Tuesday, December 29 (all times are US Eastern Standard)	
Noon-12:15 pm	*Opening Remarks & Event Overview* **Lee Whitfield** **@lee_whitfield**, SANS Institute
12:15-12:45 pm	*Keynote* **Hacking Your Brain: Using Proven Psychology Techniques to Set and Smash Goals** How can you train your brain to be its best? Based on research and time-tested techniques from the field of cognitive psychology, Stef will help you learn the tricks and shortcuts to hacking your own personal supercomputer – your brain! **Stef Rand** **@techieStef**, Associate Consultant, Mandiant
12:50-1:20 pm	**Cybersecurity Career Success for Neurodivergent Individuals** **Rin Oliver** **@kiran_oliver**, Content Marketing Manager, Esper Cybersecurity is a daunting field for many to get into. For people who are neurodivergent, this field can be even more challenging. The goal of this presentation is to highlight some of the challenges and pain points that neurodivergent people may experience when getting started in their career in cybersecurity, breaking into the industry and open source after bootcamp graduation, starting or changing careers to InfoSec, and aims to to provide implementable solutions to these challenges that are designed to make a positive impact.
1:20-1:30 pm	Break
1:30-2:00 pm	**Mini Workshop: Attack & Defend** **Tyrone E. Wilson** **@tywilson21**, Founder, Cover6 Solutions; Organizer, D.C. Cybersecurity Professionals

	Tyrone will introduce and explain active enumeration, and how you can use a tool like Security Onion to monitor and analyze network traffic. It is also a great way to develop hands-on cybersecurity experience through constant practice. Mr. Wilson will provide instruction on various tool while simulating both attack and defend methodologies.
2:05-2:35 pm	**Cybersecurity is Like Ice Cream. There Are a Whole Lot of Flavors** **Chazz Scott** **@Mr_CaViar**, Incident Response Team Lead, National Geospatial-Intelligence Agency (NGA) Cybersecurity has a vast array of career choices that can range from technical roles like a malware reverse engineer to non-technical roles like a policy analyst. Come hear Chazz as he shares first-hand knowledge and experience of his unique journey within the cybersecurity field – from working with nuclear physicists on network simulation tools and supercomputers to incident response and protecting geospatial intelligence and satellites. No matter what your interests are, cybersecurity has a career choice that's perfect for you! Do you know what your favorite flavor will be?
2:40-3:10 pm	**Social Engineering: What It Is, Why Is Matters, and What You Can Do** **Susan Fowler**, Forensic Examiner II, Walmart Technology Social engineering is manipulating a person into divulging confidential information or taking an action. Since we live and work in an information-based society, these techniques can circumvent otherwise secure processes based on a person's natural tendencies or by playing on emotional responses. We will look at an overview of how it can happen and what you can do (or not do) to protect yourself.
3:10-3:20 pm	Break
3:20-3:50 pm	**Defending Critical Infrastructure** **Robert M. Lee** **@RobertMLee**, CEO, Dragos, Inc. Generally, we only think of the infrastructure – like the power grid – that's critical to our society when it isn't working as it should. But attackers are thinking about it all the time. Our electricity production and distribution, water treatment systems, factories that produce life-saving pharmaceuticals, and so many other critical pieces of our infrastructure depend on networked systems that are vulnerable to hacking. Luckily, people like Rob are also thinking about it, and working to defend it around the clock.

3:55-4:25 pm	**Move Along; Nothing to See Here… Or Is There?** **Domenica Crognale** **@domenicacrognal**, Cyber Security, ManTech; Instructor & Author, SANS Institute No matter what you want to do, for studying, working, or playing, you can find a great app. But what happens behind the scenes when you interact with an app? What information are you unknowingly sharing and leaving behind? We'll take a closer look at what you might be missing about your favorite mobile apps.
4:30-5:00 pm	**DNS: What It Is, What It Does, and How to Defend It** **Craig Bowser** **@reswob10**, Federal Director – Data Analytics, GuidePoint Security DNS is part of the foundation of the Internet. It lets humans set up connections and interactions between machines when surfing the web, sending tweets and snaps, paying out money via Venmo and Patreon, online gaming, streaming media, and all other Internet activity seen and unseen. But for all its importance, DNS can be incredibly fragile. Servers and hosts are still vulnerable to spoofing attacks and misdirections and denial of service. In fact, just recently, a new DNS cache poisoning attack was announced (along with a patch and defensive mitigations). DNS is constantly used by bad guys to carry out attacks, orchestrate C2 (command and control), and exfiltrate data. This talk will give an overview of DNS, DNSSEC, and the new protocols of DOH and DOT that may add security and privacy. Then we will talk about how DNS can be used maliciously and how defenders can protect their networks, their data, and their users.
Wednesday, December 30 (all times are US Eastern Standard)	
Noon-12:15 pm	**Ready, Set…Go – Introducing CyberStart America** **Lauren Kleczynski**, Programs Manager K-12, SANS Institute **James Lyne** **@jameslyne,** CTO, SANS Institute **Lee Whitfield** **@lee_whitfield**, SANS Institute
12:15-12:45 pm	**Cybersecurity Careers: Where Do You Fit?** **Rob Lee** **@robtlee**, Chief Curriculum Director and Faculty Lead, SANS Institute Listening to the talks on the first day of camp, you've probably noticed there are an overwhelming number of options when it comes to cybersecurity

	careers. How does ICS differ from DFIR? How do you go threat hunting? How is a security administrator different from a security engineer? And is it necessary to specialize? Rob Lee will help you map out the possible career paths.
12:50-1:20 pm	**Now What? – Pursuing Cybersecurity After Graduation** **Rushmi Hasham**, Director of Training and Certification, Rogers Cybersecure Catalyst, Ryerson University As you're learning, the career opportunities in cybersecurity are nearly limitless, as are the paths people have taken into the field. So how do you know which path is for you? After high school, should you go to college? Do you need a 2-year or 4-year degree, or no degree at all? Are certifications and experience more important than degrees? And how do you choose a great degree program, if that's the direction you want to take? There is no one-size-fits-all answer, but Rushmi will offer advice on what to consider to identify what's best for you.
1:20-1:30 pm	Break
1:30-2:00 pm	**Protecting Your Digital Identity** **Simbiat Ozioma Sadiq @Xymbiz,** Information Security Analyst, CEH; 2020 Top 50 Women in Cybersecurity (Africa) The internet is an indispensable utility. But our heavy reliance on the internet for everything from education to banking to healthcare to our social lives makes us vulnerable to hackers. How can you protect your information, identity, and reputation?
2:05-2:35 pm	**Starting a Career as an Ethical Hacker** **Phillip Wylie** **@PhillipWylie**, Co-Author, *The Pentester Blueprint: Starting a Career as an Ethical Hacker* Ethical hacking has become a much sought-after job by people in IT, cybersecurity, or those just trying to get into the industry. In this presentation, Phillip Wylie shares what is required to start a career as an ethical hacker. The presentation combines Phillip's experience as an ethical hacker and ethical hacking instructor to give attendees a guide on how to pursue a career as an ethical hacker. Phillip shares what has worked for his students and people that he has mentored over his years as an ethical hacker. This presentation covers the job role, as well as the knowledge and skills needed to become a pentester along with the steps to achieve them.

2:40-3:10 pm	**Can People Hack Nuclear Plants?** **Gabriel Agboruche** **@ICS_Gabe,** Senior Consultant- ICS|OT, Mandiant We always hear of hackers getting into personal email accounts, social media accounts, banks and even hospitals to steal data and cause disruptions. Are there hackers that go after bigger targets? Bigger target like Nuclear Plants?! How would a hacker get into a Nuclear Plant and what would they do once they got in? Have there been any recent big hacks that we've seen in the Nuclear industry? How do cybersecurity professionals protect plants against malicious hackers? Put on your "Evil Hardhats" and join this session for the answers to these questions and more!
3:10-3:20 pm	Break
3:20-3:50 pm	**Next-Level App Hacking: Threat Modeling for Better Attacks** **Alyssa Miller** **@AlyssaM_Infosec,** Hacker & Security Researcher Attempting to hack a web or mobile application can seem daunting. How do we even start? What kind of attacks should we test? Threat modeling is usually thought of as a tool that defenders use to help them protect their systems. In this session however, we'll talk about how threat modeling can be used by hackers in their penetration tests to make sure they're attacking the right things in the right ways. Never heard of threat modeling before? That's OK!! Using a real-life web application, you'll learn about threat modeling and how it helps you figure out what is most important, why it's important, and use that information to build better attacks.
3:55-4:25 pm	**Cracking the Mystery: Quantum Cryptography and The Future of Cybersecurity** **Rajvi Khanjan Shroff**, Founder, Project Cyber Ever wondered about quantum computing? Learn about the basics of quantum cybersecurity: the BB84 Protocol, quantum key distribution, and Post Quantum Cryptography--- simply explained! We will cover if and how quantum cryptography is so much different than the cryptography that we have currently, and how the cybersecurity space might look like in the future as a result.
4:30-5:00 pm	*Event Wrap-Up & Q&A* **Lee Whitfield** **@lee_whitfield**, SANS Institute

Speaker Biographies

Gabriel Agboruche @ICS_Gabe, Senior Consultant- ICS|OT, Mandiant
Gabriel Agboruche is a Senior ICS/OT Security Consultant working for Mandiant FireEye. Traditionally educated as an Electrical/Nuclear Engineer, Gabriel transitioned to the security field shortly after the outbreak of Stuxnet where his commercial nuclear plant environment went through a drastic security transformation thrusting him into the midst of the ICS Security.

Craig Bowser @reswob10, Federal Director – Data Analytics, GuidePoint Security
Craig Bowser is an Infosec professional with over 20 years of experience in the field. He teaches SEC555 for SANS. He has worked as an Information Security Manager, Security Engineer, Security Analyst and Information System Security Officer in DoD, DOJ and Dept of Energy areas and is currently a Director of Data Analytics at GuidePoint Security. He has some letters that mean something to HR departments. He is a Christian, Father, Husband, Geek, Scout Leader who enjoys woodworking, sci-fi fantasy, home networking, tinkering with electronics, reading, and hiking. And he has a to do list that is longer than the to do slots that are open.

Domenica Crognale @domenicacrognal, Cyber Security, ManTech; Instructor & Author, SANS Institute
Domenica currently serves as a senior mobile forensic analyst at ManTech International where she dissects the plethora of interesting data left behind by third-party mobile applications. In a former role, Domenica received recognition for assisting with the Osama Bin Laden media, a highlight of her career. She's also provided training to military special forces, the United States Coast Guard and other government agencies, and has tested and validated various mobile forensics utilities and provided security assessments for many mobile applications. Domenica is a co-author and instructor of SANS FOR585: Advanced Smartphone Forensics.

Susan Fowler, Forensic Examiner II, Walmart Technology
Susan Fowler is a forensic examiner at Walmart. She was in the first Women's Immersion Academy at SANS and has earned the GSEC, GCIH and GCIA while in the program. She has a BS in Applied Information Assurance and a MS in Computer and Information Systems.

Rushmi Hasham, Director of Training and Certification, Rogers Cybersecure Catalyst, Ryerson University
Rushmi Hasham is a strong advocate for identifying and implementing unique training and employment opportunities to increase the representation of women in Cybersecurity and other technology-related careers.
In her endeavour to increase diversity in cybersecurity, Rushmi recently joined Rogers Cybersecure Catalyst, as Director of Training and Certification. The Catalyst is a not-for-profit owned by Ryerson University. The Catalyst, launched September 2018, will empower Canadians and Canadian businesses to take the opportunities and tackle the challenges of cybersecurity by driving collaboration and excellence in training and certification; commercial incubation and acceleration; applied R&D; and public education and policy development in cybersecurity. Rushmi is also a serial social-entrepreneur, founding

2 businesses in the technology services industry. She firmly follows the doctrine that business has a responsibility in lifting communities, she has weaved that doctrine into her own companies and into her work at the Catalyst. One of Rushmi's ventures has been selected as Canada's Top 50 Growth Businesses.
Rushmi lives in Mississauga with her husband Jeff and their two daughters, Natalie and Nicole.

Rob Lee @robtlee, Chief Curriculum Director and Faculty Lead, SANS Institute
Rob Lee is the Chief Curriculum Director and Faculty Lead at SANS Institute and runs his own consulting business specializing in information security, incident response, threat hunting, and digital forensics. With more than 20 years of experience in digital forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response, he is known as "The Godfather of DFIR". Rob co-authored the book *Know Your Enemy, 2nd Edition*, and is course co-author of FOR500: Windows Forensic Analysis and FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics.

Alyssa Miller @AlyssaM_Infosec, Hacker & Security Researcher
Alyssa Miller is a hacker, security advocate, professional, and public speaker with over 15 years of experience in cyber security. She believes that in today's inter-connected world, protecting privacy and building trust with secure systems are critical to protecting our way of life. As a result, she discusses real-world issues that that affect people both within and outside the security community.

Rin Oliver @kiran_oliver, Content Marketing Manager, Esper
Rin is a Platform Evangelist at Esper. They enjoy discussing all things open source, with a particular focus on diversity in tech, improving hiring pipelines in OSS for those that are neurodivergent, and removing accessibility barriers to learning programming. Rin is also a Member of Kubernetes, a contributor to Spinnaker, involved in the Kubernetes Contributor Experience SIG, and is a Storyteller on the Kubernetes Upstream Marketing Team. When not immersed in all things OSS and cloud-native, they can be found hanging out with their wife and pets, making candles, cooking, or gaming.

Chazz Scott @Mr_CaViar, Incident Response Team Lead, National Geospatial-Intelligence Agency (NGA)
Charles (Chazz) Scott is a published writer, keynote speaker, and a Cyber Defense Technologist. He holds both a Bachelor of Science degree in Computer Science and a Master of Science degree in Cyber Security from Hampton University. Chazz has worked alongside some of the most brilliant minds in national security including nuclear physicists at the National Nuclear Security Administration's Lawrence Livermore National Laboratory (LLNL), what many consider to be "the smartest square mile on Earth." As a Cyber Defense Analyst at the Nuclear Lab, Chazz contributed to developing a large-scale network web simulation capability to assist in risk-based cyber defensive strategies to counter enterprise-level

cyber threats and increase global network situational awareness. His contributions allowed researchers to effectively model network simulations using three high-performance computing (HPC) clusters which include Cab, Hera, and Catalyst. All three supercomputers were previously listed in the Top500 List of the fastest computers in the world. Currently, Chazz works for the National Geospatial-Intelligence Agency (NGA) as a Cyber Defense Engineer as the Incident Respond Team Lead in the Cybersecurity Operations Cell (CSOC) responsible for defending and responding to global cyber threats to ensure the protection of our nation's satellites in space and geospatial imagery to provide to the Intelligence Community, Department of Defense, and policymakers on Capitol Hill. Prior to NGA, Chazz held positions at the National Nuclear Security Administration's Lawrence Livermore National Laboratory (LLNL), Defense Intelligence Agency (DIA), the Defense Information Systems Agency (DISA), the National Institute of Standards of Technology (NIST) – Cybersecurity Division, and Accenture. In addition, his research has been published in numerous cybersecurity peer-reviewed journals, including the Scientific Research Publishing (SCIRP), Journal of Computer Science & Communications and The Institute of Electrical and Electronics Engineers (IEEE). Chazz has been named a BE Modern Man of 2019 by Black Enterprise Magazine, selected as Top 30 Under 30 by HBCU Buzz, and a recipient of The Positive People Award by The Baltimore Times. Chazz is a monthly contributing writer to The Baltimore Times.

Simbiat Ozioma Sadiq @Xymbiz, Information Security Analyst, CEH; 2020 Top 50 Women in Cybersecurity (Africa)

Simbiat is an information security officer for a financial institution in Nigeria. She derives passion from being an awareness advocate. Simbiat currently leads the operations team for NoGoFallMaga - An initiative of young people driven by their passion to create cybersecurity awareness to the grassroot. Simbiat was nominated as part of the Top 50 Women in Cybersecurity (Africa) for her amazing work in inspiring more women into the field and contributing to Africa's cybersecurity ecosystem. Simbiat blogs about cybersecurity in her leisure time.

Rajvi Khanjan Shroff

Rajvi Khanjan Shroff is a 10th grader with a passion for cybersecurity! With digital security becoming increasingly important, it is critical that we start to educate ourselves and become cyber-smart, and this should start with today's youth having the opportunity to take action on this regard internationally. Thus, Project Cyber was born. With this initiative, she hopes that teens all around the world will have the ability to be a part of a strong digital community centered around infosec, the first of its kind.

Lee Whitfield @lee_whitfield, SANS Institute

Lee is a digital forensic consultant and analyst for his own company, 337 Forensics. He has covered a wide array of situations during his time as a forensic investigator, everything from child abuse, intellectual property theft, attempted murder, and much more. One of his greatest successes was his work on reverse engineering Volume Shadow Copies, which had been a stumbling block for forensic investigators. Due to Lee's work and innovation, access and time to locate files were greatly reduced,

essentially allowing a forensic investigator to view the computer's contents from days, weeks, or even months before, including old or deleted files. Lee is a Senior Technical Adviser for the SANS Research and Operation Center and hosts the Forensic 4:cast podcast and awards event.

Phillip Wylie **@PhillipWylie**, Co-Author, *The Pentester Blueprint: Starting a Career as an Ethical Hacker*
Phillip Wylie is a Lead Curriculum Developer at Point3 Federal, Adjunct Instructor at Dallas College, and The Pwn School Project founder. With over 23 years of experience in information technology and cybersecurity, Phillip has spent the past 8.5 years spent as a pentester. His passion for mentoring and education inspired him to teach and found The Pwn School Project a monthly educational meetup focusing on ethical hacking and cybersecurity. Phillip teaches Ethical Hacking and Web Application Pentesting at Dallas College. He is a published author and co-author of the book “The Pentester Blueprint: Starting a Career as an Ethical Hacker” published by Wiley Publishing.