John Hubbard . . . . Gunston East (TERRACE LEVEL)

SEC488: Cloud Security Essentials (6-DAY COURSE)
Serge Borso . . . . Columbia Hall 8 (TERRACE LEVEL)

SEC497: Practical Open-Source Intelligence (OSINT) (6-DAY COURSE)
Jeff Lomas . . . . Columbia Hall 1 (TERRACE LEVEL)

SEC504: Hacker Tools, Techniques & Incident Handling (6-DAY COURSE)
Mick Douglas . . . . Int'l Ballroom West (CONCOURSE LEVEL)
Hours: 8:30 AM–7:15 PM (Day 1)

SEC530: Defensible Security Architecture & Engineering: Implementing Zero Trust for the Hybrid Enterprise (6-DAY COURSE)
Ismael Valenzuela. . . . . Columbia Hall 6 (TERRACE LEVEL)

SEC540: Cloud Security & DevSecOps Automation (5-DAY COURSE)
Eric Johnson. . . . . Morgan (CONCOURSE LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–4)

SEC541: Cloud Security Attacker Techniques, Monitoring, and Threat Detection (5-DAY COURSE)
Shaun McCullough . . . . Jefferson West (CONCOURSE LEVEL)

SEC542: Web App Penetration Testing and Ethical Hacking (6-DAY COURSE)
Bojan Zdrnja. . . . . Jay (LOBBY LEVEL)

SEC549: Cloud Security Architecture (5-DAY COURSE)
David Hazar & Simon Vernon . . . . Gunston West (TERRACE LEVEL)

SEC560: Enterprise Penetration Testing (6-DAY COURSE)
Jon Gorenflo . . . . Int'l Ballroom East (CONCOURSE LEVEL)

SEC565: Red Team Operations & Adversary Emulation (6-DAY COURSE)
David Mayer . . . . Columbia Hall 10 (TERRACE LEVEL)

SEC566: Implementing and Auditing CIS Controls (5-DAY COURSE)
Brian Ventura. . . . . Piscataway (LOBBY LEVEL)

SEC568: Product Security Penetration Testing – Safeguarding Supply Chains and Managing Third-Party Risk (5-DAY COURSE)
Douglas McKee . . . . Fairchild East (TERRACE LEVEL)

SEC588: Cloud Penetration Testing (6-DAY COURSE)
Aaron Cure . . . . Columbia Hall 9 (TERRACE LEVEL)

SEC595: Applied Data Science & AI/Machine Learning for Cybersecurity Professionals (6-DAY COURSE)
David Hoelzer . . . . Kalorama (LOBBY LEVEL)

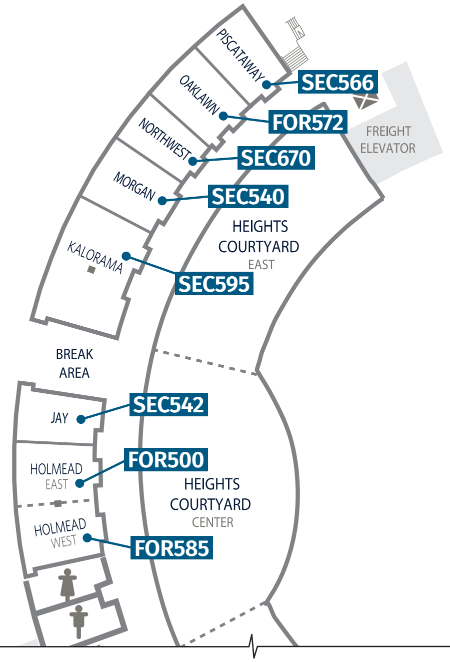
SEC617: Wireless Penetration Testing & Ethical Hacking (6-DAY COURSE)
James Leyte-Vidal. . . . . Columbia Hall 12 (TERRACE LEVEL)

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking (6-DAY COURSE)
Brandon McCrillis . . . . Fairchild West (TERRACE LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

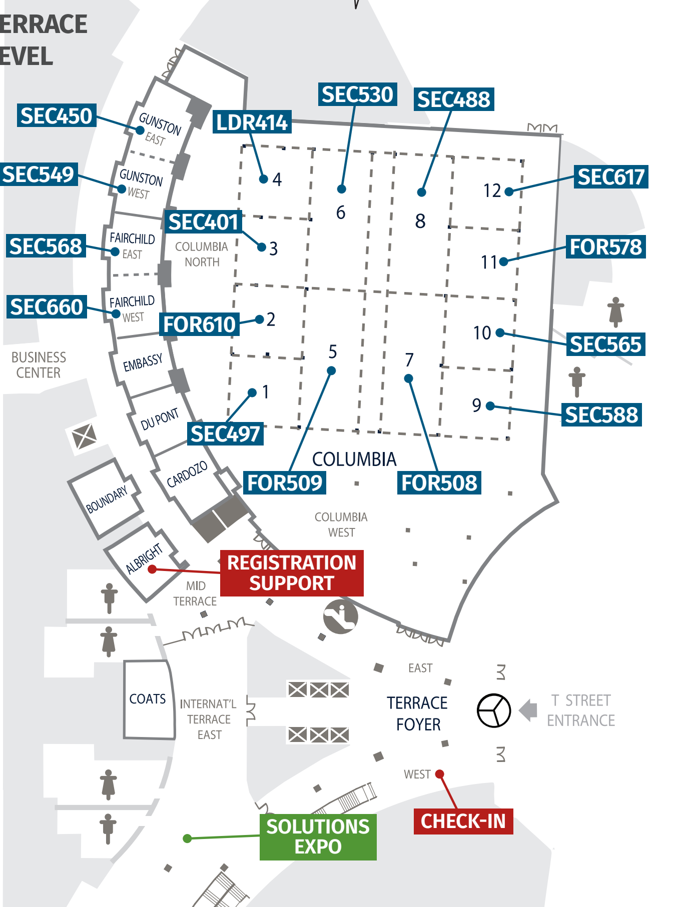
SEC670: Red Teaming Tools – Developing Windows Implants, Shellcode, Command, and Control (6-DAY COURSE)
Jonathan Reiter. . . . . Northwest (LOBBY LEVEL)
Hours: 8:30 AM–7:00 PM (Day 1); 9:00 AM–7:00 PM (Days 2–5)

HOTEL FLOOR PLAN

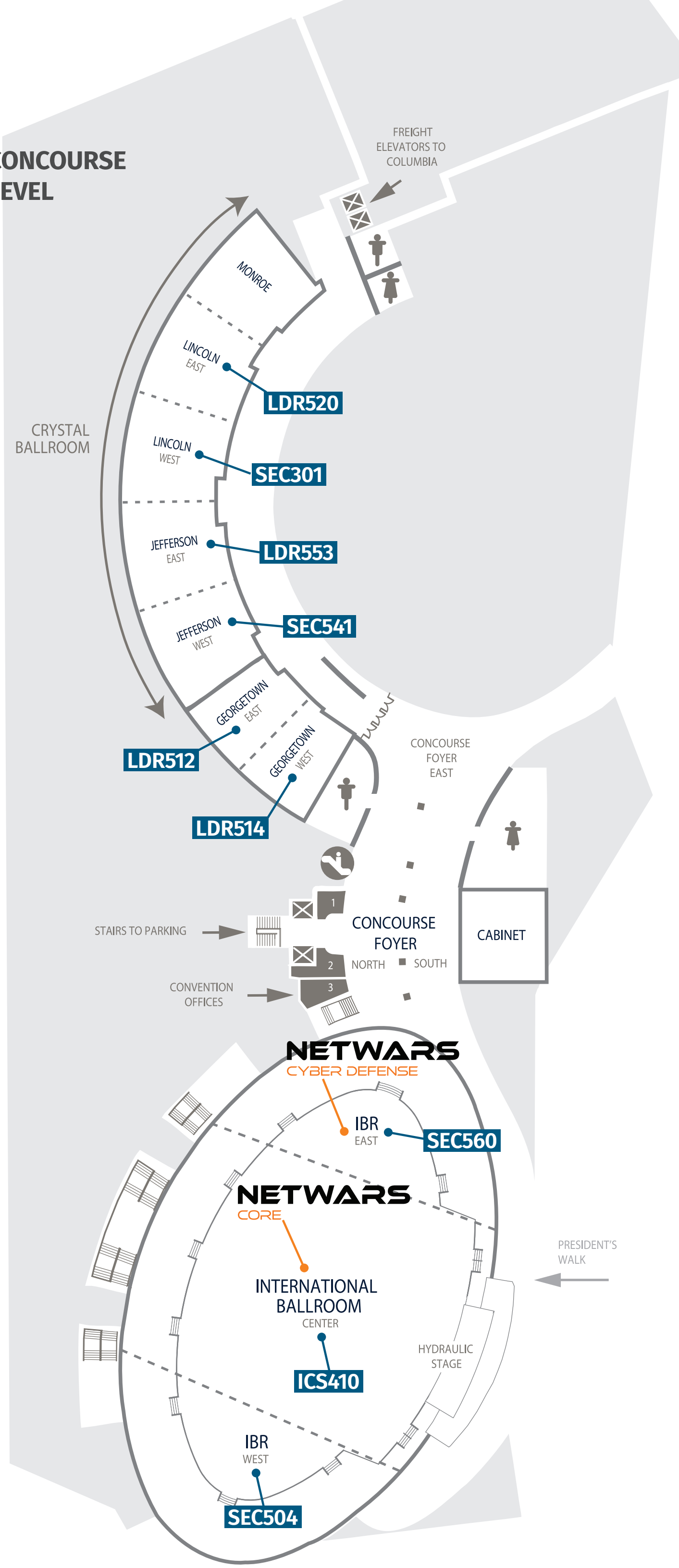
LOBBY LEVEL



TERRACE LEVEL



CONCOURSE LEVEL



Enrich Your SANS Experience!

Talks 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.

RECEPTION

SANSFIRE 2024 Welcome Reception

Monday, July 15 | 6:30–8:00 PM

LOCATION: **McClellan's Sports Bar & Patio** (LOBBY LEVEL)

Kick off your SANSFIRE 2024 experience at the Welcome Reception. Be part of this kickoff event and join the industry's most powerful gathering of cybersecurity professionals. Share stories, make connections, and learn how to make the most out of your training this week in Washington, DC. Beverages (adult and otherwise) and bites will be served. Hope to see you there!

RECEPTION

Women's Connect Reception

Tuesday, July 16 | 5:30–7:00 PM

LOCATION: **International Ballroom East** (CONCOURSE LEVEL)

SANS Institute's Women's Connect community is happy to host a networking reception at SANSFIRE to foster interaction and career advancement for women throughout cybersecurity and beyond. Please join us to build your network of women in the industry and celebrate the mission of SANS to foster diversity in cybersecurity.

SPONSORSHIP EVENT

Sponsorship Expo – Breakfast and Lunch

Wednesday, July 17 | 7:30–9:00 AM | 12:15–1:30 PM

LOCATION: **International Terrace** (TERRACE LEVEL)

Join our sponsoring exhibitors and fellow attendees for free breakfast and lunch while you become familiar with solutions and services that showcase the leading options in information security. Take time to browse the expo floor and get introduced to providers and their solutions challenges that align with security challenges being discussed in class.

KEYNOTE

25 Years of the Internet Storm Center: Time Traveling Through Sensor Data

Tuesday, July 16 | 6:30–8:00 PM

LOCATION: **Int'l Ballroom Center** (CONCOURSE LEVEL)

SPEAKER: **Dr. Johannes Ullrich, SANS Fellow**

Some of you may remember Y2K. But did you know that it sparked what is now the Internet Storm Center? Travel along and follow me through time to see how attacks, actors, and victims have changed over a quarter of a century. Did you know that GIAC wasn't a certification at all back in the day? Have you heard of "Leaves," "Code Red," and "Nimda?" We will look at data showing how the survival time of a system connected to the internet has changed. How did Windows XP SP2 drastically change the attack landscape, and how did our sensor configurations change over the years in response? But this isn't just "story time." This is about lessons learned and projecting the future: How will you be able to survive the next wave? What would I tell "young Johannes" if I could actually go back in time? Find out the answers to all of these questions and be entertained by, yes, some stories (I will leave it up to you to decide if they are good or bad stories).

BONUS SESSIONS

RECEPTION

SANSFIRE 2024 AlumNight: Powered by DFIR + Cybersecurity Leadership

Wednesday, July 17 | 5:30–6:30 PM
LOCATION: **Columbia Foyer** (TERRACE LEVEL)

Once a SANS Alumni, Always a SANS Alumni

Embark on your cybersecurity journey and make it unforgettable! Whether it's your first SANS event or you're returning for the fourth time, join us for the industry's premier gathering of cybersecurity professionals. Experience an electrifying celebration where networking, food, drinks, giveaways, and dynamic expert discussions converge. Connect with fellow SANS Alumni and Instructors, creating a vibrant atmosphere that unites both in-person students and local community experts. This is more than an event; it's an immersive experience that fuels your passion for cybersecurity and fosters invaluable connections.

HANDS-ON WORKSHOP

The SANS Internet Storm Center: How to Use it and How to Contribute, Followed by a Honeypot Workshop

Wednesday, July 17 | 6:30–8:30 PM
LOCATION: **International Ballroom East** (CONCOURSE LEVEL)
SPEAKERS: **Guy Bruneau, ISC Handler & Jesse La Grew, ISC Handler**

The Internet Storm Center has been collecting data for over two decades now. This data has always been available for free direct from our website. In this presentation you will learn how to use our various data feeds, and how to responsibly integrate them into your security operations to get the best value from these feeds. We will also show how to set up your own sensor, how to manage it, and how to learn more about attacks targeting your own network.

This event will be followed by our "Honeypot Workshop". During the workshop you will gain hands-on experience with our honeypot. You may bring your own device, but we will also give away a number of free devices to take home with you. The workshop part will only be available to students attending the prior talk in person.

ALUMNIGHT WORKSHOP OPTION 1

Cyber42 – Transformational Leader

Wednesday, July 17 | 6:45–8:45 PM
LOCATION: **Columbia 5** (TERRACE LEVEL)
SPEAKER: **Kim Jones, Associate Instructor**

Practice your strategic decision-making skills in an engaging, fun, and collaborative environment. Cyber42 is a leadership simulation game that puts you in real-world scenarios that security managers, leaders, and officers find themselves facing daily. Prepare for real-world issues through uniquely crafted cybersecurity challenges.

ALUMNIGHT WORKSHOP OPTION 2

Threat Hunting and Criminal Infrastructure Analysis

Wednesday, July 17 | 6:45–8:45 PM
LOCATION: **Columbia 6** (TERRACE LEVEL)
SPEAKER: **Sean O'Connor, Course Author**

Come join SANS "FOR589: Cybercrime Intelligence" co-author Sean O'Connor as he walks you through one of our FOR589 labs. This two-hour hands-on workshop will dive into the complexities of cybercrime infrastructure. You'll explore the essential types of infrastructure indicators—atomic, behavioral, and computed—and learn how they can be used to uncover and understand cybercrime activities. Discover how domains, IP addresses, email accounts, and more play a crucial role as Atomic Indicators, and gain insight into the significance of infrastructure-as-a-service (IaaS) in identifying the ownership of these indicators. Through practical exercises, you'll apply a sophisticated fingerprinting methodology to not just identify but predict cybercrime behaviors, enhancing your ability to analyze and combat cyber threats. This workshop is ideal for those looking to deepen their understanding of cybercrime analysis in a real-world setting.

SANS@NIGHT

QUIC and Furious

Wednesday, July 17 | 7:15–8:15 PM
LOCATION: **Georgetown West** (CONCOURSE LEVEL)
SPEAKER: **Bojan Zdrnja, Certified Instructor**

In this presentation, we will dive deep (as much as time allows) into the QUIC protocol to see why it is so interesting. We will also analyze the three most used cases with HTTP/3, DoQ and SMB over QUIC to see both how attackers can (ab)use these protocols, and what defenders can do to identify and perhaps prevent such misuse.

BONUS SESSIONS

SANS@NIGHT

HA – Not "High Availability" but "Hunting Automation

Wednesday, July 17 | 8:15–9:15 PM

LOCATION: **Georgetown West** (CONCOURSE LEVEL)

SPEAKER: **Xavier Mertens, Associate Instructor**

When I'm teaching FOR610, we cover different malware analysis approaches from static analysis up to code analysis. We don't convert the "automated" analysis part. Why? Because the training goal is to help you to address malware that failed (or evaded) sandboxes. But it does not mean that automation is not interesting, it is… definitively! It's a great way to process a huge amount of malware samples and focus only on the "interesting" ones. In this talk, I'll show you how I'm doing my hunting activities, how I collect interesting samples from mail feeds, online resources and how files are processed/stored.

SPECIAL EVENT

5K Fun Run/Walk

Thursday, July 18 | 6:45–8:00 AM

LOCATION: **Heights Courtyard – Outdoors** (LOBBY LEVEL)

Lace up your sneakers, take in the stunning cityscape, and join fellow attendees and SANS staff for our 2nd Annual SANSFIRE 5K Fun Run/Walk. Whether you're a seasoned runner or just looking for some fresh air, this 5K is the perfect way to get in your steps before class. We will meet at 6:45 AM in the hotel lobby and start at 7:00 AM. The route will take us up Connecticut Avenue past the Smithsonian National Zoo. You are welcome to stay with a group or move at your own pace. Refreshments and light energizing bites will be provided afterwards.

SPECIAL EVENT

Open Mic Night

Thursday, July 18 | 7:00–9:00 PM

LOCATION: **Jefferson West** (CONCOURSE LEVEL)

Join us for a bit of fun and music! Let's gather in the evening for some instrument playing and karaoke-style singalongs! It will be a laid-back, no pressure get-together with fellow students and some SANS faculty and staff. Join us and sing along to classics like American Pie and Country Roads. If you are so inclined, bring your own instrument!

CYBER RANGES

Core NetWars Tournament

Thursday, July 18 | 6:30–9:30 PM

LOCATION: **Int'l Ballroom Center** (CONCOURSE LEVEL)

CYBER RANGES

Cyber Defense NetWars Tournament

Thursday, July 18 | 7:15–10:15 PM

LOCATION: **Int'l Ballroom East** (CONCOURSE LEVEL)

SANS@NIGHT

Implant, Phone Home

Thursday, July 18 | 7:15–8:15 PM

LOCATION: **Columbia 5** (TERRACE LEVEL)

SPEAKERS: **Jonathan Reiter, Certified Instructor & Kevin Ott**

This presentation delves into the strategic utilization of Windows HTTP libraries, WinInet and WinHTTP, for developing red team malware tools. Starting with an overview of these libraries, we highlight their pivotal roles in Windows networked applications, particularly in covert operations and data exfiltration scenarios. The WinInet API, primarily client-focused, and the server-optimized WinHTTP API are examined for their applicability in maintaining stealthy communications with command and control servers. A practical beaconing example in C++ will demonstrate each library's functionality in simulated red team scenarios. The session concludes with a case study on certificate pinning, essential for bypassing network security measures and enhancing the stealthiness of malware communications. Attendees will leave with a comprehensive understanding of how to choose and implement the right HTTP library to bolster the effectiveness and discretion of their malware initiatives.

CYBER RANGES

Core NetWars Tournament

Friday, July 19 | 6:30–9:30 PM

LOCATION: **Int'l Ballroom Center** (CONCOURSE LEVEL)

CYBER RANGES

Cyber Defense NetWars Tournament

Friday, July 19 | 7:15–10:15 PM

LOCATION: **Int'l Ballroom East** (CONCOURSE LEVEL)

SAVE THE DATE

SANSFIRE 2025 is returning to the Washington Hilton

July 14–19, 2025

Upcoming SANS Training Events

New York City Summer	New York City, NY	Hybrid	Jul 29–Aug 3
Nashville	Nashville, TN	Hybrid	Aug 5–10
Chicago	Chicago, IL	Hybrid	Aug 12-17
Virginia Beach	Virginia Beach, VA	Hybrid	Aug 19–30
Network Security	Las Vegas, NV	Hybrid	Sep 4–9
Offensive Operations – Baltimore	Baltimore, MD	Hybrid	Sep 16–21
Managing Security Risk – Live Online		Virtual (ET)	Sep 23–28
Stay Sharp: September		Virtual (CT)	Sep 30–Oct 4
Big Easy – New Orleans	New Orleans, LA	Hybrid	Sep 30–Oct 5
Northern Virginia: Special Edition	Dulles, VA	In Person	Oct 7–11
Dallas Fall	Dallas, TX	Hybrid	Oct 14–19
Rocky Mountain Fall	Denver, CO	Hybrid	Oct 21–26
Orlando Fall	Orlando, FL	Hybrid	Oct 28–Nov 2
Stay Sharp: November		Virtual (CT)	Nov 6–8
DFIRCON Miami: Special Edition	Coral Gables, FL	Hybrid	Nov 17–23
Golden Gate	San Francisco, CA	Hybrid	Nov 18–23
Seattle	Seattle, WA	Hybrid	Dec 2–7
Cyber Defense Initiative®	Washington, DC	Hybrid	Dec 13–18
Nashville Winter	Nashville, TN	Hybrid	Jan 13–18
Stay Sharp: January		Virtual (ET)	Jan 21–23
Cyber Security East: Jan		Virtual (ET)	Jan 27–Feb 1
New Orleans	New Orleans, LA	Hybrid	Feb 17–22
San Diego Winter	San Diego, CA	Hybrid	Feb 24–Mar 1