We strive to present the most relevant, timely and valuable content. As a result, this agenda is subject to change. Please check back frequently for changes and updates.

Monday, November 13	
9:00-9:15 am	*Welcome & Opening Remarks* **Ed Skoudis, Fellow, SANS Institute**
9:15-10:00 am	*Keynote* **Hack Your Head** We all want to be better at what we do. We all want to focus on the things in our careers that are the most fun. Unfortunately, we often prioritize useless activities over the fun or important ones. We want more time to hack, more time to learn, and more time for family and friends; but there we only have so many hours in a day. In this talk, you will learn how to be more efficient and save time for both yourself and those around you. Hack your head and your schedule for a more productive, efficient, and fun life. **Tim Medin (@TimMedin), Founder, Red Siege; Certified Instructor, SANS Institute**
10:00-10:35 am	**How To Defend Against Penetration Testers...and Win** Do you believe you have what it takes to secure a network against a penetration test? Attend this talk to find out how you can be successful against penetration tests and real-world attackers. Most penetration tests are too EASILY successful; let's work together to change this! Many believe that breaking into a company's network requires custom exploits, nation-state level backdoors, and super powers. In fact, most of the time it's about guessing passwords and exploiting very well-known (and fixable) conditions in your network. This talk will guide you through securing your network the smart way, focused on closing those tried and true holes commonly exploited, but often left open by defenders. Don't think this will be easy. It's not. Attackers have a clear advantage and the defensive measures proposed require work more so than products. It may require you change things that impact culture and challenge notions such as "but, that's the way we've always done it." It's okay, we'll coach you on some communications as well! In the end, you'll learn it's not about winning; it's about getting better. If you can learn from penetration testers, that knowledge is extremely valuable. However, this talk is going to tell you what most penetration testers have in common and how to fix your architecture, culture, and behavior, resulting in so much win. **Paul Asadoorian (@securityweekly), Security Weekly, CEO; Offensive Countermeasures, CEO**

10:35-11:00 am	**Networking Break and Vendor Expo**
11:00-11:35 am	**Using the Metasploit Hardware Bridge to Attack Non-Ethernet Systems** This talk will cover usages of the Metasploit Hardware Bridge and how to integrate it into existing hardware platforms or new devices you may be creating. We will also take a tour of some of the newer tools and modules written for the hardware bridge to date. These may include vehicle hacking, RF/SDR Tools, and whatever new modules have been recently released. After attending this talk, you will understand: what the Metasploit Hardware Bridge is and how to use it; the most recent tools and techniques for using the hardware bridge; the technical foundations for the HWBridge so you can implement it in new custom projects. **Craig Smith, Research Director of Transportation Security, Rapid7; Founder, Open Garages**
11:35 am – 12:10 pm	**Searching the Void - IPv6 Network Reconnaissance** The entire IPv4 Internet can be scanned in under 10 minutes. To scan the entire IPv6 internet, it would take longer than livable lifetime of Earth. Security professionals and organizations are going to have to learn to handle networks of unimaginable scale. Fortunately, there are some tricks and best practices that pen testers can use to overcome the sheer volume of possible IPv6 addresses. This talk will cover methods to substantially shrink the number of IPv6 addresses one needs to scan and blue team-inspired techniques to find potential entry points on an IPv6 network. **Kevin Tyers (@WarOnShrugs), Information Security Engineer**
12:10-1:30 pm	**Networking Luncheon**
1:30-2:05 pm	**Being Offensive in the Workplace** Do you get excited about talks at hacker conferences, only to return to your office feeling like you have too few resources to implement anything you learned? We'll be discussing ways to start implementing internal attack and penetration programs to let you have fun in the workplace while providing value to your organization. We will start with small tasks that can be easily introduced for fast and inexpensive wins, and expand into ways to sell more complicated engagements to management. From small hacking demos in security awareness presentations, to phishing slack and hipchat, or even full scale physical penetration tests, we've got something doable for any security practitioner in nearly any environment. **Derek Rook (@_r00k_), Penetration Tester**

2:05-2:40 pm	**Introduction to Reverse Engineering for Penetration Testers** Penetration testers are busy, and the idea of performing reverse engineering, debugging, and custom exploitation can seem unrealistic given typical time constraints and the skills required. As with most skills, the more experienced you become, the more likely you can tie them into a test. Much of the work can be automated given the right tools, allowing you to focus on other tasks. Join me as I introduce disassembly and debugging. We will cover tools such as IDA and radare2 for disassembly, common debuggers such as WinDbg, Immunity, and x64dbg, and how scripting can help speed up your work. **Stephen Sims, @Steph3nSims, Senior Instructor, Author SEC660 and SEC760, SANS Institute**
2:40-3:00 pm	**Networking Break and Vendor Expo**
3:00-3:35 pm	**2> 1: Teaming Up for Social Engineering Adventures** As penetration testers we all want to provide our clients with valuable insights about their environments. This case study of a pen test performed against a health care organization describes how I teamed up with a technical colleague during onsite social engineering in order to further each of our testing objectives. It gave the client stakeholder "a more complete picture" than previous tests where social and technical testing aspects were performed well but separately. Our collaboration influenced the pretexts that were developed, the exploits/devices we used, and how we executed them. The presentation will illustrate the handoffs between the social and technical aspects of each approach we took. Attendees will learn about identifying opportunities for collaboration, taking advantage of what your collaborators have to offer, and having fun while adding value for your client. **Jen Fox (@j_fox), Sr. Security Consultant, VioPoint**
3:35-4:10 pm	**Emulating Adversary Tactics - Safely - in Industrial Networks; or, How Not to be an A**hole in ICS** Industrial networks are awesome. Industrial control systems (ICS) creating power, moving robot arms to make other machines, drilling for oil...what could be cooler? It turns out operating in these environments without killing someone is also cool. This presentation will talk through best practices of pen testing industrial environments. A heavy focus will be placed on red teaming through the emulation of adversary tactics that have worked against the ICS community before. Expect to learn what is media hype and what is extremely effective, and how to operate in a way that takes your skills and makes them valuable to an awesome community. **Robert M. Lee** (**@robertmlee**), Founder & CEO, Dragos Inc., Certified Instructor, Author, FOR578 & ICS515, SANS Institute

4:10-4:45 pm	**Honey, Please Don't Burn Down Your Office: Fun with Smart Home Automation** In the last 12 months, Ed Skoudis has been on a tear adding new automation features to his office. Some are practical, others are whimsical and weird. All of them provided valuable learning opportunities that Ed would love to share. This talk will describe some of the new technologies he's been experimenting with and the lessons he's learned, including: • Alexa versus Siri: Development tips for each environment and how to make them work together • Amazon Voice Services: High-quality, real-time, cloud-based voice synthesis for free • The Raspberry Pi Zero as a development platform • The Intel NUC as a development platform • Integrating animatronic toys into your ecosystem: How creepy is too creepy? • Do's and don'ts of home Tesla coils, Geissler tubes, and other high-voltage apparatus • Tips for keeping your mind fresh with new dev projects - Security implications of all of this stuff Where is this all headed? When does Skynet reveal its big plan? This lively talk will cover a lot of ground, but also include specific, practical advice for keeping your technical skills sharp while having fun. **Ed Skoudis, Fellow, SANS Institute**
5:30-8:30 pm	**Paint the Town Red** All work and no play makes for dull pen testers! We're breaking out for a night on the town at a local establishment. There will be snacks, drinks, and games for everyone. But don't worry; we know you need to keep your skills sharp, and you'll have an opportunity to show off and trash-talk as you work through a brand-new, custom-made Counter Hack challenge developed just for Summit attendees!

Tuesday, November 14	
9:00-9:45 am	*Keynote* **Propelling Your Pen Test Career into the Next Decade** We live in the golden age of information security, where mind-boggling breaches and pernicious malware regularly make their way into mainstream media. Never before has the role of the infosec pro been more important to top-level executives, creating tremendous opportunities for us to develop our careers for top compensation, exciting opportunities, and leadership promotions. Join Joshua Wright as he examines some of the many opportunities you can use to propel your pen test career into the next decade, with practical recommendations on what you can do to meet your career development goals. **Joshua Wright (@joswr1ght), Director, Counter Hack; Senior Instructor, SANS Institute**
9:45-10:20 am	**Beyond Scanning: Delivering Impact Driven Vulnerability Assessments** Vulnerability assessment is more than simply clicking "print" on your scanner of choice. Moving beyond a stagnant checklist-limited approach and modeling assessments after the attacker's perspective is a crucial component of any transformational vulnerability management program. Together, let's explore the world of vulnerability dominance. In this talk, we will take action on an enterprise scale by leveraging force multiplying tools and techniques like PowerShell. Instead of writing off the bulk of your assessment time managing and churning through untold quantities of data, let's target for impact. By exploring methods to deconstruct logistical precursors and integrate adversarial threat modeling, we can skip the noise and focus in on true threat signals. Using a seven-step vulnerability assessment model to guide our keystrokes, we can ensure repeatable value while delivering elite engagements. **Matt Toussain (@0sm0s1z), Founder, Spectrum Information Security; Instructor, SANS Institute; Active Duty Officer, US Air Force**
10:20-10:45 am	**Networking Break and Vendor Expo**
10:45-11:20 am	*Panel* **What the Heck is Purple Teaming, Really?** **"**Purple Teaming." The phrase gets thrown around a lot lately, but its meaning and implications are often squishy. Some people claim Purple Teaming can significantly increase the value of Red Team and Blue Team activity, others say that Purple Teaming is just another name for what we've always done with Red and Blue teams, and still others dismiss it as a silly fad. This panel will explore the real deal behind Purple Teaming and provide practical lessons in how it can be applied to improve Red and Blue lives and effectiveness. **Moderator: Ed Skoudis, Fellow, SANS Institute** **Panelists:** • **Jim Mc Murry (@jmcmurry), CEO and Founder, Milton Security Group**

	• **Lee Neely (@lelandneely), Senior Cyber Analyst, Cyber Security Program, Lawrence Livermore National Lab** • **Joe Schottman, (@JoeSchottman), Senior Cyber Threat Analyst, BB&T** • **Alissa Torres (@sibertor), Certified Instructor, SANS Institute**
11:20am-12:15 pm	**Escaping Alcatraz: Breaking out of Application Sandboxed Environments** Application sandboxing has become extremely popular. This technology makes it easier to manage a network environment easily, allows an administrator to grant access to specific applications without giving an entire desktop, and gives users remote access to company resources. There is a false sense of security with this model though. This presentation will explore various ways of breaking out of these environments to gain a foothold into a network at various levels of security as well as discuss some mitigation strategies. **Kirk Hayes (@kirkphayes), Senior Security Consultant, Rapid7**
12:15-1:30 pm	**Lunch**
1:30-2:05 pm	**Lies, Damn Lies, and Pen Tests** Penetration testing has been "normalized" as a legitimate tool in the arsenal of security practitioners, but I often find myself wondering if we've really given much thought to the practical value it represents. What, exactly, is the bar we're attempting to raise through pen testing, and are we actually raising it? Too many times, when we re-test a network, we find the same class of problem still exists. What is going wrong, can we fix it, and if so, how? **Tom Liston (@tliston), Senior Security Consultant, DarkMatter, LLC - Abu Dhabi**
2:00-2:35 pm	**WAF-aiki: Pen Test Techniques Against a Web Application Firewall** Web Application Firewalls introduce a new layer of defense, providing additional levels of protection and notification to the defender. As an attacker, the successful pen tester must incorporate the presence of a WAF into their test plan. This talk will cover several topics such as actively and passively identifying when a WAF is in the test path, how the presence of a WAF changes the rules for both the attacker and the defender, and how the WAF can be abused to improve the map of the testable surface. A survey of existing tools specific to WAF engagements will be covered, as well as a bespoke tool created to take advantage of a WAF-protected environment. **Greg Owen (@gowenfawr), Senior Principal Security Engineer, Vantiv**
2:35-3:10 pm	**Signal Safari: Investigating RF Controls with RTL-SDR** Cranes, trains, theme park rides, sirens, and …ceiling fans? Modern RF protocols have made secure wireless communications easier to implement, but there's still a horde of simpler RF control systems in the wireless world around us. Lucky for us, the onset of affordable Software Defined Radios (SDRs) means that exploring these devices is easier than ever! In this talk, we'll examine capturing and

	understanding basic RF control signals from a common household controller with the affordable RTL-SDR so you can start your own investigations. With a little knowledge of these protocols we can better explain what makes them risky to the environments we assess, practice thinking in the offensive mindset, and have some fun examining the signals around us. **Katie Knowles (@_sigil), Security Consultant, MWR Infosecurity**
3:10-3:40 pm	**Networking Break and Vendor Expo**

3:40-4:15 pm	**Privesc Playground** As organizations increase security postures, it's increasingly likely that we'll gain initial access as an unprivileged user. Sure, metasploit has "getsystem," but what happens when that doesn't work? Better yet, what if you're on Linux? In this session, Jake will walk you through hands-on demonstrations of privilege escalation, using the techniques that he uses most in his engagements. We initially wanted to turn this into a drinking game ("drink every time Jake gets root"), but after reviewing the presentation we decided that was just irresponsible. **Jake Williams (@MalwareJake), Founder, Rendition Infosec; Certified Instructor & Course Author, SANS Institute**
6:30-9:30 pm	**Core NetWars Tournament** CORE NetWars Tournament 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.

Speaker Biographies

Paul Asadoorian, Security Weekly, CEO; Offensive Countermeasures, CEO
Paul Asadoorian spent time “in the trenches” implementing security programs for a lottery company and then a large university. Paul is offensive, having spent several years as a penetration tester. He is the founder of the Security Weekly podcast network, offering several freely available shows on the topics of information security and hacking. As Product Evangelist for Tenable Network Security Paul built a library of materials on the topic of vulnerability management. In 2007 Paul co-authored a book called “WRT54G Ultimate Hacking”, and since then has been passionate about the security of IoT. When not hacking together embedded systems/IoT devices (or just plain hacking them) or coding silly projects in Python, Paul studies Kung Fu (Shaolin Long Fist) and, of course, watches Kung Fu movies.

Jen Fox (@j_fox), Sr. Security Consultant, VioPoint
Jen Fox is a Sr. Security Consultant at VioPoint. She holds the DEF CON 23 Social Engineering Capture The Flag black badge.When she isn’t asking people for their passwords or gaining unauthorized access to secured areas, she provides awareness training, risk management and compliance services for clients.

Kirk Hayes (@kirkphayes), Senior Security Consultant, Rapid7
Kirk is a Senior Security Consultant with Rapid7. Kirk has presented at DerbyCon, BSides Las Vegas, Bsides Boston, and BlackHat Tools arsenal. Kirk has written various tools to help penetration testers which can be found at Rapid7’s MooseDojo Github page (https://github.com/MooseDojo/myBFF) and Kirk’s personal Github page (https://github.com/l0gan).

Katie Knowles (@_sigil), Security Consultant, MWR Infosecurity
Katie Knowles is a Security Consultant with MWR Infosecurity. Before her switch to offense, she designed and managed enterprise security solutions at SpaceX. Katie enjoys good time spent on good projects, and loves sharing

newfound knowledge as much as she does learning it. She holds GPEN certification, and received her BS in Engineering from RIT.

Tom Liston (@tliston), Senior Security Consultant, DarkMatter, LLC - Abu Dhabi
Tom Liston is a Senior Security Consultant at Dark Matter, a security consulting firm in the UAE. He is also a Handler for the SANS Institute's Internet Storm Center and co-author of the book Counter Hack Reloaded. Since it began publishing its "Sexiest Man Alive" issue, People Magazine has consistently overlooked Mr. Liston with what can only be described as a blatantly good taste.

Jim Mc Murry (@jmcmurry), CEO and Founder, Milton Security Group
Jim Mc Murry is an accomplished technologist with an entrepreneurial mindset and more than 23 years of combined experience in security, information technology, telecommunication, networking, management and software development.

Tim Medin (@TimMedin), Founder, Red Siege; Certified Instructor, SANS Institute
Tim Medin is the founder of Red Siege, a company focused to adversary emulation and penetration testing. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim is an experienced international speaker, having presented to a organizations around the world. Tim is also the creator of the Kerberoasting, a technique to extract kerberos tickets in order to offline attack the password of enterprise service accounts. He is also a project lead of the Laudanum project.

Lee Neely, CISSP, CISA, CISM, CRISC, GMOB, GPEN, CCUV , Cyber Security Program, OMBUDS , Lawrence Livermore National Lab
Lee Neely is a Senior Cyber Analyst at LLNL, SANS Mentor and Analyst paper author. He is also the IT Director for the ISC2 East Bay Chapter and Board Treasurer for the Uncle Credit Union. His areas of expertise include mobile device and new technology security.

Greg Owen (@gowenfawr), Senior Principal Security Engineer, Vantiv
With over 20 years' experience in the computer industry, Greg has done a little bit of everything – IT, programming, architecture, security. He brings a holistic approach to whatever he's doing, whether it's defense or offense. He enjoys speaking to teach as well as learn.

Derek Rook (@_r00k_), Penetration Tester
Derek has been all over the map when it comes to technology. Having done everything from helpdesk and desktop support to web development and systems engineering, he finally found a home in security. When not building and running internal pen test programs at the office he can be found streaming instructional CTF and Boot2Root videos online. Derek holds several certifications including GWAPT, GNFA, and OSCP.

Joe Schottman, (@JoeSchottman), Senior Cyber Threat Analyst, BB&T
Joe Schottman works at BB&T as a Senior Cyber Threat Analyst in the group that handles pen testing, app sec, and purple team exercises.

Craig Smith, Research Director of Transportation Security, Rapid7; Founder, Open Garages
Craig Smith is the Research Director of Transportation Security at Rapid7 as well as the Founder of Open Garages. Open Garages is a distributed collective of performance tuners, mechanics, security researchers and artists. Craig is also the author of the *Car Hacker's Handbook* and runs a security consulting firm that specializes in automotive reverse engineering. Craig has developed many open source utilities to teach CAN bus to students and well as security penetration tools that can uncover vulnerabilities in vehicle and diagnostic systems. Craig is the core author of Metasploit's Hardware Bridge and has worked in the security field for over 20 years with the last 5 years focused on automotive.

Matt Toussain (@0sm0s1z), Founder, Spectrum Information Security; Instructor, SANS Institute; Active Duty Officer, US Air Force

Matthew Toussain is an active-duty Air Force officer and the founder of Spectrum Information Security, a firm focused on maximizing the value proposition of information security programs. As an avid information security researcher, Matthew regularly hunts for vulnerabilities in computer systems and releases tools to demonstrate the effectiveness of attacks and countermeasures. He has been a guest speaker at many conference venues, including DEFCON, the largest security conference in the world. After graduating from the U.S. Air Force Academy, where he architected and instructed the summer cyber course that now trains over 400 cadets per year, Matthew served as the Senior Cyber Tactics Development Lead for the U.S. Air Force. He directed the teams responsible for developing innovative tactics, techniques, and procedures for offensive operations as well as for cyber protection teams (CPT). Later, as a member of the 688th Cyber Warfare Wing he managed the Air Force's transition of all 18 CPTs to fully operational capability. As a founding member of Spectrum, Matthew regularly performs a wide variety of information security services. He earned his master's degree in information security engineering as one of the first graduates of the SANS Technology Institute and supports many national and international cyber competitions including the CCDC, Netwars, and the National Security Agency's Cyber Defense Exercise as a red team member and instructor.

Kevin Tyers (@WarOnShrugs), Information Security Engineer

Kevin Tyers is a long time technology nerd that loves Python, Security, and Networking. He is excited to see the recent uptick in IPv6 adoption rate. He has worked in many different positions, but currently finds himself on the Security Threat Intelligence team at a large financial technology company.

Jake Williams (@MalwareJake), Founder, Rendition Infosec; Certified Instructor & Course Author, SANS Institute

Jake is a SANS Instructor and course author. He founded Rendition Infosec, where he runs a security operations center. He also provides incident response, threat intelligence. and other infosec consulting services. Jake is proudly a certified Shadow Brokers protagonist and according to them “a former EQUATION GROUP member.”